NAT-102 Series User's Manual

Version 1.0, December 2021

www.moxa.com/product

NAT-102 Series User's 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

Moxa Americas
Toll-free: 1-888-669-2872
Tel: +1-714-528-6777
Fax: +1-714-528-6778

Moxa China (Shanghai office)
Toll-free: 800-820-5036
Tel: +86-21-5258-9955
Fax: +86-21-5258-5505

Moxa Europe
Tel: +49-89-3 70 03 99-0
Fax: +49-89-3 70 03 99-99

Moxa Asia-Pacific
Tel: +886-2-8919-1230
Fax: +886-2-8919-1231

Moxa India
Tel: +91-80-4172-9088
Fax: +91-80-4132-1045

Table of Contents

1

Introduction

Welcome to the Moxa NAT-102 Series industrial Network Address Translation device.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Features**
  - Quick and User-friendly Access Control
  - Industrial-grade and Ultra-compact Design

Overview

The NAT-102 Series is an industrial NAT device that is designed to simplify the IP configuration of machines in existing network infrastructure in factory automation environments. The NAT-102 Series provides complete NAT functionality to adapt your machines to specific network scenarios without complicated, costly, and time-consuming configurations. These devices also protect the internal network from unauthorized access by outside hosts.

Package Checklist

The NAT-102 Series is shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.

- 1 Industrial NAT device
- USB-C-to-DB9 cable
- Protective caps for unused ports
- Quick installation guide (printed)
- Warranty card

Features

- User-friendly NAT functionality simplifies network integration
- Hands-free network access control through automatic whitelisting of locally connected devices
- Ultra-compact size and robust industrial design suitable for cabinet installation
- Integrated security features to ensure device and network safety
- Supports secure boot for checking system integrity
- -40 to 75°C operating temperature range (-T model)

Quick and User-friendly Access Control

The NAT-102 Series' Auto Learning Lock feature automatically learns the IP and MAC address of locally connected devices and binds them to the access list. This feature not only helps you manage access control but also makes device replacements much more efficient.

Industrial-grade and Ultra-compact Design

The NAT-102 Series' rugged hardware makes these NAT devices ideal for deployment in harsh industrial environments, featuring wide-temperature models that are built to operate reliably in hazardous conditions and extreme temperatures of -40 up to 75°C. Moreover, the ultra-compact size allows the NAT-102 Series to be easily installed into cabinets.

2

Getting Started

This chapter explains how to access the Industrial NAT device for the first time. There are three ways to access the device: (1) serial console, (2) Telnet console, or (3) web browser. The serial console connection method, which requires using a serial cable to connect the Industrial NAT device to a PC's COM port, can be used if you do not know the Industrial NAT device's IP address. The Telnet console and web browser connection methods can be used to access the Industrial NAT device over an Ethernet LAN, or over the Internet. All monitoring and administration functions can be performed when accessing the device through a web browser. Accessing the device using the serial console and Telnet console only allow you to manage basic functions.

The following topics are covered in this chapter:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Using Telnet to Access the Industrial NAT Device's Console**
- **Using a Web Browser to Configure the Industrial NAT Device**

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

ATTENTION

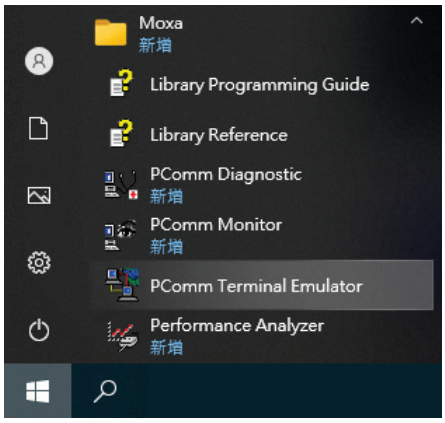
We strongly suggest that you do NOT use more than one connection method at the same time. Following this advice will allow you to maintain better control over the configuration of your Industrial NAT device.

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

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

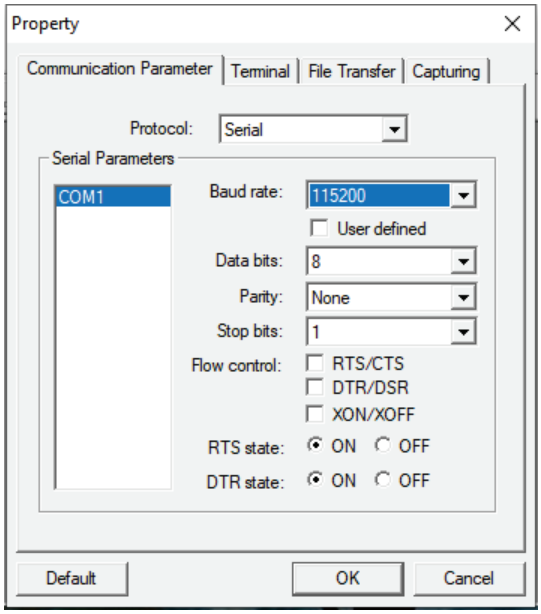
After installing PComm Terminal Emulator, perform the following steps to access the RS-232 console utility.

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

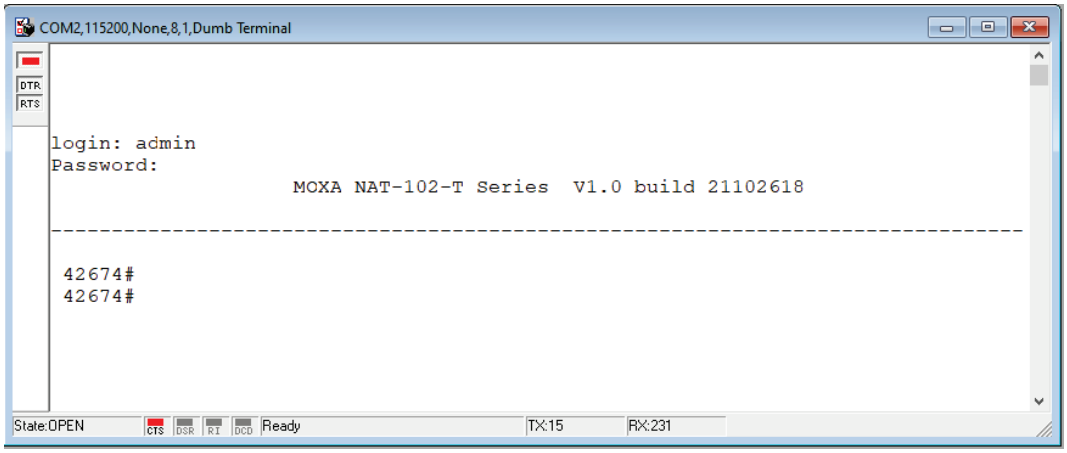


2. Click **Open** in the Port Manager menu to open a new connection.

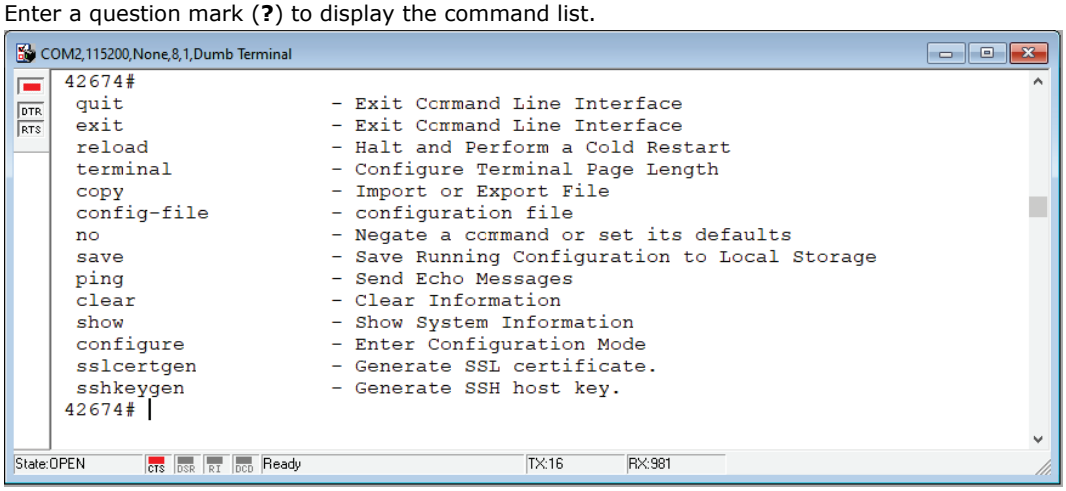
3. The **Communication Parameter** page of the **Property** window will appear. Select the appropriate COM port from the **Serial Parameters** list, 115200 for Baud Rate, 8 for Data Bits, None for Parity, and 1 for Stop Bits.



4. Click the **Terminal** tab, select VT100 for Terminal Type, and then click **OK** to continue.
5. 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**.



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



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

Admin Account Commands

Command	Description
quit	Exit Command Line Interface
exit	Exit Command Line Interface
reload	Halt and Perform a Cold Restart
terminal	Configure Terminal Page Length
copy	Import or Export File
config-file	Configure file
no	Negate a command or set its defaults
save	Save Running Configuration to Local Storage
ping	Send Echo Messages
clear	Clear Information
show	Show System Information
configure	Enter Configuration Mode
sslcertgen	Generate SSL certificate
sshkeygen	Generate SSH host key

Using Telnet to Access the Industrial NAT Device's Console

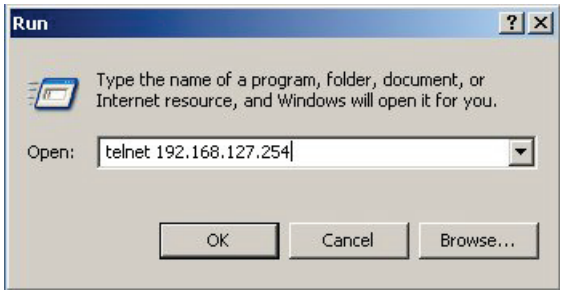
You may use Telnet to access the Industrial NAT device's console utility over a network. To access the NAT device's functions over the network (by either Telnet or a web browser) from a PC host that is connected to the same LAN as the Industrial NAT device, you need to make sure that the PC host and the Industrial NAT device are on the same logical subnet. To do this, check your PC host's IP address and subnet mask. By default, the NAT-102's LAN IP address is 192.168.127.254 and the subnet mask is 255.255.255.0 (for a Class C subnet). If you have not changed these values, and your PC host's subnet mask is 255.255.0.0, then the PC's IP address should be 192.168.xxx.xxx. On the other hand, if your PC host's subnet mask is 255.255.255.0, then its IP address should be 192.168.127.xxx.

NOTE Before accessing the console utility via Telnet, first connect the Industrial NAT device's RJ45 Ethernet LAN port 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.

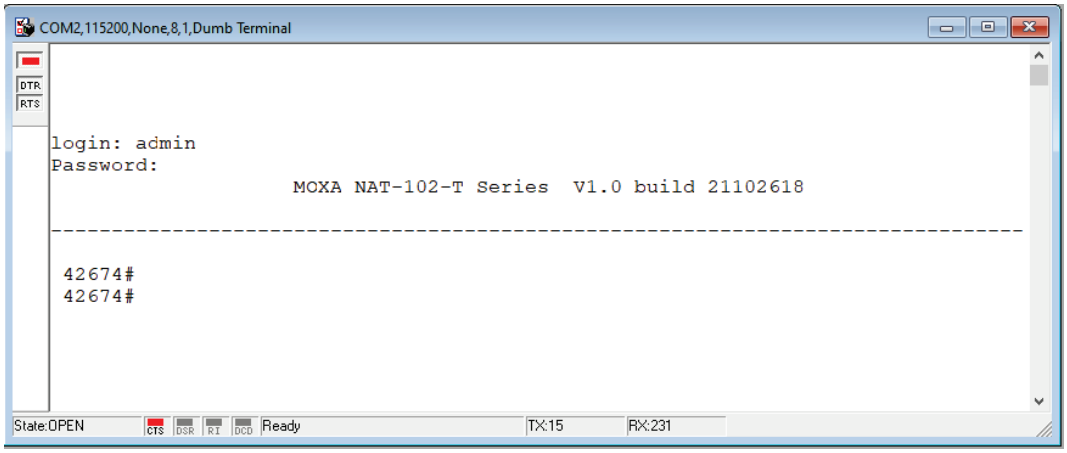
NOTE The Industrial NAT device's default LAN IP address is 192.168.127.254.

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

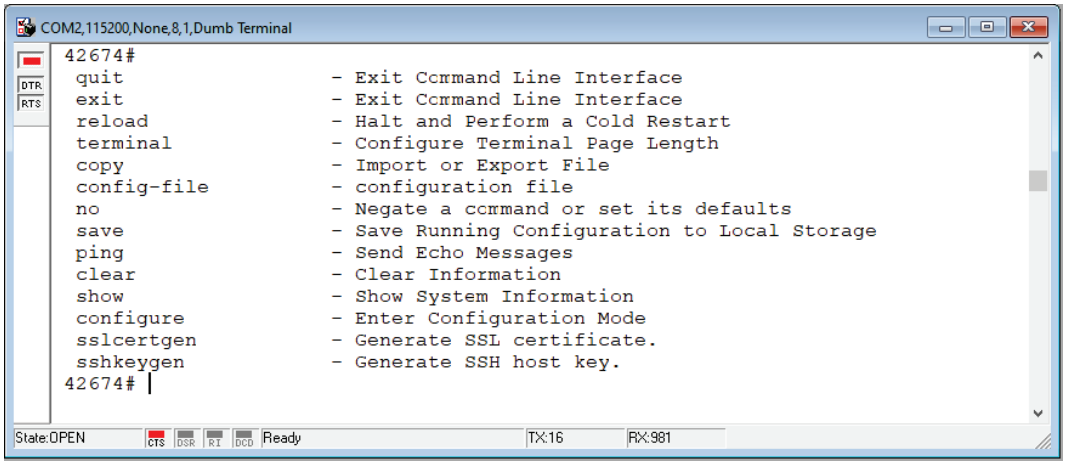
1. Click **Start** → **Run**, and then telnet to the Industrial NAT device's IP address from the Windows Run window. (You may also issue the Telnet command from the MS-DOS prompt.)



2. 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**.



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



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

Admin Account Commands

Command	Description
quit	Exit Command Line Interface
exit	Exit Command Line Interface
reload	Halt and Perform a Cold Restart
terminal	Configure Terminal Page Length
copy	Import or Export File

config-file	Configure file
no	Negate a command or set its defaults
save	Save Running Configuration to Local Storage
ping	Send Echo Messages
clear	Clear Information
show	Show System Information
configure	Enter Configuration Mode
sslcertgen	Generate SSL certificate
sshkeygen	Generate SSH host key

Using a Web Browser to Configure the Industrial NAT Device

The Industrial NAT device's web browser interface provides a convenient way to modify the NAT device's configuration settings and access the device's 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 NAT device's management and monitoring functions from a PC host connected to the same LAN as the Industrial NAT device, you must make sure that the PC host and the Industrial NAT device are connected to the same logical subnet.

NOTE Before accessing the Industrial NAT device's web browser, first connect the Industrial NAT device's RJ45 Ethernet LAN port 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.

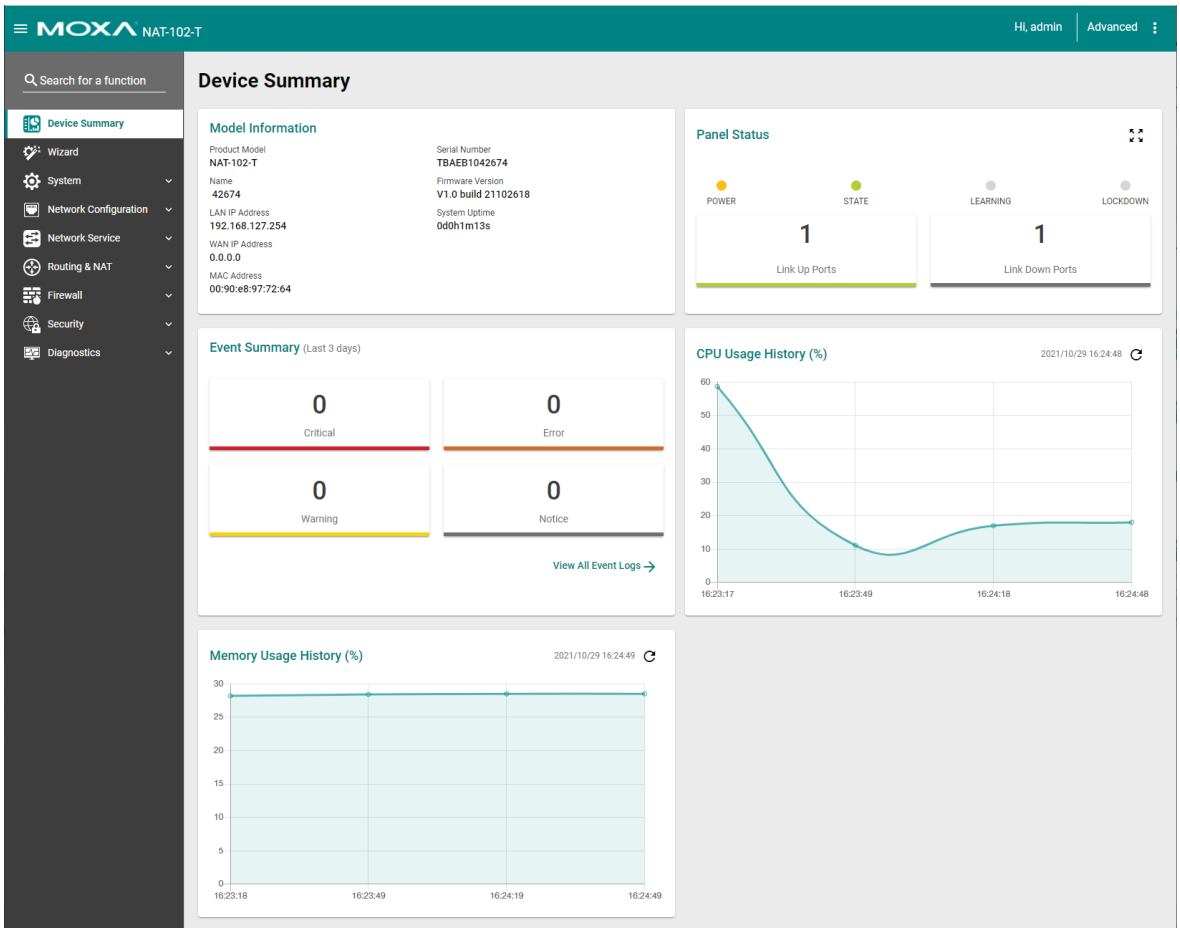
NOTE The Industrial NAT device's default LAN IP address is 192.168.127.254.

Perform the following steps to access the Industrial NAT device's web browser interface.

1. Start Internet Explorer, type the Industrial NAT device's LAN IP address in the address field and press **Enter**.

2. The web login page will open. Enter the username (**Admin** or **User**) and password If a password has not been set yet, enter the default password "**moxa**".

Use the menu tree on the left side of the screen to open the function pages to access each of the NAT's functions.



3

Device Summary and Wizard

This chapter describes how to access the Industrial NAT device'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.

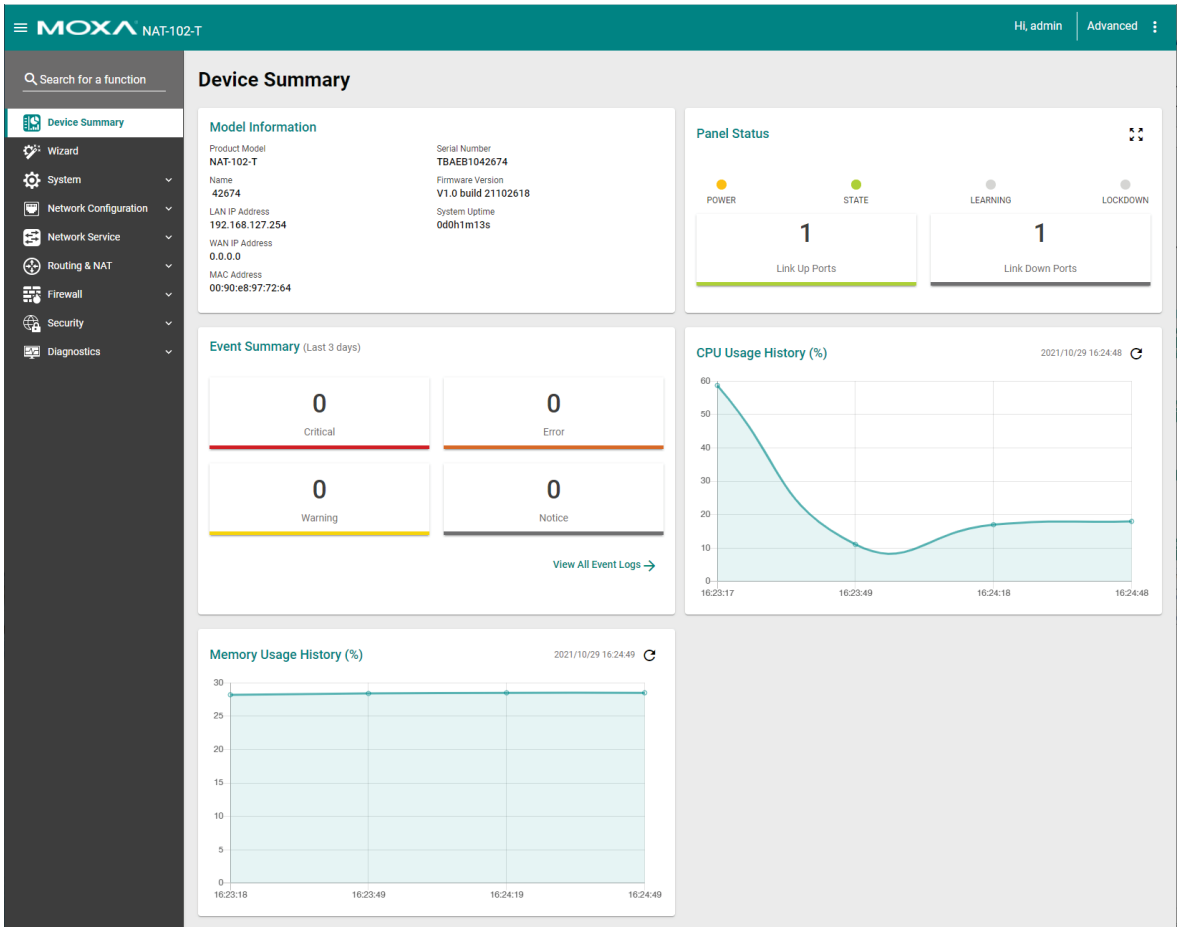
The web browser is the most user-friendly way to configure the Industrial NAT device, since you can both monitor the Industrial NAT device and use administration functions from the web browser. A serial or Telnet console connection only provides access to basic functions. In this chapter, we use the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

The following topics are covered in this chapter:

- **Device Summary**
- **Wizard**
  - Step 1: Welcome
  - Step 2: Network Configuration
  - Step 3: NAT Settings
  - Step 4: Device Lockdown
  - Step 5: Setup Complete!

Device Summary

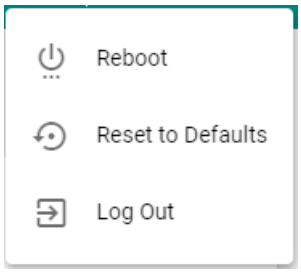
When logging in to the NAT-102, you will be presented with the Device Summary page. This overview page contains basic activity and performance information of the device.



Use the menu tree on the left side of the screen to open the different configuration pages of the NAT's functions.

Clicking  at the top-left side will close or expand the function menu.

Clicking  at the top-right side will expand the drop-down menu shown below.



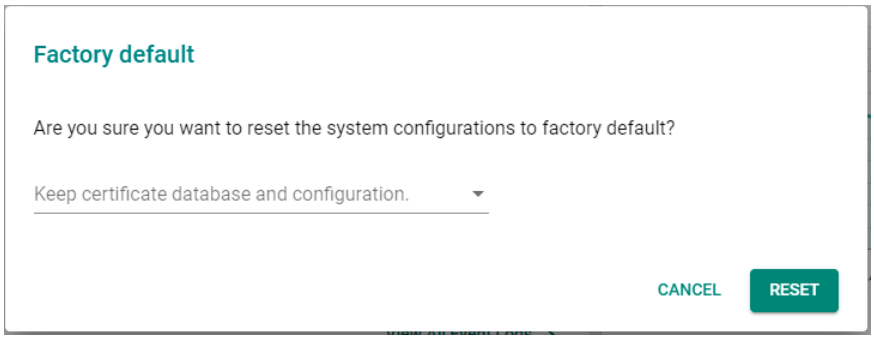
Reboot

Restart the device.

Reset to Defaults

This function will reset all settings to their factory default values. Be aware that all your configuration settings will be permanently deleted.

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



When prompted, select "**Enable**" from the drop-down menu to keep certificate database and configuration information, or select "**Disabled**" to reset everything to its their factory default value.

Log Out

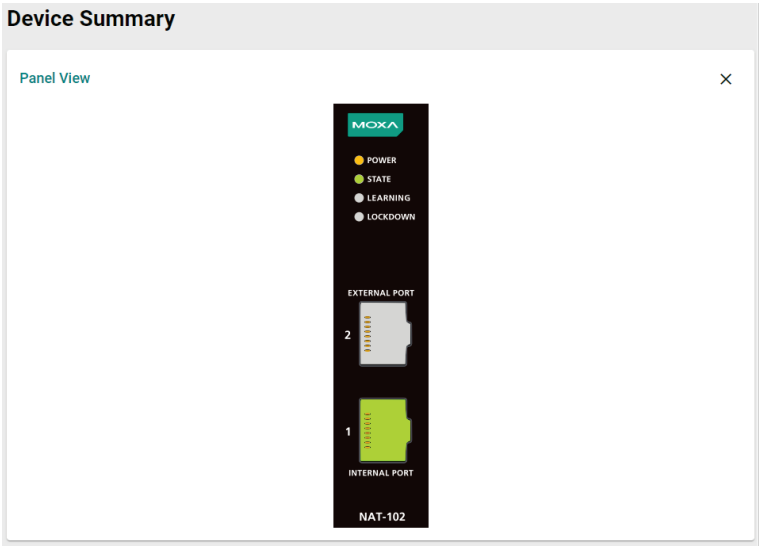
Log out of the device.

Model Information

This panel shows basic information for the NAT device.

Panel Status

Clicking ⛶ will show the Panel View, representing the faceplate of the actual NAT device.



Click ✕ to close the panel view of actual NAT device.

Event Summary

Click View All Event Logs → to jump to the Event Log page.

CPU Usage History (%)

This panel shows the device's CPU usage. Click ↻ to refresh the information.

Memory Usage History

This panel shows the device's memory usage. Click ↻ to refresh the information.

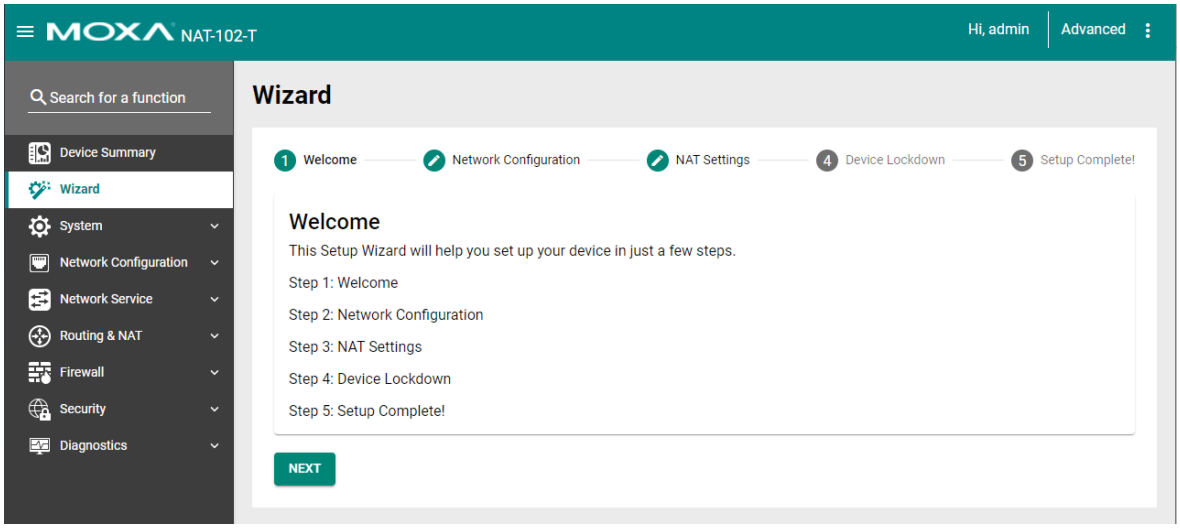
Wizard

The NAT-102 Series supports a Setup Wizard to help you quickly configure basic device settings including IP and NAT settings.

Click **Wizard** in the function column to start the Setup Wizard.

Step 1: Welcome

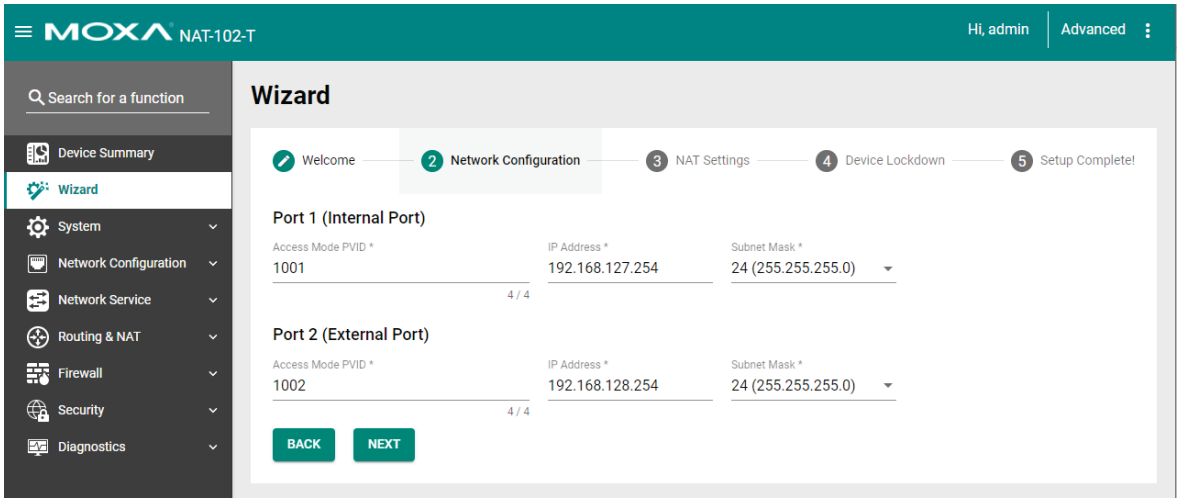
Click the **Next** to start the wizard.



Step 2: Network Configuration

Configure the IP address of Port 1 (Internal Port) and Port 2 (External Port) and define the subnet of the LAN ports on the NAT device. The default LAN IP address is 192.168.127.254, and the default subnet address is 255.255.255.0.

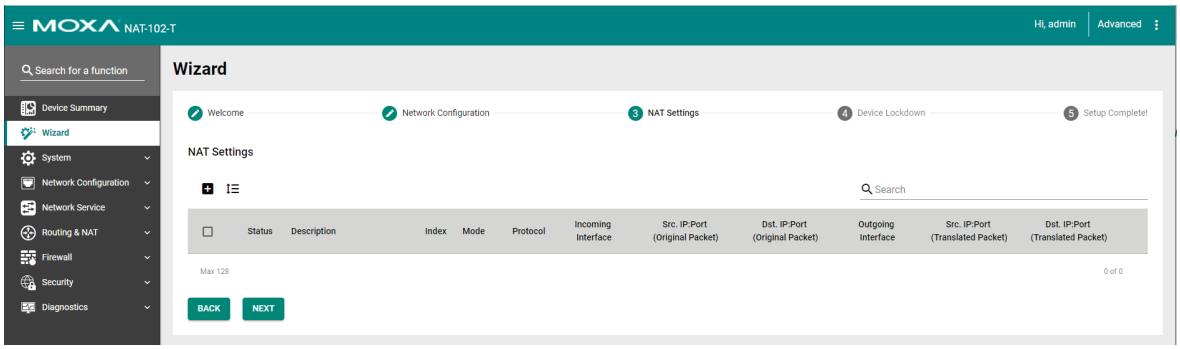
For more detailed instructions, refer to Network Configuration.



Step 3: NAT Settings

Click ⊞ to configure add a NAT rule.

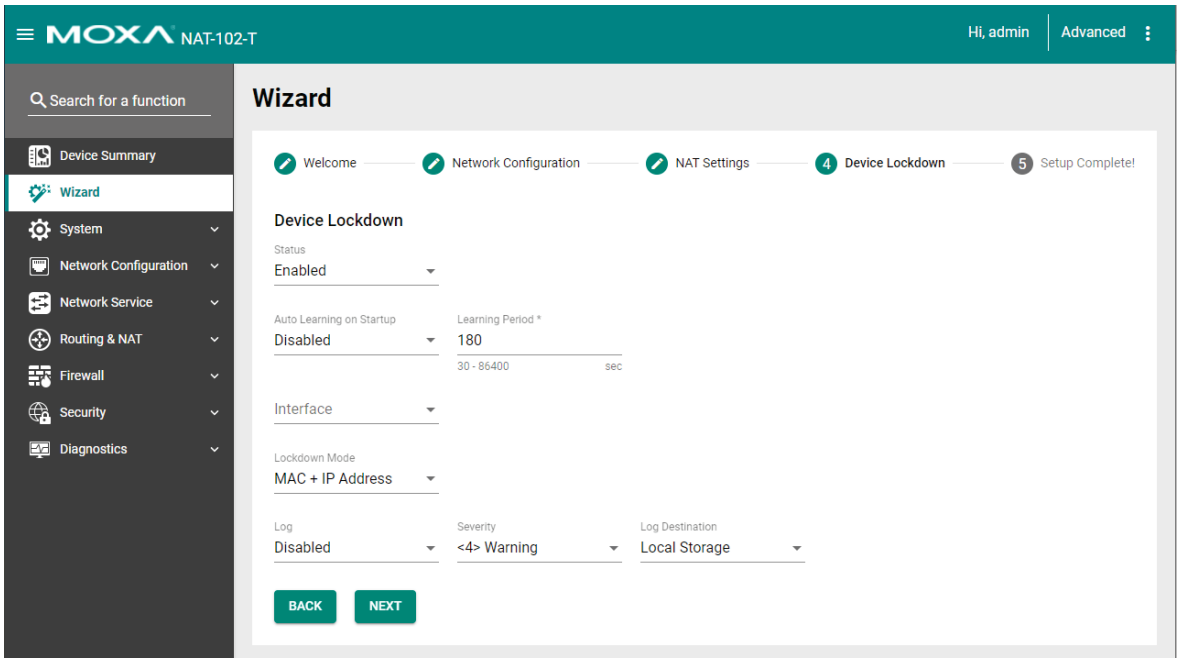
For more detailed instructions, refer to the NAT Settings section in Routing & NAT.



Step 4: Device Lockdown

Enable the device lockdown feature and select which interface you want to lock down, then click **NEXT**.

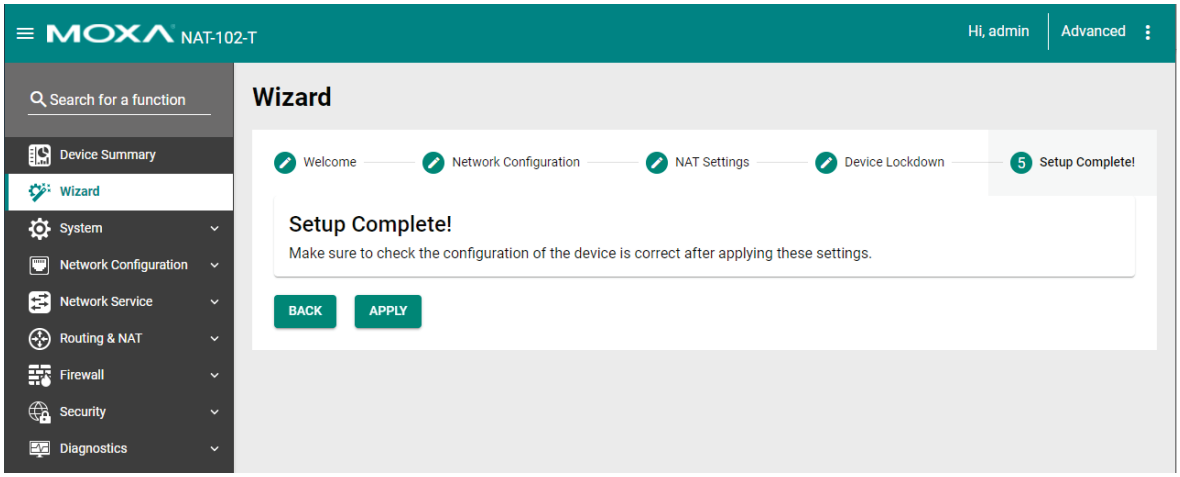
For more detailed instructions, refer to the Device Lockdown section in Security.



Step 5: Setup Complete!

Click **APPLY** to apply all settings and finish the process.

NOTE Any existing configurations will be overwritten by the new settings configured in the Setup Wizard.



4

System

The System section includes the most common settings required by administrators to maintain and control the device.

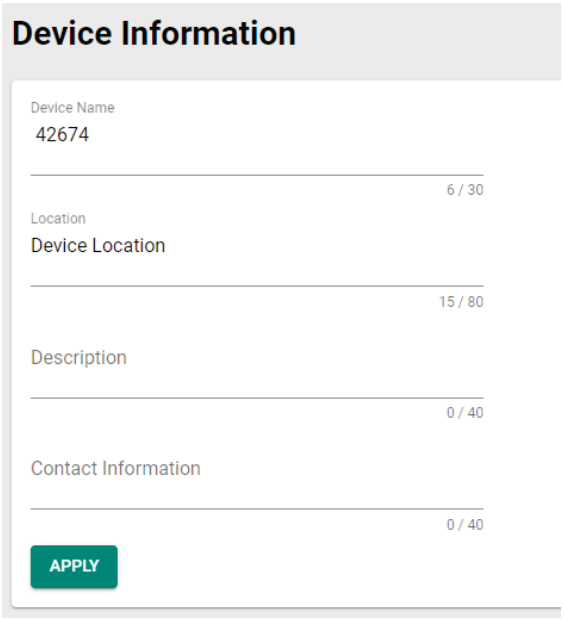
The following topics are covered in this chapter:

- **System Management**
  - Device Information
  - Firmware Upgrade
  - Configuration Backup and Restore
- **Account Management**
  - User Account
  - Password Policy
- **Management Interface**
  - User Interface
- **Time**
  - System Time
  - Time Zone

System Management

Device Information

The **Device Information** screen lets you edit information about the device 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 allows you to more easily identify the role or application of this unit. For example, “Factory NAT Device 1”.	NAT device number

Location

Setting	Description	Factory Default
Max. 80 characters	Enter a location for the device to quickly identify where the device is deployed.	Device Location

Description

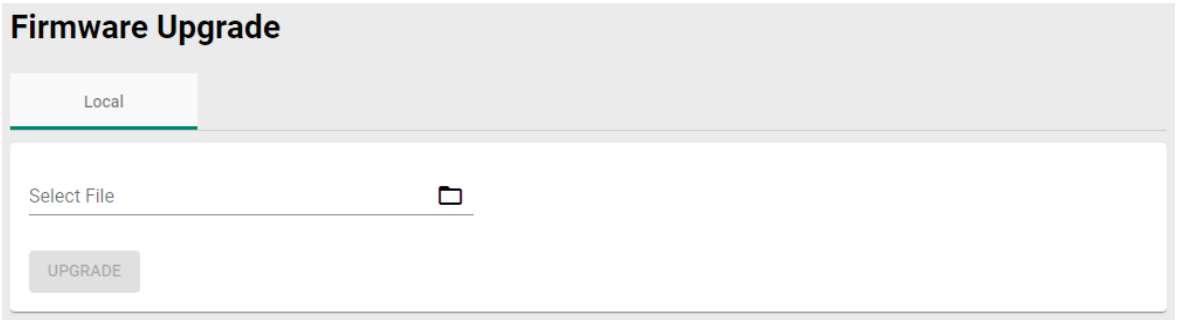
Setting	Description	Factory Default
Max. 40 characters	Enter a description for the device.	None

Contact Information

Setting	Description	Factory Default
Max. 40 characters	Enter the contact information of the person responsible for the device.	None

Firmware Upgrade

Click 🗀 to select a 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.



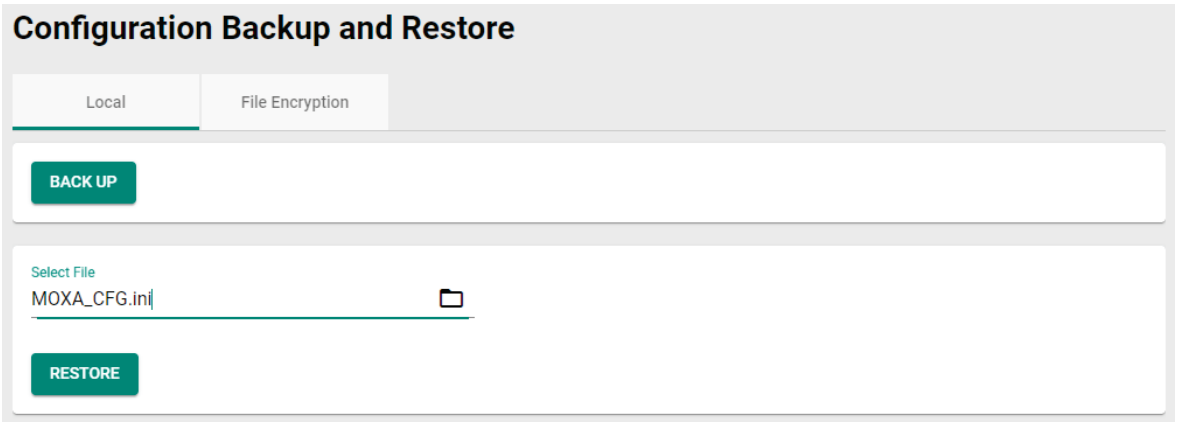
Configuration Backup and Restore

Local

On large-scale networks, administrators need to configure many network devices. This is often a time-consuming and error-prone process. By using **Configuration Backup and Restore**, you can easily duplicate the system configuration of one NAT device to other NAT devices in a short period of time.

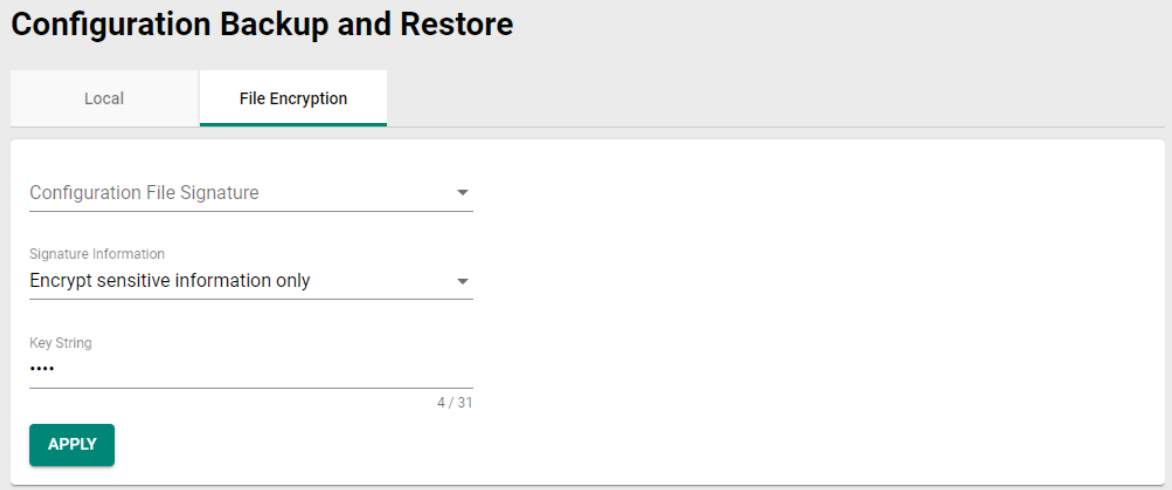
The system configuration, including firewall rules and certificates, only needs to be set up for one device and can then be backed up to a flash drive. You can then use this flash drive to quickly upload these configuration settings to other devices.

Click **BACK UP** button to back up the configuration settings, or click 🗀 to select a configuration backup file from the local host or flash drive and then click **RESTORE** to load the configuration file onto the device.



File Encryption

To export the configuration as an encrypted text-based (command line type) configuration file, select the **Configuration File Signature** and **Signature Information** options and enter an encryption key string, then click **APPLY**. The key string is also used for decrypting when importing an encrypted configuration file.



Configuration File Signature

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable 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.	Encrypt sensitive information only
Encrypt all information	Encrypt all information in the exported configuration.	

Key String

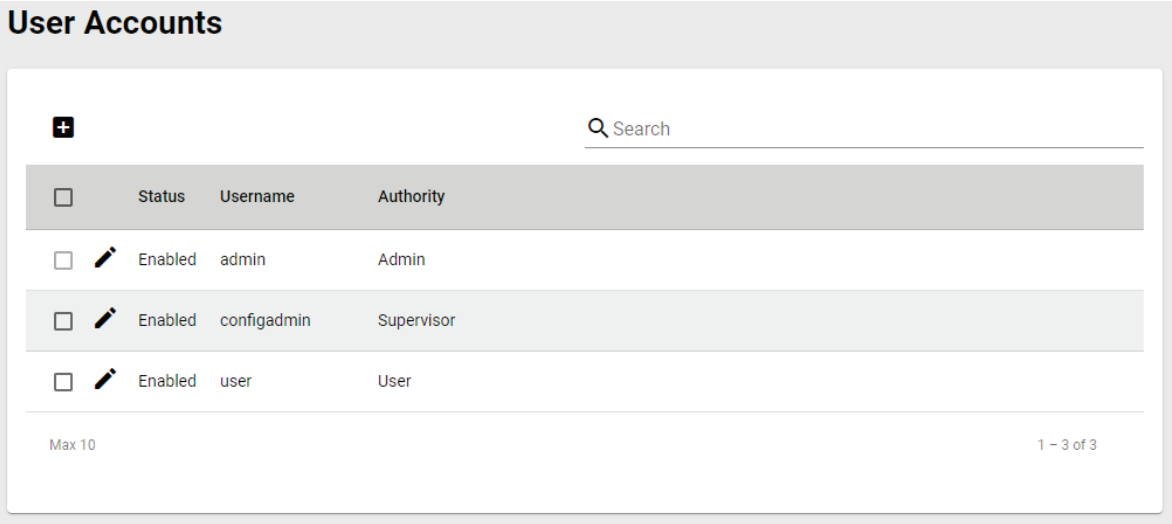
Setting	Description	Factory Default
Max. 31 characters	Enter an encryption key string. This key string is also used to decrypt encrypted configuration files.	moxa

Account Management

User Account

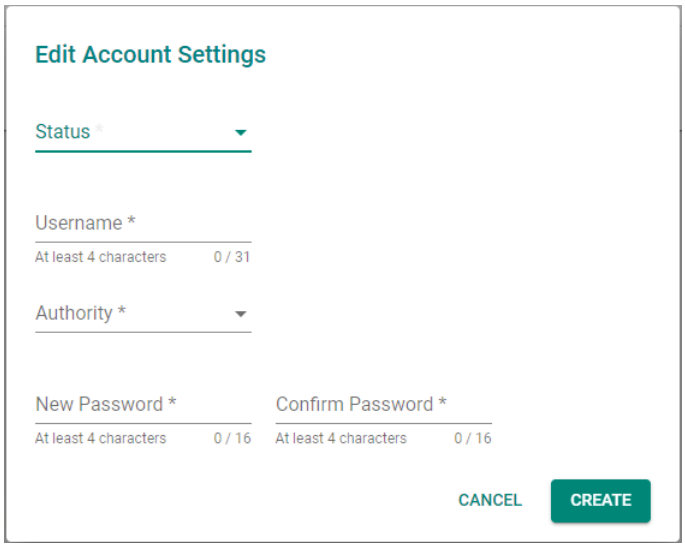
The Moxa Industrial NAT device's account management function allows you to create, manage, modify, and remove user accounts. There are three levels of configuration access, admin, supervisor, and user. The admin accounts have read/write access to all configuration parameters. Supervisors have full editing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

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



Create New Account

Click + 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 NAT device can be accessed by the enabled user.	None
Disabled	The NAT device cannot be accessed by the disabled user.	

Username

Setting	Description	Factory Default
4 to 31 characters	Enter a username for the user 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.	

New Password

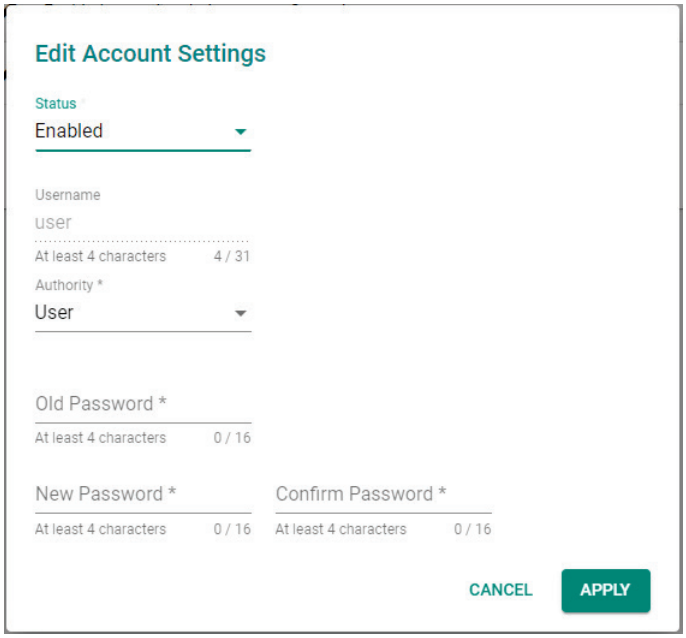
Setting	Description	Factory Default
4 to 16 characters	Enter a password for the user account.	None

Confirm Password

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

Modify Existing Account

Select the existing account from the Account List table and click to modify the account. When you are done modifying the account details, click **APPLY** to save your changes.

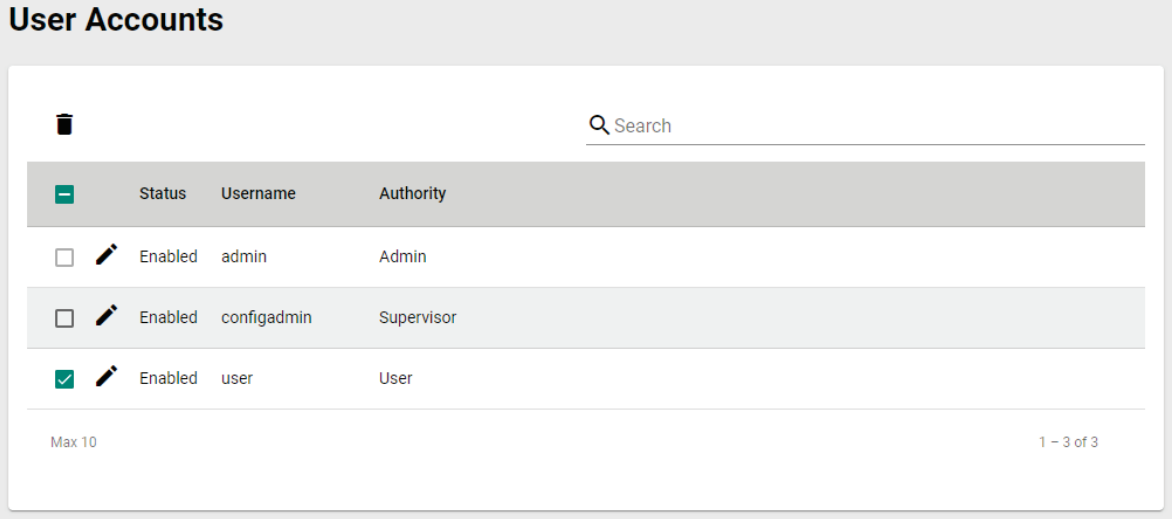


Old Password

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

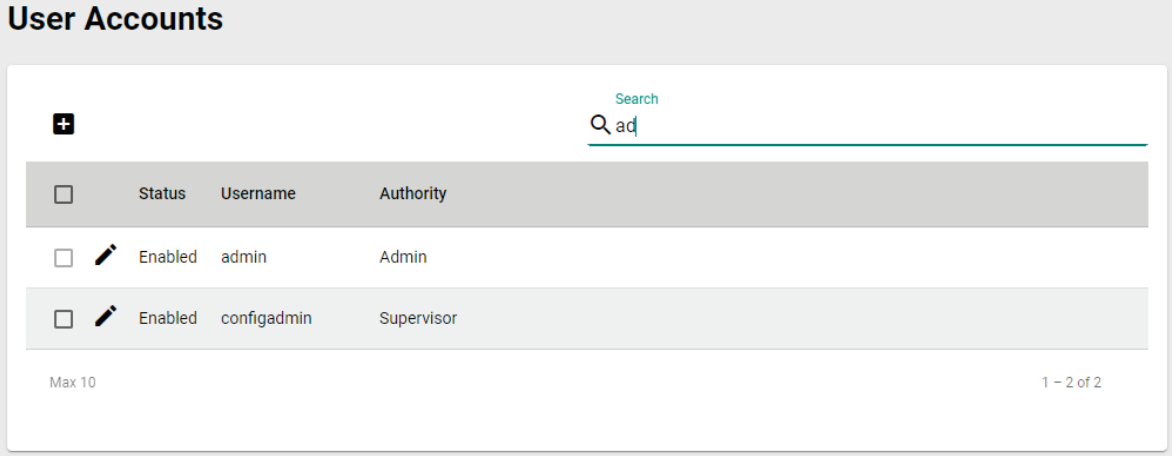
Delete Existing Account

Select the existing account from the Account List table and click to delete the account.



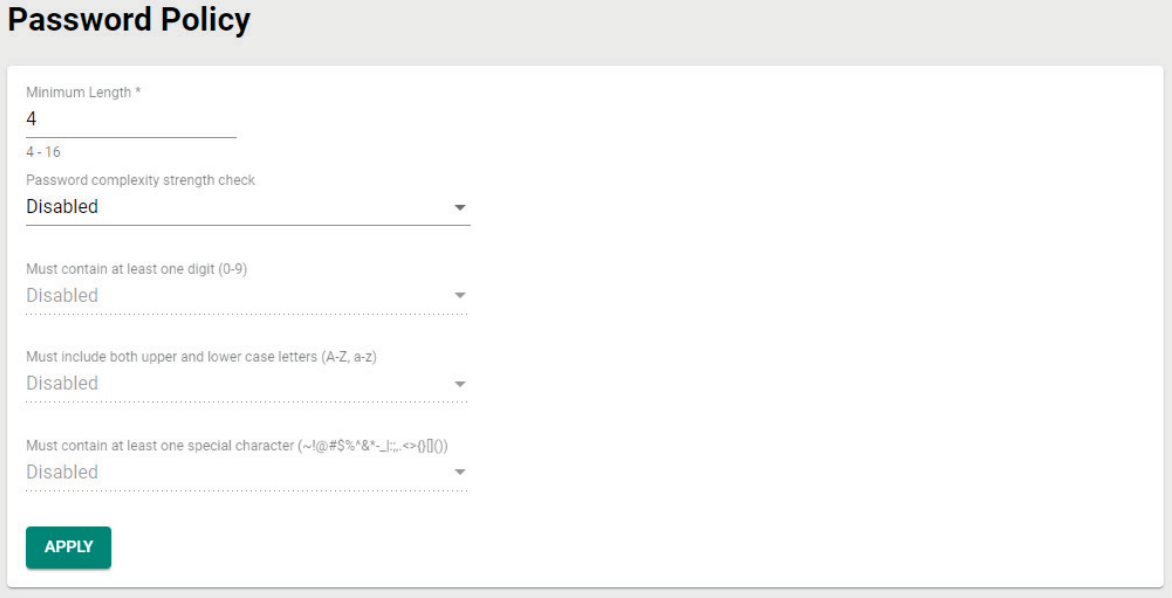
Search Existing Account

Enter the username of the account 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/Disabled	Enable or disable the password complexity strength check.	Disabled

Must contain at least one digit (0-9)

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

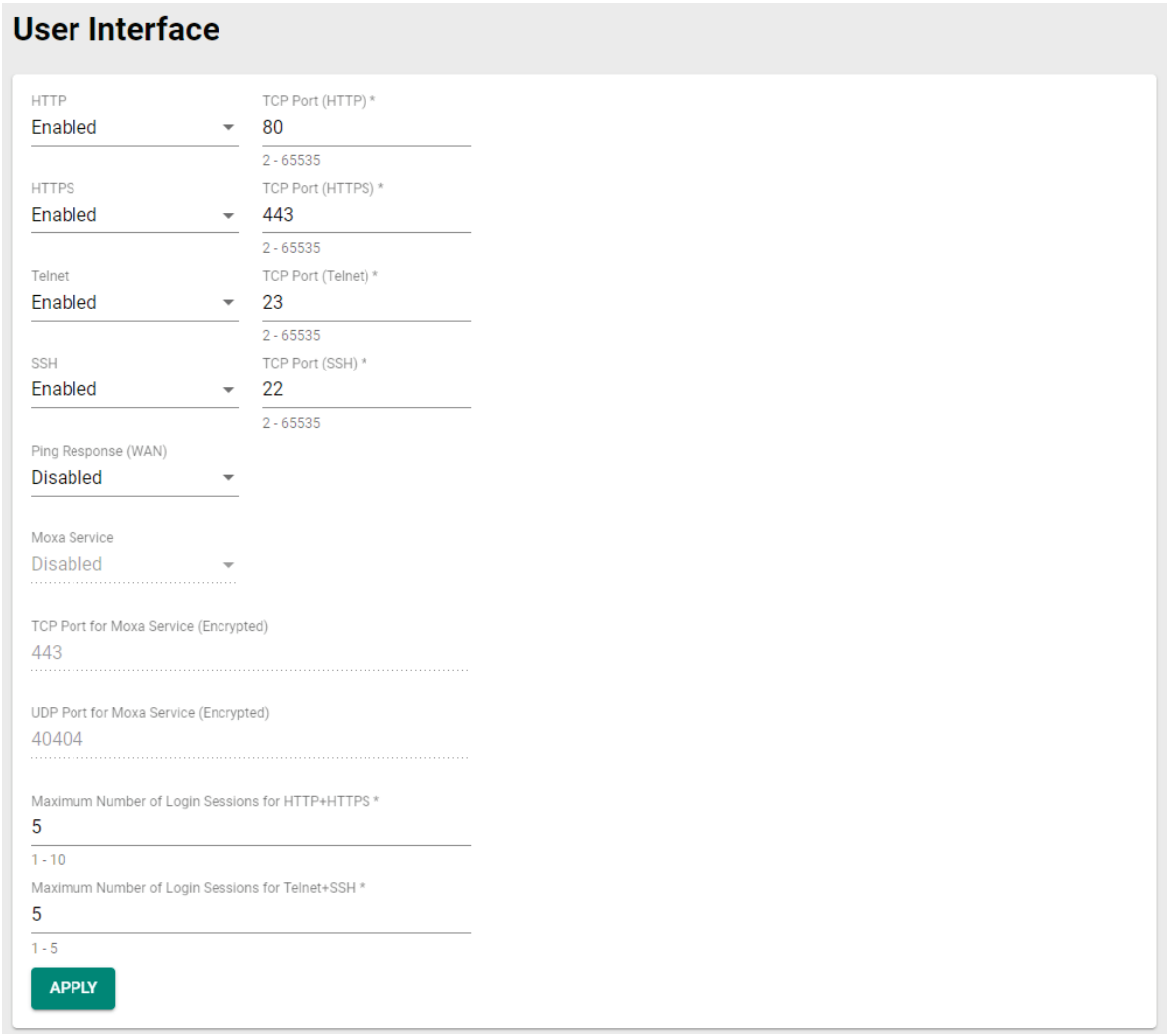
Must contain at least one special character (~!@#$%^&*-_:;,.<>{}[]())

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

Management Interface

From the Management Interface screen, you can manage from which interfaces the device can be accessed.

User Interface



HTTP

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

TCP Port (HTTP)

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

Enable HTTPS

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

TCP Port (HTTPS)

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

Enable Telnet

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

TCP Port (Telnet)

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

Enable SSH

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

TCP Port (SSH)

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

Ping Response (WAN)

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

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

MOXA Service

Setting	Description	Factory Default
Enabled/Disabled	This option will be supported in a future firmware version.	Disabled

TCP Port for Moxa Service (Encrypted)

Setting	Description	Factory Default
2 to 65535	This option will be supported in a future firmware version.	443

UDP Port for Moxa Service (Encrypted)

Setting	Description	Factory Default
2 to 65535	This option will be supported in a future firmware version.	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 NAT device using HTTP and HTTPS. The maximum number of users 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 NAT device using Telnet and SSH. The maximum number of users is 5.	5

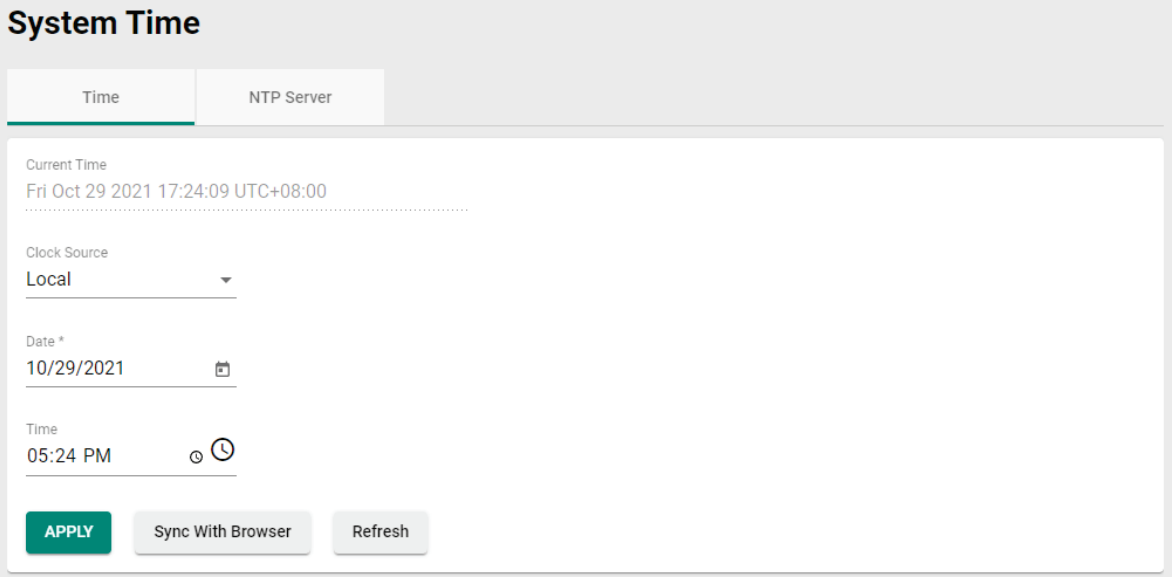
Time

System Time

The Moxa Industrial NAT device's system time can be synced with an NTP 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 NAT device does not feature a real-time clock. If there is no NTP 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 With Browser** to synchronize the device's clock with the browser time. Click **Refresh** to update 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.	

Time Server

Setting	Description	Factory Default
Time server 1/2	If SNTP or NTP is selected as the clock source, specify the time server	None

Date

Setting	Description	Factory Default
Date	Set the date manually.	Current date DD/MM/YYYY

Time

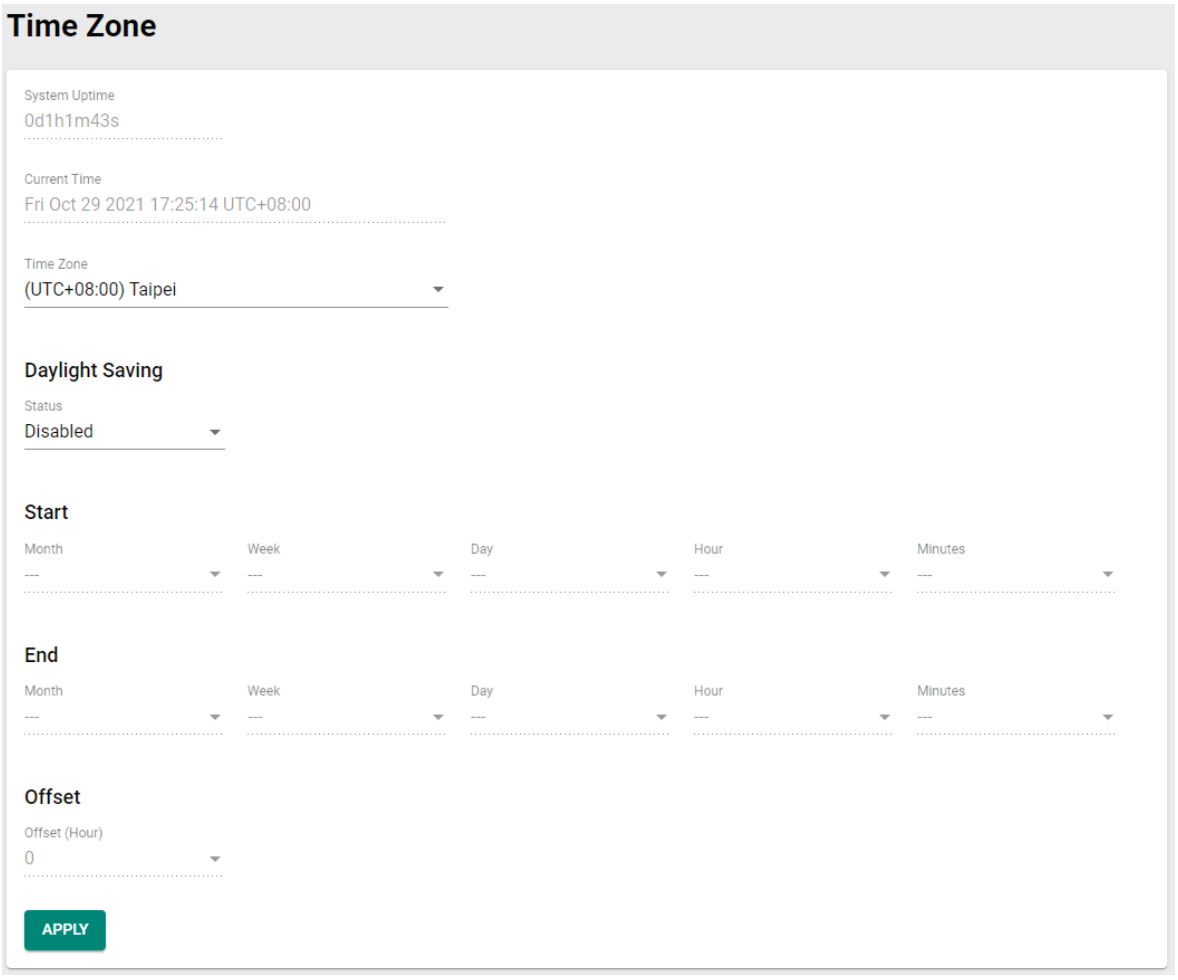
Setting	Description	Factory Default
Time	Set the time manually.	Current time HH:MM AM/PM

NTP Server

NTP Server

Setting	Description	Factory Default
Enabled/Disabled	Enables NTP server functionality for clients.	Disabled

Time Zone



System Uptime

Indicates how long the Moxa NAT device has been online for since the last cold start.

Current Time

Indicates the current date and time.

Time Zone

Setting	Description	Factory Default
Time zone	Specify the time zone, which is used to determine the local time offset from UTC.	UTC

Daylight Saving

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

Status

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

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.	None

Minutes

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

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.	None

Minutes

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

Offset

Offset (Hour)

Setting	Description	Factory Default
User-specified hour	Specify the number of hours that the time should be set forward during Daylight Saving time.	0

NOTE Changing the time zone will automatically correct the current time. Be sure to select the time zone before setting the time.

5

Network Configuration

The following topics are covered in this chapter:

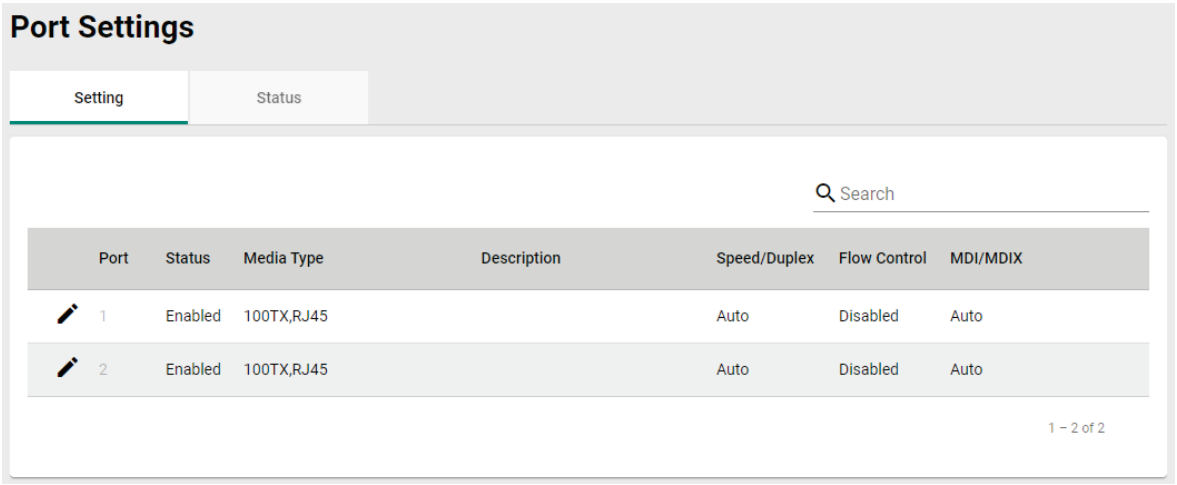
- **Port**
  - Port Settings
- **Layer 2 Switching**
  - VLAN
  - MAC Address Table
- **Layer 3 Interfaces**

Port

Port Settings

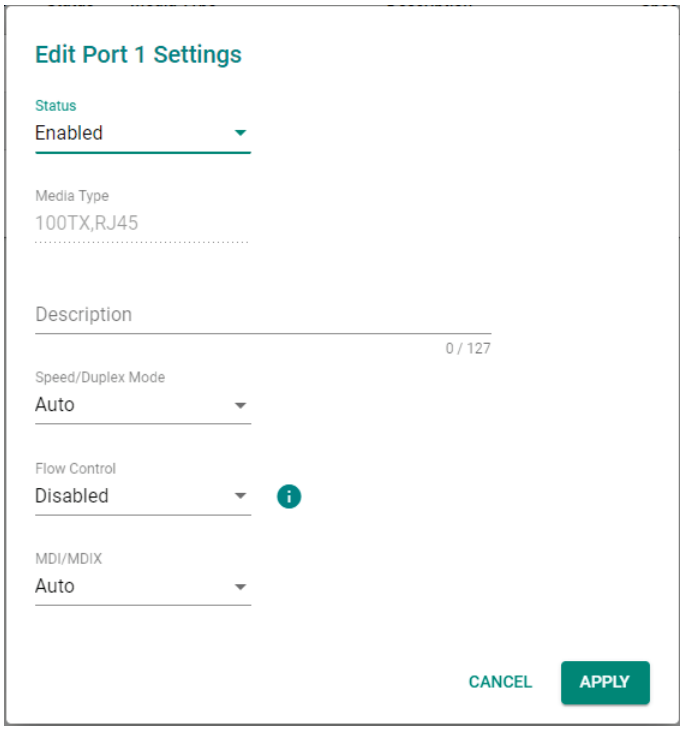
Port settings let you manage port access, port transmission speed, flow control, and port type (MDI or MDIX). The NAT-102 Series has two RJ45 Ethernet ports.

Setting



Modify Port Settings

Click ✎ to modify the settings of the corresponding port.



Status

Setting	Description	Factory Default
Enabled	Allows data transmission through the port.	Enabled
Disabled	Disables the port.	

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	Specifies an alias for the port to help administrators differentiate between different ports. Example: PLC 1	None

Speed

Setting	Description	Factory Default
Auto	Allows 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 devices will determine the best speed for that connection.	Auto
100M-Full	Select a fixed speed and duplex mode if the connected Ethernet device has trouble auto-negotiating the line speed.	
100M-Half		
10M-Full		
10M-Half		

Flow Control

This 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 NAT-102 and the connected Ethernet device.

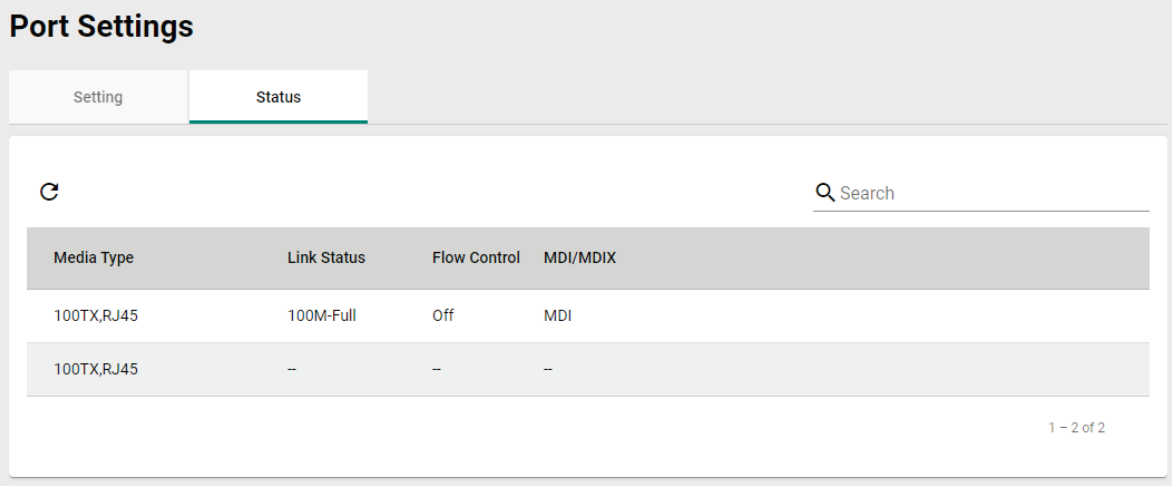
Setting	Description	Factory Default
Enable	Enables flow control for this port when the port's Speed is set to Auto.	Disabled
Disable	Disables flow control.	

MDI/MDIX

Setting	Description	Factory Default
Auto	Allows 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 for port type.	
MDIX		

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

VLAN

The VLAN section is used for configuring VLAN functionality for the NAT-102's ports.

Using Virtual LAN

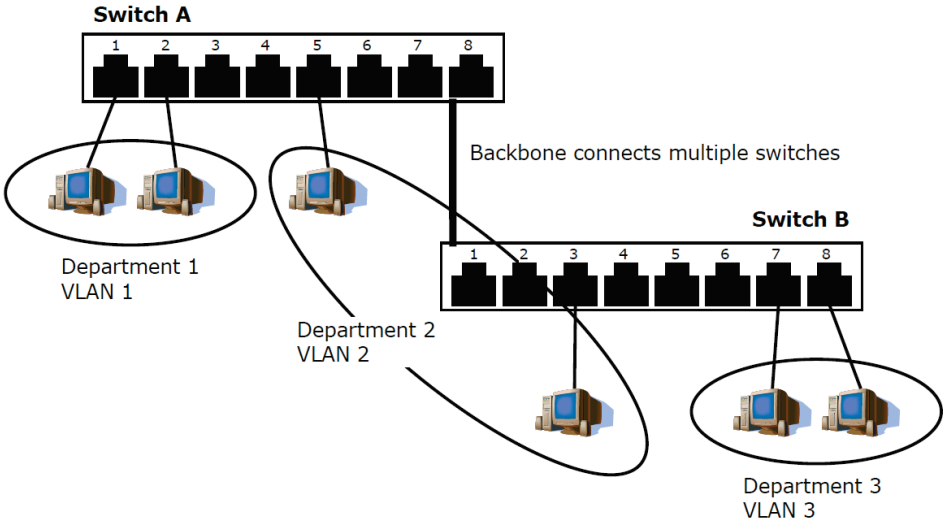
Setting up Virtual LANs (VLANs) on your Moxa Industrial NAT device increases the efficiency of your network by dividing the LAN into logical segments, as opposed to physical segments. In general, VLANs are easier to manage.

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.

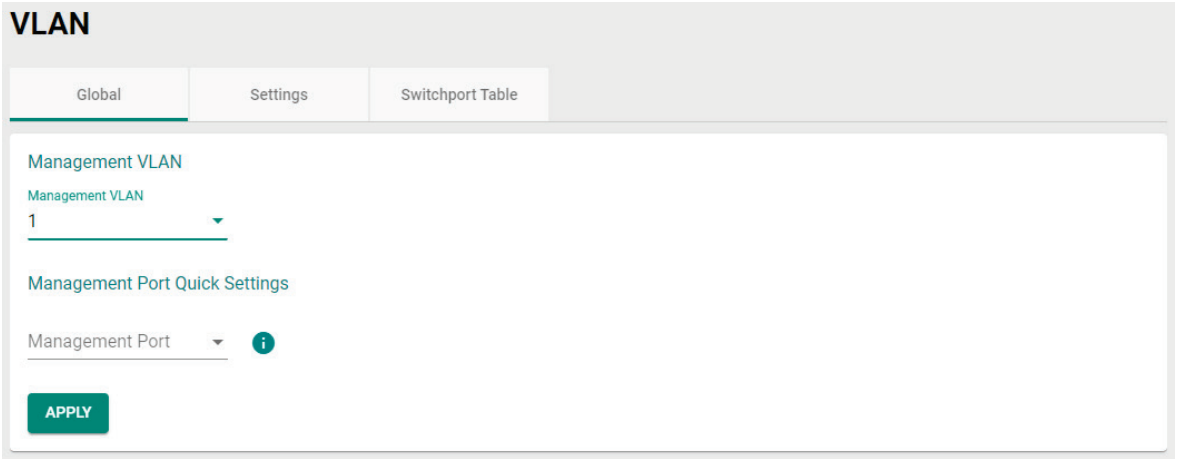
Managing a VLAN

A new or initialized Moxa Industrial NAT device contains a single VLAN—the Default VLAN. This VLAN has the following definition:

- **VLAN Name**—Management VLAN
- **Management Port**—1 (if tagging is required)

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 NAT device over the network.

Global



Management VLAN

Management VLAN

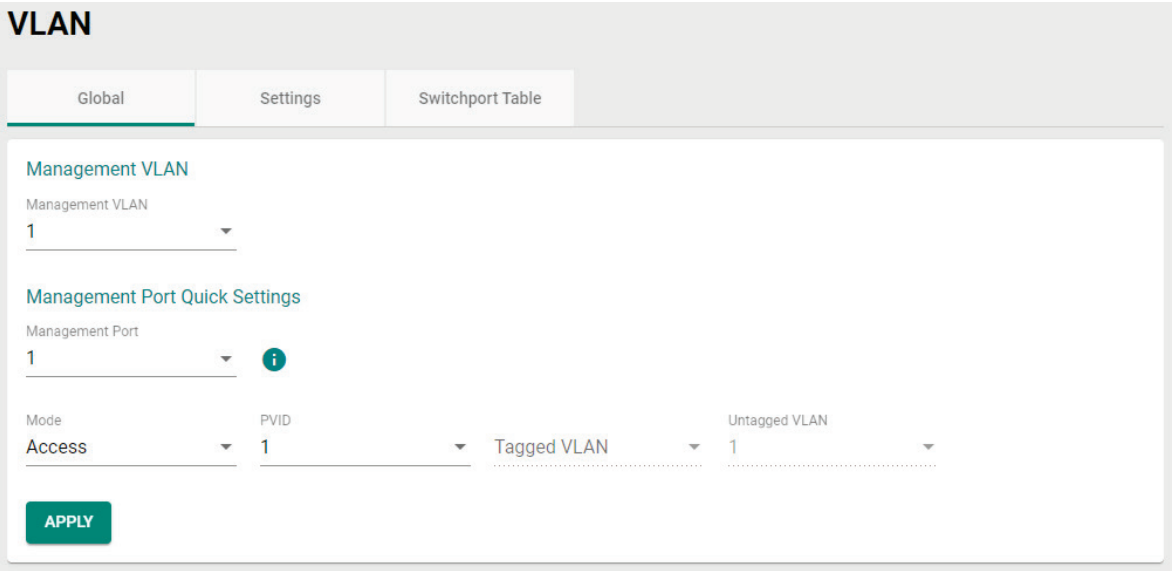
Setting	Description	Factory Default
1, 2	Select the VLAN ID of this Moxa NAT device.	1

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, 2	Select the management port of this Moxa NAT device. 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	Select the Access port type to connect single devices without tags.	Access
Trunk	Select the Trunk port type to connect another 802.1Q VLAN aware NAT device.	
Hybrid	Select Hybrid port to connect another Access 802.1Q VLAN aware NAT device or another LAN that combines tagged and/or untagged devices and/or other NAT devices/hubs.	

PVID

Setting	Description	Factory Default
1, 2	Set the default VLAN ID for untagged devices that connect to the port.	1

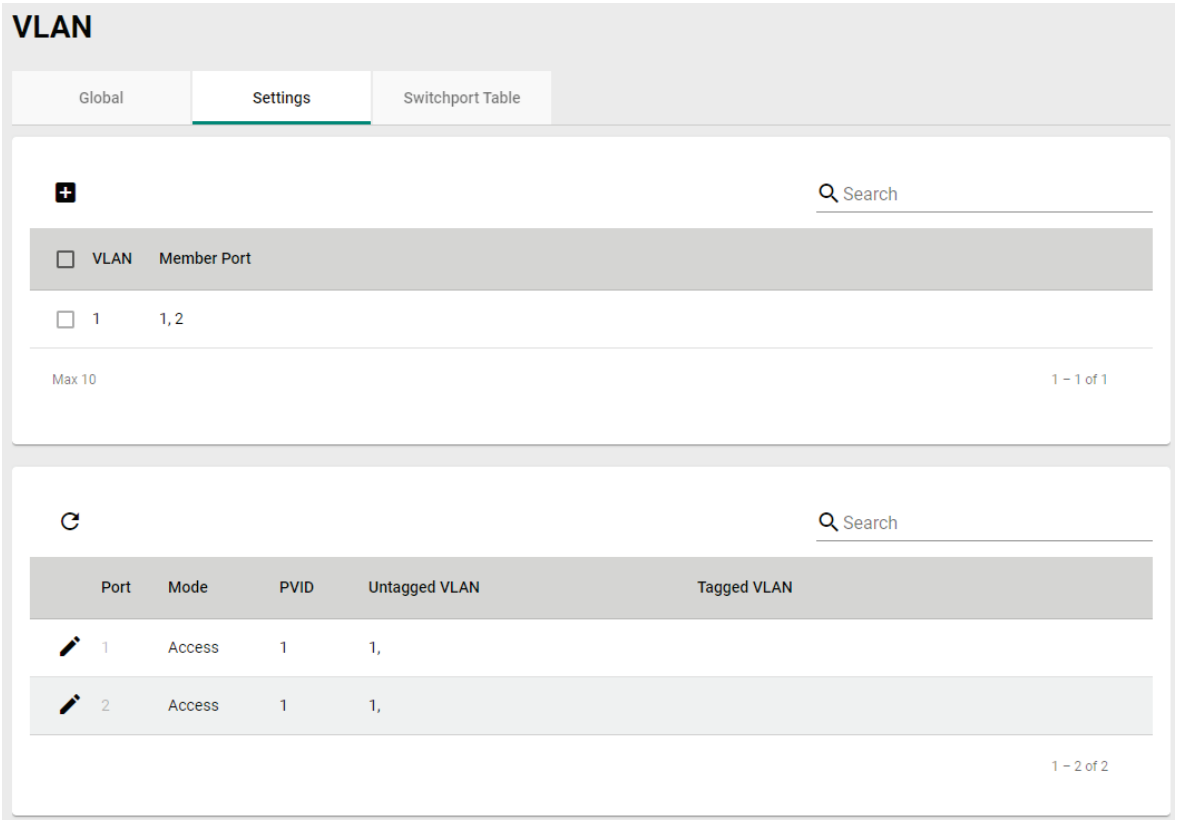
Tagged VLAN

Setting	Description	Factory Default
All Member VIDs, 1, 2	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.	1

Untagged VLAN

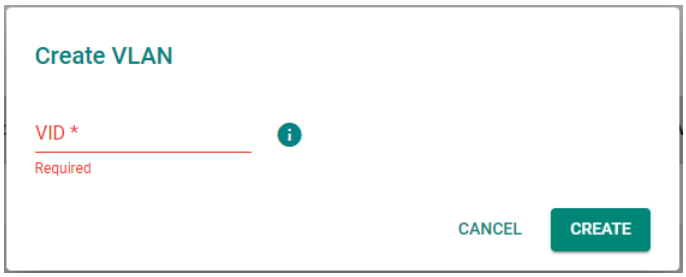
Setting	Description	Factory Default
All Member VIDs, 1, 2	If the Mode is set to Trunk or Hybrid, set the other VLAN ID for tagged devices that connect to the port and tags that need to be removed in egress packets. Use commas to separate different VIDs.	None

Settings



Create a VLAN

Click ⊞ to create a VLAN.

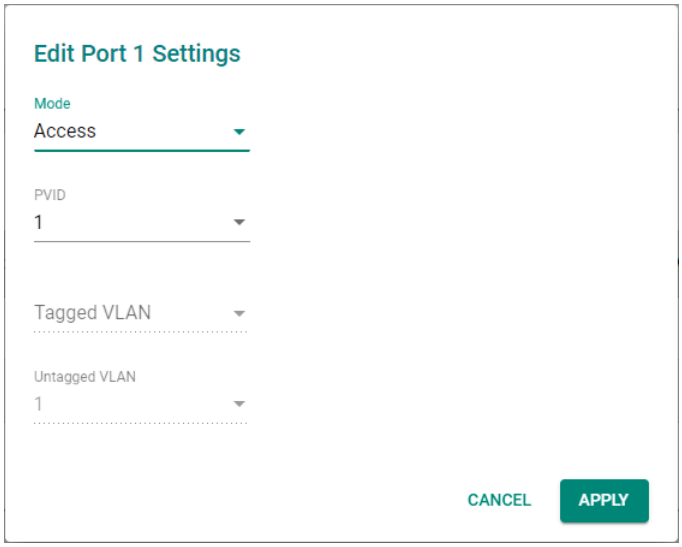


VID

Setting	Description	Factory Default
VLAN ID	Enter 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

Modify an Existing VLAN

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



Mode

Setting	Description	Factory Default
Access	Select the Access port type to connect single devices without tags.	Access
Trunk	Select the Trunk port type to connect another 802.1Q VLAN aware NAT device.	
Hybrid	Select Hybrid port to connect another Access 802.1Q VLAN aware NAT device or another LAN that combines tagged and/or untagged devices and/or other NAT devices/hubs.	

PVID

Setting	Description	Factory Default
1, 2	Set the default VLAN ID for untagged devices that connect to the port.	1

Tagged VLAN

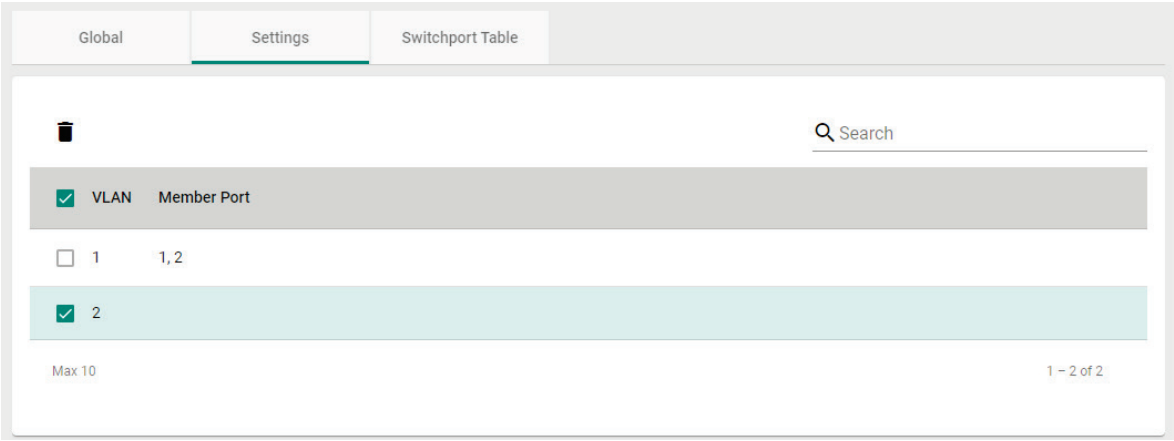
Setting	Description	Factory Default
All Member VIDs, 1, 2	If the Mode is set to Trunk or Hybrid, set the other VLAN ID for tagged devices that connect to the port. Use commas to separate different VIDs.	1

Untagged VLAN

Setting	Description	Factory Default
All Member VIDs, 1, 2	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.	None

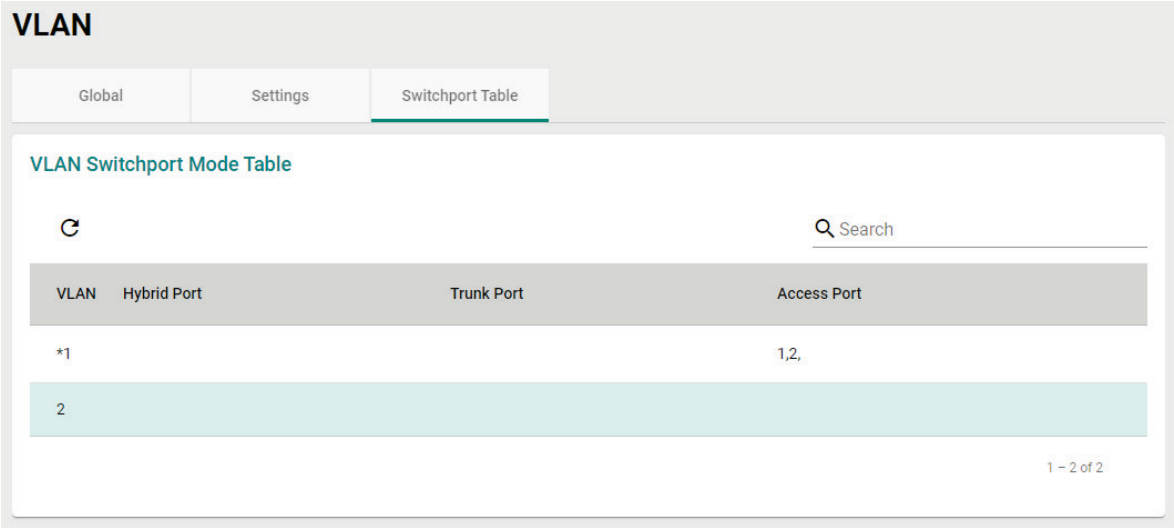
Delete a VLAN

Select the VLAN from the list and click to delete it.



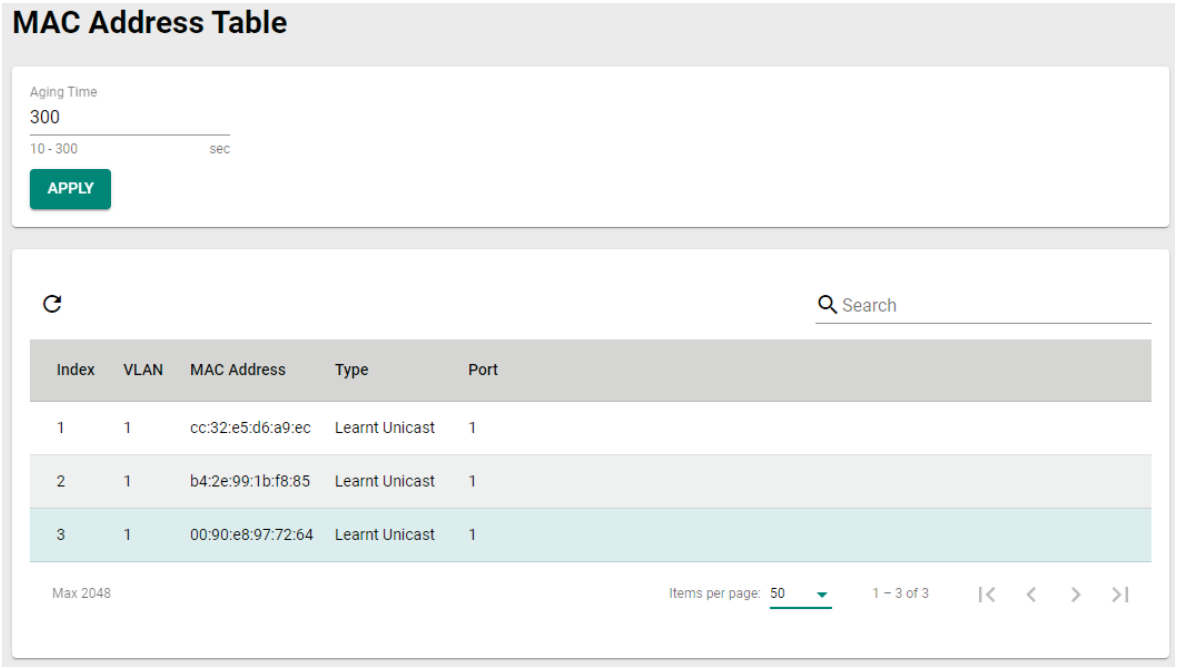
Switchport Table

From the **VLAN Switchport Mode Table**, you can review created VLAN groups, joined Access, Trunk and Hybrid ports.



MAC Address Table

The MAC address table shows the MAC address list of devices that have passed through the Moxa Industrial NAT device. The Aging Time indicates how the long the MAC address remains stored in the device before it is removed from the list. Once a MAC address is removed, the NAT device will no longer forward frames originating from this MAC address.



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

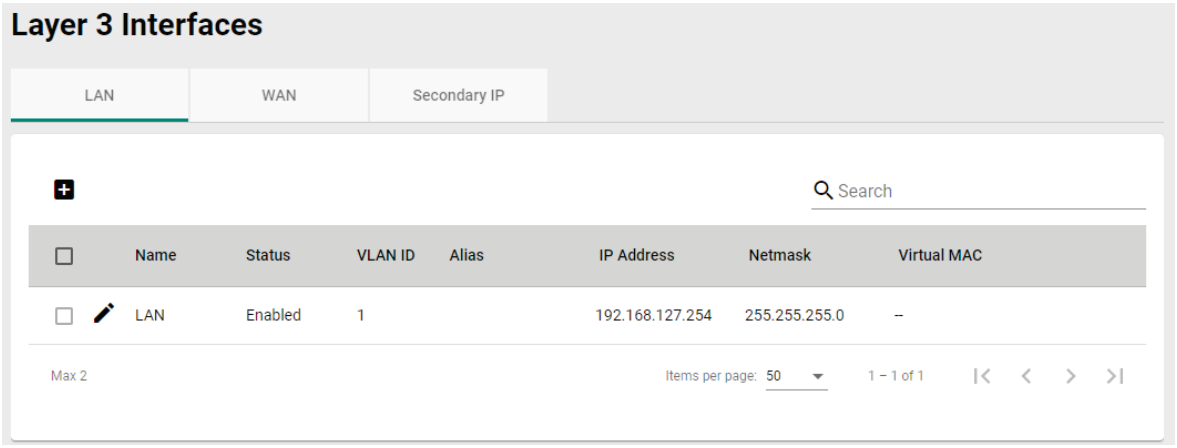
Learnt Unicast	Show all learnt Unicast MAC addresses.
Static	Show all Static, Static Lock, and Static Multicast MAC addresses.
Multicast	Show all Static Multicast MAC addresses.
Port x	Show all MAC addresses associated with a specific port.

The table displays the following information:

VLAN	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.

Layer 3 Interfaces

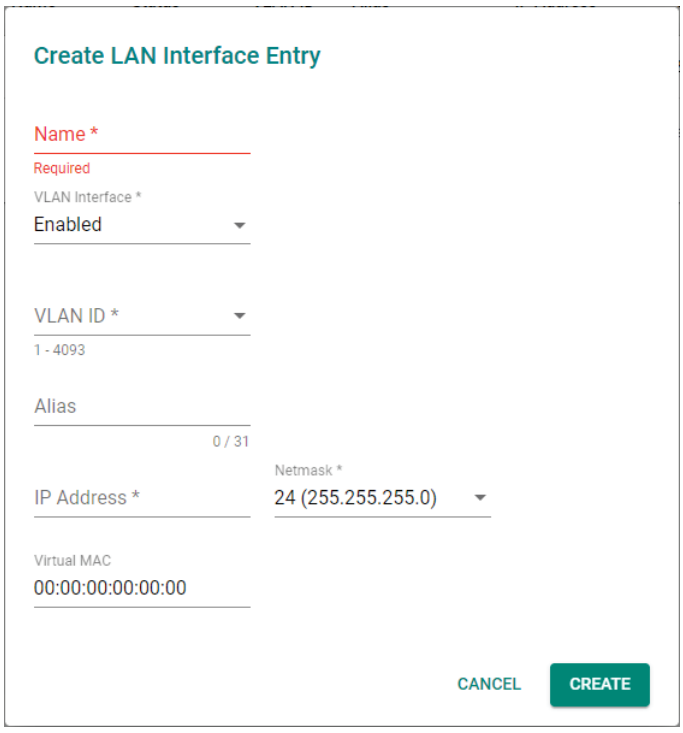
LAN



Create a LAN Interface

Click ⊞ to create a LAN Interface.

Enter the name of the LAN interface, set VLAN Interface to Enabled, select a VLAN ID that is already configured in the Layer 2 VLAN settings, and assign an Alias, IP address, Netmask, and Virtual MAC Address for the interface. Click **CREATE** to activate this interface.



Name

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

VLAN Interface

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

VLAN ID

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

Alias

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

IP Address

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

Netmask

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

Virtual MAC

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

Delete a LAN Interface

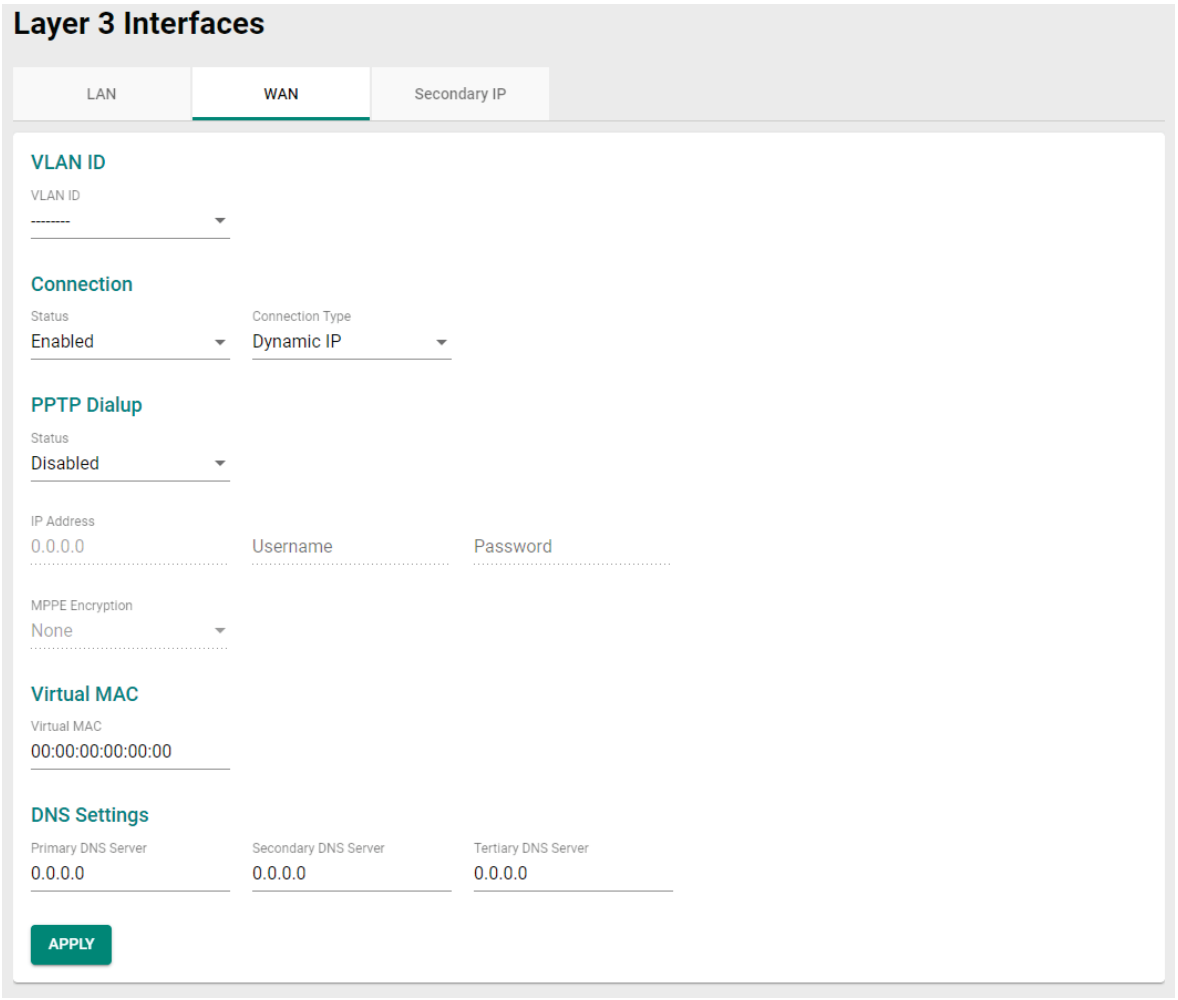
Select the entry from the LAN Interface List and click to delete it.

Modify a LAN Interface

Click to modify the attributes and click **APPLY** button to change the configuration.

NOTE You can create up to 10 LAN interfaces by configuring each port with unique VLAN ID numbers.

WAN



VLAN ID

VLAN ID

The Moxa Industrial NAT device's WAN interface is VLAN-based. All ports associated with the selected VLAN ID will act as a single WAN interface.

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

Connection

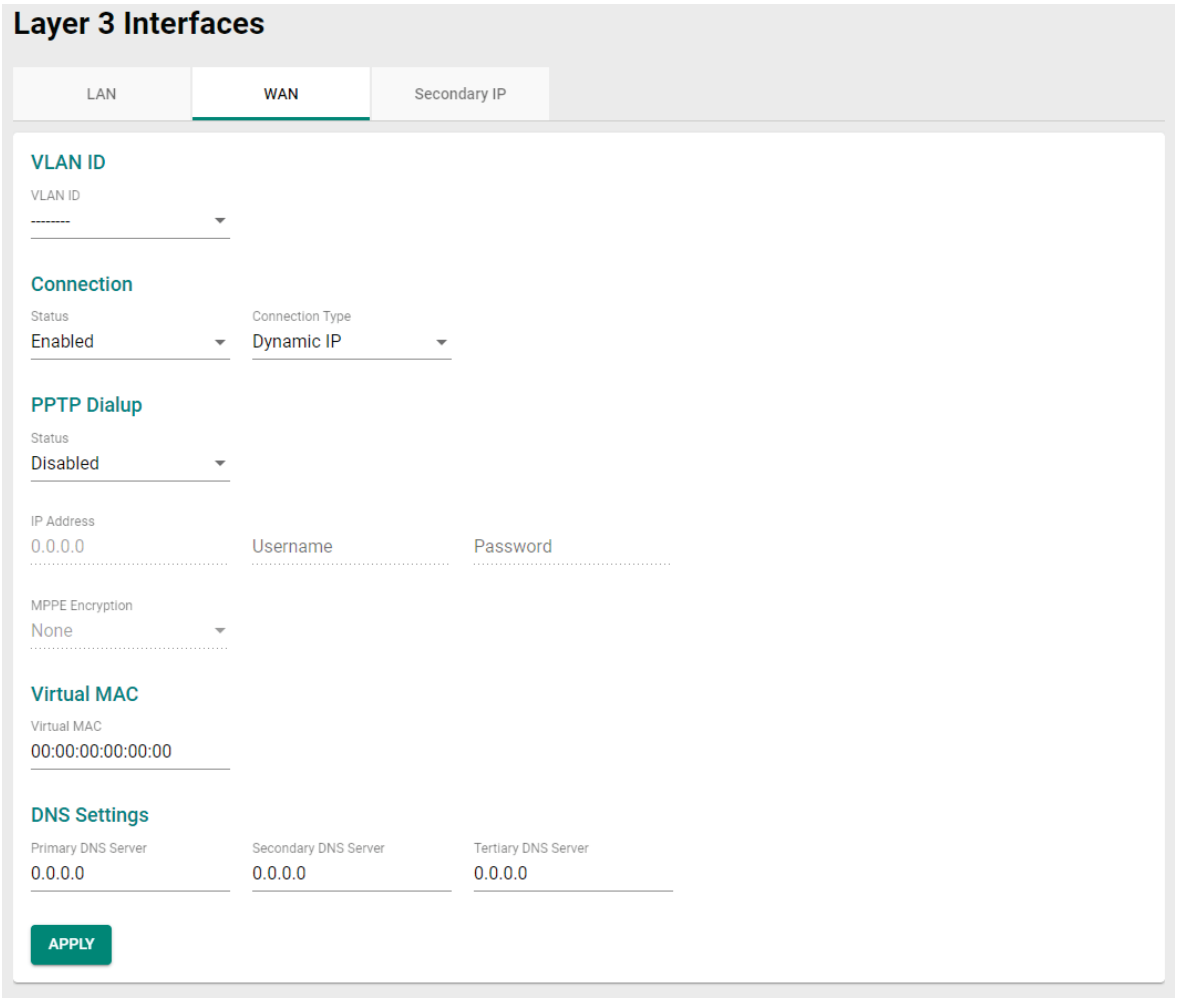
Status

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

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, Static IP, and PPPoE.	Dynamic IP

Dynamic IP Connections



PPTP Dialup

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

Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the PPTP connection.	Disabled

IP Address

Setting	Description	Factory Default
IP Address	The PPTP service IP address.	0.0.0.0

Username

Setting	Description	Factory Default
Max. 30 Characters	The username used to dial in to the PPTP service.	None

Password

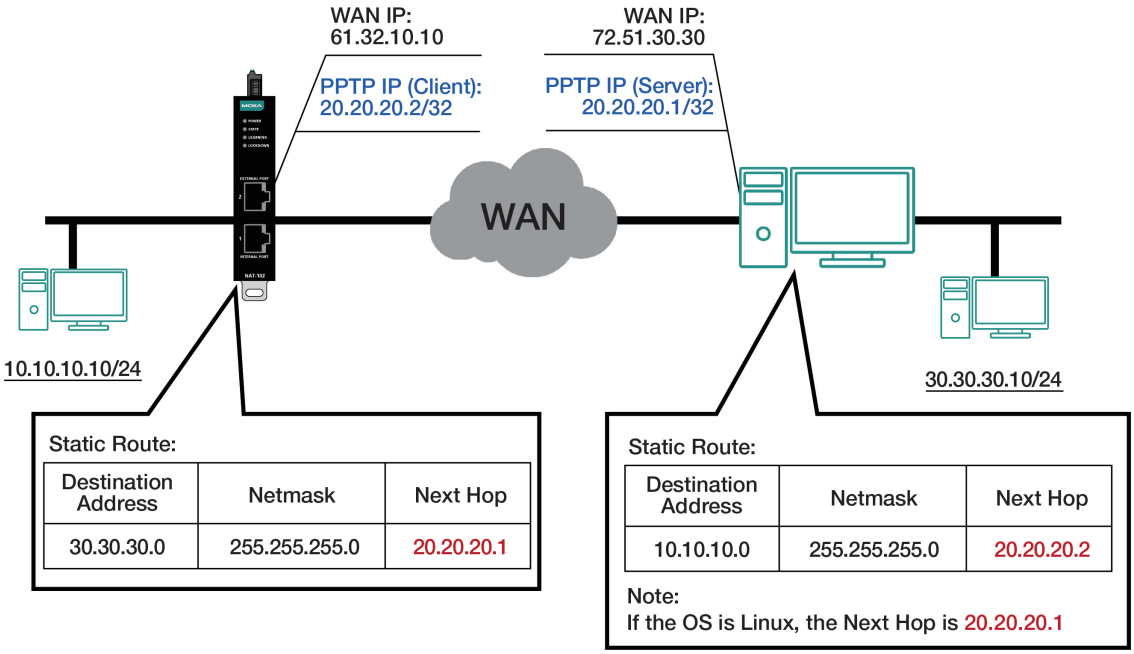
Setting	Description	Factory Default
Max. 30 characters	The password used to dial in to the PPTP service.	None

MPPE Encryption

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

Example

Suppose 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 for 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	The virtual MAC address.	None

DNS Settings

Primary DNS Server

Setting	Description	Factory Default
IP Address	The primary DNS IP address.	0.0.0.0

Secondary DNS Server

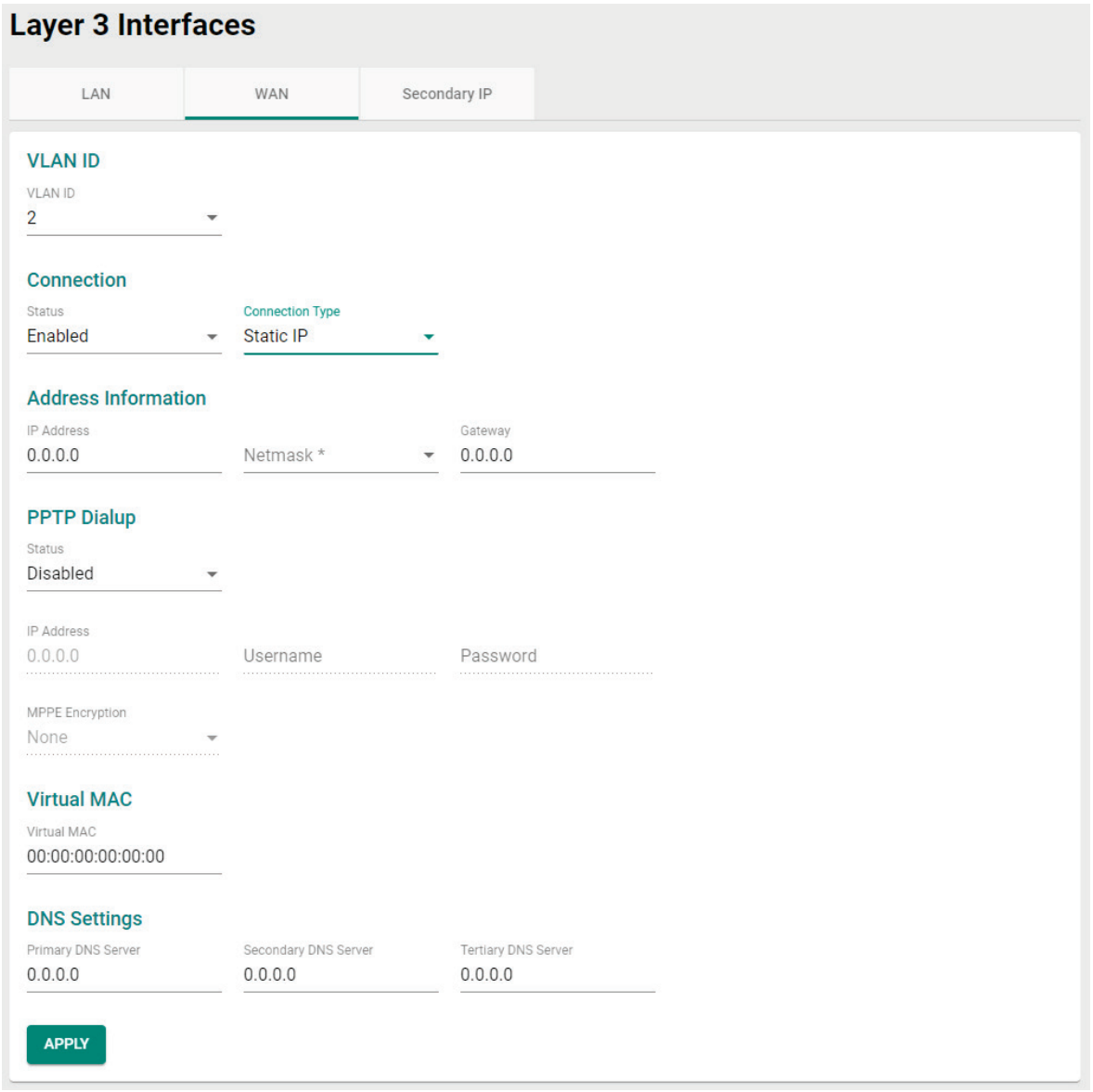
Setting	Description	Factory Default
IP Address	The secondary DNS IP address.	0.0.0.0

Tertiary DNS Server

Setting	Description	Factory Default
IP Address	The tertiary DNS IP address.	0.0.0.0

NOTE The priority of a manually configured DNS will be higher than the DNS from the PPPoE or DHCP server.

Static IP Connections



Address Information

IP Address

Setting	Description	Factory Default
IP Address	The interface IP address.	0.0.0.0

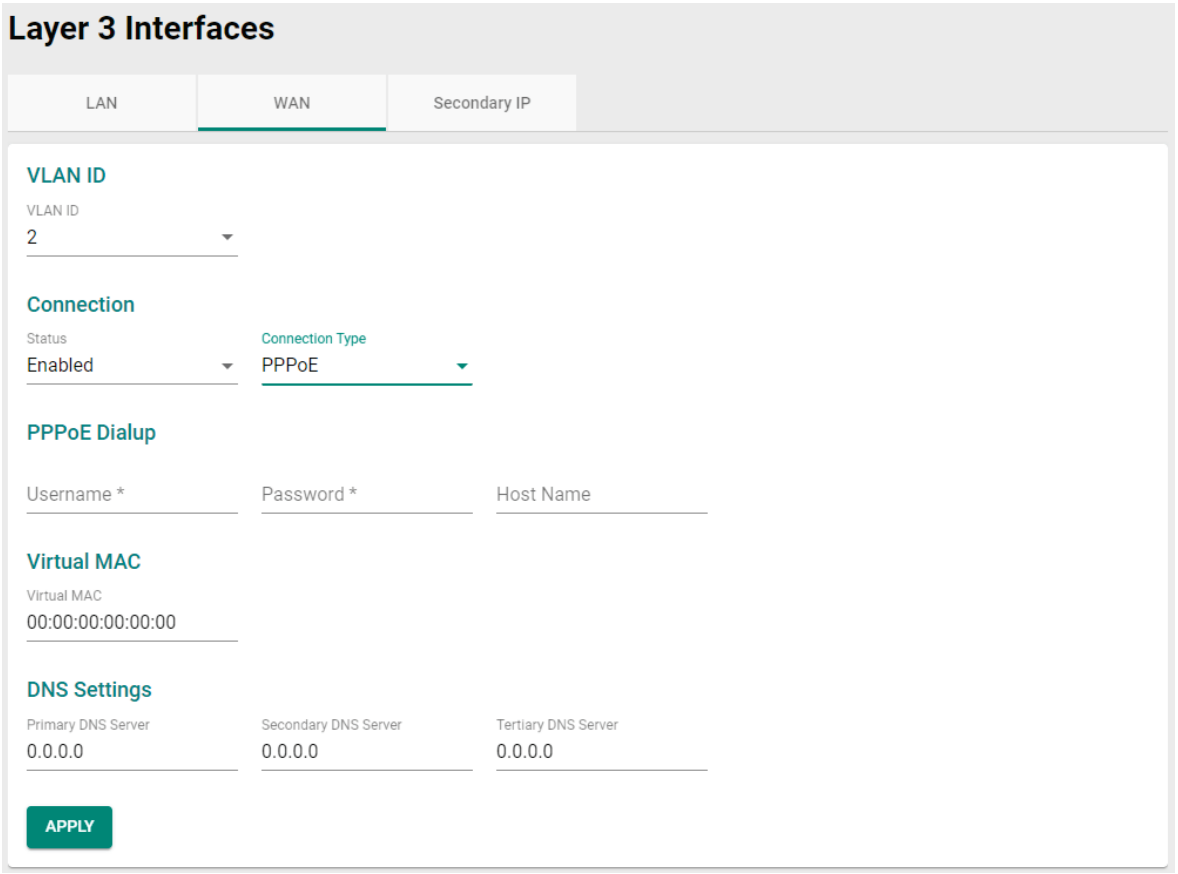
Netmask

Setting	Description	Factory Default
IP Address	The subnet mask.	None

Gateway

Setting	Description	Factory Default
IP Address	The gateway IP address.	0.0.0.0

PPPoE Connections



PPPoE Dialup

Username

Setting	Description	Factory Default
Max. 30 characters	The username used to log into the PPPoE server.	None

Password

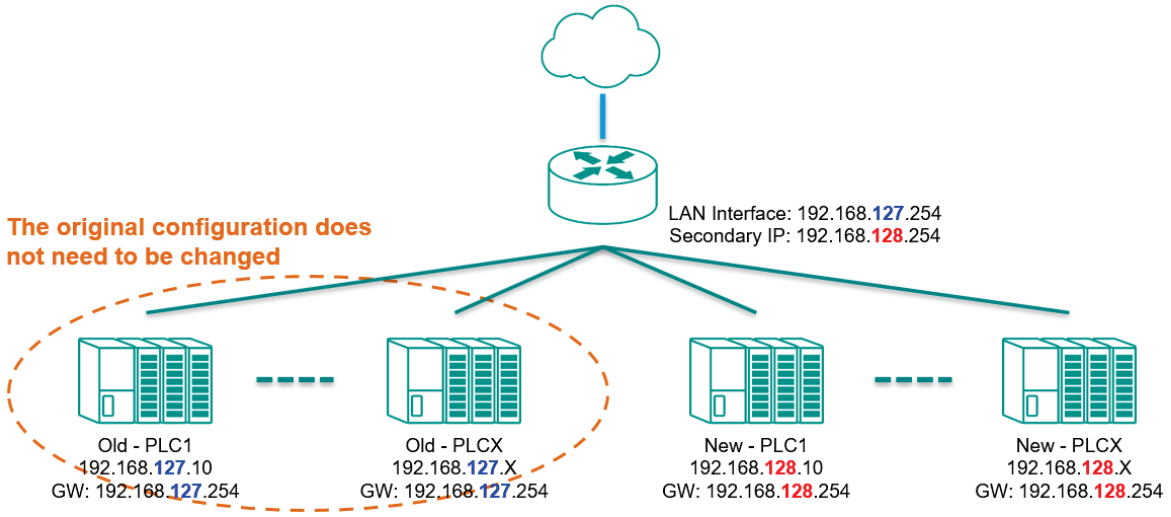
Setting	Description	Factory Default
Max. 30 characters	The password used to log into the PPPoE server.	None

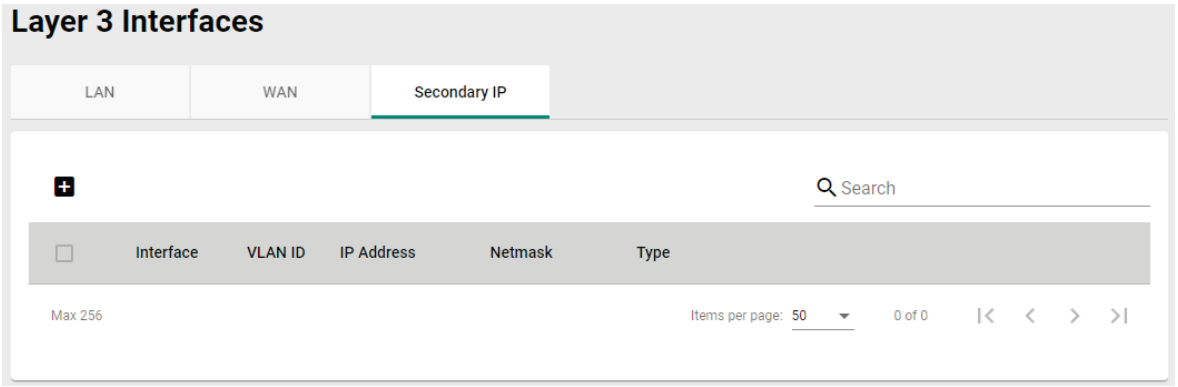
Host Name

Setting	Description	Factory Default
Max. 30 characters	The user-defined host name of the PPPoE server.	None

Secondary IP

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

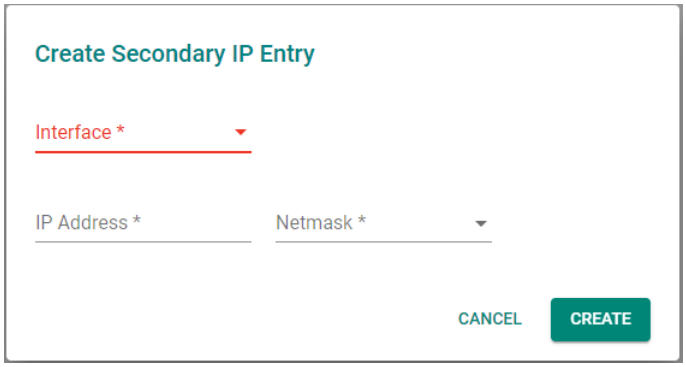




Create a Secondary IP

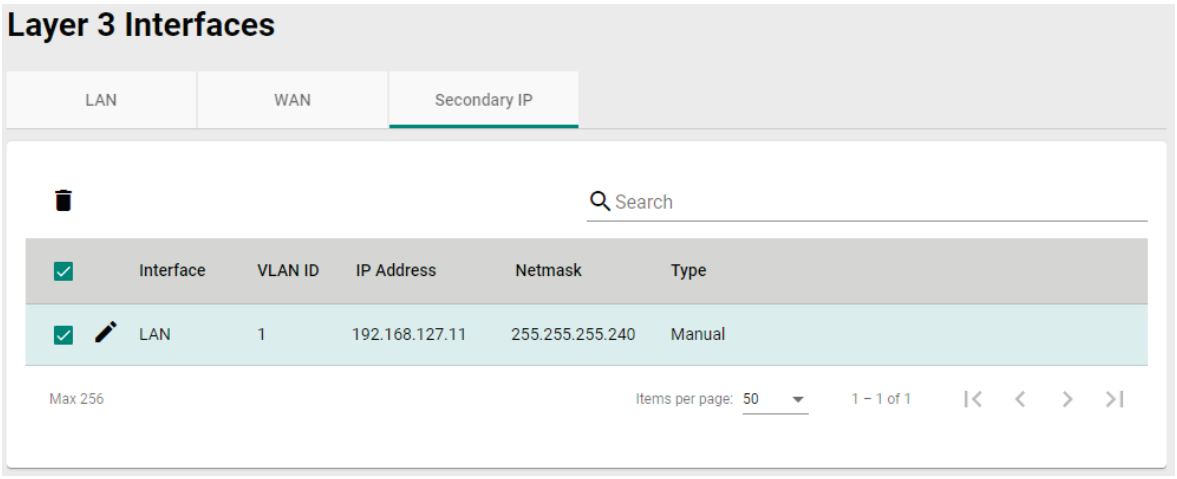
Click ⊞ to create a secondary IP.

Select the interface and assign an IP address and subnet mask for the interface. Click **CREATE** to activate this 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 attributes and click **APPLY** to change the configuration.

6

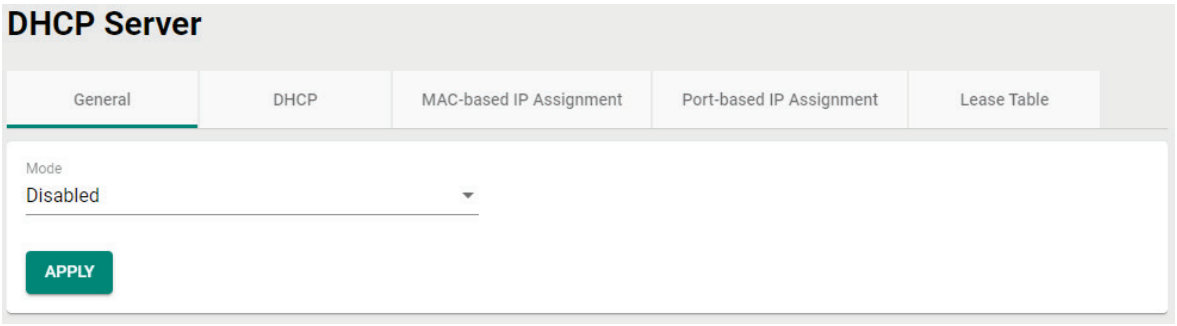
Network Service

The following topics are covered in this chapter:

- **DHCP Server**
  - General
  - DHCP
  - MAC-based IP Assignment
  - Port-based IP Assignment
  - Lease Table

DHCP Server

General

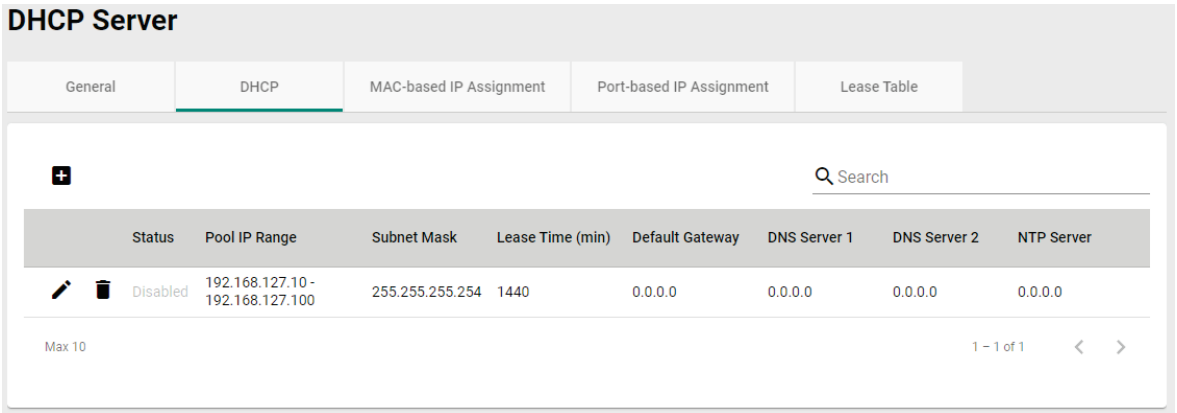


Mode

Setting	Description	Factory Default
Disabled, DHCP/MAC-based assignment, Port-based IP assignment	Select the DHCP Server Mode.	Disabled

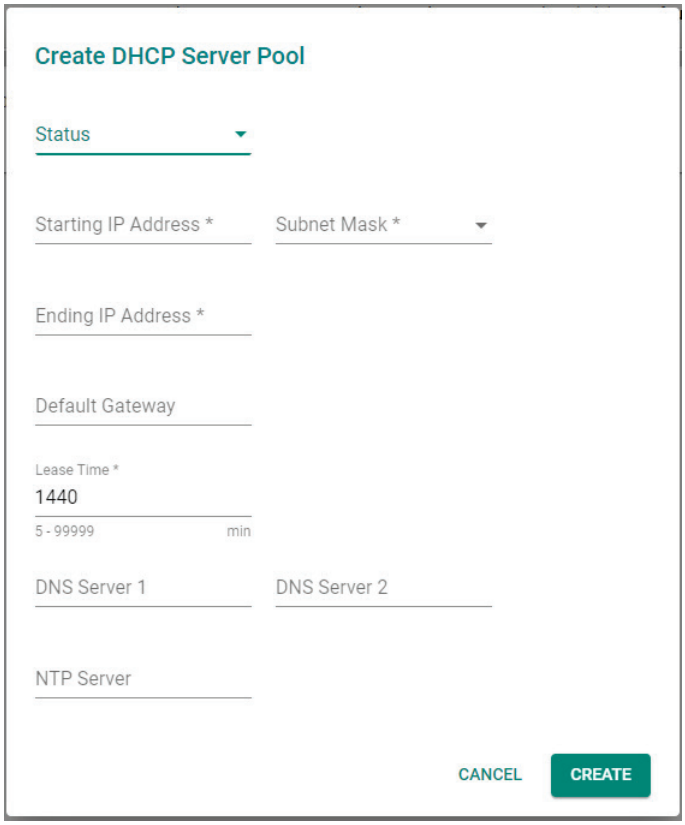
DHCP

The Industrial NAT device provides a DHCP (Dynamic Host Configuration Protocol) server function for LAN interfaces. When configured, the Industrial NAT device will automatically assign an IP address to an Ethernet device from a defined IP range.



Create a DHCP Server Pool

Click ⊞ to create a new DHCP Server Pool.



Status

Setting	Description	Factory Default
Enable/Disable	Enable or disable the DHCP server pool.	None

Starting IP Address

Setting	Description	Factory Default
IP Address	The starting IP address of the DHCP IP range.	None

Subnet Mask

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

Ending IP Address

Setting	Description	Factory Default
IP Address	The ending IP address of the DHCP IP range.	None

Default Gateway

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

Lease Time

Setting	Description	Factory Default
5 to 99999 minutes	The lease time of the DHCP server.	1440

DNS Server 1

Setting	Description	Factory Default
IP Address	The first DNS server for DHCP clients.	None

DNS Server 2

Setting	Description	Factory Default
IP Address	The second DNS server for DHCP clients.	None

NTP Server

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

NOTE

1. The DHCP Server is only available for LAN interfaces.
2. The starting and ending IP addresses of the DHCP IP pool must be in the same logical subnet.

Delete a DHCP Pool

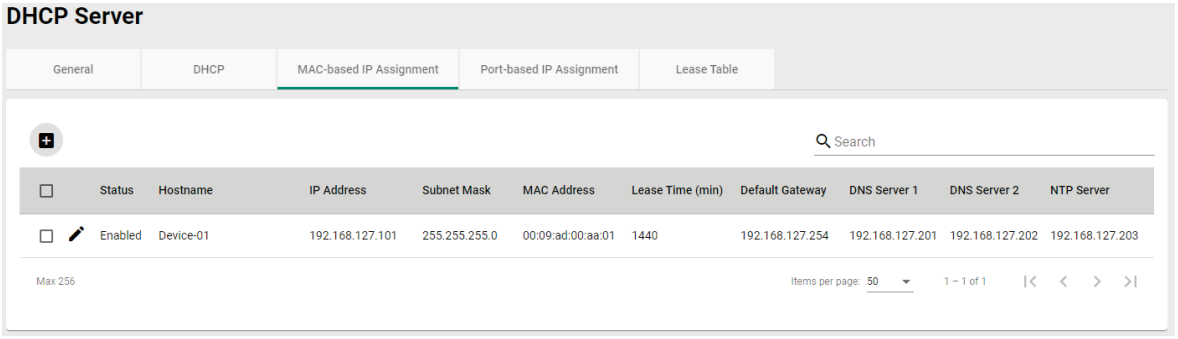
Click next to the DHCP pool entry to delete it.

Modify a DHCP Pool

Click to modify the attributes and click **APPLY** to change the configuration.

MAC-based IP Assignment

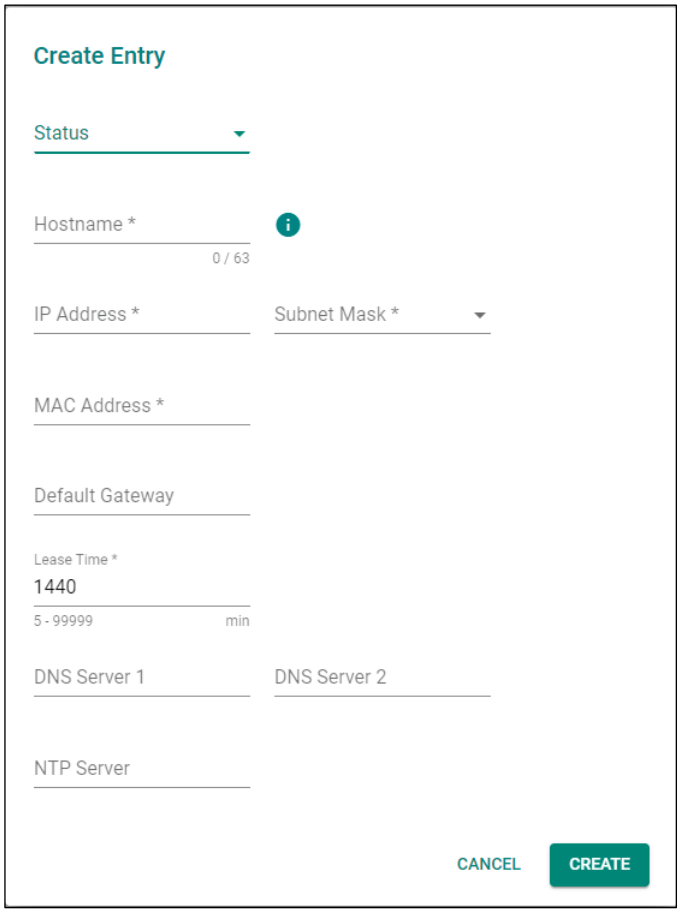
Use the MAC-based IP list to ensure that devices connected to the Industrial NAT device always use the same IP address. The MAC-based IP list matches IP addresses to MAC addresses.



In the above example, a Hostname “Device-01” was added to the list, with a MAC-based 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 NAT device, the Industrial NAT device will assign the IP address 192.168.127.101 to this device.

Create a MAC-based IP Entry

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



Status

Setting	Description	Factory Default
Enable/Disable	Enable or disable the MAC-based IP server function.	None

Hostname

Setting	Description	Factory Default
Max. 63 characters	The name of the device.	None

IP Address

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

Subnet Mask

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

MAC Address

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

Default Gateway

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

Lease Time

Setting	Description	Factory Default

5-99999 minutes	The lease time of the device.	1440

DNS Server 1

Setting	Description	Factory Default
IP Address	The first DNS server for the device.	None

DNS Server 2

Setting	Description	Factory Default
IP Address	The second DNS server for the device.	None

NTP Server

Setting	Description	Factory Default
IP Address	The NTP server for the device.	None

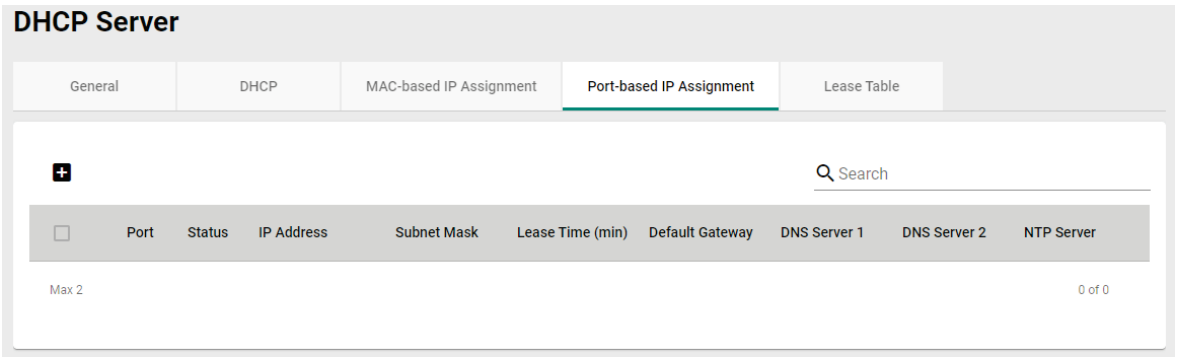
Delete a MAC-based IP Entry

Select the entry from the list and click to delete it.

Modify a MAC-based IP Entry

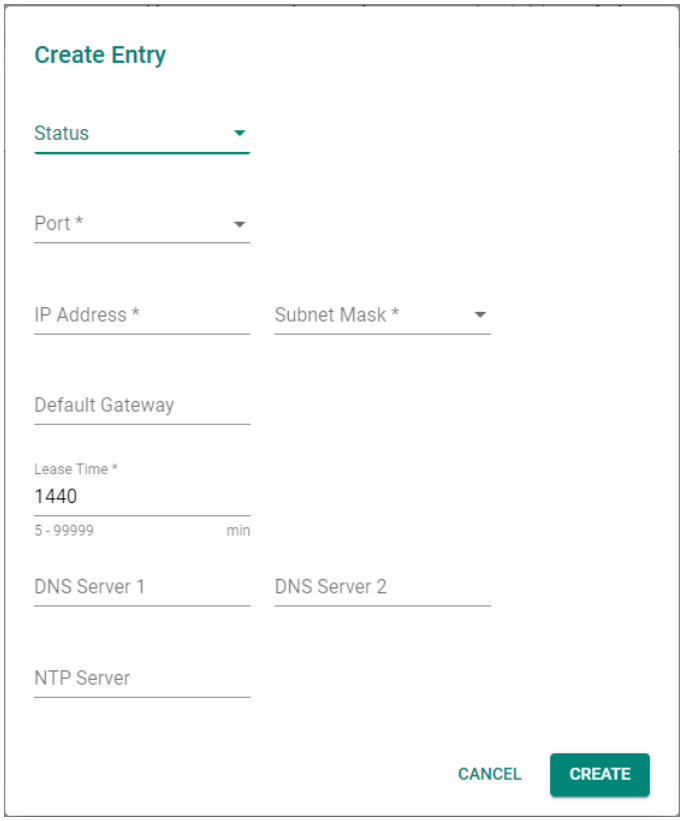
Click to modify the attributes and click **APPLY** button to change the configuration.

Port-based IP Assignment



Create a Port-based IP Entry

Click to create Port-based IP list.



Status

Setting	Description	Factory Default
Enable/Disable	Enable or disable the Port-based IP function.	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	The IP address of the connected device.	None

Subnet Mask

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

Default Gateway

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

Lease Time

Setting	Description	Factory Default
5-99999 minutes	The lease time of the connected device.	1440

DNS Server 1

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

DNS Server 2

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

NTP Server

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

Delete a Port-based IP Entry

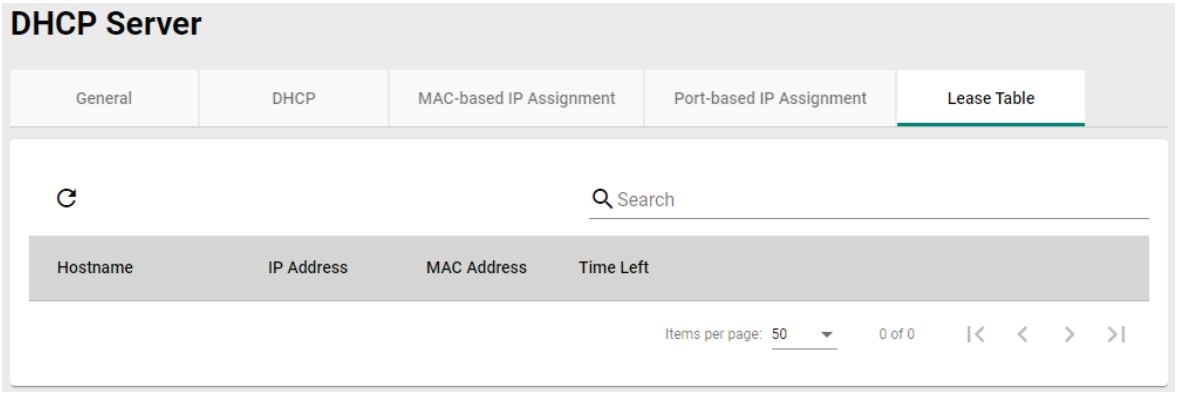
Select the entry from the list and click to delete it.

Modify a Port-based IP Entry

Click to modify the attributes and click **APPLY** to change the configuration.

Lease Table

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



7

Routing & NAT

The following topics are covered in this chapter:

- **Unicast Routing**
  - Static Routes
  - Routing Table
- **NAT Settings**
  - NAT Concept
  - 1-to-1 NAT Overview
  - 1-to-1 NAT
  - N-to-1 NAT
  - PAT
  - Advance

Unicast Routing

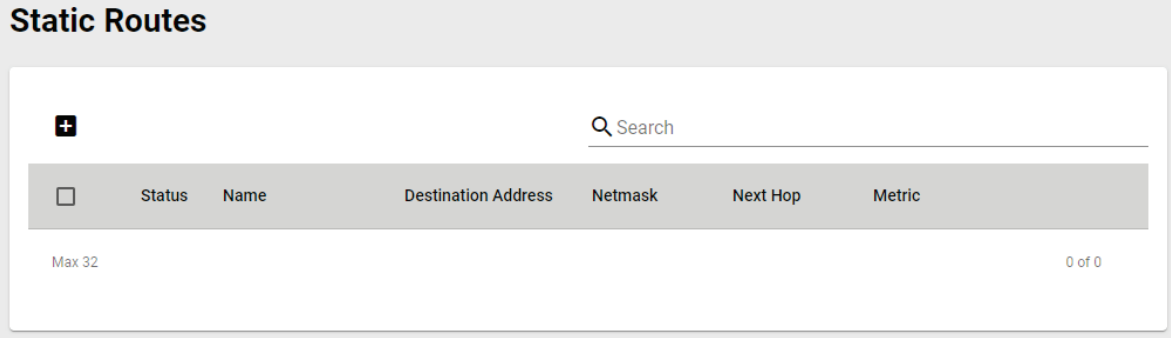
The Industrial NAT device supports static routing. A routing entry includes the following items: the destination address, the next hop address (which is the next router along the path to the destination address), and a metric that represents the cost to access a different network.

Static Route

You can define static routes by specifying the next hop (or router) that the Industrial NAT device forwards data to within a specific subnet. The settings of the Static Route will be added to the routing table and stored on the Industrial NAT device.

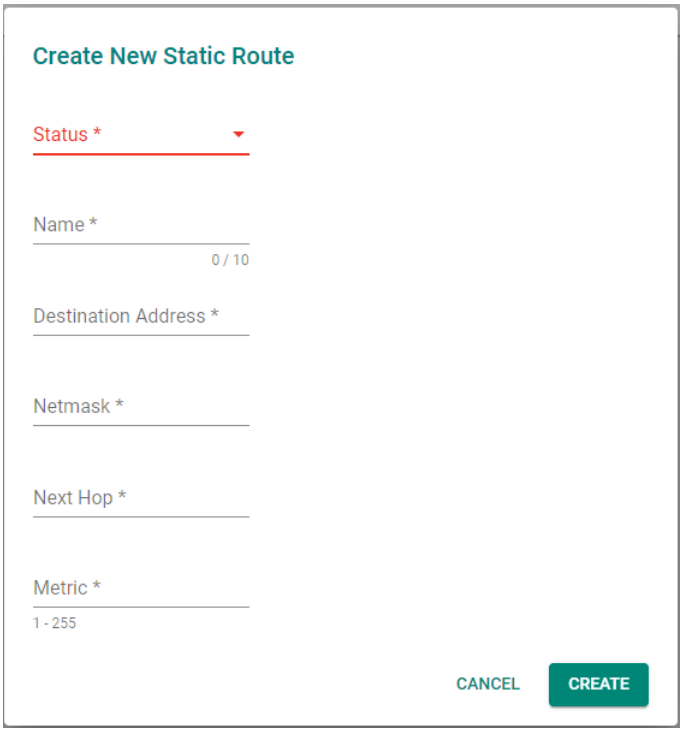
Static Routes

The Static Routes page is used to configure the Industrial NAT device's static routing table.



Create a Static Route

Click ⊞ to create new static route. Click **CREATE** to add the entry to the Static Routing Table.



Status

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

Name

Setting	Description	Factory Default
10 characters	The name of the static route.	None

Destination Address

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

Netmask

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

Next Hop

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

Metric

Setting	Description	Factory Default
Metric	Specify the cost of the route.	None

Delete a Static Route

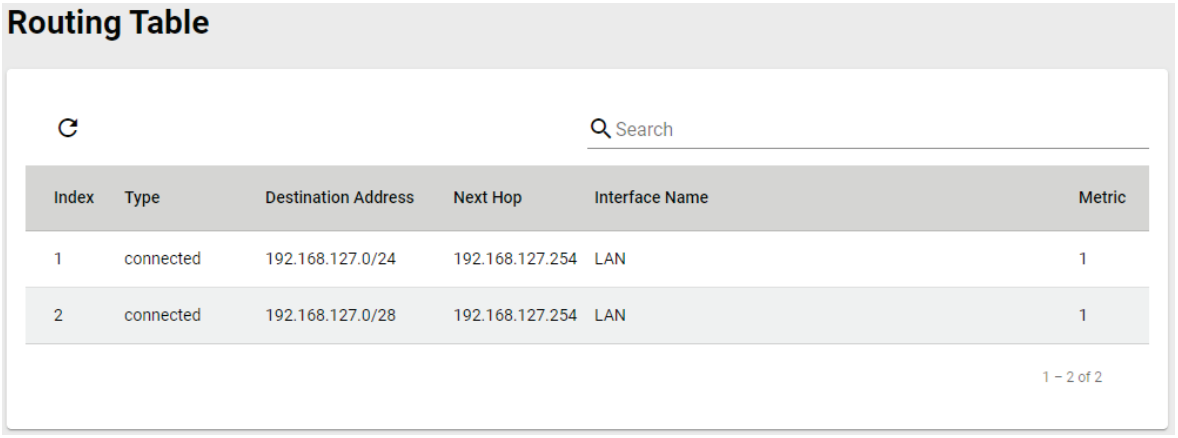
Select the entry from the list and click to delete it.

Modify an Existing Static Route

Click to modify the attributes and click **APPLY** to change the configuration.

Routing Table

The Routing Table page shows all routing entries.



NAT Settings

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:

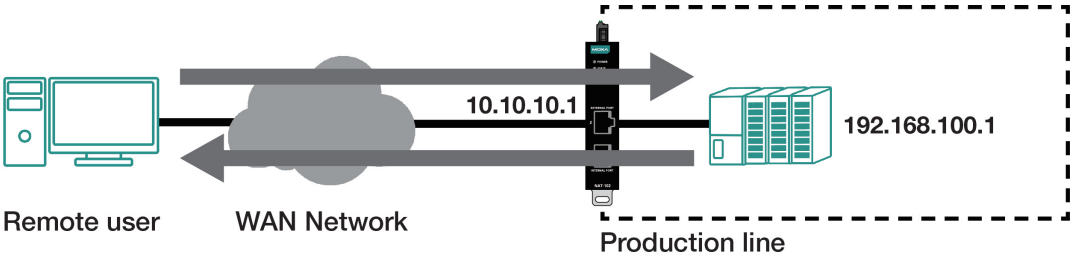
- The N-1 or Port forwarding NAT function hides the internal IP address of a critical network or device to increase the security of industrial network applications.
- NAT uses the same private IP address for different, but identical, groups of Ethernet devices. For example, 1-to-1 NAT makes it easy to 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 with the first policy (Index=1); if the packet matches this policy, the Industrial NAT device will translate the address immediately and will then start checking the next packet. If the packet does not match this policy, it will check with the next policy.

NOTE The NAT-102 supports a maximum of 128 NAT policies.

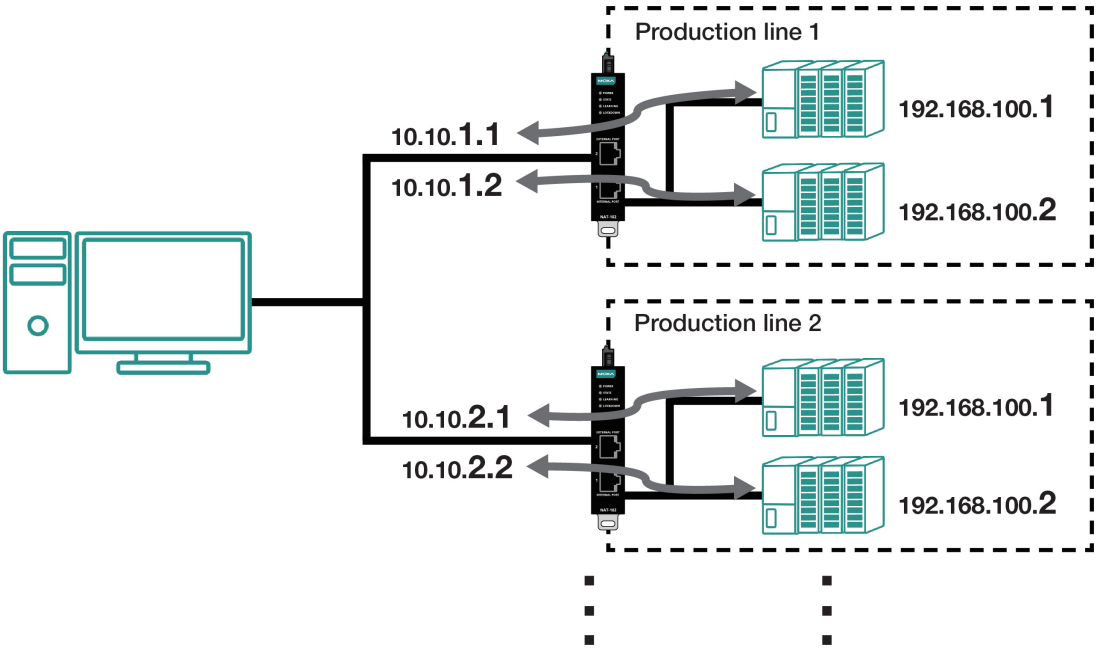
1-to-1 NAT Overview

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 unidirectional 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 Settings in Production Line 1

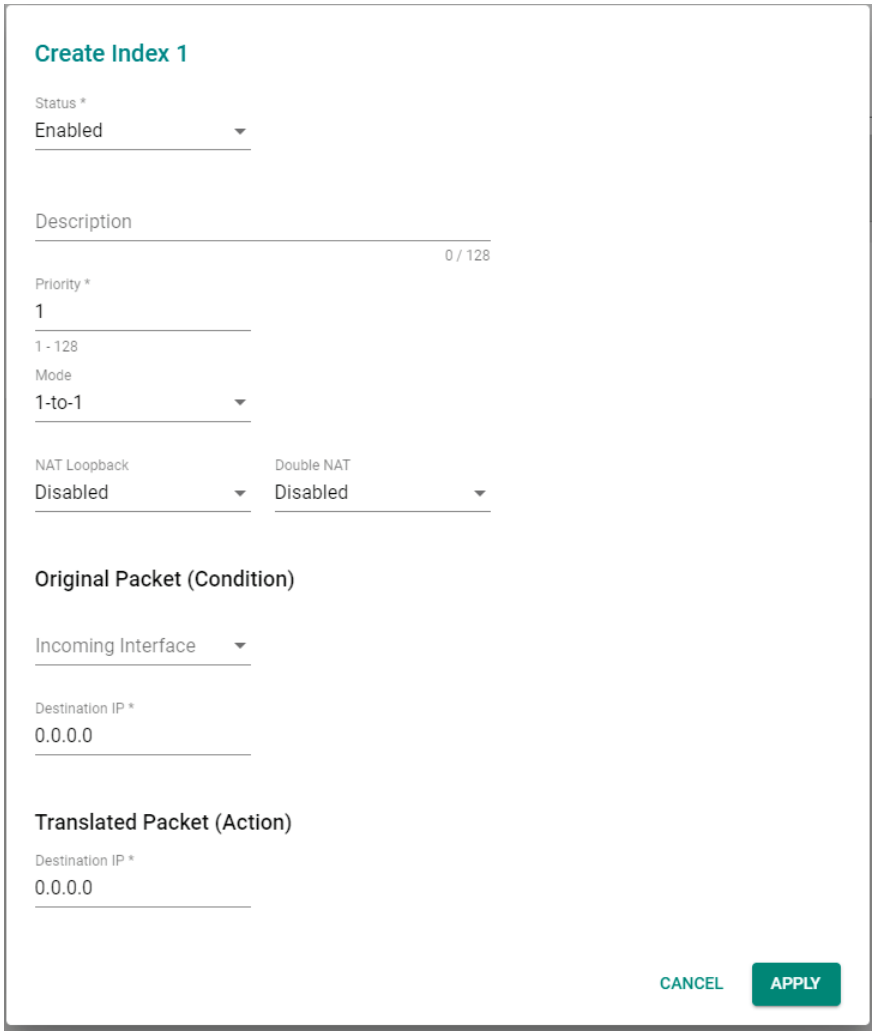
	Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
☐ ✎	Enabled	1-to-1_production_line_1-1	1	1-to-1		WAN	Any:Any	10.10.1.1:Any	All	Any:Any	192.168.100.1:Any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

Create a 1-to-1 NAT Entry



Status

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

Description

Setting	Description	Factory Default
Description	Enter the name of the NAT rule.	None

Priority

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

NAT Mode

Setting	Description	Factory Default
1-to-1 N-to-1 PAT Advance	Select the NAT type.	1-to-1

NAT Loopback

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

Double NAT

Setting	Description	Factory Default
Enable/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 incoming interface for 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

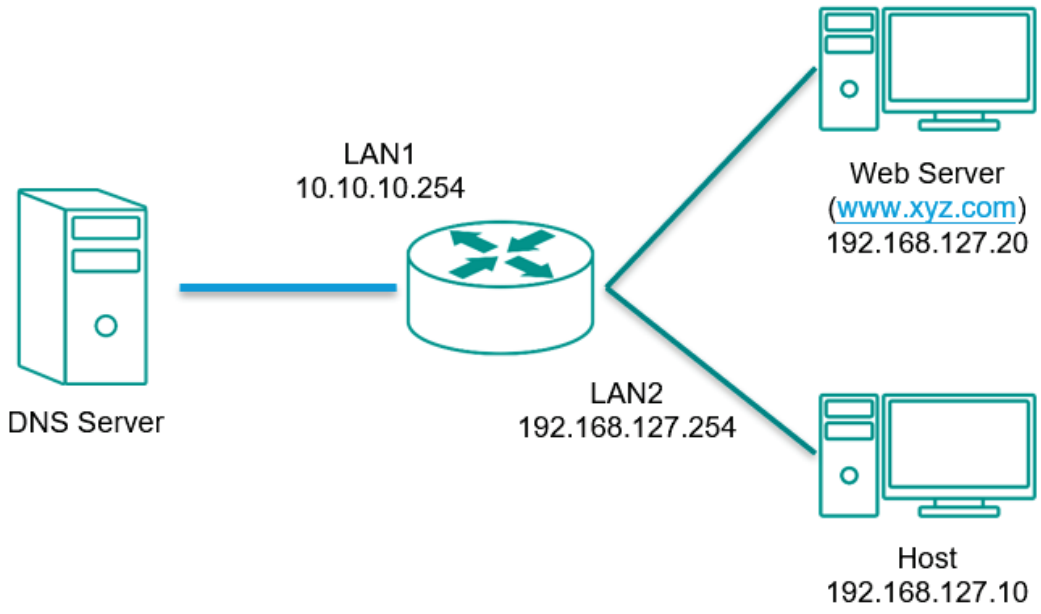
Translated Packet (Action)

Destination IP

Setting	Description	Factory Default
IP Address	Specify the Internal IP address in LAN network area	0.0.0.0

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 replies the Web Server IP: 10.10.10.20
3. The Host will start to send the request packets to 10.10.10.20.

With NAT Loopback disabled:

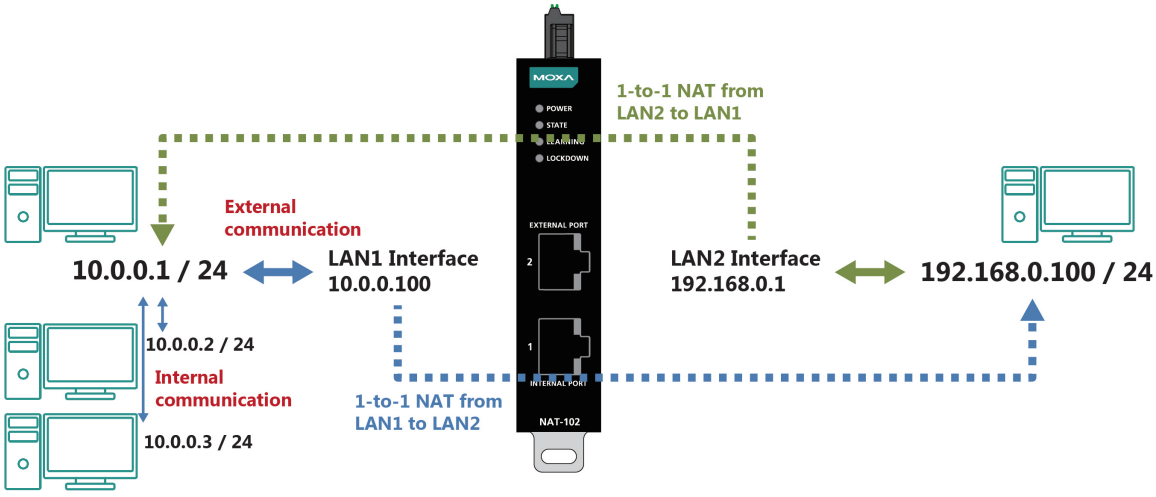
- Because the request packet comes from Host, the incoming interface does not match any NAT rule.
- The NAT-102 will receive the request packet because the NAT rule has created secondary IP: 10.10.10.20.
- The NAT-102 sends the response packet to Host itself.
- Host will access the NAT-102's web page via www.xyz.com.

With NAT Loopback enabled:

- The NAT-102 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 NAT-102. The NAT-102 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



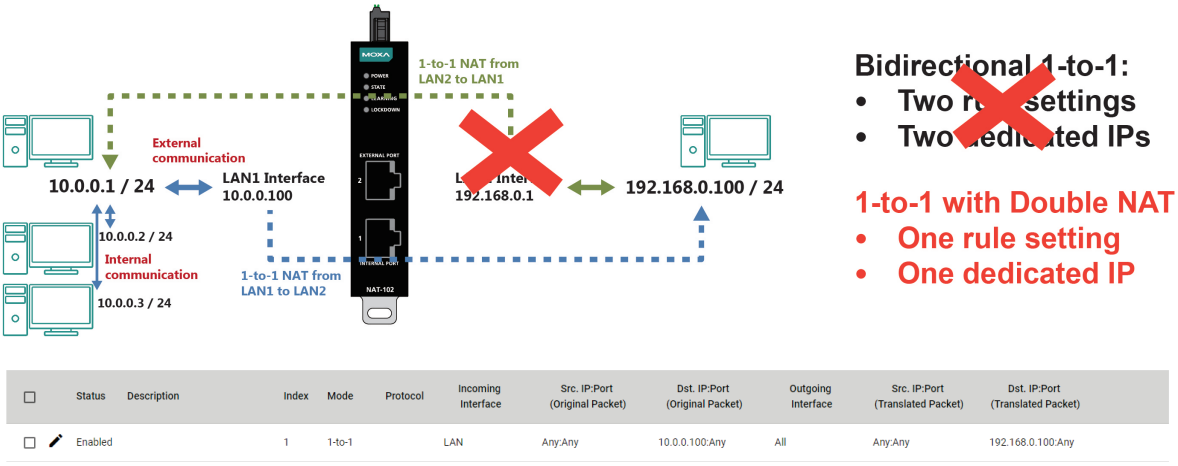
Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
Enabled		1	1-to-1		LAN	Any:Any	192.168.0.1:Any	All	Any:Any	10.0.0.1:Any
Enabled		2	1-to-1		WAN	Any:Any	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 NAT-102 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



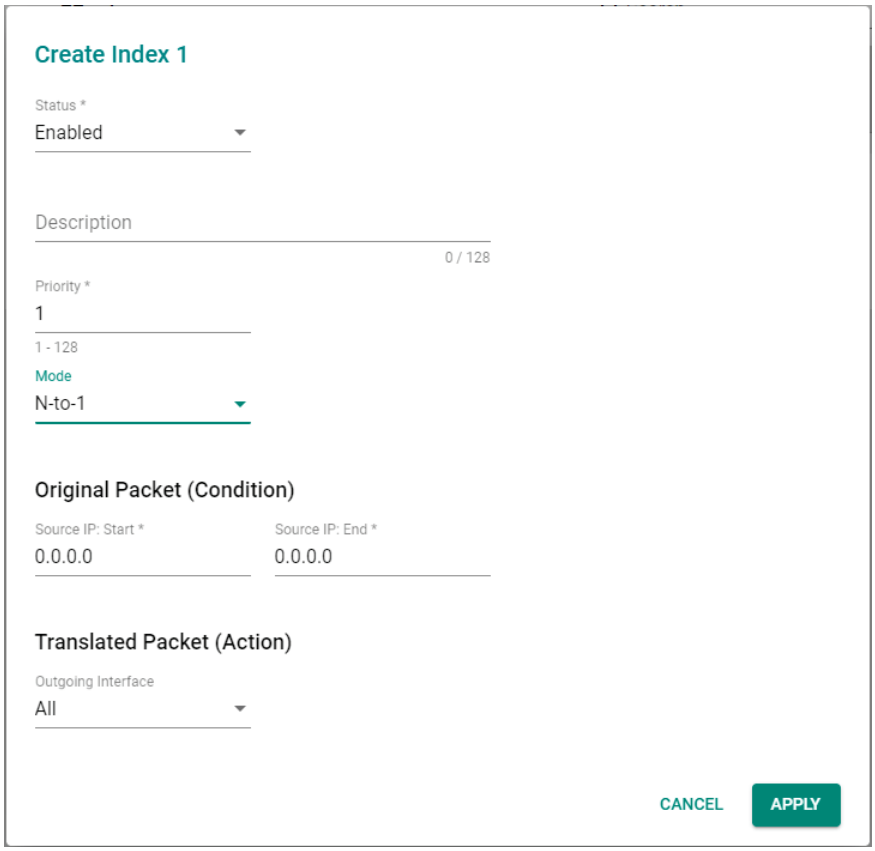
Status	Description	Index	Mode	Protocol	Incoming Interface	Src. IP:Port (Original Packet)	Dst. IP:Port (Original Packet)	Outgoing Interface	Src. IP:Port (Translated Packet)	Dst. IP:Port (Translated Packet)
Enabled		1	1-to-1		LAN	Any:Any	10.0.0.100:Any	All	Any:Any	192.168.0.100:Any

NOTE The Industrial NAT device 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 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 external 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".

The N-1 NAT function is a one-way connection from an internal secure area to an external non-secure area. The user can initialize the connection from the internal to the external network but not the other way around.



Status

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

Description

Setting	Description	Factory Default
Description	Enter the name of the NAT rule.	None

Priority

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

NAT Mode

Setting	Description	Factory Default
1-to-1 N-to-1 PAT Advance	Select the NAT type.	1-to-1

Original Packet (Condition)

Source IP: Start

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

Source IP: End

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

Translated Packet (Action)

Outgoing Interface

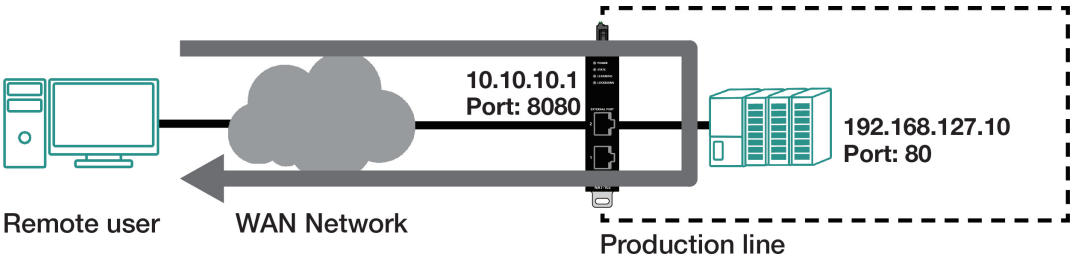
Setting	Description	Factory Default
All LAN WAN	Select the outgoing interface for the NAT rule.	All

PAT (Port Address Translation)

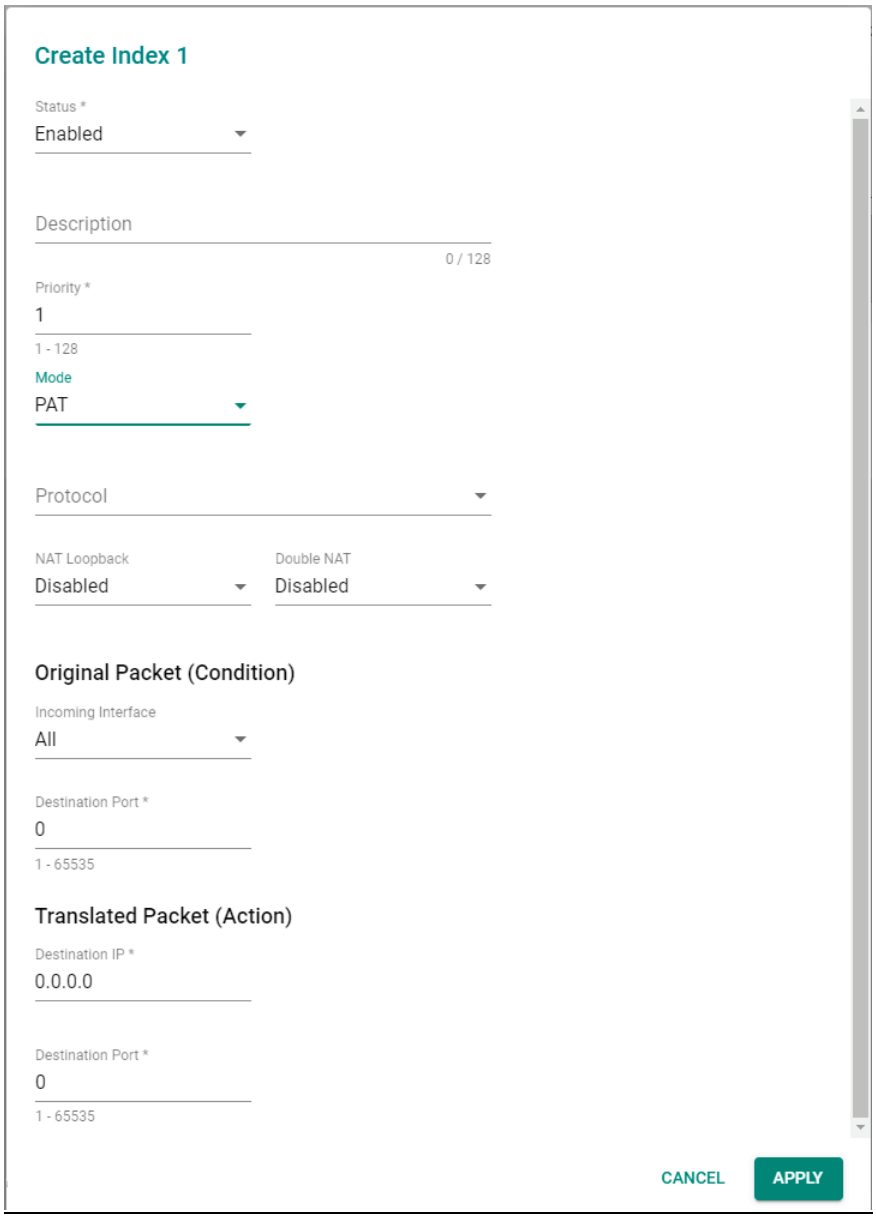
If the initial connection is from outside the LAN, but the user still wants to hide the internal IP address, one way to do this is to use the PAT NAT function.

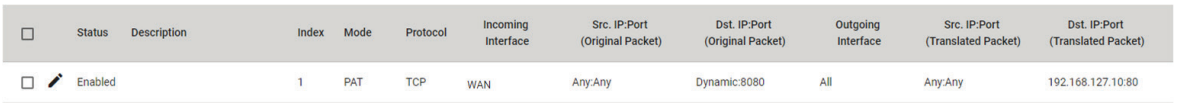
The user can specify the port number of an external IP address (WAN1 or WAN2) in the Port Forwarding policy list. For example, if the IP address of a web server in the internal network is 192.168.127.10 with port 80, the user can set up a Port Forwarding policy to let remote users connect to the internal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



Create a PAT NAT Entry





Enable

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

Description

Setting	Description	Factory Default

Description	Enter the name of the NAT rule.	None

Priority

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

NAT Mode

Setting	Description	Factory Default
1-to-1 N-to-1 PAT Advance	Select the NAT type.	1-to-1

Protocol

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

NAT Loopback

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

Double NAT

Setting	Description	Factory Default
Enable/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

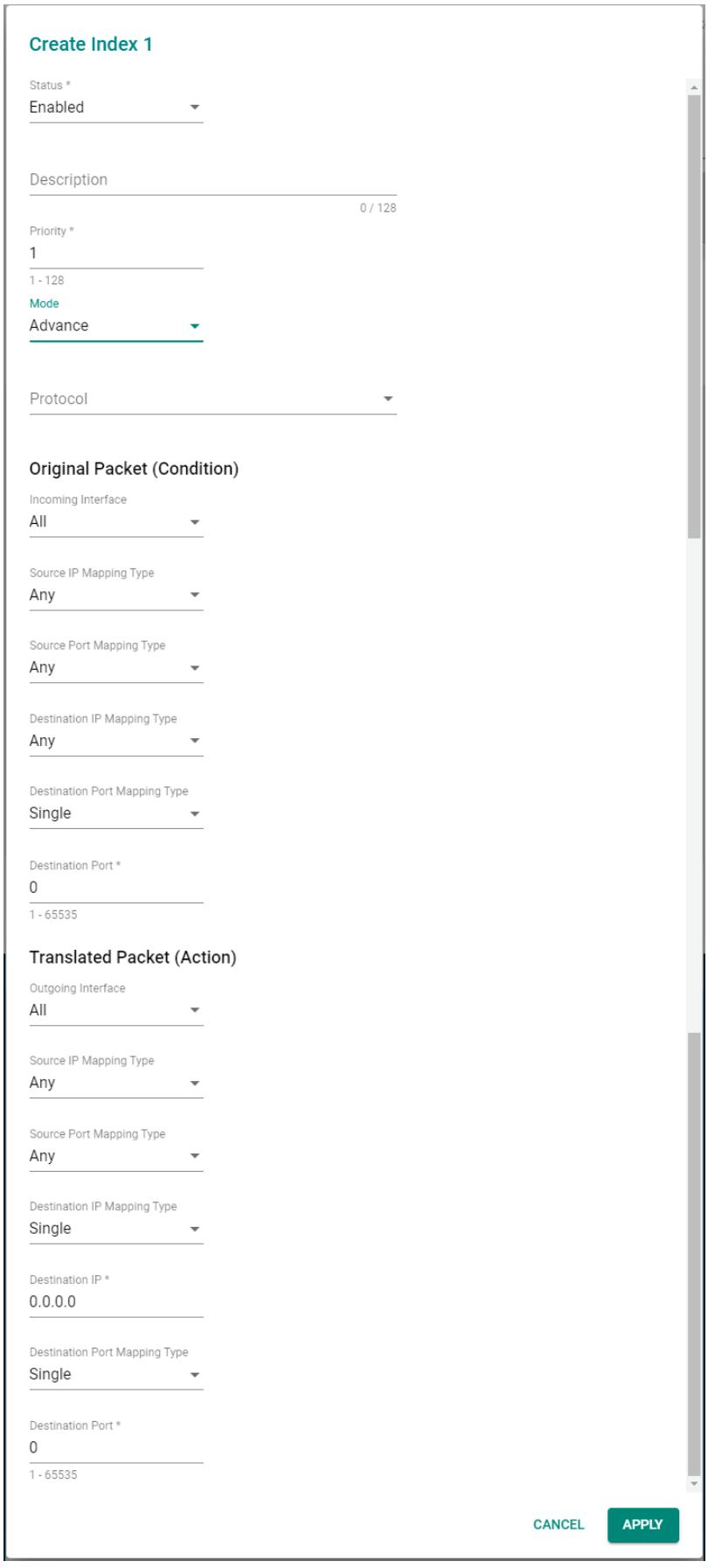
Setting	Description	Factory Default
IP Address	Specify the translated IP address in the internal network.	0.0.0.0

Destination Port

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

Advance

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



Enable

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

Description

Setting	Description	Factory Default
Description	Enter the name of the NAT rule.	None

Priority

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

NAT Mode

Setting	Description	Factory Default
1-to-1 N-to-1 PAT Advance	Select the NAT type.	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.	All

Source IP Mapping Type

Setting	Description	Factory Default
Any Single Range Subnet mask	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 Port Mapping Type

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

Destination Port

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

Translated Packet (Action)

Outgoing Interface

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

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 in 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

Destination Port

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

8

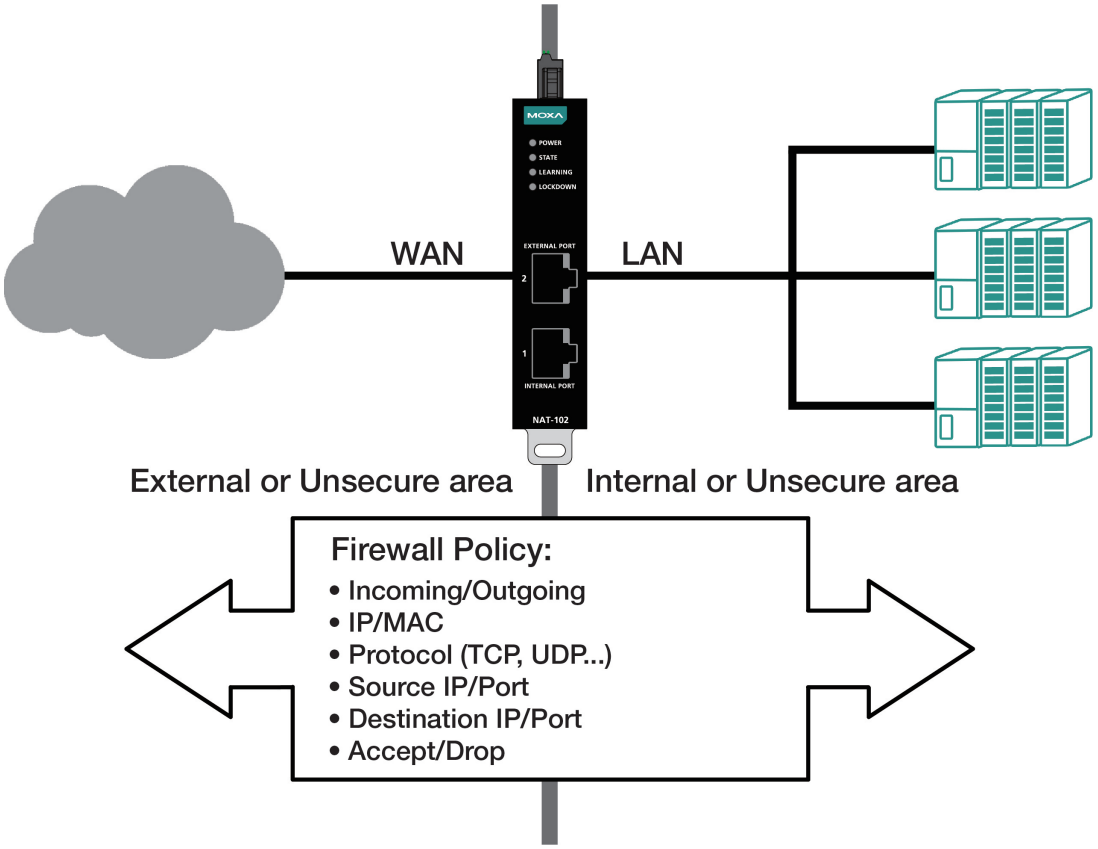
Firewall

The following topics are covered in this chapter:

- **Policy Concept**
- **Layer 3 Policy**
  - Create a New Firewall Policy
  - Automation Profile

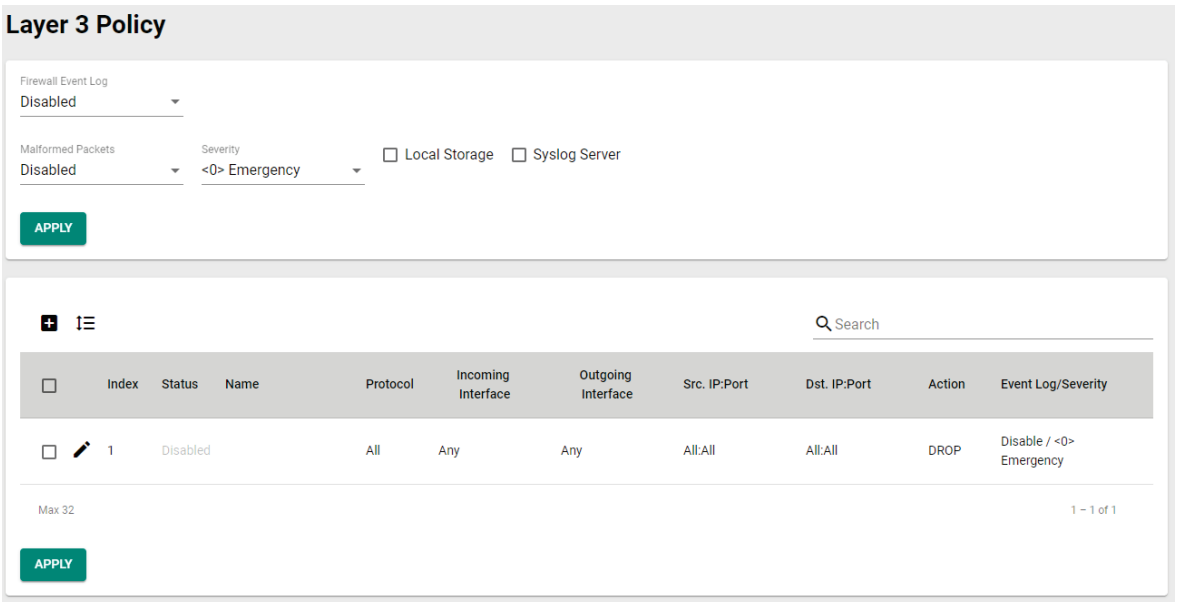
Policy Concept

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 (the non-secure part) and an internal network (the secure part).



Layer 3 Policy

The Industrial NAT device's firewall policy provides secure traffic control and allows users to have more control over network traffic based on certain parameters.



Firewall Event Log

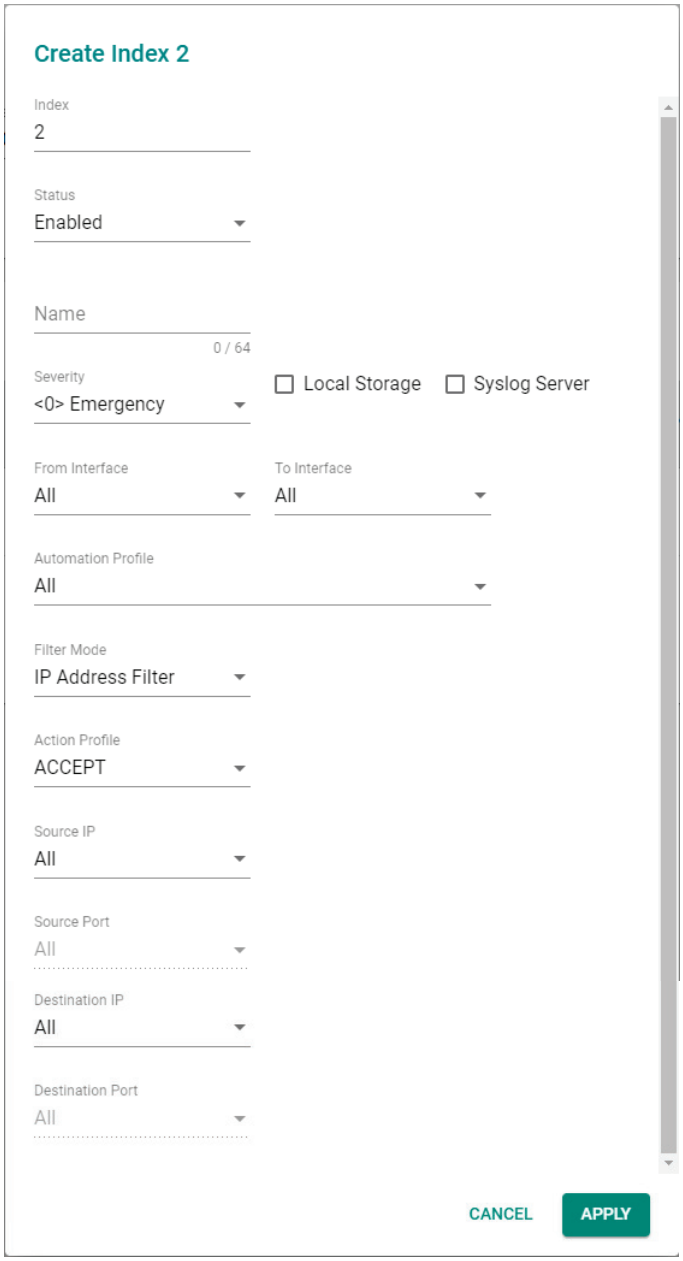
If enabled, the Industrial NAT device keeps real-time event logs for different types of firewall events. You can choose to save these logs locally or send them to the Syslog server.

Malformed Packets

Enable this option to have the system record event logs when malformed packets are dropped. These logs can be stored locally or be sent to a syslog server. You can also adjust the severity of these events.

Create a New Firewall Policy

Click ⊞ to create a new firewall policy.



Index

The index number is generated automatically.

Status

Setting	Description	Factory Default
Enable/Disable	Enable or disable the firewall policy.	Enabled

Name

Setting	Description	Factory Default
Custom string	Enter a name for the firewall rule.	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 firewall event.	<0> Emergency

Local Storage

Setting	Description	Factory Default
Check/Uncheck	When checked, the firewall white/blacklist rule event logs are stored in the local storage and will show in "Event Log" table.	Unchecked

Syslog Server

Setting	Description	Factory Default
Check/Uncheck	When checked, firewall white/blacklist rule event logs are sent to a Syslog server.	Unchecked

From Interface

Setting	Description	Factory Default
All LAN WAN Any	Select the From interface.	All

To Interface

Setting	Description	Factory Default
All LAN WAN Any	Select the To interface.	All

Automation Profile

Setting	Description	Factory Default
Refer to the Automation Profile section.	Select the Protocol parameters for the firewall policy.	None

Filter Mode

Setting	Description	Factory Default
IP Address Filter	The firewall policy will filter based on IP address.	IP Address Filter

Source MAC Filter	The firewall policy will filter based on MAC address and source. This mode is disabled and its functionality is replaced by the "Port Security/Device Lockdown" feature instead.	

Action Profile

Setting	Description	Factory Default
Accept	The packet will be allowed through if it matches the firewall policy.	Accept
Drop	The packet will be denied if it matches the firewall policy.	

Source IP

Setting	Description	Factory Default
All	The firewall policy will check all source IP addresses in the packet.	All
Single	The firewall policy will check for a single specified source IP address in the packet.	
Range	The firewall policy will check for source IP addresses in the packet within the specified range.	

Source Port

Setting	Description	Factory Default
All	The firewall policy will check all source port numbers in the packet.	All
Single	The firewall policy will check for a single specified source port number in the packet.	
Range	The firewall policy will check for source port numbers in the packet within the specified range.	

Destination IP

Setting	Description	Factory Default
All	The firewall policy will check all destination IP addresses in the packet.	All
Single	The firewall policy will check for a single specified destination IP address in the packet.	
Range	The firewall policy will check for destination IP addresses in the packet within the specified range.	

Destination Port

Setting	Description	Factory Default
All	The firewall policy will check all destination port numbers in the packet.	All
Single	The firewall policy will check for a single specified destination port number in the packet.	
Range	The firewall policy will check for destination port numbers in the packet within the specified range.	

NOTE The Industrial NAT device's firewall function will check if incoming or outgoing packets match the firewall policy. It starts by matching the packet to 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 match it with the next policy.

NOTE The NAT-102 supports a maximum of 32 firewall policies.

Delete a Firewall Policy

Select the policy from the list and click to delete it.

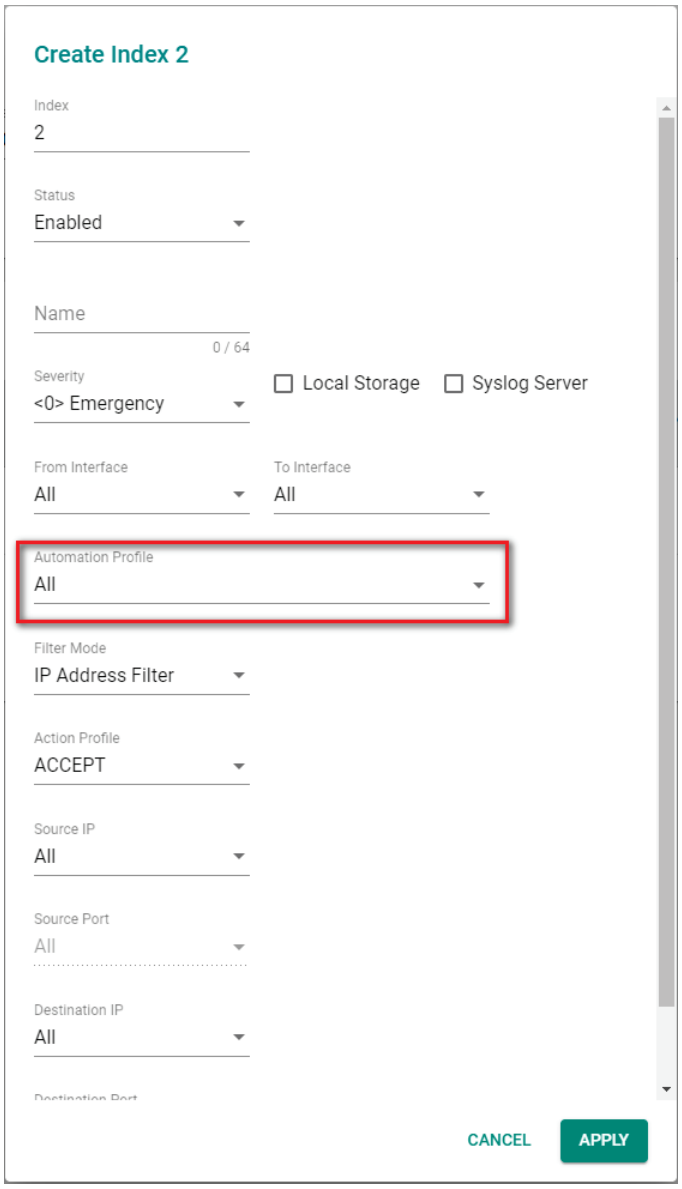
Modify a Firewall Policy

Click to modify the attributes and click **APPLY** to change the configuration.

Automation Profile

Ethernet Fieldbus protocols are popular in industrial automation applications. In fact, many Fieldbus protocols (e.g., EtherNet/IP and Modbus TCP/IP) can operate on an industrial Ethernet network, with the Ethernet port number defined by IANA (Internet Assigned Numbers Authority). The Industrial NAT device supports the **Automation Profile** feature, which includes 45 different pre-defined profiles (Modbus TCP/IP, Ethernet/IP, etc.), allowing users to create an industrial Ethernet Fieldbus firewall policy with just a single click.

For example, if the you want to create a Modbus TCP/IP firewall policy for an internal network, you just need to select the **TCP** or **UDP** protocol from the **Automation Profile** drop-down menu on the **Create a New Firewall Policy** page.



The following table shows the Automation Profile for Ethernet Fieldbus Protocol and the corresponding port number:

Ethernet Fieldbus Protocol	Port Number
TCP	34980
UDP	34980
ICMP	N/A
EtherNet/IP I/O (TCP)	2222
EtherNet/IP I/O (UDP)	2222
EtherNet/IP messaging (TCP)	44818
EtherNet/IP messaging (UDP)	44818
FF Annunciation (TCP)	1089
FF Annunciation (UDP)	1089
FF Fieldbus Message Specification (TCP)	1090
FF Fieldbus Message Specification (UDP)	1090
FF System Management (TCP)	1091
FF System Management (UDP)	1091
FF LAN Redundancy Port (TCP)	3622
FF LAN Redundancy Port (UDP)	3622
LonWorks (TCP)	2540
LonWorks (UDP)	2540
LonWorks2 (TCP)	2541
LonWorks2 (UDP)	2541
Modbus TCP/IP (TCP)	502
Modbus TCP/IP (UDP)	502
PROFInet RT Unicast (TCP)	34962
PROFInet RT Unicast (UDP)	34962
PROFInet RT Multicast (TCP)	34963
PROFInet RT Multicast (UDP)	34963
PROFInet Context Manager (TCP)	34964
PROFInet Context Manager (UDP)	34964
IEC 60870-5-104 process control over IP (TCP)	2404
IEC 60870-5-104 process control over IP (UDP)	2404
DNP3 (TCP)	20000
DNP3 (UDP)	20000

The Automation Profile also includes entries for other commonly used Ethernet protocols listed in the following table:

Ethernet Protocol	Port Number
IPsec NAT-Traversal (TCP)	4500
IPsec NAT-traversal (UDP)	4500
FTP-data (TCP)	20
FTP-data (UDP)	20
FTP-control (TCP)	21
FTP-control (UDP)	21
SSH (TCP)	22
SSH (UDP)	22
Telnet (TCP)	23
Telnet (UDP)	23
HTTP (TCP)	80
HTTP (UDP)	80
IPsec (TCP)	1293
IPsec (UDP)	1293
L2TP (TCP)	1701
L2TP (UDP)	1701

Ethernet Protocol	Port Number
PPTP (TCP)	1723
PPTP (UDP)	1723
RADIUS (TCP)	1812
RADIUS (UDP)	1812
RADIUS Accounting (TCP)	1813
RADIUS Accounting (UDP)	1813
Ethercat (TCP)	34980
Ethercat (UDP)	34980

9

Security

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 NAT device 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 NAT device.

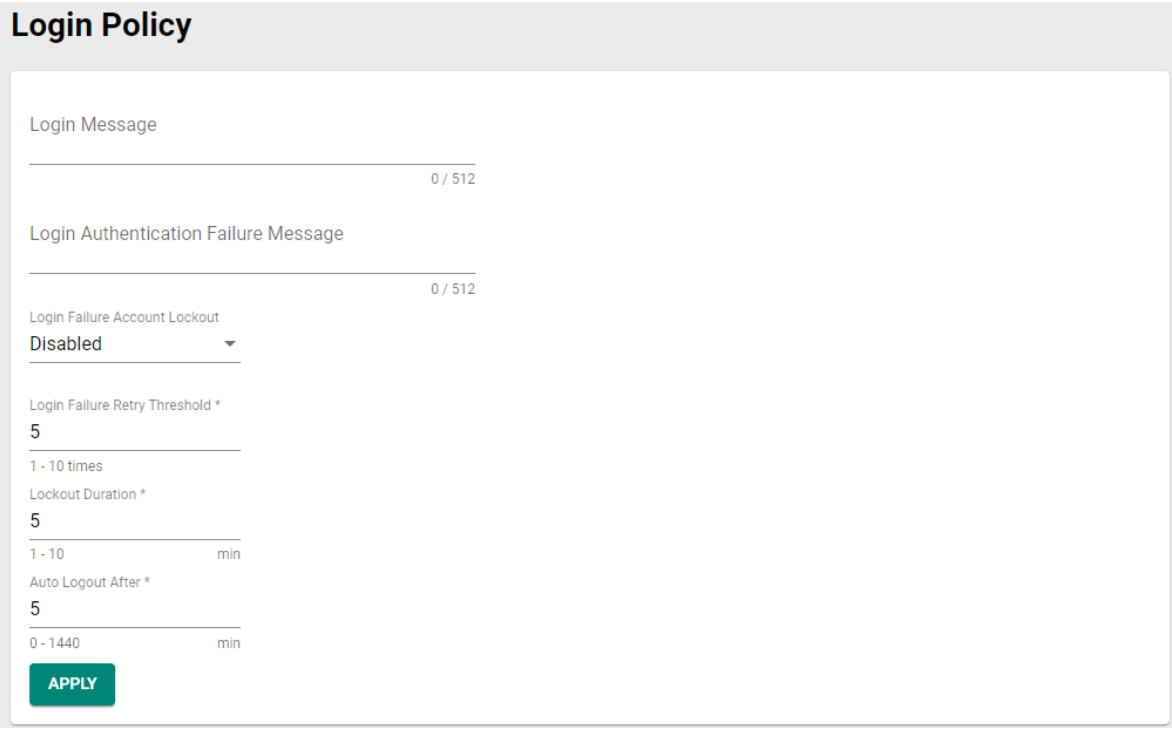
Certificates are a time-based authentication mechanism. Before processing certificates, make sure the Industrial NAT device's clock is synced properly. For more details regarding system time synchronization, refer to the Time section.

The following topics are covered in this chapter:

- **Device Security**
  - Login Policy
  - Trusted Access
  - SSH & SSL
- **Network Security**
  - Port Security

Device Security

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 a message that will appear if the user failed to log in.	None

Login Failure Account Lockout

Setting	Description	Factory Default
Enabled/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

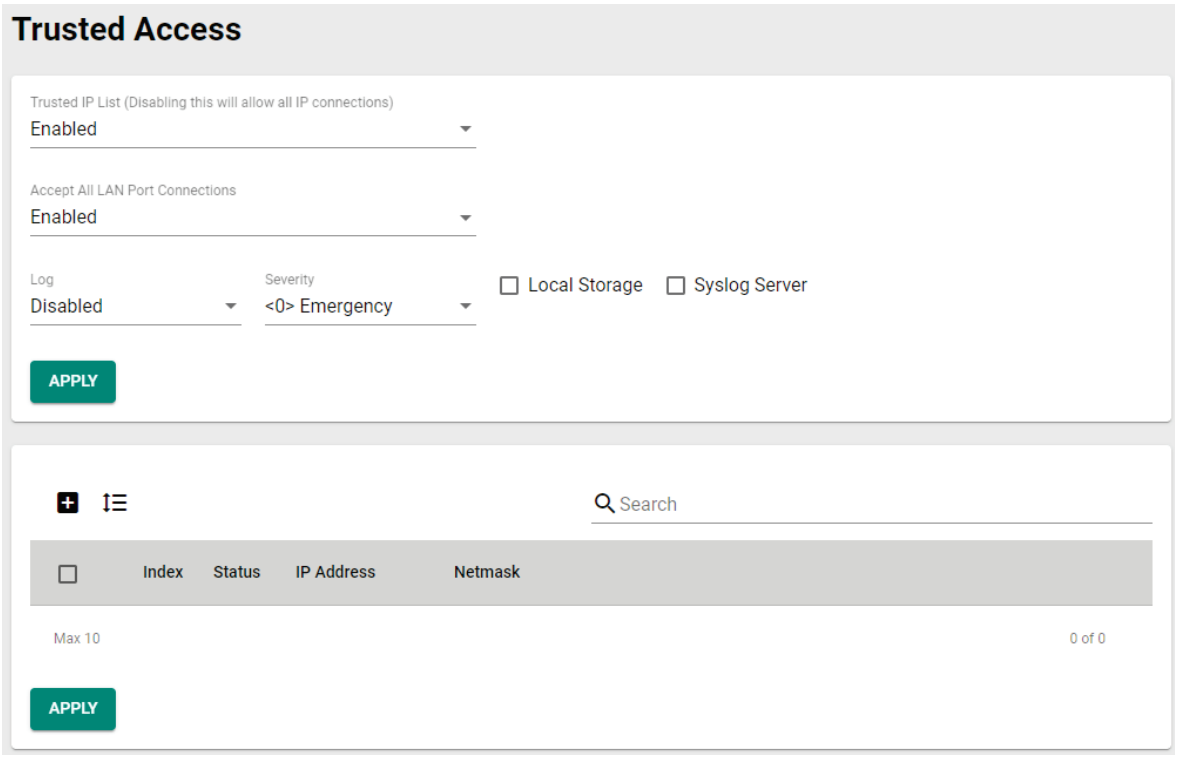
Setting	Description	Factory Default
1 to 10 minutes	Specify the lockout duration.	5

Auto Logout After

Setting	Description	Factory Default
Max. 1440 minutes	When the user is idle for the specified duration, the user will be automatically logged out from the device. The default duration is 5 minutes.	5

Trusted Access

The NAT device uses an IP address-based filtering method to control access.



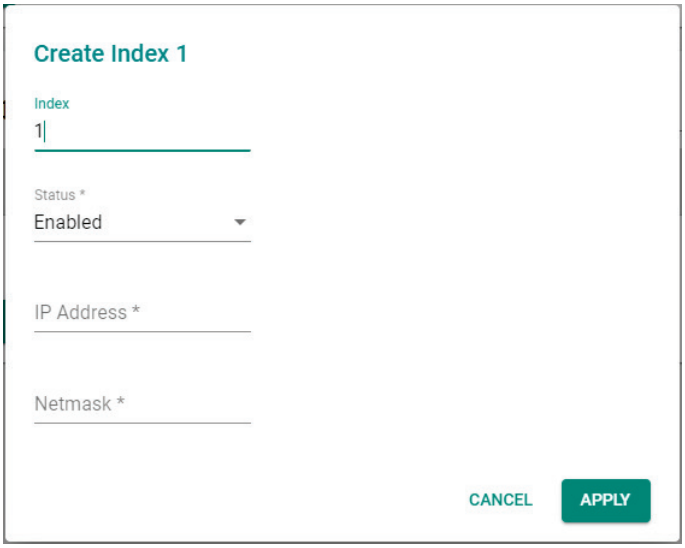
Enable Logging Trusted Access Events

To enable the Trusted Access event log function, select set the Log option to Enable and check either or both the Local Storage or Syslog Server options. You may also define the severity of the Trusted Access types and record it in the event.

Create a Trusted Access Entry

You can control which IP addresses can have access to the Moxa industrial NAT device by adding them to the Trusted Access list. If enabled, only addresses on the list will be allowed access to the Moxa industrial NAT device.

Click ⊞ to add an IP address to the Trusted Access list.



Each IP address and netmask entry can be tailored for different situations, for example:

- **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

Delete a Trusted Access Entry

Select the entry from the Trusted Access List and click to delete it.

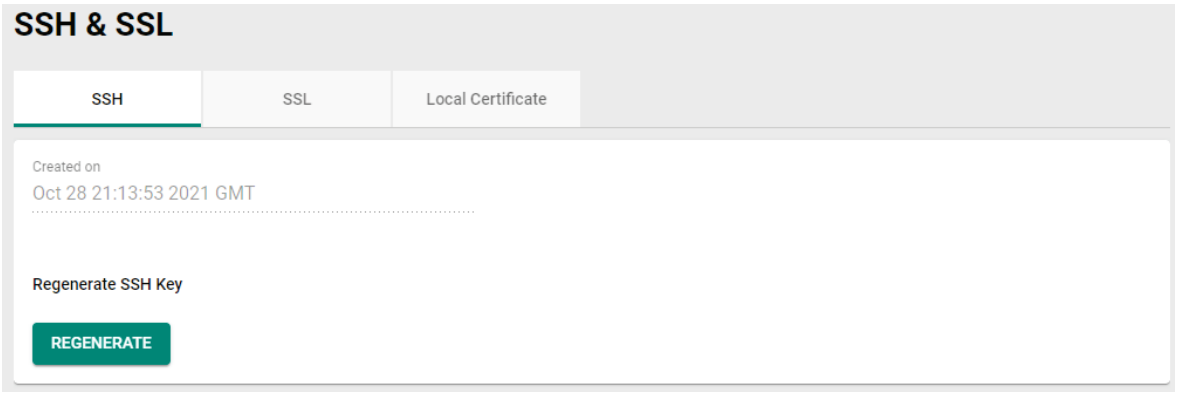
Modify a Trusted Access Entry

Click to modify the attributes and click **APPLY** to change the configuration.

SSH & SSL

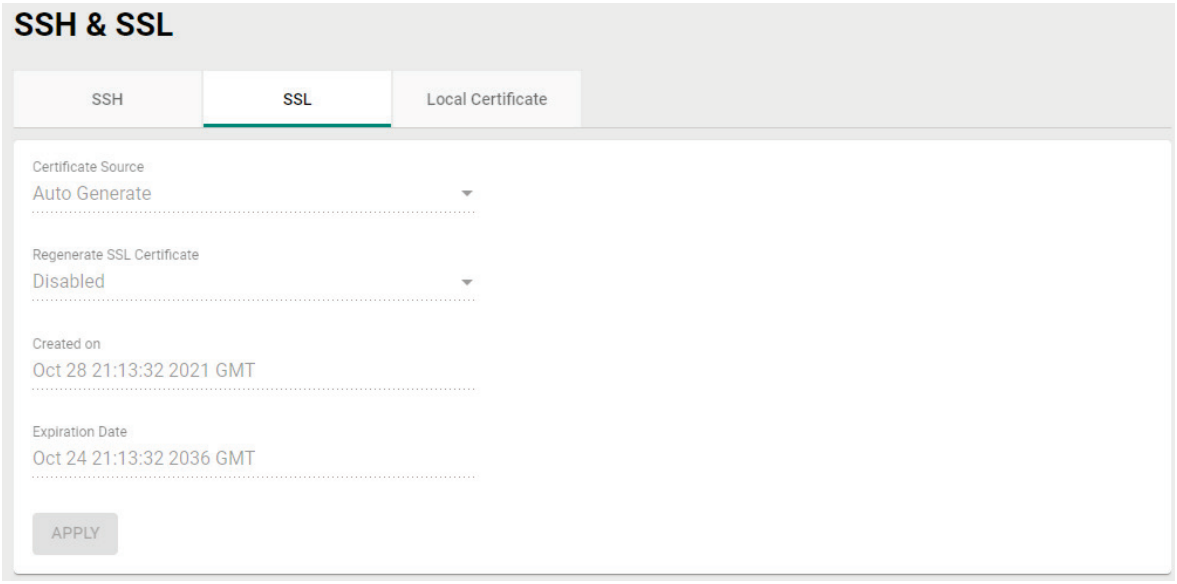
SSH

The NAT device will generate a SSH certificate automatically by default. If not, click **REGENERATE** to regenerate the SSH host key.



SSL

On the SSL screen, you can generate an SSL certificate.



Certificate Source

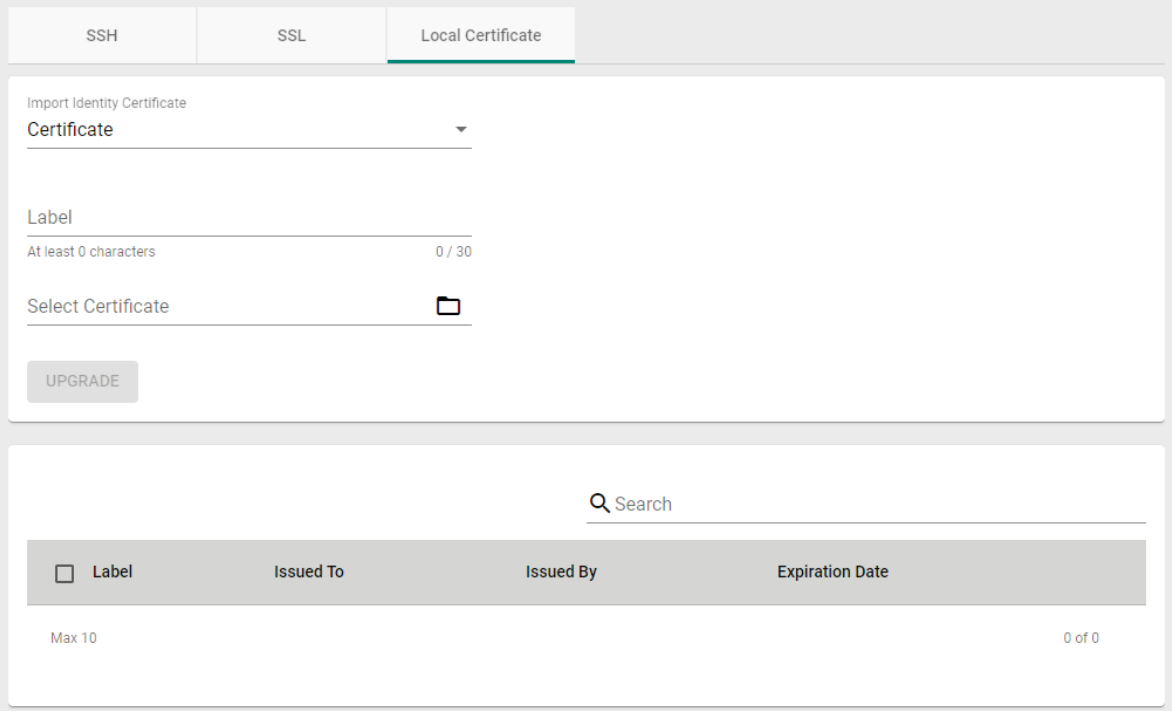
Setting	Description	Factory Default
Auto Generate	The NAT device will generate a certificate automatically. If not, select "Enabled" in Regenerate SSL Certificate to generate a certificate.	Auto Generate
Local Certificate Database	Select the certificate you want to import into Local Certificate Database. The certificate that can be loaded here is limited to "Certificate from CSR" and "Certificate From PKCS#12".	

Regenerate SSL Certificate

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable SSL Key regeneration.	Disabled

Local Certificate

You can manually import certificates to the Industrial NAT device.



Import Identity Certificate

Setting	Description	Factory Default
Certificate, Certificate from PKCS#12	Select the type of certificate. Valid certificates must have the .crt file extension. Certificate from PKCS#12 must have the .p12 file extension.	Certificate

Label

Setting	Description	Factory Default
Max. 30 characters	Enter a label for the certificate.	None

Select Certificate

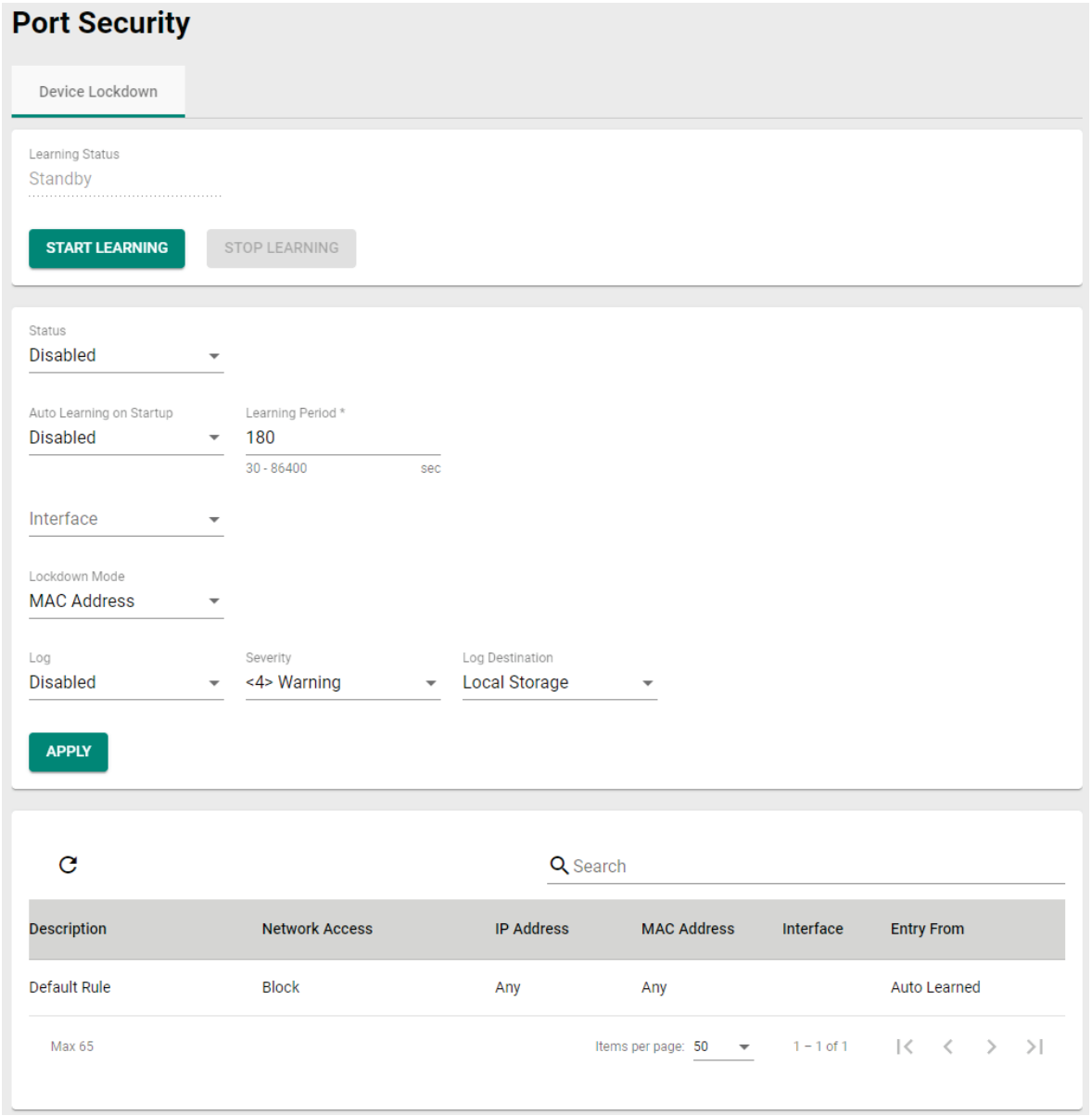
Setting	Description	Factory Default
Select Certificate	Click and select the certificate you want to import. The certificate that can be loaded here is limited to "Certificate from CSR" and "Certificate From PKCS#12".	None

Network Security

Port Security

Device Lockdown

Device Lockdown provides an easy way to automatically establish firewall whitelisting. Users do not need to know the device IP or MAC to establish firewall rules. The Learning function allows the device to learn device information through network traffic to set up whitelisting rules.



Manual Learning

Click **START LEARNING** to have the device learn the whitelist information from ARP tables through network traffic. Click **STOP LEARNING** to stop the process.

Configure Automatic Learning

Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the automatic learning function.	Disabled

Auto Learning on Startup

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable auto learning on startup.	Disabled

Learning Period

Setting	Description	Factory Default
30 to 86400 seconds	Specify the duration auto learning will be enabled for.	180

Interface

Setting	Description	Factory Default
LAN/WAN	Select an interface to lock down. Only one interface can be locked down at any given time.	None

Lockdown Mode

Setting	Description	Factory Default
MAC Address, MAC+IP Access	Select the firewall filtering criteria.	MAC Address

Log

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable device lockdown 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 device lockdown events.	<4> Warning

Log Destination

Setting	Description	Factory Default
Local Storage/Syslog Server	Choose to store device lockdown event logs locally or send them to a Syslog server.	Local Storage

10

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 NAT device also provides **Ping** tools for administrators to diagnose network systems.

The following topics are covered in this chapter:

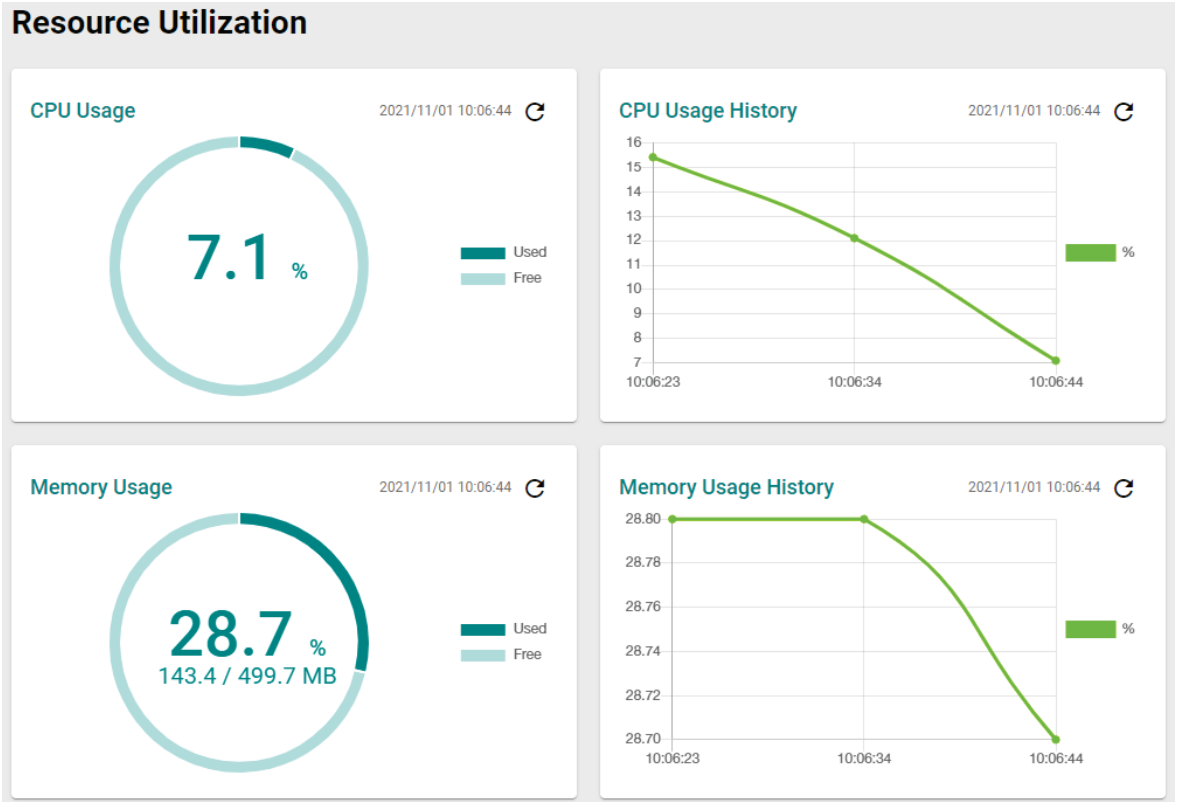
- **System Status**
  - Resource Utilization
- **Log & Event Notification**
  - Event Log
  - Event Notification
  - Syslog
  - Email Notifications
- **Tools**
  - Ping

System Status

Resource Utilization

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

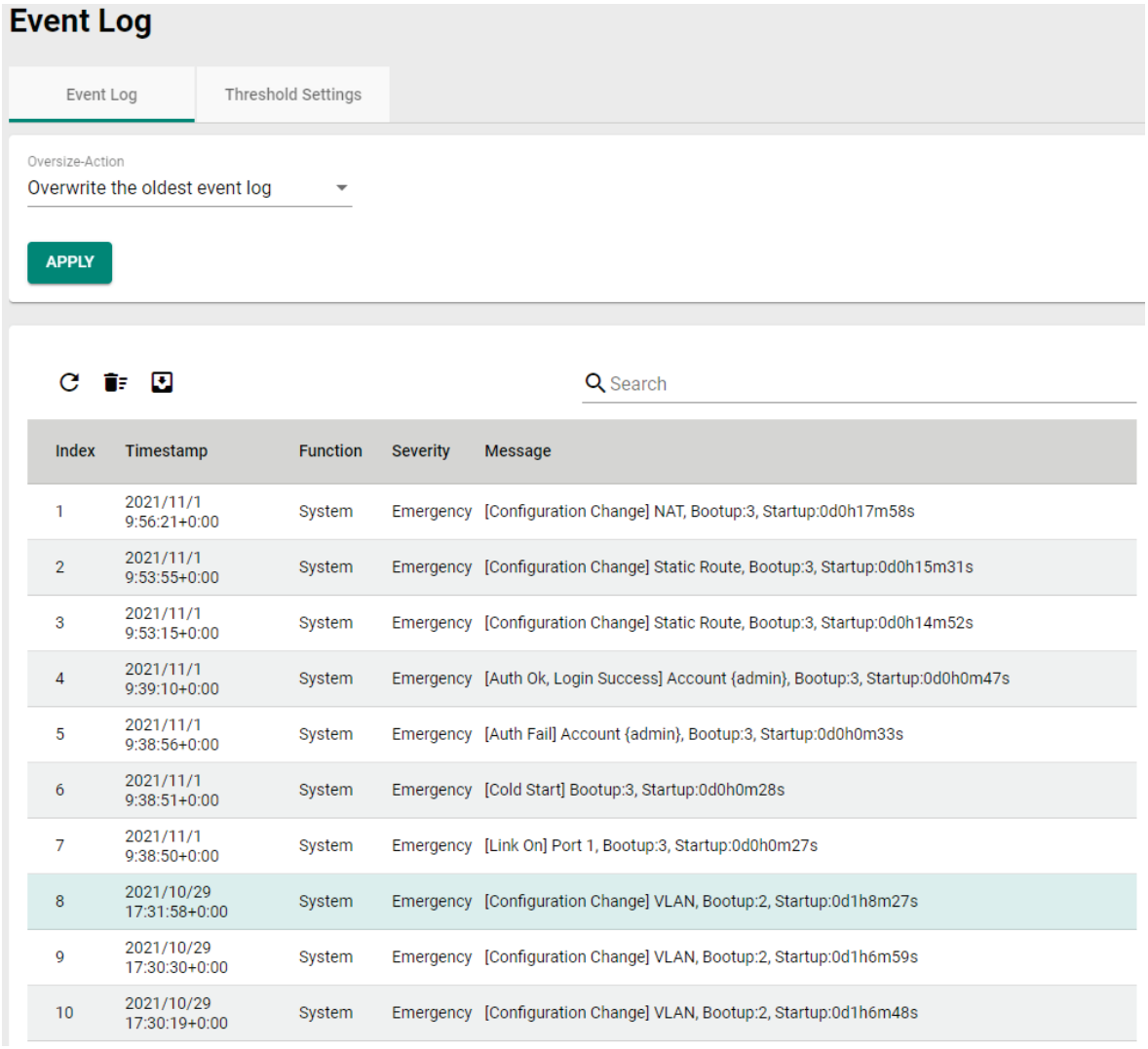
Click ↻ to refresh the information.



Log & Event Notification

Event Log

Event Log



Index	Timestamp	Function	Severity	Message
1	2021/11/1 9:56:21+0:00	System	Emergency	[Configuration Change] NAT, Bootup:3, Startup:0d0h17m58s
2	2021/11/1 9:53:55+0:00	System	Emergency	[Configuration Change] Static Route, Bootup:3, Startup:0d0h15m31s
3	2021/11/1 9:53:15+0:00	System	Emergency	[Configuration Change] Static Route, Bootup:3, Startup:0d0h14m52s
4	2021/11/1 9:39:10+0:00	System	Emergency	[Auth Ok, Login Success] Account {admin}, Bootup:3, Startup:0d0h0m47s
5	2021/11/1 9:38:56+0:00	System	Emergency	[Auth Fail] Account {admin}, Bootup:3, Startup:0d0h0m33s
6	2021/11/1 9:38:51+0:00	System	Emergency	[Cold Start] Bootup:3, Startup:0d0h0m28s
7	2021/11/1 9:38:50+0:00	System	Emergency	[Link On] Port 1, Bootup:3, Startup:0d0h0m27s
8	2021/10/29 17:31:58+0:00	System	Emergency	[Configuration Change] VLAN, Bootup:2, Startup:0d1h8m27s
9	2021/10/29 17:30:30+0:00	System	Emergency	[Configuration Change] VLAN, Bootup:2, Startup:0d1h6m59s
10	2021/10/29 17:30:19+0:00	System	Emergency	[Configuration Change] VLAN, Bootup:2, Startup:0d1h6m48s

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

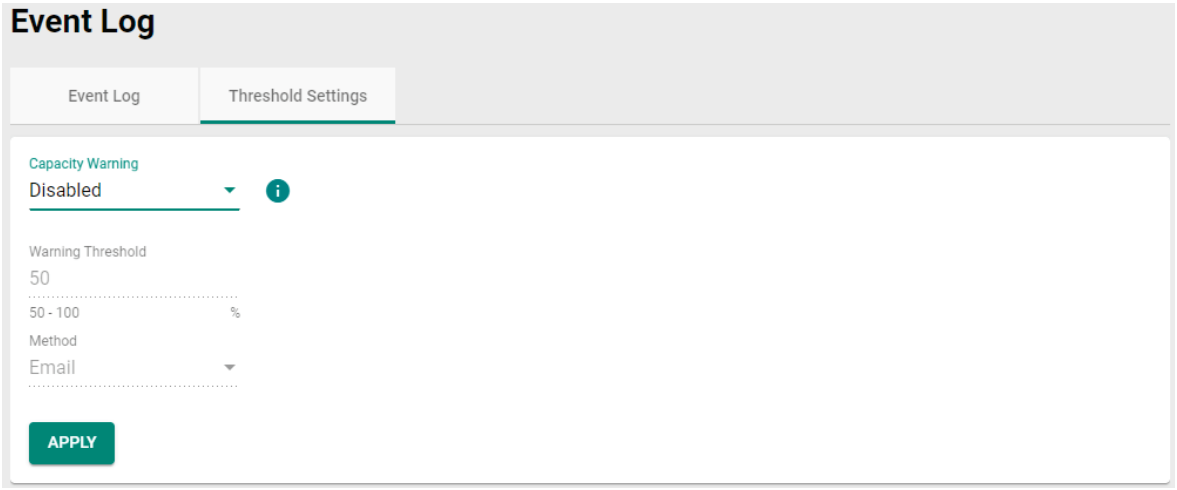
Click to refresh the event logs.

Click to delete all logs.

Click to export all logs to a file.

Threshold Settings

In the Threshold Settings screen, you can set up an early warning that triggers when the log storage has exceeded the specified storage threshold.



Capacity Warning

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable capacity warning. 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 %	Enter the threshold percentage of the current storage. Once the storage exceeds this value, the warning will trigger.	50

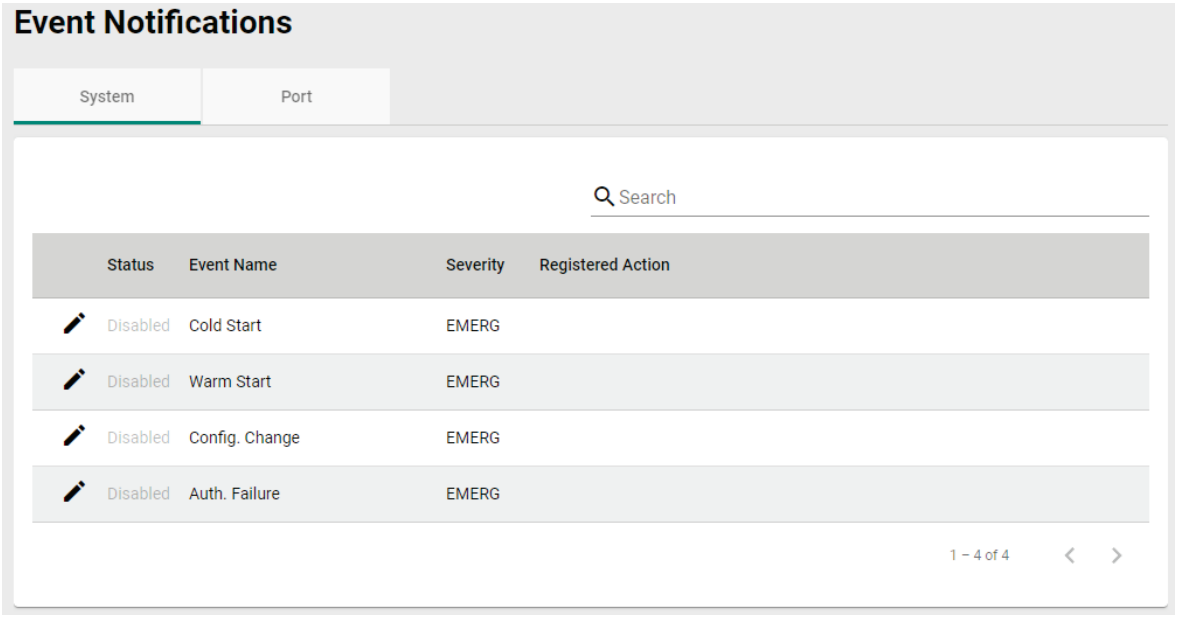
Method

Setting	Description	Factory Default
Email	Choose how the warning is sent.	Email

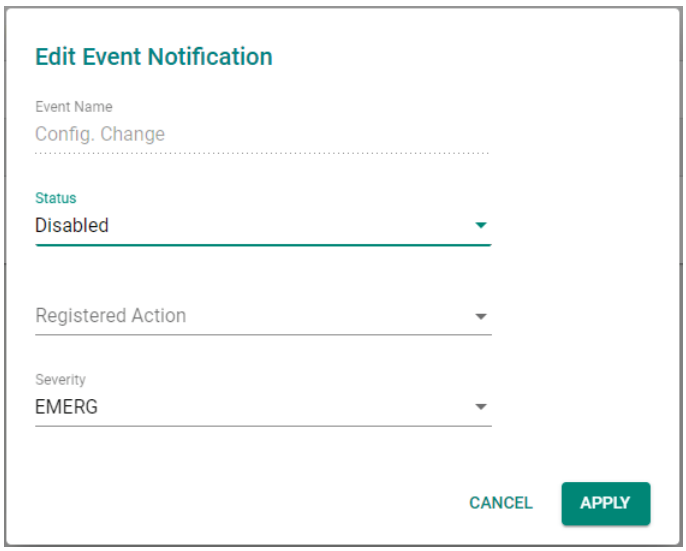
Event Notification

System

System Events are related to the overall function of the device. Each event can be activated independently with different warning approaches. Administrator also can decide the severity of each system event.



Click ✎ to modify the System Event Notification.



Event Name

Setting	Description
Cold Start	The power input was cut off and then reconnected.
Warm Start	The device was rebooted, such as when network parameters are changed (IP address, subnet mask, etc.).
Config. Change	A configuration item has been changed.
Auth. Failure	An incorrect username or password was entered.

Status

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

Registered Action

There are two response actions available on the NAT Series when events are triggered.

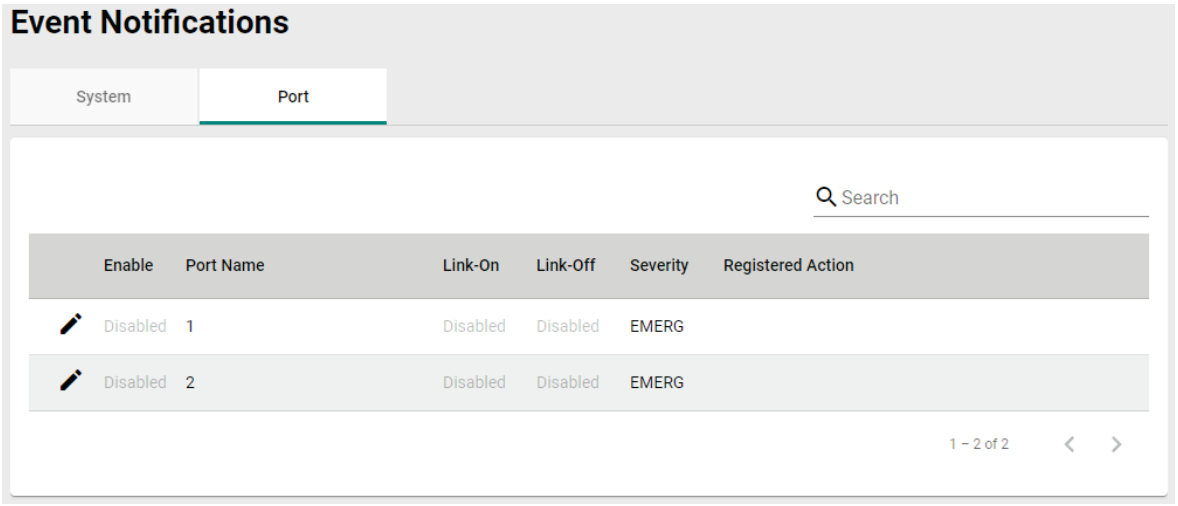
Setting	Description	Factory Default
E-Mail	The device will send a notification to the email server defined in the Email Setting section.	None
Syslog	The device will record the event on the syslog server defined in the Syslog Server Setting section.	

Severity

Setting	Description	Factory Default
EMERG	System is unusable	EMERG
ALERT	Action must be taken immediately	
CRIT	Critical conditions	
ERROR	Error conditions	
WARN	Warning conditions	
NOTICE	Normal but significant condition	
INFO	Informational messages	
DEBUG	Debug-level messages	

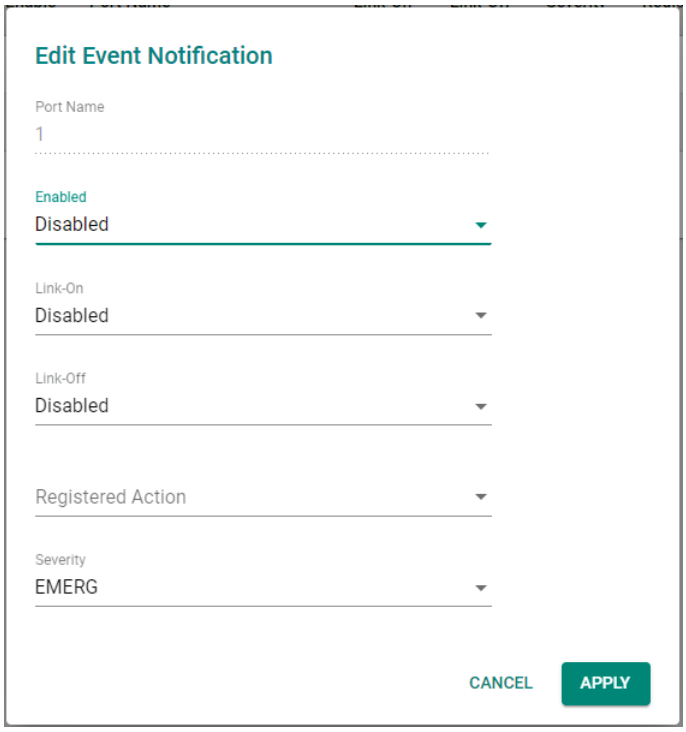
Port

Port Events are related to the activity of a specific port.



Modify a Port Event Notification

Click ✎ to modify the Port Event Notification.



Port Name

This is the physical port (1 or 2) on the NAT-102 device.

Status

Setting	Description	Factory Default
Enable/Disabled	Enable or disable event notifications for the port.	Disabled

Link-On

Setting	Description	Factory Default
Enable/Disabled	If enabled, an event is triggered when the port is connected to another device.	Disabled

Link-Off

Setting	Description	Factory Default
Enable/Disabled	If enabled, an event is triggered when the port is disconnected (e.g., the cable is pulled out, or the connected device is shut down).	Disabled

Registered Action

There are two response actions available on the NAT series when events are triggered.

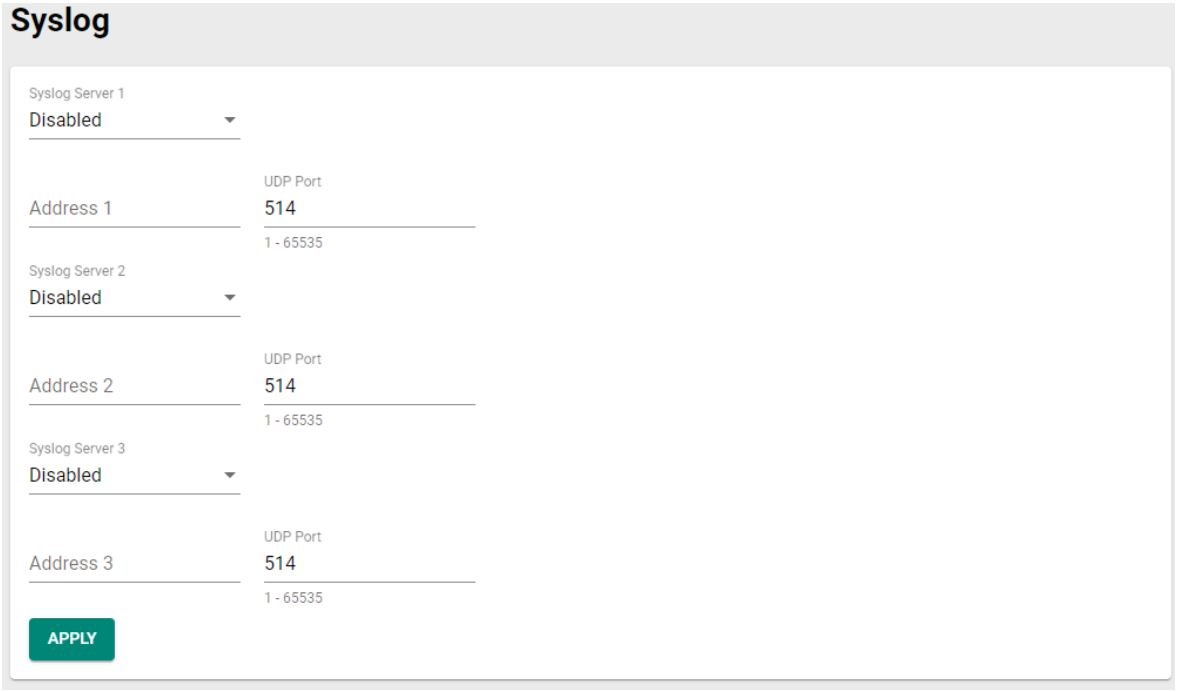
Setting	Description	Factory Default
E-Mail	The device will send a notification to the email server defined in the Email Setting section.	None
Syslog	The device will record the event on the syslog server defined in the Syslog Server Setting section.	

Severity

Setting	Description	Factory Default
EMERG	System is unusable	EMERG
ALERT	Action must be taken immediately	
CRIT	Critical conditions	

Setting	Description	Factory Default
ERROR	Error conditions	
WARN	Warning conditions	
NOTICE	Normal but significant condition	
INFO	Informational messages	
DEBUG	Debug-level messages	

Syslog



Syslog Server 1/2/3

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable syslog server 1/2/3.	Disabled

Address 1/2/3

Setting	Description	Factory Default
Address 1/2/3	Enter the IP address of Syslog server 1/2/3.	None

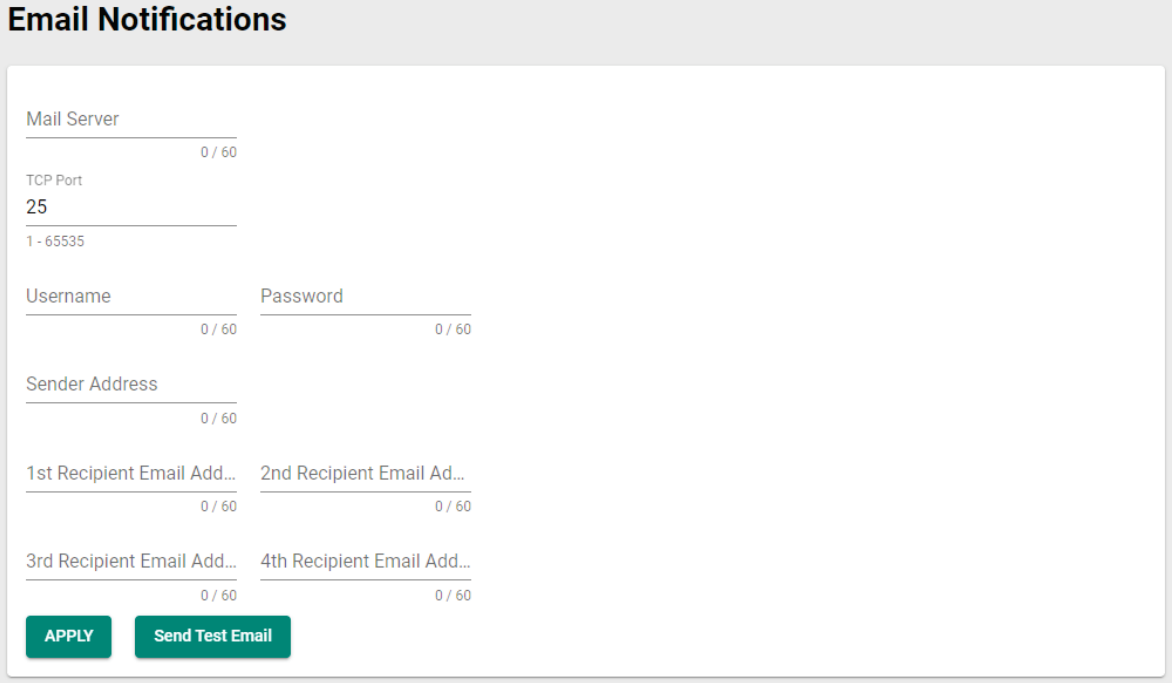
UDP Port

Setting	Description	Factory Default
1 to 65535	Enter the UDP port of Syslog server 1/2/3.	514

NOTE The following events will be recorded into the Moxa industrial NAT device's Event Log table, and will then be sent to the specified Syslog Server:

- Cold start
- Warm start
- Configuration change activated
- Authentication fail
- Port link on/off

Email Notifications



Mail Server

Setting	Description	Factory Default
Max. 60 characters	The email server address.	None

TCP Port

Setting	Description	Factory Default
1 to 65535	The TCP port of the email server.	25

Username

Setting	Description	Factory Default
Max. 60 characters	The username used to log in to the email server.	None

Password

Setting	Description	Factory Default
Max. 60 characters	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. of 60 characters	You can set up to 4 email addresses to receive alarm emails from the NAT device.	None

Send Test Email

After you complete the email settings, click **APPLY** to apply the settings first and then press the **Send Test Email** button 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.

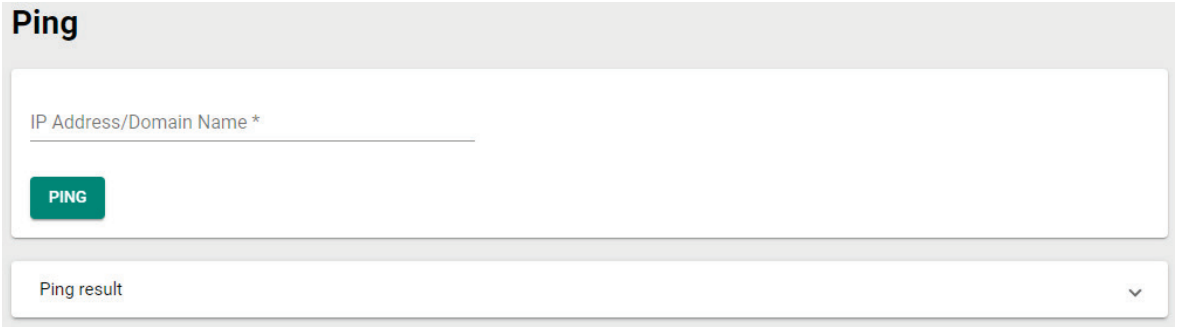
We strongly recommend not entering your account name and password if auto warning e-mail messages are delivered without an authentication mechanism.

Tools

Ping

The Ping function uses the ping command to give you a simple but powerful tool for troubleshooting network problems.

Enter the target IP address or domain name you want to ping in the IP Address/Domain Name field and click **PING**. Click ⌄ to expand the results of the ping test to identify any possible problems.



A

Account Privileges List

This appendix lists the privileges for the different account roles.

User Role Privileges

The following table lists the privileges of the different user roles for the functions of the device.

The table uses the follow letter designations:

- **R**: Read-only privilege
- **W**: Write privilege
- **R/W**: Read/write privilege

Function	**Account Privilege**		
System	**Admin**	**Supervisor**	**User**
System Management			
- Device Information	R/W	R/W	R
- Firmware Upgrade	R/W	R/W	R
- Configuration Backup and Restore	R/W	R/W	R
- Restore	R/W	R/W	R
Account Management			
- User Account	R/W	R	R
- Password Policy	R/W	R/W	R
Management Interface			
- User Interface	R/W	R/W	R
Time			
- System Time	R/W	R/W	R
- Time Zone	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	R	R
Layer 3 Interface	R/W	R/W	R
Network Service	**Admin**	**Supervisor**	**User**
DHCP Server	R/W	R/W	R
Routing & NAT	**Admin**	**Supervisor**	**User**
Unicast Routing			
- Static Routes	R/W	R/W	R
- Routing Table	R	R	R
NAT Setting	R/W	R/W	R
Firewall	**Admin**	**Supervisor**	**User**
Layer 3 Policy	R/W	R/W	R

Security	Admin	Supervisor	User
Device Security			
- Login Policy	R/W	R/W	R
- Trusted Access	R/W	R/W	R
- SSH & SSL	R/W	R/W	R
Network Security			
- Port Security	R/W	R/W	R
Diagnosis	**Admin**	**Supervisor**	**User**
System Status			
- Resource Utilization	R/W	R/W	R
Log & Event Notification			
- Event Log	R/W	R/W	R
- Event Notifications	R/W	R/W	R
- Syslog	R/W	R/W	R
- Email Notifications	R/W	R/W	R
Tools			
- Ping	R/W	R/W	R