OnCell G4300-LTE4 Series User Manual

Version 1.0, July 2023

www.moxa.com/products

OnCell G4300-LTE4 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 OnCell G4300-LTE4 Industrial LTE Cat 4 Secure Cellular Router Series. These all-in-one Firewall/NAT/VPN secure cellular routers are designed to connect Ethernet and serial devices to the Internet with network IP security.

Overview

As the world's network and information technology matures, cellular connectivity is becoming a major communications interface in many industrial communications and IoT applications.

The OnCell G4300-LTE4 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 cellular 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 ETC systems in transportation.

To enhance industrial reliability, high-level EMS and wide-temperature support give the OnCell G4300-LTE4 Series the highest level of device stability for any demanding environment. In addition to dual-SIM GuaranLink, the OnCell G4300-LTE4 Series supports WAN network redundancy to ensure uninterrupted connectivity. The OnCell G4300-LTE4 Series also comes with a 3-in-1 serial port for serial communication over LTE cellular networks to enable data exchange with serial/Ethernet devices.

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
- DIN-rail mounting kit (attached to the Industrial Secure Router's rear panel by default)
- Quick installation guide (printed)
- Warranty card

Features

- High-performance global LTE router with full GbE ports
- All-in-one firewall/NAT/VPN/router/switch
- Powerful power management tools for wake-up scheduling
- Visualize OT security with the MXsecurity management software
- Secure remote access tunnel with VPN
- GuaranLink technology and redundant SIMs for reliable cellular connectivity
- Easy network setup with Network Address Translation (NAT)
- Precise GNSS for location-based application
- Security features based on IEC 62443/NERC CIP
- Supports secure boot for checking system integrity
- -40 to 75°C operating temperature range (-T model)

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.

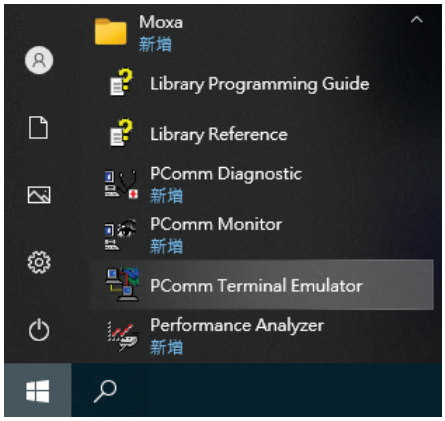
Before running PComm Terminal Emulator, use a USB-C-to-DB9-F (or USB-C-to-DB25-F) cable to connect the Industrial Secure Router's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up).

NOTE

We recommend using the Moxa CBL-USBCF9-GY-150 console cable, which can be purchased separately.

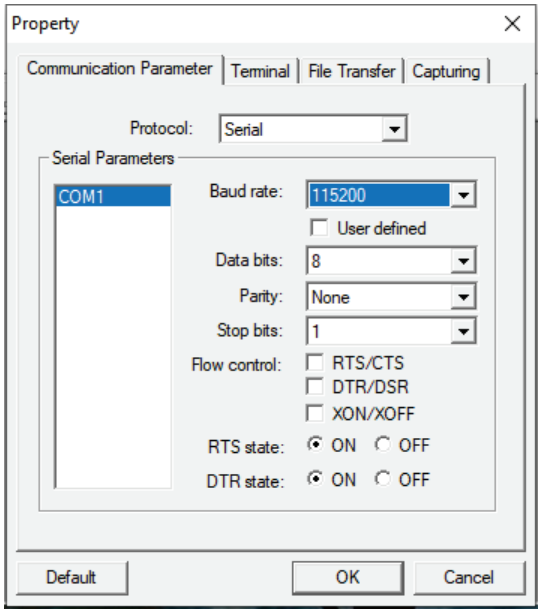
After installing PComm Terminal Emulator, perform the following steps to access the RS-232 console utility.

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

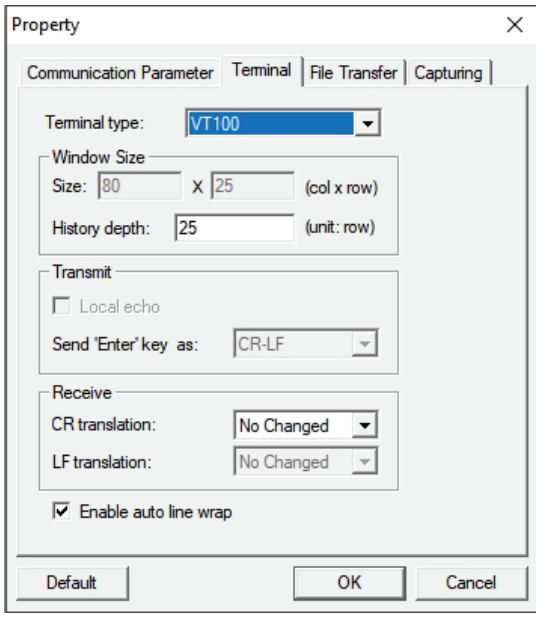


2. Click **Open** in the Port Manager menu to open a new connection.

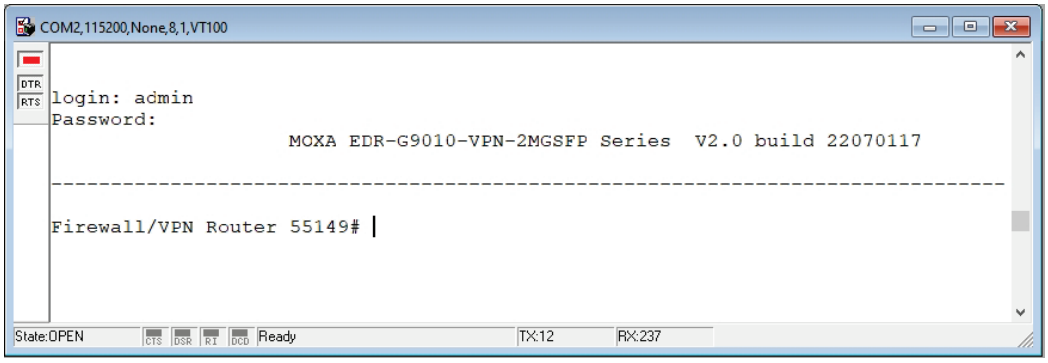
3. The **Communication Parameter** page of the **Property** window will appear. Select the appropriate COM port from the **Serial Parameters** list and configure the following values:
Baud Rate: 115200
Data Bits: 8,
Parity: None
Stop Bits: 1.



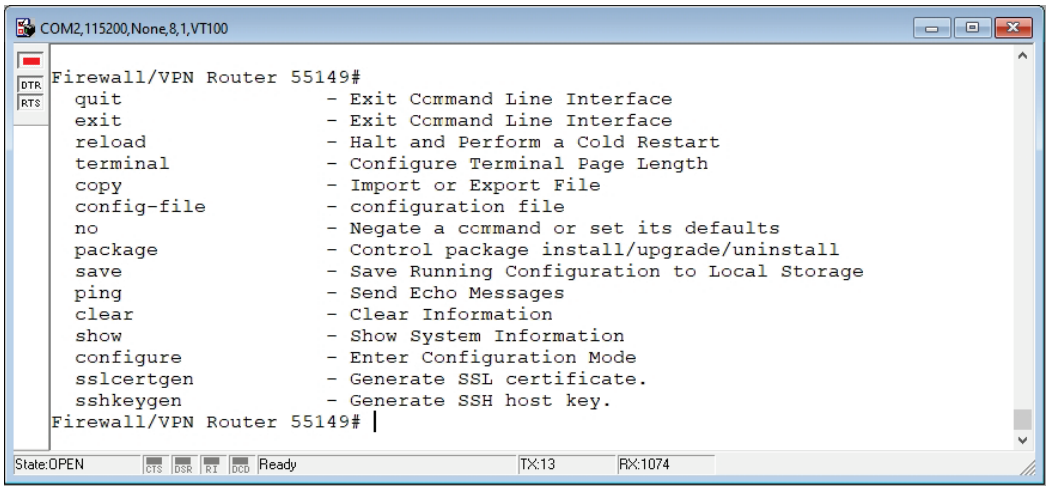
4. Click the **Terminal** tab, select **VT100** for Terminal Type, then click **OK** to continue.



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 device'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

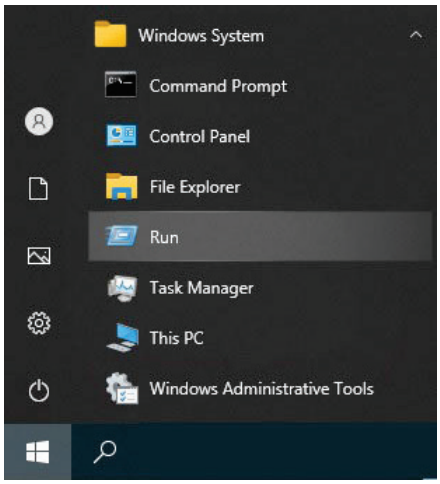
Before accessing the console utility via Telnet, first connect one of the Industrial Secure Router's RJ45 Ethernet LAN ports to your Ethernet LAN, or directly to your PC's Ethernet card (NIC). You can use either a straight-through or cross-over Ethernet cable.

NOTE

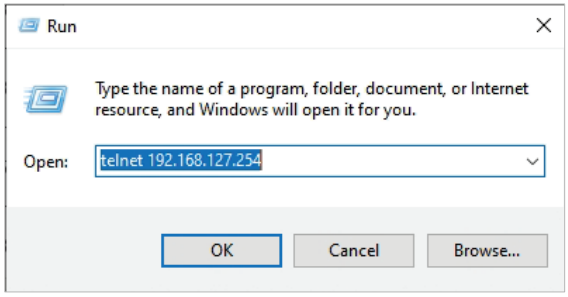
The Industrial Secure Router's default LAN IP address is 192.168.127.254.

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

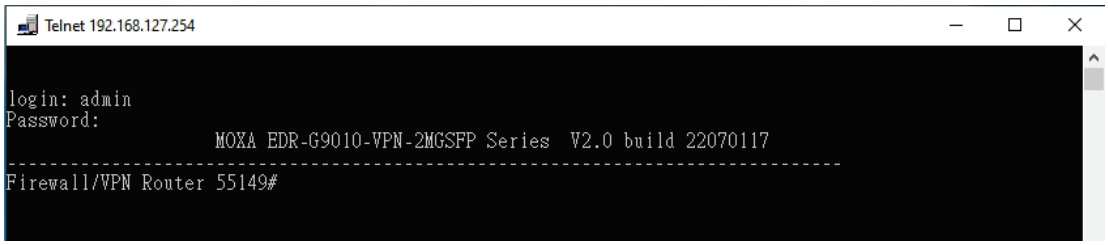
1. Click **Start > Windows System > Run** from the Windows desktop.



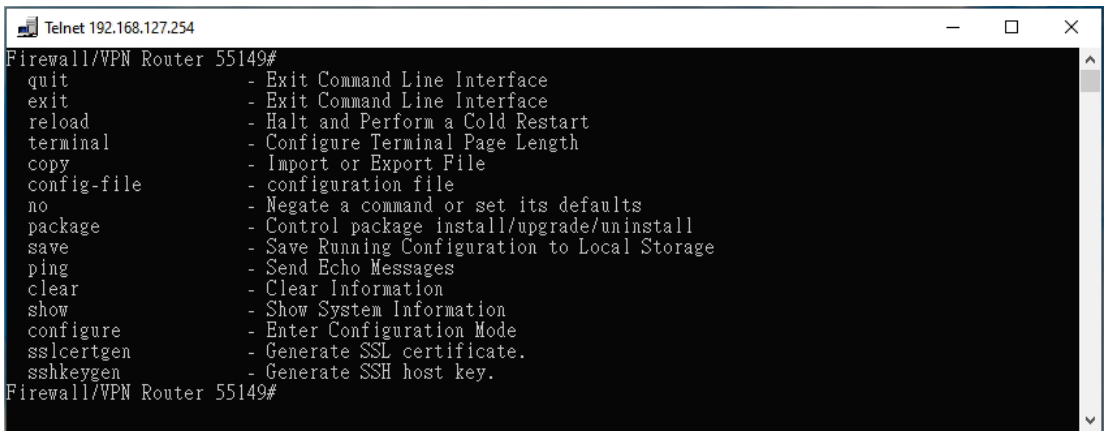
2. Enter "telnet 192.168.127.254" and click **OK** to connect to the Industrial Secure Router's IP address. You may also issue the Telnet command from the MS-DOS prompt.



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

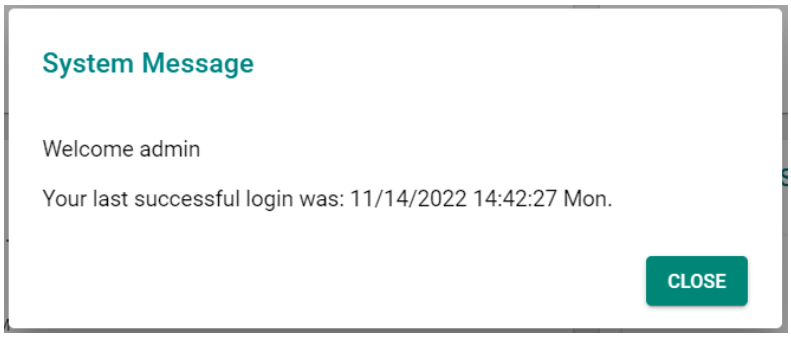
The Industrial Secure Router's default LAN IP address is 192.168.127.254.

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

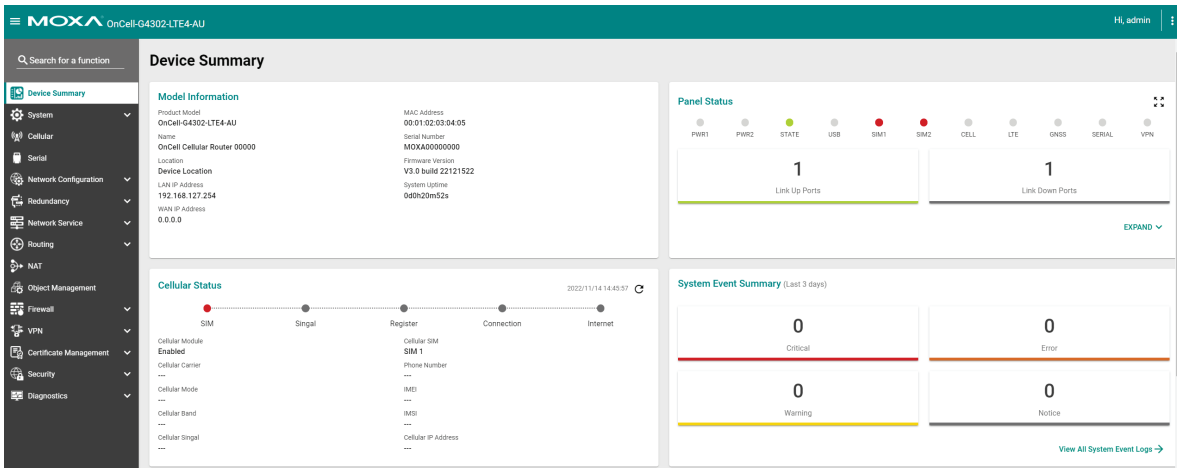
1. Open a web browser and type the Industrial Secure Router's LAN IP address (**192.168.127.254**) in the address bar and press **Enter**.

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.

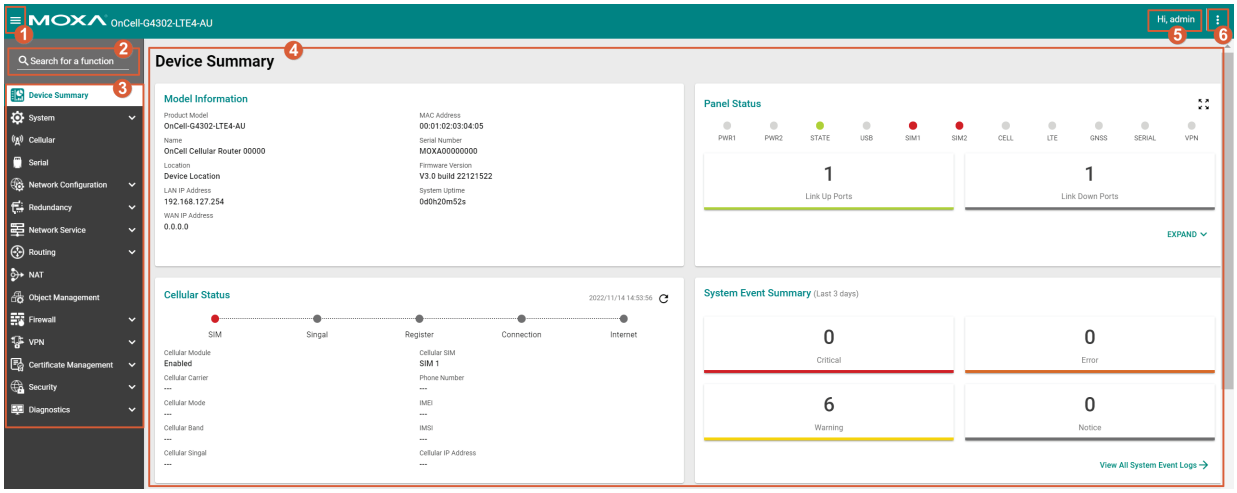


3. Device Summary

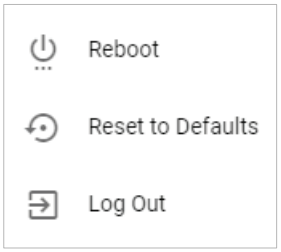
In this chapter, we explain how to access the Industrial Secure Router's configuration options, perform monitoring, and use administration functions. There are three ways to access these functions: (1) RS-232 console, (2) Telnet console, and (3) web browser.

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.

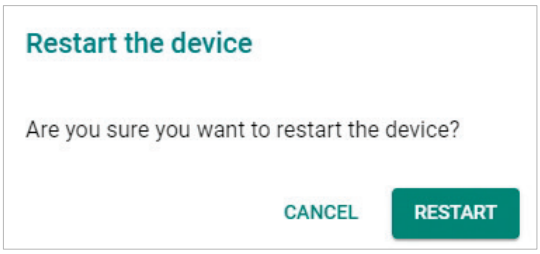
Function Introduction



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.

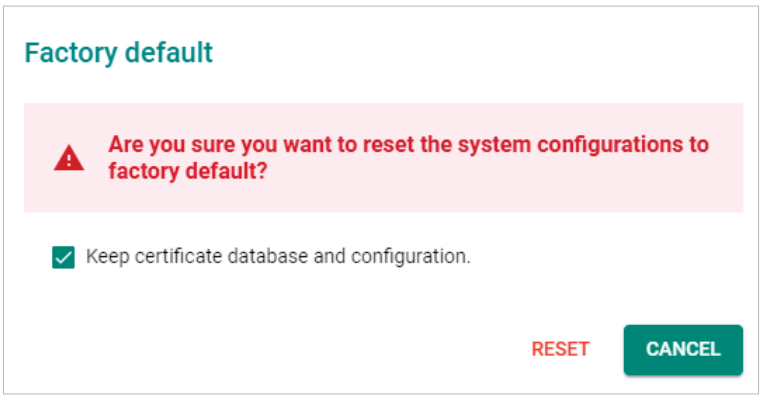


Reboot



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.

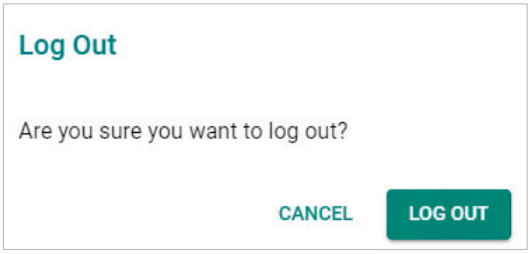
NOTE

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

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.

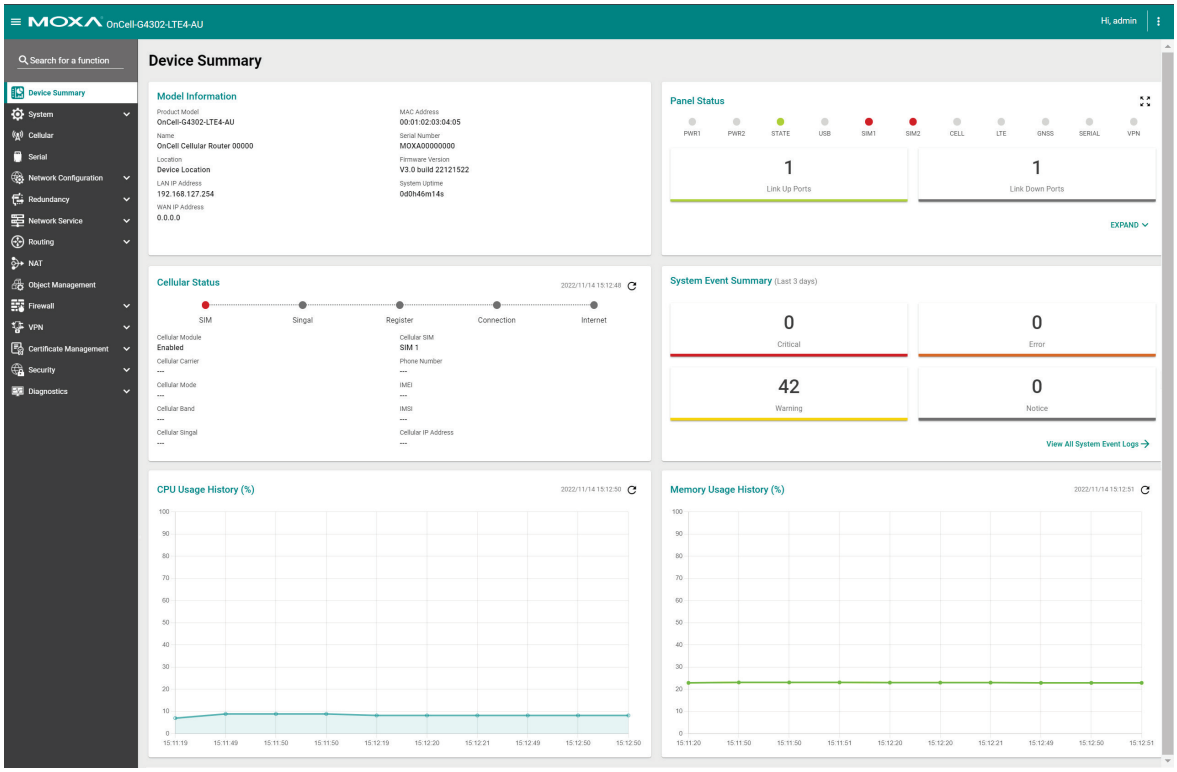
Log Out



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.



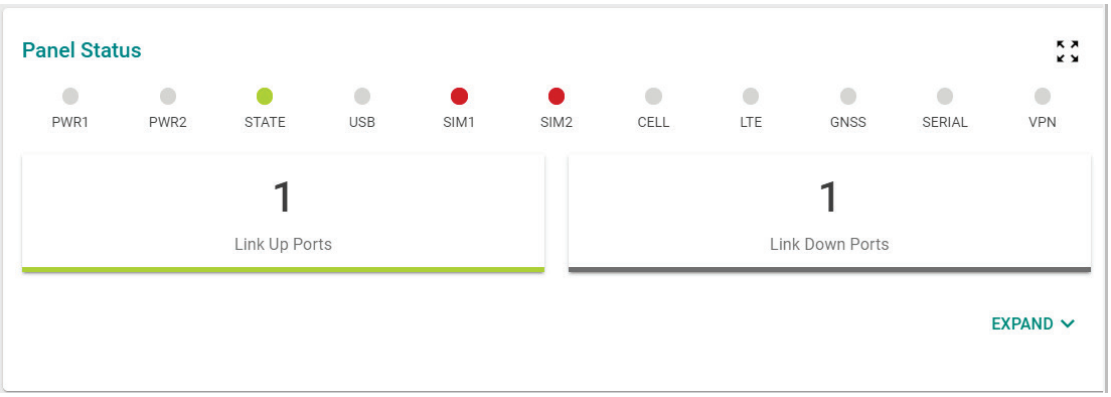
See the following sections for a more detailed description of each widget on the summary page.

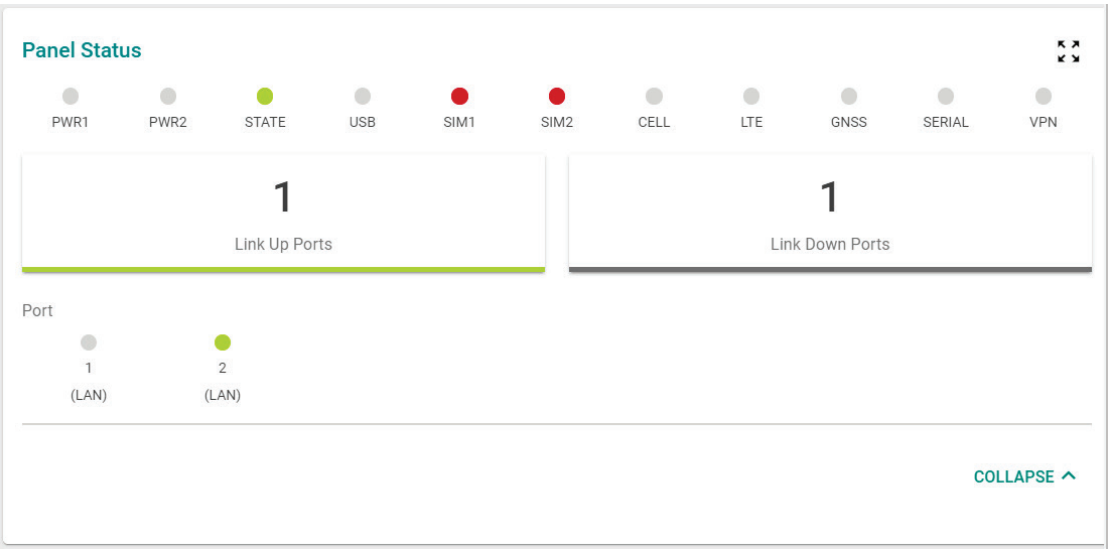
Model Information

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.





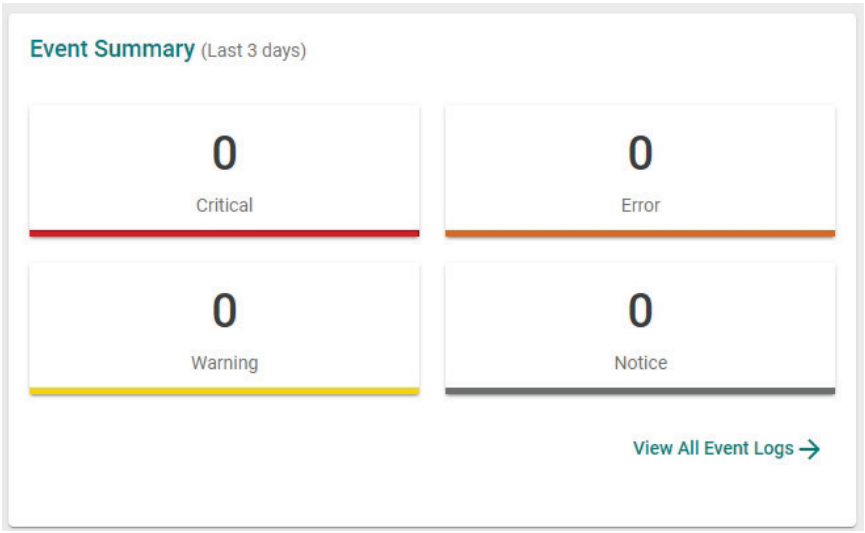
Panel View

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.

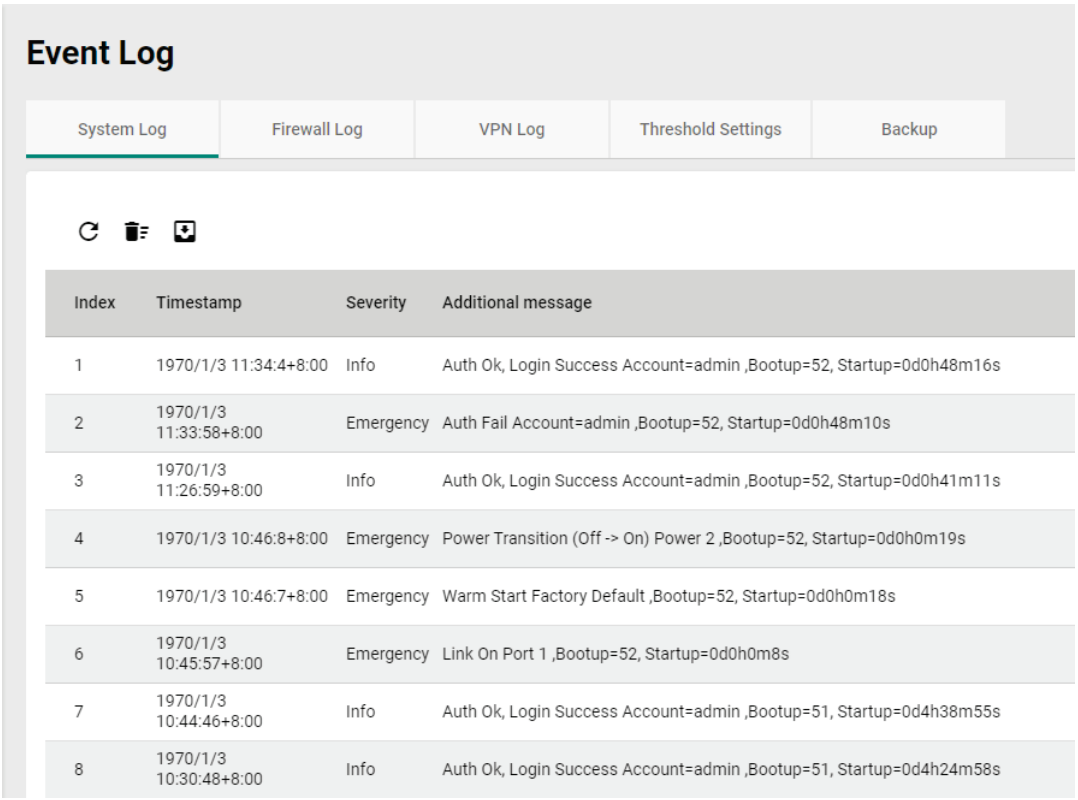
The panel view figure varies depending on the product model you are using.

Event Summary (Last 3 Days)

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



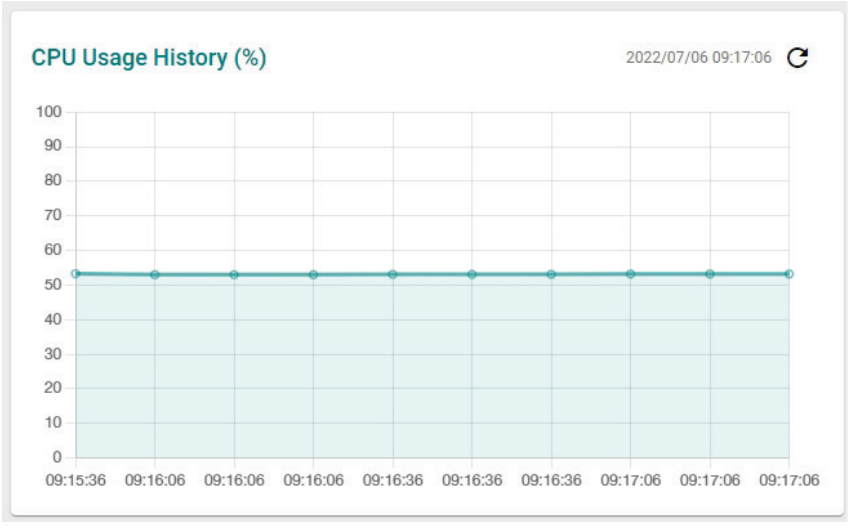
Click View All Event Logs → to go to the Event Log page, where you can view all event logs in more detail.



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

CPU Usage History (%)

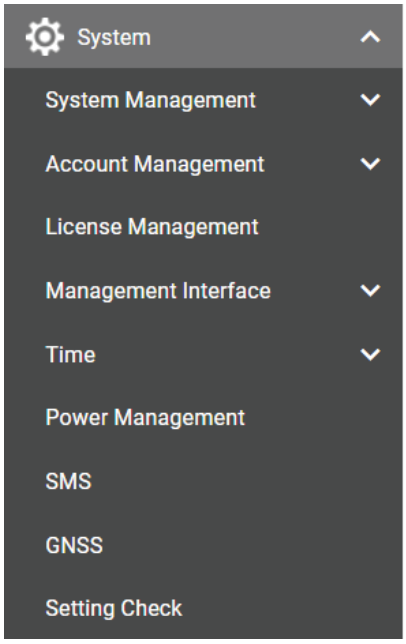
This panel shows the device's CPU usage. The data will be shown as a percentage over time. Click the icon to refresh the graph.



4. System

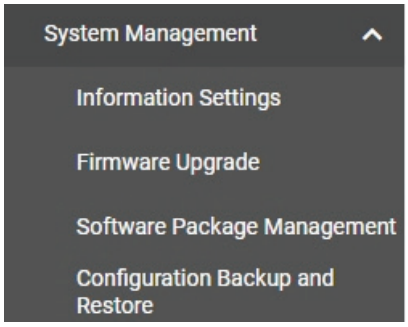
The **System** section includes the most common settings required by administrators to maintain and control the Moxa Industrial Secure Router.

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



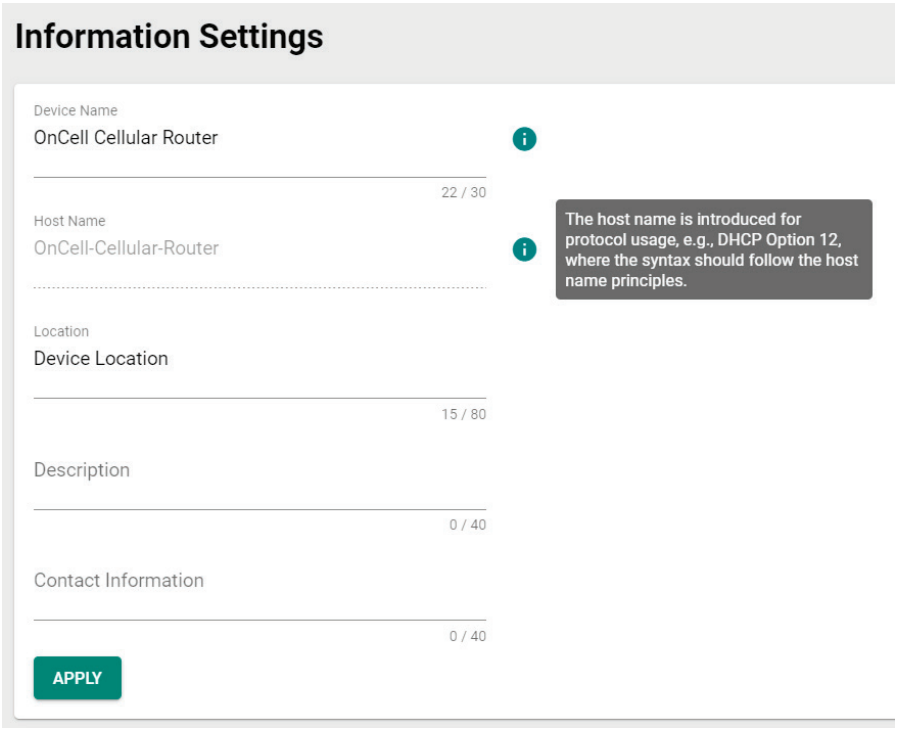
System Management

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".	OnCell Cellular Router

Host Name

Setting	Description	Factory Default
Max. 80 characters	Enter the host name for the device for protocol use (e.g. DHCP Option 12).	OnCell-Cellular-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

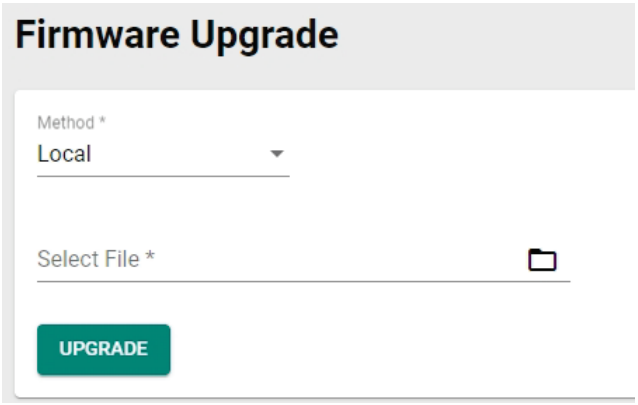
There are five ways to update your Moxa router's firmware: from a local *.rom file, by remote TFTP server, USB tool, SCP server, and SFTP server.

NOTE

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

Local

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



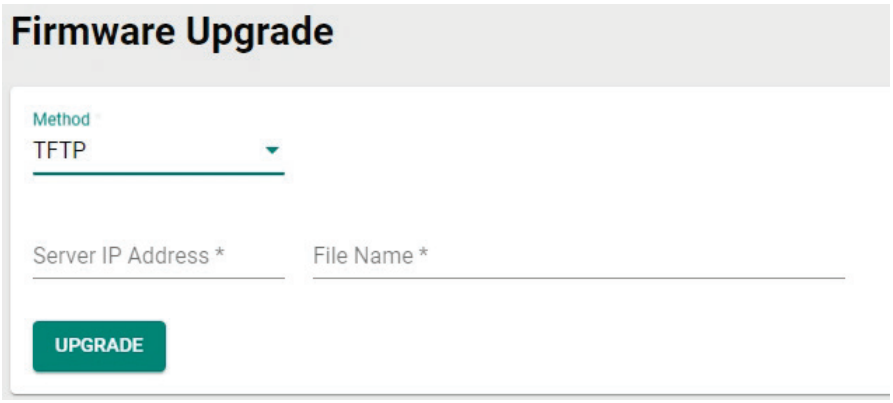
Select File

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.

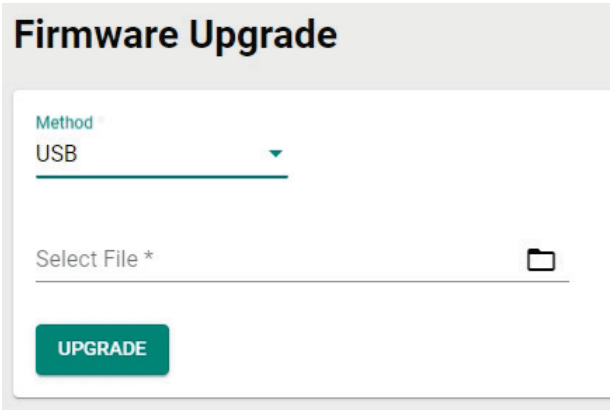
USB

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

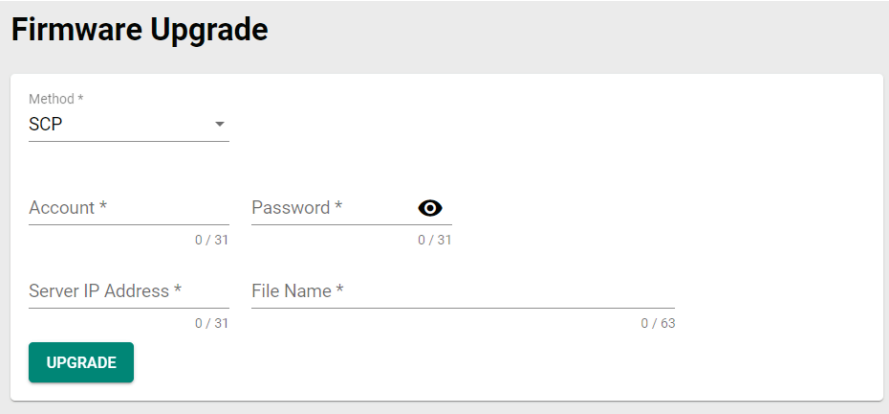
The ABC-02 USB is an optional accessory and must be purchased separately.

NOTE

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

SCP

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



Account

Setting	Description	Factory Default
Max. 31 characters	Enter the username for SCP authentication.	None

Password

Setting	Description	Factory Default
Max. 31 characters	Enter the password for SCP authentication.	None

Server IP Address

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

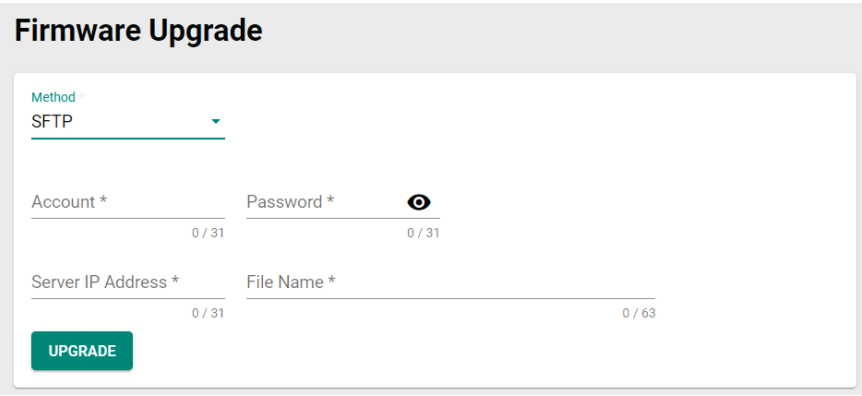
File Name

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.

SFTP

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



Account

Setting	Description	Factory Default
Max. 31 characters	Enter the username for SFTP authentication.	None

Password

Setting	Description	Factory Default
Max. 31 characters	Enter the password for SFTP authentication.	None

Server IP Address

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

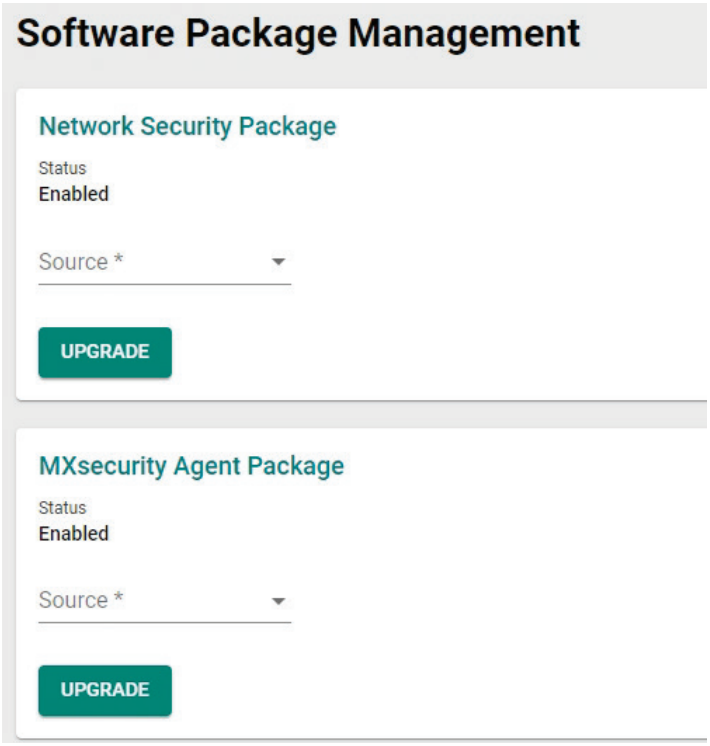
File Name

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.

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

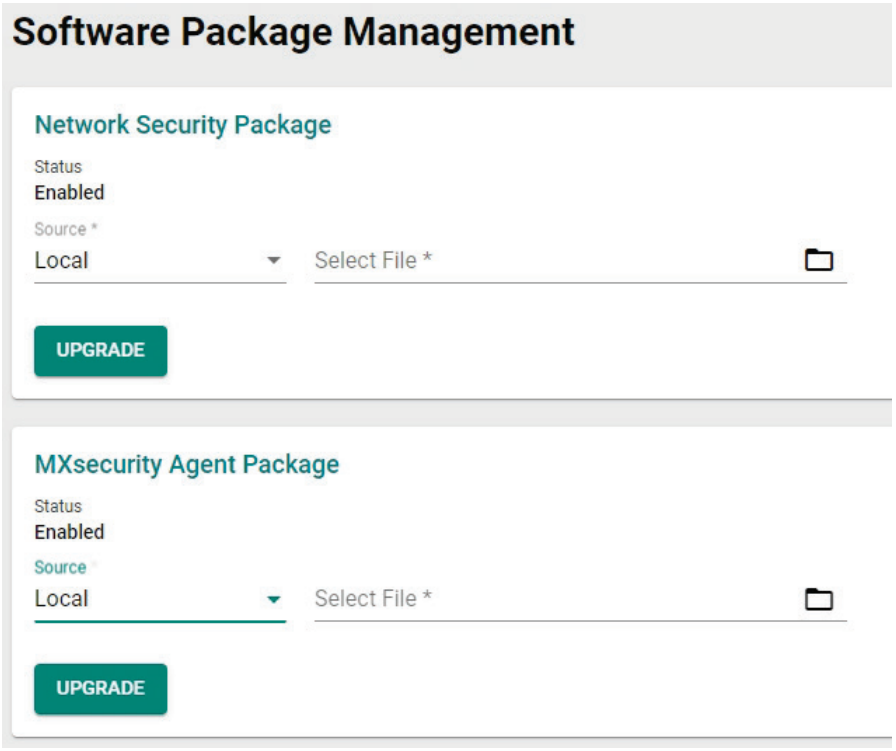
Setting	Description	Factory Default
Enabled	The package is installed and is working normally.	Enabled
Disabled	The package is installed but was abnormally terminated.	
Uninstalled	No package is installed.	

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

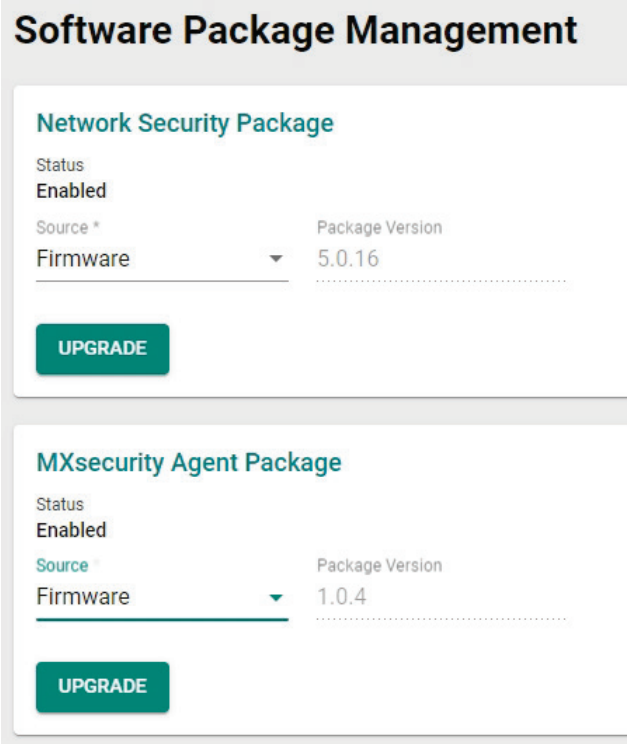
Select **Local** from the drop-down menu under **Source** to update an existing package using a local file.

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

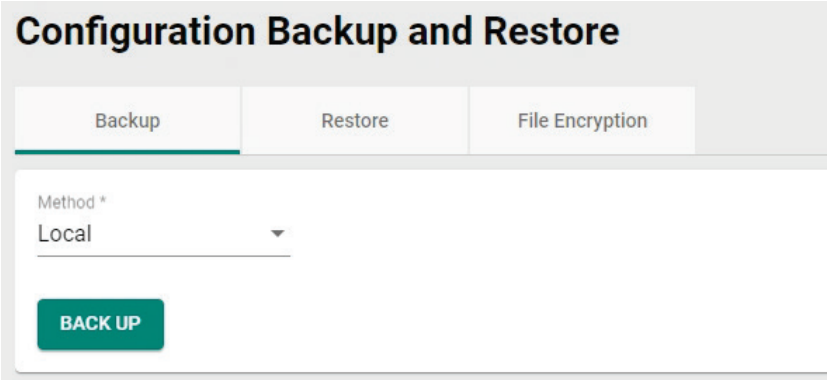
This shows the target firmware version. Click **UPGRADE** to start the upgrade process. This procedure will take several minutes to complete.

Configuration Backup and Restore

Backup

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

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



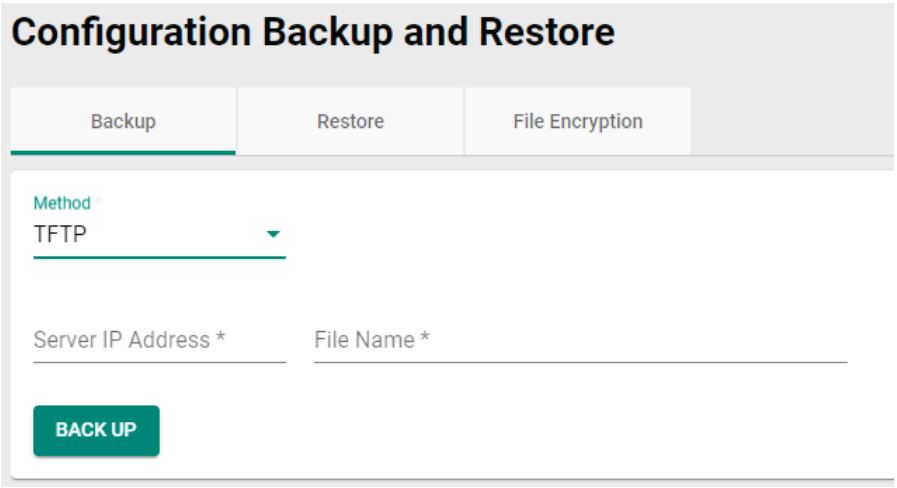
There are five ways to back up the configuration of your Industrial Secure Router: to the local host computer, to a remote TFTP server, to a Moxa ABC-02 USB tool, to a SCP server, or to a SFTP server.

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

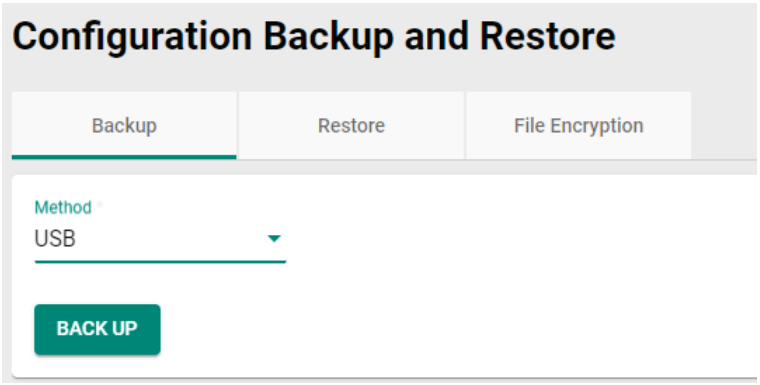
File Name

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**.



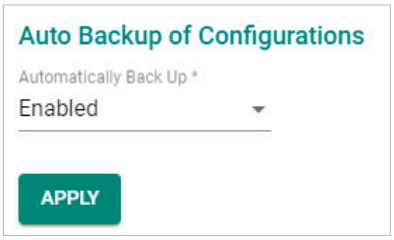
Insert the Moxa ABC-02 USB-based configuration tool into the USB port of the Industrial Secure Router and click **BACK UP** to back up the system configuration file to the tool.

NOTE

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

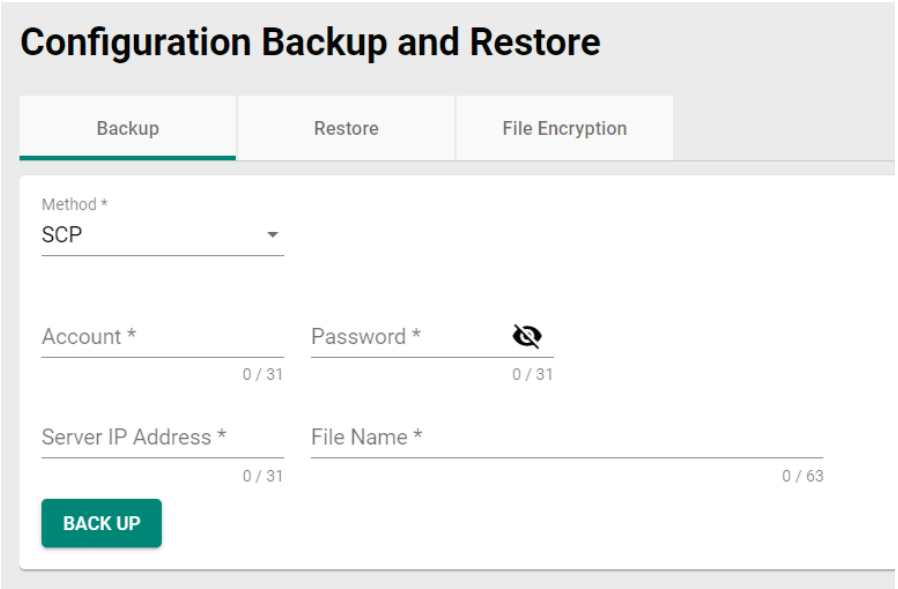
Auto Backup of Configurations

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



SCP

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



Account

Setting	Description	Factory Default
Max. 31 characters	Enter the username for SCP authentication.	None

Password

Setting	Description	Factory Default
Max. 31 characters	Enter the password for SCP authentication.	None

Server IP Address

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

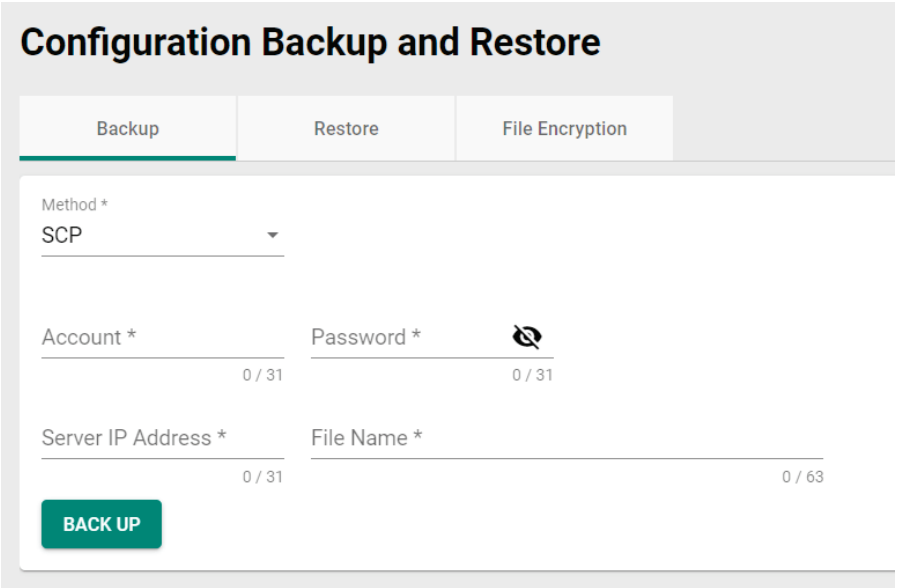
File Name

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.

SFTP

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



Account

Setting	Description	Factory Default
Max. 31 characters	Enter the username for SFTP authentication.	None

Password

Setting	Description	Factory Default
Max. 31 characters	Enter the password for SFTP authentication.	None

Server IP Address

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

File Name

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

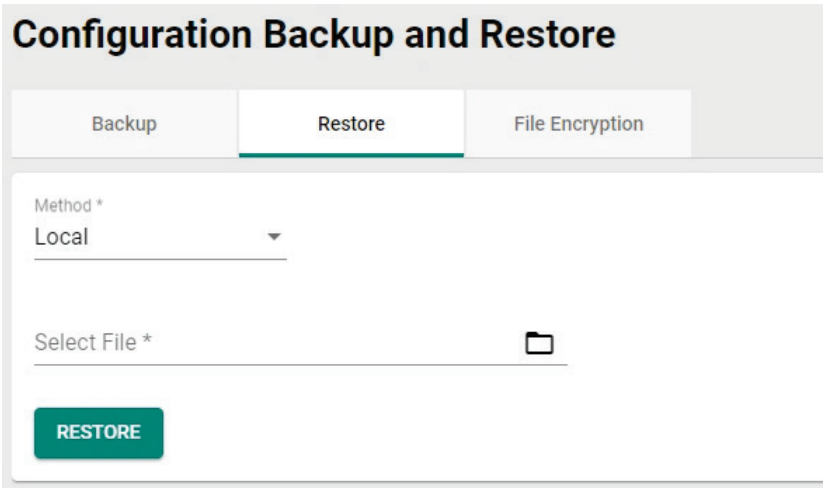
When finished, click **BACK UP** to back up the system configuration file.

Restore

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

NOTE

1. When importing a configuration file into the device, the system will check the integrity of the file. If the integrity check fails, the system will record an event log.
2. If it is necessary to verify the integrity of the configuration file when the system is running, the administrator can use the **show integrity check** CLI command.



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

Local

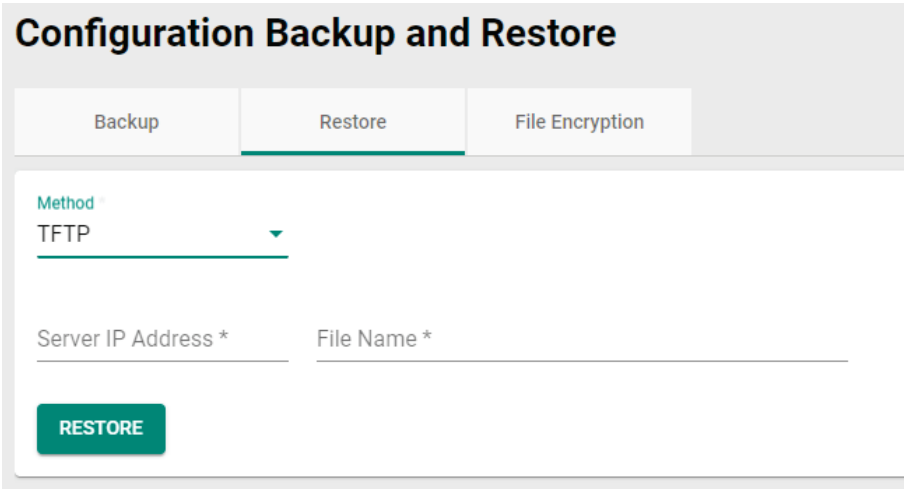
Select **Local** from the drop-down list under **Method**

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

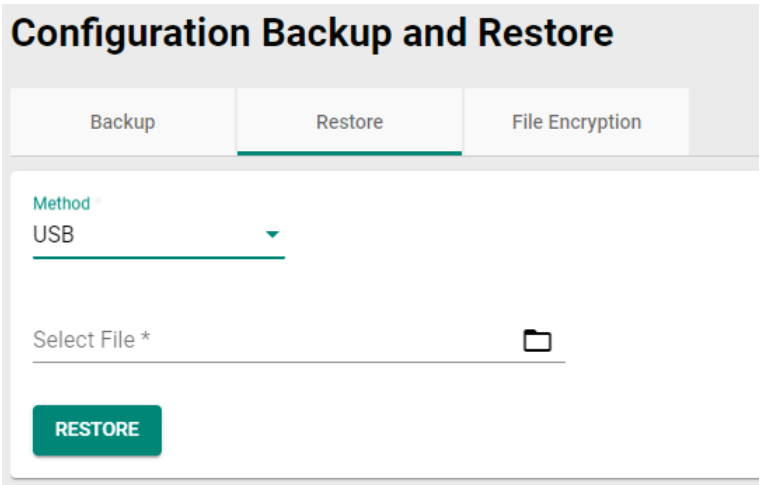
File Name

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**.



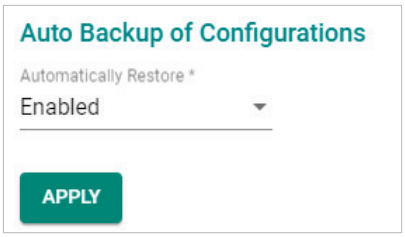
Insert the Moxa ABC-02 USB-based configuration tool into the USB port of the Industrial Secure Router and click **RESTORE** to restore the system configuration.

NOTE

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

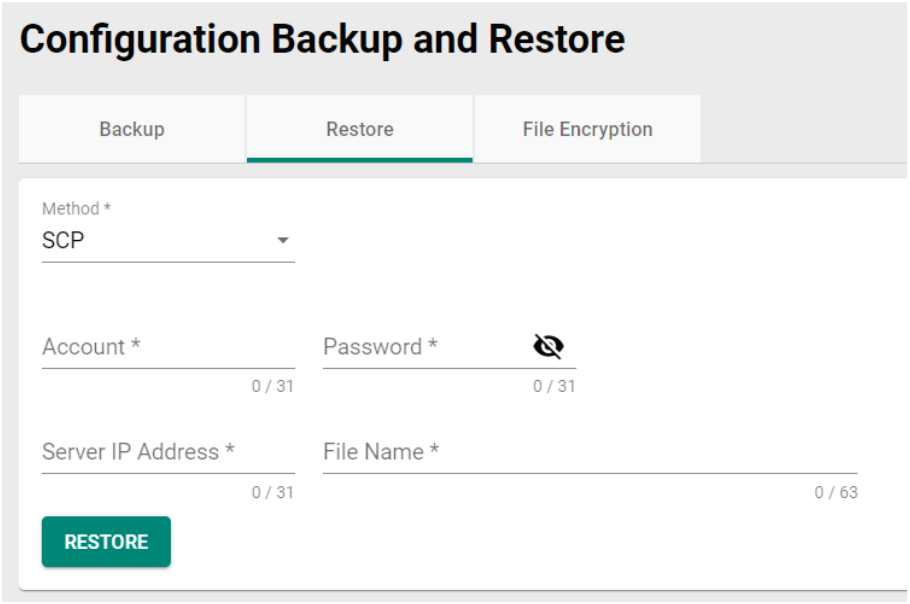
Auto Backup of Configurations

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



SCP

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



Account

Setting	Description	Factory Default
Max. 31 characters	Enter the username for SCP authentication.	None

Password

Setting	Description	Factory Default
Max. 31 characters	Enter the password for SCP authentication.	None

Server IP Address

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

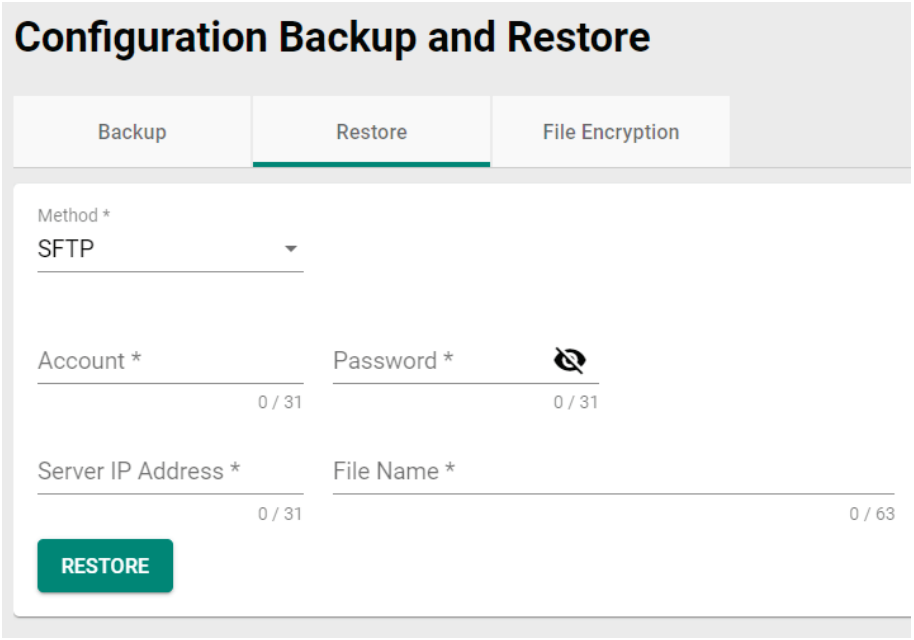
File Name

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.

SFTP

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



Account

Setting	Description	Factory Default
Max. 31 characters	Enter the username for SFTP authentication.	None

Password

Setting	Description	Factory Default
Max. 31 characters	Enter the password for SFTP authentication.	None

Server IP Address

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

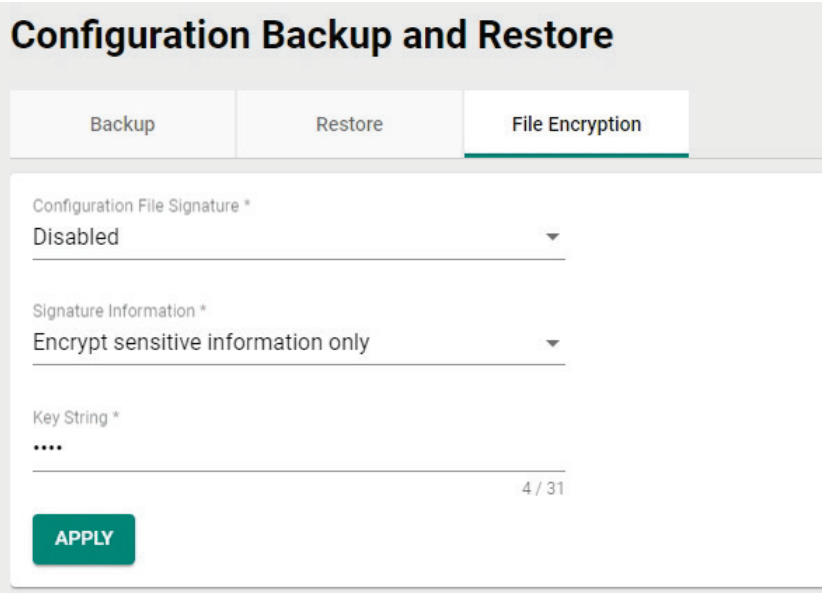
File Name

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.

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.	

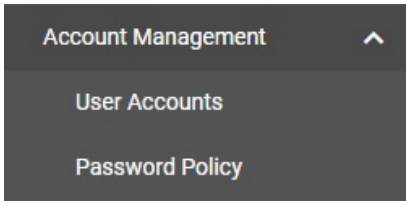
Key String

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**.

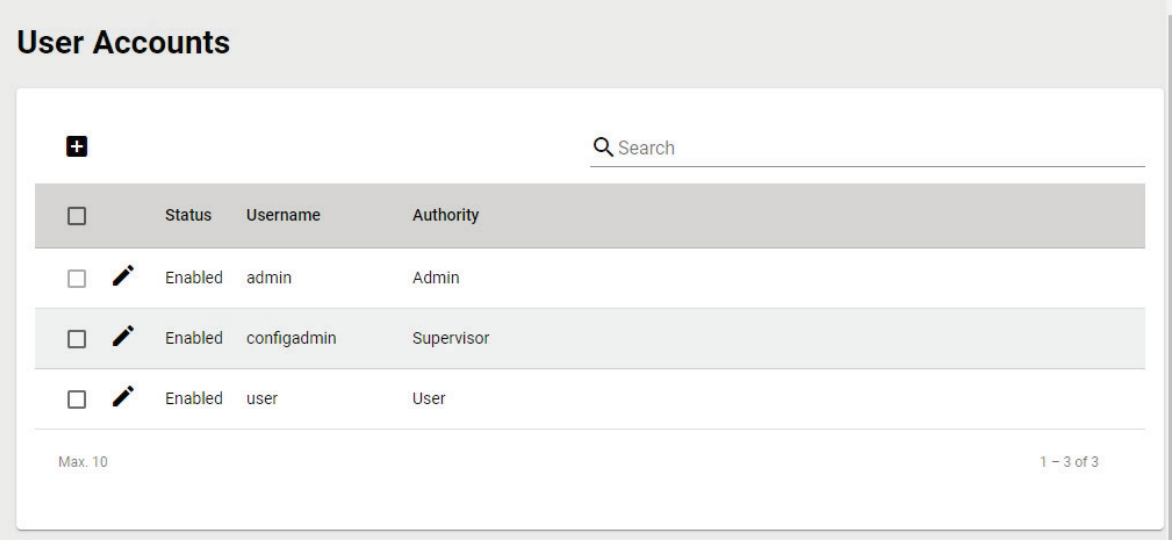


User Accounts

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.

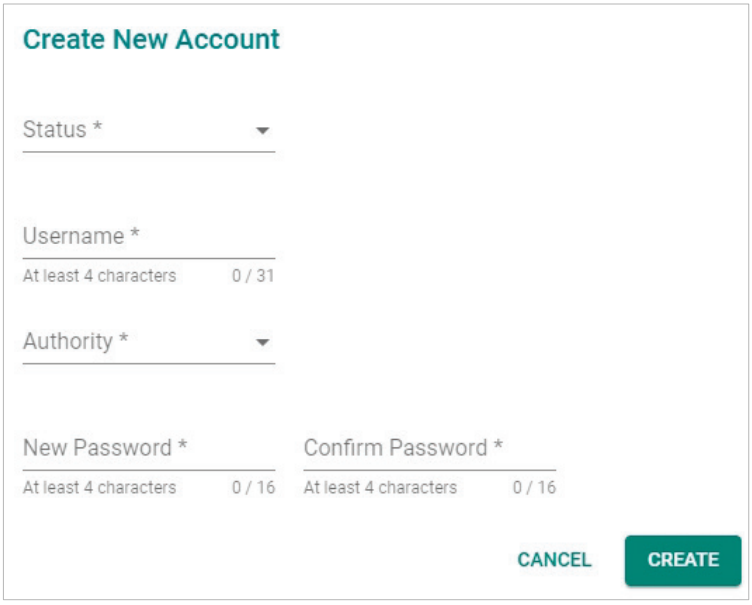
NOTE

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.
3. For security reasons, it is recommended for the administrator to keep a record of the account list and associated users.



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

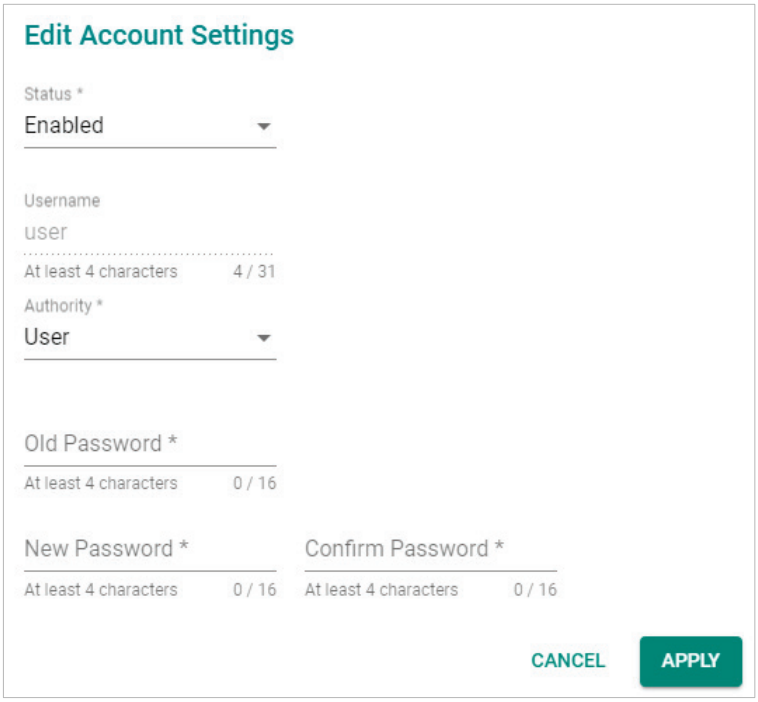
Setting	Description	Factory Default
4 to 16 characters	Enter a password for the account.	None

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

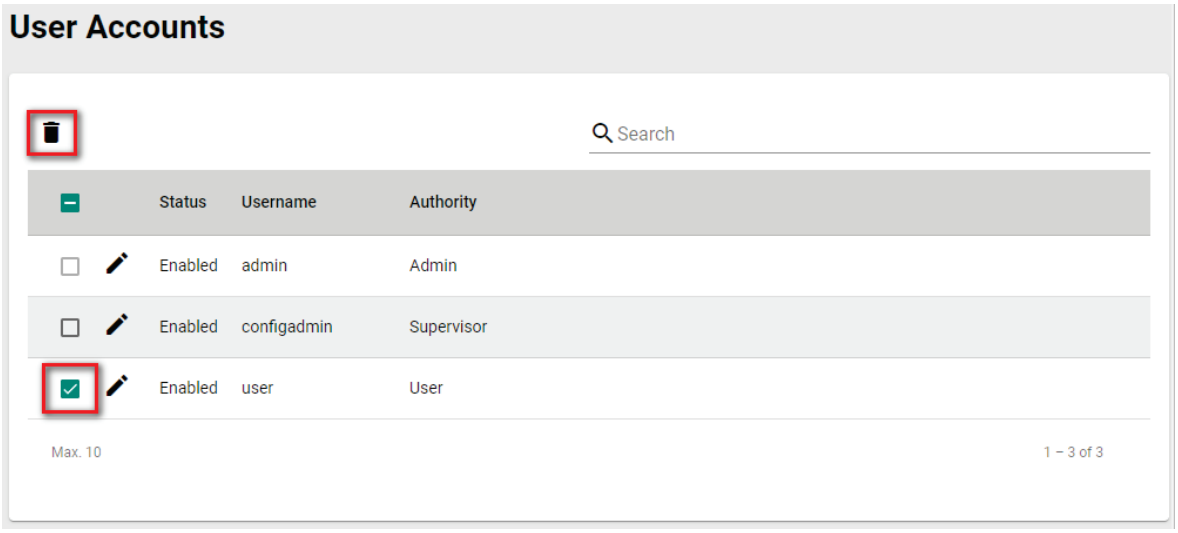
Confirm Password

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

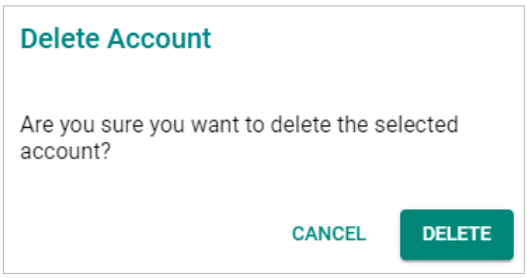
When finished, click **APPLY** to save your changes.

Delete an Existing Account

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

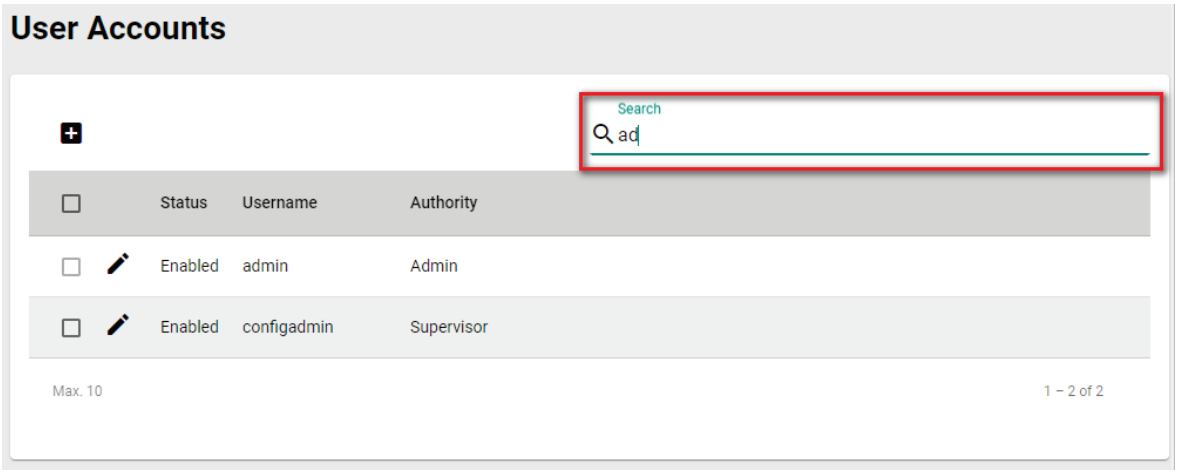


Click **DELETE** to delete the account



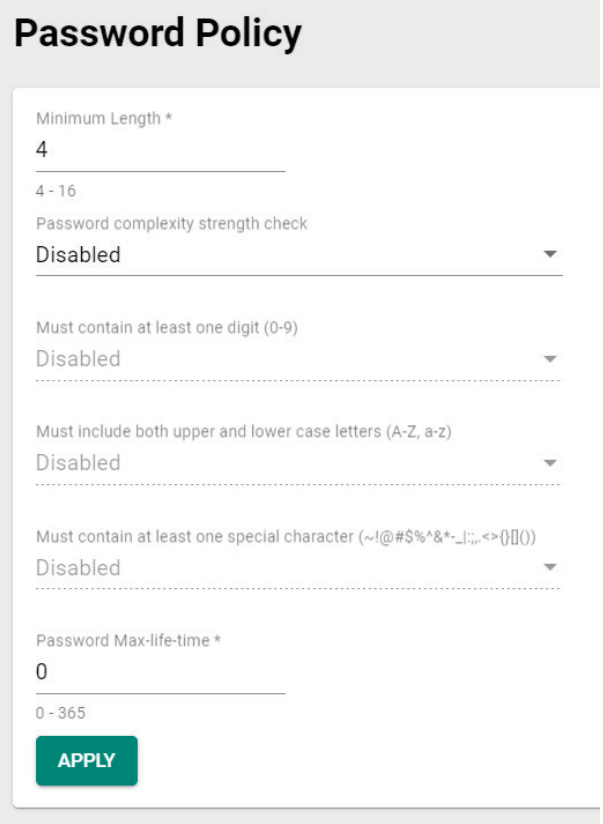
Search for an Existing Account

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

Password Max-life-time

Setting	Description	Factory Default
0-365	Specify how long passwords remain valid for (in days). If set to 0, passwords do not expire.	0

NOTE

For security reasons, the administrator should set the minimum password length to 16 and enable all the password complexity check options.

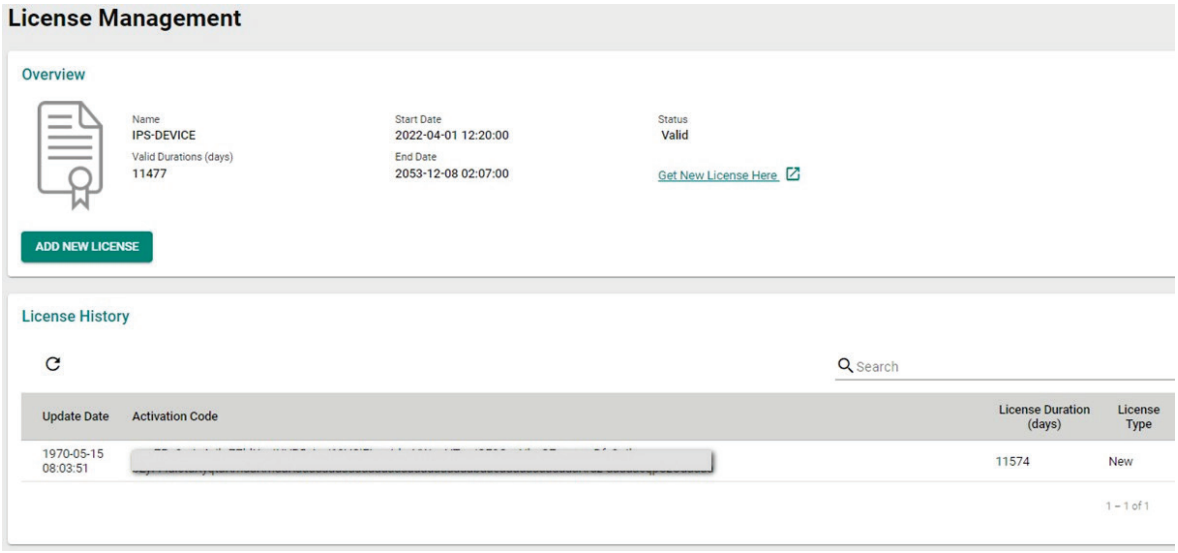
NOTE

For security reasons, the administrator should set a maximum password lifetime to make sure users are required to update their password frequently.

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.

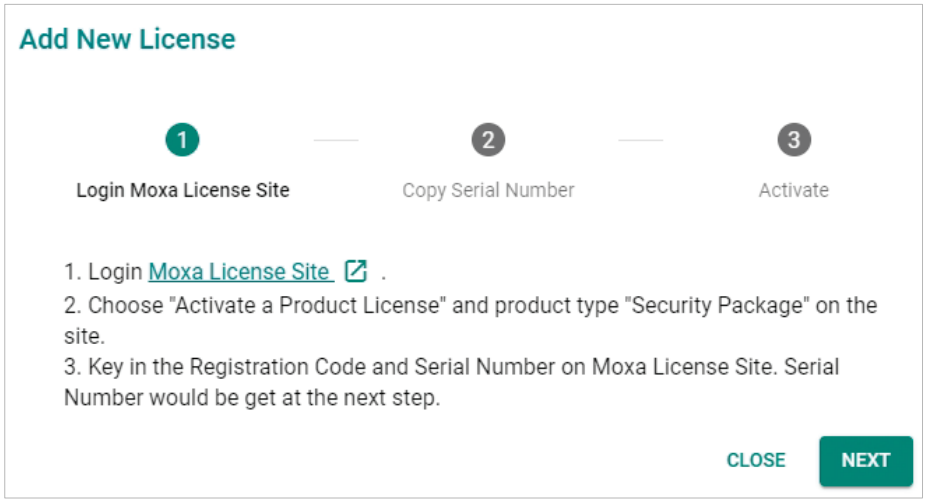
Enter the full or partial license number in the Search field. Any licenses matching the search criteria will be shown in the License List table.

Add a New License

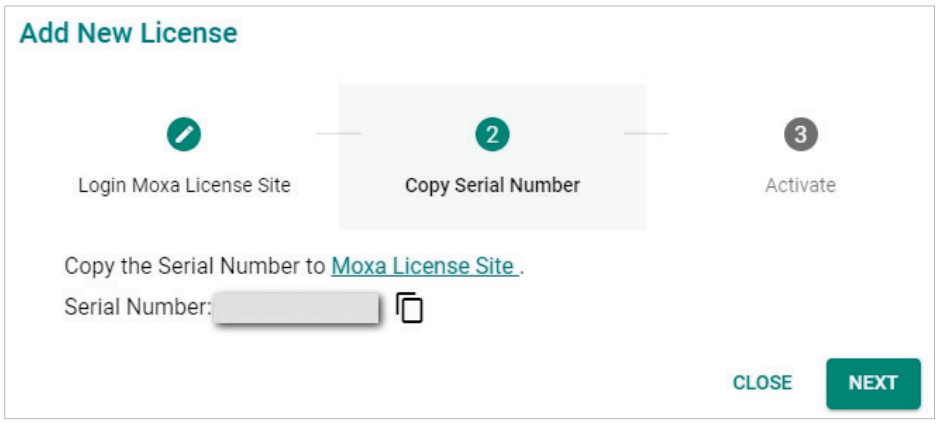
Whenever a new Industrial Secure Router license is activated in the license management portal, the system will generate an activation code that can be used to activate the license on the Industrial Secure Router.

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

   The **Add New License** screen appears.

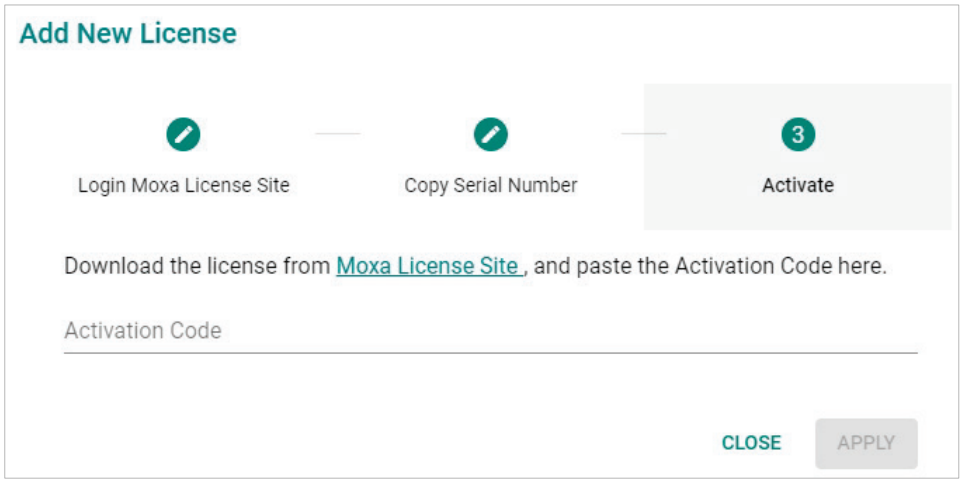


3. Click **Next**.
4. Click the icon to copy the serial number and store it somewhere where it can be easily copied from. Use the serial number to activate the license in the Moxa license management portal.



5. Click **Next**.

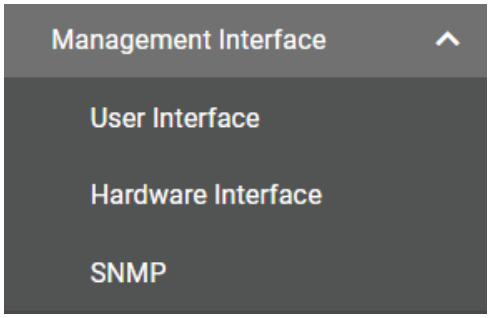
6. Enter the activation code from the email you have received after activating the license in the license management portal.



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,** and **SNMP**.

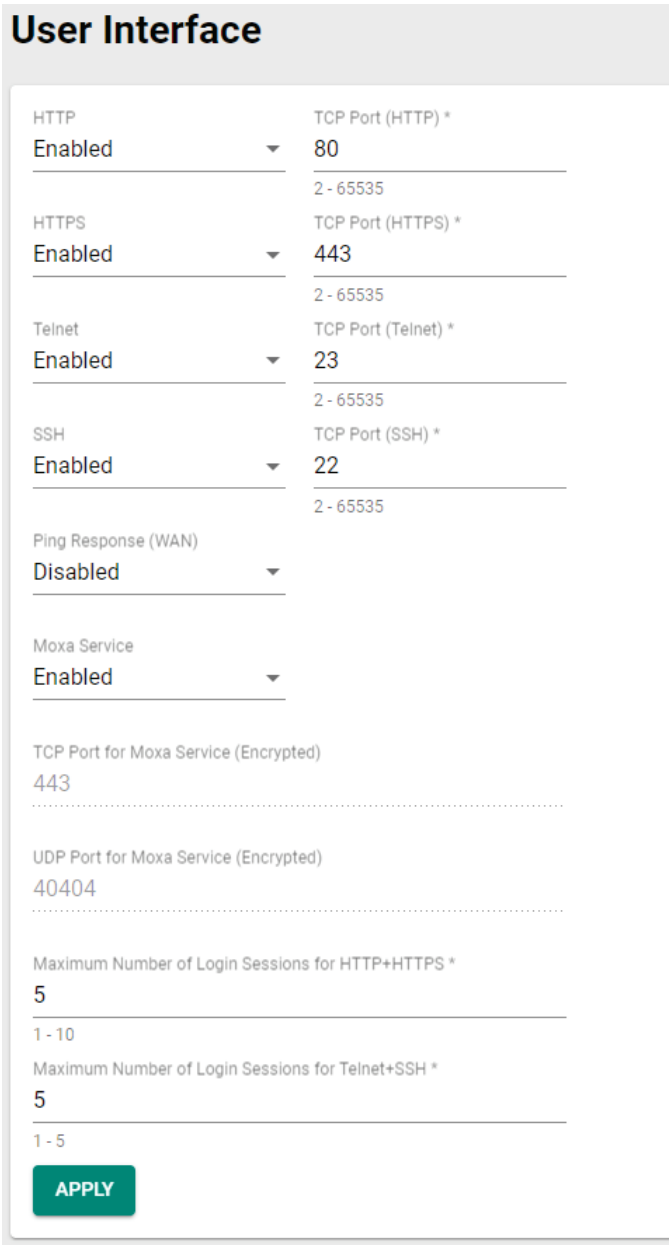


User Interface

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

NOTE

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



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

The administrator can manually import a self-signed certificate (in .p12 format) for web server (HTTPS) services. However, the administrator should check the root certificate and validity of the signature before importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked and if so, the certificate must be replaced. When the browser verifies the signature and accesses the device, it will return the subject name which the administrator can use to confirm the connected device is authorized.

NOTE

1. The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations.
2. The lifetime of certificates generated for web server (HTTPS) services should be short and in accordance with the organization's security procedures and requirements.

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.	Disabled

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

1. Moxa Service is only used for Moxa network management software.
2. Moxa Service is only available for user accounts with admin privileges.

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

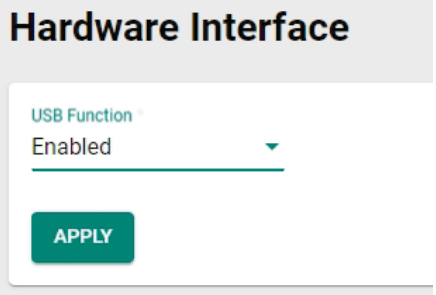
Maximum Number of Login Sessions for Telnet+SSH

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.

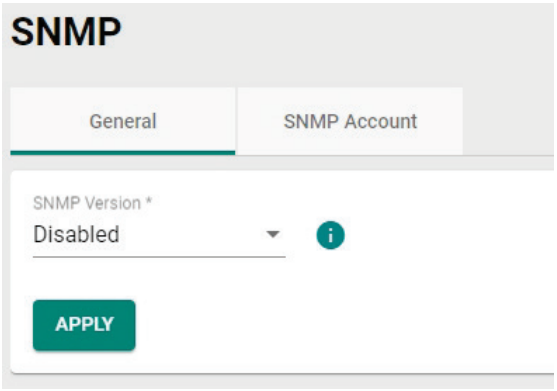
SNMP security modes and security levels supported by the Industrial Secure Router are listed in the following table.

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.

Protocol Version	UI Setting	Authentication Type	Data Encryption	Method
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

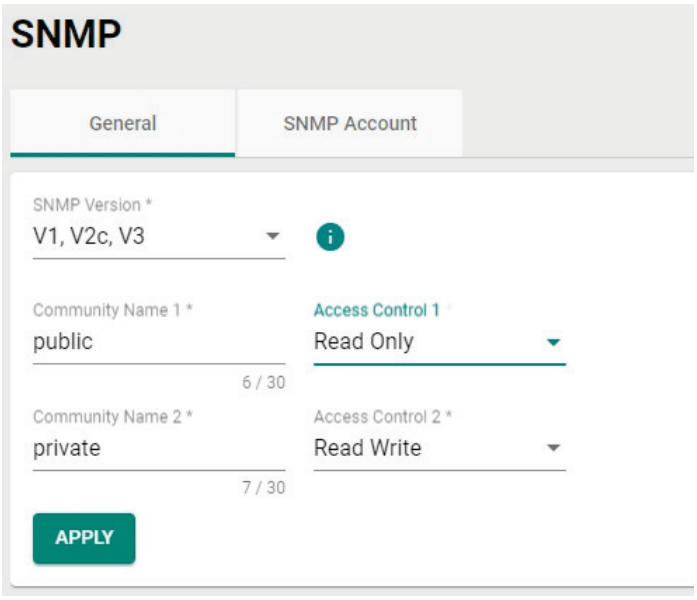
The SNMP page is used to enable or disable SNMP. Depending on the selected SNMP version, additional configuration parameters will become available.



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

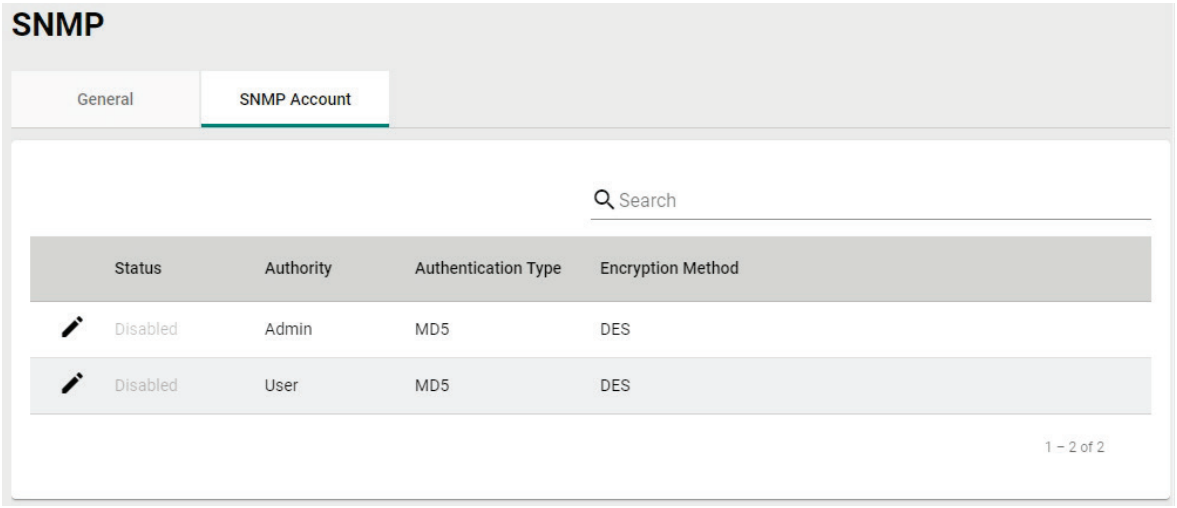
Setting	Description	Factory Default
Max. 30 characters	Use a community string match for authentication	public/private

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

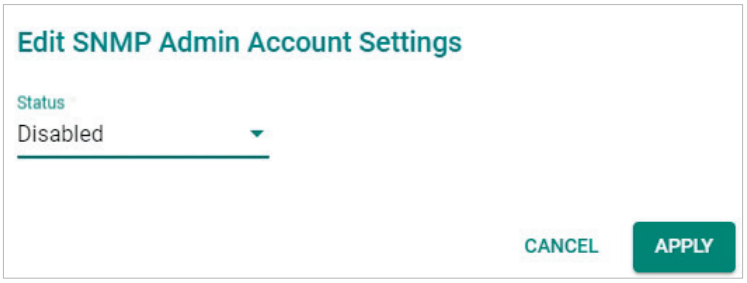
SNMP Account

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

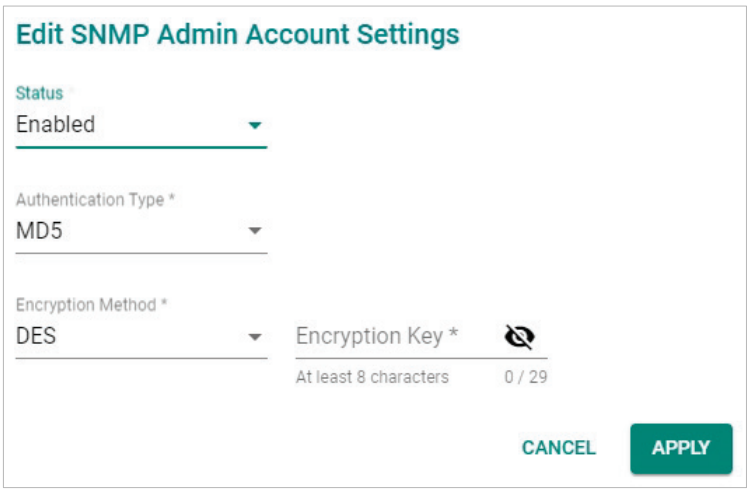


Modify an Existing SNMP Account

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

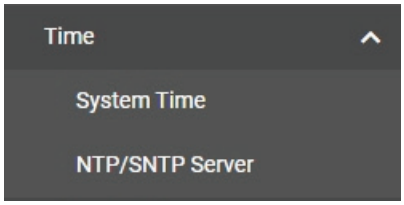
Encryption Key

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.

Time

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



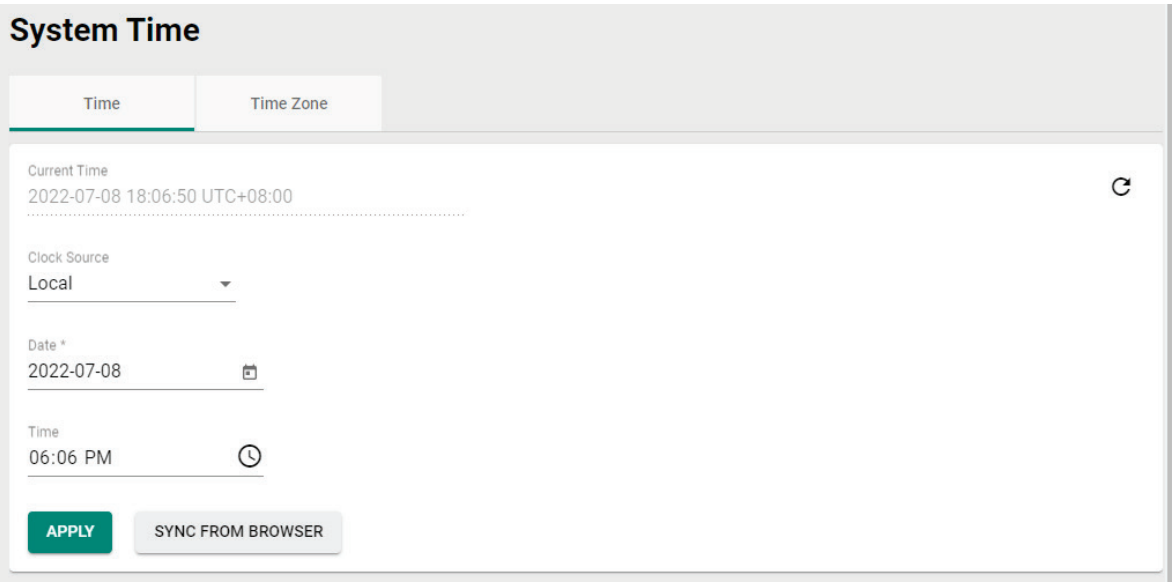
System Time

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.

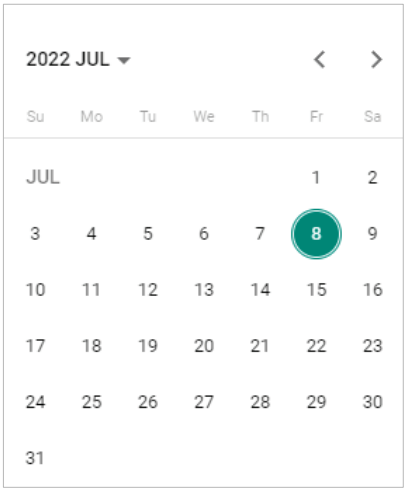
Clock Source

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

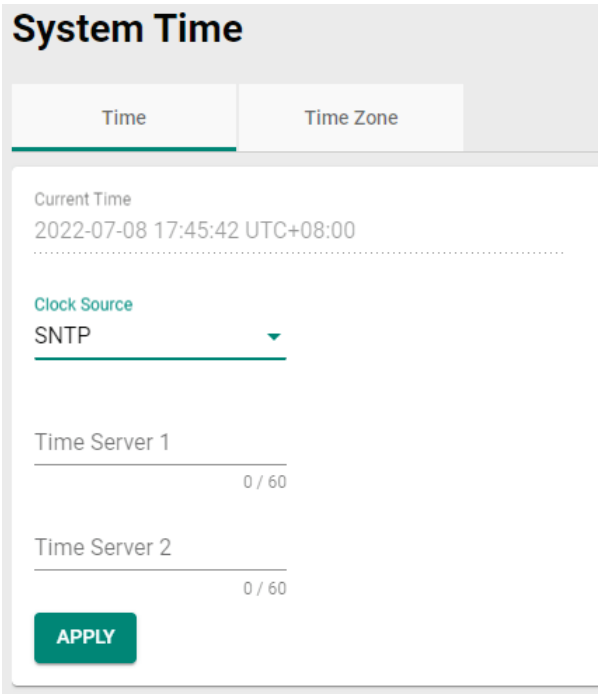


Time

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

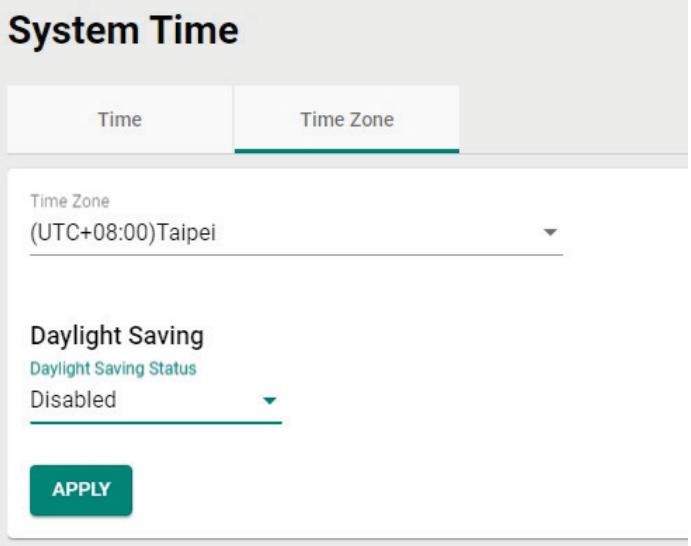
Setting	Description	Factory Default
0 to 60 characters	Specify the IP or domain address of the primary time server (e.g., 192.168.1.1, time.stdtime.gov.tw, or time.nist.gov).	None

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)

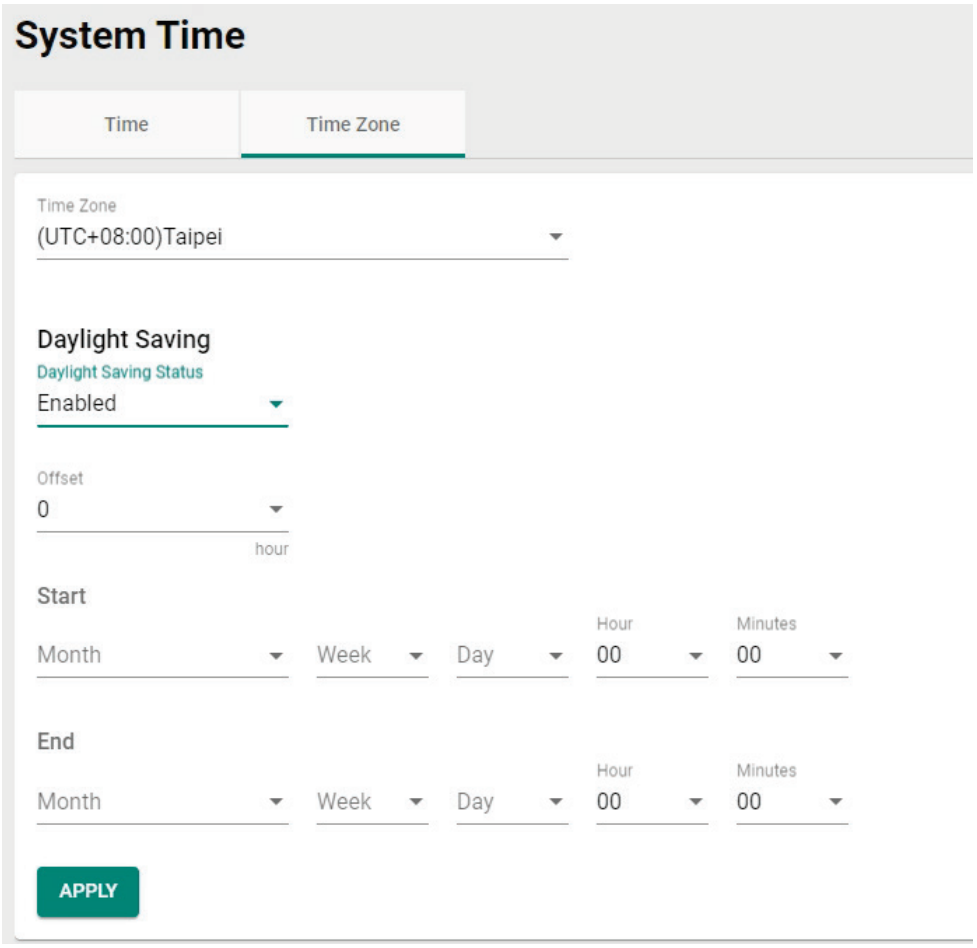
Daylight Saving

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

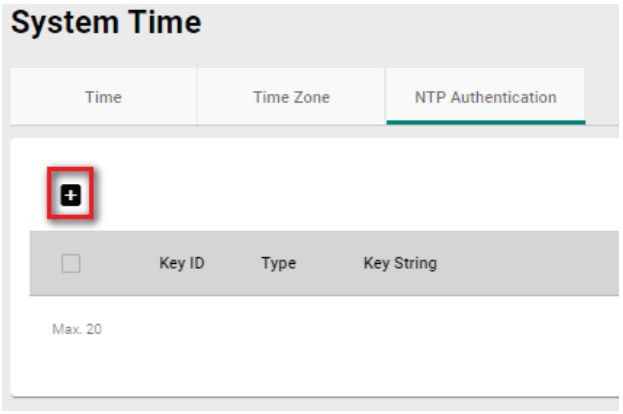
NOTE

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

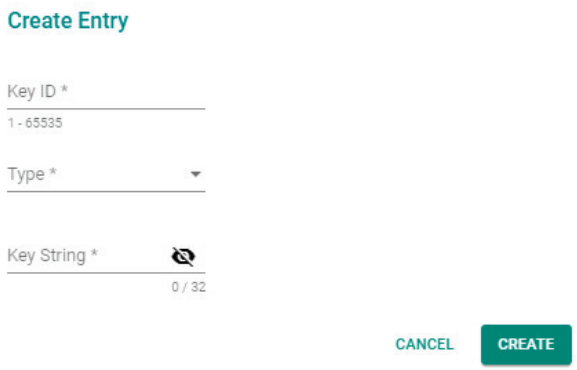
NTP Authentication

This section describes how to configure NTP Authentication.

To create a new entry, click the **NTP Authentication** tab, then click the **Add** (**+**) icon.



Configure the following settings:



Key ID

Setting	Description	Factory Default
1 to 65535	Enter the Key ID to use for NTP authentication.	None

Type

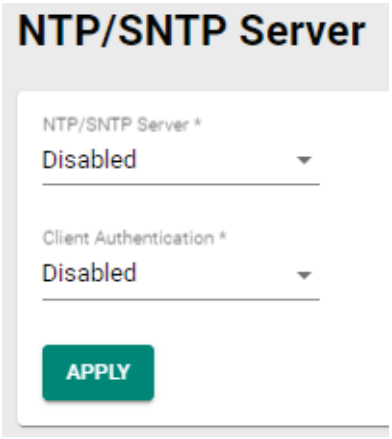
Setting	Description	Factory Default
MD5 or SHA-512	Choose the authentication type.	None

Key String

Setting	Description	Factory Default
0 to 32 characters	Enter the password to use for the authentication key.	None

When finished, click **CREATE**.

NTP/SNTP Server



NTP/SNTP Server

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

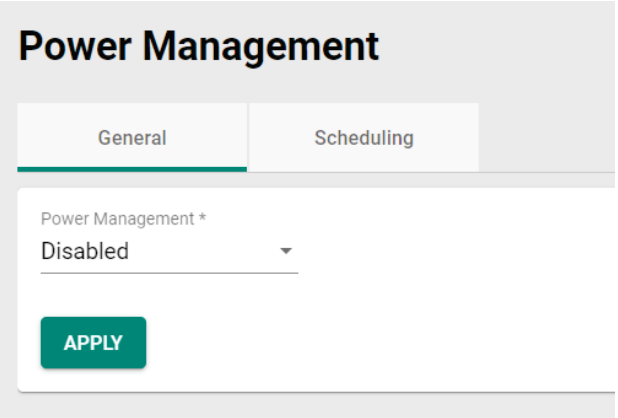
Client Authentication

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable NTP authentication for clients.	Disabled

Power Management

General

The General tabs lets you enable power management functionality. If enabled, you can control how and when the device enters a power-saving state. If disabled, the device will never enter power-saving mode.

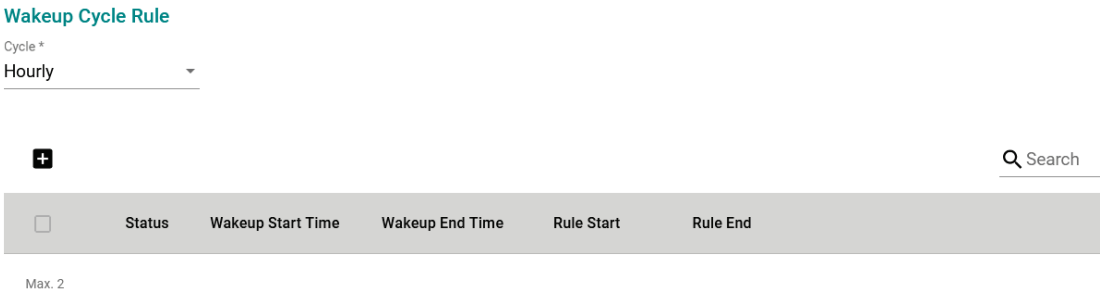


Power Management

Setting	Description	Factory Default
Disabled	Disable power management.	Disabled
Scheduling	Control the device's power saving state based on a user-configured schedule. Refer to the Scheduling section.	

Scheduling

From the Scheduling screen, you can create cyclical power management rules to control when the device goes into and leaves power saving mode. Cycle rules will repeat based on the configured schedule.

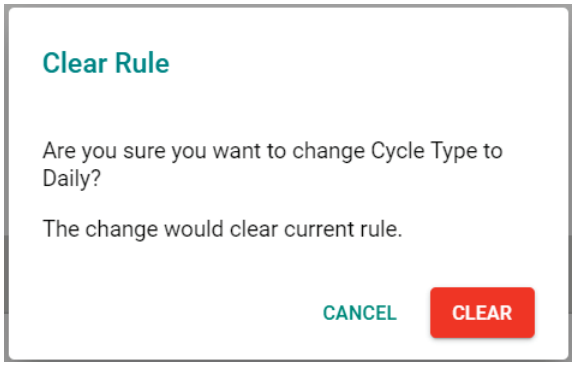


Cycle

Setting	Description	Factory Default
Hourly	The device will enter and leave power saving mode at the specified time every hour. Refer to Create an Hourly Cycle Rule for more information.	Daily
Daily	The device will enter and leave power saving mode at the specified time each day. Refer to Create a Daily Cycle Rule for more information.	
Weekly	The device will enter and leave power saving mode on the specified day and time of every week. Refer to Create a Weekly Cycle Rule for more information.	
Monthly	The device will enter and leave power saving mode on the specified day and time of every month. Refer to Create a Monthly Cycle Rule for more information.	

NOTE

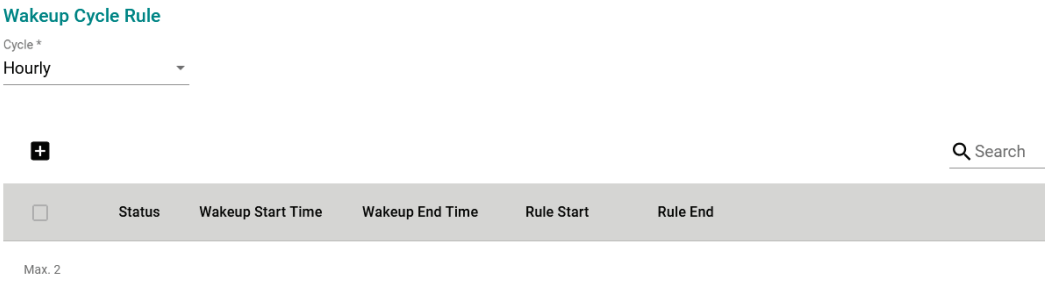
Only one type of wakeup cycle rule (e.g. daily, weekly, …) can be active at any given time. If a rule of another cycle type is created, all existing rules will be deleted.



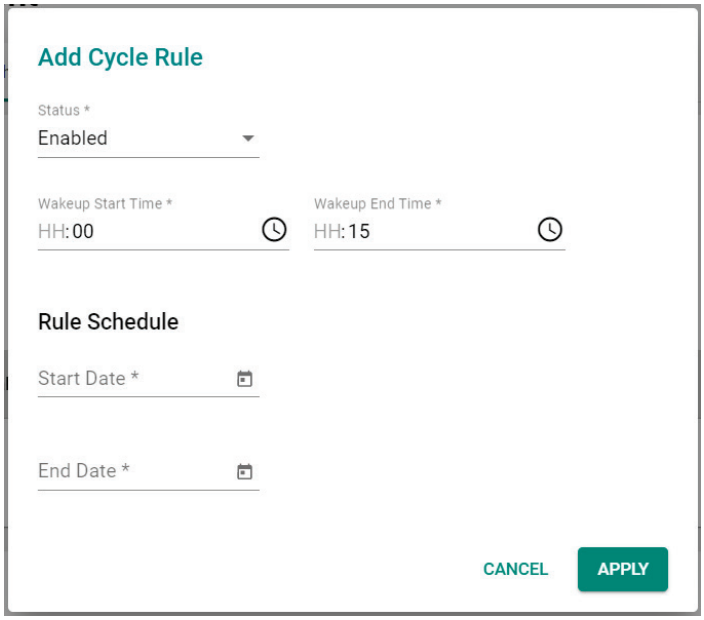
NOTE

To avoid the system from entering power saving mode and interrupting your configuration session, all rules should be scheduled to start at least 15 minutes later than the time the rule is created. If the rule is set to start within 15 minutes after being created, the system will ignore the first cycle of that rule and start at the next cycle.

Create an Hourly Cycle Rule



With the Cycle type set to **Hourly**, from the Wakeup Cycle Ruler list, click the **Add** ( ) icon to add a new entry.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the cycle rule.	Enabled

Wakeup Start Time

Setting	Description	Factory Default
00 to 59	Specify the minutes when the device will leave power saving mode each hour.	00

Wakeup End Time

Setting	Description	Factory Default
00 to 59	Specify the minutes when the device will enter power saving mode each hour.	15

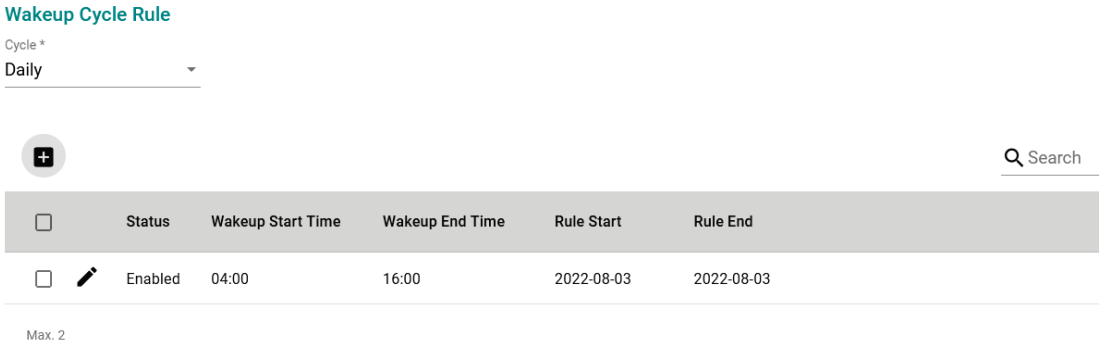
Start Date

Setting	Description	Factory Default
Date	Specify the date this cycle rule will take effect.	None

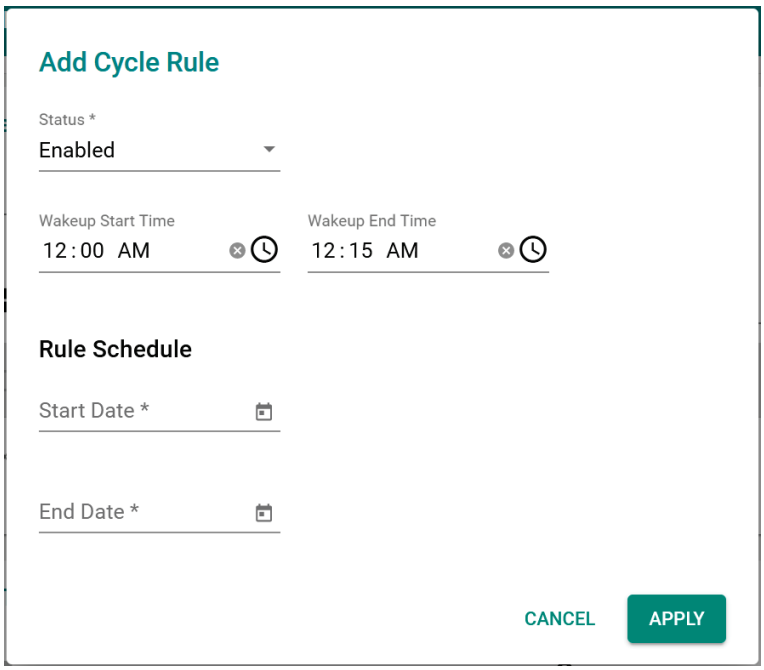
End Date

Setting	Description	Factory Default
Date	Specify the date this cycle rule will end.	None

Create a Daily Cycle Rule



With the Cycle type set to **Daily**, from the Wakeup Cycle Rule list, click the **Add** ( ) icon to add a new entry.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the cycle rule.	Enabled

Wakeup Start Time

Setting	Description	Factory Default
Time	Specify the hour and minutes when the device will leave power saving mode each day. Alternatively, click the clock icon and select the time from the drop-down list.	12:00 AM

Wakeup End Time

Setting	Description	Factory Default
Time	Specify the hour and minutes when the device will enter power saving mode each day. Alternatively, click the clock icon and select the time from the drop-down list.	12:15 AM

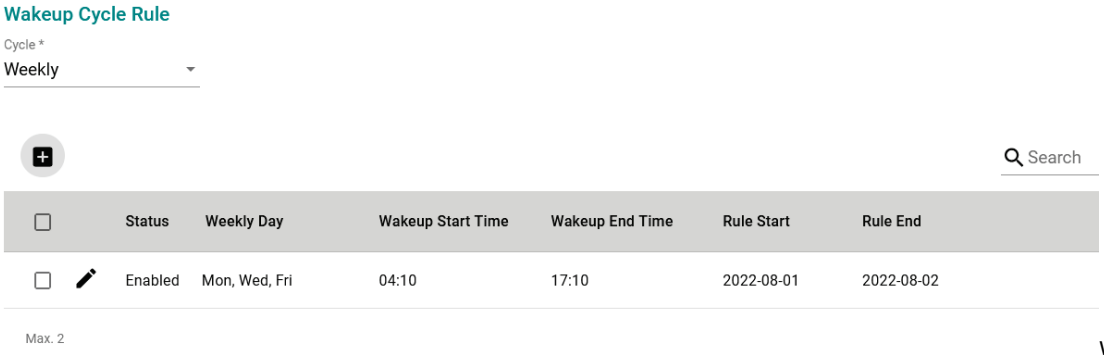
Start Date

Setting	Description	Factory Default
Date	Specify the date this cycle rule will take effect.	None

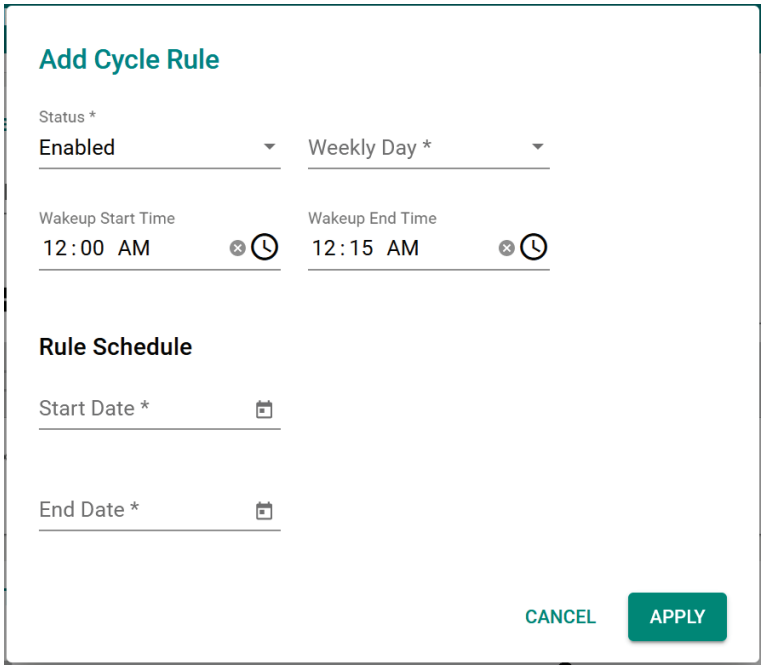
End Date

Setting	Description	Factory Default
Date	Specify the date this cycle rule will end.	None

Create a Weekly Cycle Rule



With the Cycle type set to **Weekly**, from the Wakeup Cycle Rule list, click the **Add** ( ) icon to add a new entry.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the cycle rule.	Enabled

Weekly Day

Setting	Description	Factory Default
Checkbox	Select the days of the week on which the device will leave power saving mode.	None

Wakeup Start Time

Setting	Description	Factory Default
Time	Specify the hour and minutes when the device will leave power saving mode each day. Alternatively, click the clock icon and select the time from the drop-down list.	12:00 AM

Wakeup End Time

Setting	Description	Factory Default
Time	Specify the hour and minutes when the device will enter power saving mode each day. Alternatively, click the clock icon and select the time from the drop-down list.	12:15 AM

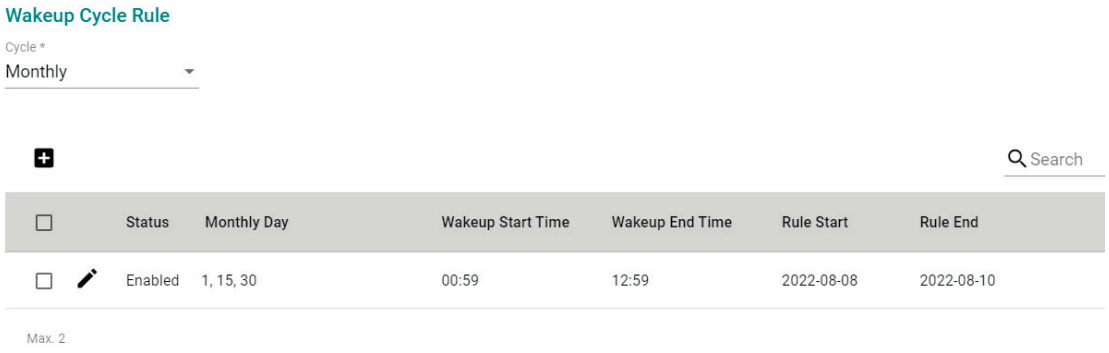
Start Date

Setting	Description	Factory Default
Date	Specify the date this cycle rule will take effect.	None

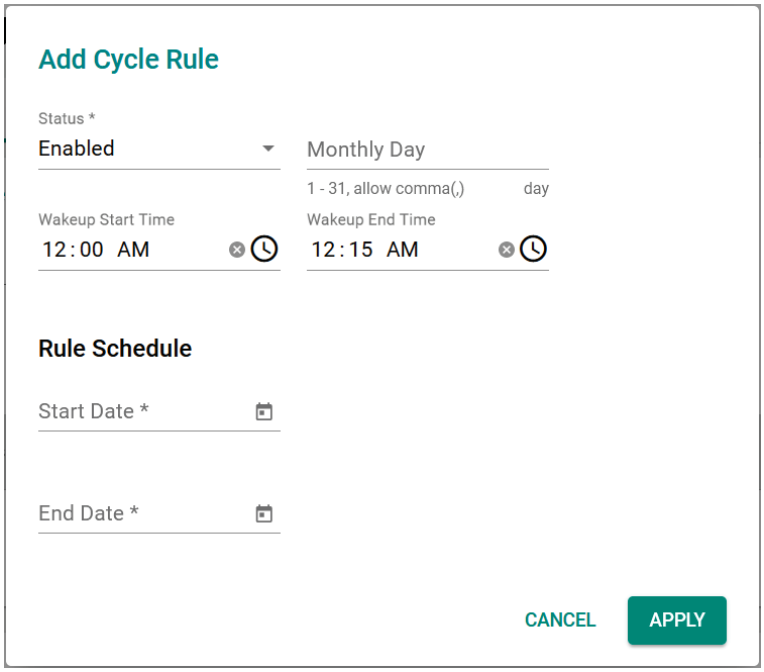
End Date

Setting	Description	Factory Default
Date	Specify the date this cycle rule will end.	None

Create a Monthly Cycle Rule



With the Cycle type set to **Monthly**, from the Wakeup Cycle Rule list, click the **Add** ( ) icon to add a new entry.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the cycle rule.	Enabled

Monthly Day

Setting	Description	Factory Default
1 to 31	Specify the days of the month on which the device will leave power saving mode. You can configure multiple days, separated by a comma (e.g. 1,2,16). If there is any month during the active period of this rule that does not have the specified day(s), the system will ignore the rule for those days.	None

Wakeup Start Time

Setting	Description	Factory Default
00 to 59	Specify the hour and minutes when the device will leave power saving mode each day. Alternatively, click the clock icon and select the time from the drop-down list.	12:00 AM

Wakeup End Time

Setting	Description	Factory Default
00 to 59	Specify the hour and minutes when the device will enter power saving mode each day. Alternatively, click the clock icon and select the time from the drop-down list.	12:15 AM

Start Date

Setting	Description	Factory Default
Date	Specify the date this cycle rule will take effect.	None

End Date

Setting	Description	Factory Default
Date	Specify the date this cycle rule will end.	None

Modify a Cycle Rule

From the Wakeup Cycle Rule list, click the pencil ( ) icon next to the entry you want to edit.

Depending on the type of rule, refer to the following sections for a description of each field:

- Create an Hourly Cycle Rule
- Create a Daily Cycle Rule
- Create a Weekly Cycle Rule
- Create a Monthly Cycle Rule

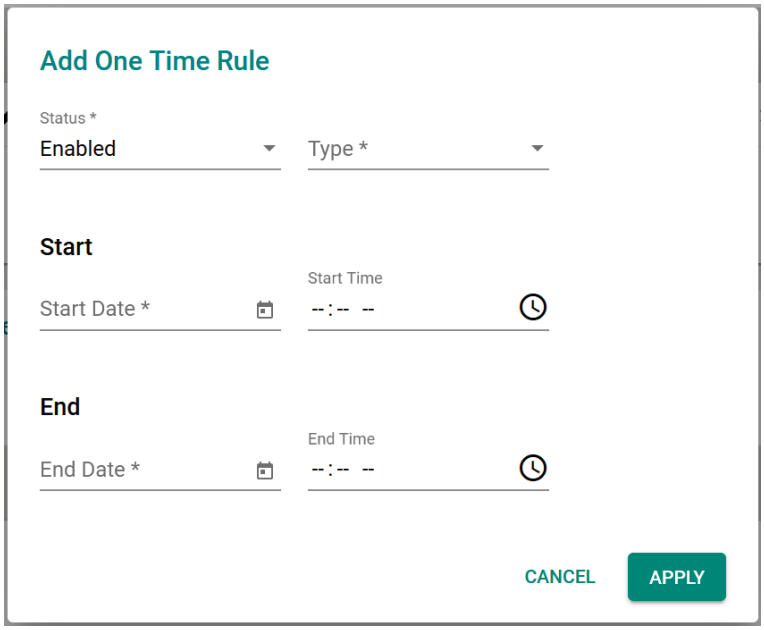
Delete a Cycle Rule

To delete one or multiple cycle rule(s), select the entries from the Wakeup Cycle Rule list and click the icon.

Create a One-time Rule

One-time rules allow you to configure the power saving schedule for a specific period. These rules do not repeat and have a higher priority than cycle rules. A maximum of 12 one-time rules can be created.

From the One Time Rule list, click the **Add** ( ) icon to add a new entry.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the one-time rule.	Enabled

Type

Setting	Description	Factory Default
Power Saving	The device will enter power saving mode for the specified period.	Enabled
Wake Up	The device will leave power saving mode for the specified period. This requires an active cycle rule.	

Start Date

Setting	Description	Factory Default
Date	Specify the date this one-time rule will take effect.	None

End Date

Setting	Description	Factory Default
Date	Specify the date this one-time rule will end.	None

Modify a One-time Rule

From the One Time Rule list, click the pencil ( ) icon next to the entry you want to edit.

Refer to Create a One-time Rule for a description of each field.

Delete a One-time Rule

To delete one or multiple one-time rule(s), select the entries from the One Time Rule list and click the icon.

SMS

When the cellular connection is not available or if there is limited service, SMS provides an emergency recovery mechanism and a way for performing out-of-band management. The remote SMS control feature enables users to get the current cellular status of the device, re-establish the cellular connection, and restart the system by sending specific SMS messages to the device. To ensure the security of out-of-band communication, the SMS function supports password protection and trusted number authentication.

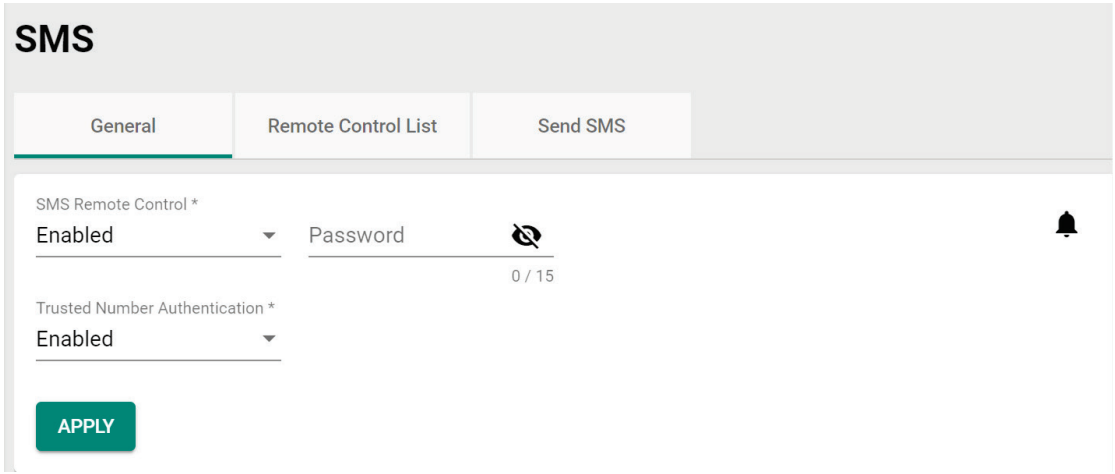
With wireless out-of-band management, engineers can control and troubleshoot remote devices, avoiding costly onsite visits by service technicians and minimizing service downtime.

NOTE

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

General

From the General tab, you can enable SMS functionality and configure trusted number authentication.



SMS Remote Control

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable remote control SMS. If enabled, the device can be controlled remotely through specific SMS messages.	Enabled

Password

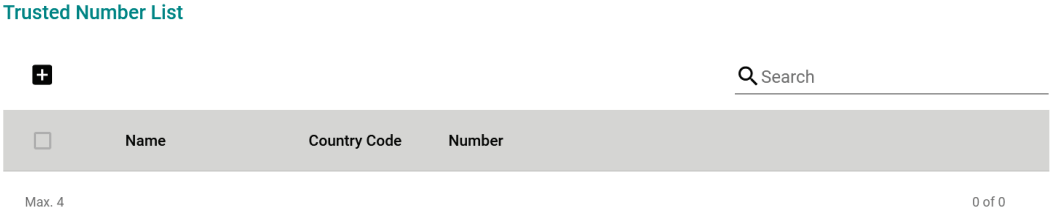
Setting	Description	Factory Default
0 to 15	Specify how long (in minutes) the device will wait before entering power-saving mode if the conditions are met.	None

Trusted Number Authentication

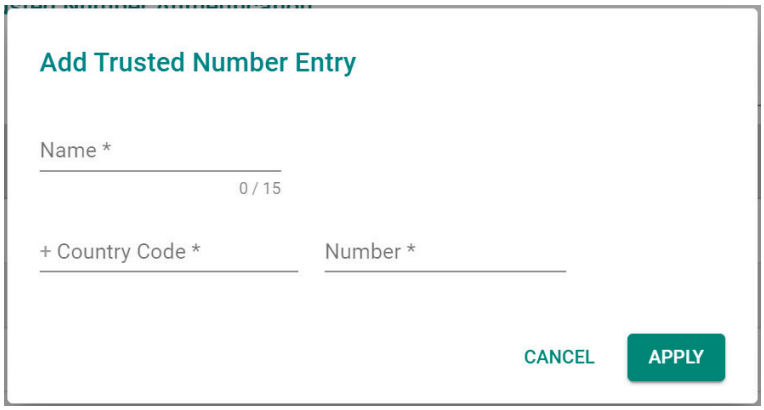
Setting	Description	Factory Default
Enabled or Disabled	Enable or disable trusted number authentication. If enabled, the device will only accept SMS messages from numbers added to the Trusted Numbers List. If disabled, the device can be controlled by messages sent from any number. Refer to Adding a Trusted Number.	Enabled

Add a Trusted Number

The device supports up to 4 trusted numbers.



Click the **Add** ( ) icon in the Trusted Number List to add a new entry.



Name

Setting	Description	Factory Default
0 to 15 characters	Enter a name for the number. This is for reference only and helps identify the number more easily.	None

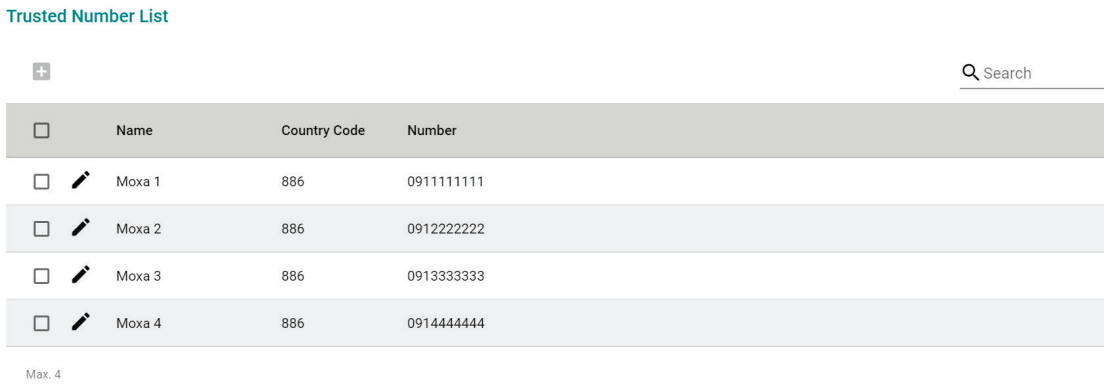
Country Code

Setting	Description	Factory Default
Country code	Specify the country code of the number.	None

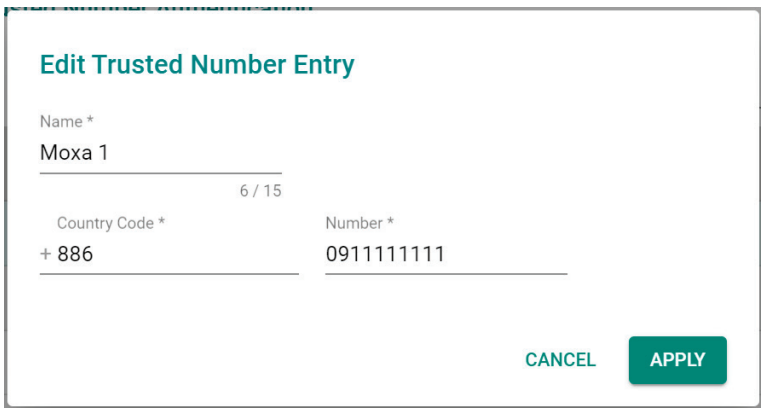
Number

Setting	Description	Factory Default
Phone number	Enter the phone number.	None

Modify a Trusted Number



Click the pencil ( ) icon next to the entry you want to edit.



Name

Setting	Description	Factory Default
0 to 15 characters	Enter a name for the number. This is for reference only and helps identify the number more easily.	None

Country Code

Setting	Description	Factory Default
Country code	Specify the country code of the number.	None

Number

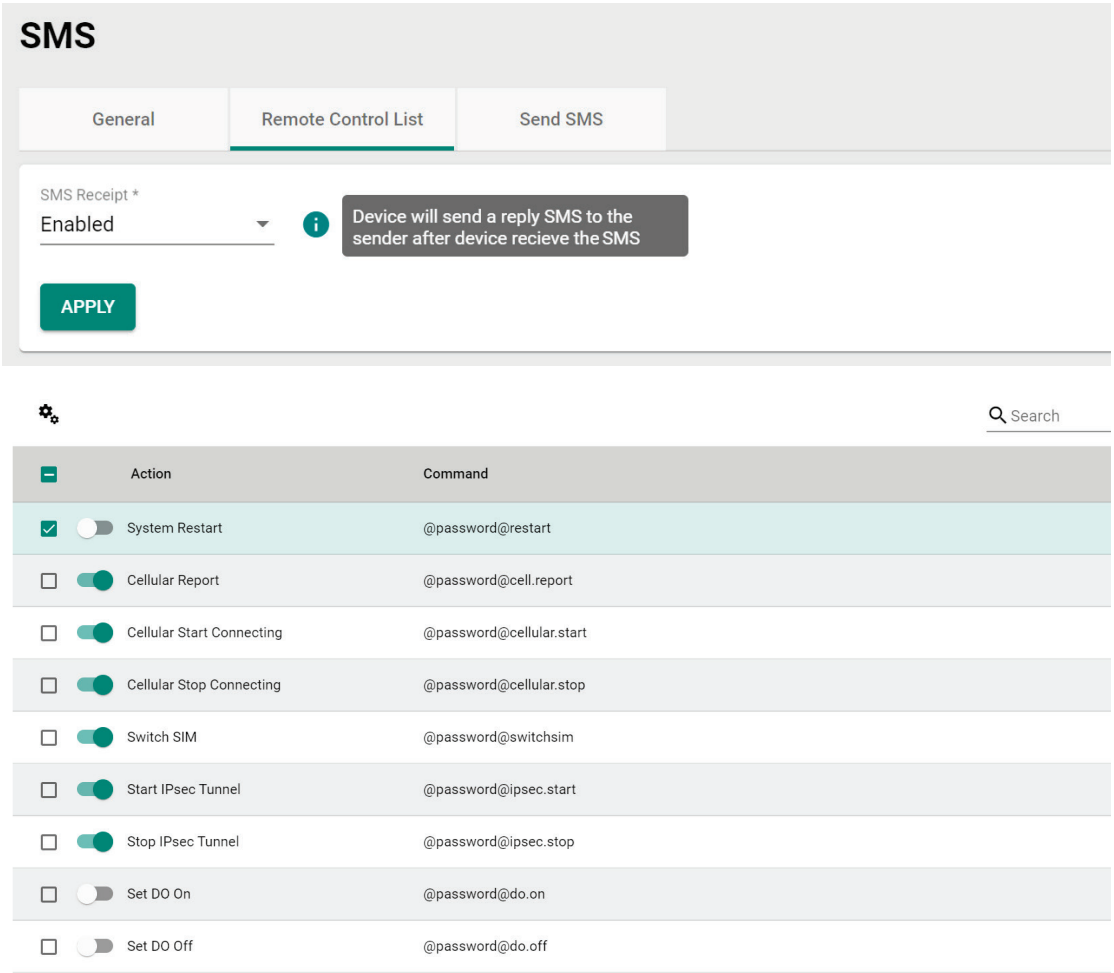
Setting	Description	Factory Default
Phone number	Enter the phone number.	None

Delete a Trusted Number

In the Trusted Number List, check the box of the number(s) you want to delete and click the trashcan ( ) icon.

Remote Control List

From the Remote Control List, you can select which SMS commands to enable.



SMS Receipt

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable SMS receipts. If enabled, the device will send a confirmation SMS when receiving a command SMS.	Enabled

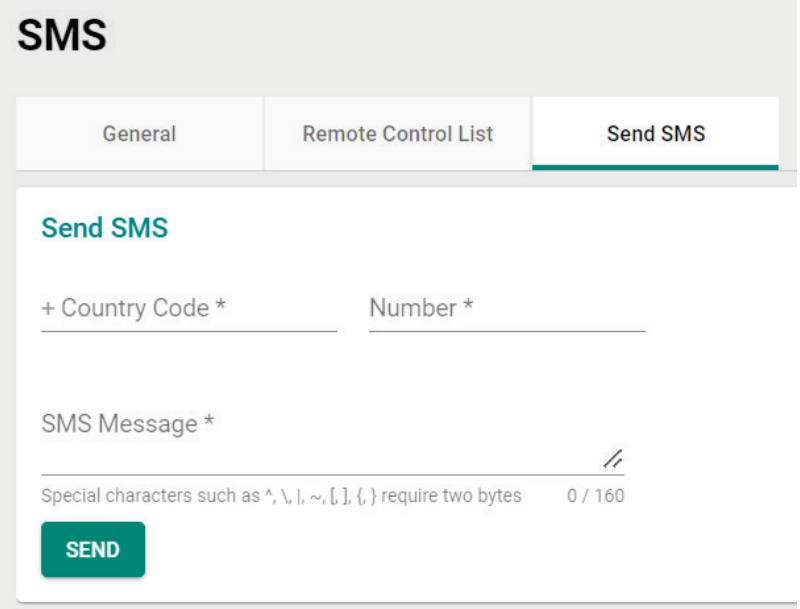
Use the toggle buttons to enable or disable the corresponding SMS command. Alternatively, check the boxes of the commands you want to manage and use the **Quick Setting** ( ) icon to enable or disable the selected commands in bulk.

Refer to the table below for an overview of each command.

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

Send SMS

From the Send SMS screen, you can send a personalized SMS message from the device to the specified recipient.



Country Code

Setting	Description	Factory Default
Country code	Specify the country code of the recipient's number.	None

Number

Setting	Description	Factory Default
Phone number	Enter the recipient's phone number.	None

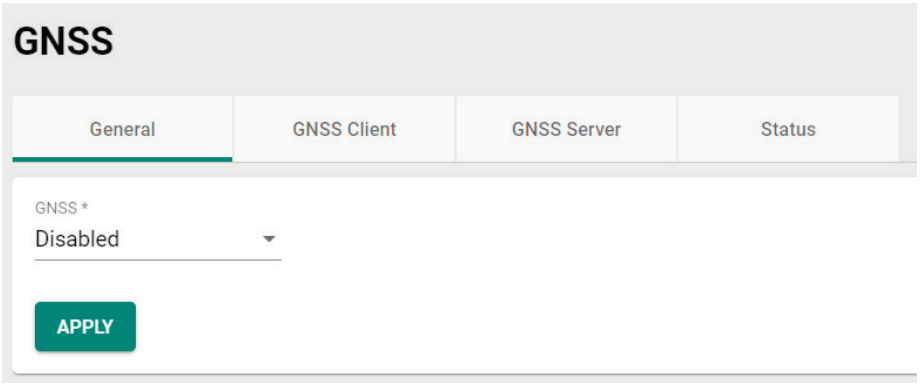
Message

Setting	Description	Factory Default
0 to 160 characters	Enter a message.	Enabled

GNSS

General

From the General screen, you can enable or disable GNSS functionality.

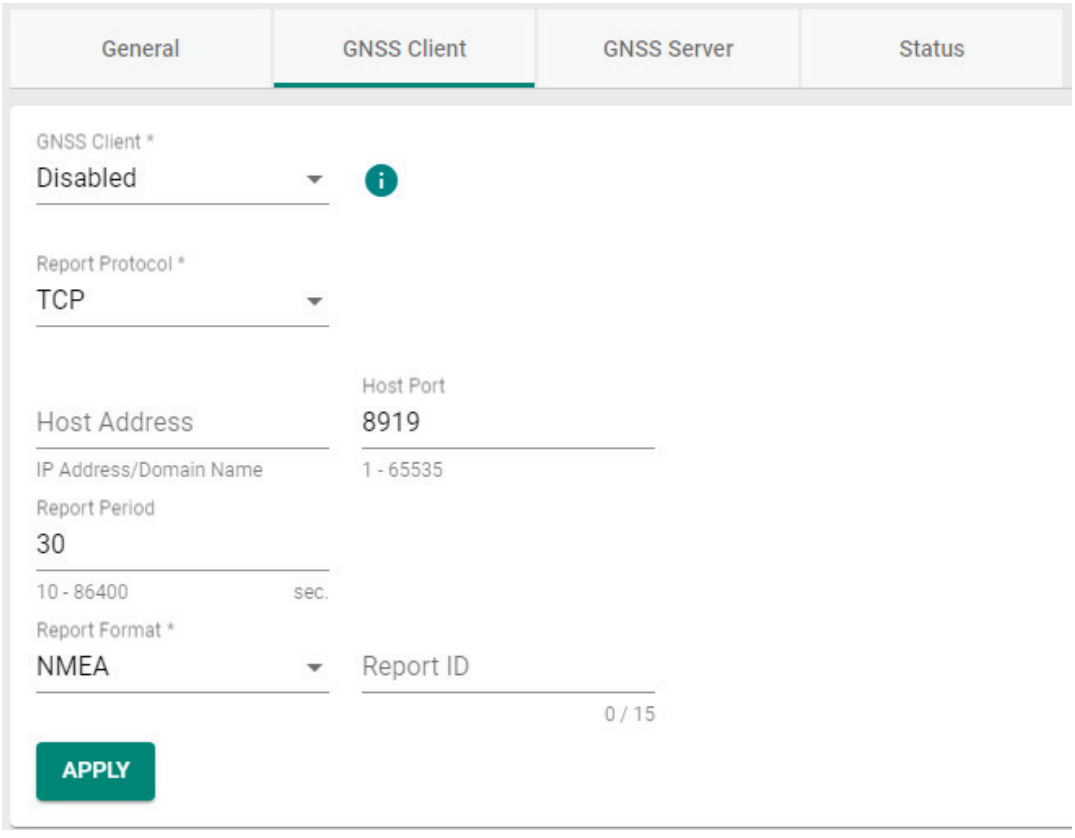


GNSS

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable GNSS functionality. If enabled, the device will use satellite positioning to show its real-time physical location on the map.	Enabled

GNSS Client

From the GNSS Client screen, you can configure GNSS Client settings which will allow the system to send GNSS data to a user-configured server.



GNSS Client

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable GNSS Client functionality. If enabled, the device will send GNSS data to the configured server at a specified interval.	Disabled

Report Protocol

Setting	Description	Factory Default
TCP	Send reports over TCP. This requires a receipt from the server to confirm the data was delivered.	TCP
UDP	Send reports over UDP. This does not require a receipt from the server.	

Host Address

Setting	Description	Factory Default
IP address/domain name	Enter the IP address or host name of the server that will receive the GNSS data.	None

Host Port

Setting	Description	Factory Default
1 to 65535	Enter the TCP or UDP port number of the server that will receive the GNSS data.	8919

Report Period

Setting	Description	Factory Default
10 to 86400	Specify the interval (in seconds) at which GNSS data reports are generated.	30

Report Format

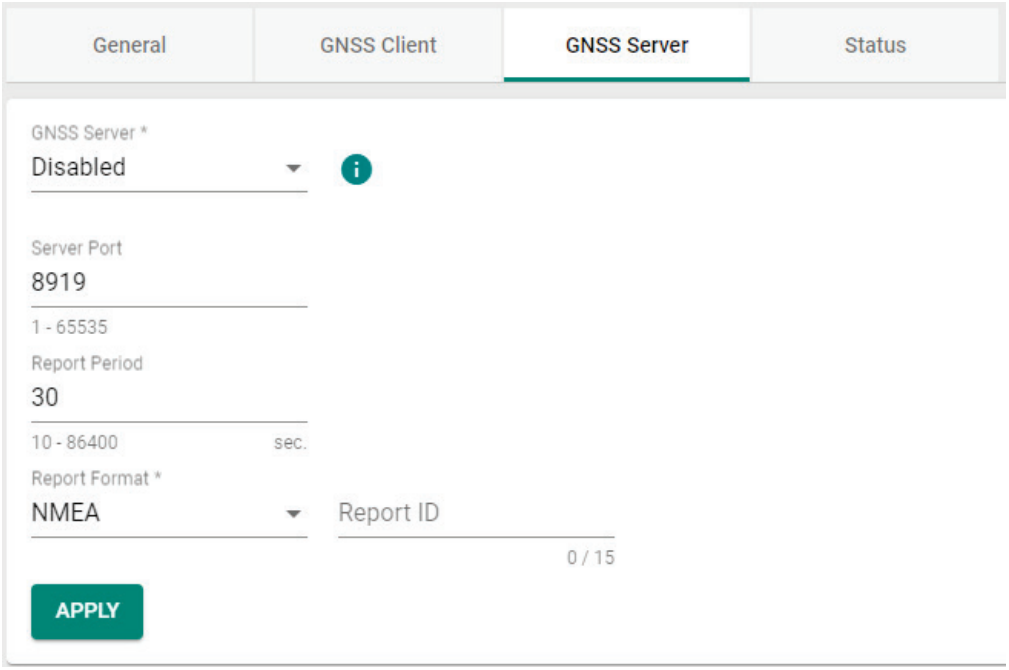
Setting	Description	Factory Default
NMEA	Send GNSS data in the standard NMEA format.	NMEA
General	Send GNSS data in latitude-longitude format.	

Report ID

Setting	Description	Factory Default
Max. 15 characters	Enter the ID of the GNSS data report header. The Report ID and device MAC address will be included in the NMEA or General format.	None

GNSS Server

From the GNSS Server screen, you can configure the GNSS Server to allow clients to request GNSS data reports.



GNSS Server

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable GNSS Server functionality. If enabled, clients will be able to request GNSS data reports from this server.	Disabled

Server Port

Setting	Description	Factory Default
1 to 65535	Enter the UDP port number for clients to access the server.	8919

Report Period

Setting	Description	Factory Default
10 to 86400	Specify the interval (in seconds) at which GNSS data reports are generated.	30

Report Format

Setting	Description	Factory Default
NMEA	Send GNSS data in the standard NMEA format.	NMEA
General	Send GNSS data in latitude-longitude format.	

Report ID

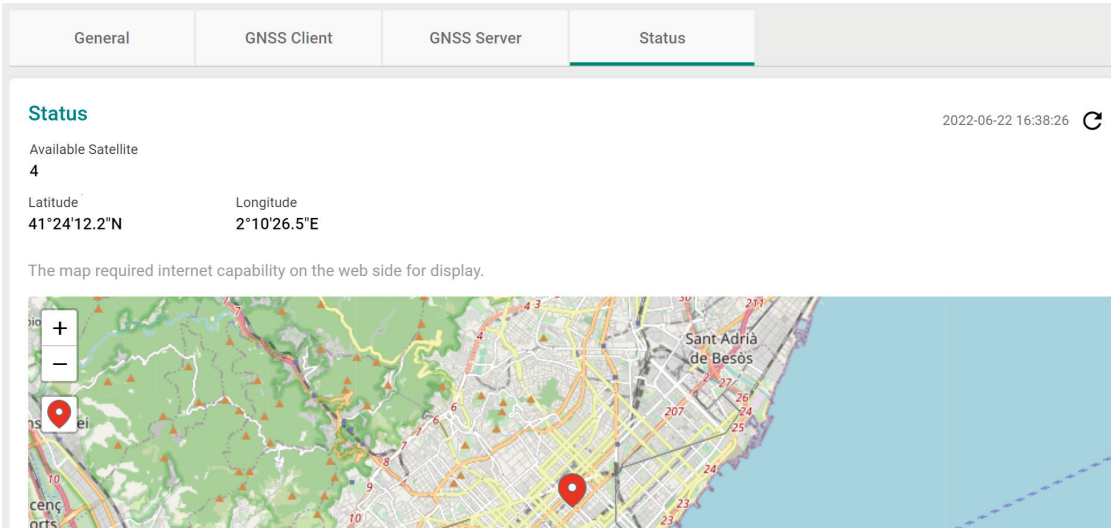
Setting	Description	Factory Default
Max. 15 characters	Enter the ID of the GNSS data report header. The Report ID and device MAC address will be included in the NMEA or General format.	None

Status

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

NOTE

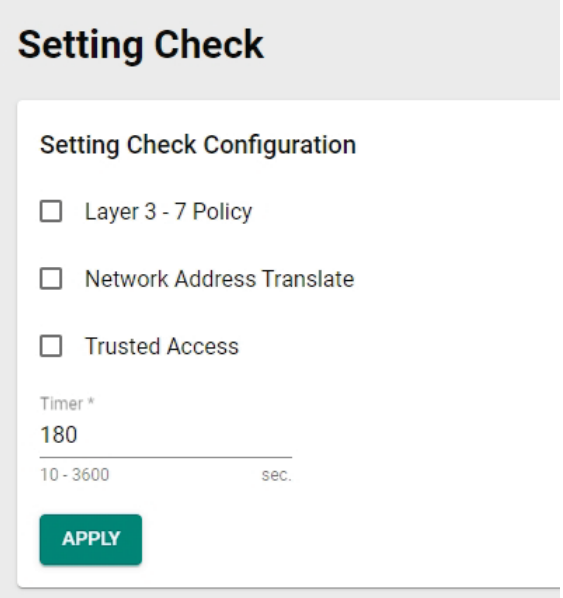
The device's physical location and coordinates will only show if GNSS is enabled. Refer to the General section.



Field	Description
Available Satellite	The number of satellites being contacted.
Latitude	The north–south position of the device.
Longitude	The east–west position of the device.
	Click to refresh the coordinate data.
	Click to zoom in or zoom out on the map.
	Click to center the device on the map.

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 industrial secure router. 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.

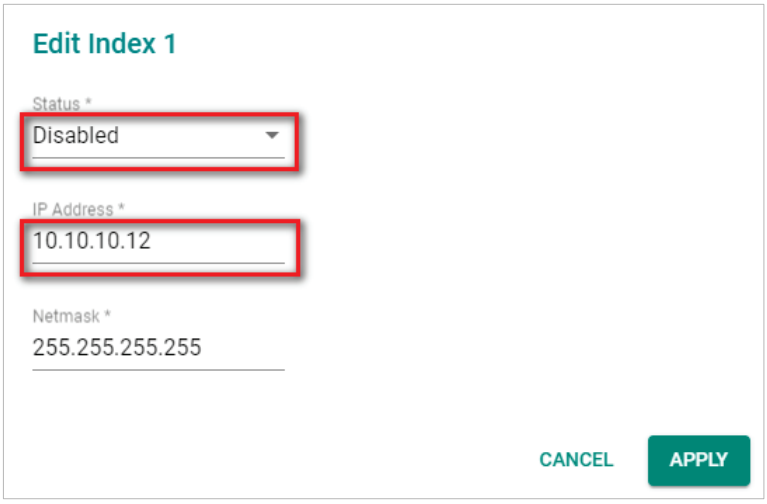
Trusted Access

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

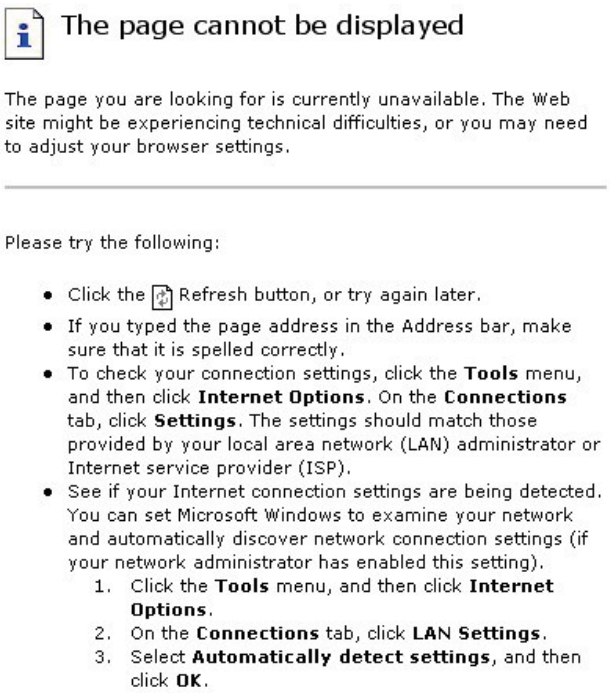
Timer

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.

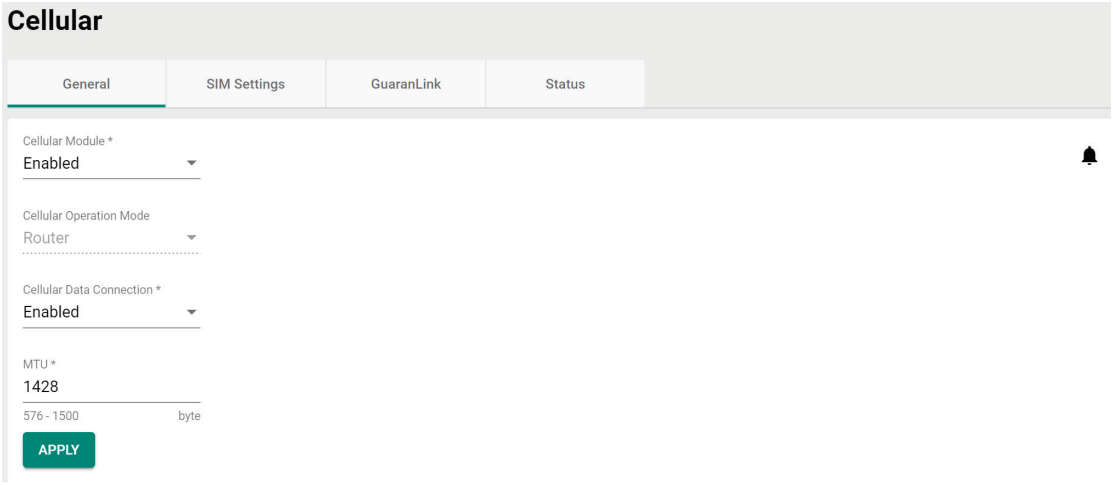


If the new configuration does not block the remote user's connection to the Industrial Secure Router, the user will see the Setting Check Confirmed page. Click **CONFIRM** to save and apply the changes.

Cellular

The Cellular section allows users to configure mobile network connection settings.

General



Cellular Module

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the cellular module for establishing cellular connections, send SMS messages, and use GNSS services.	Enabled

Cellular Operation Mode

Setting	Description	Factory Default
Router	The device will function as an IP router for IP data communication.	Router

Cellular Data Connection

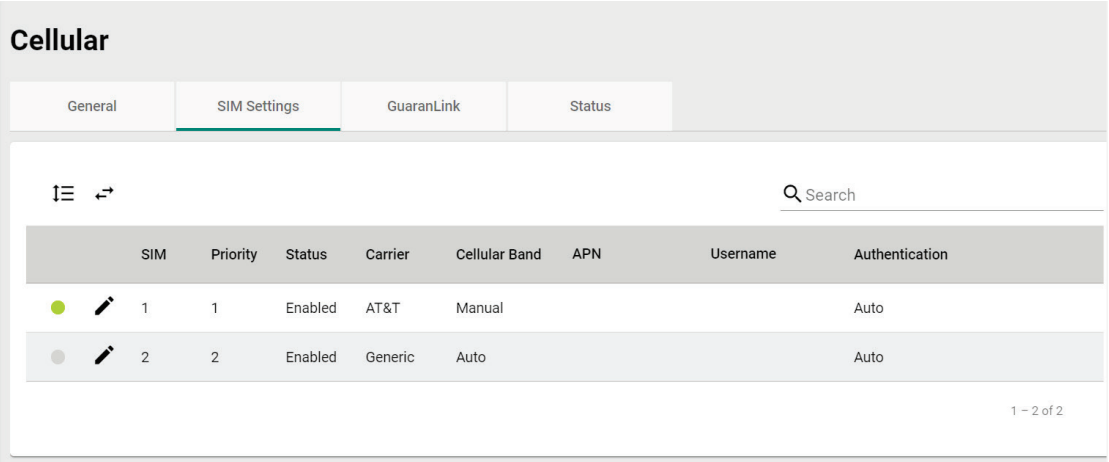
Setting	Description	Factory Default
Enabled or Disabled	Enable or disable cellular data connections. If enabled, cellular connections will incur data usage cost based on the ISP used.	Enabled

MTU

Setting	Description	Factory Default
576 to 1500	Enter the Maximum Transmission Unit (MTU) value for router mode. The recommended MTU size may vary depending on the cellular carrier. Make sure the end device is set to the same MTU value for optimal performance.	Enabled

SIM Settings

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



Reordering SIM Card Priority

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

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

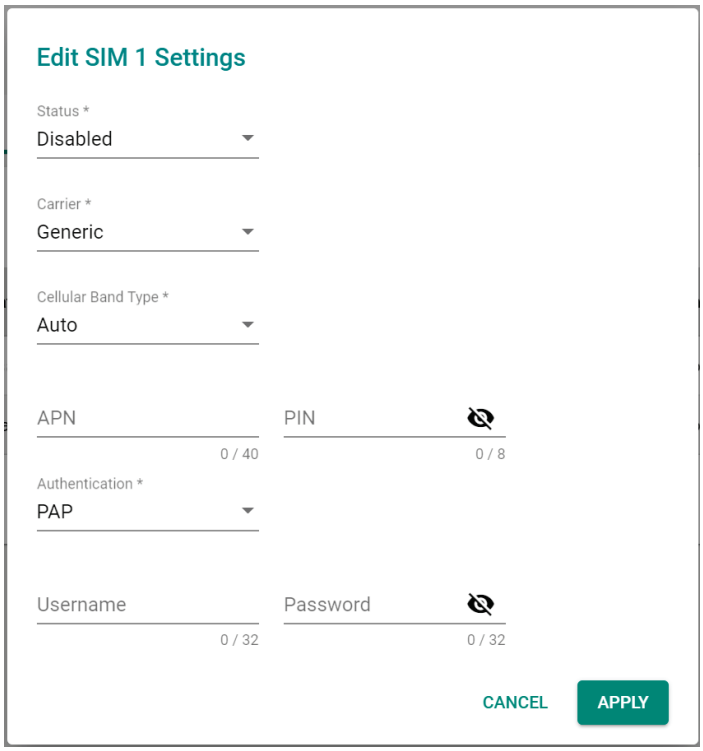
Changing the Active SIM Card

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

Click the **Change SIM** ( ) icon to swap the active SIM card.

Editing SIM Card Settings

Click the pencil ( ) icon next to the SIM card you want to modify to edit its parameters.



Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the SIM card.	Enabled

Carrier

Setting	Description	Factory Default
Carrier	Select the carrier to use with the SIM card.	Generic

Cellular Band Type

Setting	Description	Factory Default
Auto	The device automatically negotiates the optimal cellular band frequency with the base station.	Auto
Manual	Manually specify the cellular band frequencies to use.	

Cellular Band (for Manual cellular band type)

Setting	Description	Factory Default
Checkbox	Select which cellular frequencies to use with this SIM card. Make sure your cellular carrier supports the selected bands.	Enabled

APN

Setting	Description	Factory Default
APN	Enter the access point network (APN) information if provided by your cellular carrier. The cellular carrier may provide different APN information to provide different service levels.	Enabled

PIN

Setting	Description	Factory Default
Max. 8 characters	Enter the PIN number to unlock the SIM card.	None

NOTE

Entering the wrong PIN code three times in a row will lock the SIM card.

Authentication

Setting	Description	Factory Default
Auto	Set up a session without specifying the authentication method.	Auto
PAP	Use PAP (Password Authentication Protocol) authentication. PAP will send the username and password to the server for authentication against the server's database.	
CHAP	Use CHAP (Challenge-Handshake Authentication Protocol) authentication. CHAP will generate a password which is changed frequently for improved identity security.	

Username (for PAP authentication)

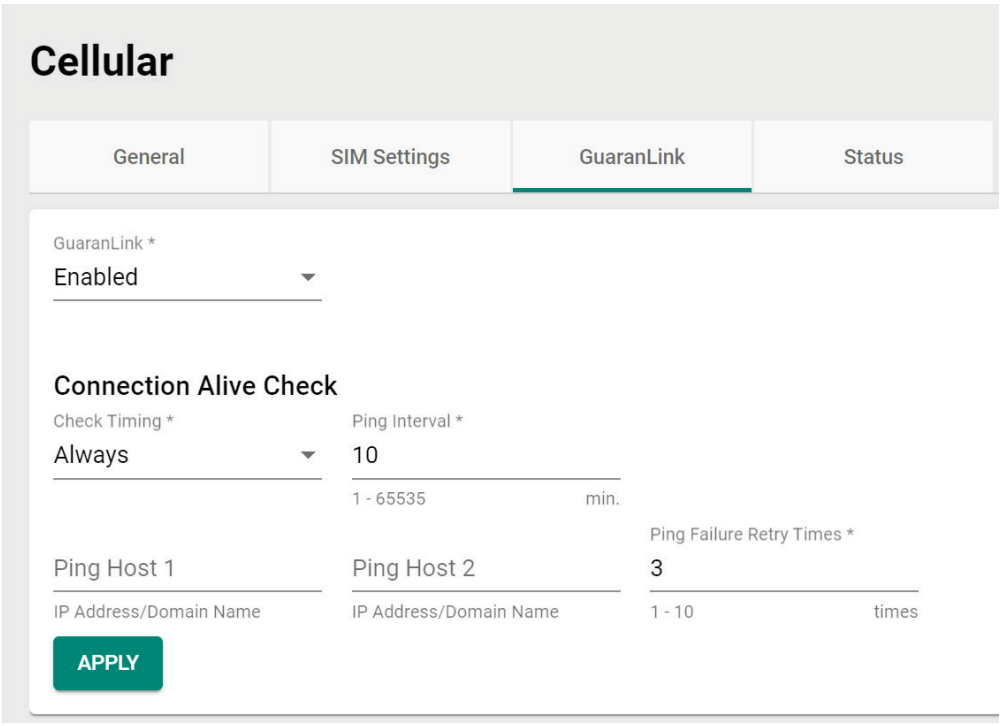
Setting	Description	Factory Default
Max. 32 characters	Enter the username for PAP authentication.	None

Password (for PAP authentication)

Setting	Description	Factory Default
Max. 32 characters	Enter the password for PAP authentication.	None

GuaranLink

A number of factors can contribute to connection failures in cellular communications, including loss of cellular signal, interference, connection errors caused by the base station, or termination by the operator for unknown reasons. Moxa's proprietary GuaranLink feature, which is different from the basic heartbeat function, enables reliable connectivity with 3 different connection checks and 4 levels of recovery actions. It is designed to fulfill different needs like minimizing the cellular cost without sending excessive cellular packets or optimizing the time it takes to swap to the backup SIM.



GuaranLink

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable GuaranLink. If enabled, the device will monitor cellular connections. If a connection failure is detected, the device will attempt to automatically recover the connection. Note that enabling this function will send additional alive check cellular messages, which may incur additional cellular costs.	None

Check Time

Setting	Description	Factory Default
Always	The device will constantly send out alive check packets to check for cellular connection issues.	Always
Idle Transmission	The device will only send alive check packets when the device has not received any data transmissions during the specified Ping Interval period (in minutes).	
Poor Signal	The device will only send alive check packets when the device identifies poor signal quality.	

If **Check Time** is set to **Always**, configure the following parameters:

Ping Interval

Setting	Description	Factory Default
1 to 86400	Specify the interval (in seconds) at which the device will send out an alive check packet.	10

Ping Host 1/2

Setting	Description	Factory Default
IP address/domain name	Enter the IP address or domain name of the remote host to ping. If both ping host 1 and 2 are configured, the device will perform connection alive checks for both hosts simultaneously. The device will only consider the connection failed if the device receives no response from both hosts.	8.8.8.8

Ping Failure Retry Times

Setting	Description	Factory Default
1 to 10	Specify the number of times the device will perform the connection alive check. If the check fails the specified number of retry times, the device will determine the cellular connection has failed and will initiate the GuaranLink recovery process.	3

If **Check Time** is set to **Idle Transmission**, configure the following parameters:

Idle Transmission Interval

Setting	Description	Factory Default
1 to 600	Specify the interval (in minutes) the device will wait for data transmissions. If no data transmissions take place during the interval, the device will perform a connection alive check.	5

Ping Host 1/2

Setting	Description	Factory Default
IP address/domain name	Enter the IP address or domain name of the remote host to ping. If both ping host 1 and 2 are configured, the device will perform connection alive checks for both hosts simultaneously. The device will only consider the connection failed if the device receives no response from both hosts.	None

Ping Failure Retry Times

Setting	Description	Factory Default
1 to 10	Specify the number of times the device will perform the connection alive check. If the check fails the specified number of retry times, the device will determine the cellular connection has failed and will initiate the GuaranLink recovery process.	3

If **Check Time** is set to **Poor Signal**, configure the following parameters:

Signal Checking Interval

Setting	Description	Factory Default
1 to 600	Specify the interval (in minutes) the device will check the host for poor signal quality. If the device identifies the host has poor signal quality, the device will perform a connection alive check.	5

Ping Host 1/2

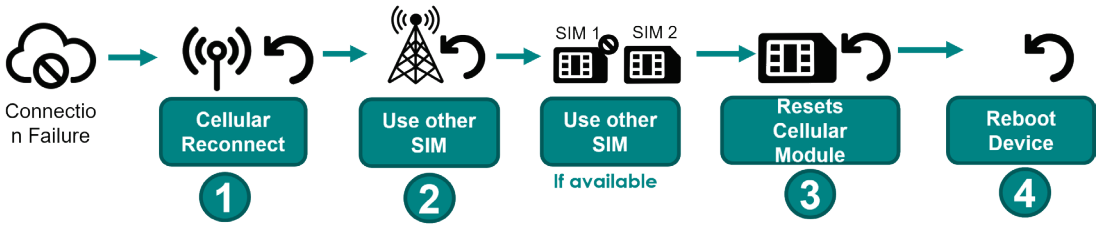
Setting	Description	Factory Default
IP address/domain name	Enter the IP address or domain name of the remote host to ping. If both ping host 1 and 2 are configured, the device will perform connection alive checks for both hosts simultaneously. The device will only consider the connection failed if the device receives no response from both hosts.	None

Ping Failure Retry Times

Setting	Description	Factory Default
1 to 10	Specify the number of times the device will perform the connection alive check. If the check fails the specified number of retry times, the device will determine the cellular connection has failed and will initiate the GuaranLink recovery process.	3

GuaranLink Recovery Settings

GuaranLink follows a sequential 4-stage recovery process to restore a failed cellular connection. If the first recovery action fails, it will move to the next action.



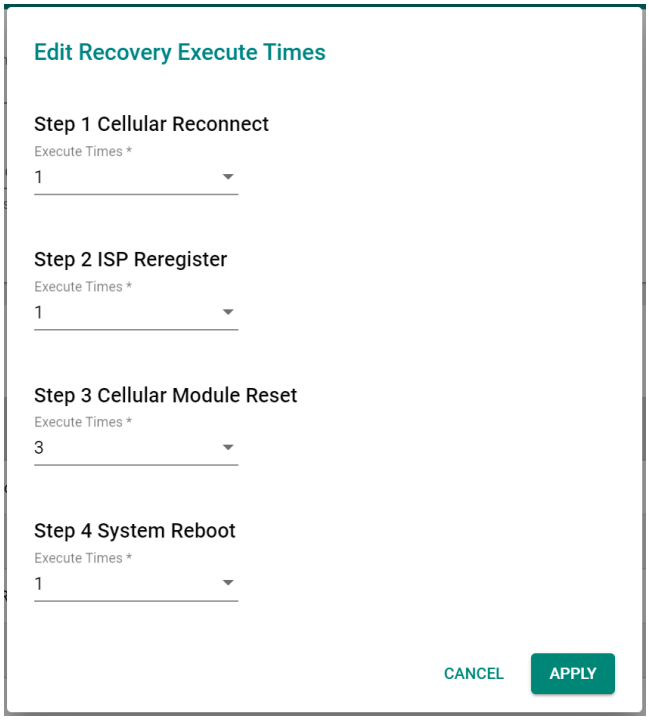
Editing GuaranLink Recovery Settings

You can adjust the criteria of these recovery options based on your specific requirements.

Click the pencil ( ) icon to modify the relevant recovery stage parameters.

GuaranLink Recovery Settings

Recovery Step	Recovery Action	Execute Times
1	Cellular Reconnect	1
2	ISP Reregister	1
3	Cellular Module Reset	3
4	System Reboot	1



Step 1 Cellular Reconnect

Setting	Description	Factory Default
0 to 5	The device will disconnect and attempt to re-establish the cellular connection for the specified number of attempts. If the connection is not restored after the specified amount of execute times, the device will move on to the next recovery step. If set to 0, the device will skip this step and move on to the next recovery step.	1

Step 2 ISP Reregister

Setting	Description	Factory Default
0 to 5	The device will re-register with the ISP to obtain a new IP address from the base station. If the connection is not restored after the specified amount of execute times, the device will move on to the next recovery step. If set to 0, the device will skip this step and move on to the next recovery step.	1

Step 3 Cellular Module Reset

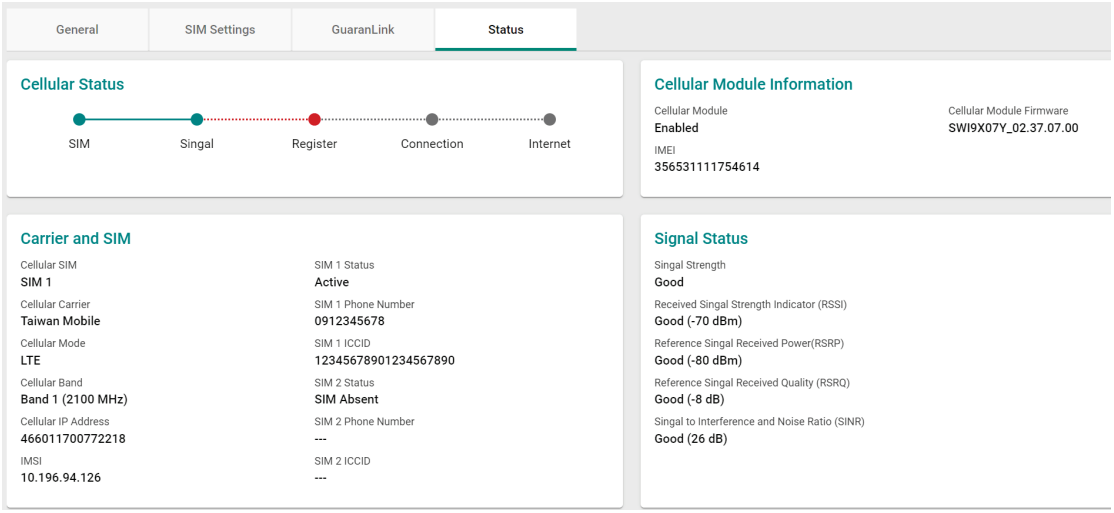
Setting	Description	Factory Default
0 to 10	The device will reset the cellular module. If the connection is not restored after the specified amount of execute times, the device will move on to the next recovery step. If set to 0, the device will skip this step and move on to the next recovery step.	3

Step 4 System Reboot

Setting	Description	Factory Default
0 to 1	The device will reboot the system. If the connection is not restored after the specified amount of execute times, the device will move on to the next recovery step. If set to 0, the device will not perform a system reboot.	1

Status

The Status screen shows the current status of the cellular connection, information about the cellular carrier and SIM card, cellular module, and signal strength.



Cellular Status

Field	Description
SIM	The status of the SIM card. Green: The SIM card is active Red: The SIM card is inactive.

Field	Description
Signal	The cellular signal status. Green: The signal is good. Red: No signal.
Register	The cellular registration status. Green: The device successfully registered with the base station. Red: The device failed to register with the base station.
Connection	The network connection status. Green: The device obtained an IP address from the base station. Red: The device failed to obtain an IP address from the base station.
Internet	The Internet connection status. Green: The device is connected to the Internet. Red: The device failed to connect to the Internet.

Cellular Module Information

Field	Description
Cellular Module	The current status of the cellular module.
Cellular Module Software	The firmware version of the cellular module.
IMEI	The International Mobile Equipment Identity number.

Carrier and SIM

Field	Description
Cellular SIM	The SIM card used for establishing the cellular connection.
Cellular Carrier	The cellular service provider used.
Cellular Mode	The cellular connection technology (LTE, HSPA, …) used.
Cellular Band	The cellular band frequency in use.
Cellular IP Address	The cellular IP address assigned by the cellular carrier.
IMSI	The International Mobile Subscriber Identity number.
SIM 1 Status	The status of the SIM card installed in SIM slot 1.
SIM 1 Phone Number	The phone number of the SIM card in SIM slot 1.
SIM 1 ICCID	The Integrated Circuit Card ID of the SIM card in SIM slot 1.
SIM 2 Status	The status of the SIM card installed in SIM slot 2.
SIM 2 Phone Number	The phone number of the SIM card in SIM slot 2.
SIM 2 ICCID	The Integrated Circuit Card ID of the SIM card in SIM slot 2.

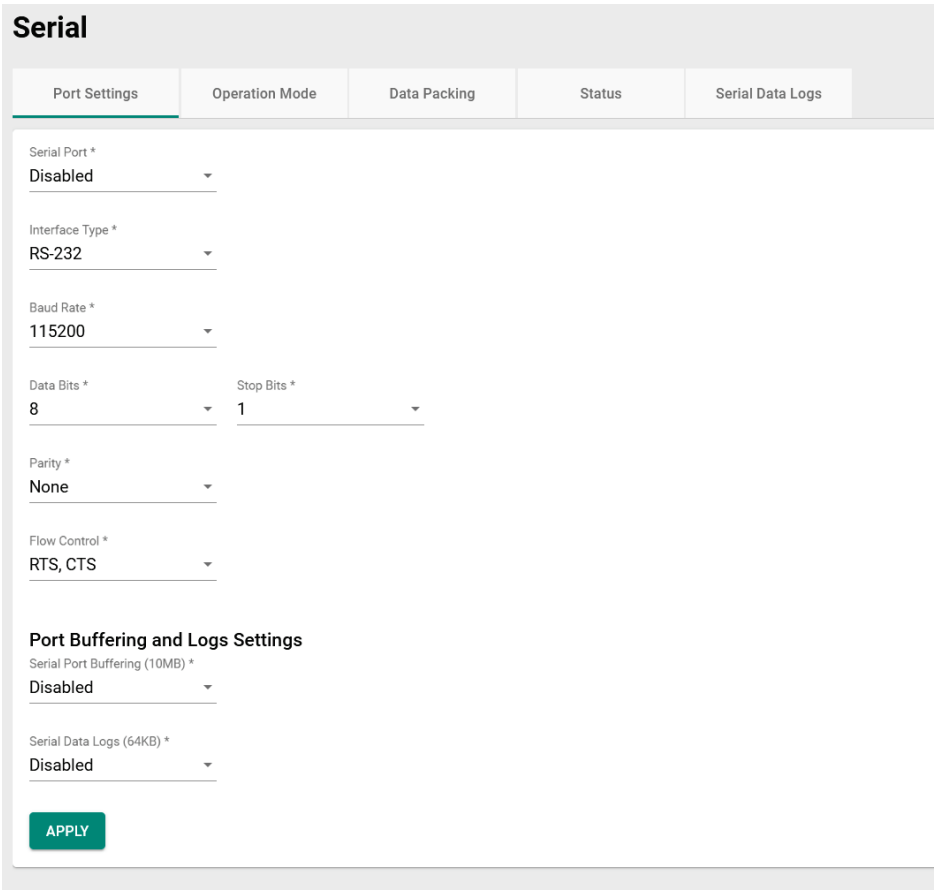
Signal Status

Field	Description
Signal Strength	The current overall signal strength of the device.
RSRP (Reference Signal Received Power)	The current RSRP. Good: Higher than -85dBm Average: -85 to -105dBm Poor: -105 to -115 dBm Inadequate: Less than-115 dBm
RSSI (Received Signal Strength Indicator)	The current RSSI. Good: Higher than -73 dBm Average: -73 to -89 dBm Poor: -89 to -113 dBm Inadequate: Less than -113 dBm
RSRQ (Reference Signal Received Quality)	The current RSRQ. Good: Higher than -10 dB Average: -10 to -15 dB Poor: -15 to -20 dB Inadequate: Less than -20 dB
SINR (Signal to Interference and Noise Ratio)	The current SINR. Good: Higher than 25 dB Average: 11 to 25 dB Poor: 3 to 11 dB Inadequate: Less than 3 dB

Serial

Port Settings

The Port Settings screen lets you enable or disable the serial port and configure the serial communication parameters. When enabled, the device allows for traditional serial (RS-232/422/485) devices to transmit data over the cellular network. The serial port settings on the device should match the parameters configured for the connected serial device. Refer to the serial device's user manual to determine the appropriate serial communication parameters.



Serial Port

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

Interface Type

Setting	Description	Factory Default
RS-232, RS-422, 2-wire-RS-485, 2-wire-RS-485	Select the serial interface for the serial device.	RS-232

Baud Rate

Setting	Description	Factory Default
300 to 921600	Specify the data transmission rate to and from the serial device.	115200

Data Bits

Setting	Description	Factory Default
5 to 8	Specify the size of the data character.	8

Stop Bits

Setting	Description	Factory Default
1 to 2	Specify the size of the stop character.	1

Parity

Setting	Description	Factory Default
None, Even, Odd, Space, Mark	Select the parity mode. Even and Odd parity provide rudimentary error-checking. Space and Mark parity are rarely used.	None

Flow Control

Setting	Description	Factory Default
None, RTS/CTS, DTR/DSR, Xon/Xoff	Select the flow control method. This determines how the system will suspend and resume data transmissions to prevent data loss. RTS/CTS (hardware) flow control is recommended.	RTS/CTS

Port Buffering

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable serial port buffering. If the WAN connection is down, the router will keep the serial data and retransmit the buffered data when the WAN connection is back. If disabled, serial data is lost if the WAN connection is down.	Disabled

NOTE

Port buffering can be used in Real COM, Reverse Real COM, RFC2217, TCP Server, and TCP Client modes. For other modes, the port buffering settings will have no effect. The maximum buffer size is 10 MB. Buffer data exceeding 10 MB will overwrite previous data.

Serial Data Logs

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable serial data logs. If enabled, the router will store the serial data logs on the system RAM.	Disabled

NOTE

The system RAM can save up to 64 kb of serial data logs. Serial log data will be cleared when the router powered off.

Operation Mode

The industrial secure router enables traditional serial (RS-232/422/485) devices to transmit data over the cellular network and allows you to access, manage, and configure remote facilities and equipment over the cellular network from anywhere in the world. The operation mode determines how the device's serial port will interact with the network. Which operation mode to select will depend on your specific application.

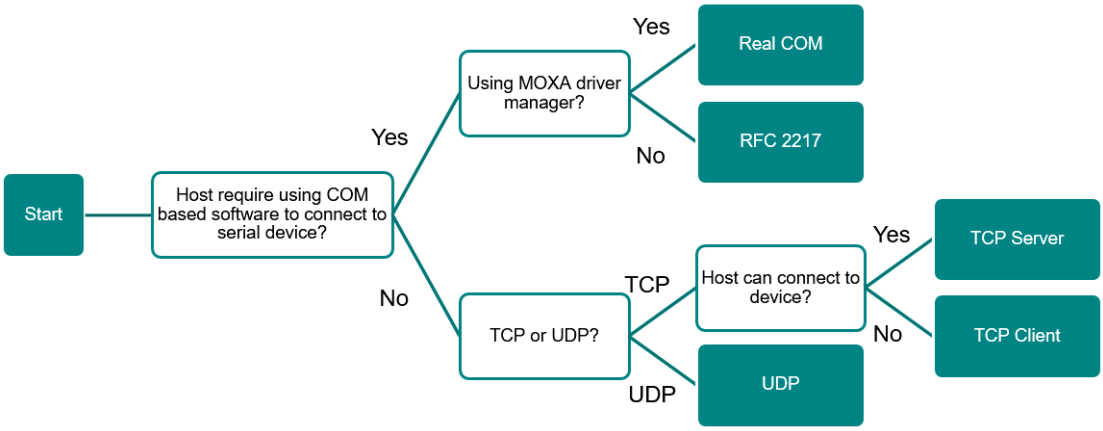
Traditional SCADA and data collection systems rely on the serial port to collect data from various types of instruments. Some software is required to connect the serial device to the COM port on the host computer. The Real COM and RFC 2217 modes allow you to expand a virtual COM port for a host computer on demand. As long as your host computer supports the TCP/IP protocol, SCADA and data collection systems will be able to access all instruments connected to a standard TCP/IP network, regardless of whether the devices are used locally or at a remote site.

The main difference between Real COM and RFC 2217 mode is that Real COM mode requires MOXA Windows Driver Manager to be installed on the host. The RFC 2217 mode allows third party drivers that support the RFC 2217 standard to perform virtual COM mapping to the serial port on the industrial secure router.

Some applications do not require the serial device to be physically connected connect to a COM port, but only need to establish a connection to receive data from the serial device. In that case, you can use TCP or

UDP mode to establish the connection. The main difference between the TCP and UDP protocols is that TCP guarantees delivery of data by requiring the recipient to send an acknowledgement to the sender. UDP does not require this type of verification, making it possible to offer faster delivery.

TCP Server mode allows the host to request a connection to the industrial secure router. In TCP Client mode, the industrial secure router actively establishes a connection to a host computer for serial data transmission. If the industrial secure router is using a cellular connection and is difficult to access via fixed IP or VPN, you should select TCP Client mode and directly connect to the host.

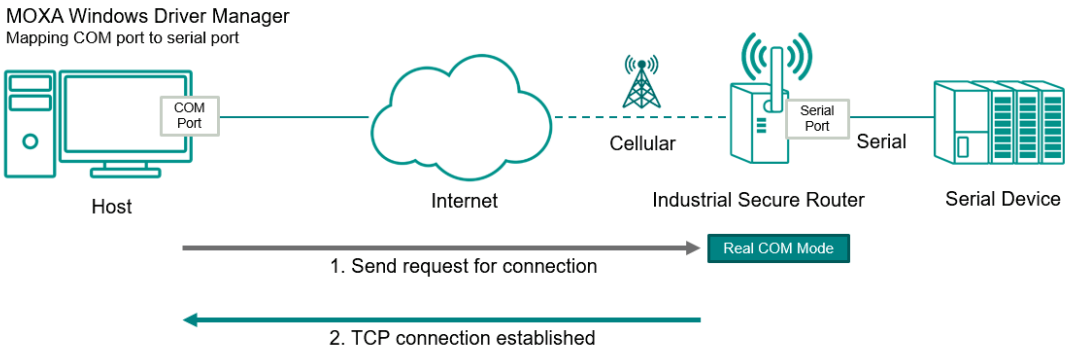


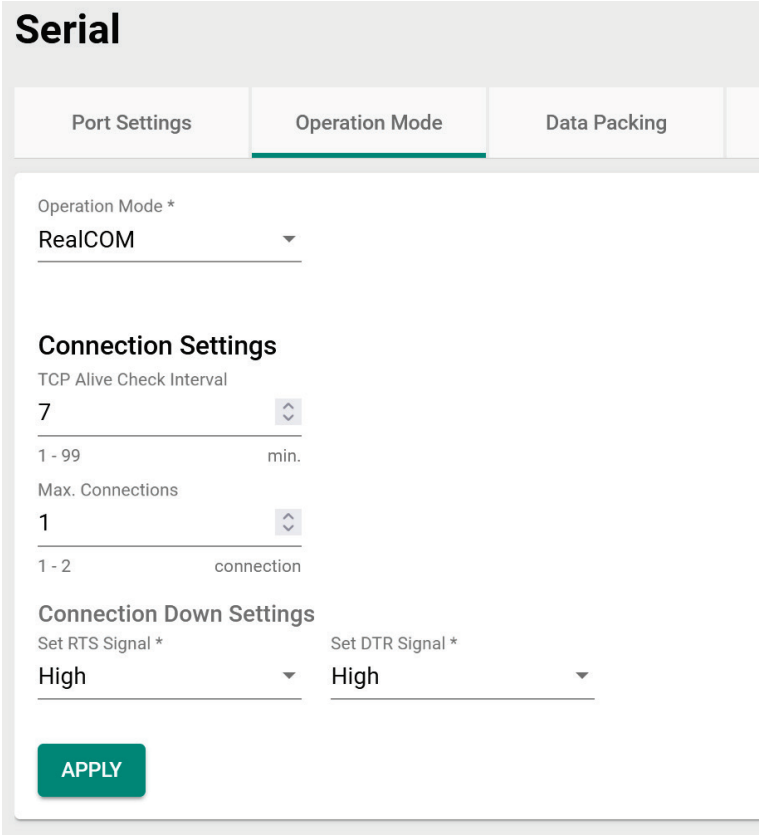
Real COM Mode

In Real COM mode, the bundled drivers can establish a transparent connection between a host and a serial device by mapping the serial port on the industrial secure router to a local COM port on the host computer.

One of the major benefits of using Real COM mode is that it allows you to use software that was written for strictly serial communication applications. The Moxa driver manager intercepts data sent to the host's COM port, packs it into a TCP/IP packet, and then redirects it through the host's Ethernet card to the Internet. At the other end of the connection, the industrial secure router accepts the IP frame from the cellular network, unpacks the TCP/IP packet, and then transparently sends the data through the serial port to the attached serial device. This operation mode supports up to 2 simultaneous connections, enabling multiple hosts to collect data from the same serial device at the same time.

Make sure your cellular service provider offers a fixed public IP address or VPN solution to allow the host to access to the industrial secure router.





Connection Settings

TCP Alive Check Interval

Setting	Description	Factory Default
1 to 99	Specify the interval (in minutes) at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any "keep alive" packets. Disabling this option can help free up device resources.	7

Max. Connections

Setting	Description	Factory Default
1 to 2	Specify the maximum number of simultaneous connections that the port will accept. Up to 2 hosts can simultaneously collect data from the same serial device.	1

Connection Down Settings

You can configure what happens to the RTS and DTR signals when the cellular or Ethernet connection goes down. For some applications, serial devices require RTS or DTR signals sent via the serial port to know the cellular or Ethernet link status.

Set RTS Signal

Setting	Description	Factory Default
High	The cellular or Ethernet connection status will not affect RTS signals.	High
Low	If the cellular or Ethernet connection is lost, RTS signals will change to low.	

Set DTR Signal

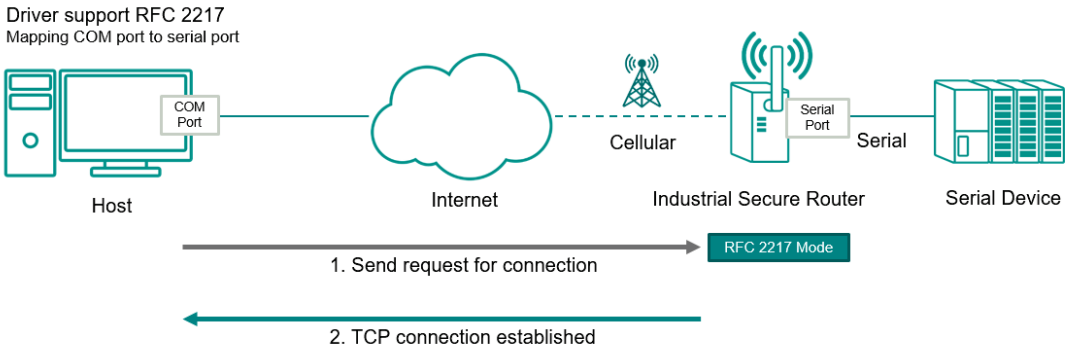
Setting	Description	Factory Default
High	The cellular or Ethernet connection status will not affect DTR signals.	High

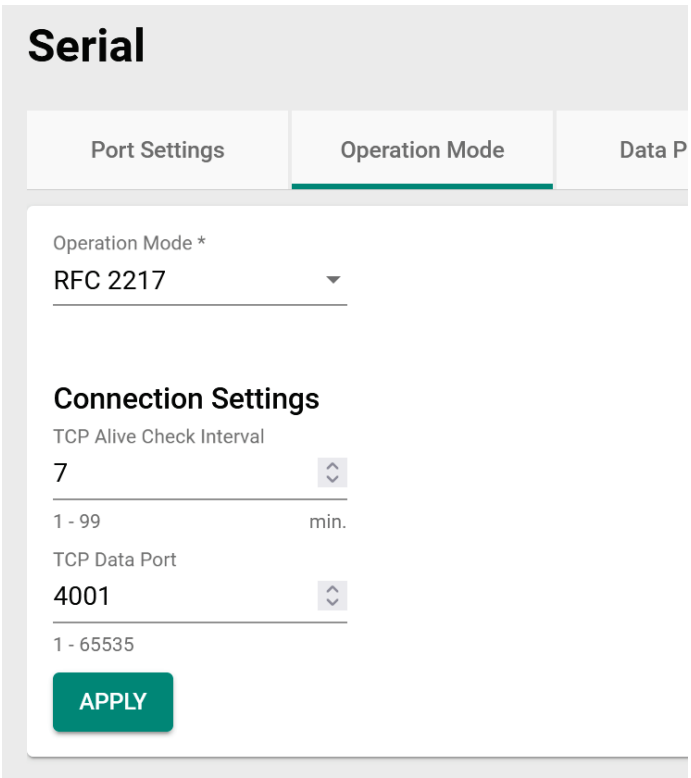
Setting	Description	Factory Default
Low	If the cellular or Ethernet connection is lost, DTR signals will change to low.	

RFC 2217 Mode

Similar to Real COM mode, RFC-2217 mode also uses a driver to establish a transparent connection between a host computer and a serial device by mapping the serial port on the Industrial Secure Router to a local COM port on the host computer. RFC2217 defines general COM port control options based on the Telnet protocol. Third party drivers supporting RFC-2217 are widely available on the Internet and can be used to implement virtual COM mapping to serial port on the Industrial Secure Router.

Make sure your cellular service provider offers a fixed public IP address or VPN solution to allow the host to access to the industrial secure router.





TCP Alive Check Interval

Setting	Description	Factory Default
1 to 99	Specify the interval (in minutes) at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any "keep alive" packets. Disabling this option can help free up device resources.	7

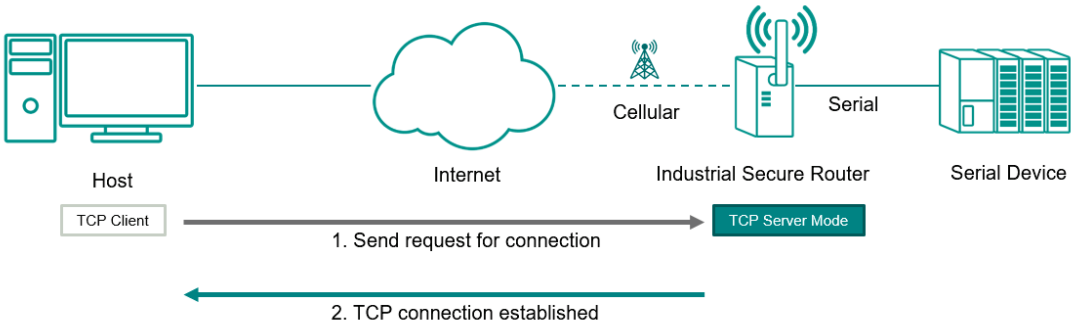
TCP Data Port

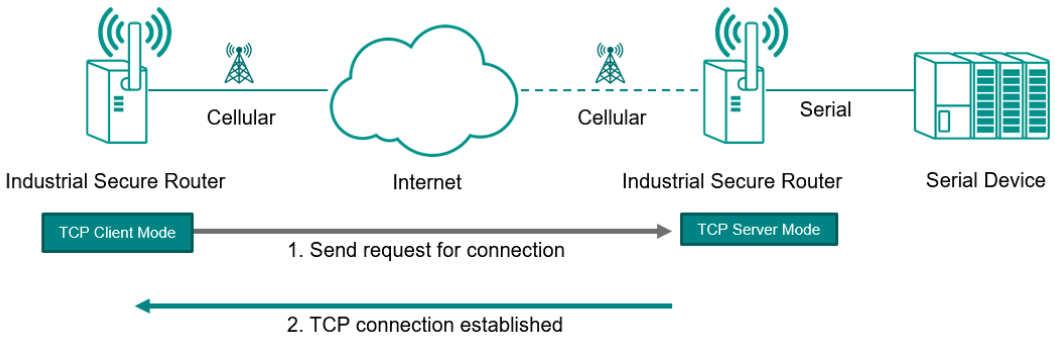
Setting	Description	Factory Default
1 to 65535	Specify the TCP port number for the serial port used to listen to connections and used by other devices to contact the serial port. To avoid conflicts with well-known TCP ports, the default is set to 4001.	4001

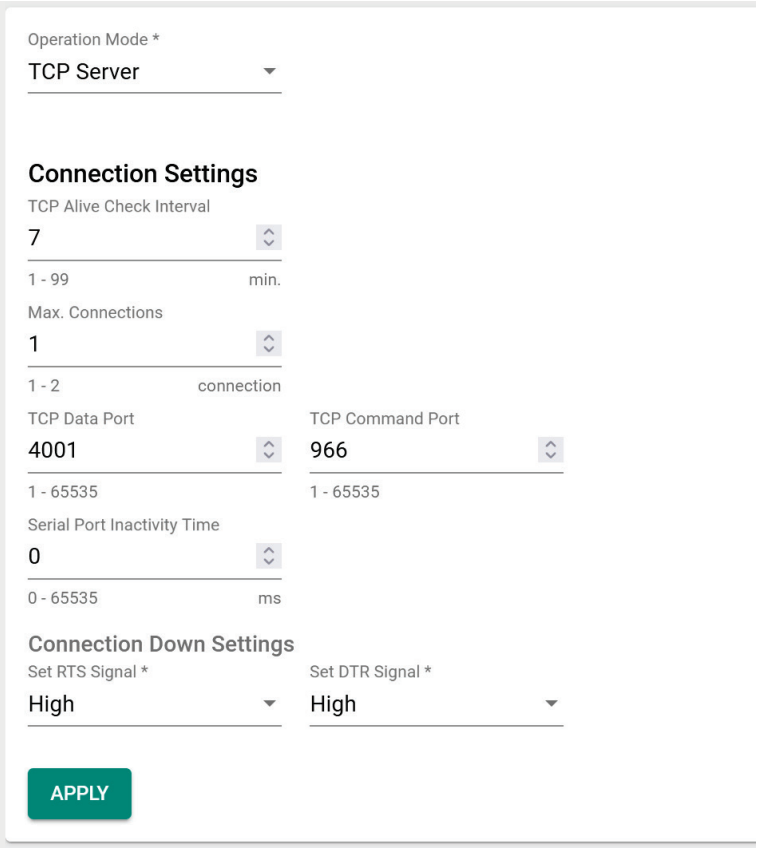
TCP Server Mode

In TCP Server mode, the serial port on the Industrial Secure Router is assigned a unique IP/port combination on a TCP/IP network. The host computer initiates contact with the Industrial Secure Router, establishes the connection, and receives data from the serial device. This operation mode supports up to 2 simultaneous connections, enabling multiple hosts to collect data from the same serial device at the same time.

Make sure your cellular service provider offers a fixed public IP address or VPN solution to allow the host to access to the industrial secure router.







TCP Alive Check Interval

Setting	Description	Factory Default
1 to 99	Specify the interval (in minutes) at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any "keep alive" packets. Disabling this option can help free up device resources.	7

Max. Connections

Setting	Description	Factory Default
1 to 2	Specify the maximum number of simultaneous connections that the port will accept. Up to 2 hosts can simultaneously collect data from the same serial device.	1

TCP Data Port

Setting	Description	Factory Default
1 to 65535	Specify the TCP port number for the serial port used to listen to connections and used by other devices to contact the serial port. To avoid conflicts with well-known TCP ports, the default is set to 4001.	4001

TCP Command Port

Setting	Description	Factory Default
1 to 65535	Specify the TCP port number for MOXA IP-Serial Library commands. It is not necessary to reference this port number in your application when using the Moxa IP-Serial Library, since the library automatically obtains the number from the device server. Only change this setting if there is a port number conflict with another application or device.	996

Serial Port Inactivity Time

Setting	Description	Factory Default
1 to 65535	Specify the time limit (in ms) for keeping the connection open if there is no data to or from the serial device. If there is no activity for the specified time period, the connection will be terminated. A setting of 0 means the system will always keep the TCP connection open regardless of data activity. For many applications, this option should be set to 0, as the serial device may be idle for long periods of time.	0

ATTENTION

Serial Port Inactivity Time setting should be greater than the Force Transmit Interval under Data Packing setting page. Otherwise, the connection may be closed before the data in the buffer can be transmitted. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.

Connection Down Settings

You can configure what happens to the RTS and DTR signals when the cellular or Ethernet connection goes down. For some applications, serial devices require RTS or DTR signals sent via the serial port to know the cellular or Ethernet link status.

Set RTS Signal

Setting	Description	Factory Default
High	The cellular or Ethernet connection status will not affect RTS signals.	High
Low	If the cellular or Ethernet connection is lost, RTS signals will change to low.	

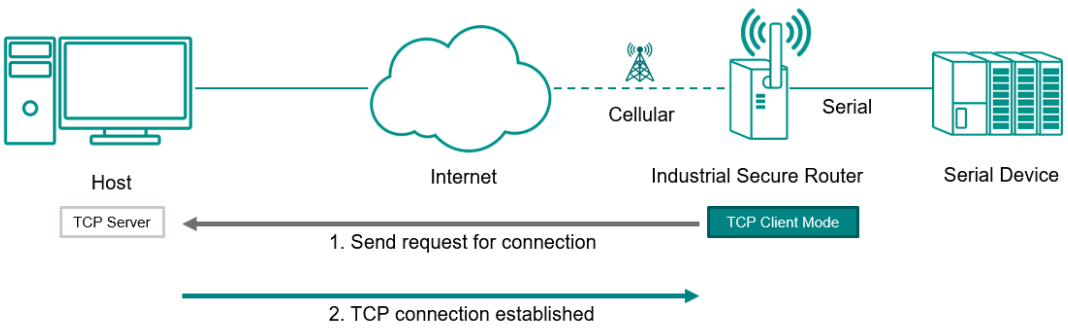
Set DTR Signal

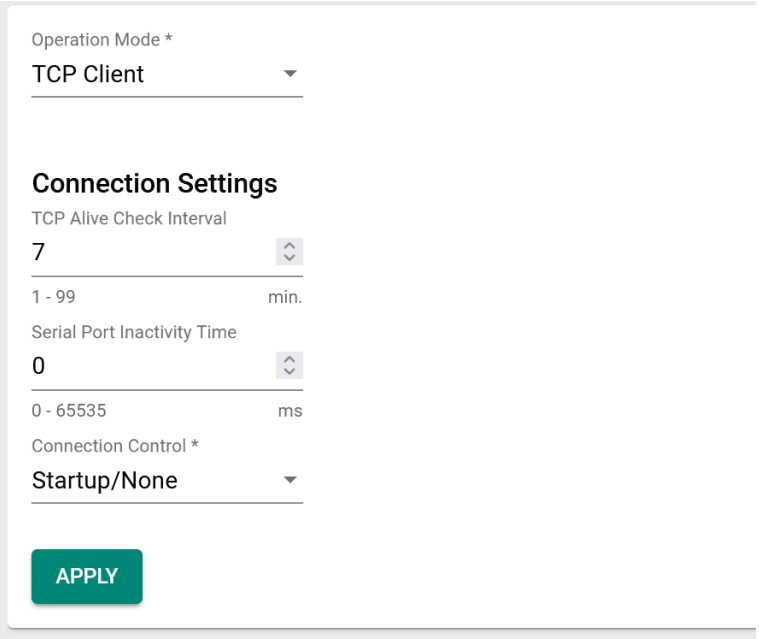
Setting	Description	Factory Default
High	The cellular or Ethernet connection status will not affect DTR signals.	High
Low	If the cellular or Ethernet connection is lost, DTR signals will change to low.	

TCP Client Mode

In TCP Client Mode, the Industrial Secure Router can actively establish a TCP connection with a pre-determined host computer when serial data arrives. After the data has been transferred, the Industrial Secure Router can disconnect automatically from the host computer by using the TCP alive check time or inactivity time settings.

Make sure your cellular service provider offers a fixed public IP address or VPN solution to allow the host to access to the industrial secure router.





TCP Alive Check Interval

Setting	Description	Factory Default
1 to 99	Specify the interval (in minutes) at which to check if the TCP connection is still alive. If there is no response from the other end of the connection after the specified time, the TCP connection will be terminated. A setting of 0 means the system will keep the TCP connection open and will not send any "keep alive" packets. Disabling this option can help free up device resources.	7

Serial Port Inactivity Time

Setting	Description	Factory Default
1 to 65535	Specify the time limit (in ms) for keeping the connection open if there is no data to or from the serial device. If there is no activity for the specified time period, the connection will be terminated. A setting of 0 means the system will always keep the TCP connection open regardless of data activity. For many applications, this option should be set to 0, as the serial device may be idle for long periods of time.	0

ATTENTION

Serial Port Inactivity Time setting should be greater than the Force Transmit Interval under Data Packing setting page. Otherwise, the connection may be closed before the data in the buffer can be transmitted. To prevent the unintended loss of data due to the session being disconnected, it is highly recommended that this value is set large enough so that the intended data transfer is completed.

ATTENTION

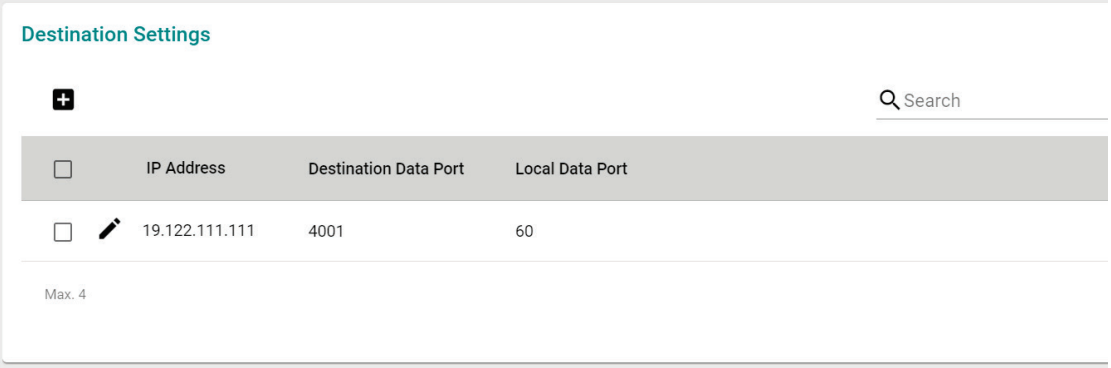
The serial port inactivity time is only applied when the **Connection Control** option (see below) is set to **Any Character/Inactivity Time**.

Connection Control

Setting	Description	Factory Default
Startup/None	A TCP connection will be established on startup and will remain active indefinitely.	Startup/None

Setting	Description	Factory Default
Any Character/None	A TCP connection will be established when any character is received from the serial interface and will remain active indefinitely.	
Any Character/ Inactivity Time	A TCP connection will be established when any character is received from the serial interface and will be disconnected after the specified Serial Port Inactivity Time.	
DSR On/DSR Off	A TCP connection will be established when a DSR "On" signal is received and will be disconnected when a DSR "Off" signal is received.	
DSR On/None	A TCP connection will be established when a DSR "On" signal is received and will remain active indefinitely.	
DCD On/DCD Off	A TCP connection will be established when a DCD "On" signal is received and will be disconnected when a DCD "Off" signal is received.	
DCD On/None	A TCP connection will be established when a DCD "On" signal is received and will remain active indefinitely.	

Destination Settings



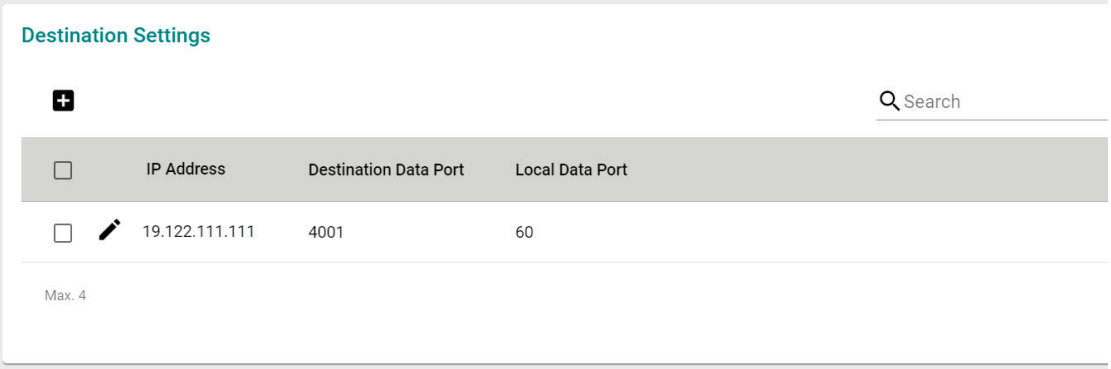
From the Destination Settings table, you can configure up to 4 remote host destinations.

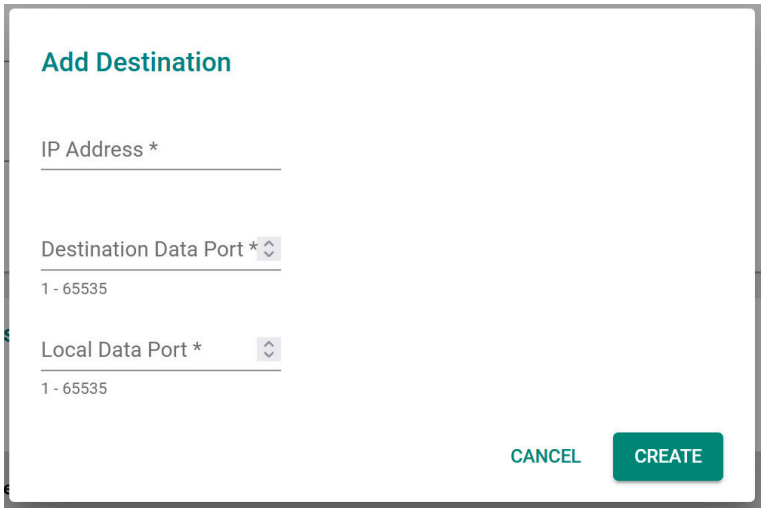
Add a Destination Entry (TCP)

From the Destination Settings table, click the **Add** ( ) icon to add a new entry.

ATTENTION

While the Industrial Secure Router supports connections to up to 4 remote hosts, a low connection speed or throughput on one of the connections will affect the performance of the other active connections.





IP Address

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

Destination Data Port

Setting	Description	Factory Default
1 to 65535	Enter the TCP port number of the remote host.	None

Local Data Port

Setting	Description	Factory Default
1 to 65535	Specify a designated local port or leave this field blank to let the system assign a port.	None

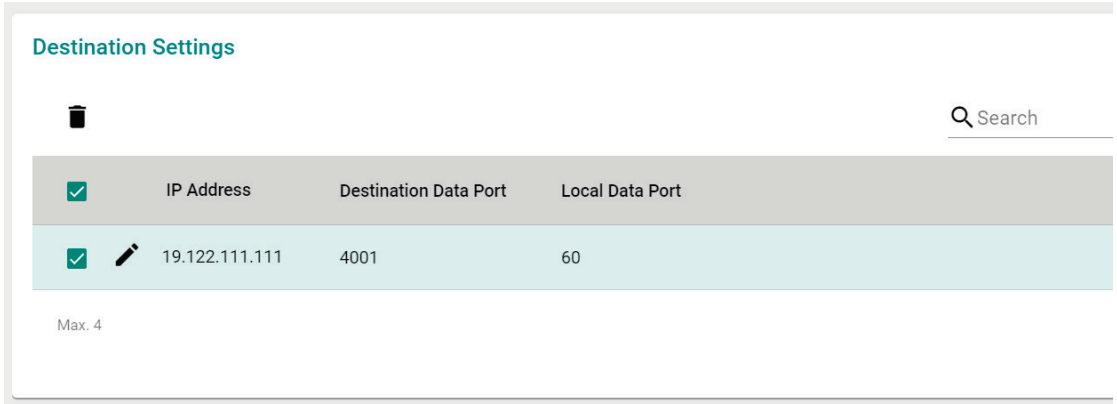
Modify a Destination Entry (TCP)

From the Destination Settings table, click the **Edit** ( ) icon to edit an existing entry.

Refer to Add a Destination Entry (TCP) for information about each field.

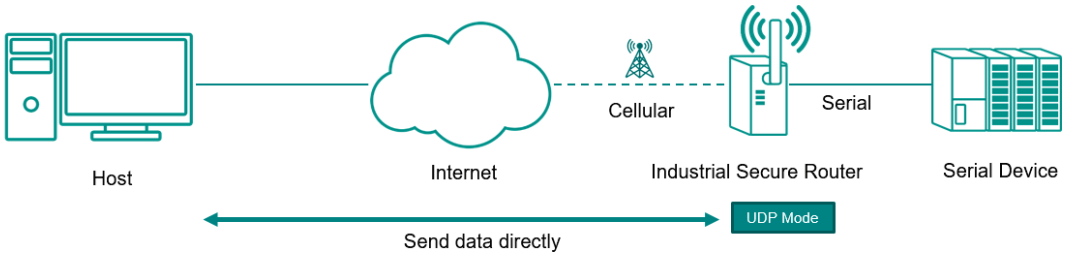
Delete a Destination Entry

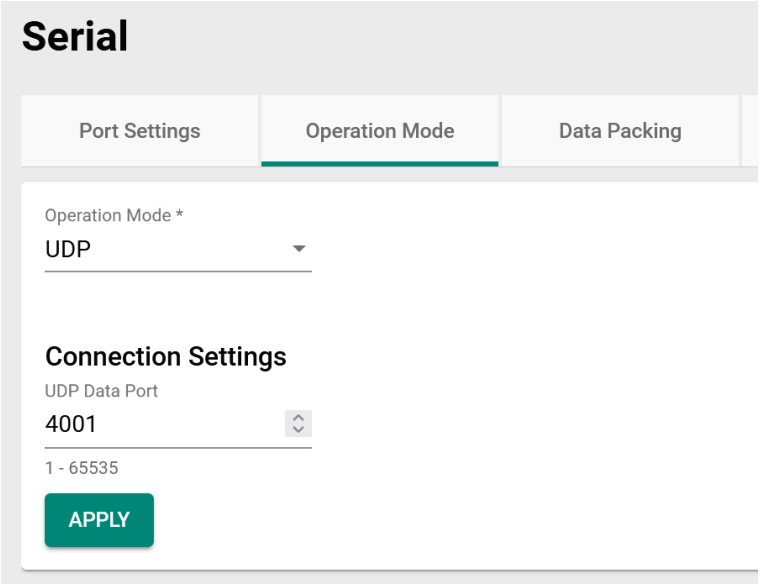
From the Destination Settings table, check the box of the entry or entries you want to delete and click the **Delete** ( ) icon.



UDP Mode

Compared to TCP communication, UDP is faster and more efficient. In UDP mode, you can unicast to one host or multicast to multiple hosts and the serial device can receive data from one or multiple host computers. These traits make UDP mode especially well-suited for message display applications.



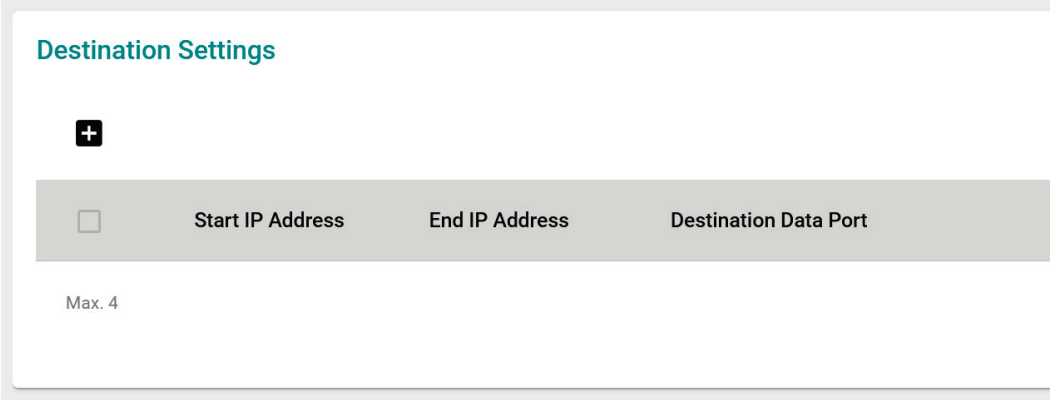


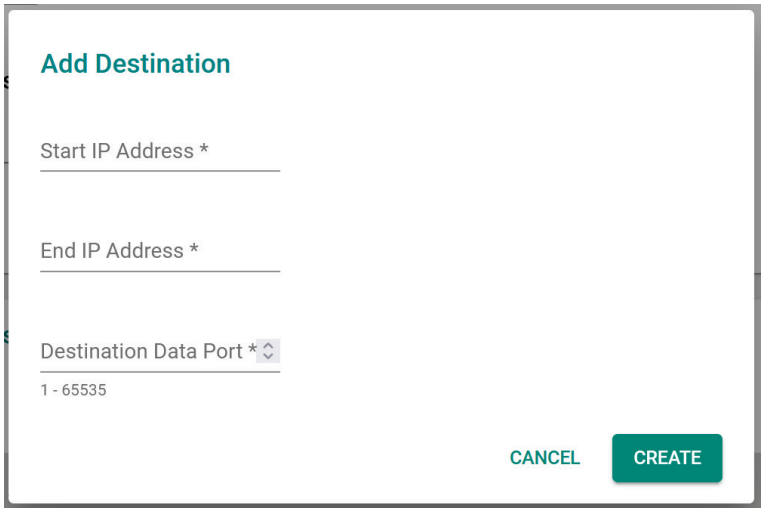
UDP Data Port

Setting	Description	Factory Default
1 to 65535	Enter the UDP port number for contacting the serial device.	4001

Add a Destination Entry (UDP)

From the Destination Settings table, click the **Add** ( ) icon to add a new entry.





Start IP Address

Setting	Description	Factory Default
IP Address	Enter the starting IP address of the IP range of the remote host.	None

End IP Address

Setting	Description	Factory Default
1 to 65535	Enter the ending IP address of the IP range of the remote host.	None

ATTENTION

The maximum IP address range size is 64 addresses. However, when using multicast, you may enter IP addresses in the form xxx.xxx.xxx.255 in the **Start IP Address** field. For example, enter 192.168.127.255 to allow the system to broadcast UDP packets to all hosts with IP addresses between 192.168.127.1 and 192.168.127.254.

Destination Data Port

Setting	Description	Factory Default
1 to 65535	Enter the UDP port number of the remote host.	None

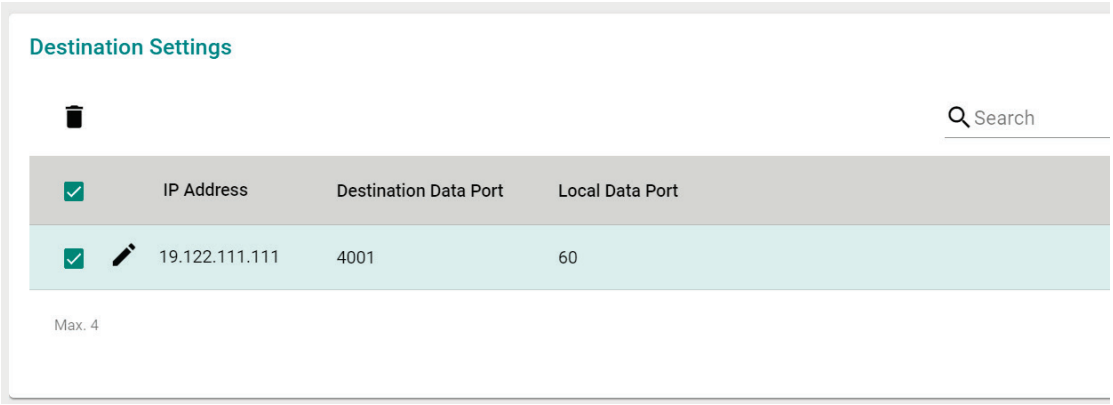
Modify a Destination Entry (UDP)

From the Destination Settings table, click the **Edit** ( ) icon to edit an existing entry.

Refer to Add a Destination Entry (UDP) for information about each field.

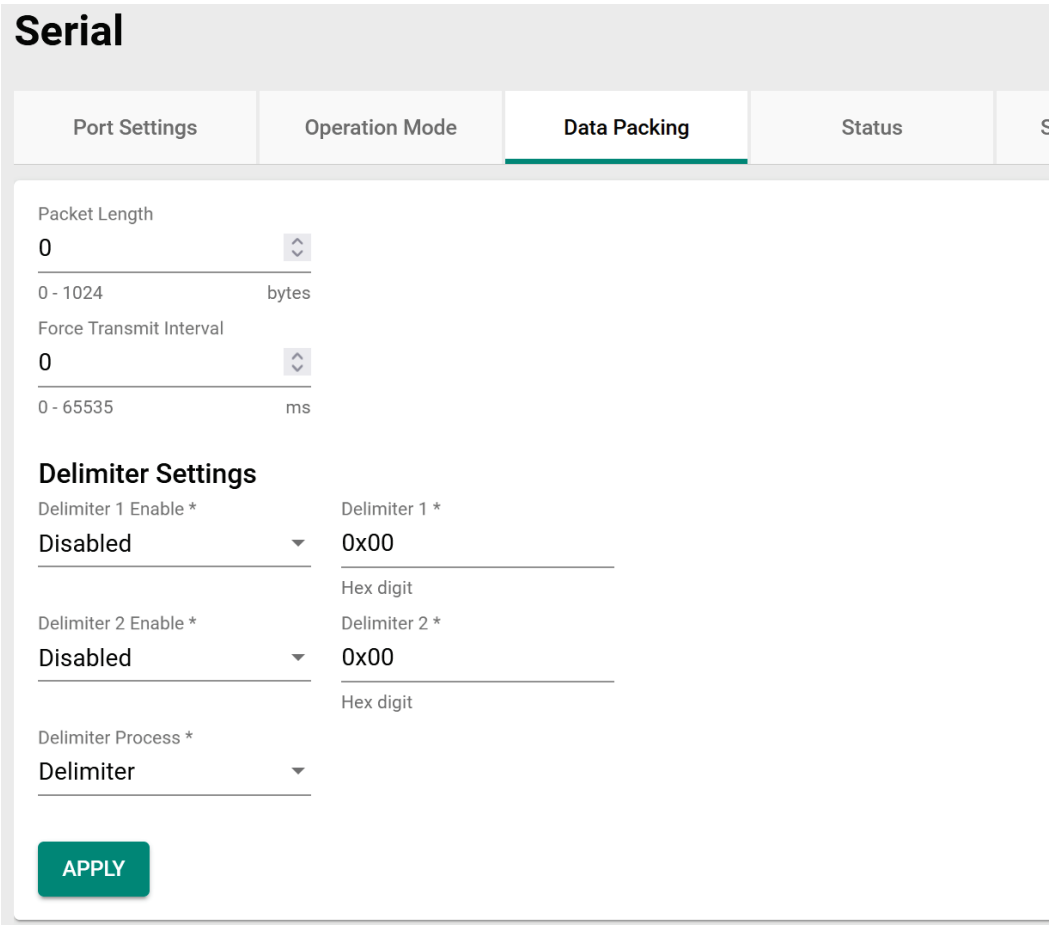
Delete a Destination Entry

From the Destination Settings table, check the box of the entry or entries you want to delete and click the **Delete** ( ) icon.



Data Packing

From the Data Packing screen, you can configure the conditions and delimiter settings for serial port data buffering and transmission.



Packet Length

Setting	Description	Factory Default
0 to 1024	Specify the Packet Length (in bytes) for the serial port buffer. The packet length refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. At the default packet length of 0, no maximum amount is specified and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. If a packet length of 1 to 1024 bytes is specified, data in the buffer will be sent as soon as it reaches the specified length.	0

Force Transmit Interval

Setting	Description	Factory Default
0 to 65535	Specify the interval (in ms) to force-transmit serial port data if no activity is recorded. This setting controls data packing by the amount of time that elapses between bits of data. As serial data is received, it accumulates in the device port's buffer. If serial data is not received for the specified amount of time, the data that is currently in the buffer is packed for network transmission. A setting of 0 means that data in the buffer will not be automatically packed when additional data is not received from the device.	0

Delimiter Settings

Delimiter 1/2 Enable

Setting	Description	Factory Default
Enabled	The serial port will queue the data in the buffer and send it to the cellular or Ethernet port when a specific character, entered in hex format, is received. A second delimiter character can be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	Disabled
Disabled	The serial port will not check any specific character for data transmission.	

Delimiter 1/2

Setting	Description	Factory Default
Hex digit	Enter the specific character that acts as the delimiter to control when data should be sent.	0x00

ATTENTION

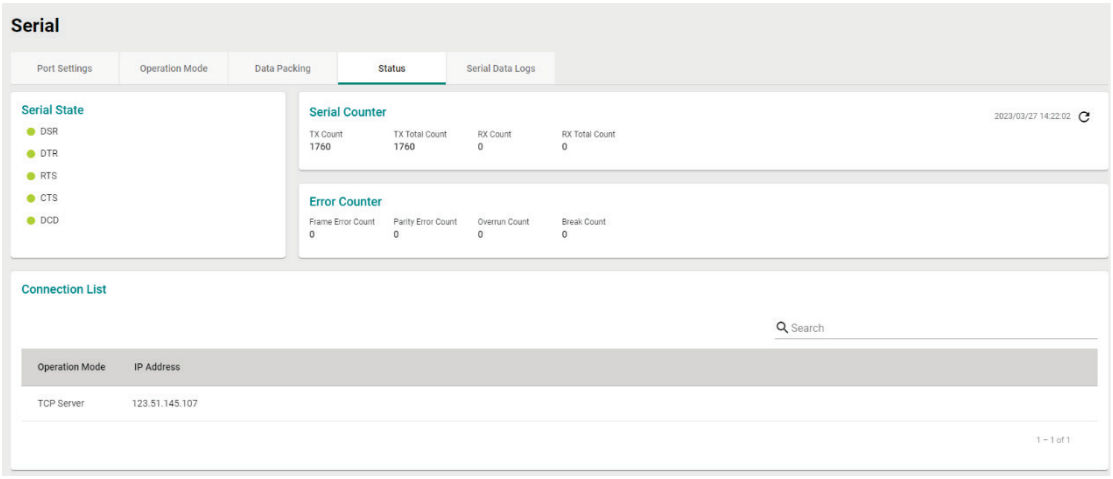
When the device port buffer is full, the data will be packed for network transmission regardless of the Delimiter 1, Delimiter 2, and Force Transmit Interval settings.

Delimiter Process

Setting	Description	Factory Default
Delimiter	Data in the buffer will be transmitted when the delimiter is received.	Delimiter
Delimiter + 1	Data in the buffer will be transmitted after 1 additional byte is received following the delimiter.	
Delimiter + 2	Data in the buffer will be transmitted after 2 additional bytes are received following the delimiter.	
Strip Delimiter	Data in the buffer is first stripped of the delimiter before being transmitted.	

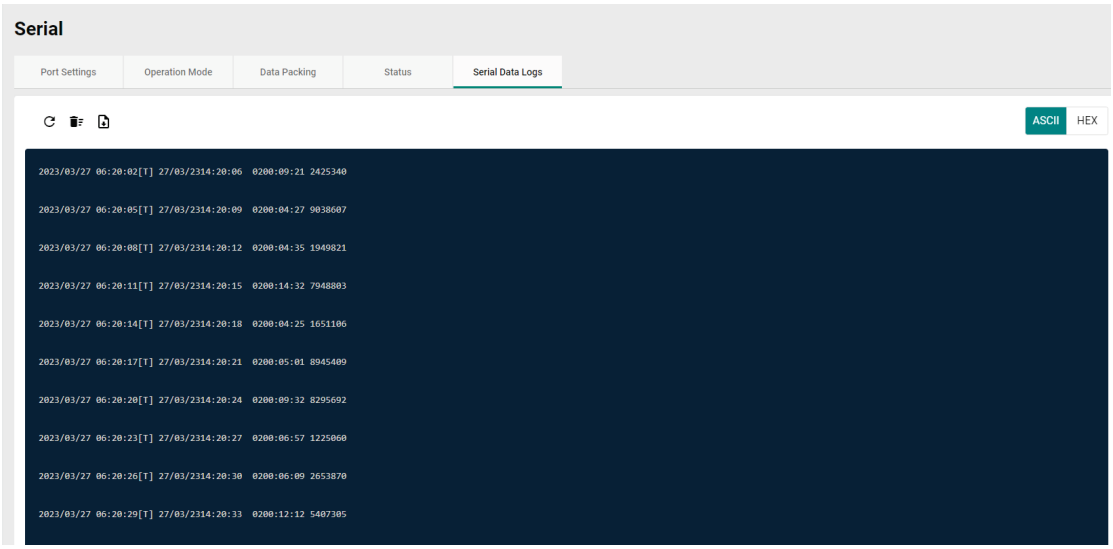
Status

The Status screen provides detailed statistics and information about the serial port data and connections.



Serial Data Logs

The Serial Data Logs screen shows a record of all collected serial data logs, viewable in ASCII or HEX format.



Click the icon to refresh the serial data logs.

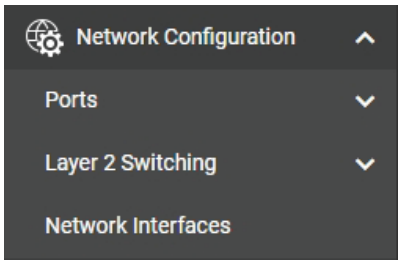
Click the icon to delete all serial data logs.

Click the icon to export all serial data logs to a file.

5. Network Configuration

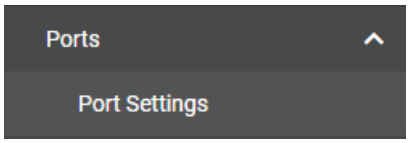
This chapter describes how to configure the physical ports and network interfaces of the Industrial Secure Router.

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



Ports

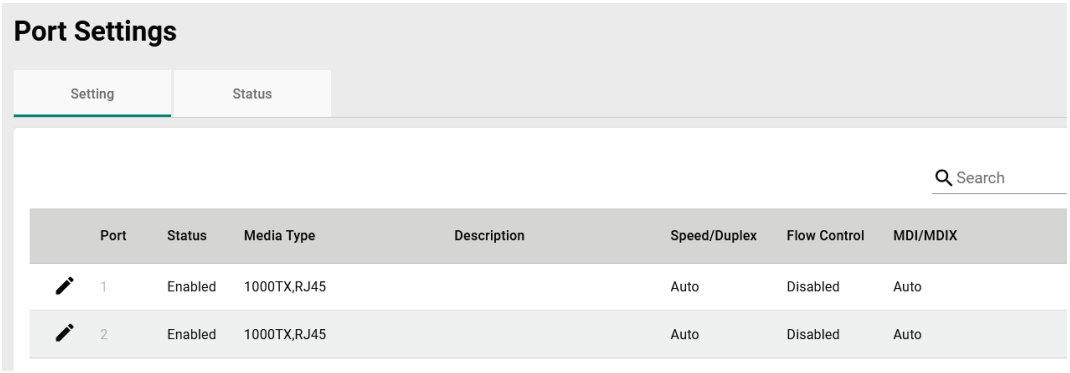
From the **Ports** section, the following functions can be configured: **Port Settings**.



Port Settings

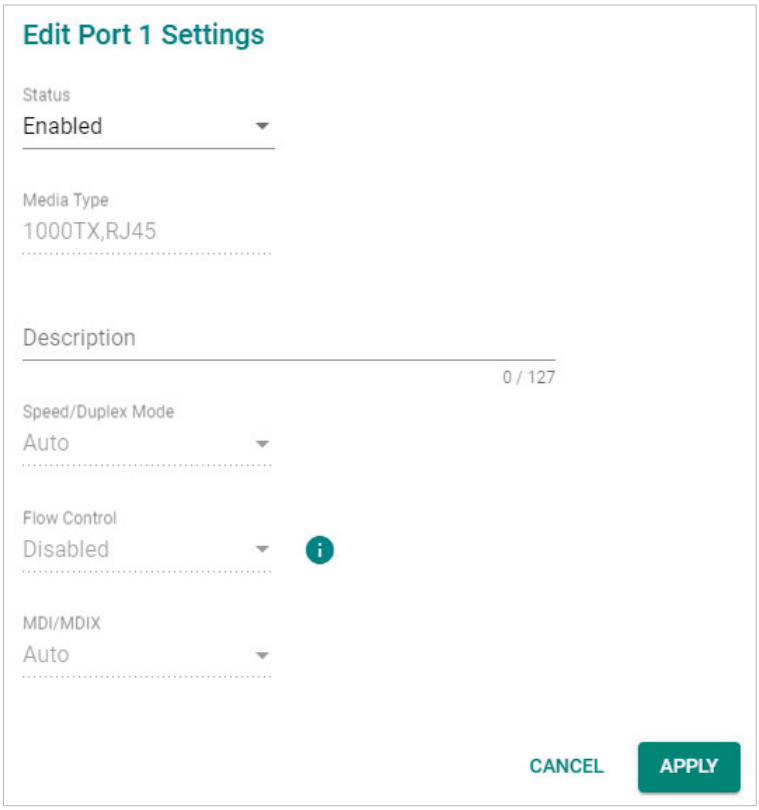
Port settings let you manage port access, port transmission speed, flow control, and port type (MDI or MDIX).

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

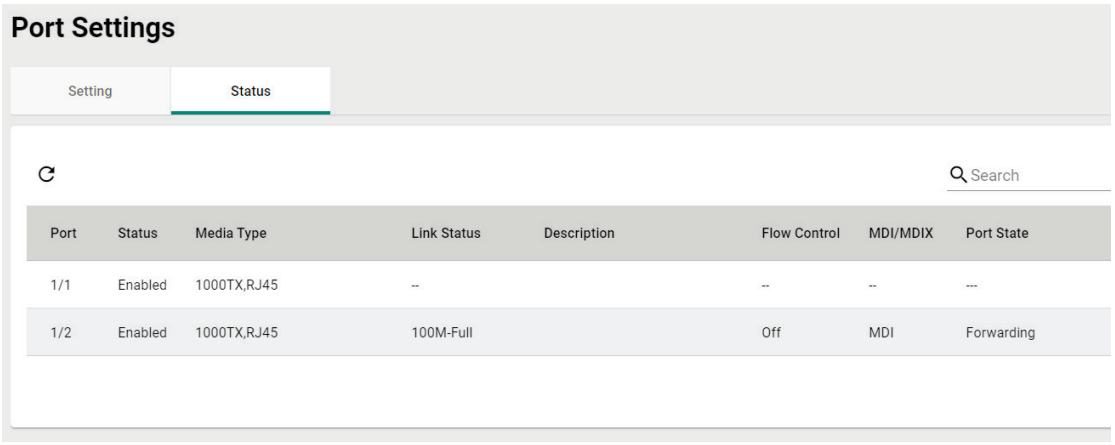
MDI/MDIX

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.

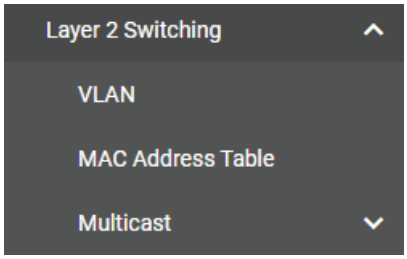
Status

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



Layer 2 Switching

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



VLAN

Using Virtual LAN

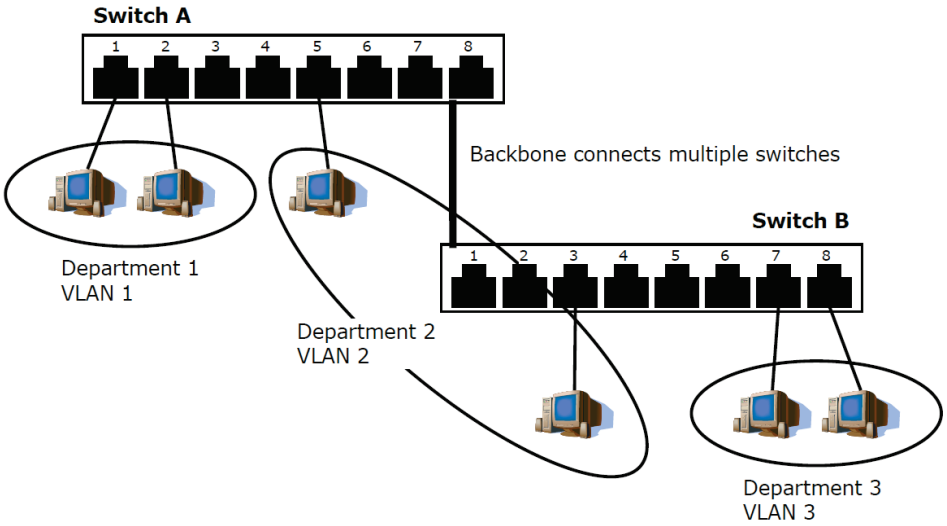
Setting up Virtual LANs (VLANs) on your Moxa industrial secure router increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

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.

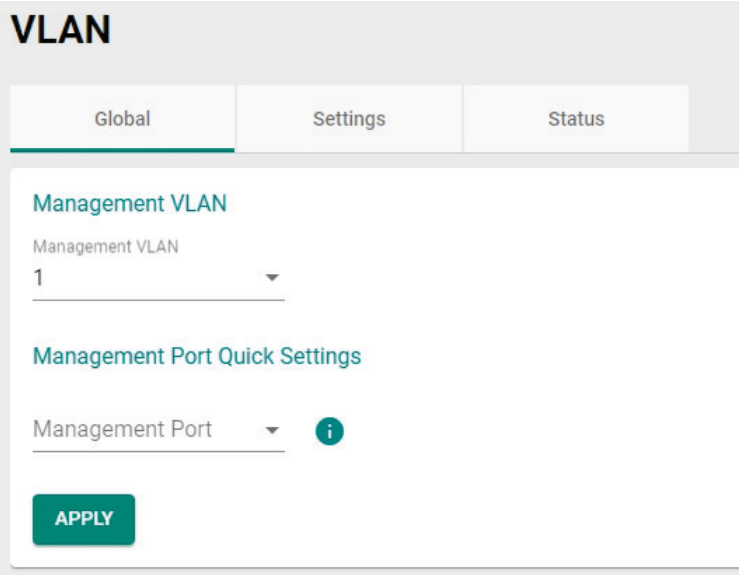
Moxa's switch supports three types of VLAN port settings:

- **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.

Global

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



Management VLAN

Management VLAN

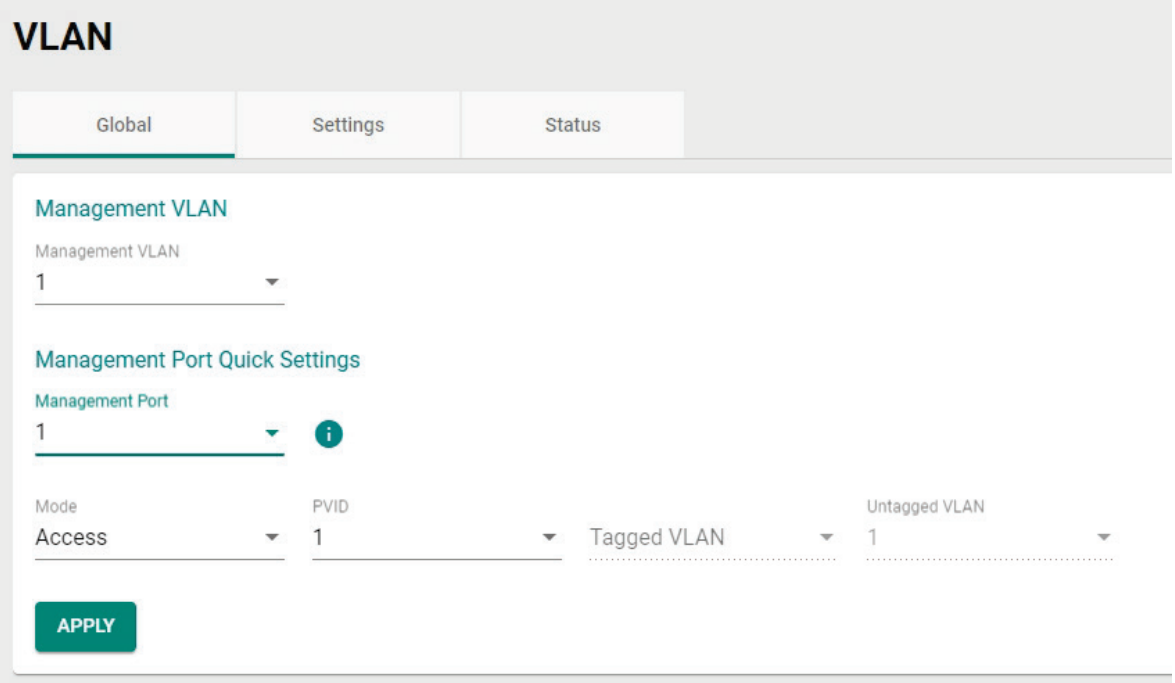
Setting	Description	Factory Default
1 to 16	Select the management VLAN ID from the drop-down menu.	1

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 2	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

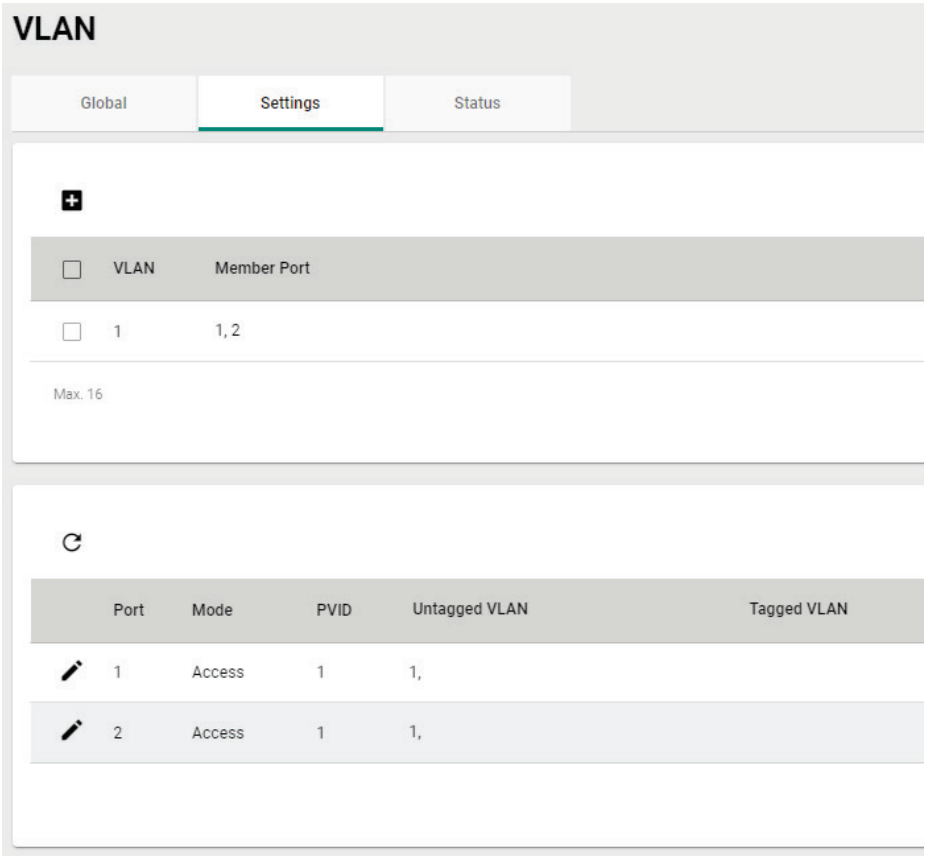
Setting	Description	Factory Default
All Member VIDs, 1 to 16	If the Mode is set to Trunk or Hybrid, set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	Access mode: None Trunk or Hybrid mode: 1

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
VLAN
Member Port
1
1, 2
Max. 16
Port
Mode
PVID
Untagged VLAN
Tagged VLAN
1
Access
1
1,
2
Access
1
1,

Create a VLAN

Click the icon to create a VLAN.

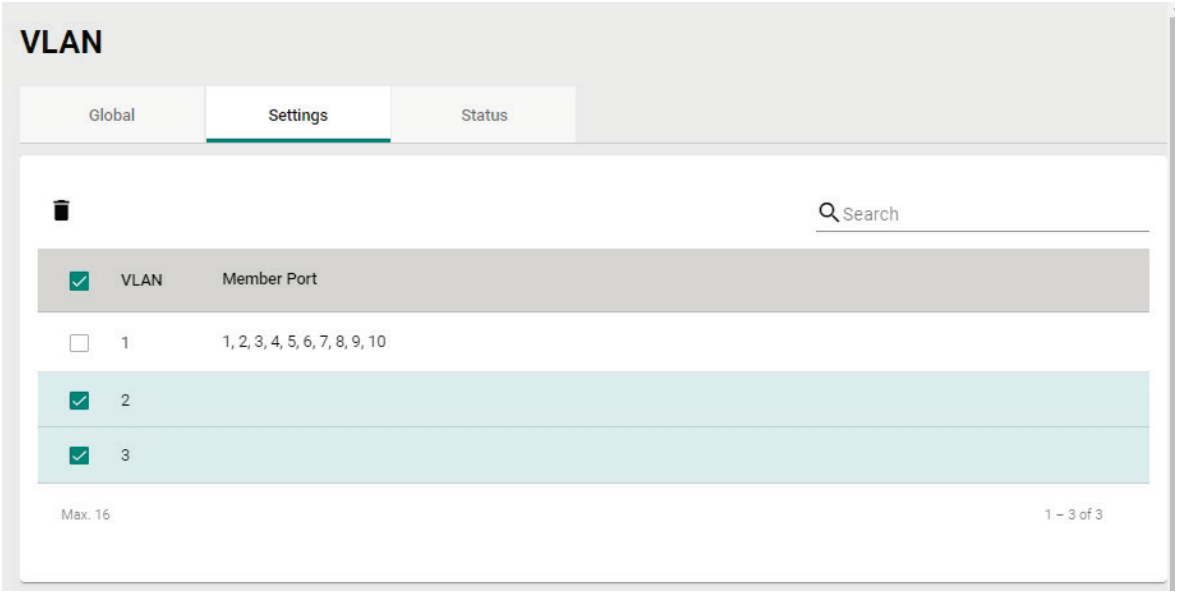
VID

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

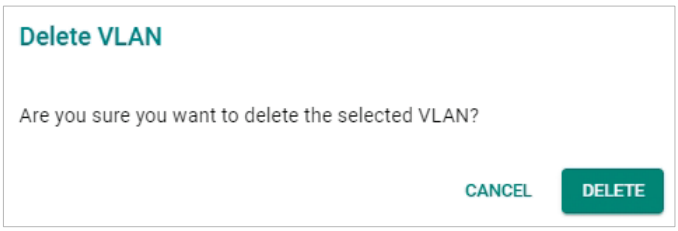
When finished, click **CREATE** to create the VLAN.

Delete a VLAN

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

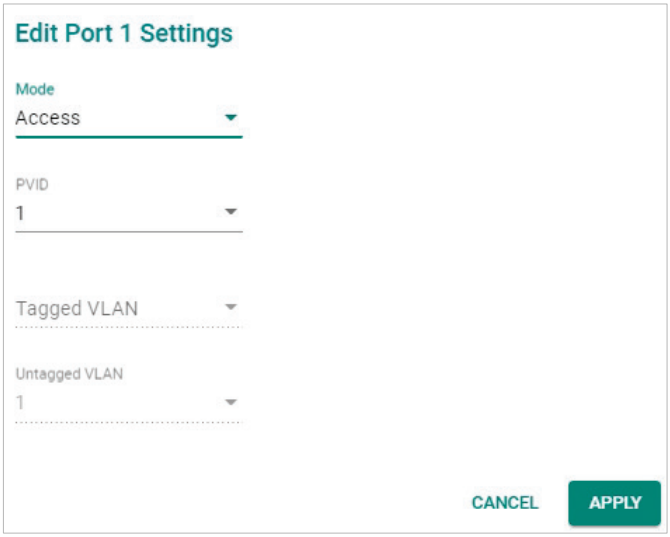


Click **DELETE** to delete the selected items.



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

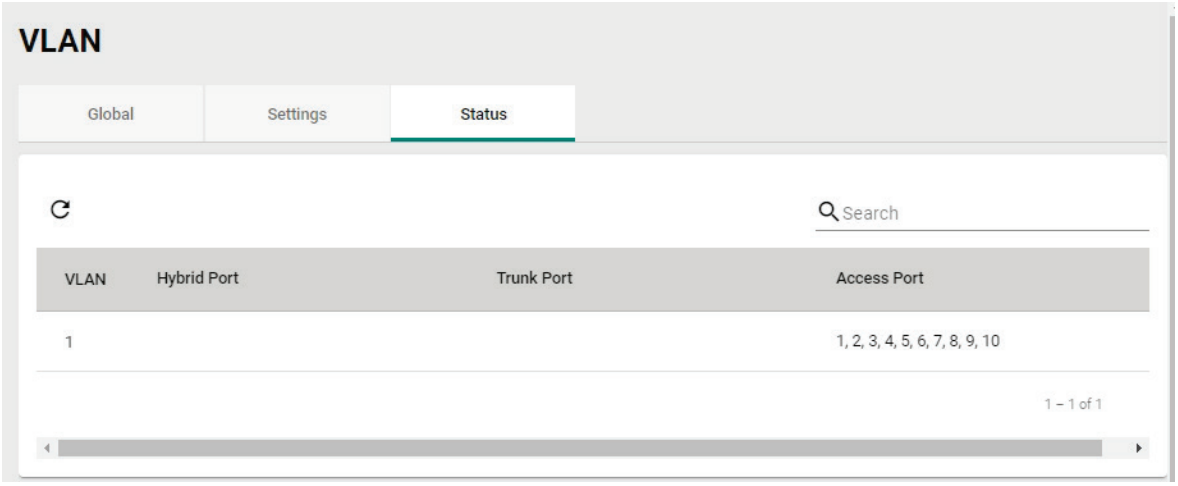
Untagged VLAN

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

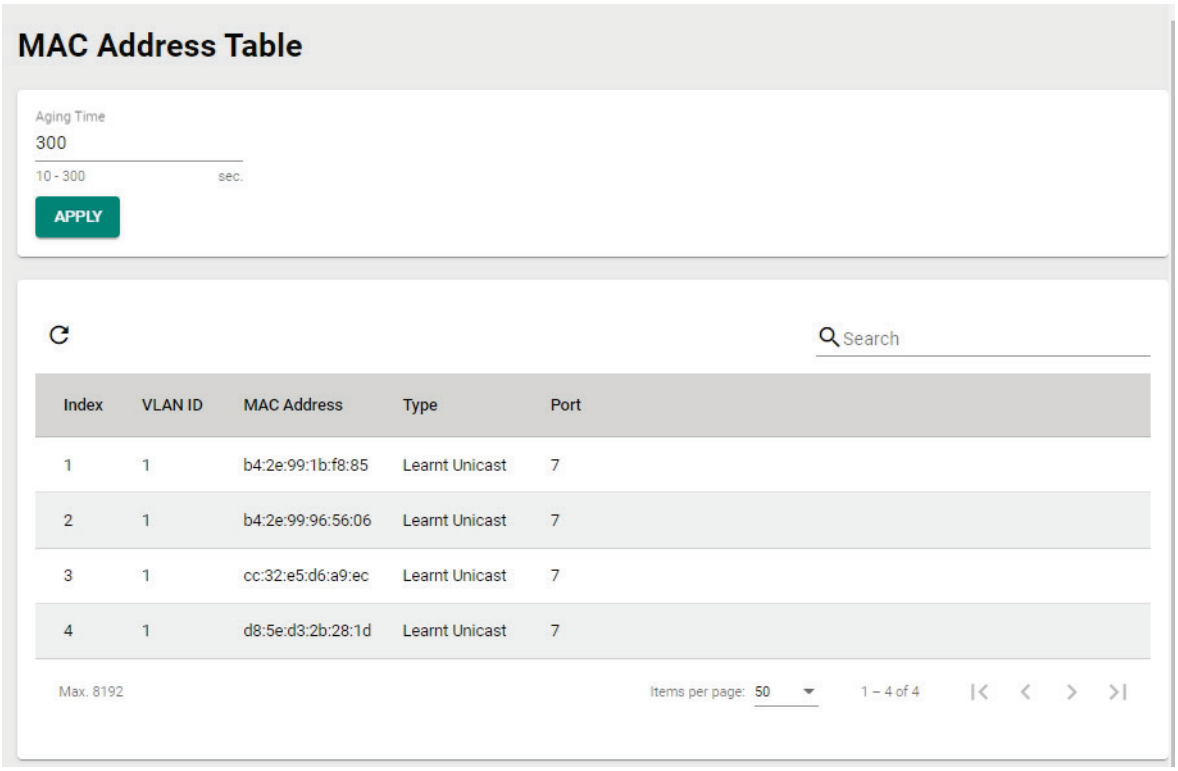
From the **Status** tab, you can review created VLAN groups, joined access ports, trunk ports, and hybrid ports. Click the icon to refresh the information in the VLAN Status Table.



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.

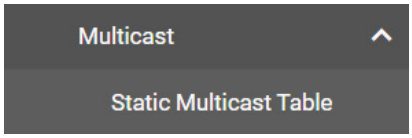
Learnt Unicast	Show all learnt Unicast MAC addresses.
Static	Show all Static, Static Lock, and Static Multicast MAC addresses.
Multicast	Show all Static Multicast MAC addresses.
Port x	Show all MAC addresses associated with a specific port.

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.

Multicast

Multicast filtering improves the performance of networks that carry multicast traffic. This section covers the Static Multicast Table page 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).

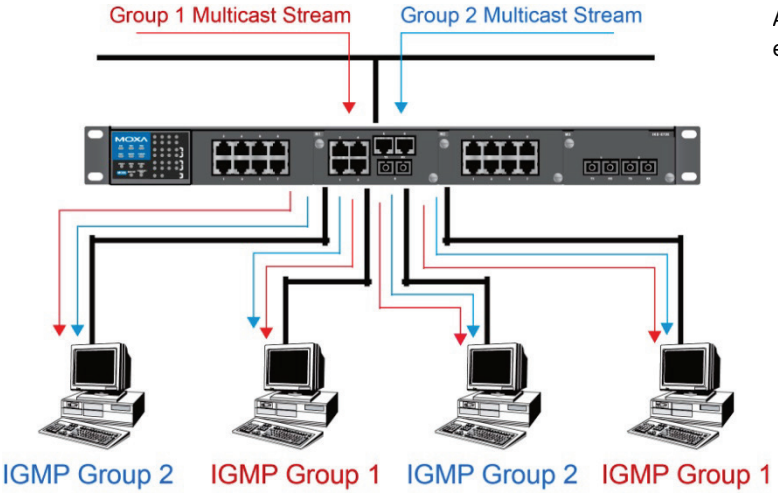
Multicast transmission makes more sense and is more efficient than unicast transmission for some applications. For example, multicasts are often used for video-conferencing, since high volumes of traffic must be sent to several end-stations at the same time, but where broadcasting the traffic to all 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.

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

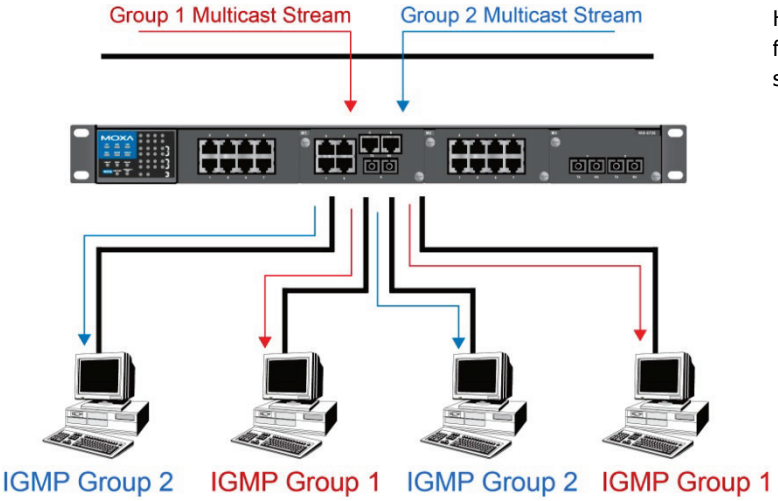
registered end-stations. The following two figures illustrate how a network behaves without multicast filtering, and with multicast filtering.

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

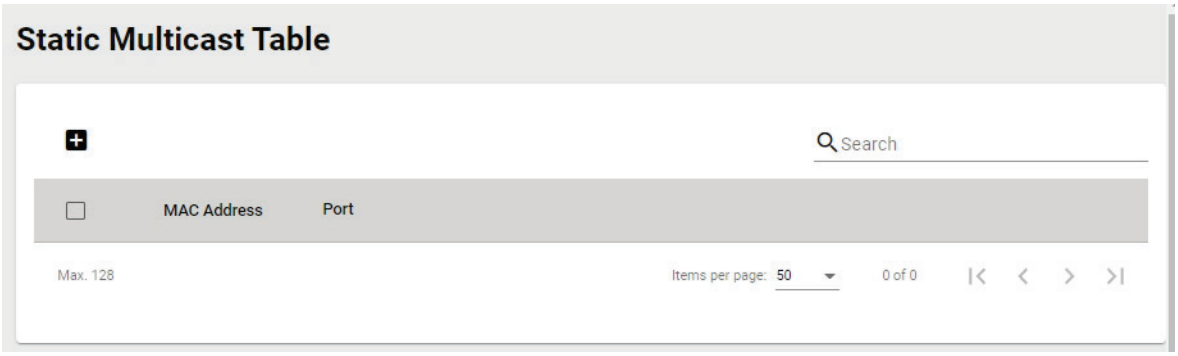
Some devices may support multicast packets, but not support IGMP Snooping. The Moxa industrial secure router supports adding multicast groups manually to enable multicast filtering.

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.

Static Multicast Table

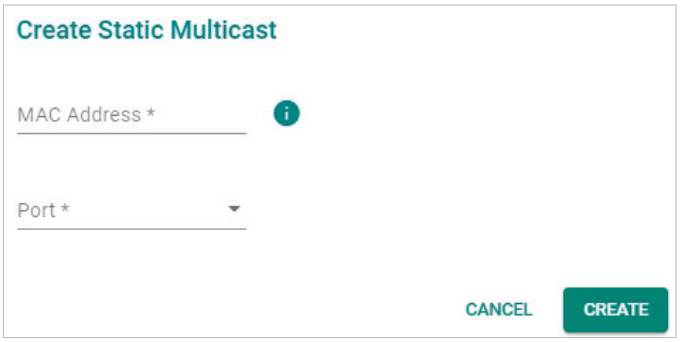
From the Static Multicast Table, you can create static multicast entries.



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

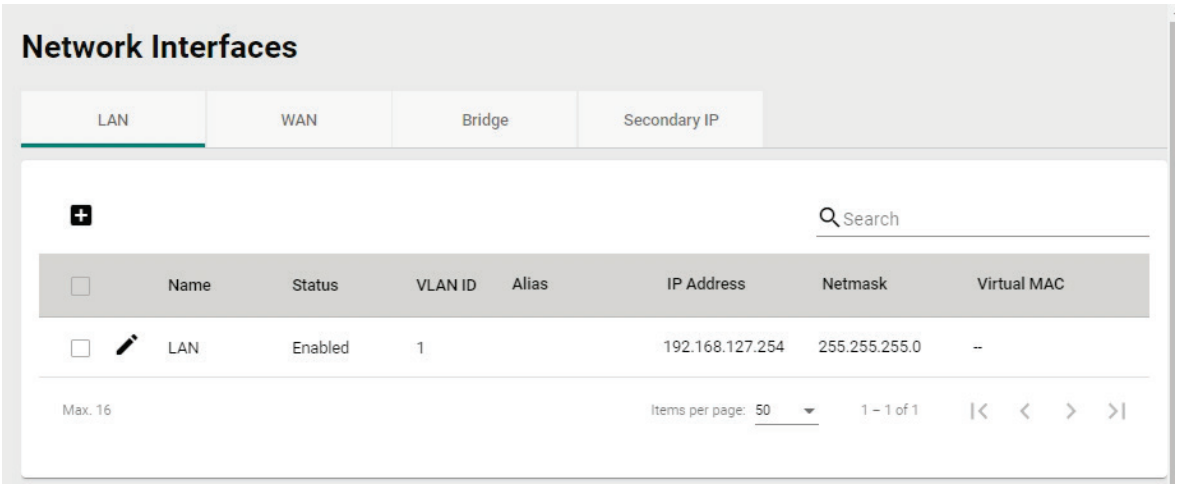
Port

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.

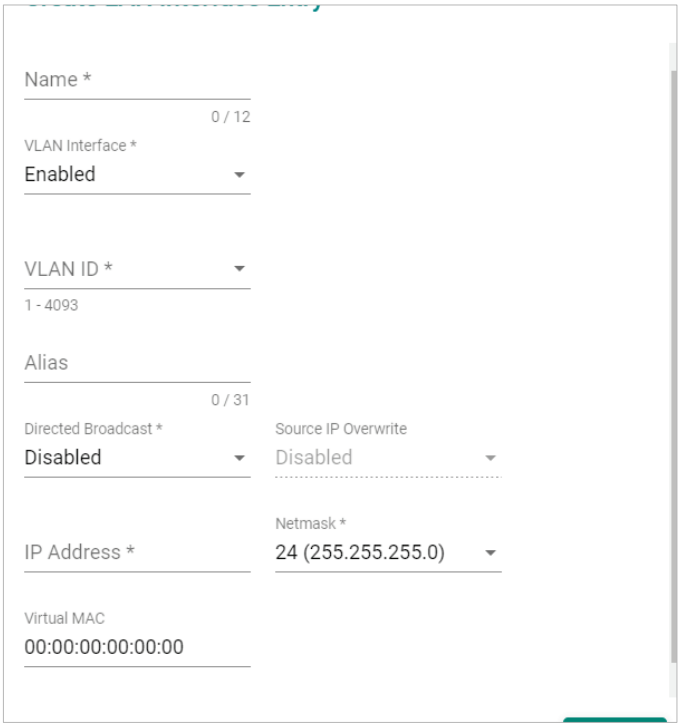
Network Interface

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

Directed Broadcast

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

Source IP Overwrite

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

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

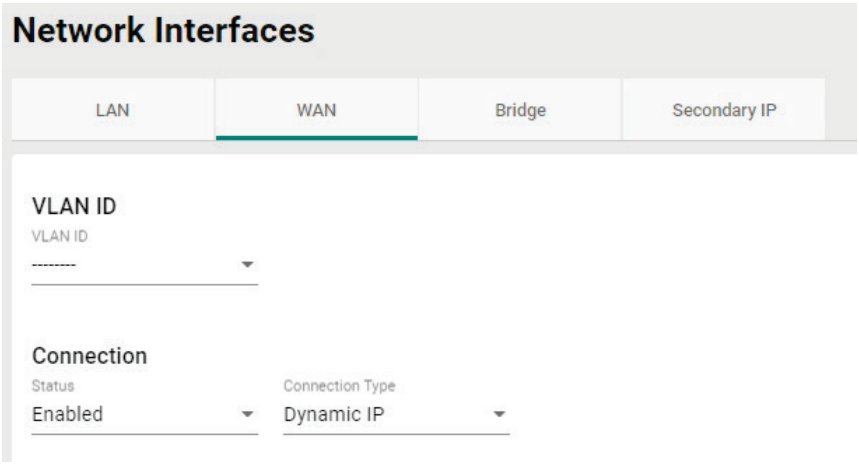
Select the item(s) you want to delete in the LAN Interface List, click the icon. When prompted to confirm, click **DELETE** to delete the selected item(s).

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

> **NOTE**
>
> This section is for Ethernet WAN settings only and does not cover cellular WAN. For cellular WAN settings, refer to Cellular.



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.

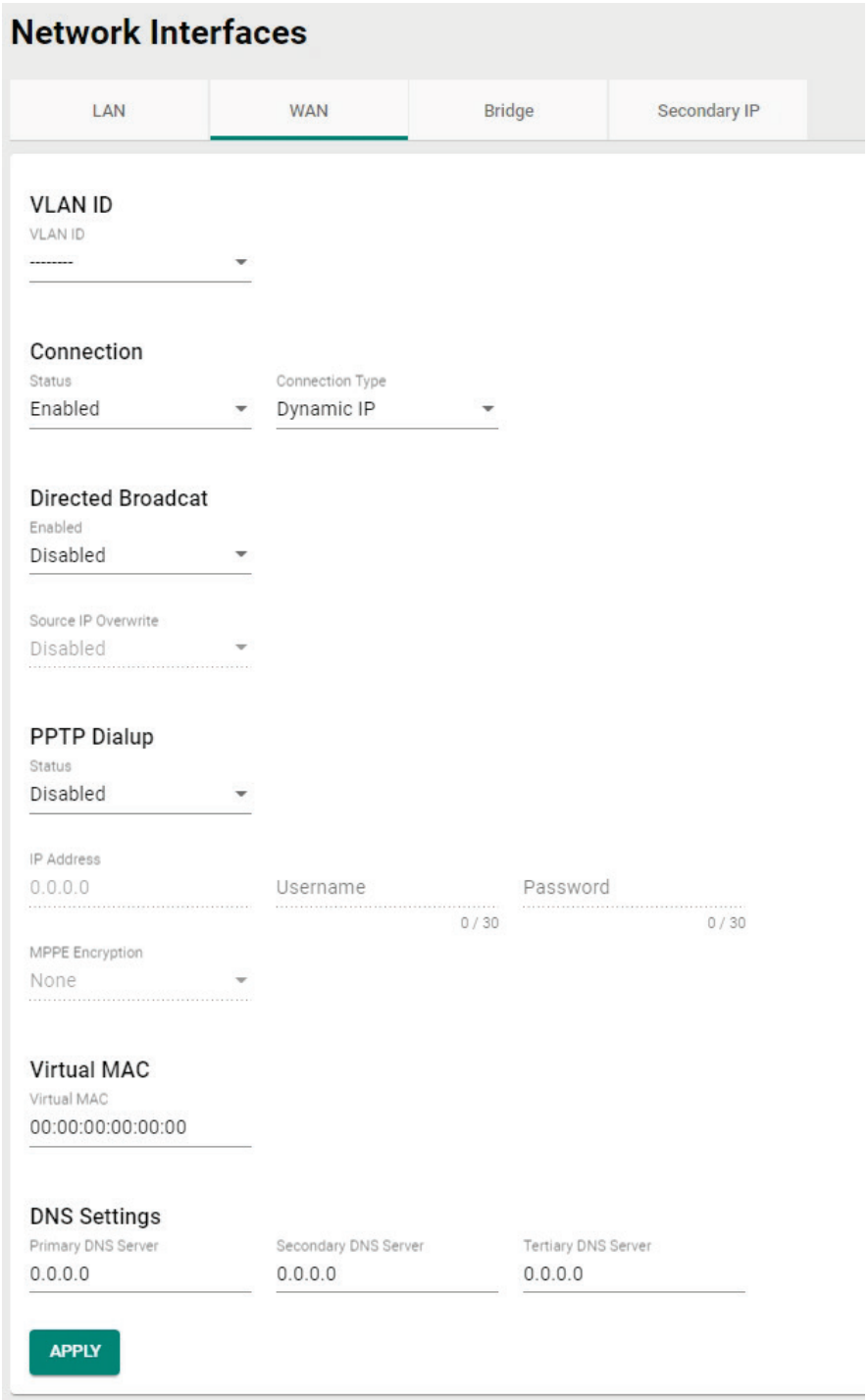
Status

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

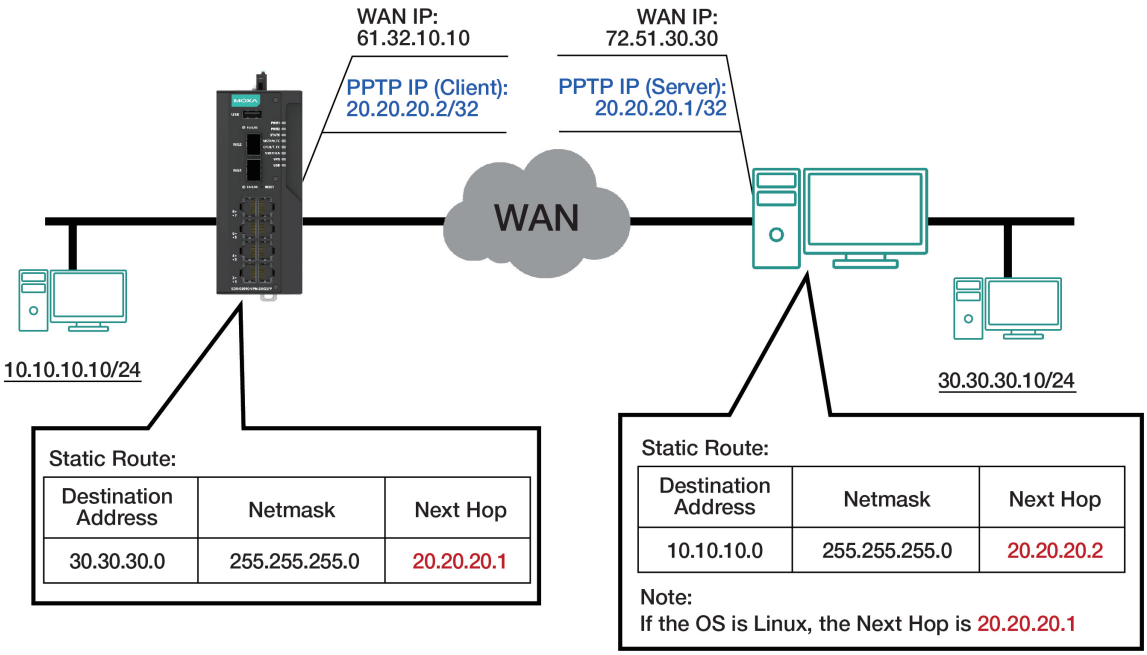
Setting	Description	Factory Default
Max. 30 characters	Enter the password used for dialing in to the PPTP service.	None

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

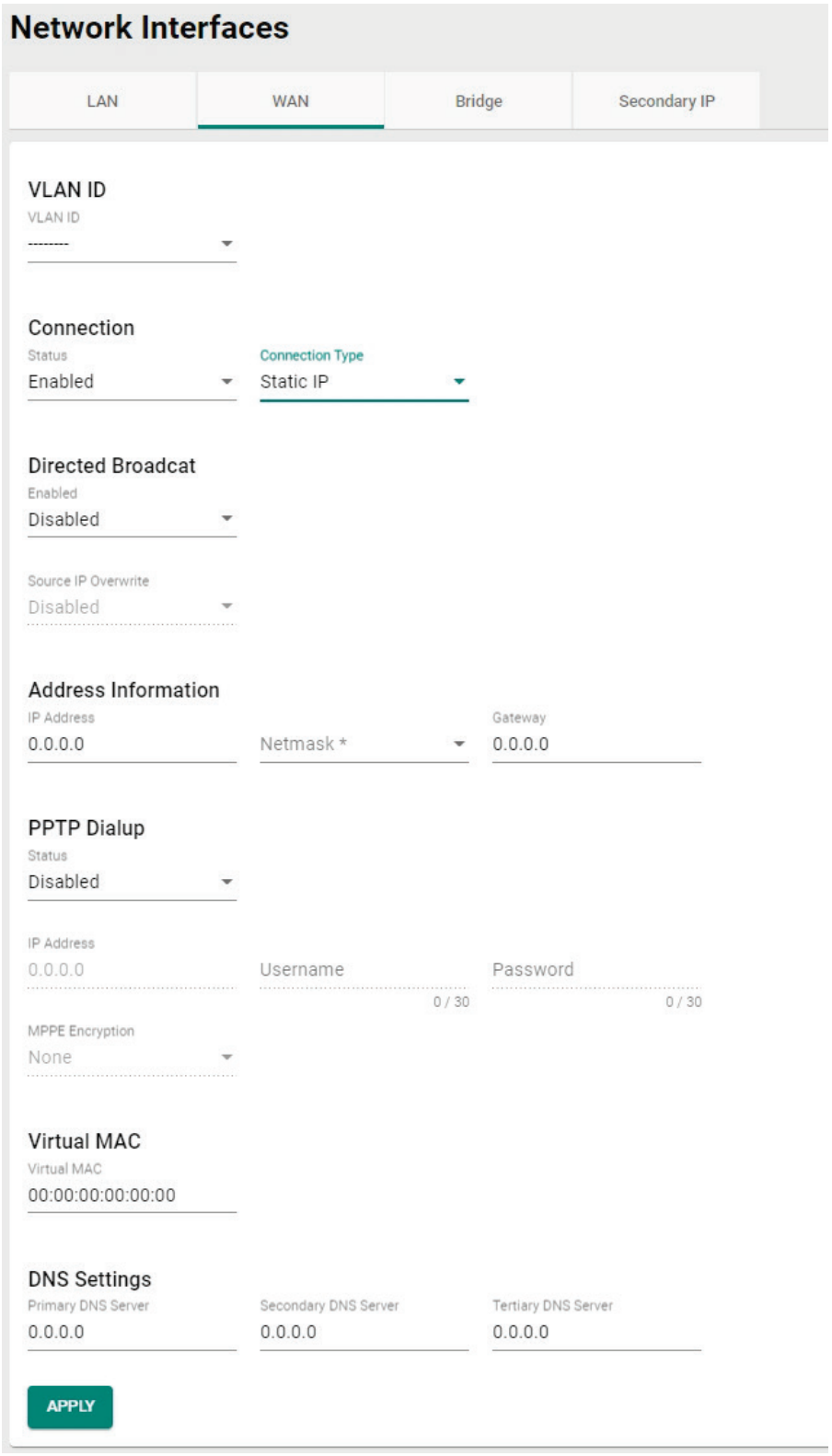
Setting	Description	Factory Default
IP Address	Enter the tertiary DNS IP address.	0.0.0.0

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

Netmask

Setting	Description	Factory Default
IP Address	Specify the netmask.	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

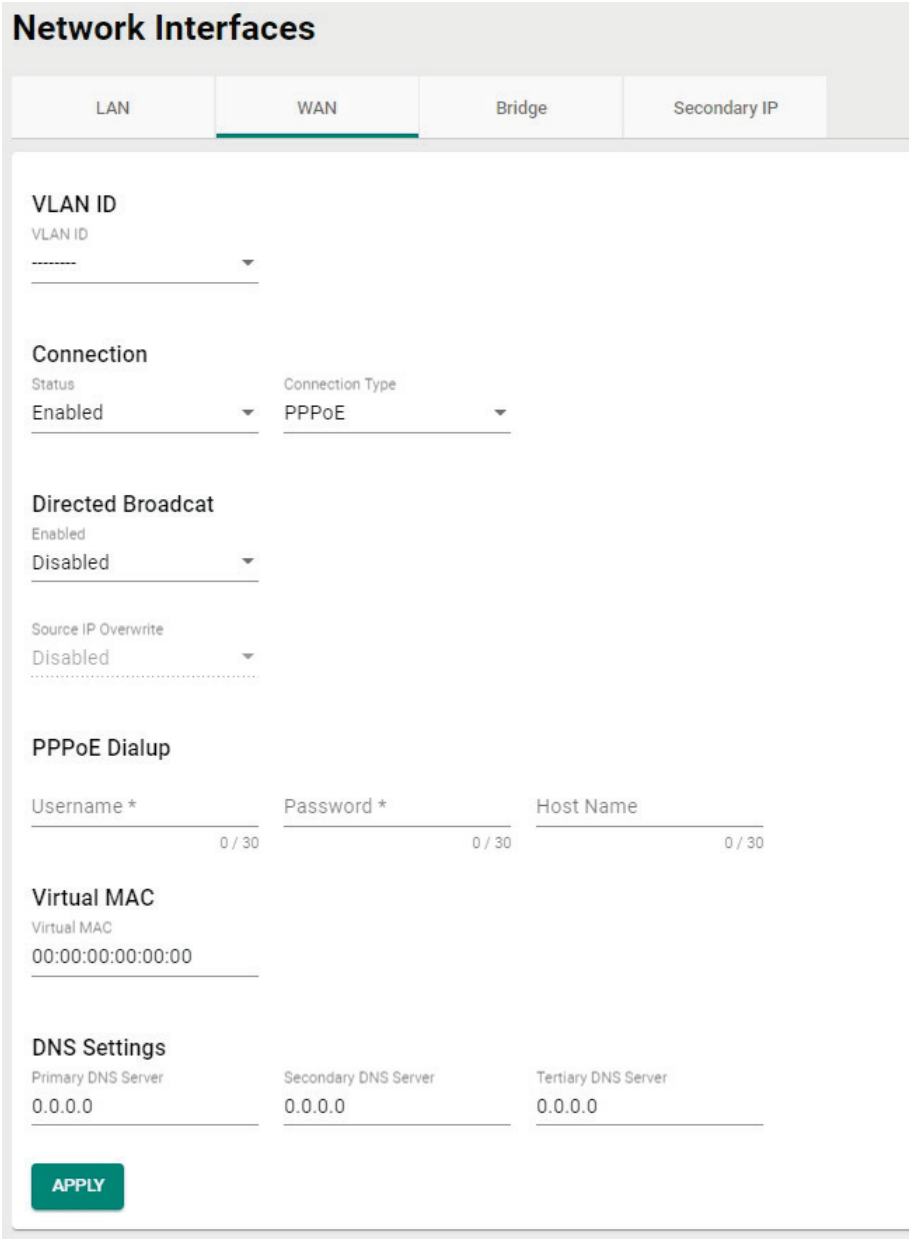
Setting	Description	Factory Default
IP Address	Enter the tertiary DNS IP address.	0.0.0.0

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.

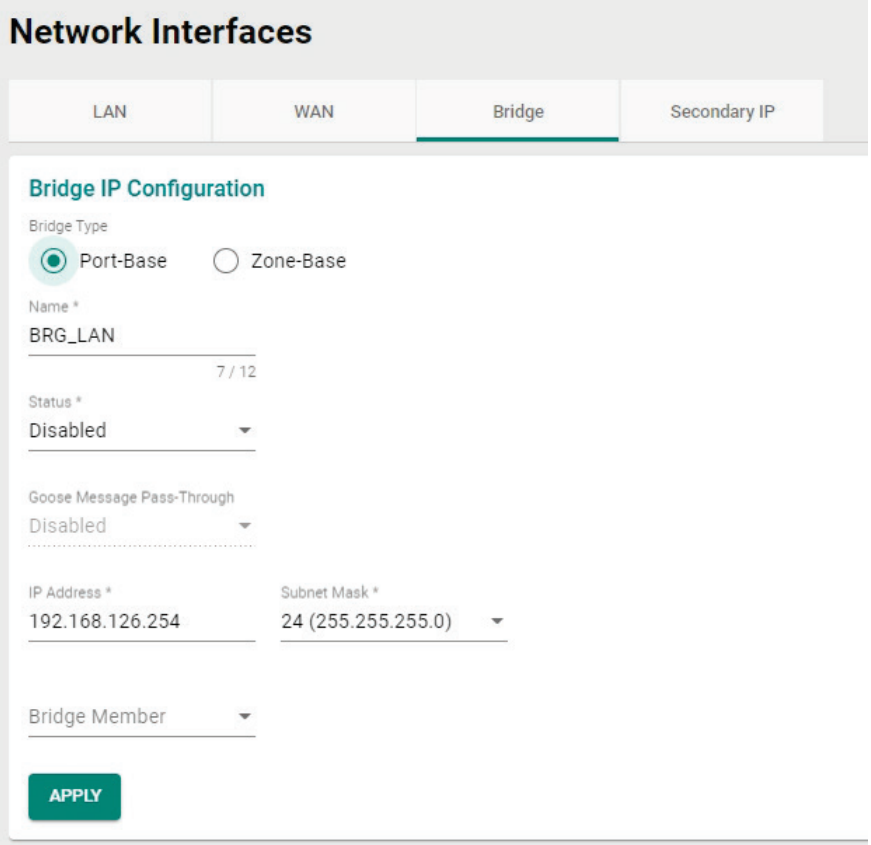
Similarly, when ports are associated with different VLANs, the packets transmitted within these VLANs will be routed by the switching chip locally, without being inspected by the firewall. However, in some scenarios, it is required to filter specific packets transmitted between VLANs. By adding VLANs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

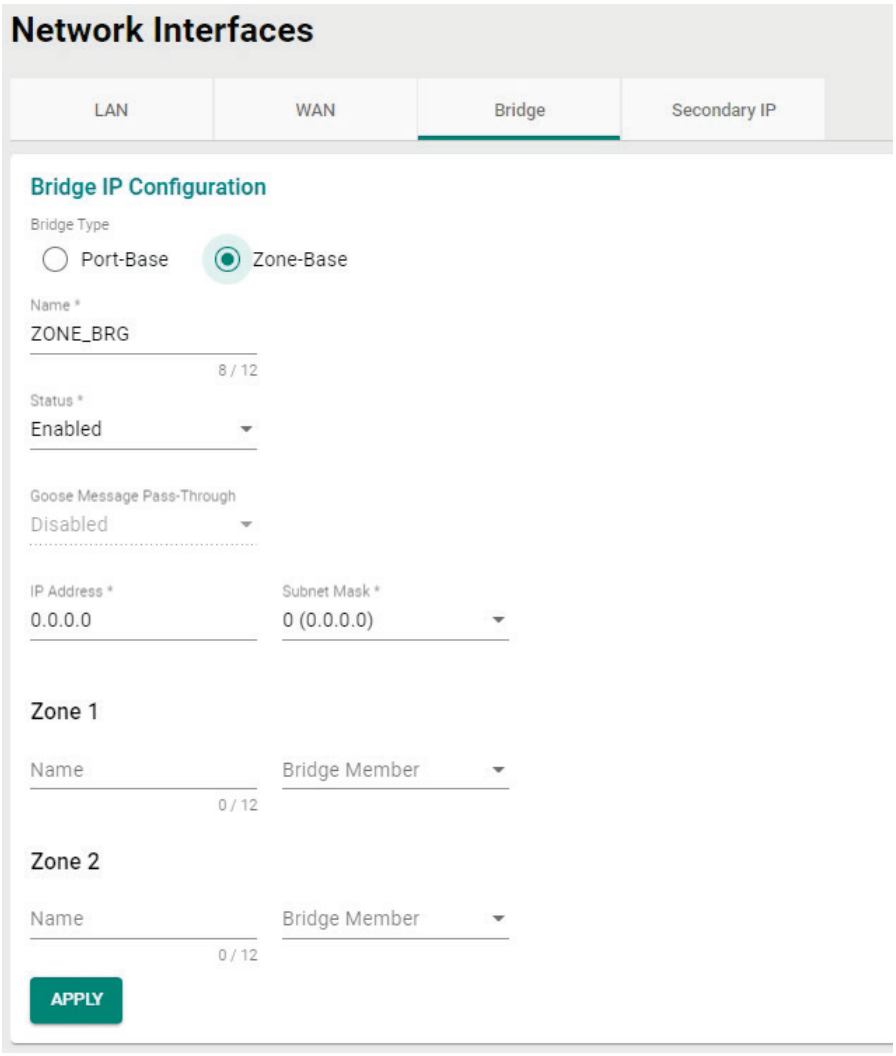
Setting	Description	Factory Default
Port	Select the port that will act as the bridge port.	None

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

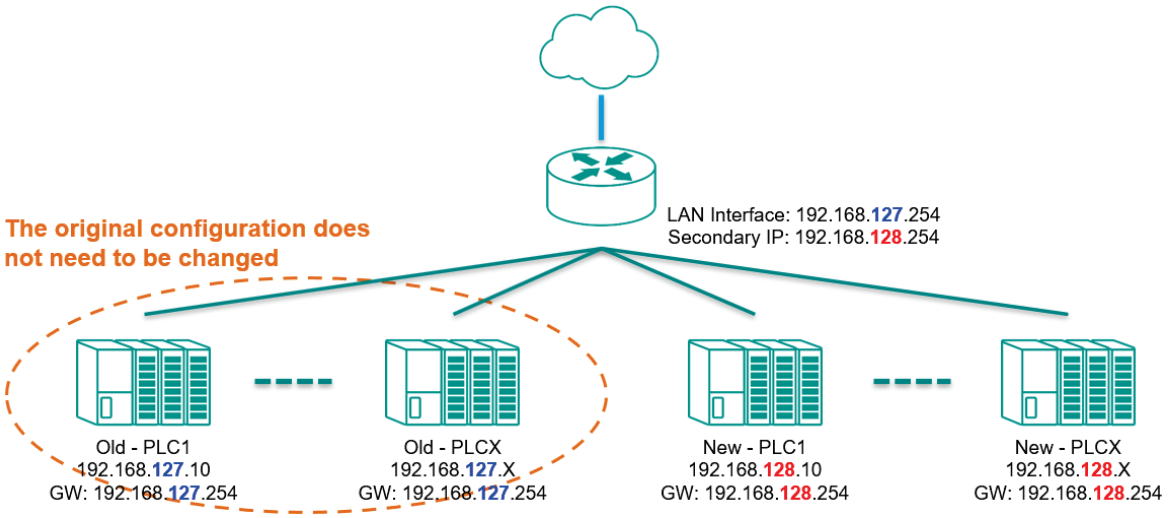
When finished, click **APPLY** to save your changes.

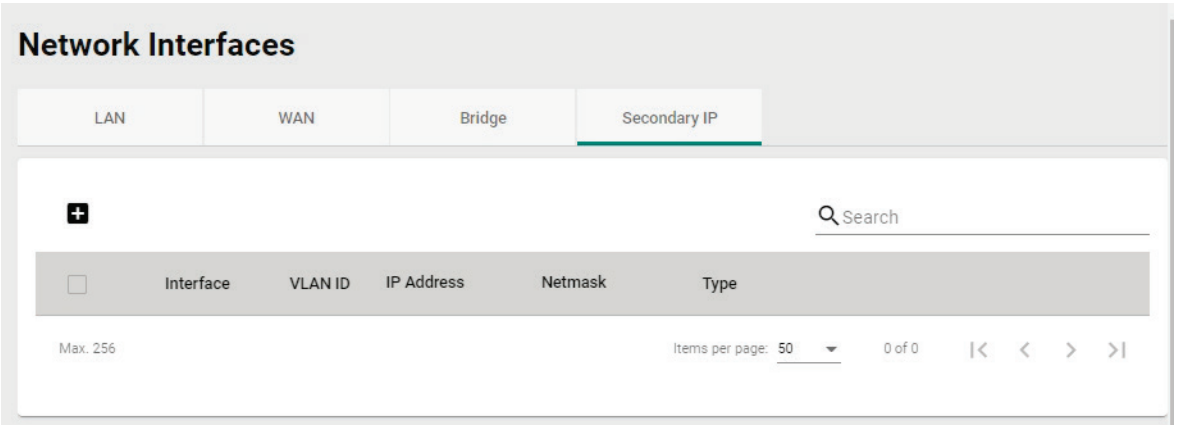
NOTE

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

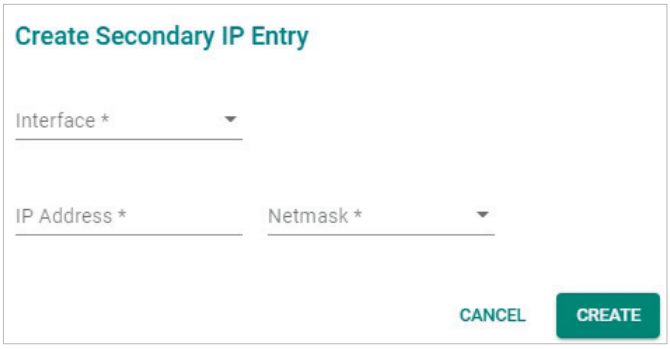
The Layer 3 interface can also act as a secondary IP. As shown in the example below, if the user needs additional IP addresses in the LAN segment but does not want to change the settings of the original interface IP/device, the secondary IP can be used to create a new network segment.





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

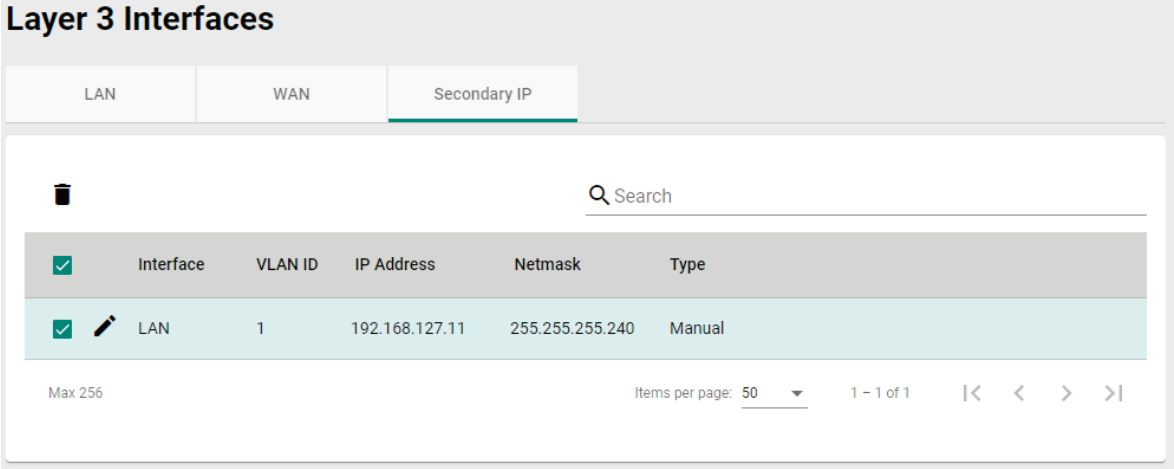
Netmask

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.

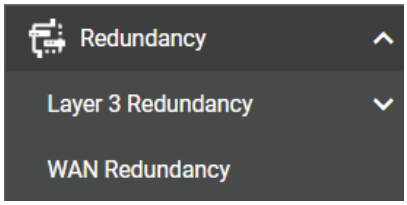


Modify a Secondary IP

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

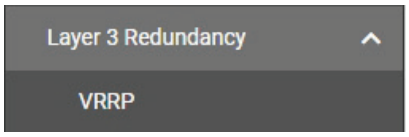
6. Redundancy

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



Layer 3 Redundancy

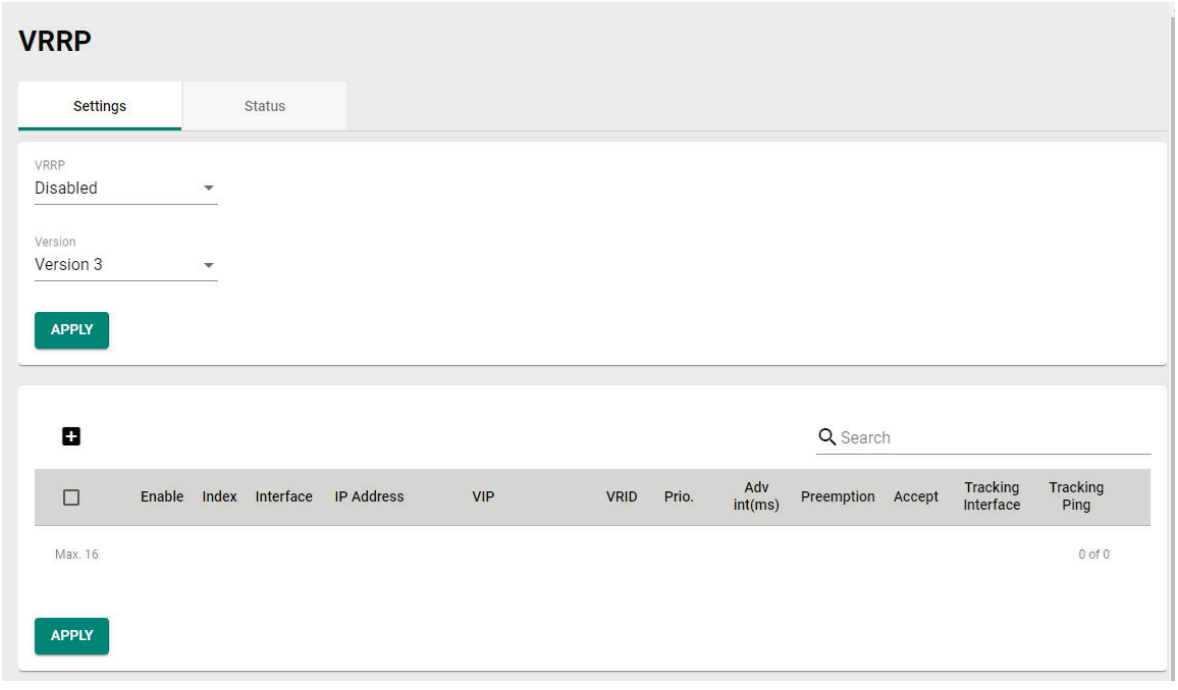
From the Layer 3 Redundancy section you can configure VRRP Settings.



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

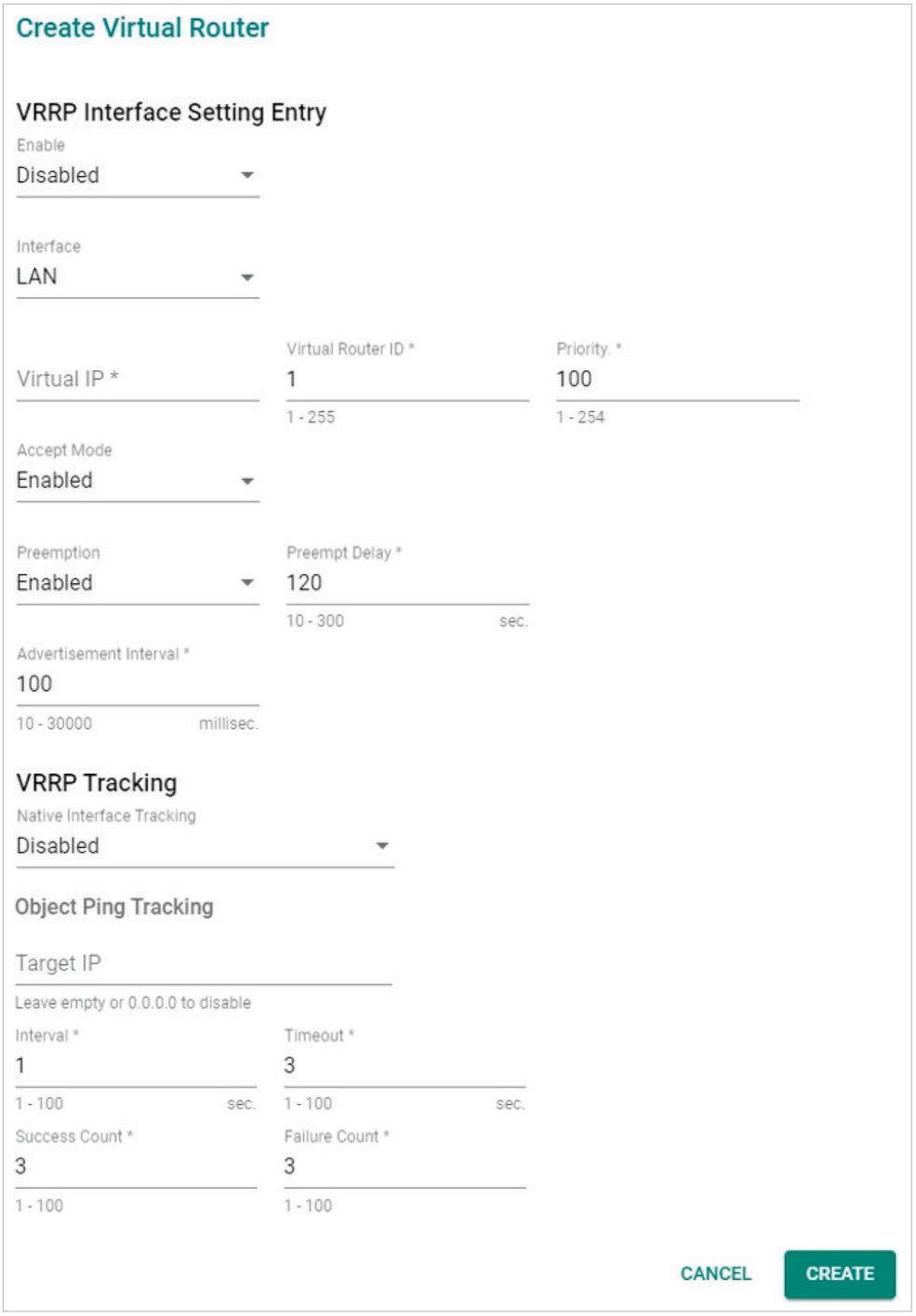
Version

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

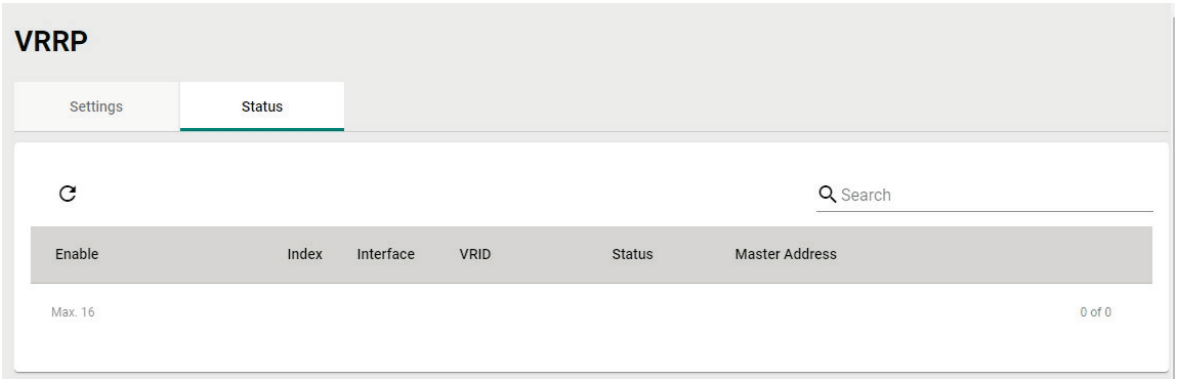
Failure Count

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.



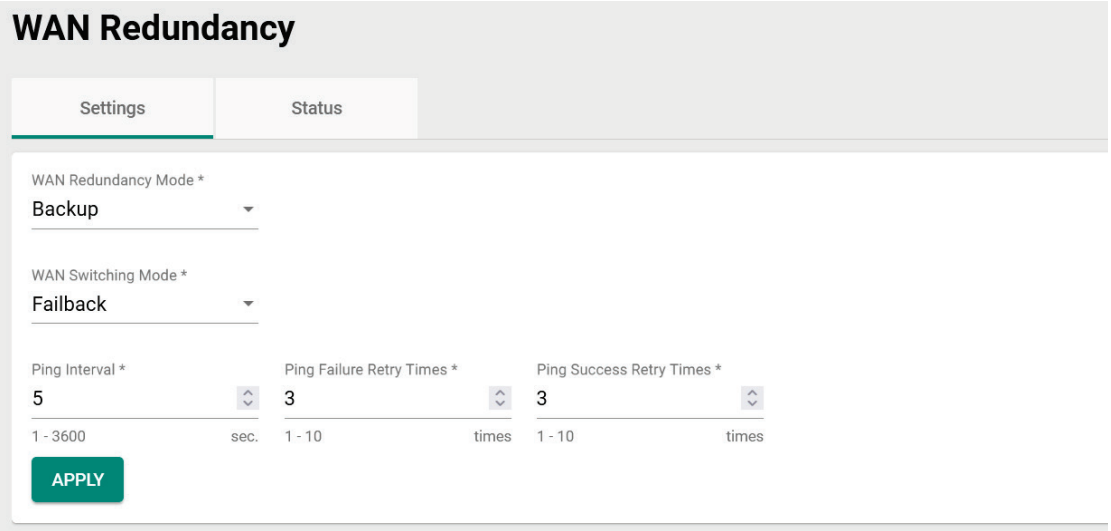
Click the icon to refresh the information.

WAN Redundancy

The WAN Redundancy feature provides failover between different WAN interfaces. When the device is in WAN Backup mode, only one WAN interface connects to the internet. If the Internet connection on the active WAN interface becomes unavailable, the system will automatically switch to the other WAN interface to recover the connection.

Settings

From the Settings screen, you can configure the redundancy mode, switching mode, and connection health ping settings.



WAN Redundancy Mode

Setting	Description	Factory Default
Disabled	Disable redundancy. If the connection on the WAN interface becomes unavailable, the connection will be lost.	Disabled
Backup	If the connection on the active WAN interface becomes unavailable, the system will automatically switch to the other WAN interface to recover the connection.	

WAN Switching Mode

Setting	Description	Factory Default
Failover	The system will only switch to the backup WAN interface when the current WAN interface becomes unavailable.	Failback
Failback	The system will switch to the backup WAN interface when the current WAN interface becomes unavailable. When the original higher priority WAN interface recovers, the system will switch back.	

Ping Interval

Setting	Description	Factory Default
1 to 3600	Specify the interval (in seconds) at which the device will perform a connection alive check.	5

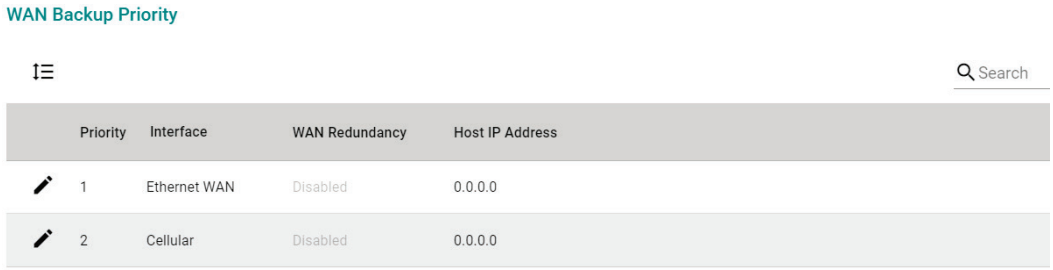
Ping Failure Retry Times

Setting	Description	Factory Default
1 to 10	Specify the number of times the device will ping the configured host IP through the active WAN interface. If the ping check consecutively fails for the specified number of retries, the device will consider the WAN interface unavailable and will switch to the backup WAN interface. The host IP is configured per WAN interface. Refer to Modify a WAN Redundancy Interface.	3

Ping Success Retry Times

Setting	Description	Factory Default
1 to 10	Specify the number of times the device will ping the configured host IP through the higher priority WAN interface in Failback mode. If the ping check consecutively succeeds for the specified number of retries, the device will consider the WAN interface recovered and will switch back to that WAN interface. The host IP is configured per WAN interface. Refer to Modify a WAN Redundancy Interface.	3

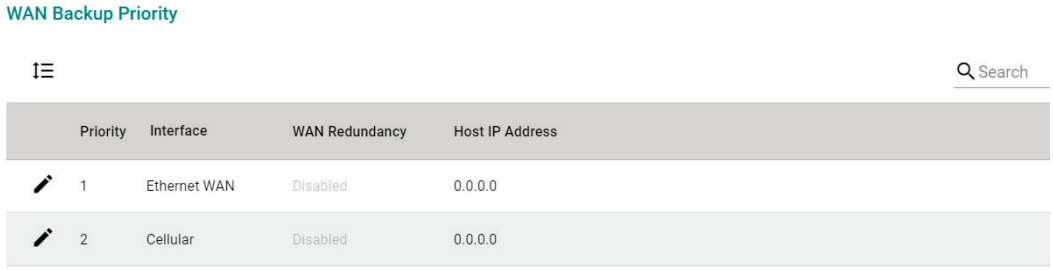
Reorder the WAN Interface Priority



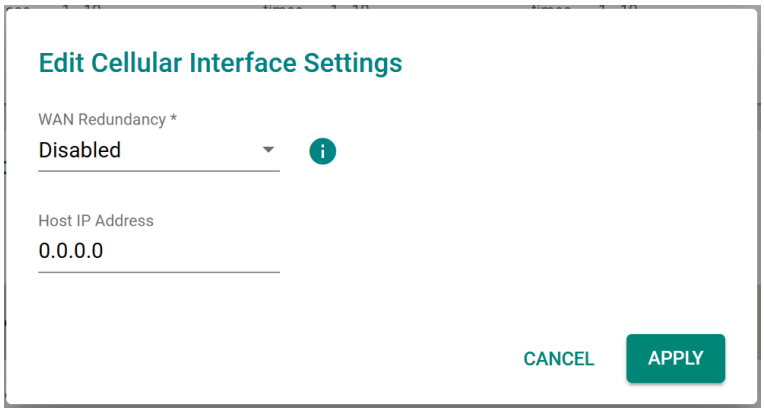
From the WAN Backup Priority table, click the **Reorder** ( ) icon, then click and drag the interface to its desired priority.

The device will always connect to the Internet through WAN interface with the highest priority, while the other WAN interface will act as a backup. If WAN redundancy is enabled, the system will switch to the backup interface if the active WAN interface becomes unavailable.

Modify a WAN Redundancy Interface



From the WAN Backup Priority table, click the **Edit** ( ) icon to edit the settings of that WAN interface.



WAN Redundancy

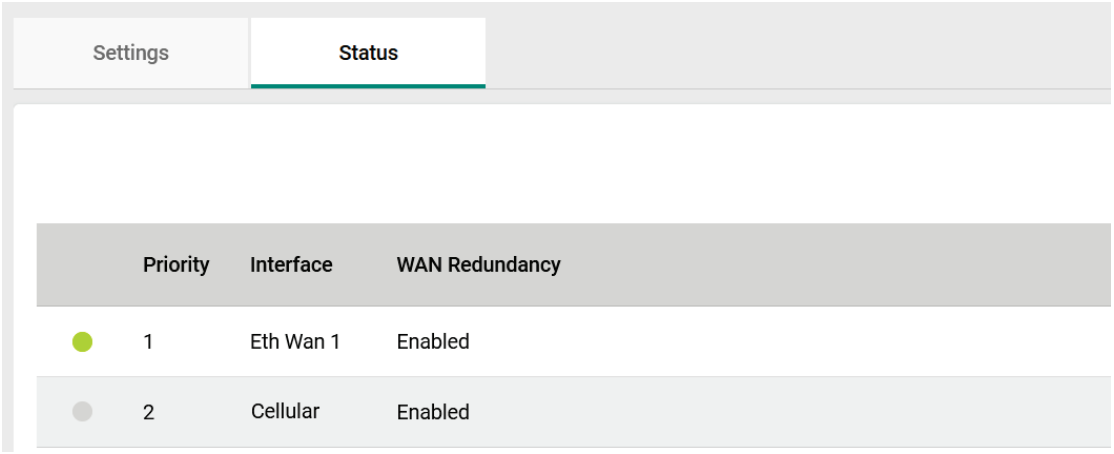
Setting	Description	Factory Default
Enabled or Disabled	Enable or disable WAN redundancy functionality for this interface.	Disabled

Host IP Address

Setting	Description	Factory Default
IP address	Enter the ping host IP address. This is used to perform WAN connection alive checks.	0.0.0.0

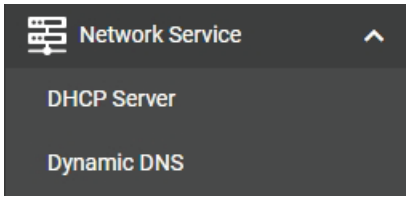
Status

The Status screen shows the current connection and redundancy status of the WAN interfaces. A green dot indicates an Internet connection is established on that interface. A grey dot means the interface is not in use.



7. Network Service

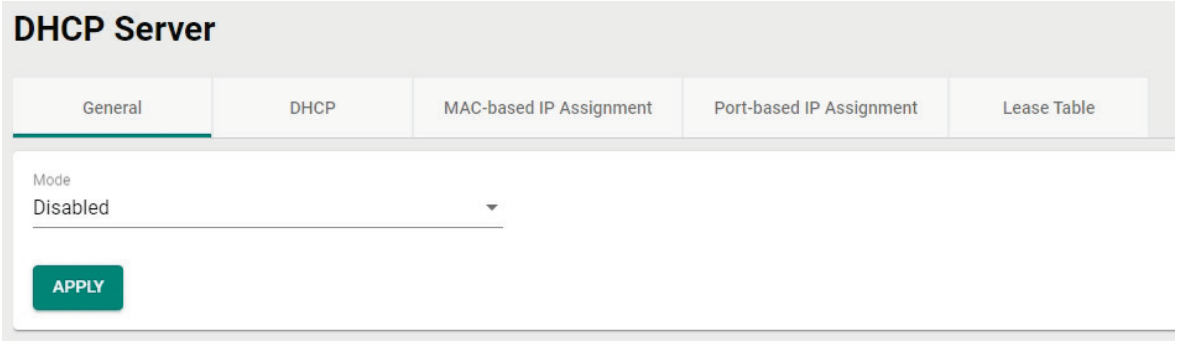
From the **Network Service** section the following functions can be configured: **DHCP Server,** and **Dynamic DNS**.



DHCP Server

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

General Settings



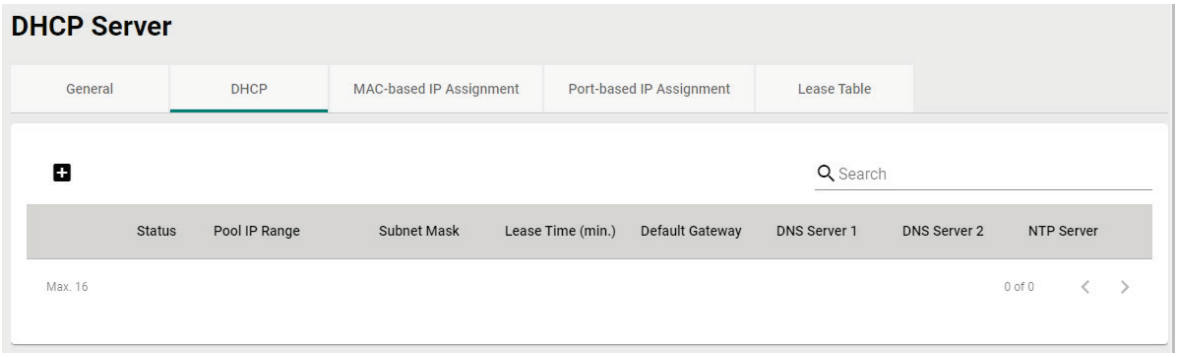
DHCP Server Mode

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.

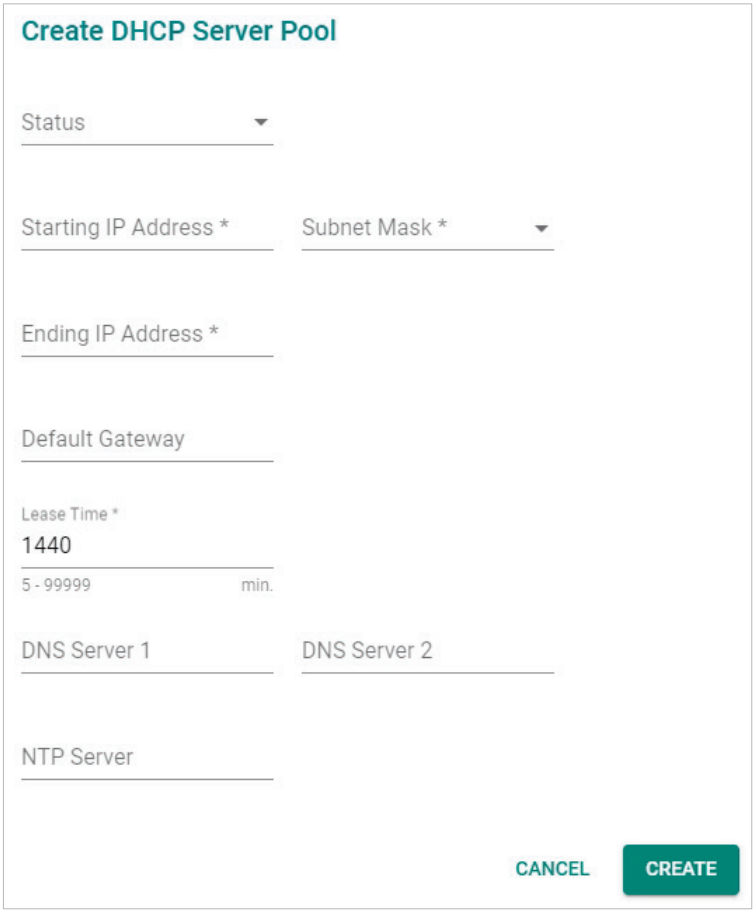
DHCP

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

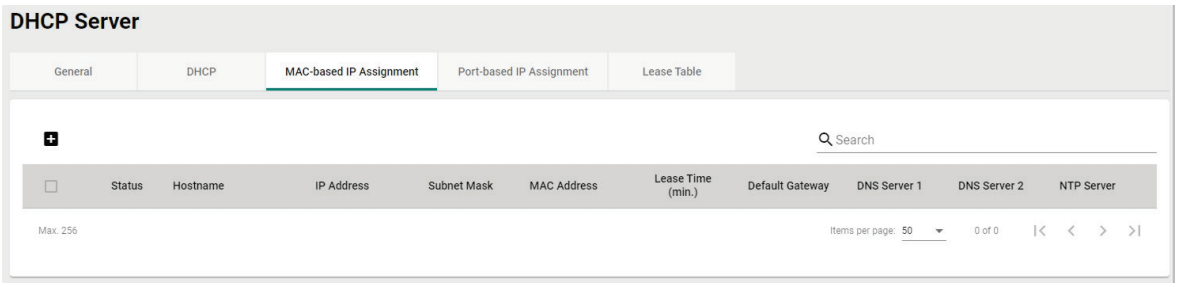
Click  next to the DHCP Server pool entry you want to delete.

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

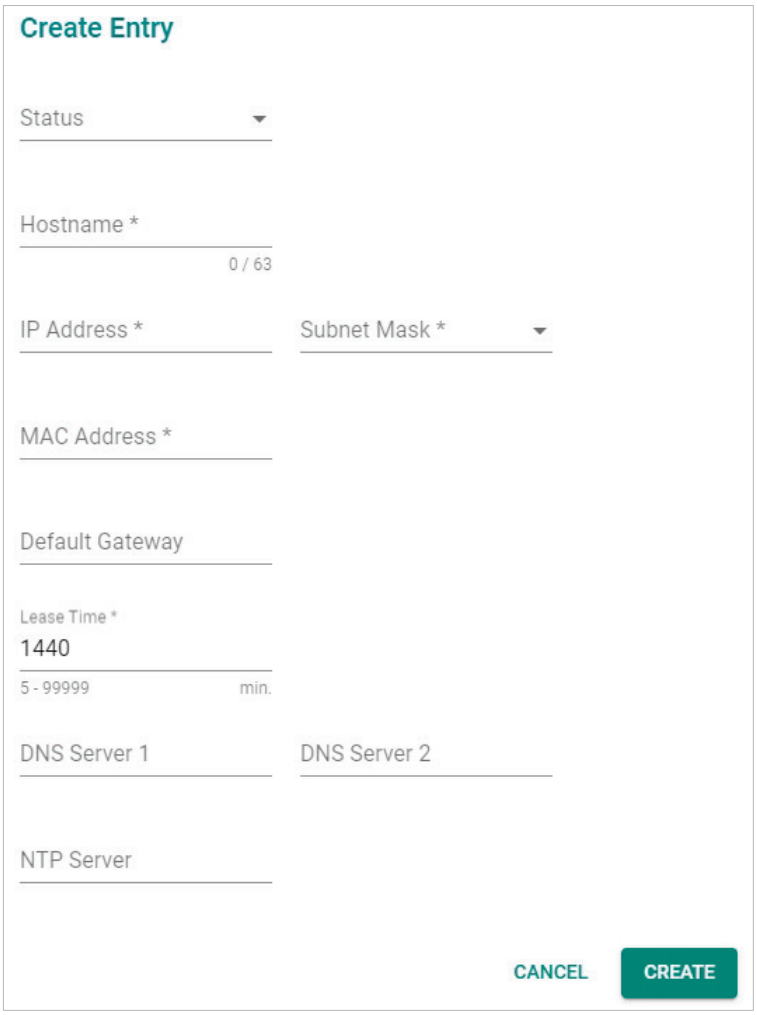
Use the Static DHCP list to ensure that devices connected to the Industrial Secure Router always use the same IP address. The static DHCP list matches IP addresses to MAC addresses.



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.

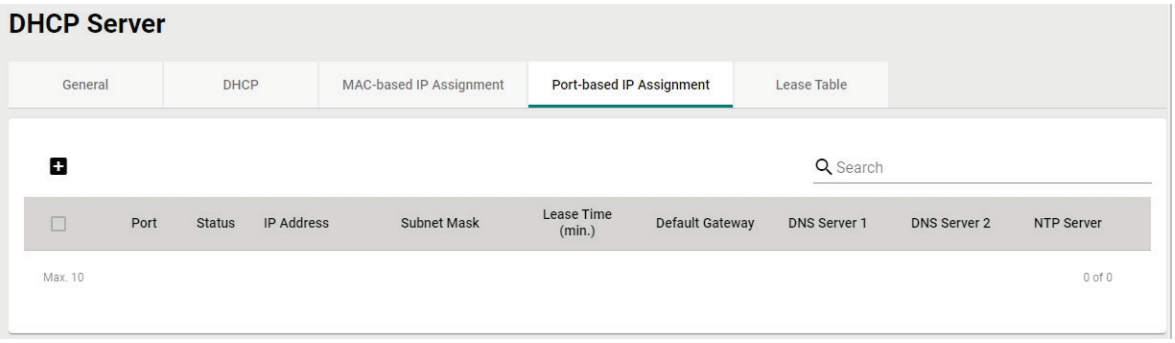
Delete a MAC-based IP Entry

Select the entry from the list and click .

Modify a MAC-based IP Entry

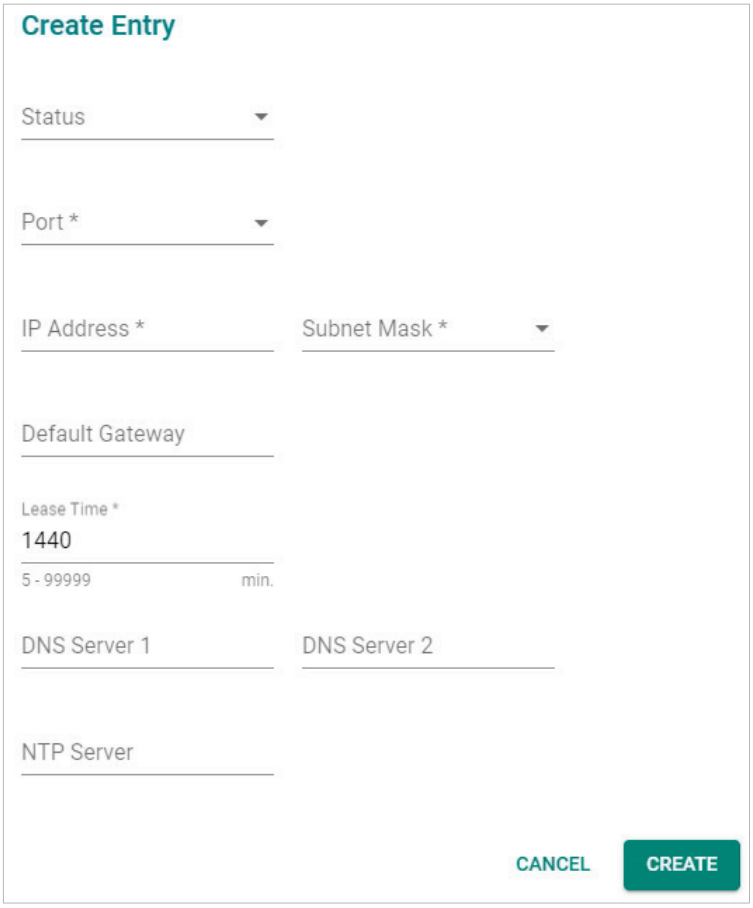
Click next to the MAC-based IP entry you want to modify. When finished, click **APPLY** to save your changes.

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

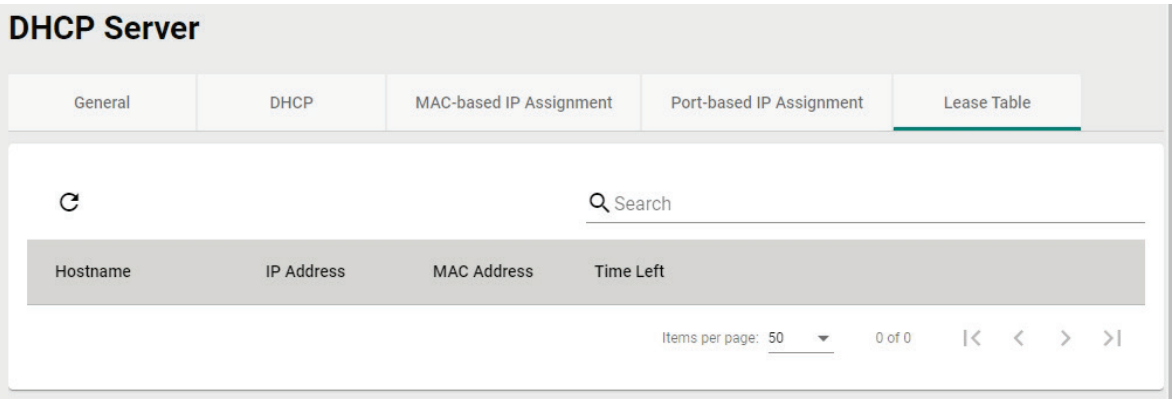
Select the entry from the list and click .

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

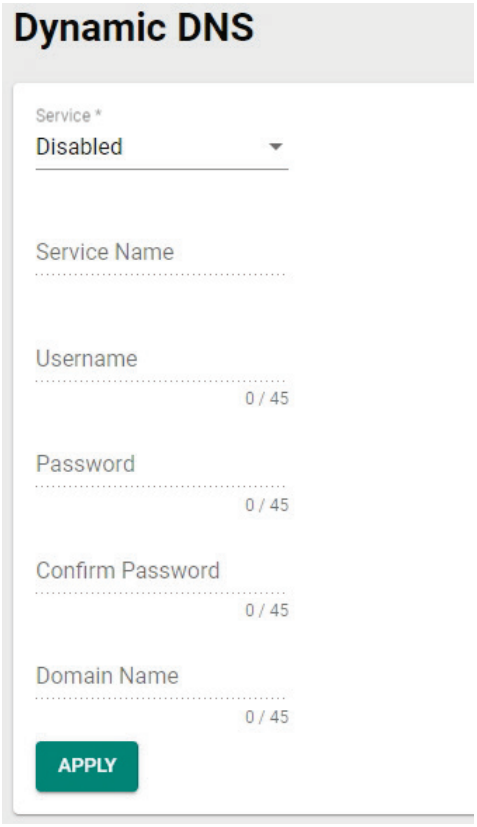
The Lease Table provides an overview of the current DHCP clients.



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

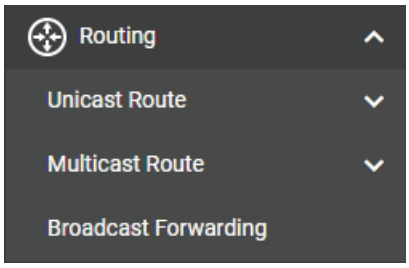
Domain name

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

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

8. Routing

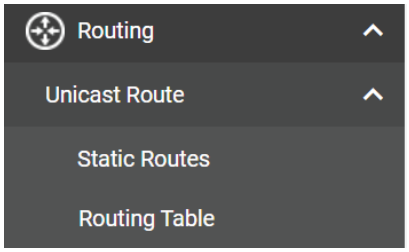
From the **Routing** section, you can configure the **Unicast Route**, **Multicast Route**, and **Broadcast Forwarding** settings.



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.

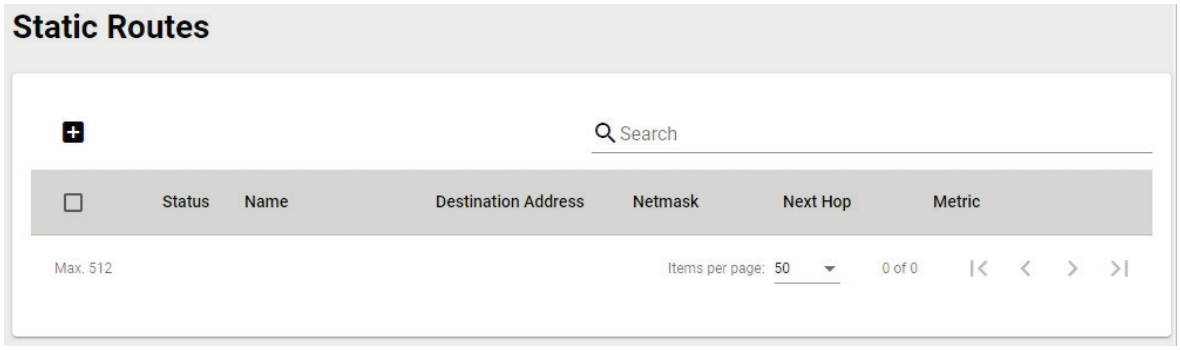
From the **Unicast Route** section, the following functions can be configured: **Static Routes, RIP, OSPF,** and **Routing Table**.



Static Routes

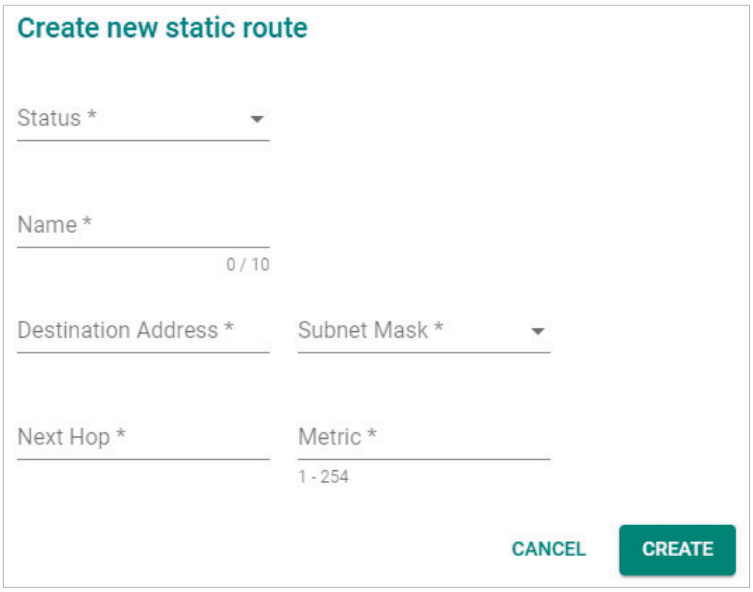
The Static Routing page is used to configure the Industrial Secure Router's static routing table.

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

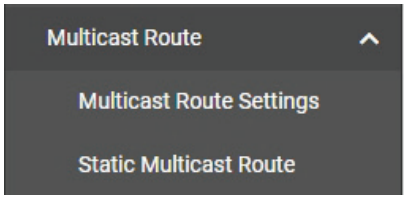
Select the entry from the list and click 🗑.

Modify an Existing Static Route

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

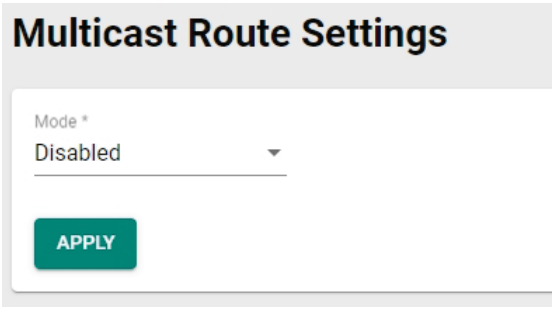
Multicast Route

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**.



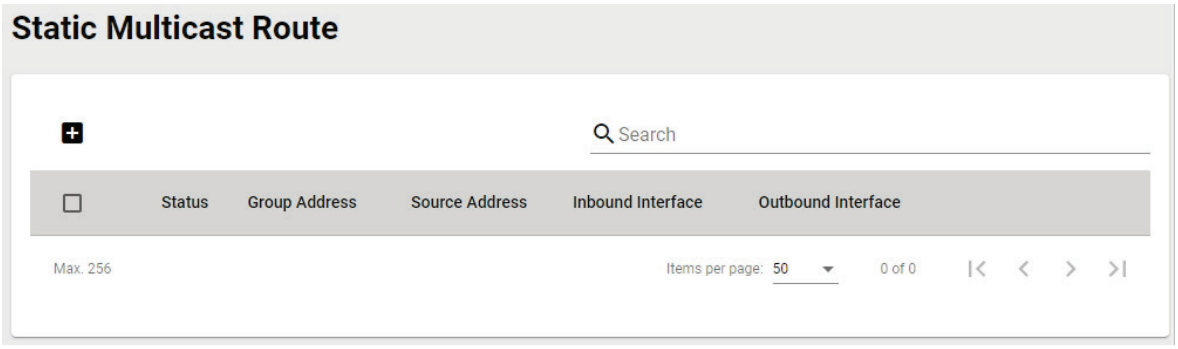
Mode

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.

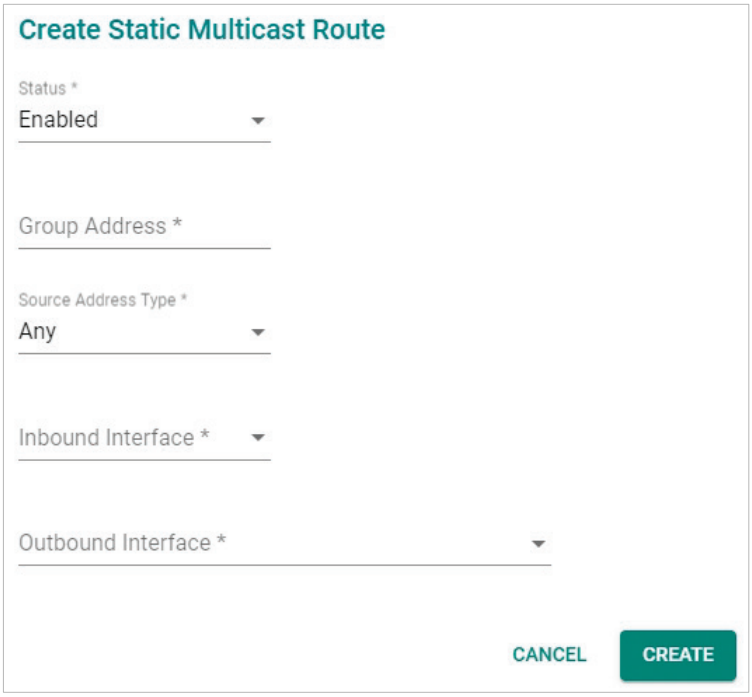
Static Multicast Route

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

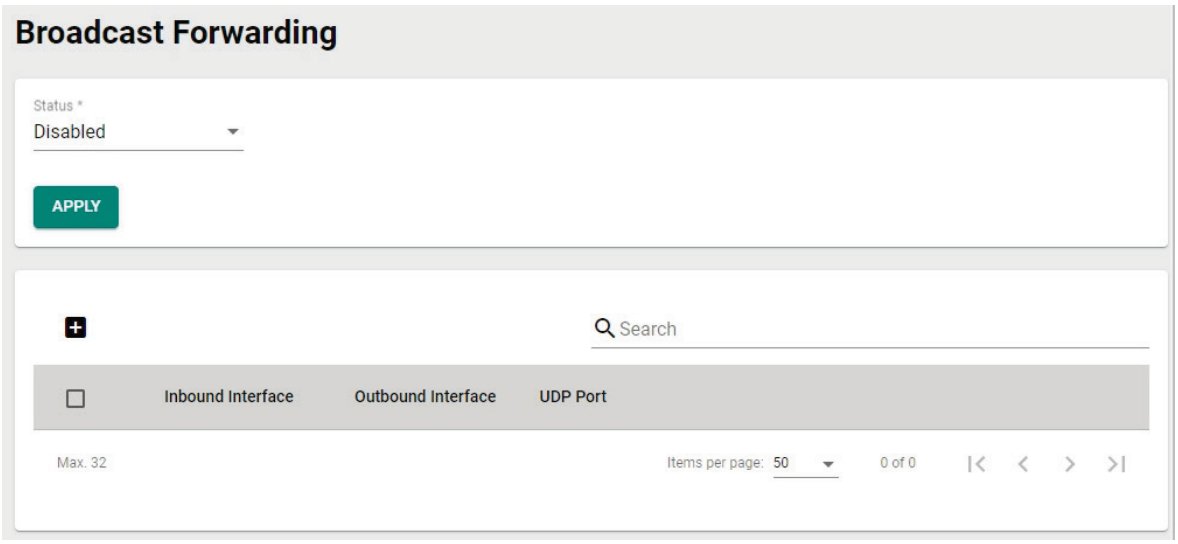
Click the icon next to the entry you want to modify. When finished, click **APPLY** to save your changes.

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.



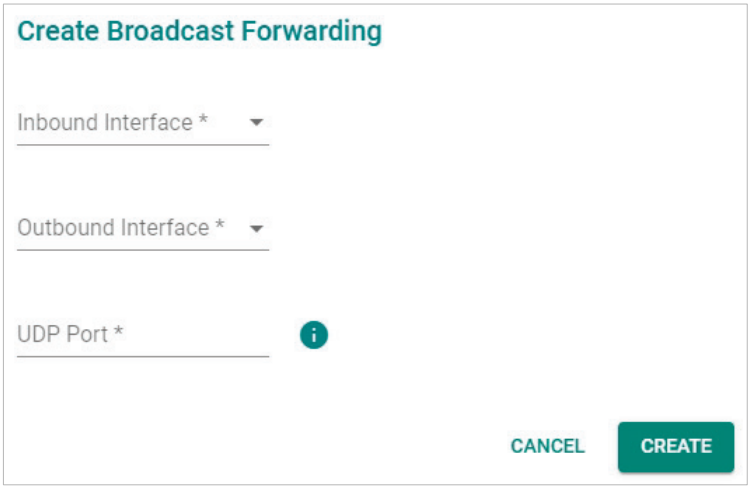
Status

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

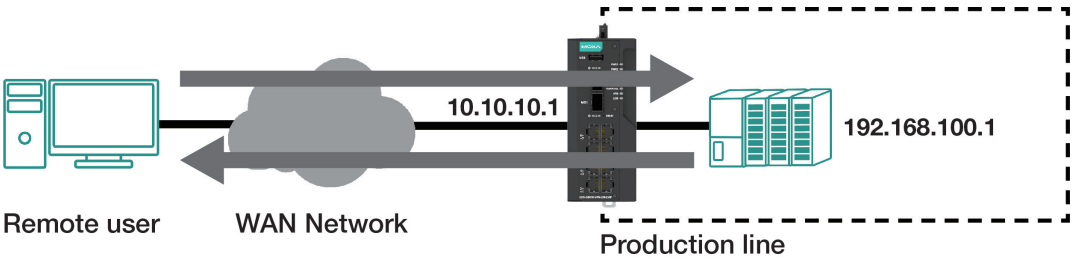
The NAT function will check if incoming or outgoing packets match the policy. It starts by checking the packet against the first policy (Index=1); if the packet matches this policy, the Industrial Secure Router will translate the address immediately and then start checking the next packet. If the packet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

NOTE

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

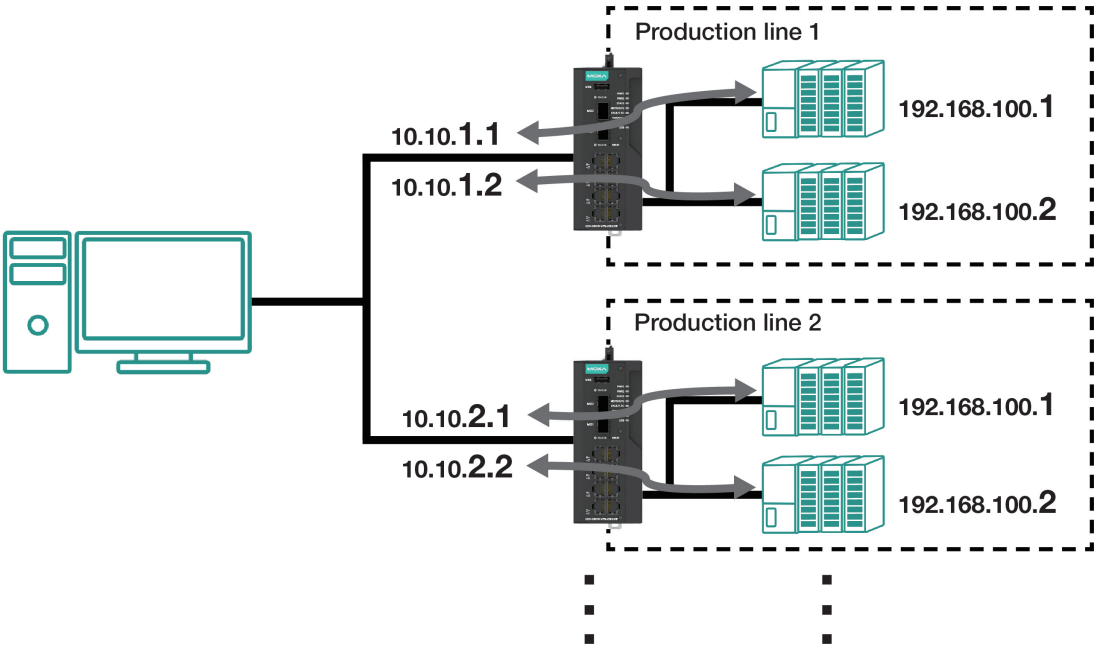
1-to-1 NAT Overview

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.



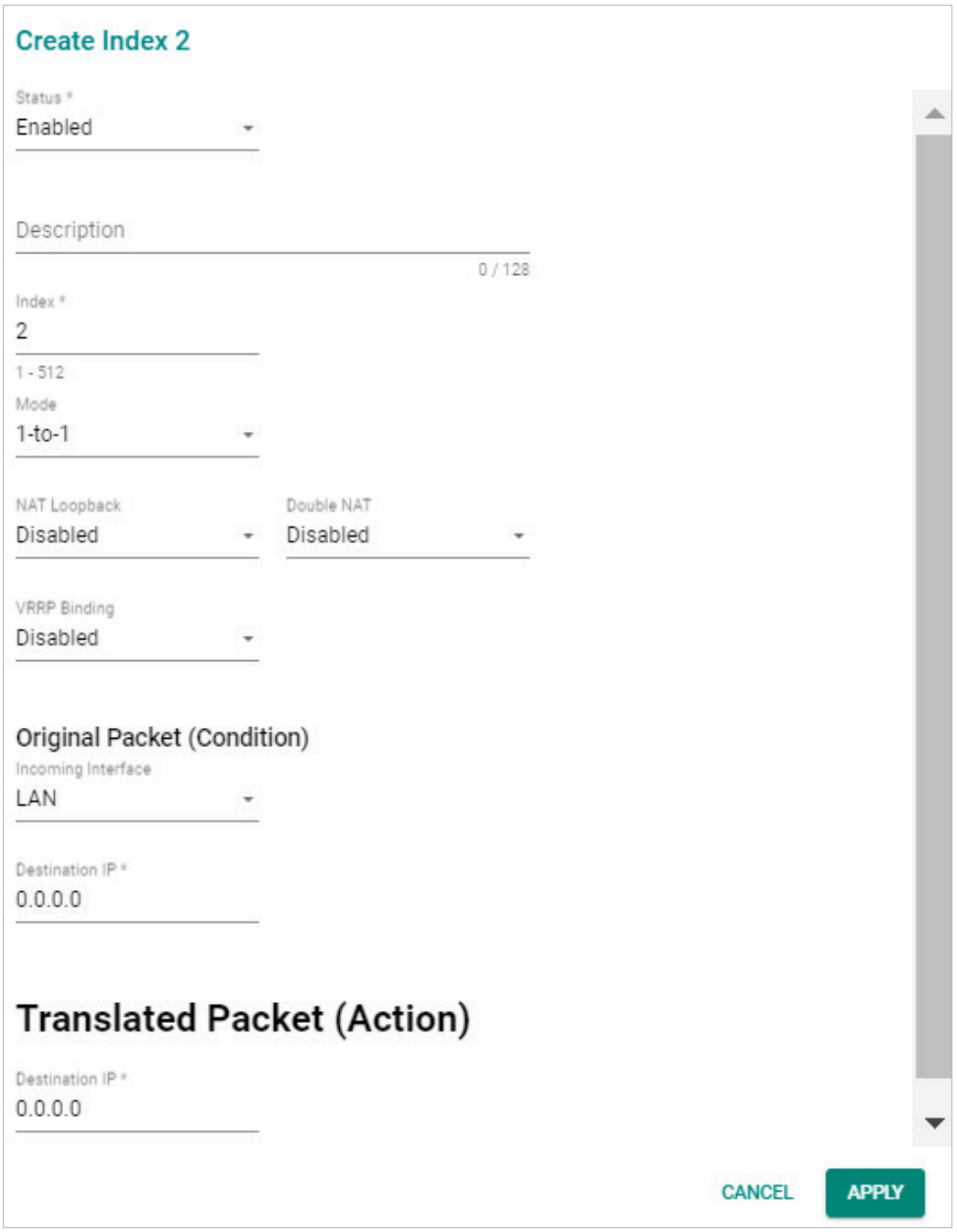
1-to-1 NAT Setting in Production Line 1

	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

Index

Setting	Description	Factory Default
1 to 512	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)

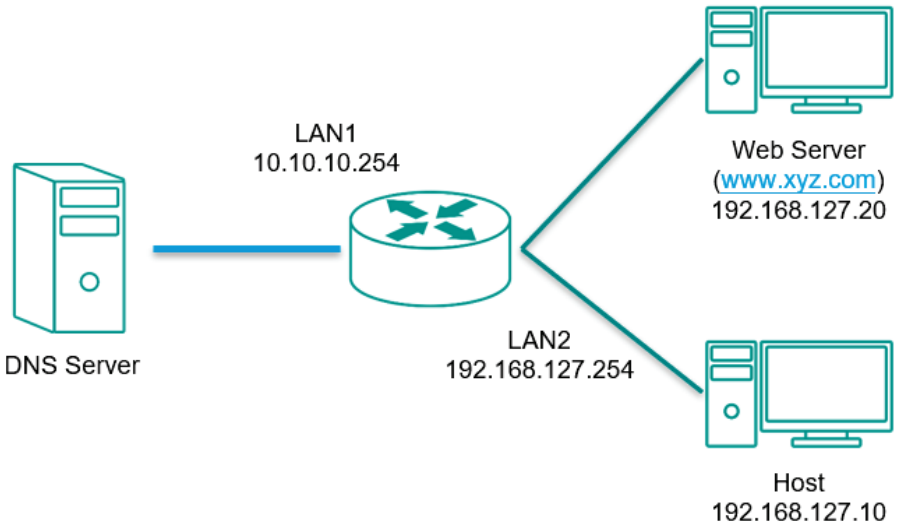
Destination IP

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:

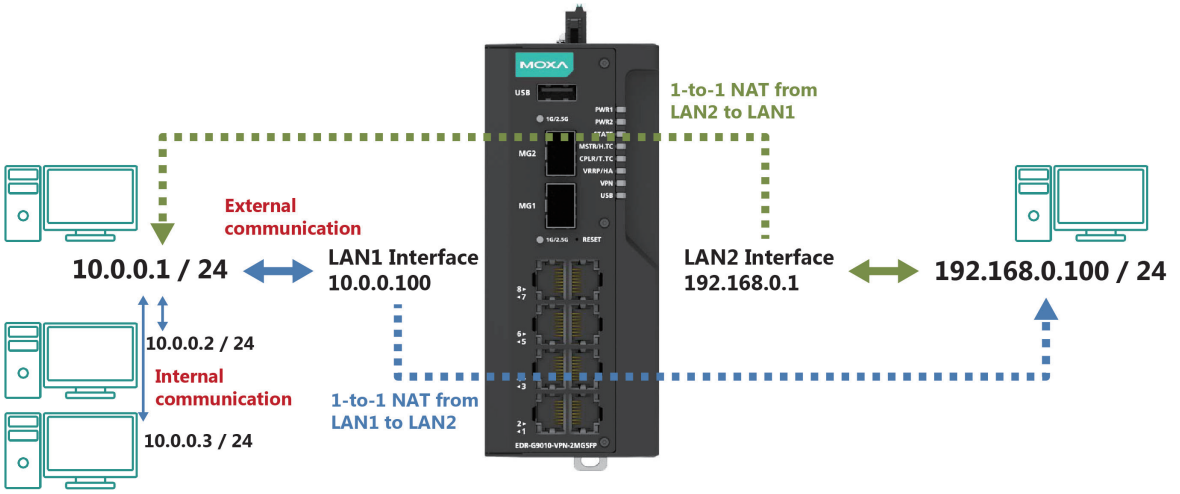
- Because the request packet comes from Host, the incoming interface does not match any NAT rule.
- The Industrial Secure Router will receive the request packet because the NAT rule has created a secondary IP: 10.10.10.20.
- The Industrial Secure Router sends the response packet to Host itself.
- Host will access the Web Server via www.xyz.com.

With NAT Loopback enabled:

- The Industrial Secure Router 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 Industrial Secure Router. The Industrial Secure Router 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



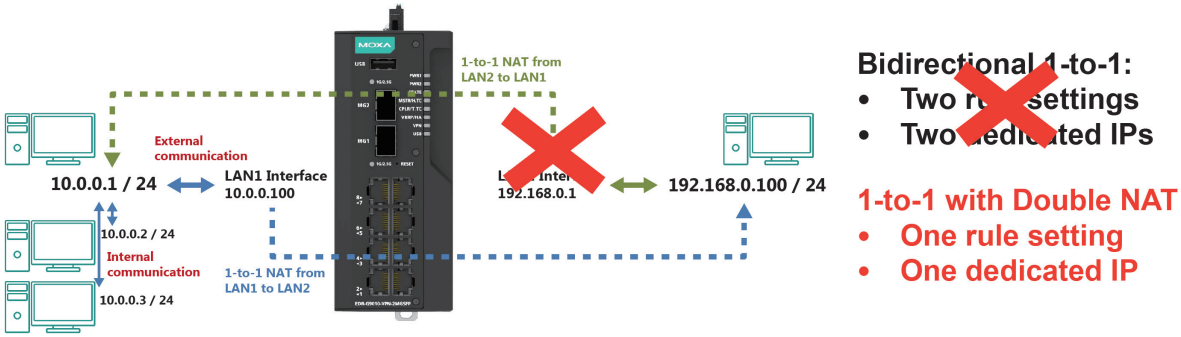
Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
Enabled		1	1-to-1		LAN	Any:Any	192.168.0.1:Any	All	Any:Any	10.0.0.1:Any
Enabled		2	1-to-1		WAN	Any:Any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



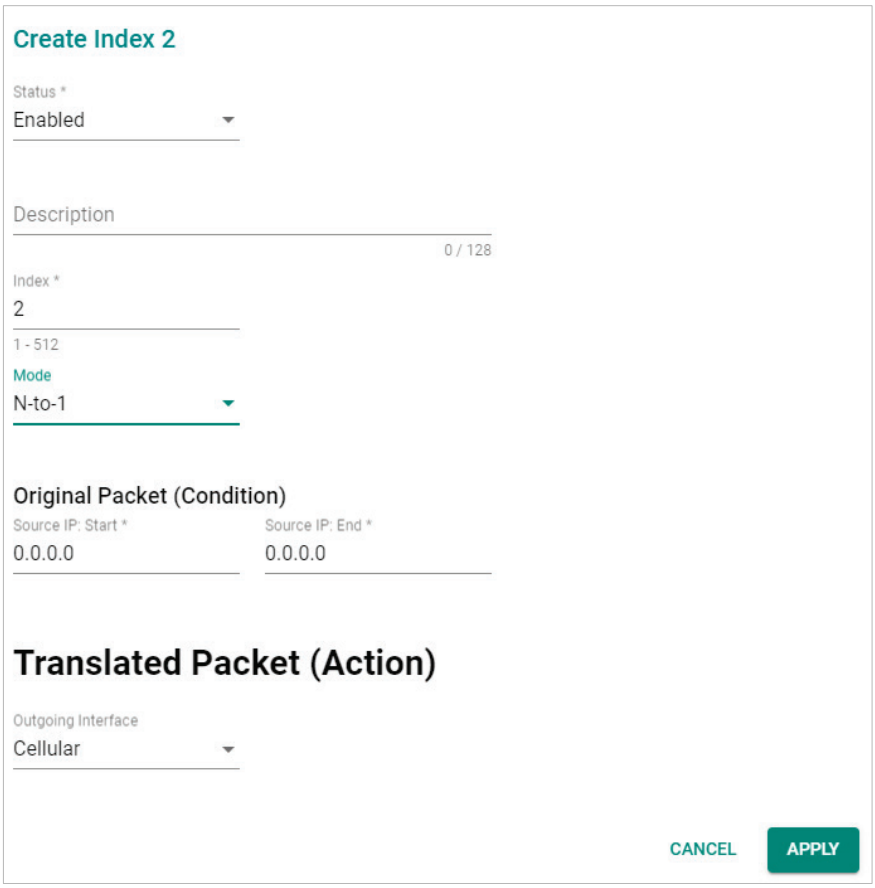
Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
Enabled		1	1-to-1		LAN	Any:Any	10.0.0.100:Any	All	Any:Any	192.168.0.100:Any

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

Index

Setting	Description	Factory Default
1 to 512	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
Cellular LAN Active WAN	Select the outgoing interface for the NAT rule.	LAN

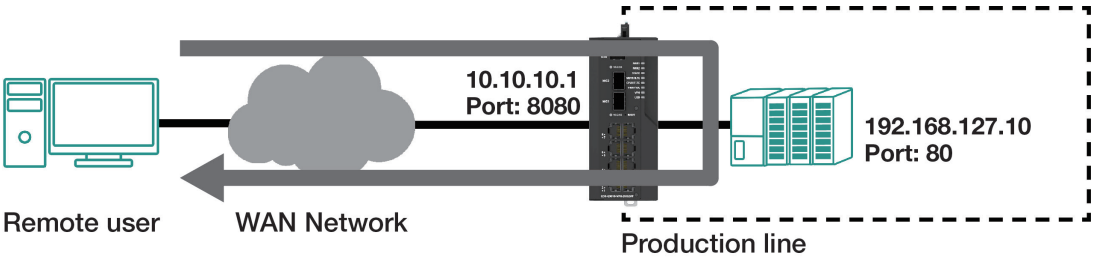
When finished, click **APPLY** to save your changes.

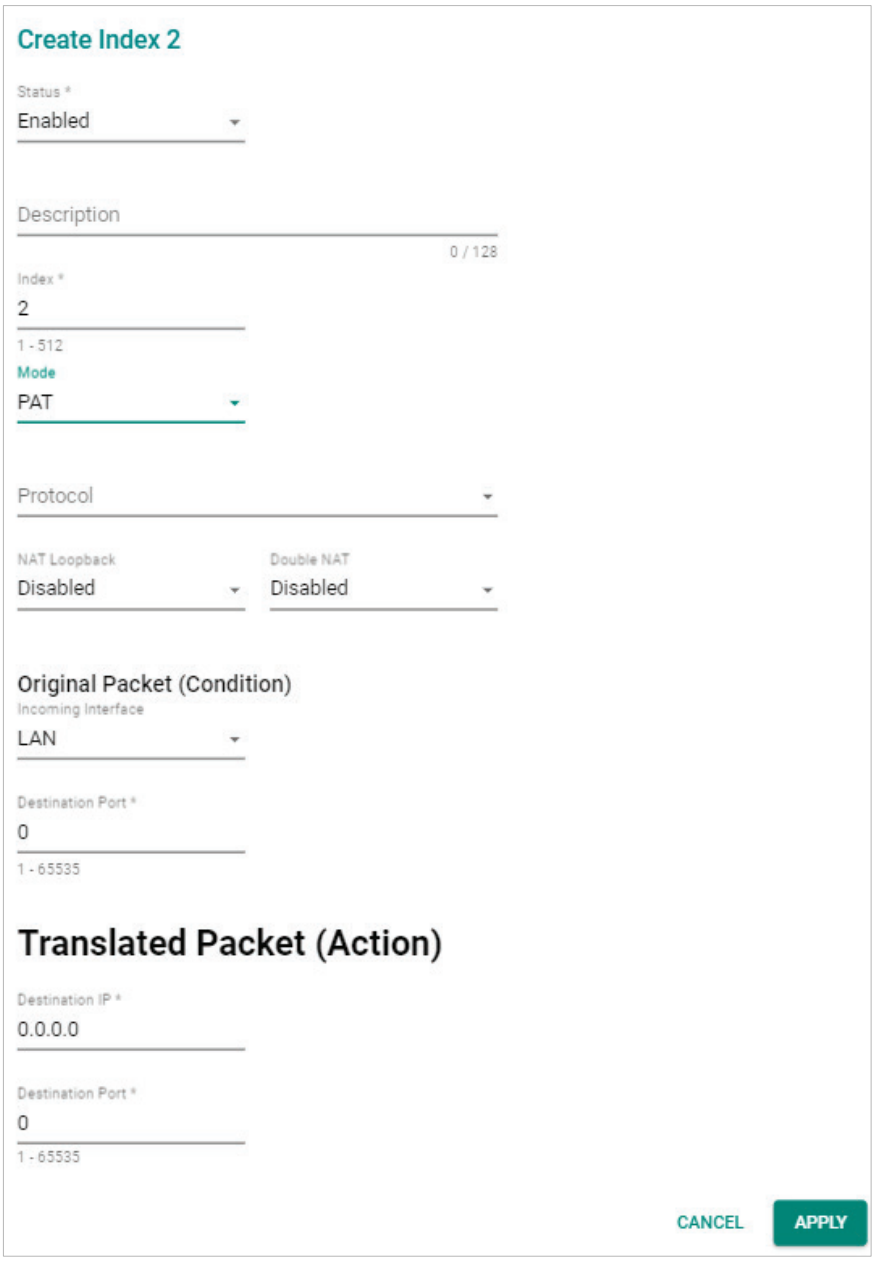
PAT (Port Address Translation)

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

Index

Setting	Description	Factory Default
1 to 512	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 2
Status *
Enabled
Description
0 / 128
Index *
2
1 - 512
Mode
Advance
Protocol
Original Packet (Condition)
Incoming Interface
LAN
Source IP Mapping Type
Any
Source Port Mapping Type
Any
Destination IP Mapping Type
Any
Destination Port Mapping Type
Single
Destination Port *
0
1 - 65535
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
Single
Destination Port *
0
1 - 65535
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

Index

Setting	Description	Factory Default
1 to 512	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

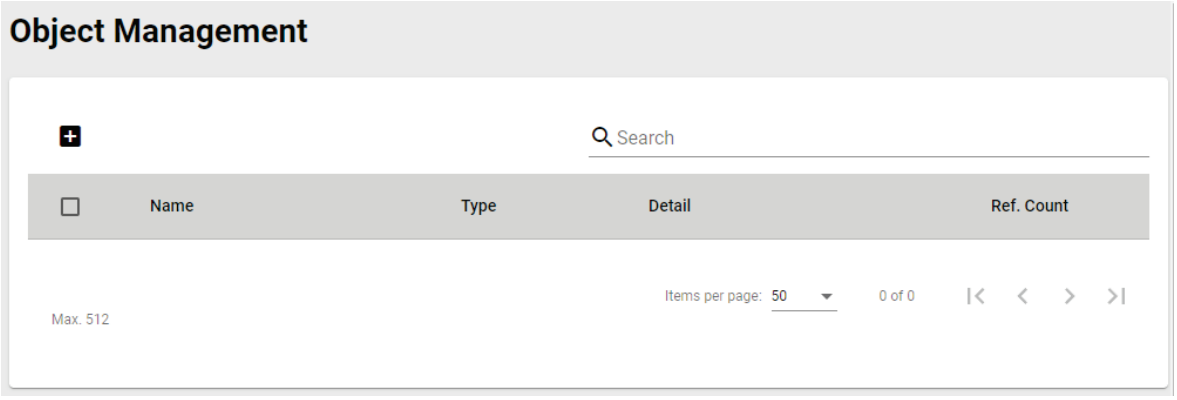
When finished, click **APPLY** to save your changes.

10. Object Management

Overview

The 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 Industrial Secure Router supports a maximum of 512 objects.

Create a New Object

The Industrial Secure Router 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

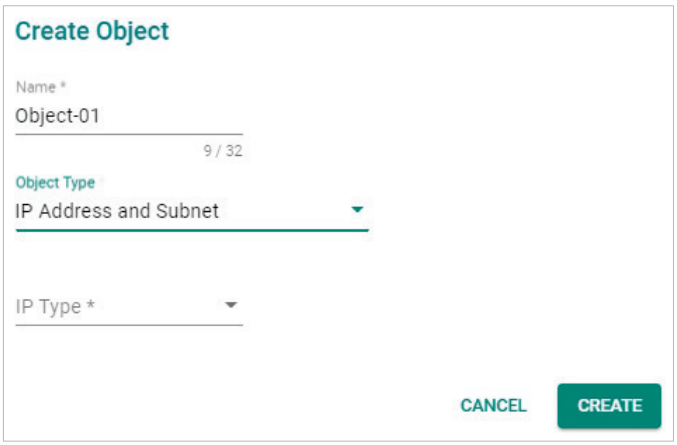
Object Type

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.

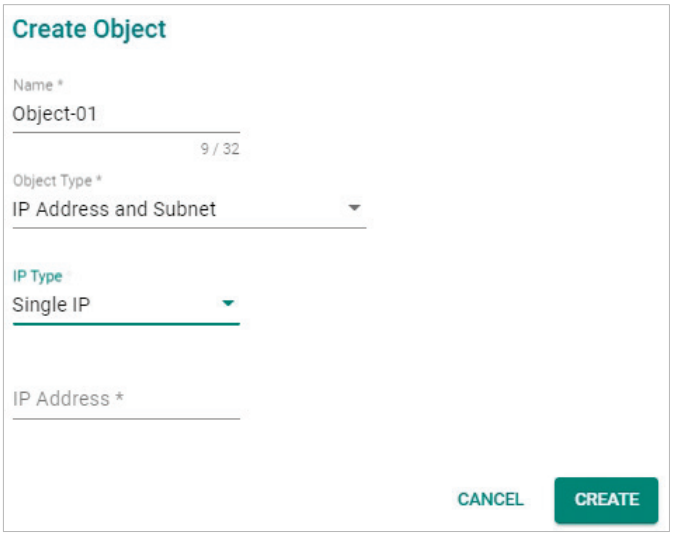
On the **Object Management** page, click the ⊞ icon to create a new object and select **IP Address and Subnet** as the Object Type.



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

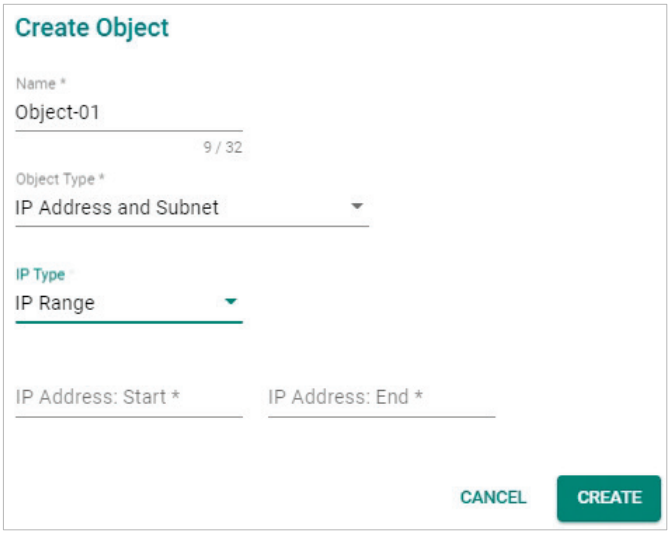
Single IP



IP Address

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

IP Range



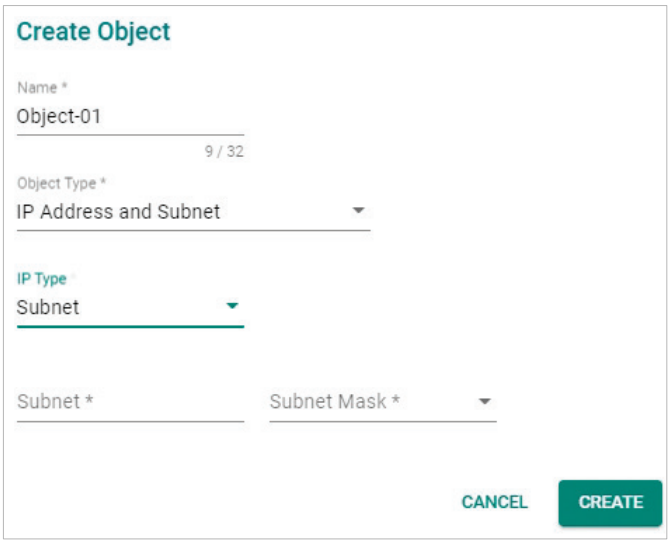
IP Address: Start

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

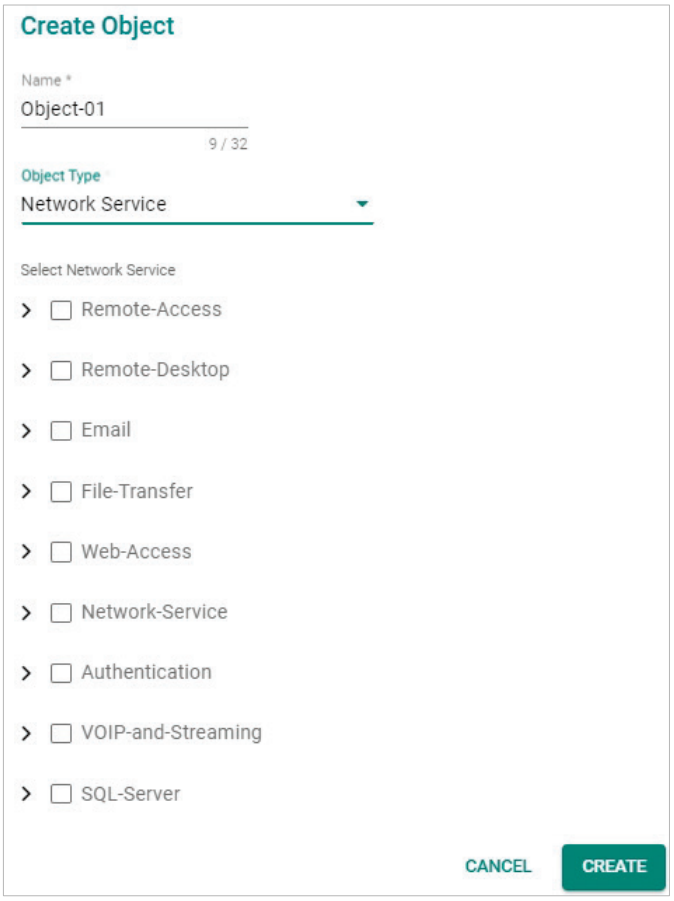
Setting	Description	Factory Default
IP address	Select the subnet mask for this IP address.	None

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.

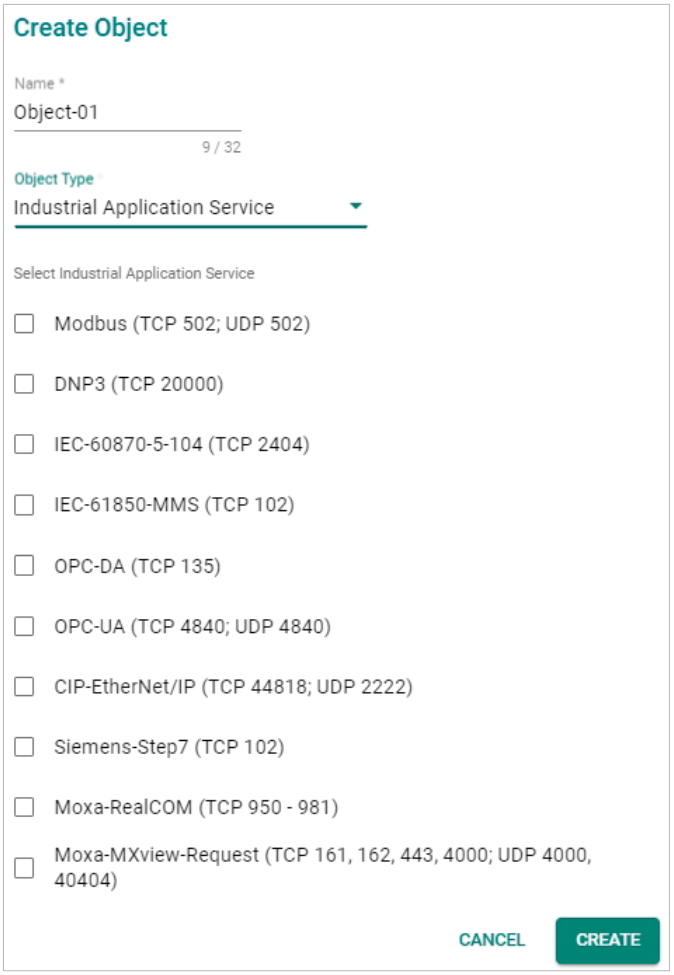
Service Name	Protocol (Port Number)
Remote-Access	WINS (TPC 1512; UDP 1512)
	TELNET (TCP 23)
	SSH (TCP 22)
Remote-Desktop	PC-Anywhere (TCP 5631; UDP 5632)
	Chrome-Remote-Desktop (UDP 5222)
	AnyDesk (TCP 6568, 7070; UDP 50001 - 50003)
	Teamviewer (TCP 5938)
	RDP (TCP 3389)
	VNC (TCP 5900)
	X-WINDOW (TCP 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.

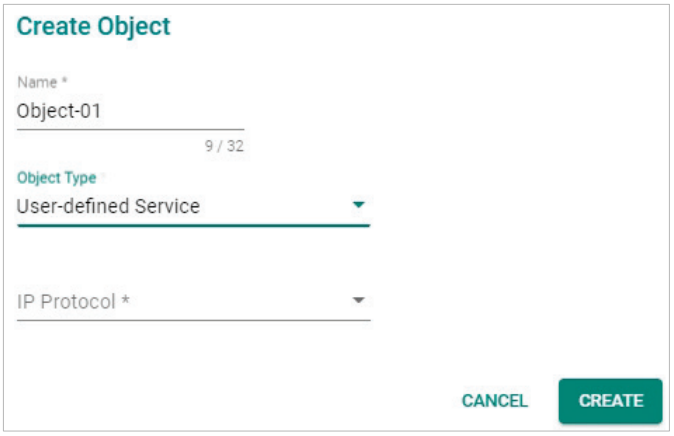
Service Name	Port Number
Modbus	TCP 502; UDP 502
DNP3	TCP 20000
IEC-60870-5-104	TCP 2404
IEC-61850-MMS	TCP 102
OPC-DA	TCP 135
OPC-UA	TCP 4840; UDP 4840
CIP-EtherNet/IP	TCP 44818; UDP 2222
Siemens-Step7	TCP 102
Moxa-RealCOM	TCP 950 – 981
Moxa-MXview-Request	TCP 161, 162, 443, 4000; UDP 4000, 40404

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.

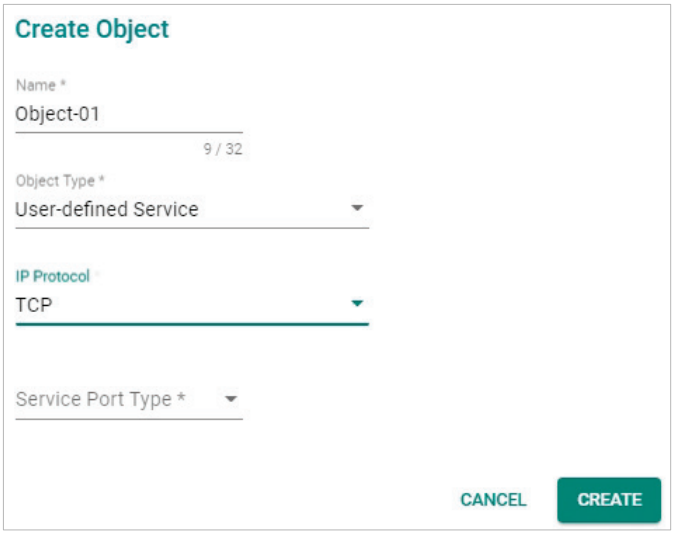
On the **Object Management** page, click the ⊞ icon to create a new object and select **User-defined Service** as the Object Type.



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

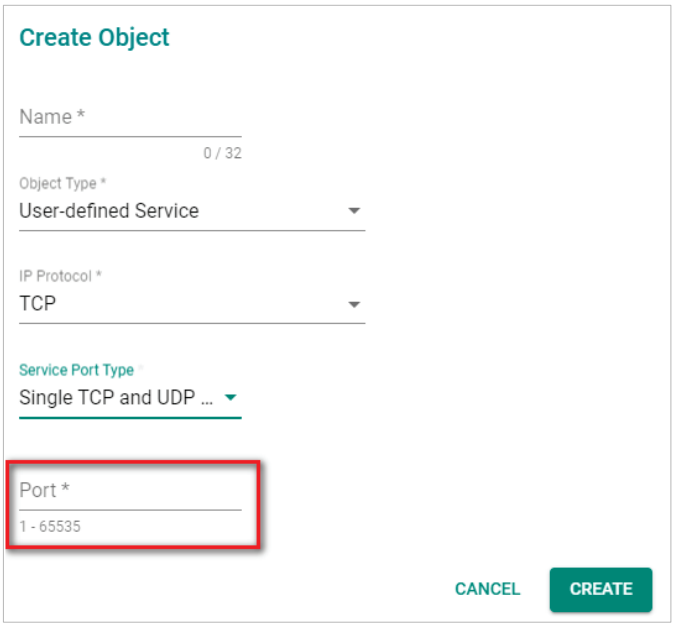
TCP, UDP, TCP and UDP



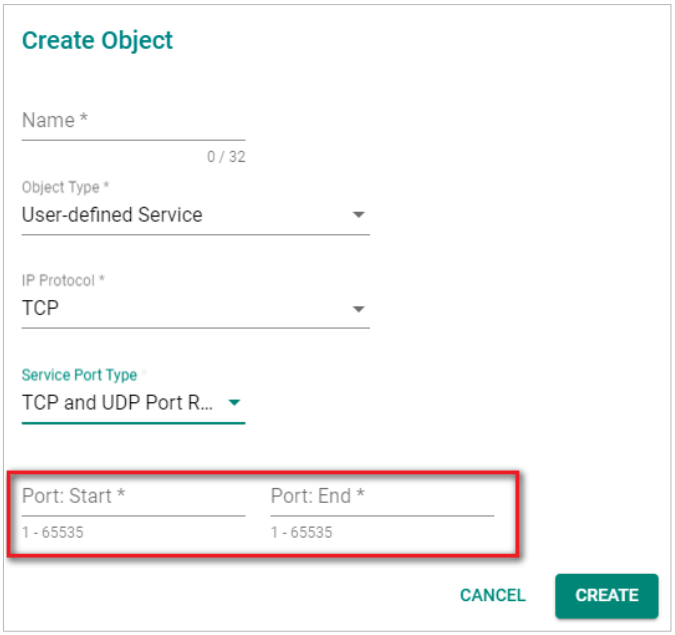
Service Port Type

Setting	Description	Factory Default
Any, Single TCP and UDP Port, TCP and UDP Port Range	Select a port type for the protocol.	None

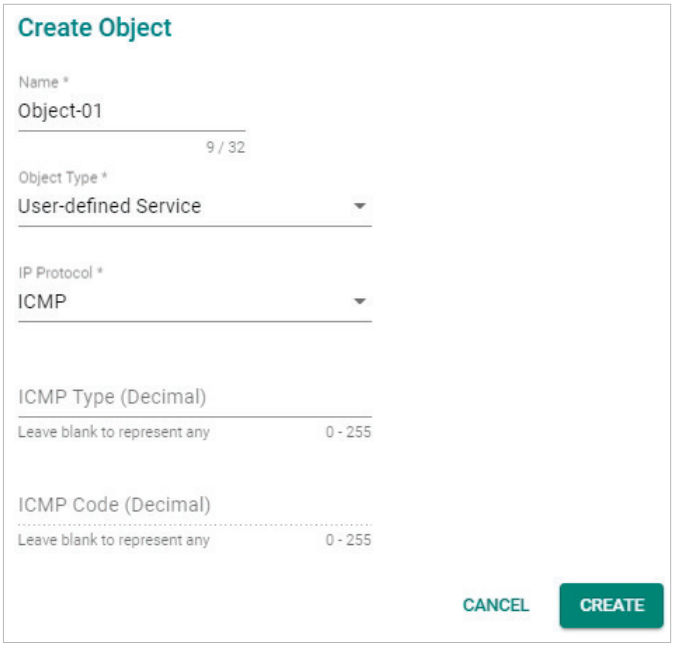
If you selected **Single TCP and UDP Port** as the port type, you also need to specify a port number. The port number range is between 1 to 65535.



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



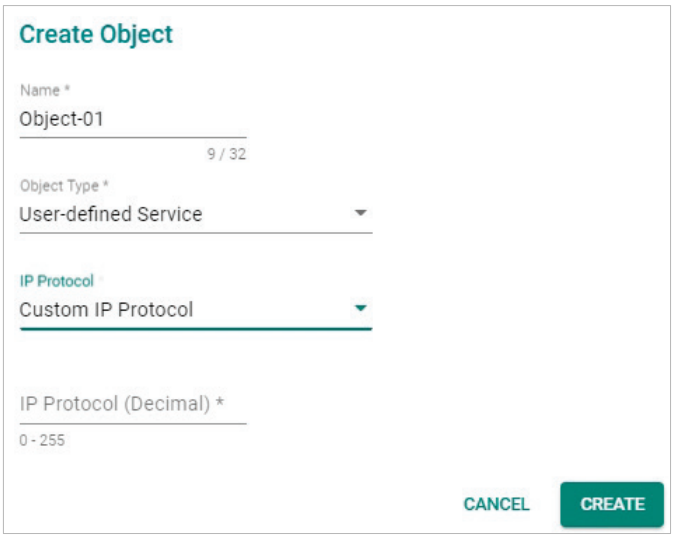
ICMP Type (Decimal)

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



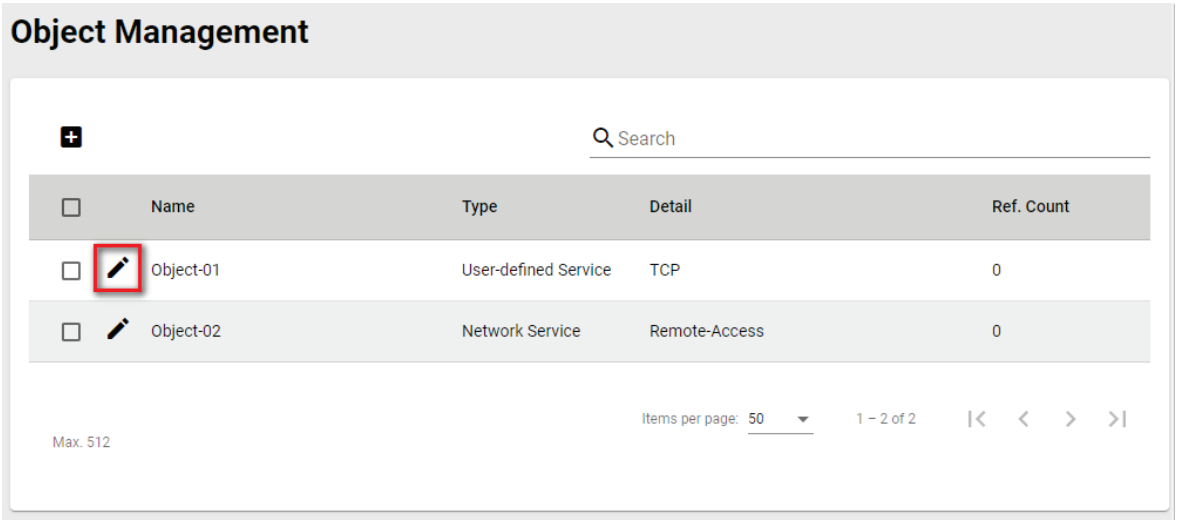
IP Protocol (Decimal)

Setting	Description	Factory Default
0 to 255	Specify the IP protocol value.	None

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

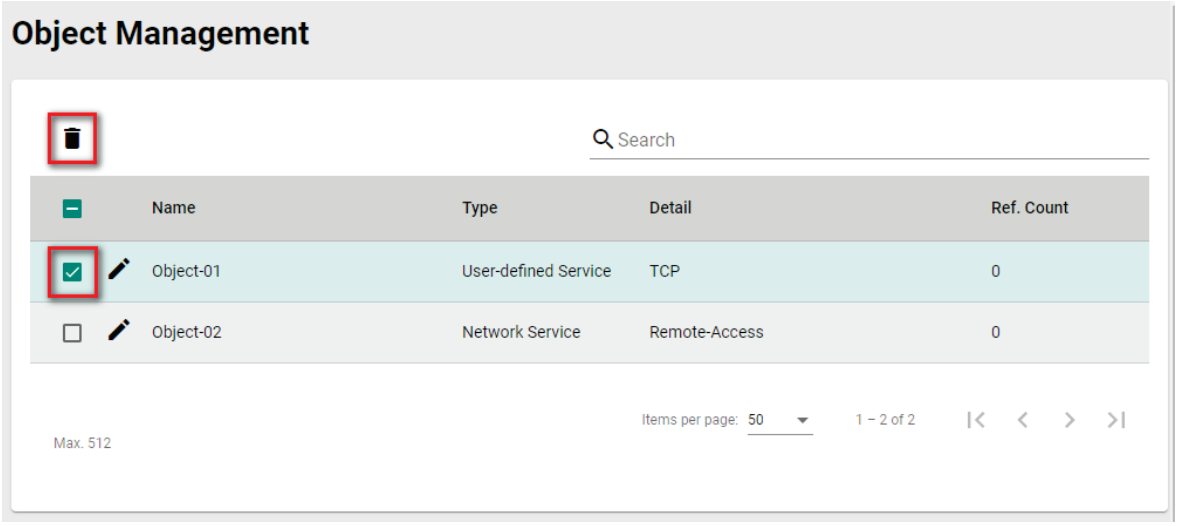
Modify an Existing Object

In the object list, click the **Edit** (✎) icon next to entry you want to modify. When finished, click **APPLY** to save your changes.



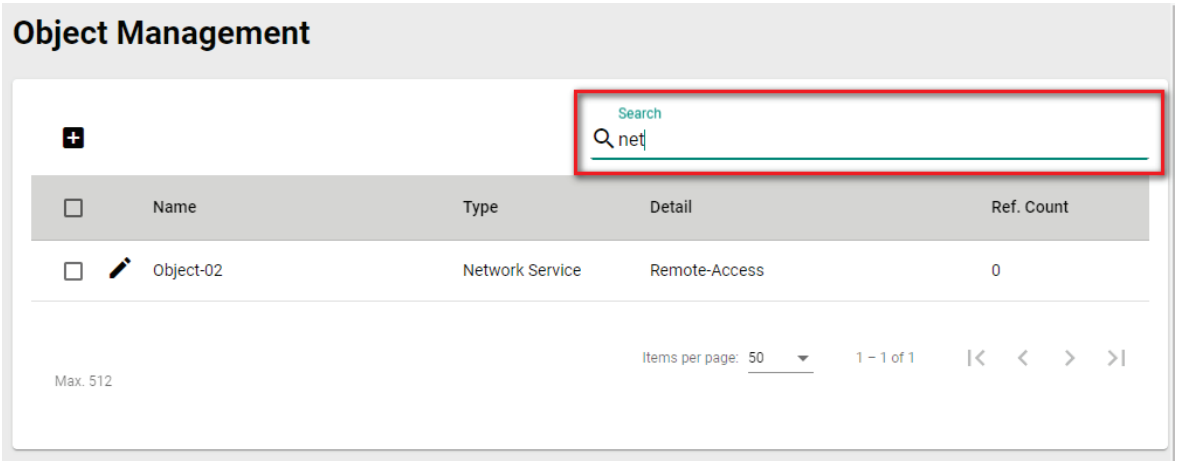
Delete an Object

Select the item(s) in the object list, click the **Delete** (🗑) icon. When prompted to confirm, click **DELETE** to delete the object(s).



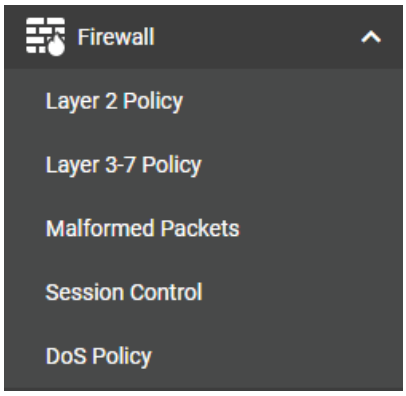
Search for an Object

Enter a search term in the Search field. Any object matching the search criteria will be shown in the object list.



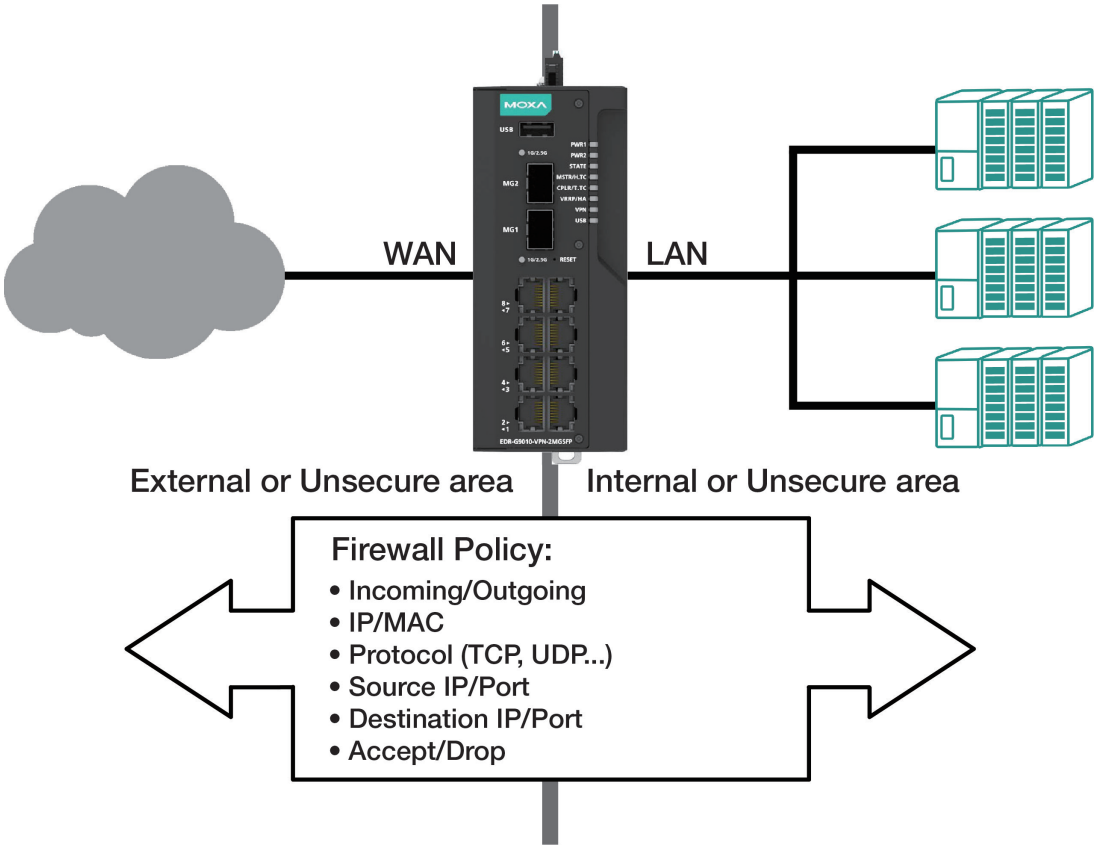
11. Firewall

From the **Firewall** section you can configure the **Layer 2 Policy**, **Layer 3-7 Policy**, **Malformed Packets**, **Session Control**, and **DoS Policy** settings.



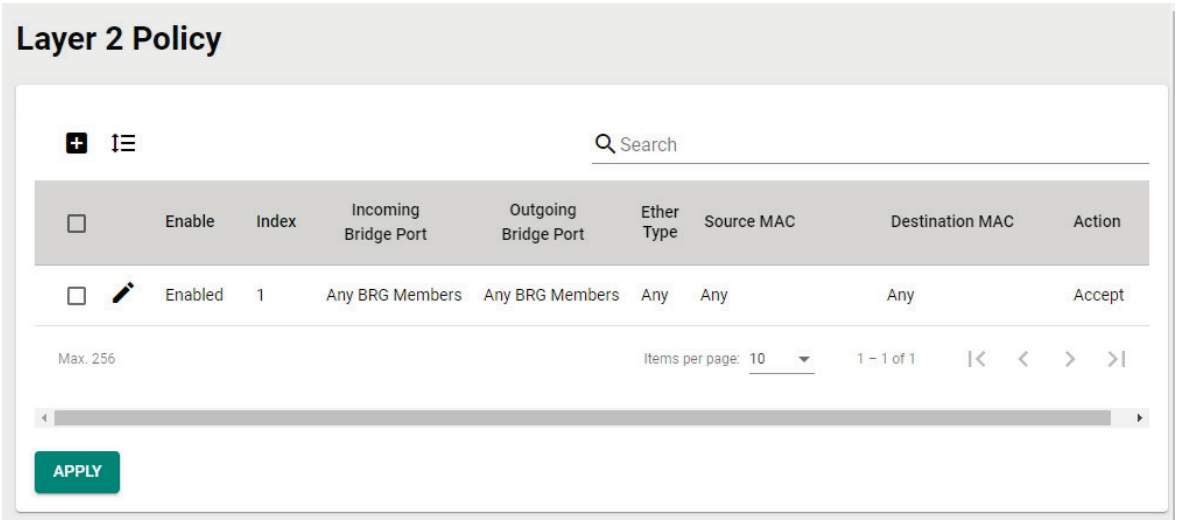
Policy Concept

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).



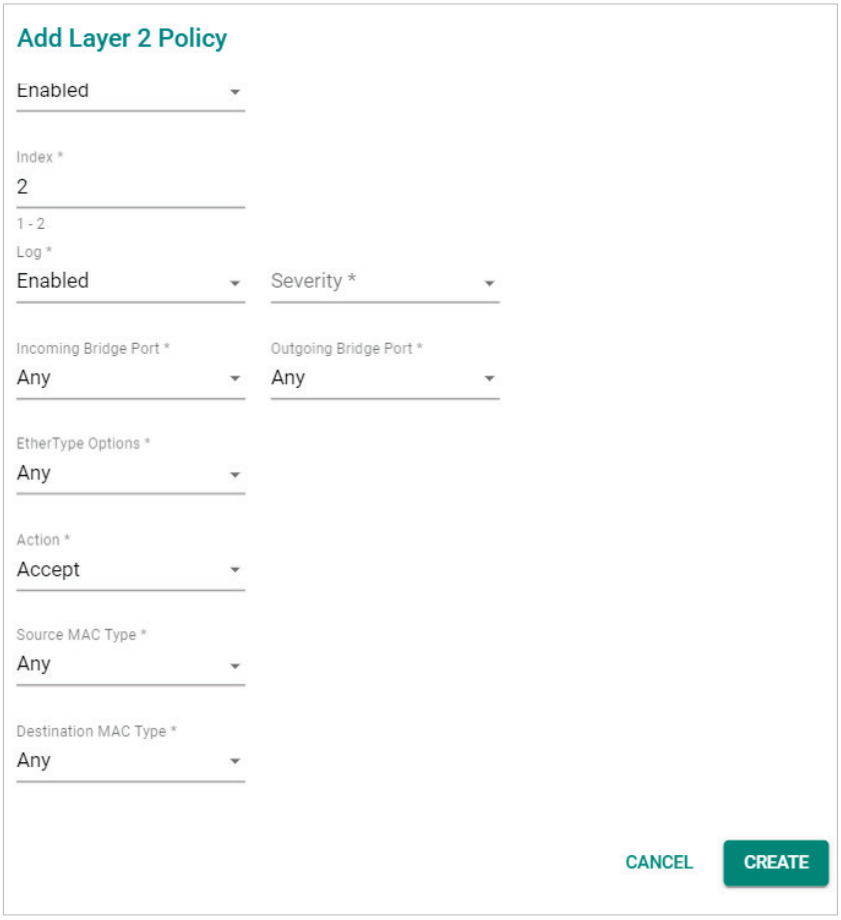
Layer 2 Policy

The Industrial Secure Router 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

Log

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable firewall event logging.	Enabled

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 log events.	None

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).

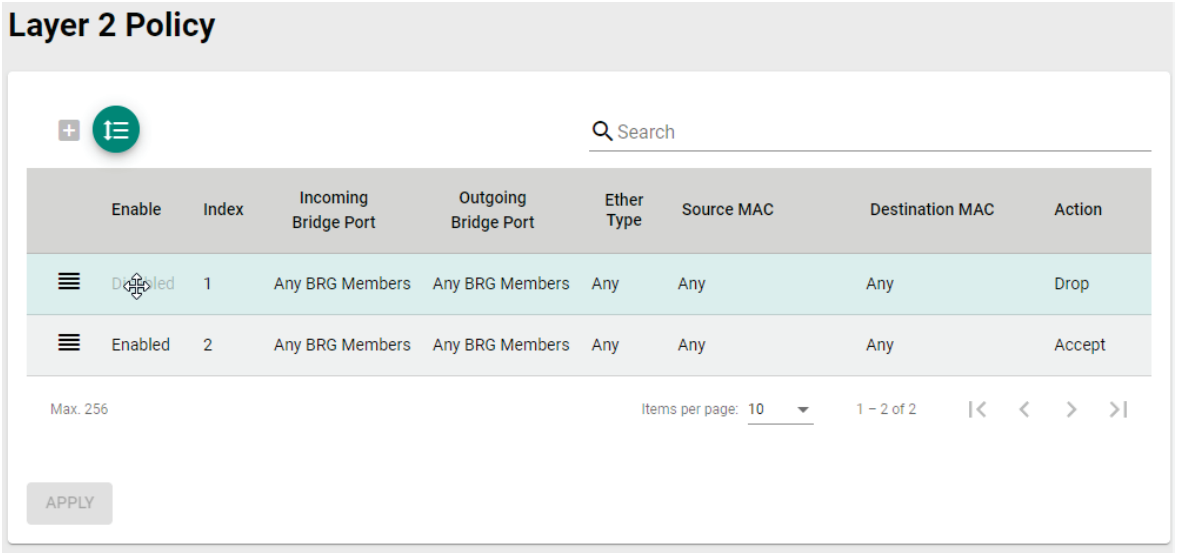
Search for a Existing Layer 2 Policy

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

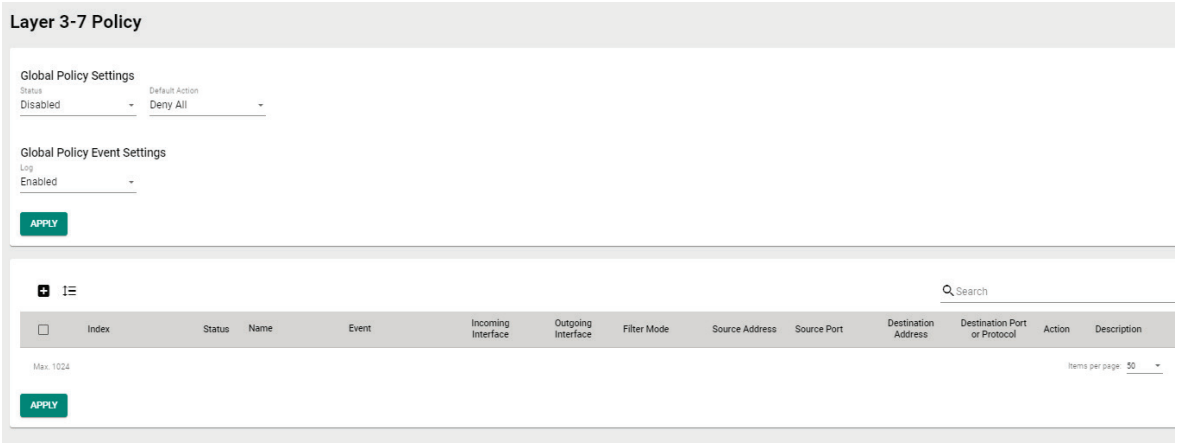
The following table shows the Layer 2 protocol types commonly used in Ethernet frames.

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)

Type	Layer 2 Protocol
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.

Status

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.	

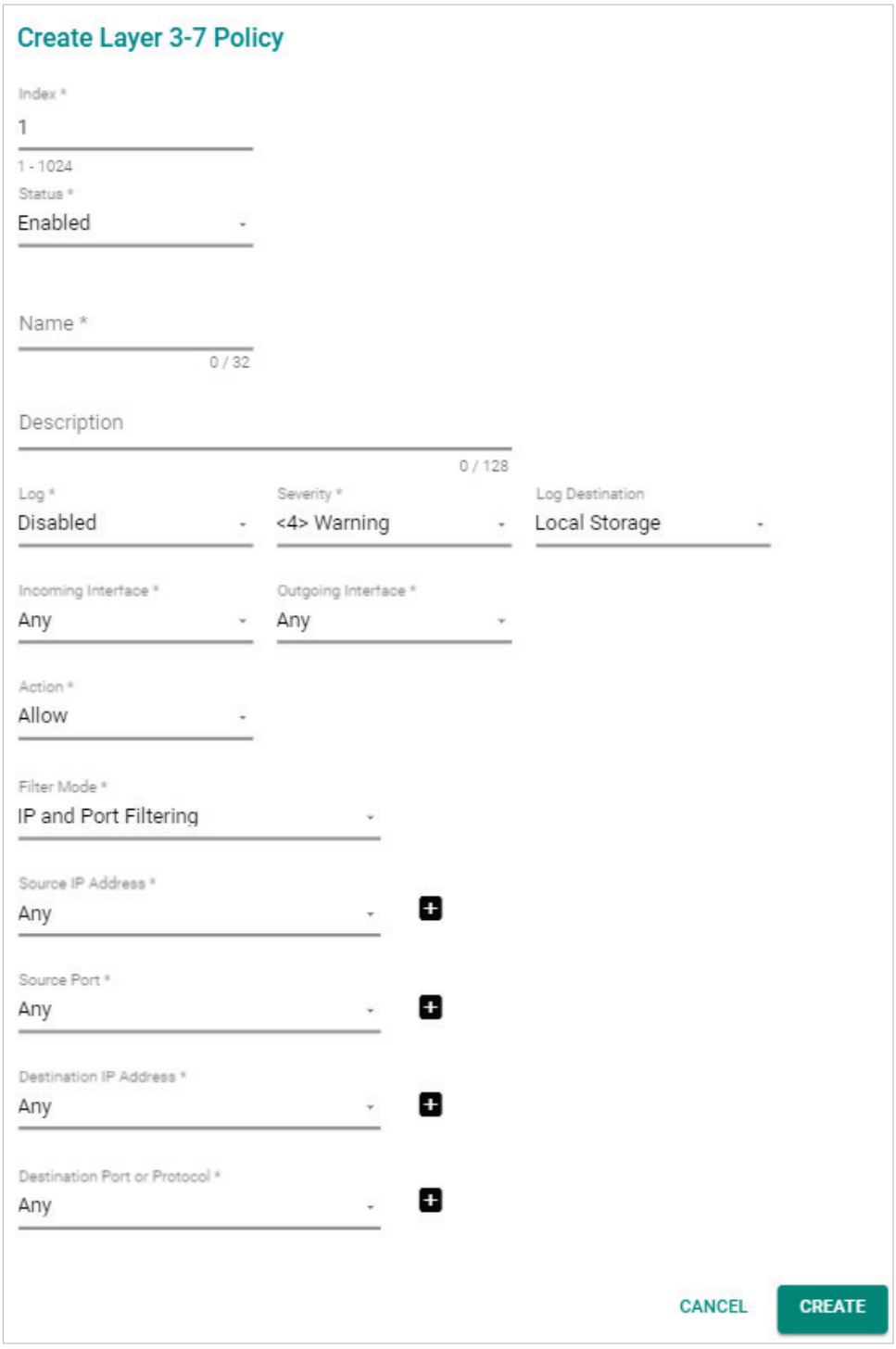
Policy Event Global Setting

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

Status

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 Industrial Secure Router 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.

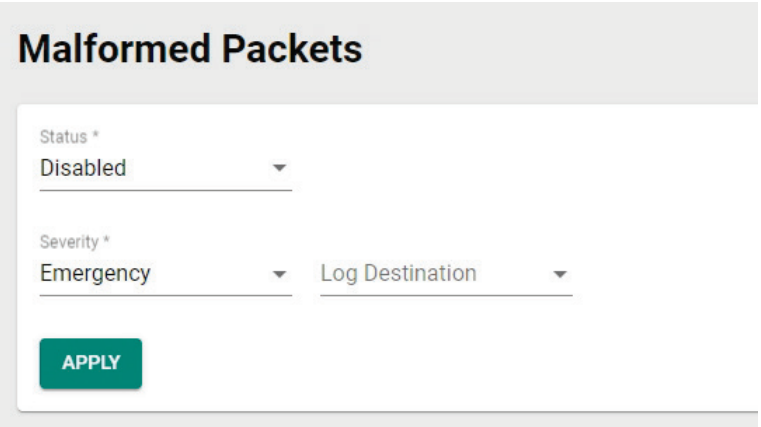
Reorder Existing Layer 3 – 7 Policy

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

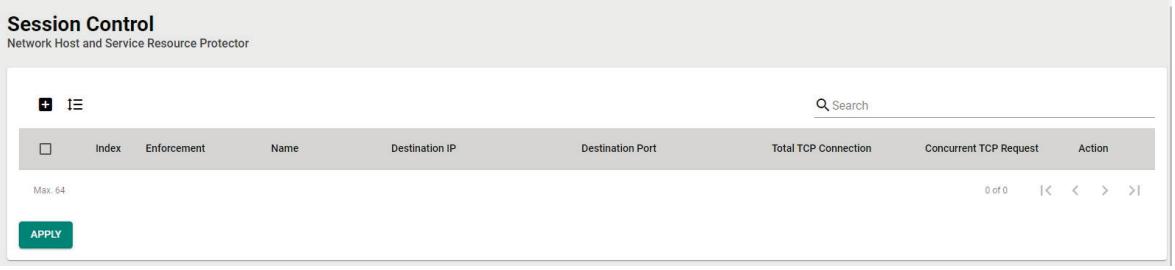
Setting	Description	Factory Default
Local Storage	The malformed packets event logs are stored in the local storage and will show in the Event Log table.	None
Syslog	The malformed packets event logs are sent to a Syslog server.	
Trap	The malformed packets event logs are sent by SNMP Trap.	

Session Control

The Industrial Secure Router supports session control to help users protect backend hosts or services and avoid system abnormalities.

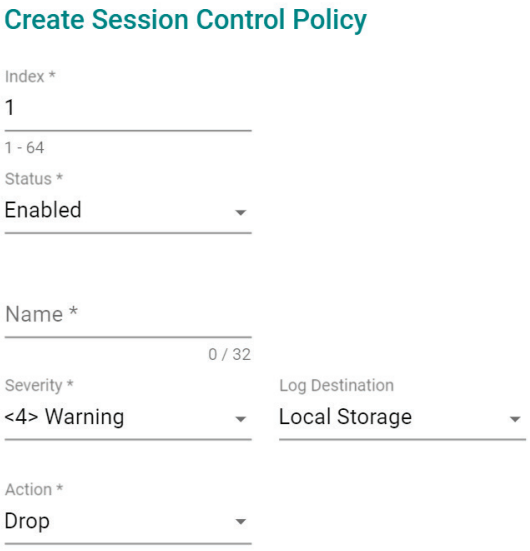
NOTE

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. 64	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

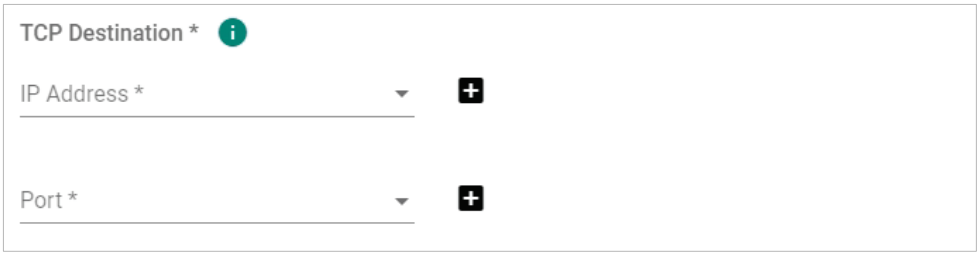
Log Destination

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.

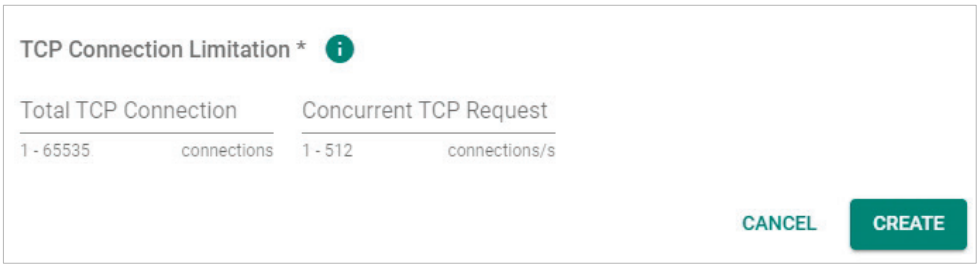
IP Address

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

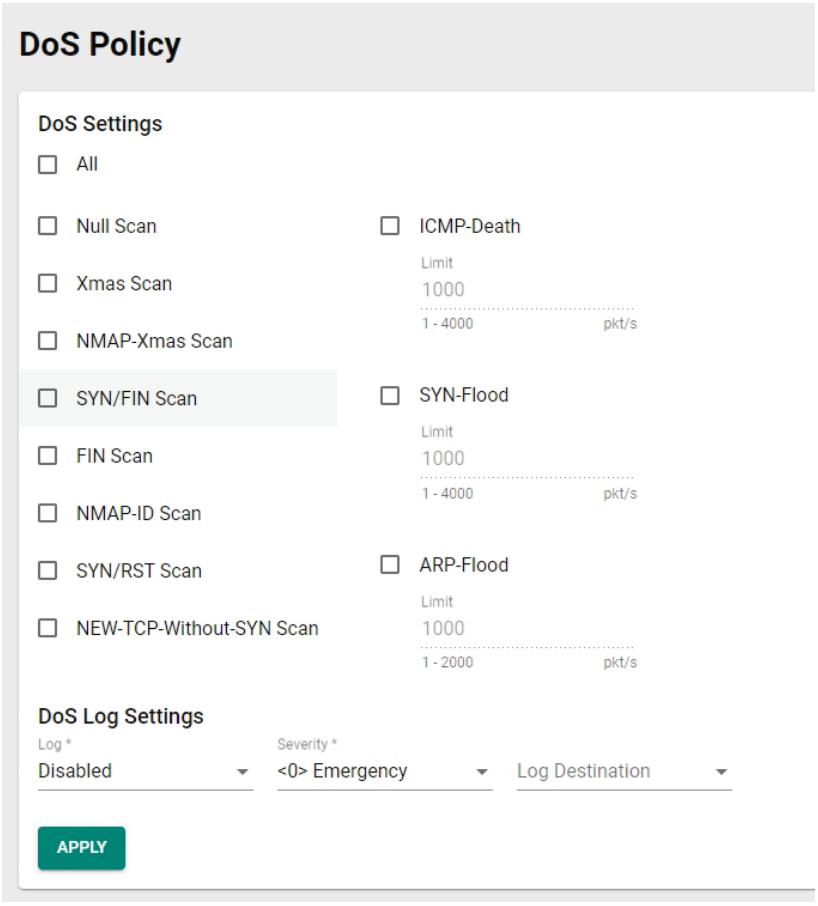
Enter the search term in the **Search** field. Anything matching the search criteria will be shown in the Session Control policy list table.

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.	Checked

Null Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable Null Scan.	Checked

Xmas Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable Xmas Scan.	Checked

NMAP-Xmas Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable NMAP-Xmas Scan.	Checked

SYN/FIN Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable SYN/FIN Scan.	Checked

FIN Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable FIN Scan.	Checked

NMAP-ID Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable NMAP-ID Scan.	Checked

SYN/RST Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable SYN/RST Scan.	Checked

NEW-TCP-Without-SYN Scan

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable NEW-TCP-Without-SYN Scan.	Checked

ICMP-Death

Setting	Description	Factory Default
Checked or Unchecked	Enable or disable the ICMP-Death protection.	Checked
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.	Checked
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	Checked
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.	

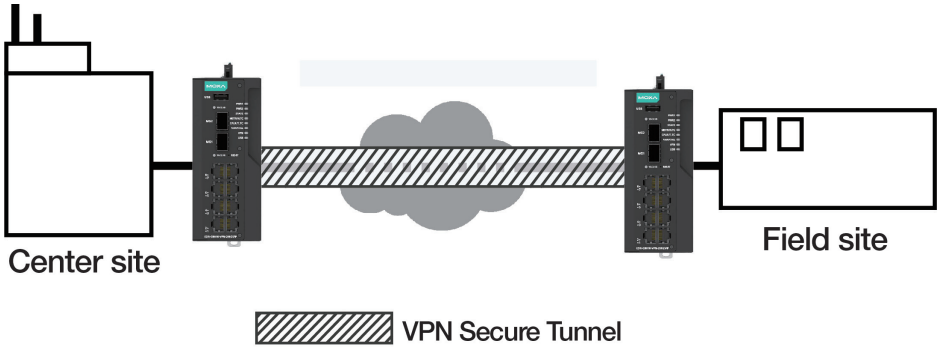
When finished, click **APPLY** to save your changes.

12. VPN (Virtual Private Network)

From the **VPN** section, you can configure **IPSec** 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.

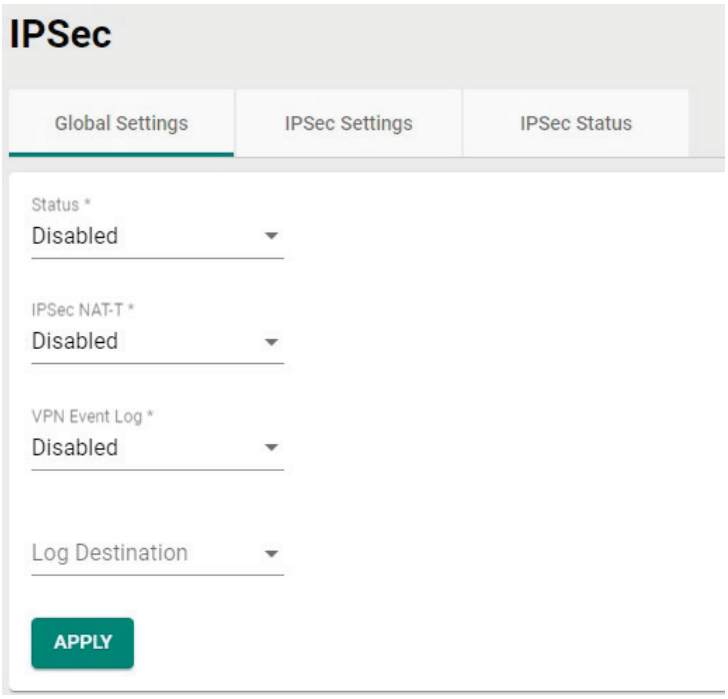
Data Exchange (IPsec Phase 2): In Phase 2, the VPN gateways negotiate to determine additional IPsec connection details, which include the data encryption algorithm.

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

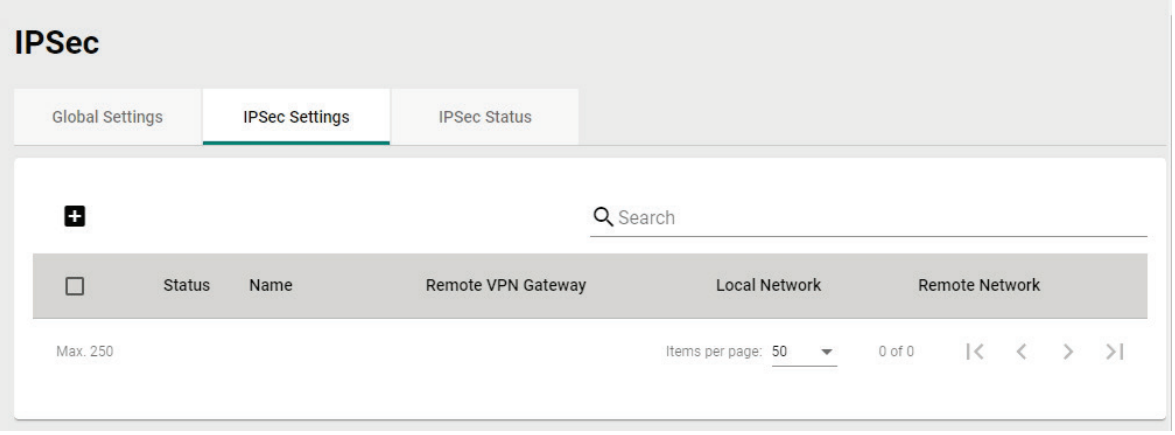
Severity

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

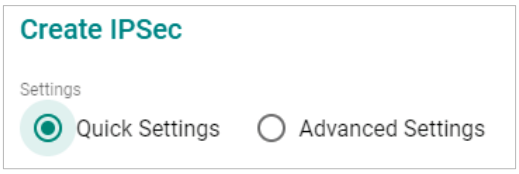


Create an IPsec Entry

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.

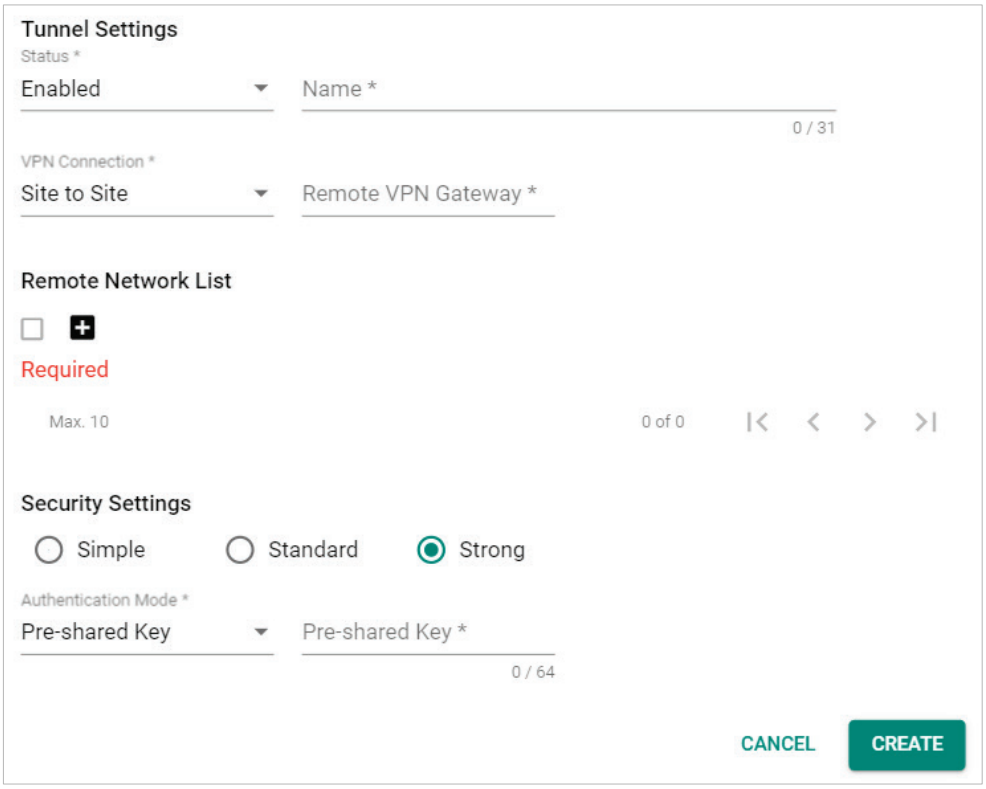


When choosing the Quick Settings mode, the user just needs to configure the following:

- 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

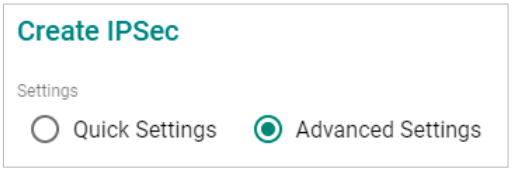


NOTE

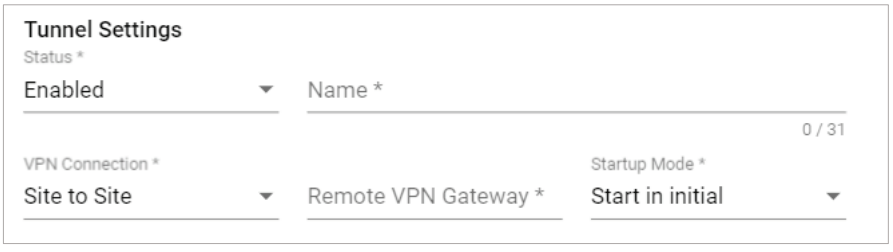
The Encryption Strength, Authentication Mode, and Pre-Shared Key configuration should be identical for both Industrial Secure Router units.

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. 31 characters	Enter a name for this VPN tunnel.	None

NOTE

The name cannot start with a number.

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

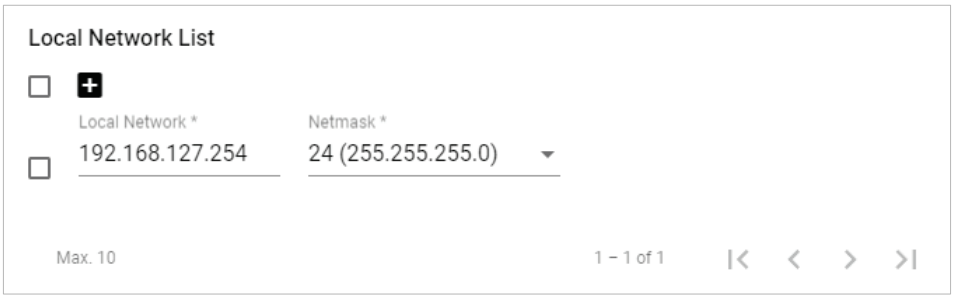
Startup Mode

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

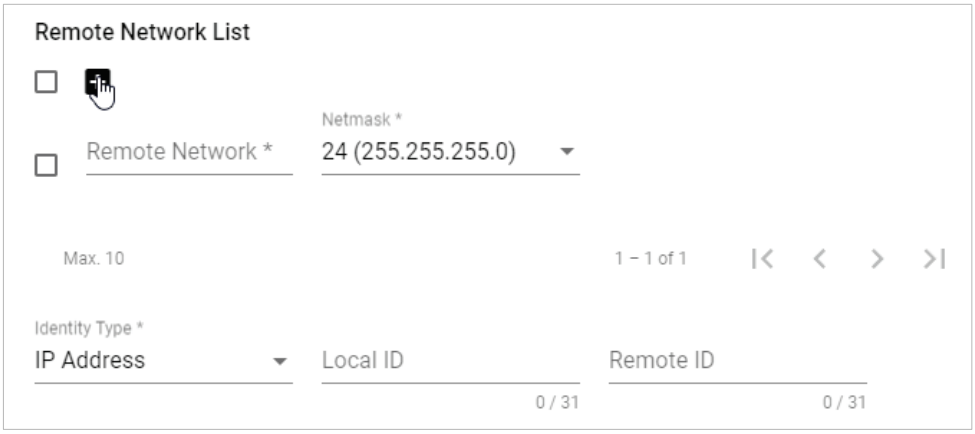


Local Network/Netmask

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.



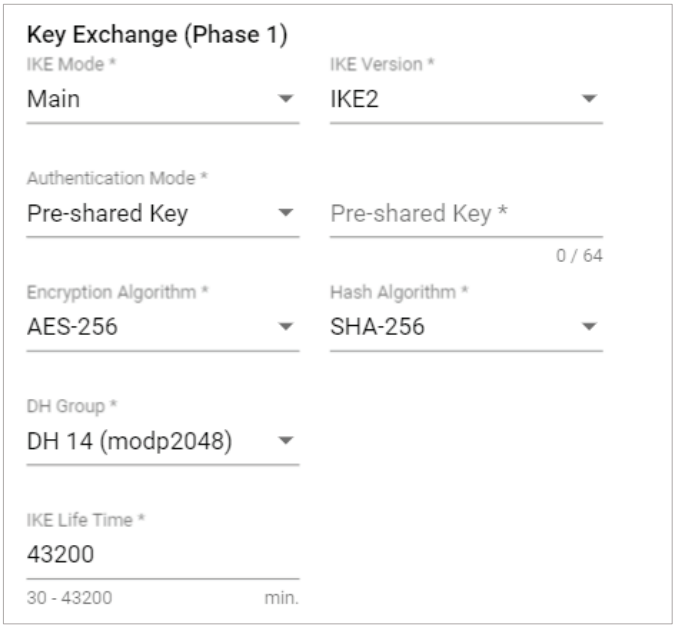
Remote Network/Netmask

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.	None
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.	None

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

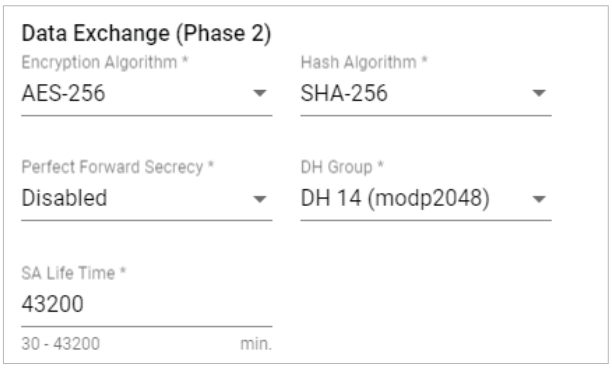
DH Group

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)

SA 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

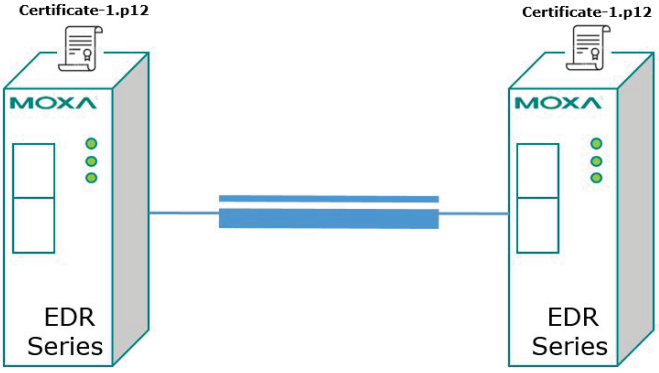
In the following section, we will consider five common user scenarios. The purpose of each example is to give a clearer understanding of two authentication modes 'X.509' and 'X.509 with CA'.

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)

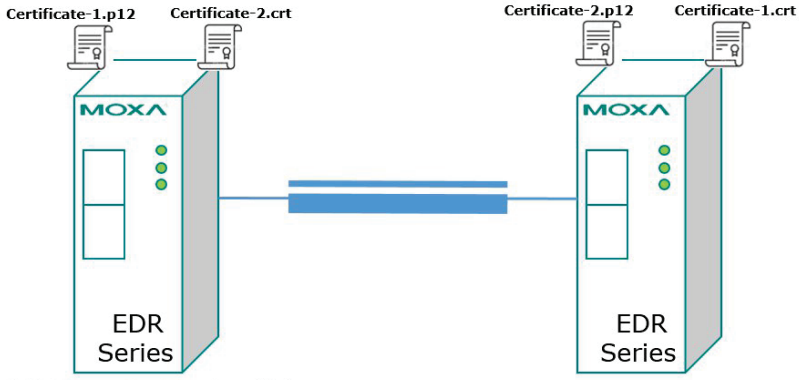
1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Enter "IPSec setting", and in "Advanced Setting", select X.509 authentication mode.
3. In "Local", select No.1
4. In "Remote", select No.1

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)

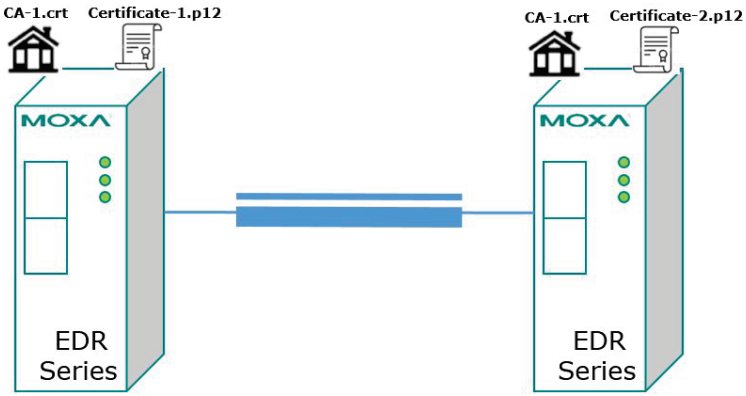
1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Import **Certificate-2.crt** file or **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.
3. Enter "IPSec setting", and in "Advanced 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)

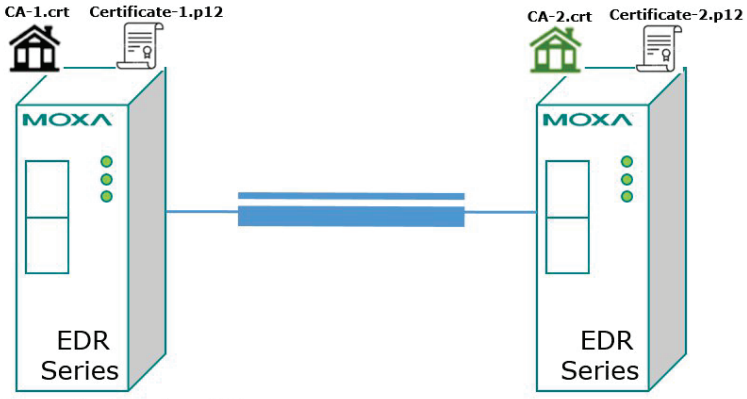
1. Import **Certificate-1.p12** file in "Local Certificate", and label it a number. Here take No.1 as an example.
2. Import **CA-1.crt** file in "Trusted CA Certificate".
3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.
4. In "Local", select No.1

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)

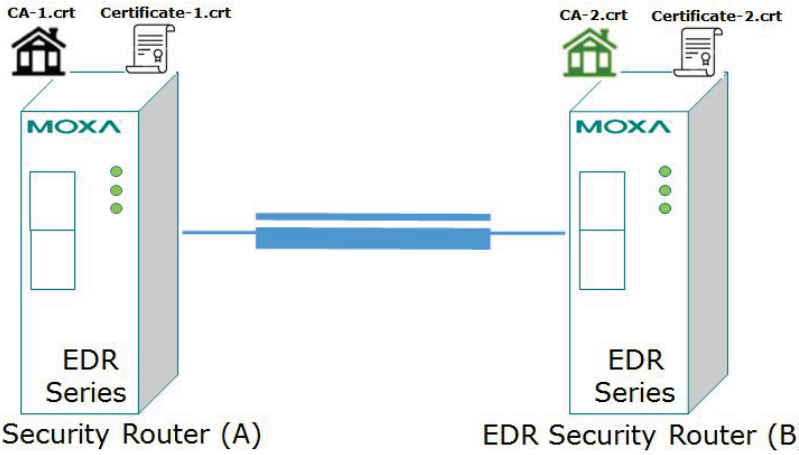
1. Import **Certificate-2.p12** file in "Local Certificate", and label it a number. Here take No.2 as an example.
2. **Import CA-1.crt file and CA-2.crt file** in "Trusted CA Certificate".
3. Enter "IPSec setting", and in "Advanced Setting", select X.509 With CA authentication mode.
4. In "Local", select 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

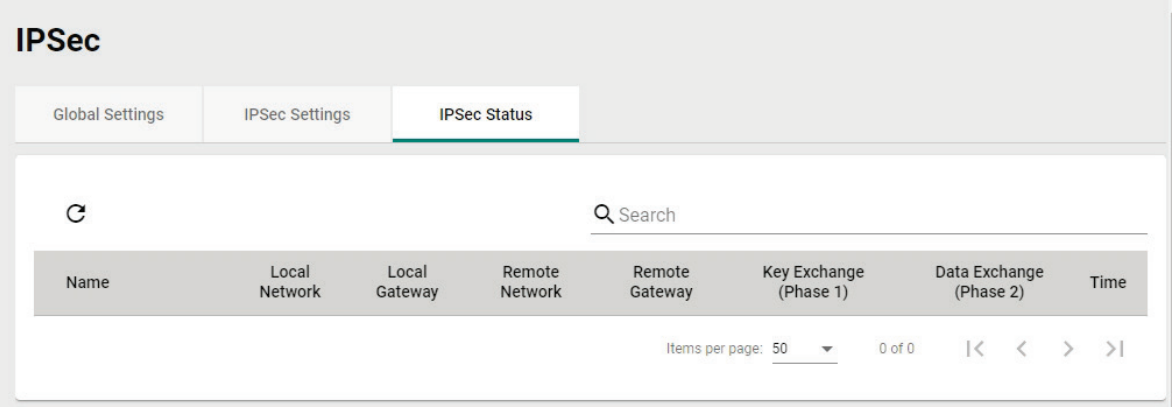
EDR Security Router (B)

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.

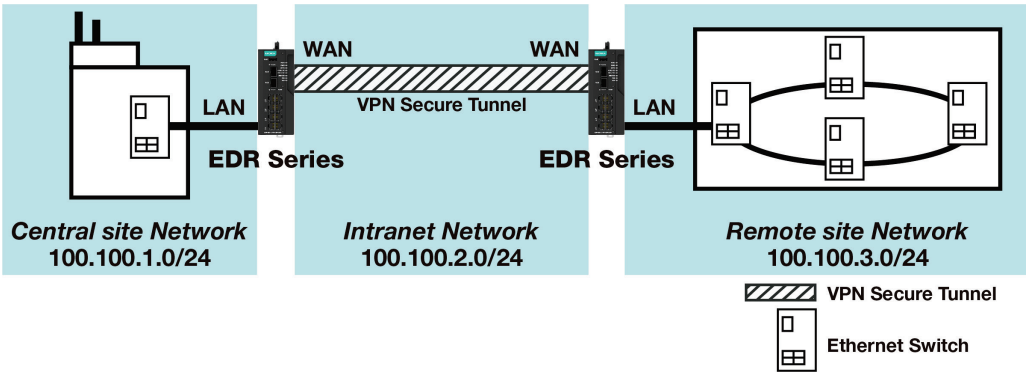


Click the icon to refresh the information.

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.

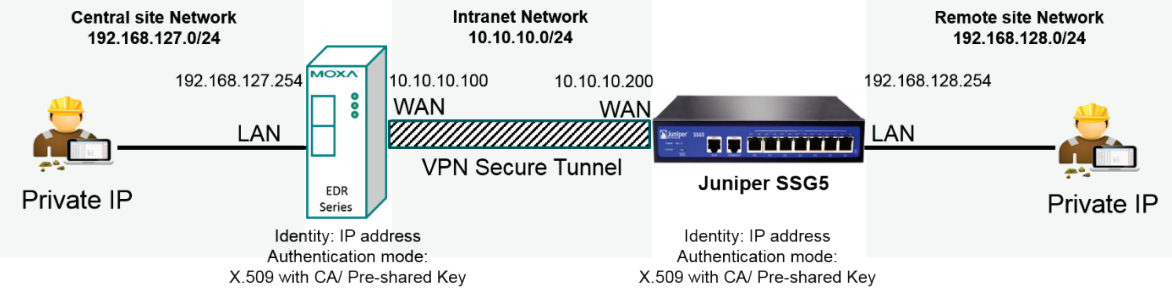
	Configuration	Industrial Secure Router (1)	Industrial Secure Router (2)
Interface Setting	WAN IP	100.100.2.1	100.100.2.2
	LAN IP	100.100.1.1	100.100.3.1

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	Industrial Secure Router	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	Industrial Secure Router	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

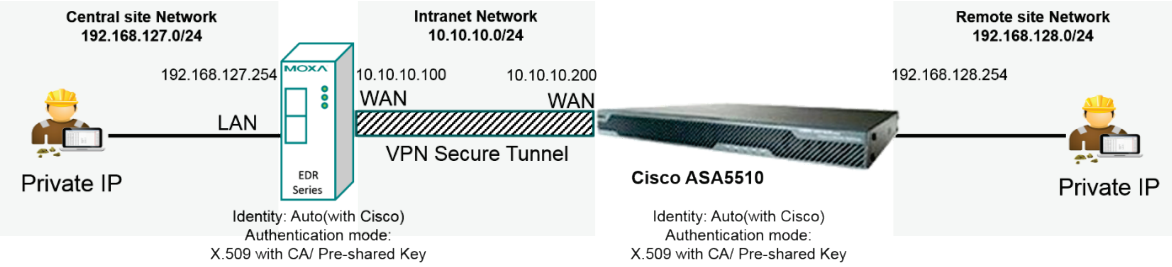
Note that to establish a VPN connection with Juniper systems, the Identity should set to "**IP Address**" and the authentication mode should set to "**Pre-Shared Key**" or "**X.509 with CA**". During the Industrial Secure Router compliance test with the Juniper SSG5, all Identity modes except "IP Address" 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.

Industrial Secure Router 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	Moxa Industrial Secure Router	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	Moxa Industrial Secure Router	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.

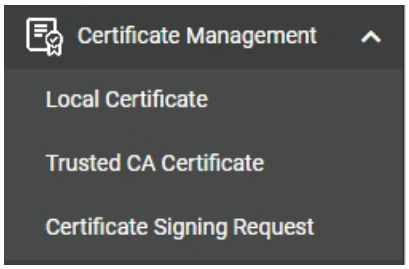
Industrial Secure Router VPN Settings for compatibility with Cisco systems		Authentication mode		
		Pre-shared Key	X.509	X.509 With CA
Identity	IP Address	Supported	Not supported	Not supported
	FQDN	Supported		
	Key ID	Supported		
	Auto(with Cisco)	Supported		Supported

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.



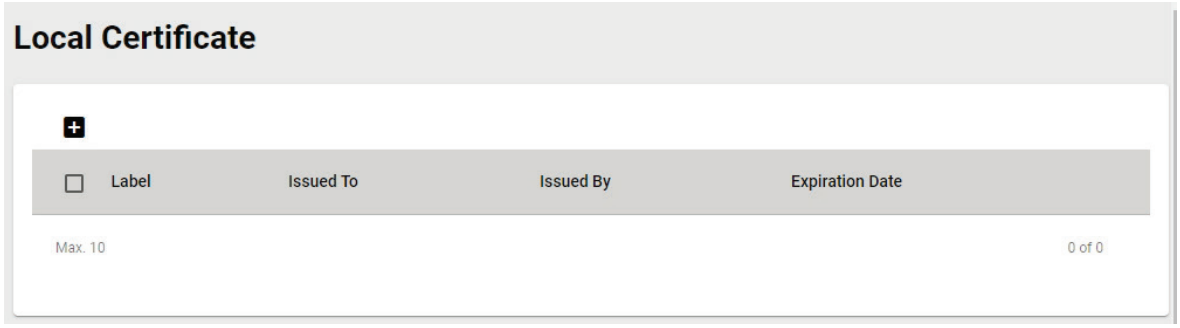
NOTE

For security reasons, if the device is deployed without a CA server environment, we strongly recommend using short lifetime certificates (e.g., 24 hours) to ensure system security.

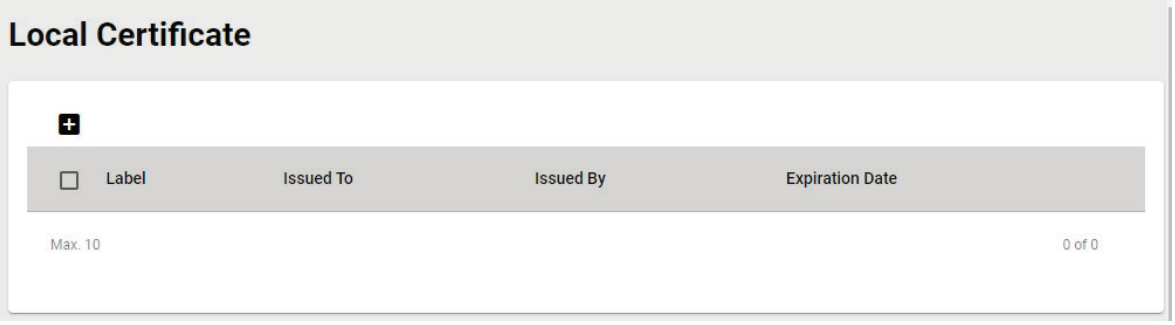
Local Certificate

From the **Local Certificates** screen, users can import certificates issued by the CA into the Industrial Secure Router.

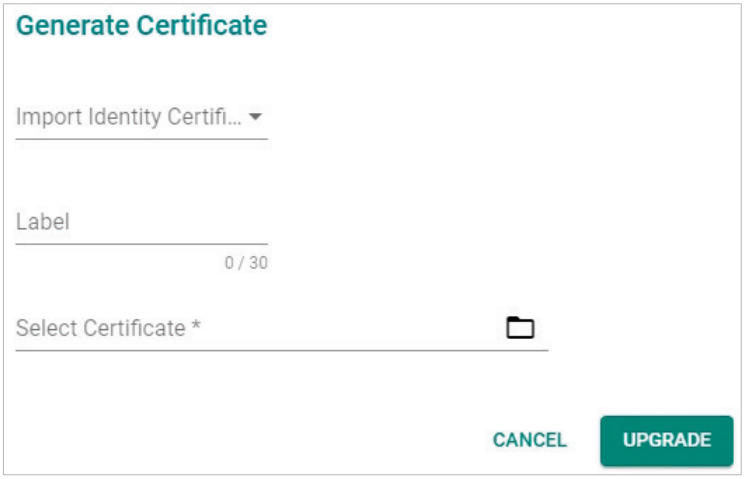
Depending on the selected certificate, some settings may differ. Refer to the following sections:
Import a Certificate
Import a Certificate From CSR
Import a Certificate from PKCS#12



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

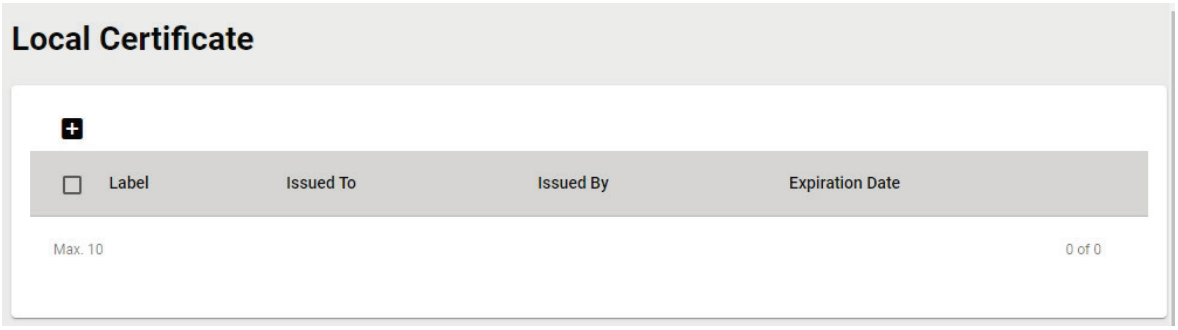
Select Certificate

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

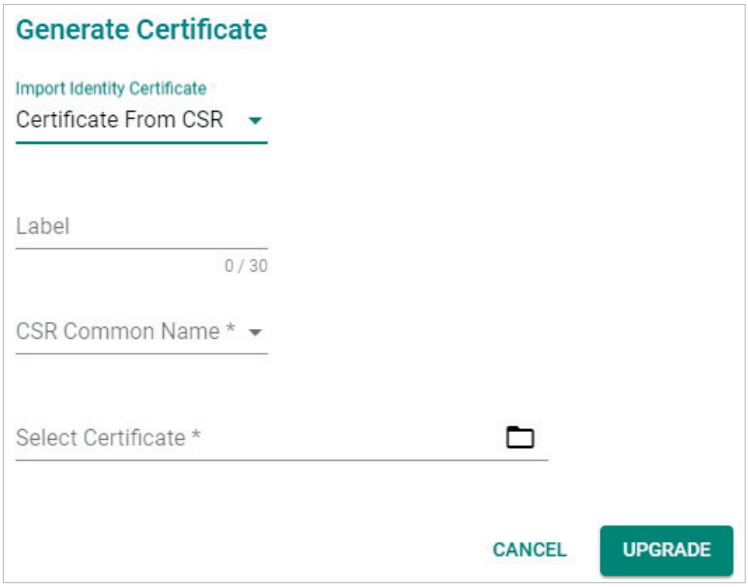
When finished, click **UPGRADE** to import the selected certificate.

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

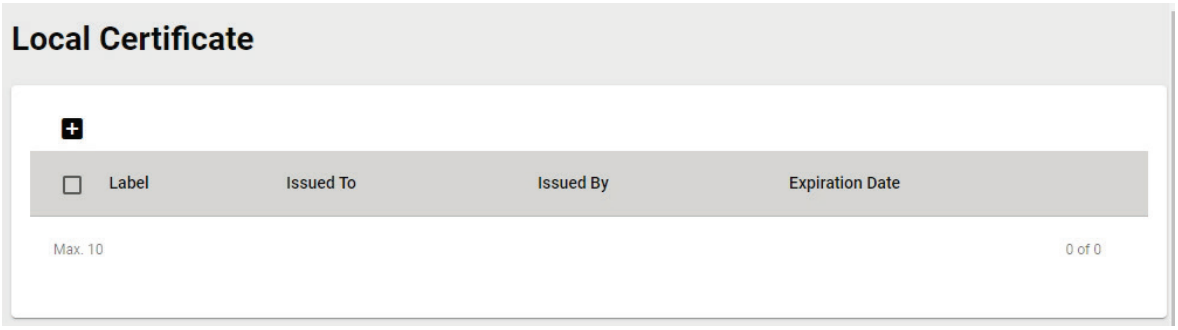
Select Certificate

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

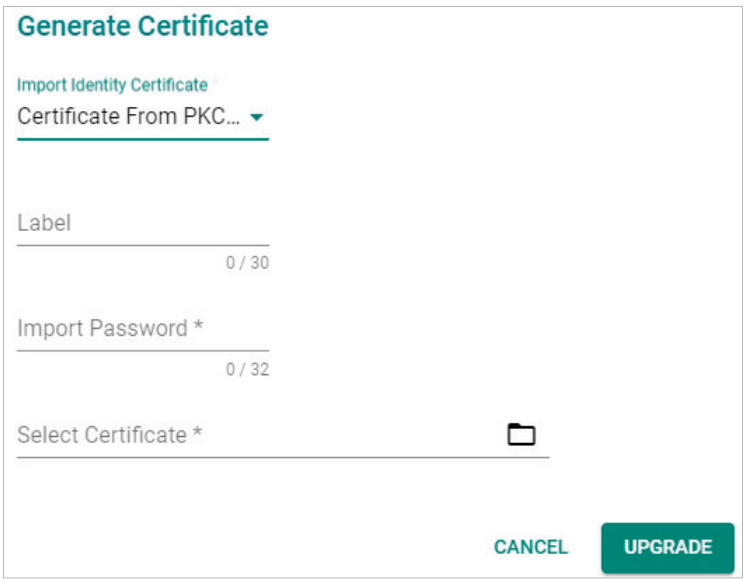
When finished, click **UPGRADE** to import the selected certificate.

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

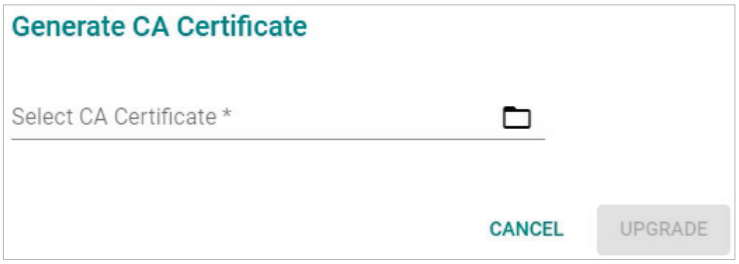
When finished, click **UPGRADE** to import the selected certificate.

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.

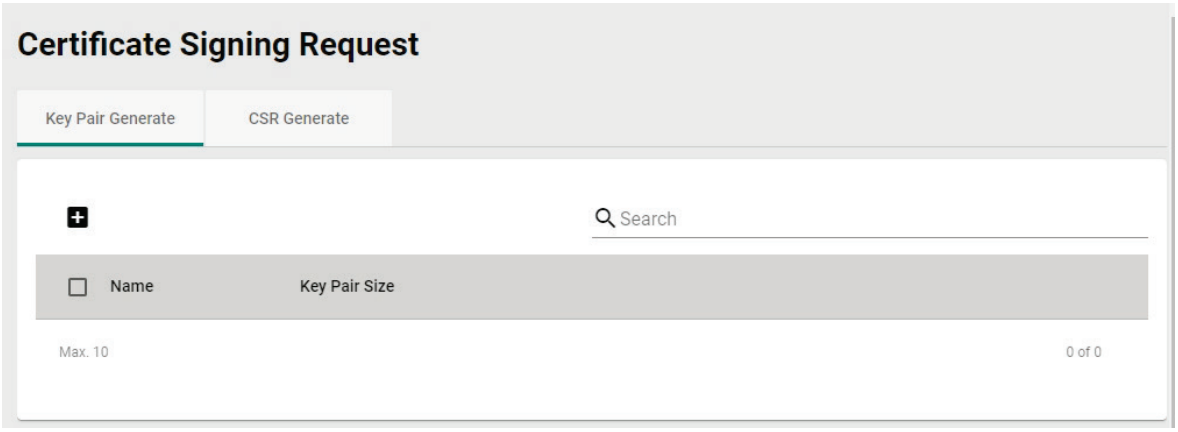
Click the icon to add a CA Certificate.



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.

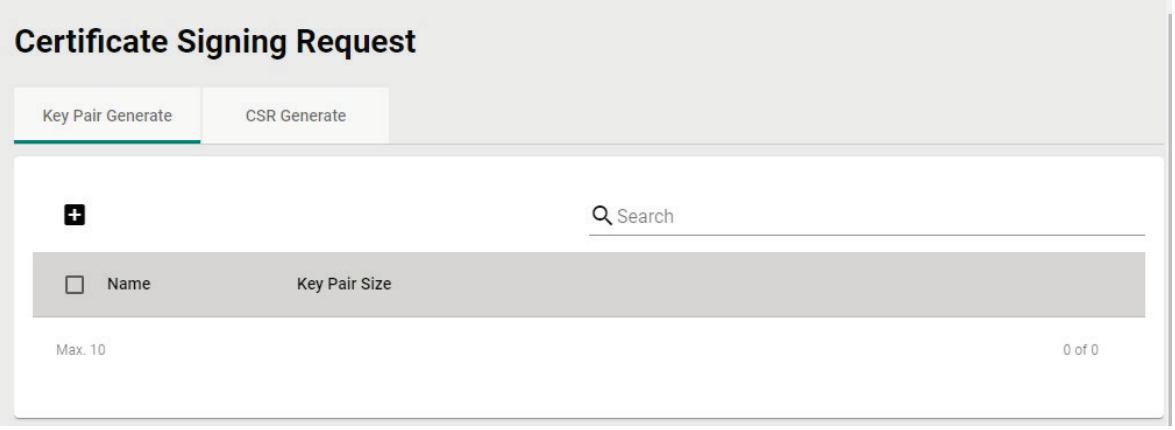
Step 1: Generate a Private Key

Step 2: Generate the CSR

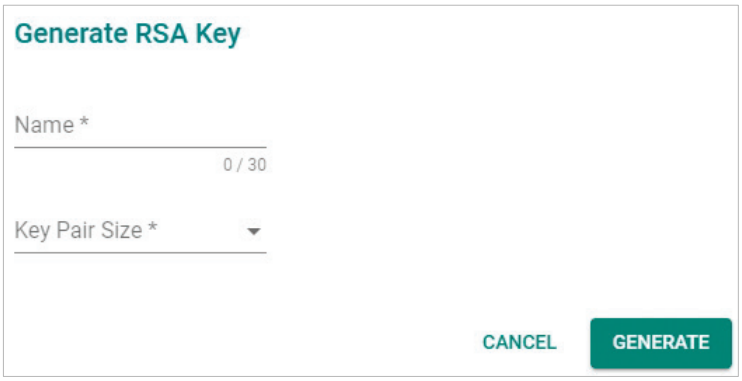
Key Pair Generate

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

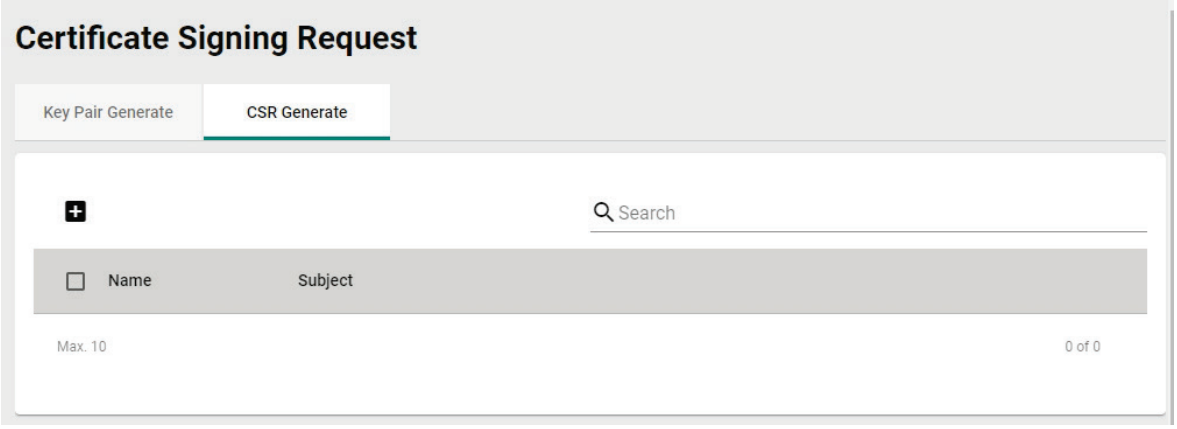
Setting	Description	Factory Default
1024 Bit or 2048 Bit	Select the key pair size of each private key.	None

When finished, click **GENERATE** to generate the RSA key.

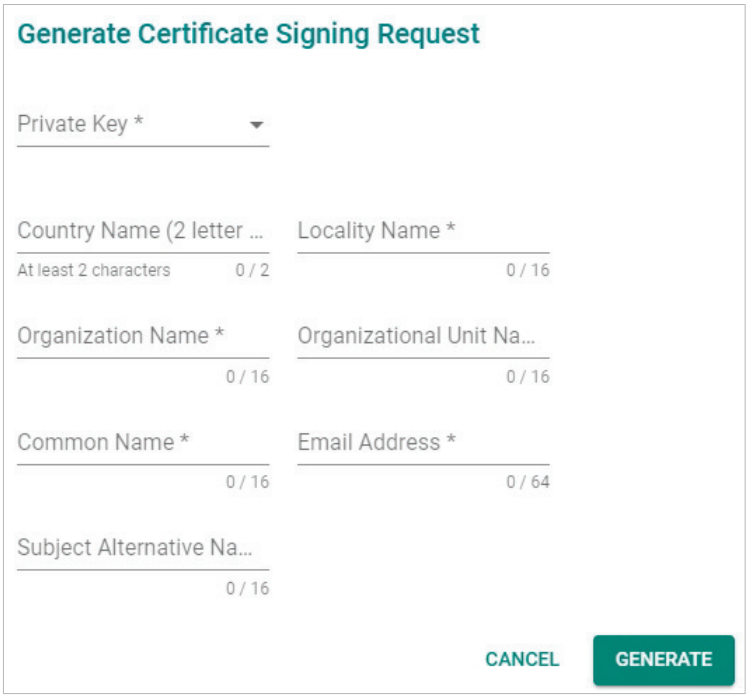
To delete the RSA key, select the RSA key in the RSA key List and click the 🗑 icon, then click **DELETE** to delete the RSA key.

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

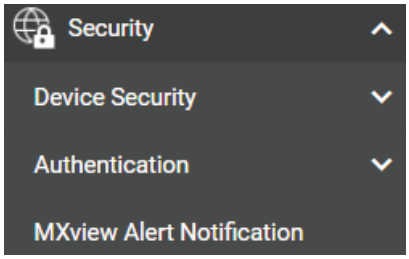
When finished, click **GENERATE** to generate the CSR.

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.

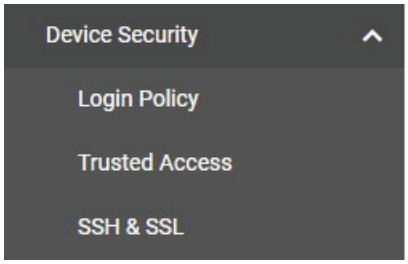
14. Security

From the **Security** section, you can configure **Device Security**, **Authentication**, and **MXview Alert Notification** settings.

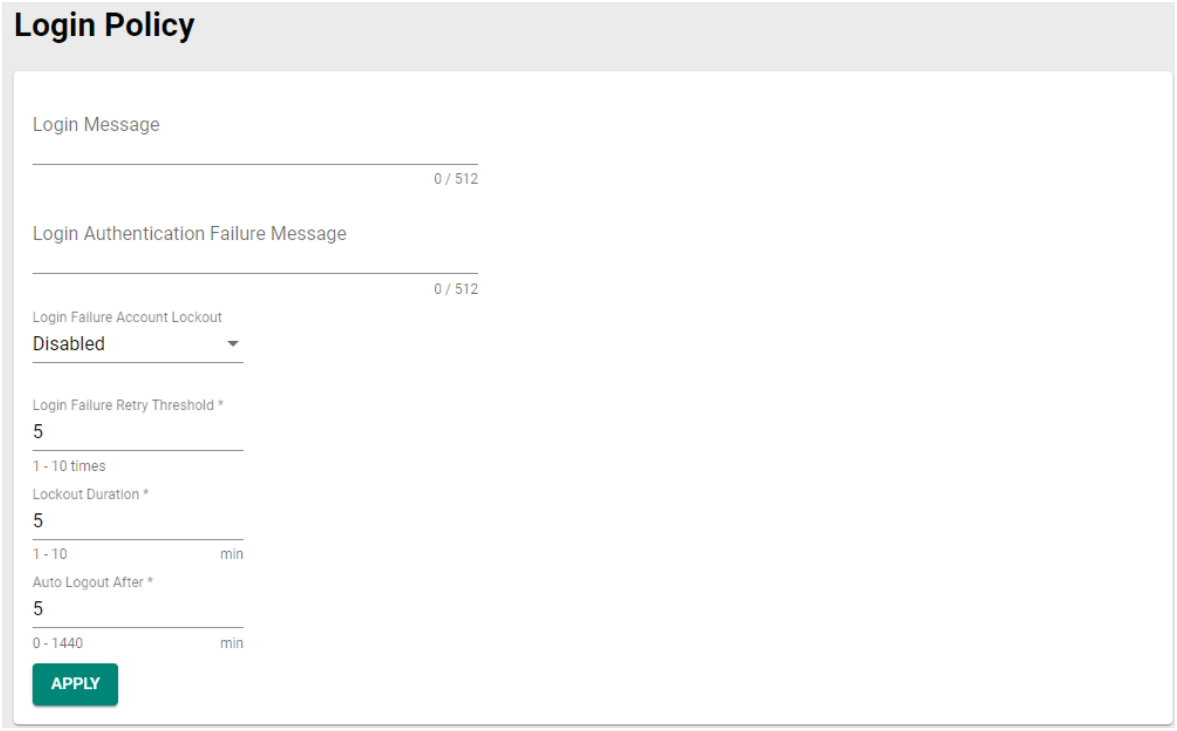


Device Security

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

Note

The Login Authentication Failure Message should not include any password or other sensitive information.

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

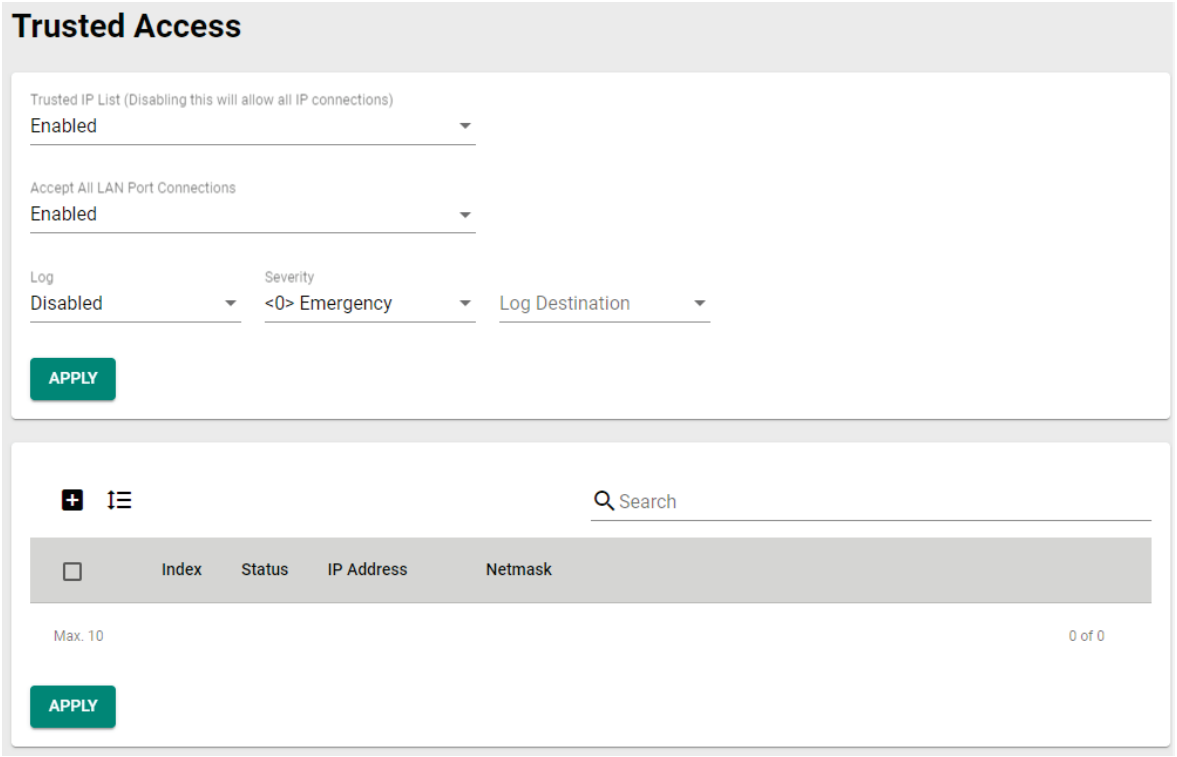
Auto Logout After

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.	0

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

Trusted Access

The Industrial Secure Router 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
Emergency Alert Critical Error Warning Notice Informational Debug	Select the severity of the Trusted Access event.	Emergency

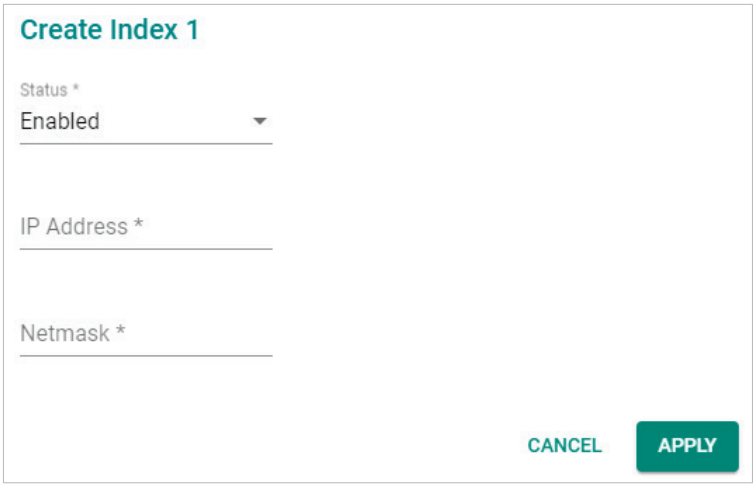
Log Destination

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.

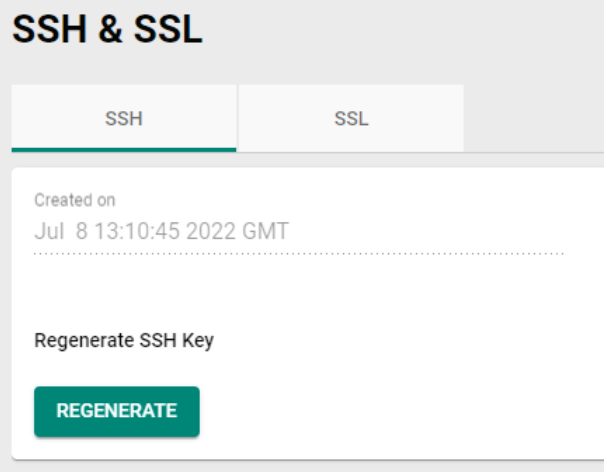
Delete a Trusted Access Entry

Select the entry from the Trusted Access List and click the 🗑 icon, then click **DELETE** to delete it.

SSH & SSL

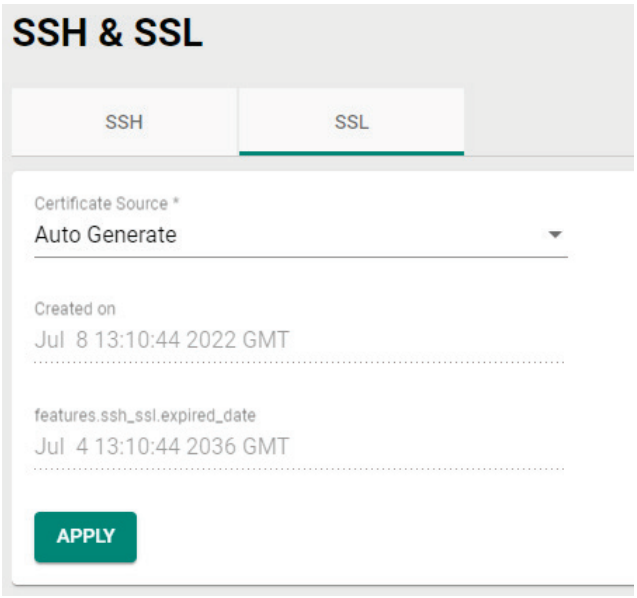
SSH

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.



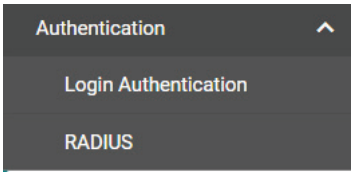
Certificate Source

Setting	Description	Factory Default
Auto Generate	The Industrial Secure Router will generate a certificate automatically.	Auto Generate
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".	

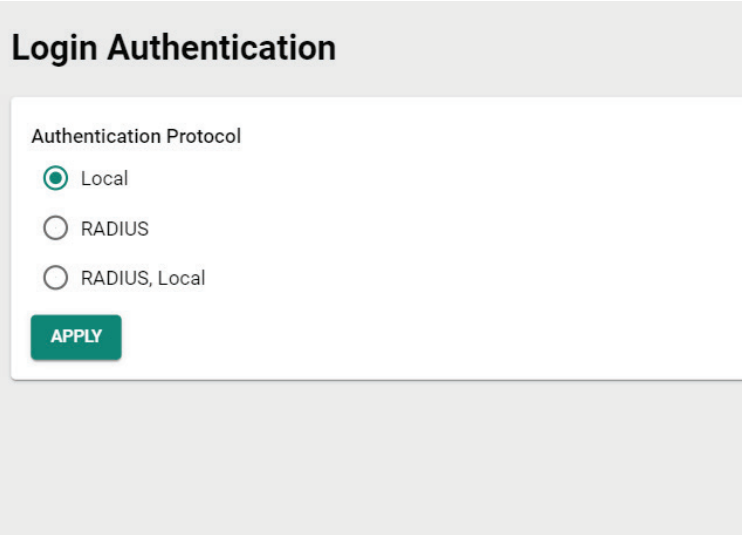
When finished, click **APPLY** to save your changes.

Authentication

From the **Authentication** section, the following functions can be configured: **Login Authentication** and **RADIUS**.



Login Authentication



Authentical Protocol

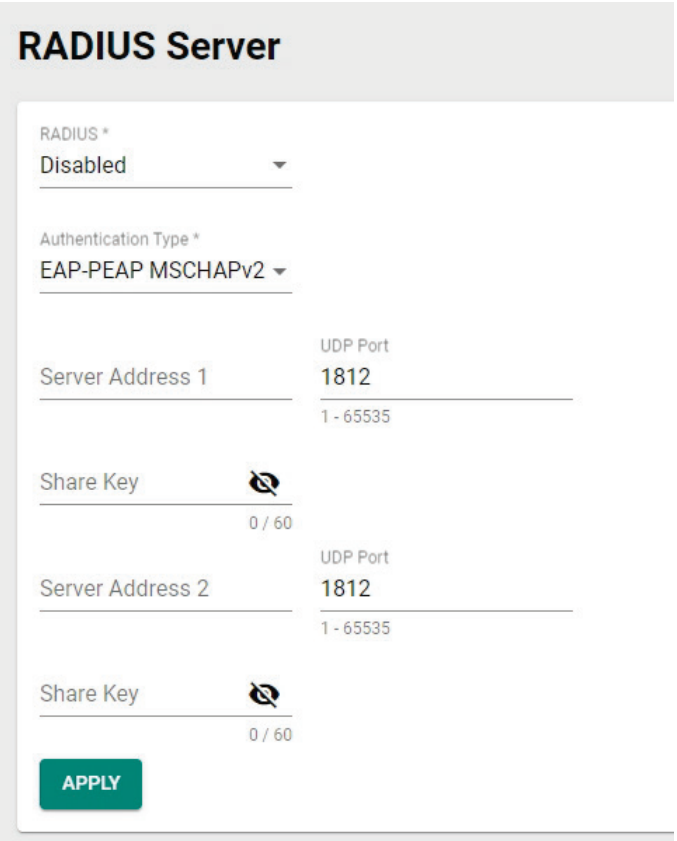
Setting	Description	Factory Default
Local RADIUS RADIUS, Local	Select the login authentication protocol for the device.	Local

RADIUS

Users can set up two RADIUS servers, one primary and one secondary backup server. When the primary RADIUS server becomes unavailable, the Industrial Secure Router will switch to the backup RADIUS server.

Note

For security reasons, it is recommended for administrators to periodically change the RADIUS server password.



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

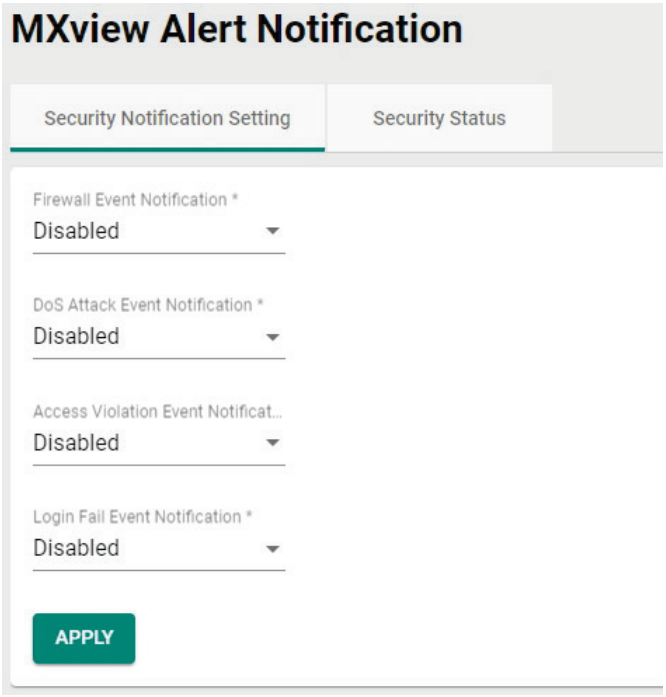
Setting	Description	Factory Default
Server Address 1/2 (0 to 64)	Specify the first and second RADIUS authentication server IP address or server name.	None
UDP Port (1 to 65535)	Specify the first and second RADIUS server port number.	1812
Shared key (max. 60 characters)	Specify the shared key for the 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 Industrial Secure Router 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

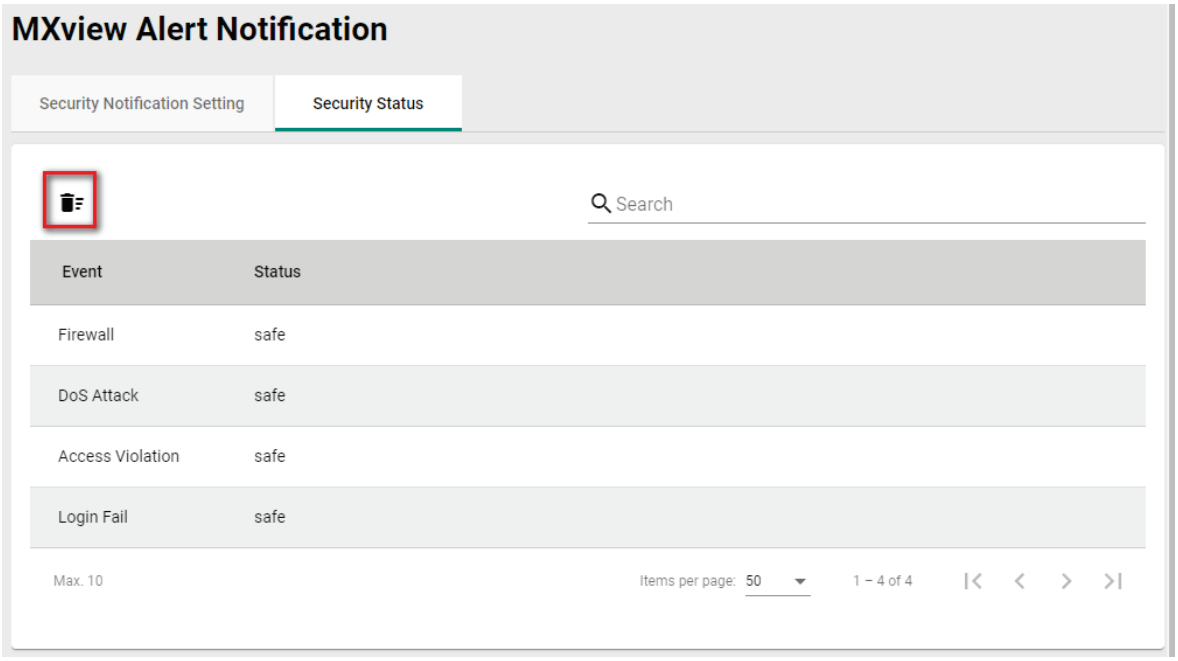
Login Fail Event Notification

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.

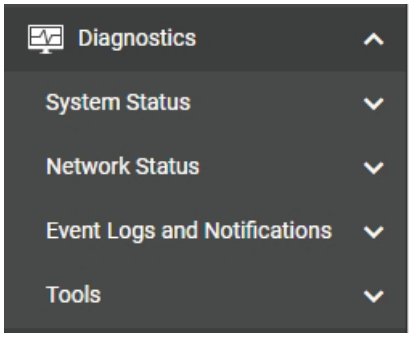


15. Diagnostics

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.

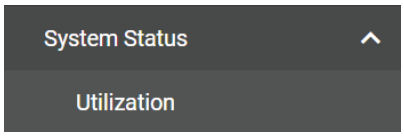
From the **Diagnostics** section, you can configure the **System Status, Network Status, Event Logs and Notifications,** and **Tools** configurations.



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.

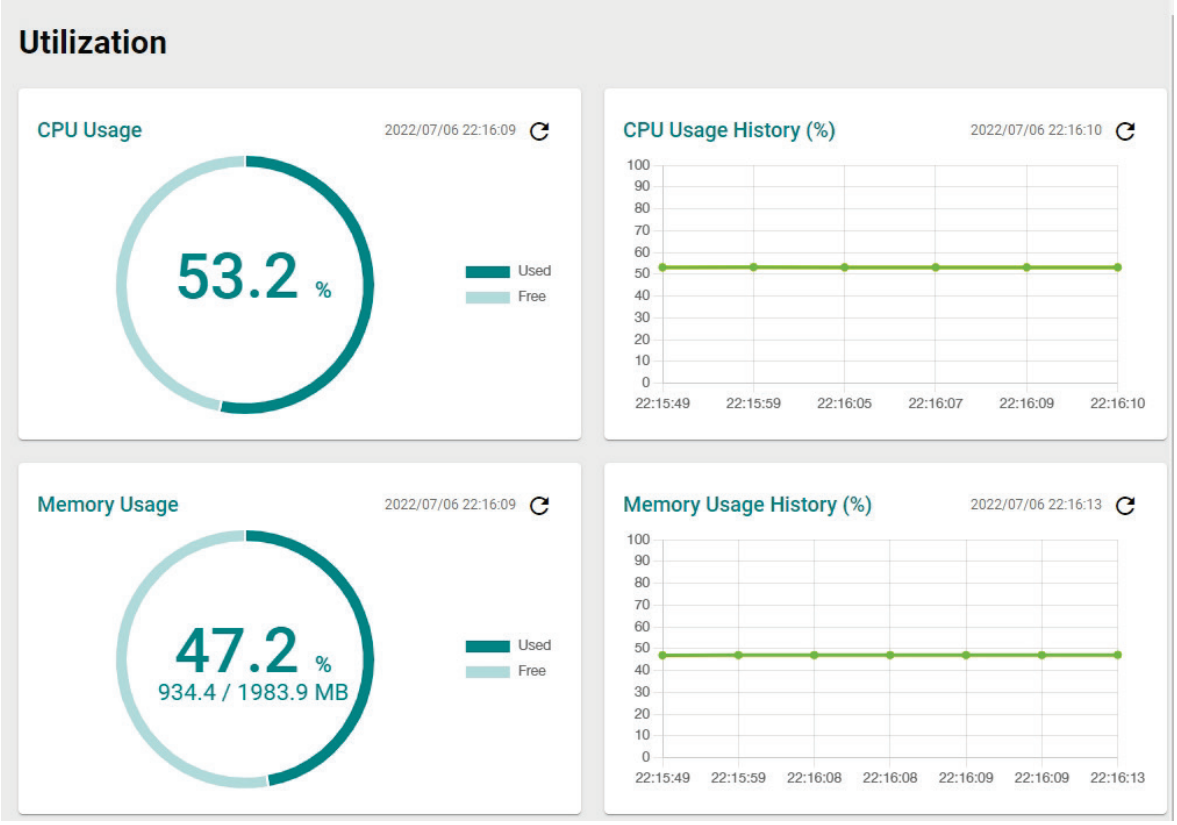
From the **System Status** section, the following functions can be configured: **Utilization**.



Utilization

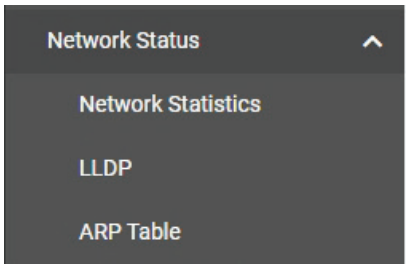
On the **Utilization** page, you can view the system resource utilization history, including the current and historical CPU and memory usage.

Click the icon on the upper-right corner of each graph to refresh the data.



Network Status

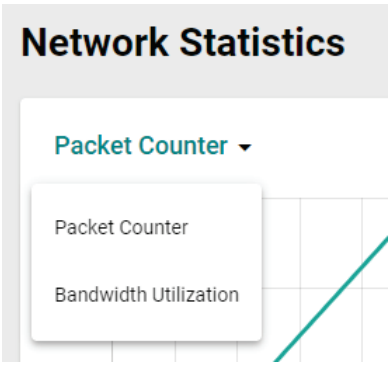
From the **Network Status** section, the following functions can be configured: **Network Statistics, LLDP,** and **ARP Table**.



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.

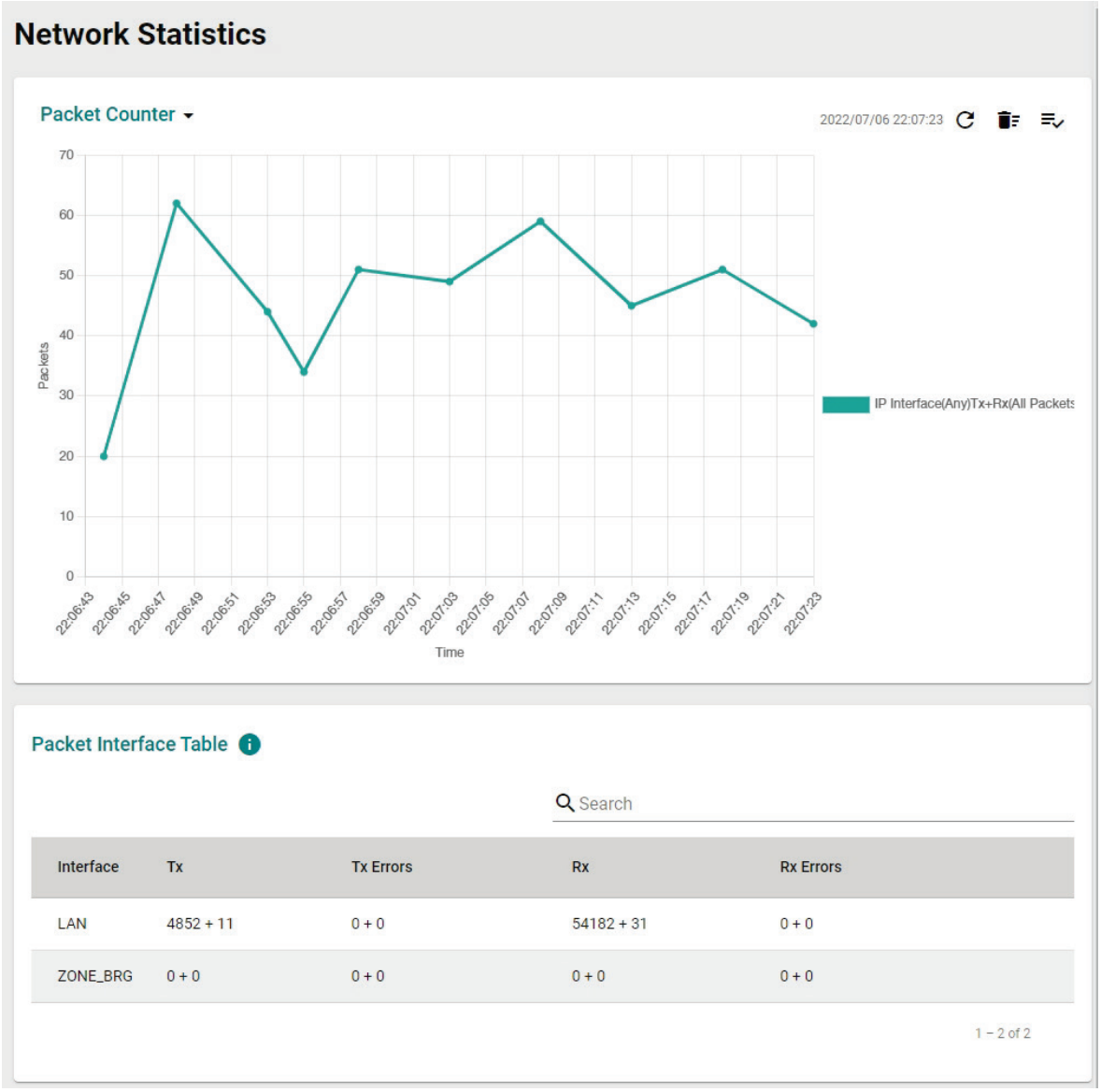


Display Mode

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

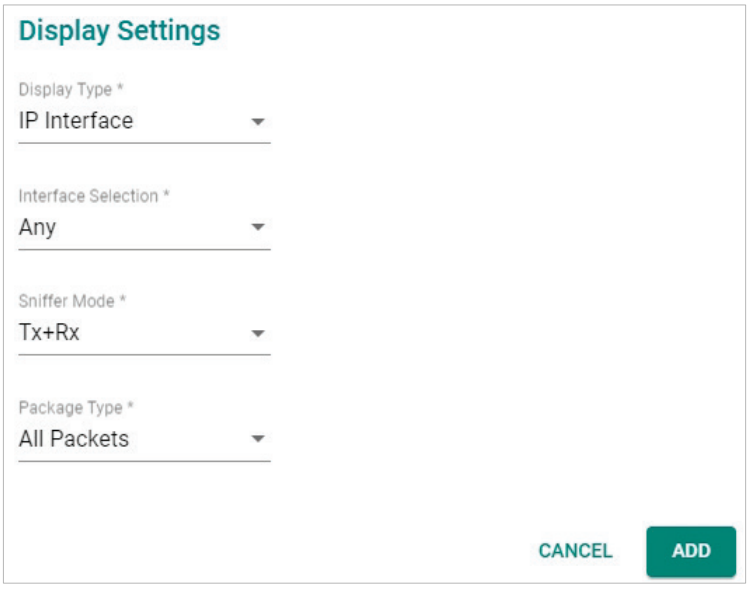
In the **Packet Counter** view, users can monitor the total amount of packets per second for each interface (**IP Interface)**, each port, or port group (**Ports**). Users can choose which packet flows to monitor, **TX Packets**, **RX Packets**, or both (**TX/RX**). **TX Packets** are packets sent out 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

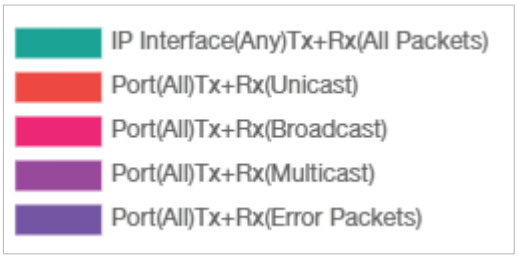
Setting	Description	Factory Default
TX+RX, TX, RX	Select which packet flow to monitor.	TX+RX

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:

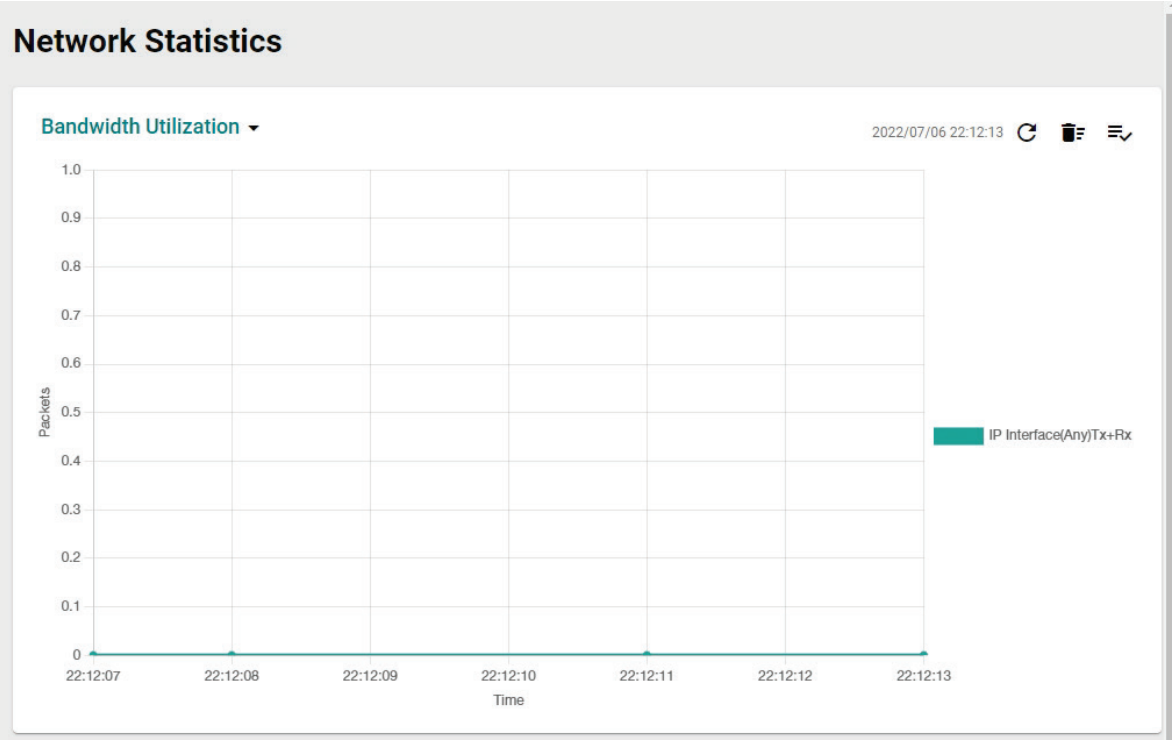


Packet Interface Table

The packet flow format is Total Packets + Packets in the past 5 seconds. The data is updated every 5 seconds.

Bandwidth Utilization

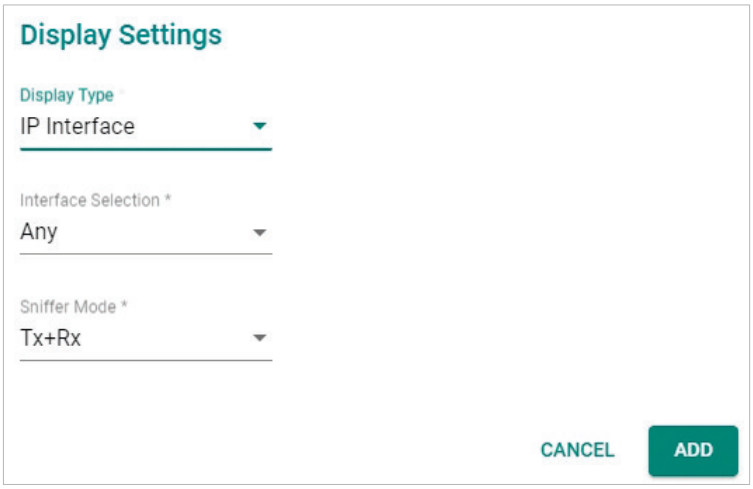
Select **Bandwidth Utilization** from the drop-down menu in the **Network Statistics** page to view the current bandwidth usage.



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.

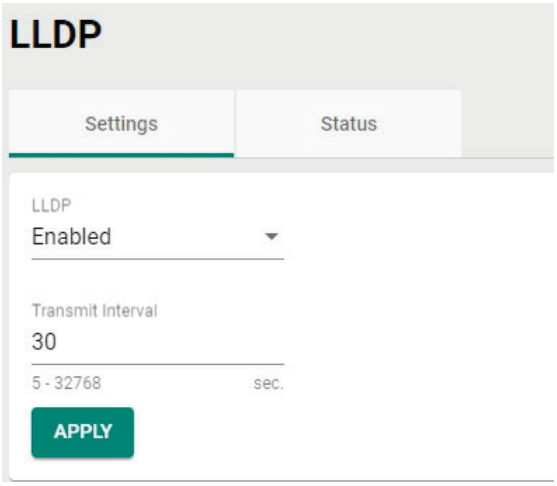
LLDP

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



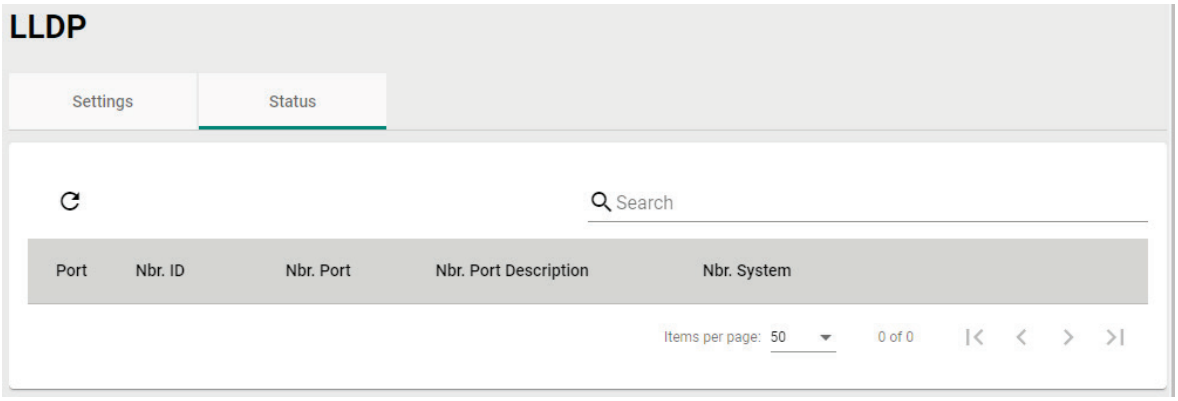
LLDP

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



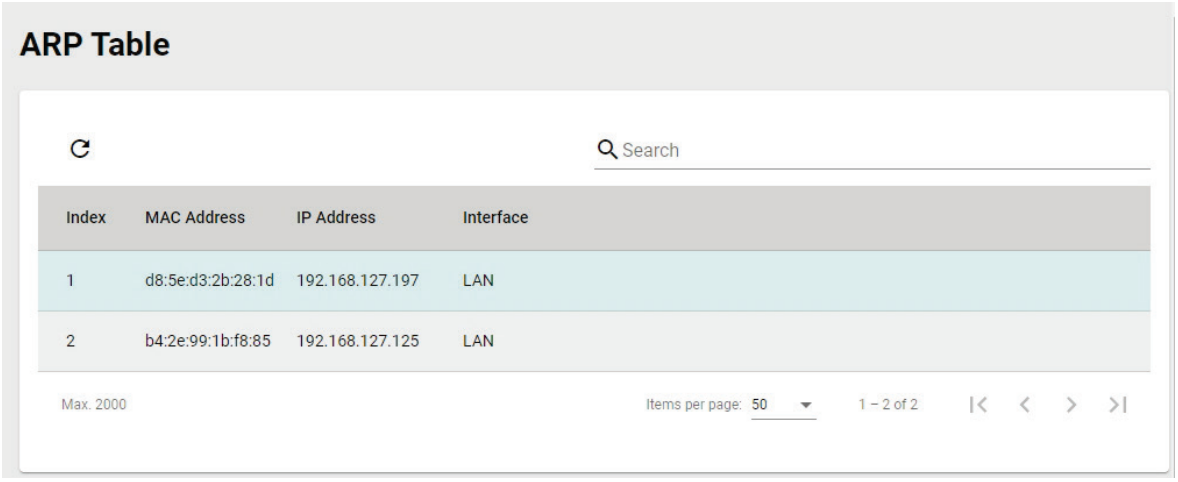
The LLDP table displays the following information:

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.

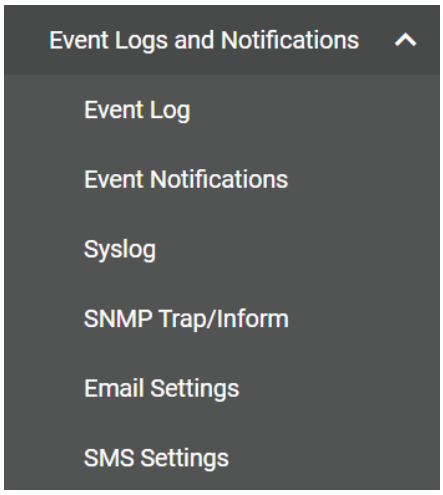
ARP Table

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, Email Settings**, and **SMS Settings**.

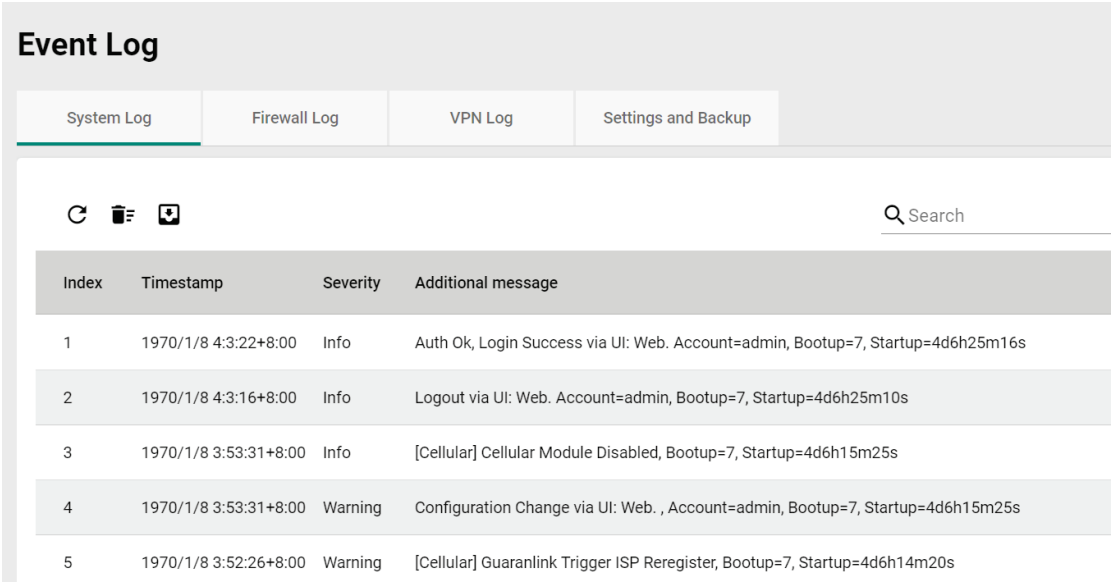


Event Log

> **Note**
>
> The timestamp on event logs will automatically synchronize with the NTP/SNTP server and applies to all new event logs.

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.

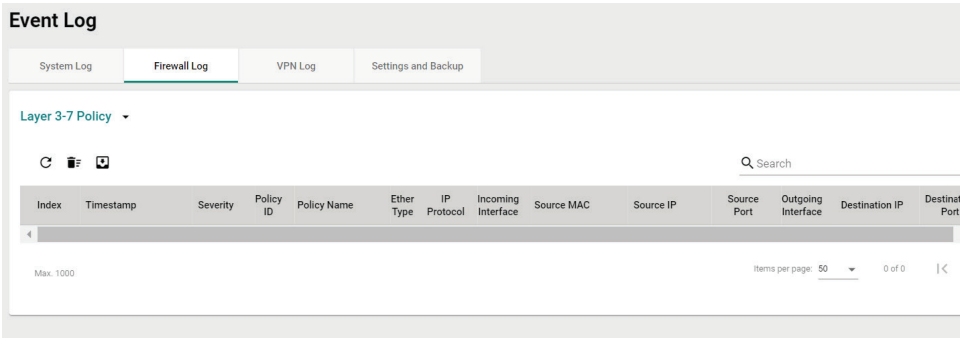
Click the icon to export all system logs to a file.

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
- Session Control
- Layer 2 Policy



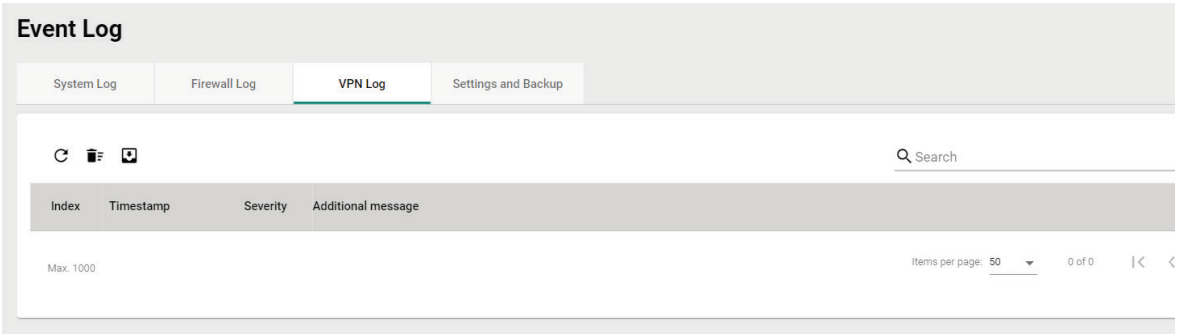
Click the icon to refresh the firewall logs.

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.



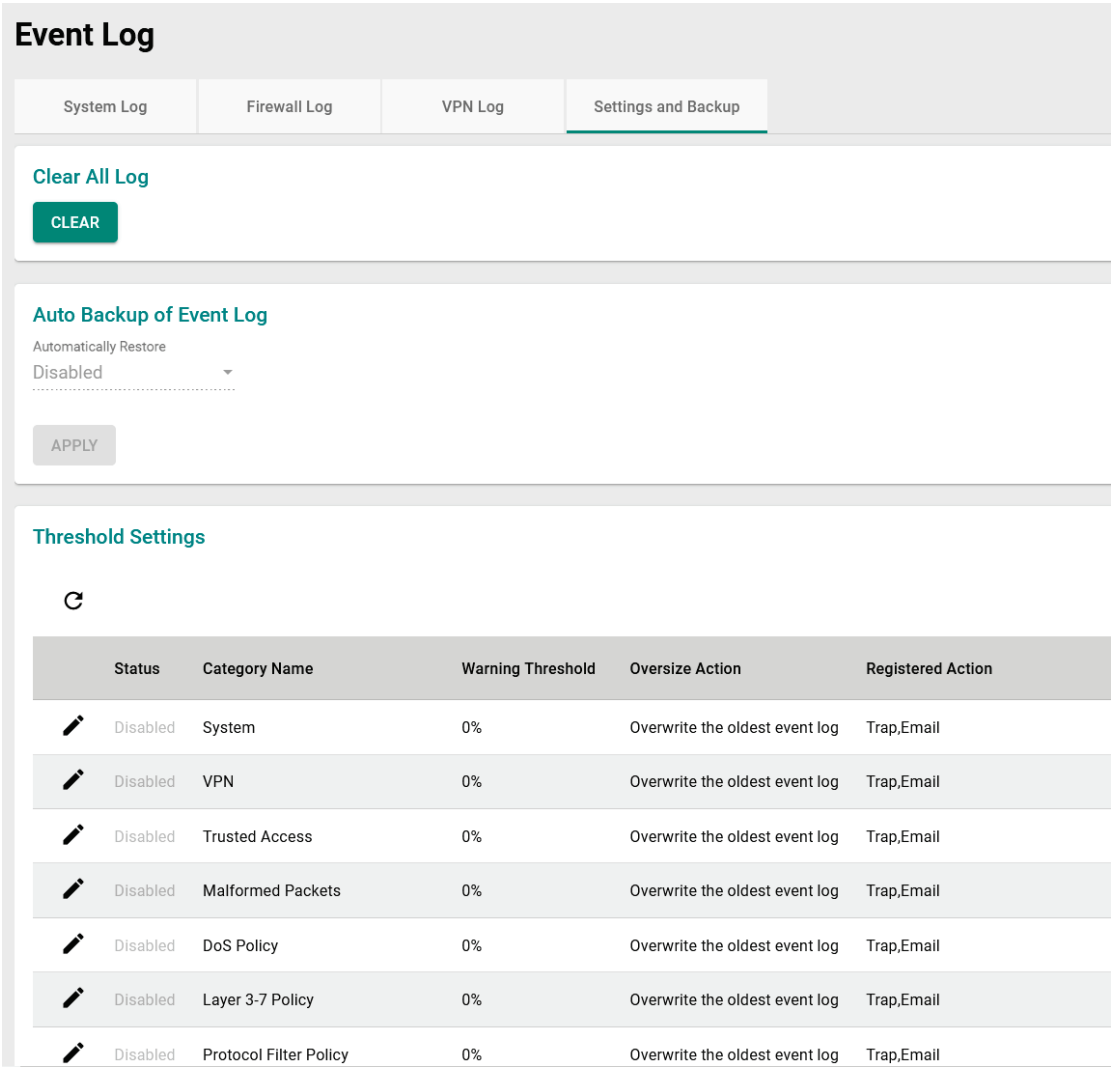
Click the icon to refresh the VPN logs.

Click the icon to delete all VPN logs.

Click the icon to export all VPN logs to a file.

Settings and Backup

On the **Settings and Backup** screen, users can clear all logs, enable automatic log backups, and configure capacity warnings and oversize actions that trigger when the log storage has exceeded the specified storage threshold.



Clear All Log

Click **CLEAR** to immediately clear all event logs.

Auto Event Log Backup

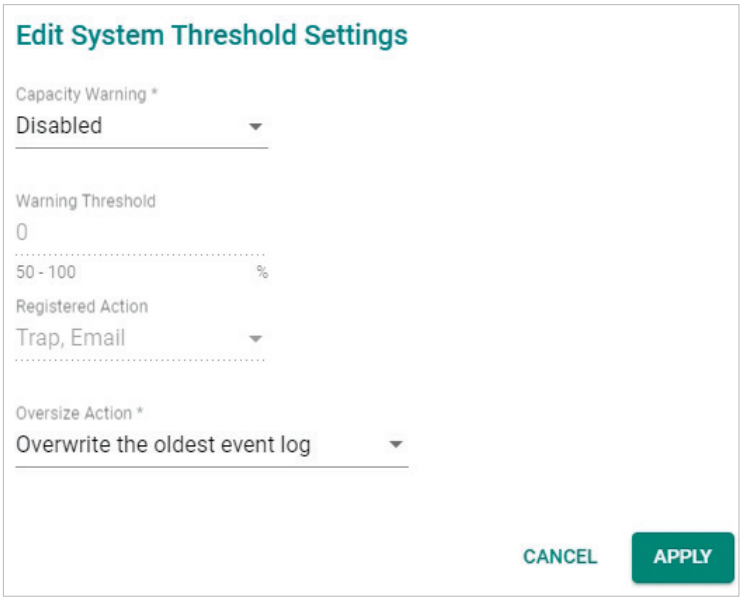
Setting	Description	Factory Default
Enabled or Disabled	Enable or disable automatic event log backups.	Disabled

Threshold Settings

Click the icon to refresh the threshold settings.

Modify an Event Threshold Setting

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

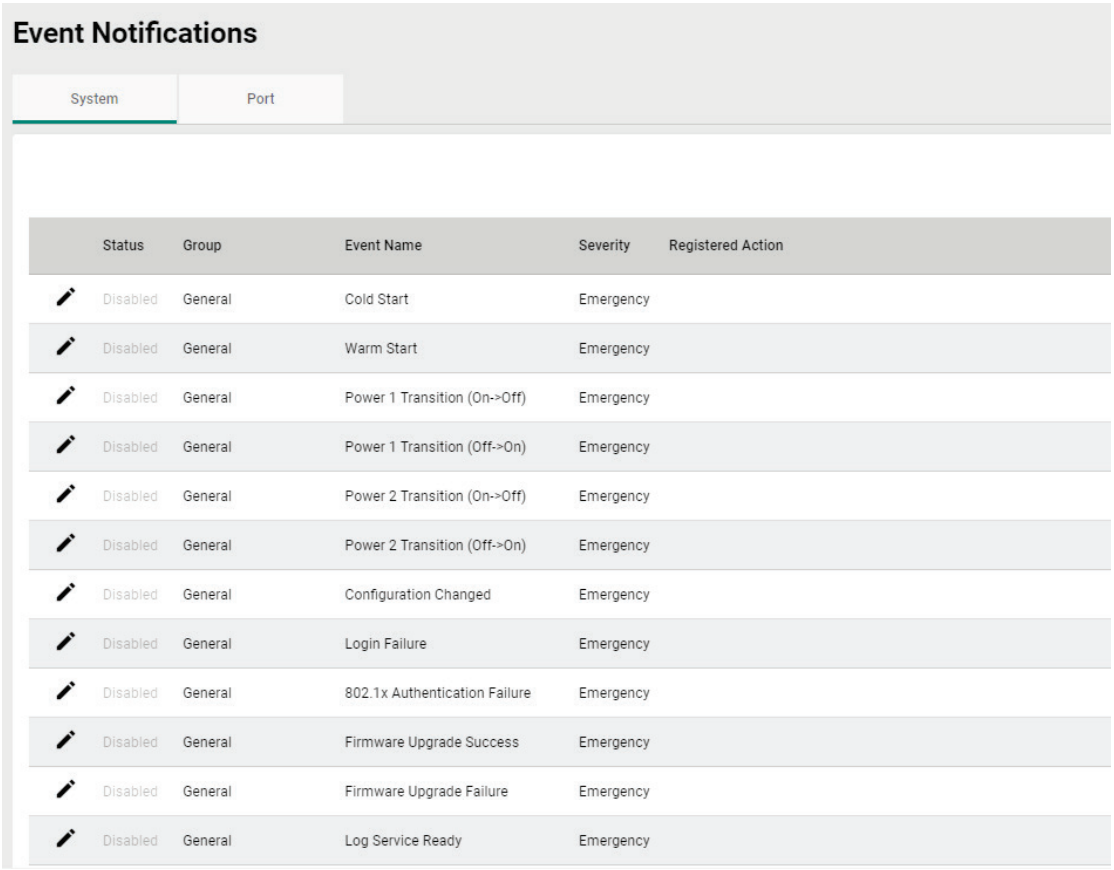
When finished, click **APPLY** to save your changes.

Event Notifications

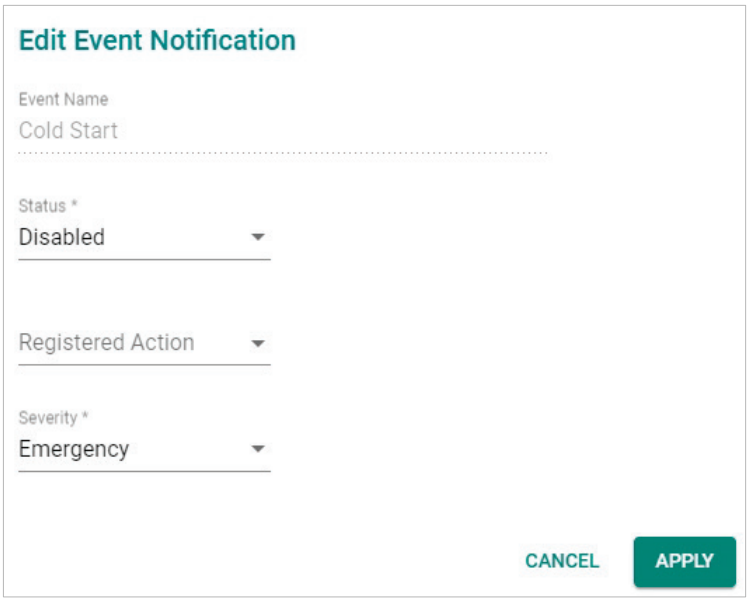
Since industrial Ethernet devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that an industrial secure router that connects to these devices must provide system maintainers with real-time alarm messages. Even 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. Administrators 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
General	Cold Start
General	Warm Start

System Events	Description
General	Power 1 Transition (On to Off)
General	Power 1 Transition (Off to On)
General	Power 2 Transition (On to Off)
General	Power 2 Transition (Off to On)
General	DI (Off)
General	DI (On)
General	Config. Change
General	Auth. Failure
General	802.1X Auth. Failure
General	Firmware Upgrade Success
General	Firmware Upgrade Failure
Redundancy	VRRP State Change
VPN	VPN Connected
VPN	VPN Disconnected
Firewall	Firewall Policy
Power Management	Power Saving Start
Power Management	Power Saving End
Power Management	Scheduling Rule Expired
SMS	Wrong Password
SMS	Wrong Command
SMS	Wrong Format
SMS	Command Disabled
SMS	Trusted Number Authentication Fail
Cellular	IP Change
Cellular	Cellular Module Fail
Cellular	SIM detect Fail
Cellular	PIN code Fail
Cellular	SIM switch
Cellular	GuaranLink Cellular Reconnect
Cellular	Guaranlink Trigger ISP Reregister
Cellular	Guaranlink Trigger Cellular Module Reset
Cellular	Guaranlink Trigger System Reboot
WAN Redundancy	WAN Interface Change
WAN Redundancy	WAN Interface Ping Fail

Status

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable system event notifications.	Disabled

Registered Action

There are five 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.	
SMS	The event log is sent through SMS defined in the SMS section.	

Severity

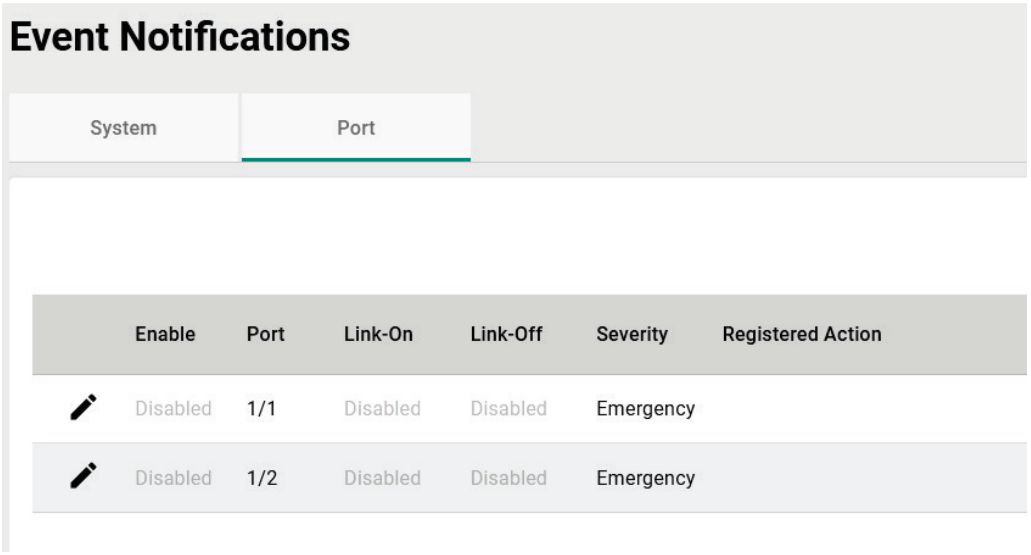
Setting	Description	Factory Default
Emergency	System is unusable	Emergency
Alert	Action must be taken immediately	
Critical	Critical conditions	

Setting	Description	Factory Default
Error	Error conditions	
Warning	Warning conditions	
Notice	Normal but significant condition	
Info	Informational messages	
Debug	Debug-level messages	

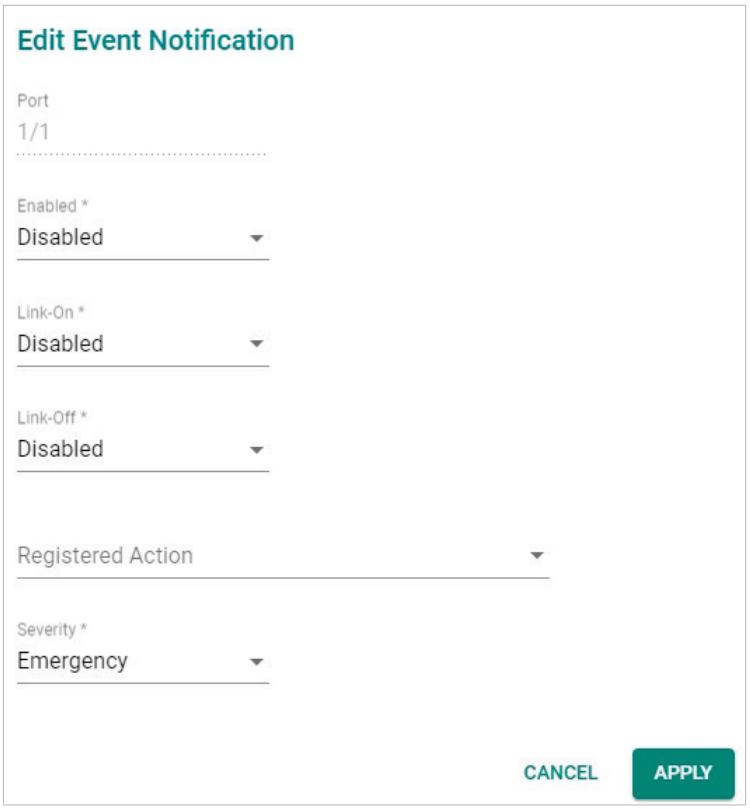
When finished, click **APPLY** to save your changes.

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 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 five 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.	

Setting	Description	Factory Default
SMS	The event log is sent through SMS defined in the SMS section.	

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.

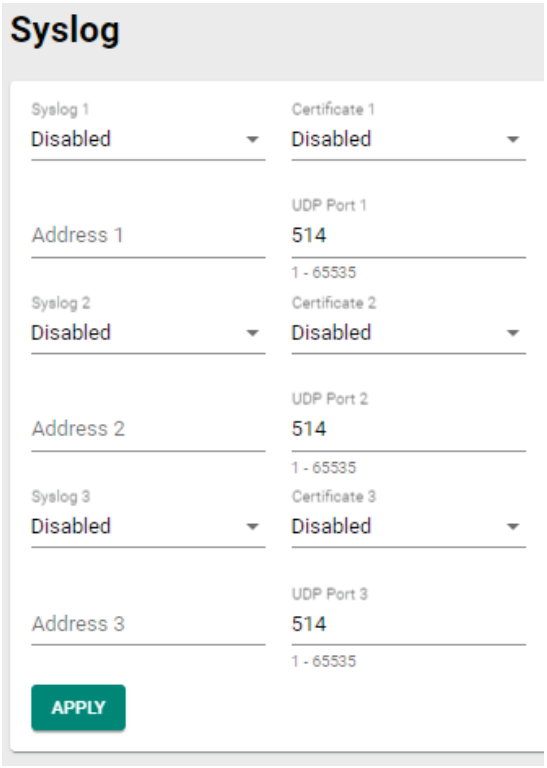
The administrator can manually import a self-signed certificate for syslog client services. However, the administrator should check the root certificate and validity of the signature before importing, according to the organization's security procedures and requirements. After importing a certificate, the administrator should check if the certificate has been revoked and if so, the certificate must be replaced. When the device sends the imported certificate to the syslog server, the syslog server will attempt to verify the certificate by searching the approved certificate pool on the server to identify the imported certificate.

Note

1. The encryption algorithm of keys should be selected based on internationally recognized and proven security practices and recommendations.
2. The lifetime of certificates generated for syslog client services should be short and in accordance with the organization's security procedures and requirements.

Note

For security reasons, it is recommended to send event logs to a centralized Syslog server for continuous network event monitoring.



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

Certificate 1/2/3C

Setting	Description	Factory Default
Enabled or Disabled	Enable or disable the use of Syslog server certificates. If enabled, select a previously imported certificate.	Disabled

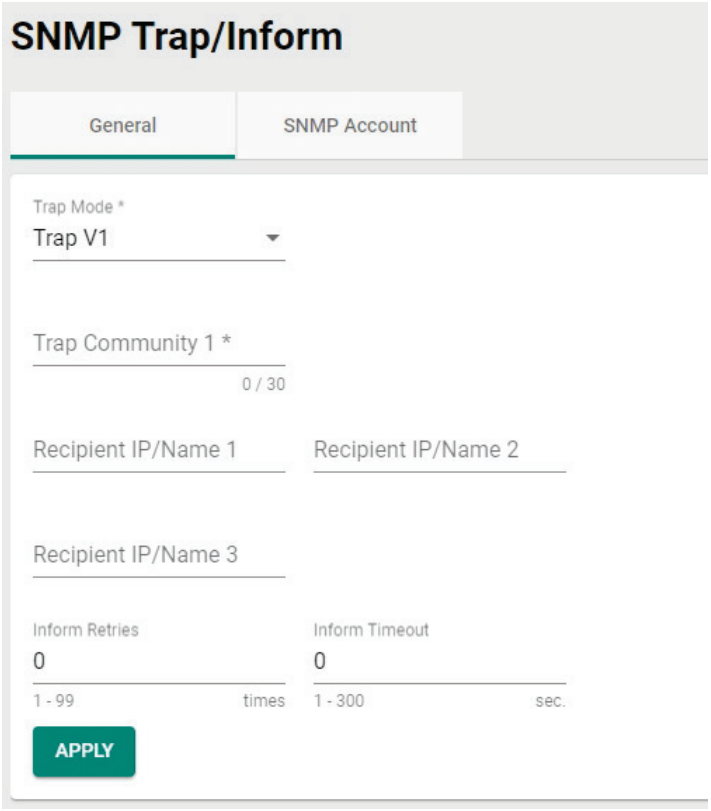
UDP Port

Setting	Description	Factory Default
1 to 65535	Specify the UDP port of the Syslog server.	514

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

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.	public

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

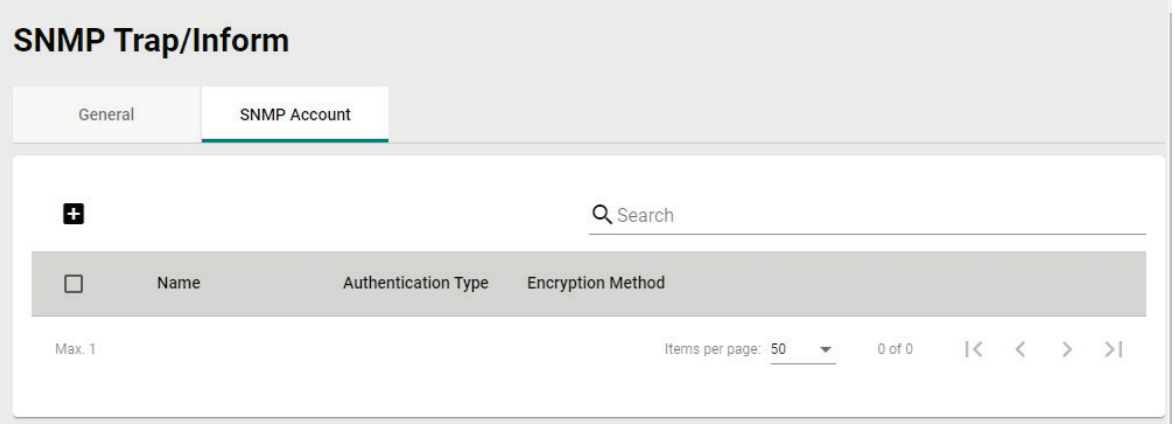
Inform Retries

Setting	Description	Factory Default
1 to 99 times	Specify the allowed number of retries for attempting to reconnect to a server.	0

Inform Timeout

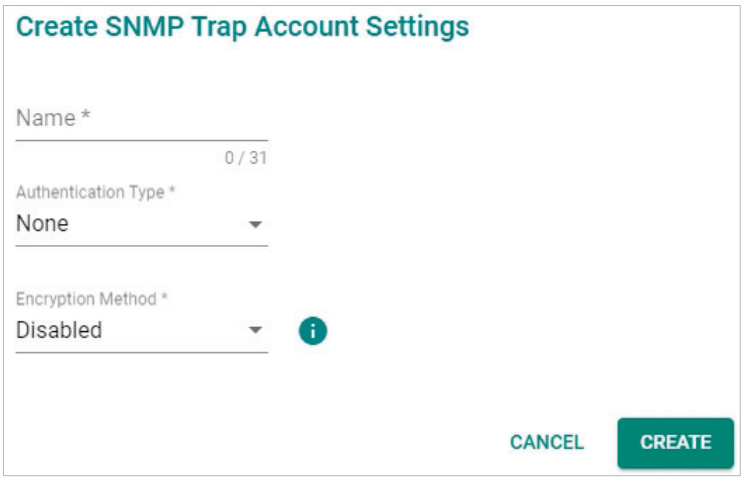
Setting	Description	Factory Default
1 to 300 seconds.	Set the retry interval when trying to reconnect to a server.	0

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

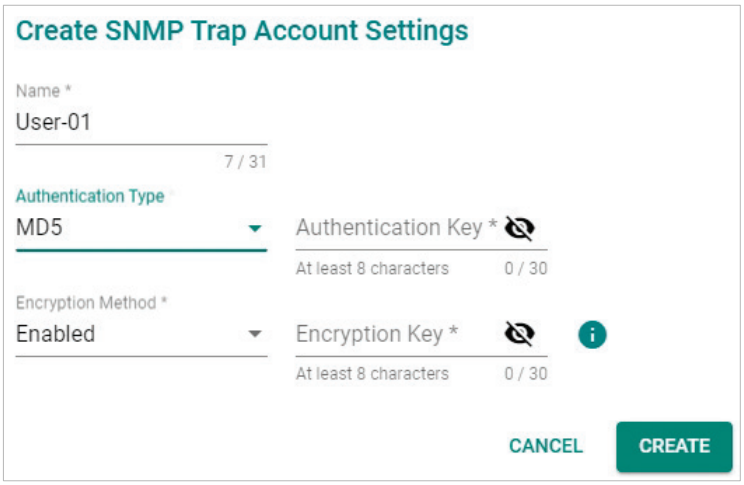
Authentication Type

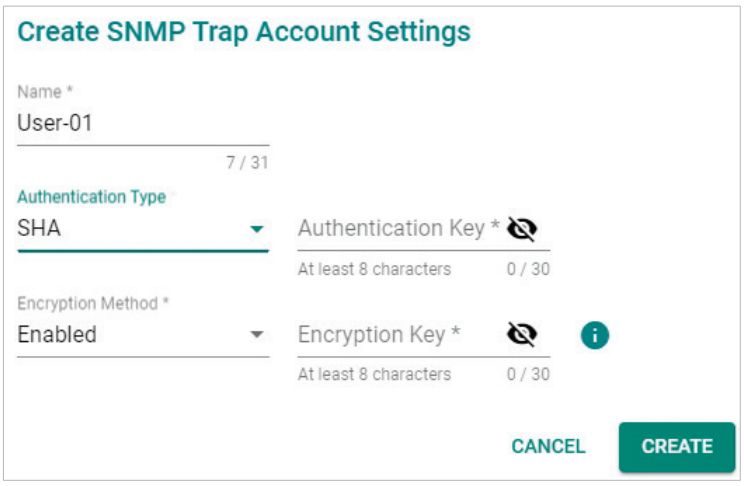
Setting	Description	Factory Default
None	No authentication type will be used.	None
MD5	Use MD5 authentication.	
SHA	Use SHA authentication.	

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.

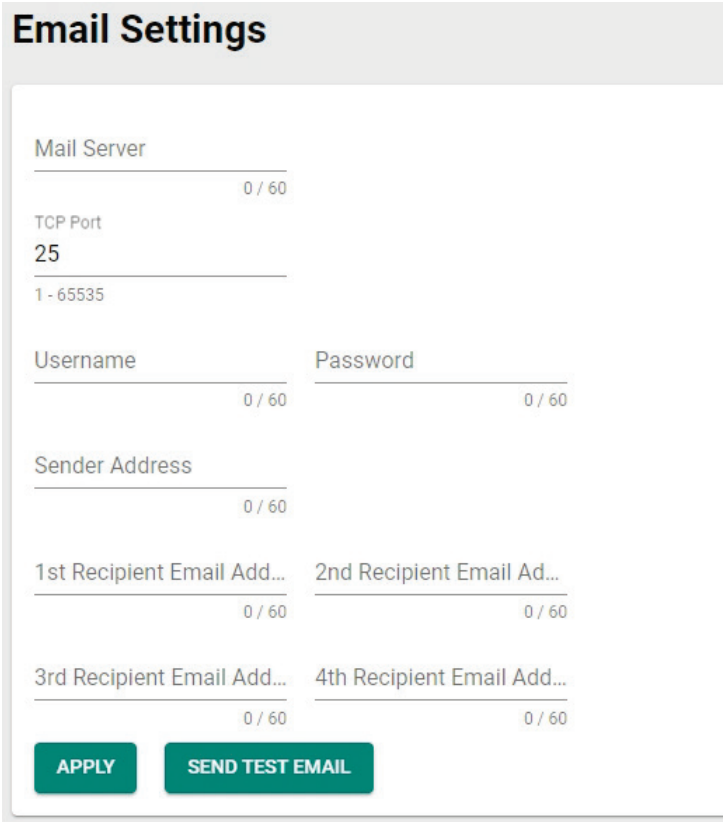
Modify an Existing SNMP Trap Account

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.

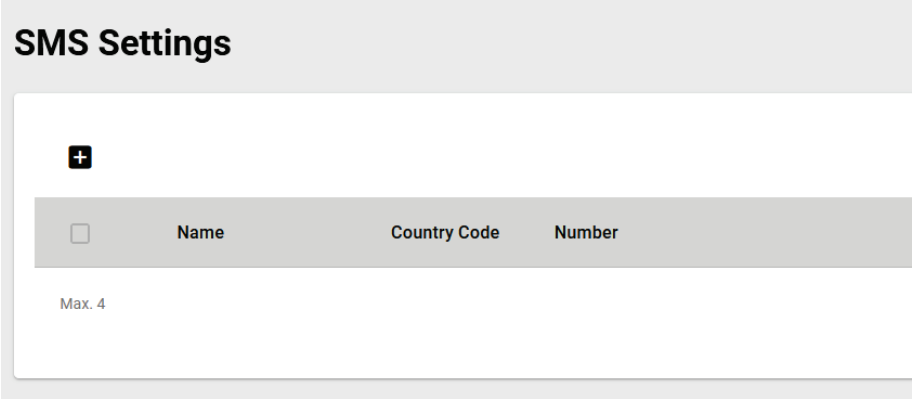
NOTE

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.

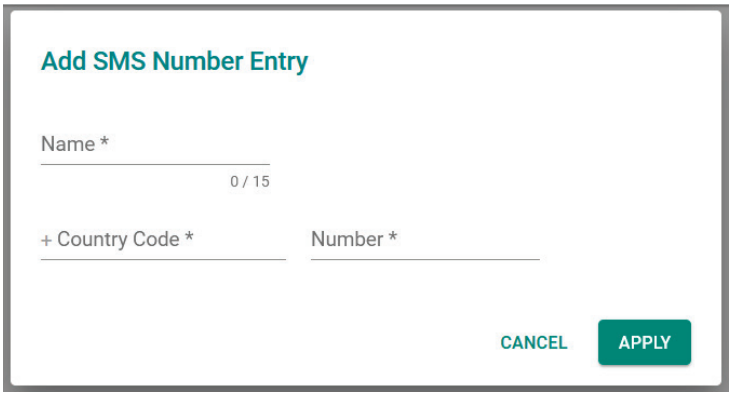
SMS Settings

From the **SMS Settings** screen, you can configure up to four SMS recipients.



Add an SMS Recipient

Click the **Add** ( ) icon to add a new entry.



Name

Setting	Description	Factory Default
Max. 15 characters	Enter the SMS recipient's name.	None

Country Code

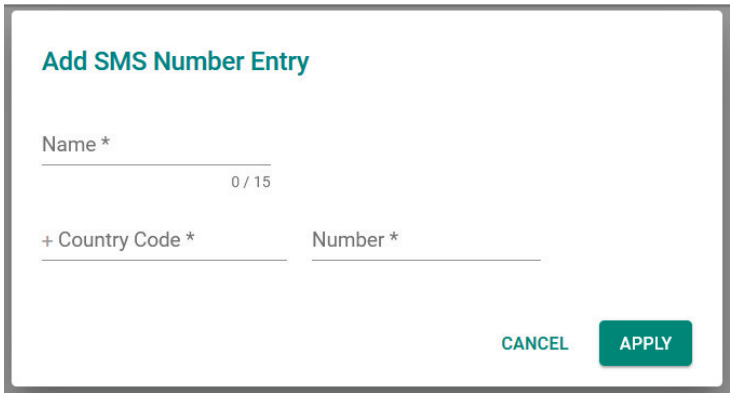
Setting	Description	Factory Default
Country code	Enter the SMS recipient number's country code.	None

Number

Setting	Description	Factory Default
Phone number	Enter the SMS recipient's phone number.	None

Modify an SMS Recipient

Click the pencil ( ) icon next to the entry you want to edit.



Name

Setting	Description	Factory Default
Max. 15 characters	Enter the SMS recipient's name.	None

Country Code

Setting	Description	Factory Default
Country code	Enter the SMS recipient number's country code.	None

Number

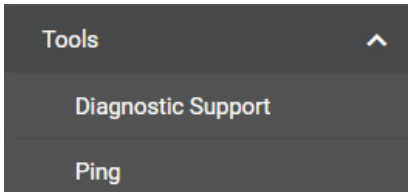
Setting	Description	Factory Default
Phone number	Enter the SMS recipient's phone number.	None

Delete an SMS Recipient

Select the item(s) in the SMS recipient List. Click the icon and click **DELETE** to delete the item(s).

Tools

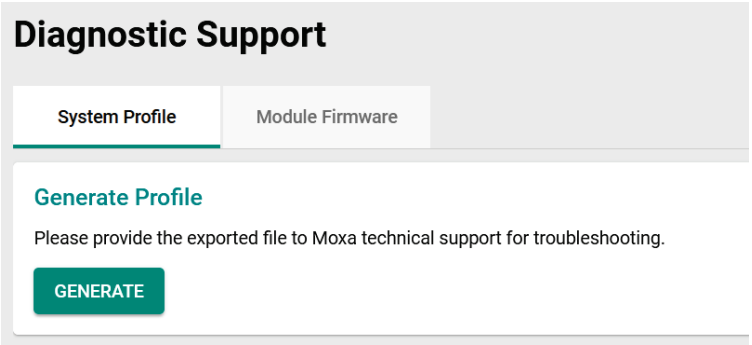
From the **Tools** section, the following functions can be configured: **Diagnostic Support,** and **Ping**.



Diagnostic Support

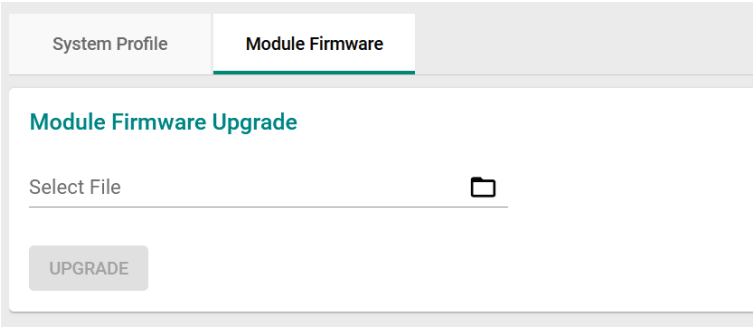
System Profile

From the System Profile screen, users can generate the device information including system logs, system status, and configurations to a file for troubleshooting purposes.

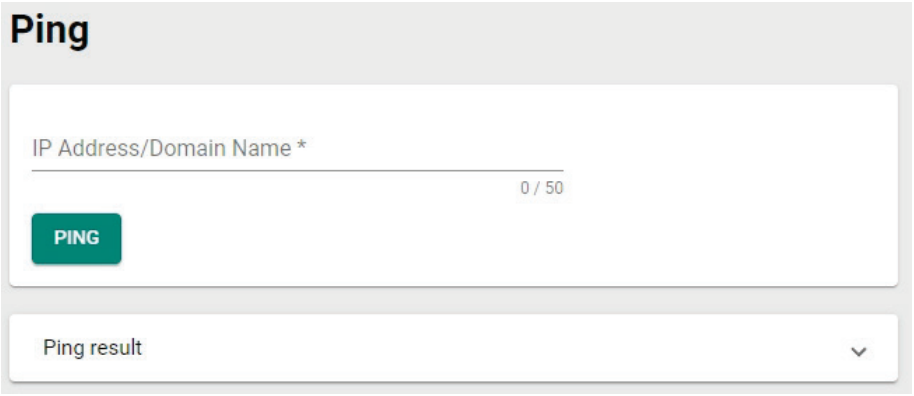


Module Firmware

From the Module Firmware screen, users can upgrade the firmware of the cellular module using a firmware file provided by Moxa Technical Support.

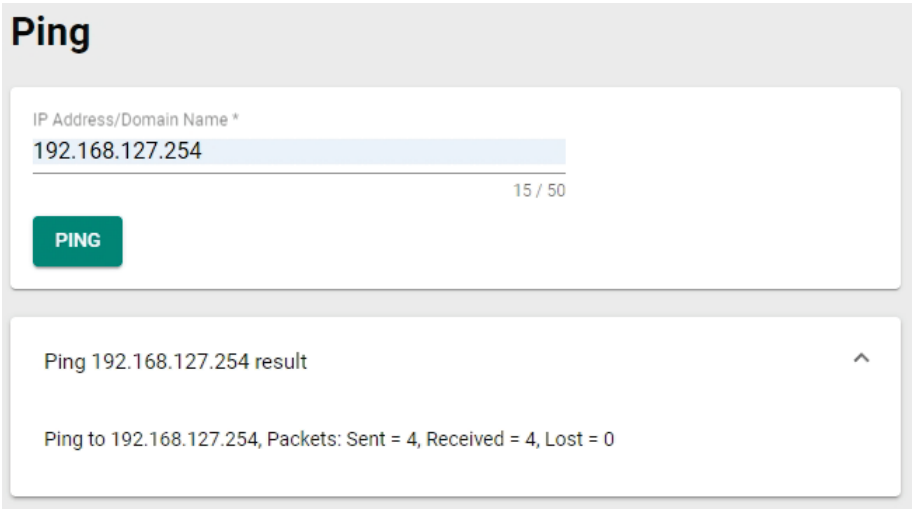


Ping



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.


Ping
IP Address/Domain Name *
192.168.127.254
15 / 50
PING
Ping 192.168.127.254 result
Ping to 192.168.127.254, Packets: Sent = 4, Received = 4, Lost = 0

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.

Note

The User Role Privileges are fixed and cannot be changed. If your application has specific privilege requirements, please contact Moxa for customization support.

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	No Access	No Access
- Software Package Management	R/W	No Access	No Access
- Configuration Backup and Restore	R/W	No Access	No Access
Account Management			
- User Account	R/W	No Access	No Access
- Password Policy	R/W	No Access	No Access
License Management	R/W	R	R
Management Interface			
- User Interface	R/W	R/W	R
- Hardware Interface	R/W	R/W	R
- SNMP	R/W	No Access	No Access
- MXsecurity	R/W	R/W	No Access
Time			
- System Time	R/W	R/W	R
- NTP/SNTP Server	R/W	R/W	R
Setting Check	R/W	R/W	R
Power Management	R/W	R/W	R
SMS	R/W	R/W	R
GNSS	R/W	R/W	R
Cellular	**Admin**	**Supervisor**	**User**
Cellular	R/W	R/W	R
Serial	**Admin**	**Supervisor**	**User**
Serial	R/W	R/W	R
Network Configuration	**Admin**	**Supervisor**	**User**
Port			
- Port Settings	R/W	R/W	R
Layer 2 Switching			
- VLAN	R/W	R/W	R
- MAC Address Table	R/W	R/W	R

Function	Account Privilege		
- Multicast	R/W	R/W	R
Network Interface	R/W	R/W	R
Redundancy	**Admin**	**Supervisor**	**User**
Layer 3 Redundancy			
- VRRP	R/W	R/W	R
WAN Redundancy	R/W	R/W	R
Network Service	**Admin**	**Supervisor**	**User**
DHCP Server	R/W	R/W	R
Dynamic DNS	R/W	R/W	R
Routing	**Admin**	**Supervisor**	**User**
Unicast Routing			
- Static Routes	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
VPN	**Admin**	**Supervisor**	**User**
IPsec	R/W	R/W	R
Certification Management	**Admin**	**Supervisor**	**User**
Local Certificate	R/W	No Access	No Access
Trusted CA Certificate	R/W	No Access	No Access
Certificate Signing Request	R/W	No Access	No Access
Security	**Admin**	**Supervisor**	**User**
Device Security			
- Login Policy	R/W	R	R
- Trusted Access	R/W	R/W	R
- SSH & SSL	R/W	R/W	No Access
Authentication			
- Login Authentication	R/W	No Access	No Access
RADIUS	R/W	No Access	No Access
MXview Alert Notification	R/W	R/W	R
Diagnosis	**Admin**	**Supervisor**	**User**
System Status			
- Utilization	R/W	R/W	R
Network Status			
- Network Statistics	R	R	R
- LLDP	R/W	R/W	R
- ARP Table	R	R	R
Event Log & Notifications			
- Event Log	R/W	R/W	R
- Event Notifications	R/W	R/W	R
- Syslog	R/W	R	R
- SNMP Trap/Inform	R/W	No Access	No Access
- Email Settings	R/W	R	R
- SMS Settings	R/W	R	R
Tools			
- Diagnostic Support	R/W	R/W	R

Function	Account Privilege		
- Ping	R/W	R/W	R

C. Security Guidelines

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

Installation

Physical Installation

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

Account Management

Follow these best practices when setting up an account:

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

Vulnerable Network Ports

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

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

Operation

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

TLS V1.2

Cypher Suite Name	Key Exchange	Authentication	Encryption	Hash Function
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	ECDHE	ECDSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	ECDHE	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	Ephemeral DH	RSA	AES128	SHA256
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	Ephemeral DH	RSA	AES256	SHA384
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256	Ephemeral DH	RSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE-RSA_WITH_AES256-SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDHE	RSA	AES128	SHA256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256	ECDHE	ECDSA	CHACHA20-POLY1305	SHA256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	ECDHE	RSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	ECDHE	ECDSA	AES256	SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	ECDHE	ECDSA	AES128	SHA256

TLS V1.3

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

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

Browser	Version
Microsoft Edge	All
Microsoft Internet Explorer	v11 or above
Mozilla Firefox	v27 or above
Google Chrome	v38 or above
Apple Safari	v7 or above

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

3. The device supports event logs and syslog for SIEM integration:
   a. Event log: Due to limited storage capacity, the event log can only accommodate a maximum of 1,000 entries per category. Administrators can set a warning for a pre-defined threshold. We

recommend that users regularly back up system event logs. Please refer to the Event Log section for detailed instructions.

b. Syslog: the device supports syslog, and advanced secure TLS-based syslog for centralized SIEM integration. Please refer to the Syslog section for detailed instructions.

4. The device can provide information for control system inventory:
   a. SNMPv1, v2c, v3: We recommend administrators use SNMPv3 with authentication and encryption to manage the network. Please refer to the SNMP for detailed instructions.
   b. Telnet/SSH: We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
   c. HTTP/HTTPS: We recommend that administrators use HTTPS with a certificate that has been granted by a Certificate Authority to configure the device.
5. Denial of Service protection: To avoid disruption of the normal operation of the router, administrators should configure the QoS and DoS policy functions. The device supports ingress rate limiting and egress shaper. Administrators can decide how to deal with excess data flow and configure the device accordingly. This process will regulate the resulted data rate per port. Please refer to the QoS section for detailed instructions. Furthermore, the device provides 9 different DoS functions for detecting or defining abnormal packet formats or traffic flows. Please refer to the DoS (Denial of Service) Policy section for detailed instructions.
6. Time synchronization with authentication: Time synchronization is crucial for process control. To prevent malicious attacks whereby the settings are changed without permission, authentication must be in place between the NTP server and client. The device supports NTP with a pre-shared key. Please refer to the Time section for detailed instructions.
7. Periodically regenerate the SSH and SSL certificates: Even though the device supports RSA 2048-bit and SHA-256 to ensure sufficient complexity, we strongly recommend that users frequently renew their SSH key and SSL certificate in case the key is compromised. Please refer to the SSH & SSL section for detailed instructions.
8. Below is the list for the protocol port numbers used for all external interfaces:

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

Maintenance

1. Perform firmware upgrades frequently to enhance features, deploy security patches, or fix bugs.
2. Frequently back up the system configurations: In order to properly protect the system configuration files from being tampered with, the device supports password encryption and signature authentication for backup files.
3. Examine event logs frequently to detect any anomalies.
4. To report vulnerabilities of Moxa products, please submit your findings on the following web page: https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability.

Decommission

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