TAP-M310R Series User Manual

Version 1.1, November 2025

www.moxa.com/products

TAP-M310R Series User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About This Manual 5
Symbol Definition for Web Interface Configurations 5
About Note, Attention, and Warning 6
Configuration Reminders 7
A: About Mandatory Parameters 7
B: Preconfiguring Settings 7
2. Getting Started 9
Functional Design 9
LED Indicators 9
Reset Button 12
First-time Installation and Configuration 12
Communication Testing 15
3. Web Interface Configuration 17
Function Introduction 17
Device Summary 18
Device Information 18
System Information 18
System Status 18
Security Status 19
System 19
System Management 20
Account Management 30
Management Interface 39
Time 46
Wi-Fi 51
Wireless Settings 51
Connection Management 71
Wi-Fi Security 78
Ports 81
Port Settings 82
Layer 2 Switching 83
VLAN 84
Storm Protection (TAP-M310R-1P1R1S and -1P2R1S Only) 88
Turbo Chain (TAP-M310R-1P1R1S and -1P2R1S Only) 89
IP Configuration 91
General Settings 91
IPv6 92
IP Configuration Status 95
Network Service 96
DHCP Server 96
DHCPv6 Server 96
Routing and NAT 98
Routing 98
NAT 100
Firewall 106
Layer 2 Policy 106
Layer 3 Policy 108
Certificate Management 110
Certificates 111
CA Certificates 112
Security 112
Device Security 113
Diagnostics 115
Security Status 115
System Status 116
Network Status 119
Event Logs and Notifications 122
Tools 132

Setup Wizard 141
Wi-Fi Basic 141
Wi-Fi Security 144
System 146
Connect to Wireless Controller System (WCS) 148
General Settings 148
Connection Status 149
Maintenance and Tools 149
Language 150
Disable Auto Save 151
Locator 151
Reboot 152
Reset to Defaults 153
Renew Device Unique Key 155
Change Password 155
Log Out 157
A. Supporting Information 158
Device Recovery 158
B. Accessing the Serial Consoles 160
RS-232 Console Configuration (115200, None, 8, 1, VT100) 160
Configuration by Telnet and SSH Consoles 162
C. Security Guidelines 164
Installation 164
Physical Installation 164
Account Management 165
Vulnerable Protocols 165
Operation 166
Defense-in-depth Strategy 166
Maintenance 167
Decommission 167
D. Service Authority Table 168

1. About This Manual

Thank you for purchasing a Moxa's TAP-M310R Series product. Read this user's manual to learn how to connect your Moxa product with various interfaces and how to configure all settings and parameters via the user-friendly web interface. Since all TAP-M310R Series use the same firmware image, the screenshots for common features will be identical for all models, with the exception of the model name.

Three methods can be used to connect to the Moxa's device, which all will be described in the next two chapters. See the following descriptions for each chapter's main functions.

Chapter 2: Getting Started

In this chapter, we provide instructions on how to initialize the configuration on Moxa's product. We provide two interfaces to access the configuration settings: CLI (Command Line Interface) via the RS-232 console or SSH/Telnet interfaces, and web interface.

Chapter 3: Web Interface Configuration

In this chapter, we explain how to access the TAP-M310R Series various configuration, monitoring, and management functions. These functions can be accessed through a web browser, or through the command line console (CLI). In this manual, we describe how to configure the TAP-M310R Series functions via the web interface, which provides the most user-friendly way to configure a Moxa device. For more information on how to configure the TAP-M310R Series using the command line interface, refer to the TAP-M310R Series Command Line Interface User Manual.

Symbol Definition for Web Interface Configurations

The Web Interface Configuration includes various symbols. For your convenience, refer to the following table for the meanings of the symbols.

Symbols	Meanings
	Add
	Read detailed information
	Clear all
	Column selection
	Refresh
	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save the configuration.
	Export
	Edit
	Perform a Wi-Fi site survey (Client mode only)
	Re-authentication
	Delete
	Panel View

Symbols	Meanings
	Expand
	Collapse
	Hint or additional information
	Settings
	Data comparison
	Menu icon
	Change mode
	Locator
	Reboot
	Reset to defaults
	Logout
	Increase
	Decrease
	Equal
	Menu
	Search
	Hide text that is typed into a text box (usually used when typing a password)
	Show text typed into a text box (usually used when checking a password)

About Note, Attention, and Warning

Throughout the whole manual, you may see notes, attentions, and warnings. The definition of each type is explained below.

Note: This is used to provide additional information for a function, feature, or scenario. Here is an example:

NOTE

Reset to Default button is disabled by default; users need to enable it in the web console if they want to use it.

Attention: This is used to notify readers of matters or situations that require extra attention to avoid possible issues. Here is an example:

ATTENTION

When a different type of module has been inserted into the TAP-M310R Series, we suggest you configure the settings, or use reset-to-default.

Warning: This is used to notify readers of matters or situations that require extra attention to avoid serious harm to the user or the device. Here is an example:

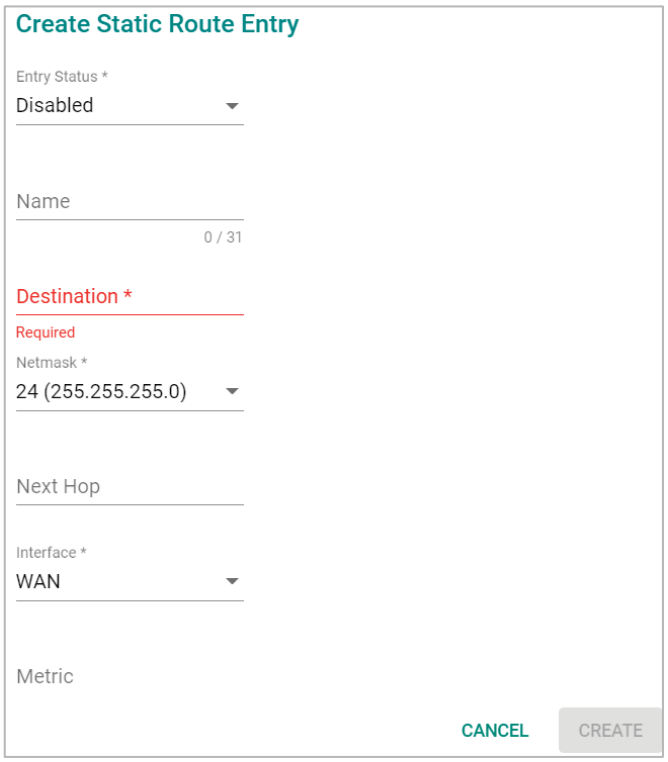
WARNING

There is a risk of explosion if the battery is replaced by an incorrect type.

Configuration Reminders

In this section, several examples will be used to remind users when configuring the settings for Moxa's TAP-M310R Series.

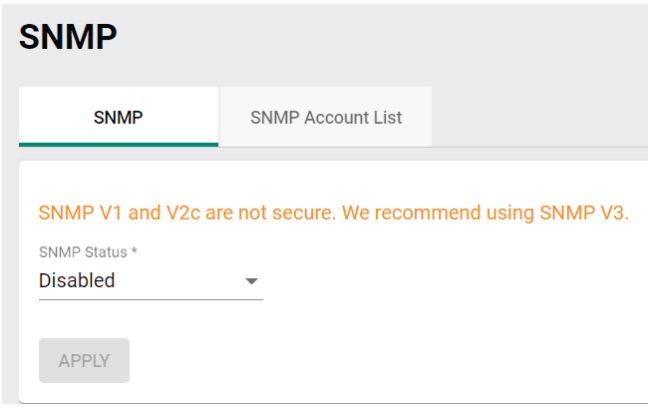
A: About Mandatory Parameters



- The items with asterisks mean they are mandatory parameters that must be provided. In the figure above, the parameters for Entry Status, Destination, and Interface are required to be able to save or apply the configuration.
- If an item is marked in red means this item has been skipped. You need to fill in the parameters or you cannot apply or create the function.
- Some parameter values will be limited to a specific range. If the values exceed the range, it cannot be applied or created.
- Configuration input fields universally do not allow the following special characters: backslash (\), apostrophe ('), double quotes ("), backtick (`).

B: Preconfiguring Settings

Some function settings can be configured while the function is disabled. These changes will take effect when the function is enabled, without having to reconfigure the settings again. For example, on the SNMP configuration page, users can configure the SNMP Account List settings while SNMP is disabled. When SNMP is enabled, the previously configured Account List settings will take effect.


SNMP
SNMP
SNMP Account List
SNMP V1 and V2c are not secure. We recommend using SNMP V3.
SNMP Status *
Disabled
APPLY

2. Getting Started

In this chapter, we provide an overview of the TAP-M310R Series, and explain how to log into the Moxa's TAP-M310R Series for the first time through the web-based interface.

Functional Design

LED Indicators

The LEDs on the front panel of the TAP-M310R Series provide a quick and easy means of determining the current operational status and wireless settings.

The front panel of each module contains several LED indicators. The function of each LED is described in the following tables.

Radio Module

LED	Color	State	Description
PWR L	Green	On	Power is being supplied from a power module on the left side (if any).
		Off	Power is not being supplied from a power module on the left side.
PWR R	Green	On	Power is being supplied from a power module on the right side (if any).
		Off	Power is not being supplied from a power module on the right side.
PWR	Green	On	Power is being supplied to the 24 VDC input of the radio module.
		Off	Power is not being supplied via the 24 VDC input of the radio module, or the switch module is present.
SYS	Green	On	Indicates a system initialization failure, configuration error, or system error. This LED will be off during the regular boot up process.
	Red	On	System startup is complete, and the system is operating normally.
LAN1	Red	On	The LAN port's 2500 Mbps link is active.
		Blinking	Data is being transmitted at 2500 Mbps.
	Green	On	The LAN port's 10/100/1000 Mbps link is active.
		Blinking	Data is being transmitted at 10/100/1000 Mbps
	Green/ Amber	Off	The LAN port is inactive.

LED	Color	State	Description
2.4G	Green	On	The device is in Client(-router) or Slave mode and an active link is established to an AP or master on the 2.4 GHz band.
		Blinking	Traffic is being transmitted in Client(-router) or Slave mode over the 2.4 GHz band.
	Amber	On	The device is in AP, Master, Sniffer mode and the 2.4 GHz band is active.
		Blinking	Traffic is being transmitted in AP or Master mode over the 2.4 GHz band.
	Green/ Amber	Off	The 2.4 GHz band is disabled, not working properly, or the device is in Client(-router) or Slave mode without a connection to an AP or Master.
5G	Green	On	The device is in Client(-router) or Slave mode and an active link is established to an AP or master on the 5 GHz band.
		Blinking	Traffic is being transmitted in Client(-router) or Slave mode over the 5 GHz band.
	Amber	On	The device is in AP, Master, or Sniffer mode and the 5 GHz band is active.
		Blinking	Traffic is being transmitted in AP or Master mode over the 5 GHz band.
	Green/Amber	Off	The 5 GHz band is disabled, not working properly, or the device is in Client(-router)/Slave mode without a connection to an AP or Master.

Switch Module

For models with a switch module only (TAP-M310R-1P1R1S, -1P2R1S).

LED	Color	State	Description
PWR L	Green	On	Power is being supplied from a power module on the left side (if any).
		Off	Power is not being supplied from a power module on the left side.
PWR R	Green	On	Power is being supplied from a power module on the right side (if any).
		Off	Power is not being supplied from a power module on the right side.
HEAD	Green	On	Turbo Chain redundancy is enabled, and the Head port is in the Link Up Forward (LUF) state.

LED	Color	State	Description
		Blinking	Turbo Chain redundancy is enabled, and - the switch module is the Head switch, and the Head port is not in the Link Up Forward (LUF) state. - the switch module is the Member switch, and Member port 1 is not in the Link Up Forward (LUF) state. - the switch module is the Tail switch, and the Member port is not in the Link Up Forward (LUF) state.
		Off	The Moxa Turbo Chain or the Moxa Turbo Chain is enabled, and - the switch module is the Member switch and Member port 1 is in the Link Up Forward (LUF) state. - the switch module is the Tail switch, and the Member port is in the Link Up Forward (LUF) state.
TAIL	Green	On	Turbo Chain redundancy is enabled, and the Tail port is in the Link Up Forward (LUF) state.
		Blinking	The Moxa Turbo Chain is enabled, and - the switch module is the Head switch, and the Head Port is not in the Link Up Forward (LUF) state. - the switch module is the Member switch, and Member Port 2 is not in the Link Up Forward (LUF) state. - the switch module is the Tail switch, and the Member Port is not in the Link Up Forward (LUF) state.
		Off	Turbo Chain redundancy is disabled or Turbo Chain redundancy is enabled, and - the switch module is the Head switch, and the Member Port is in the Link Up Forward (LUF) state. - the switch module is the Member switch, and Member Port 2 is in the Link Up Forward (LUF) state.
LAN2/3 (SFP)	Green	On	The LAN port's 2500 Mbps link is active.
		Blinking	Data is being transmitted at 2500 Mbps.
	Amber	On	The LAN port's 10/100/1000 Mbps link is active.
		Blinking	Data is being transmitted at 10/100/1000 Mbps
	Green/ Amber	Off	The LAN port is inactive, the SFP module or SFP cabling is attached properly.
LAN4/5	Green	On	The LAN port's 2500 Mbps link is active.
		Blinking	Data is being transmitted at 2500 Mbps.
	Amber	On	The LAN port's 10/100/1000 Mbps link is active.
		Blinking	Data is being transmitted at 10/100/1000 Mbps
	Green/ Amber	Off	The LAN port is inactive.

Power Module

For models with a power module only (TAP-M310R-1P1R1S, -1P2R1S, -NPS-1P1R).

LED	Color	State	Description
PWR	Green	On	The power module is active and supplying power.
		Off	The power module is idle and not supplying power.

Reset Button

The Reset is located on the front panel of the device. You can reboot the TAP-M310R series or reset it to factory default settings by pressing the **RESET** button with a pointed object such as an unfolded paper clip.

- **System reboot:** Hold down the Reset button for 1 to 5 seconds and then release. The SYS LED will blink at 1 Hz.
- **Reset to factory default:** Hold down the Reset button for longer than 5 seconds until the SYS LED starts blinking green. Release the button to reset the TAP-M310R Series to its factory default settings. The SYS LED will blink at 4 Hz.
- **Abort the action:** Hold the Reset button down for longer than 10 seconds and then release to abort the reset action. The SYS LED will stop blinking and turn solid.

NOTE

The reset to default factory settings function of the reset button is disabled by default and must be enabled in the web console. Refer to the Reset Button Active Duration section for more detailed information.

First-time Installation and Configuration

Before installing the TAP-M310R Series, make sure that all items in the Package Checklist listed in the Quick Installation Guide are in the box. You will need access to a notebook computer or PC equipped with an Ethernet port.

Step 1: Connect the TAP to a suitable power source.

The TAP-M310R Series supports multiple power input options, depending on the model used. Refer to the Quick Installation Guide (QIG) for more details and instructions.

Step 2: Connect the TAP device's LAN1 port to a notebook or PC.

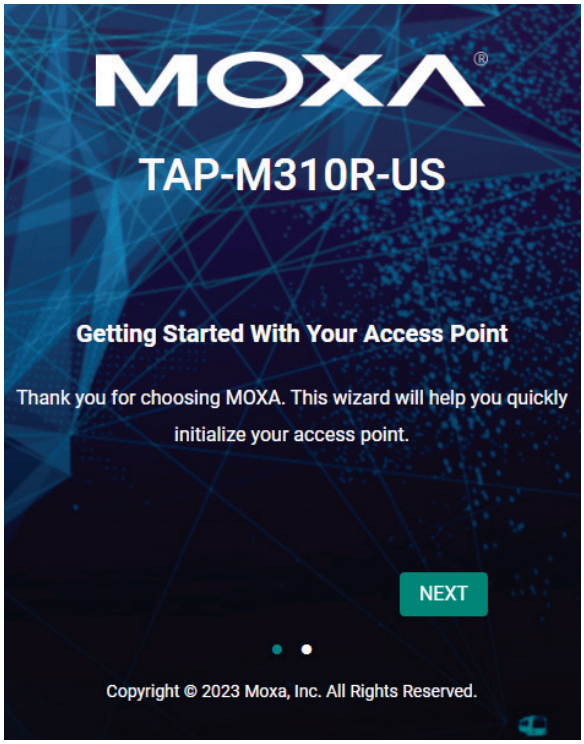
The LED indicator on the TAP Series' LAN port will light up when a connection is established.

Step 3: Set up the computer's IP address.

Choose an IP address on the same subnet as the TAP Series. Since the TAP Series' default IP address is **192.168.127.253**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**, where xxx is a value between 1 and 252.

Step 4: Access the homepage of the TAP.

Open your computer's web browser and type **https://192.168.127.253** in the address field to access the TAP's homepage. If successfully connected, the TAP's interface homepage will appear. Click **NEXT**.

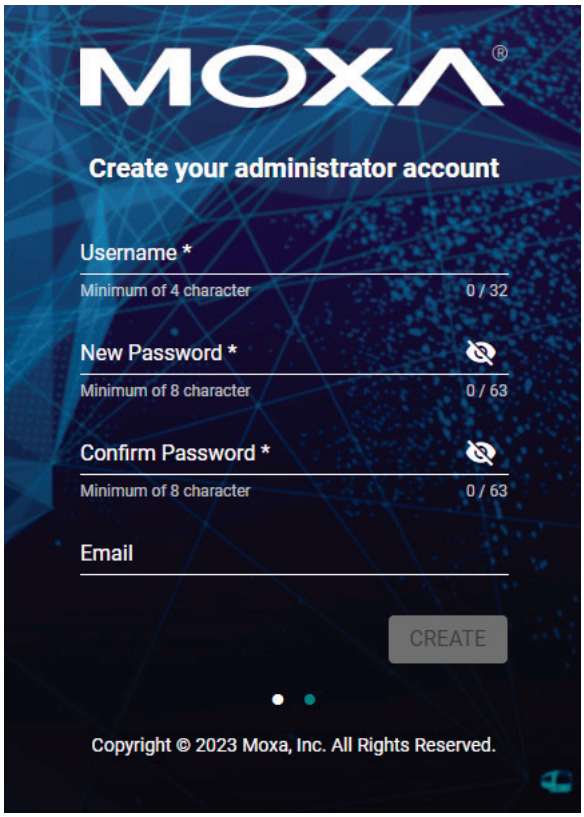


Step 5: Create a user account and password.

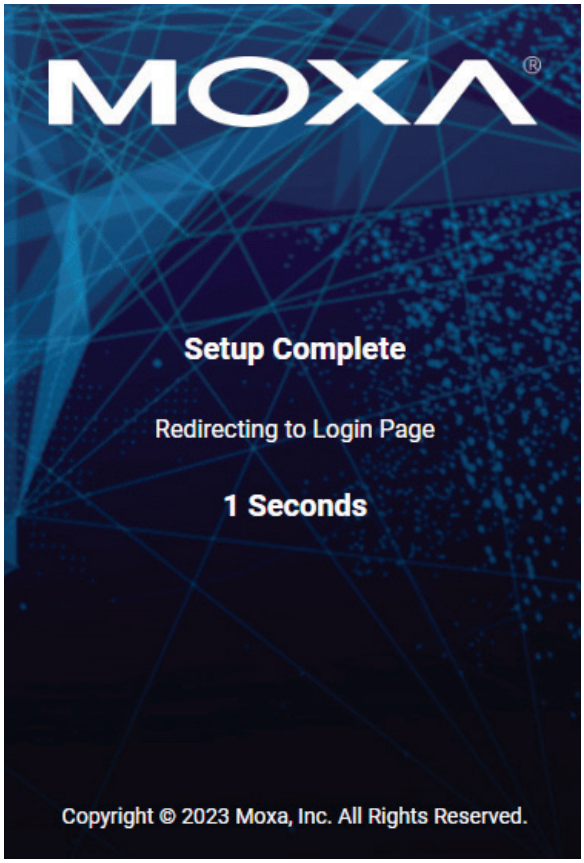
There is no default user account and password. Enter the username, password, and email address for your user account and click **CREATE**.

NOTE

The username and password are case-sensitive.



After creating your account, you will be automatically redirected to the login screen.



Step 6: Log in to the device.

Enter your username and password and click **LOG IN**.

Communication Testing

After installing the TAP-M310R Series you can run a sample test to make sure the TAP-M310R Series and the wireless connection are functioning normally.

How to Test the TAP-M310R Series as an AP

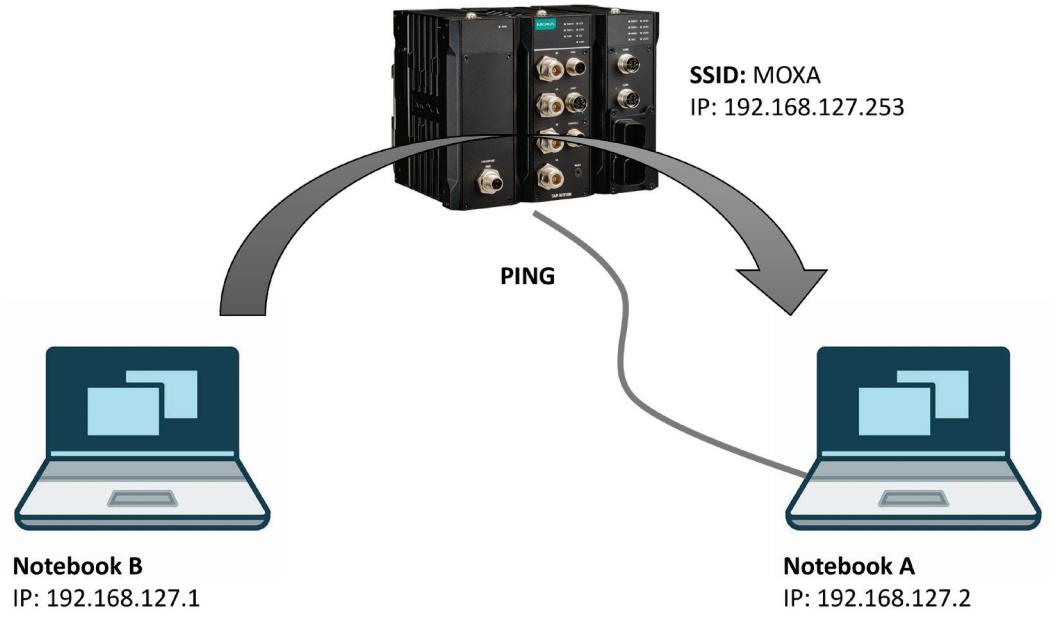
TAP-M310R-1P1R1S and -1P2R1S only

If you are testing the TAP-M310R Series device as an AP, you will need a second notebook computer equipped with a WLAN card. Configure the WLAN card to connect to the TAP-M310R Series and change the IP address of the second notebook (Notebook B) so that it is on the same subnet as the first notebook (Notebook A), which is connected to the TAP-M310R Series.

After configuring the WLAN card, establish a wireless connection with the TAP-M310R Series and open a DOS window on Notebook B. At the prompt, type the following command:

ping *<IP address of notebook A>*

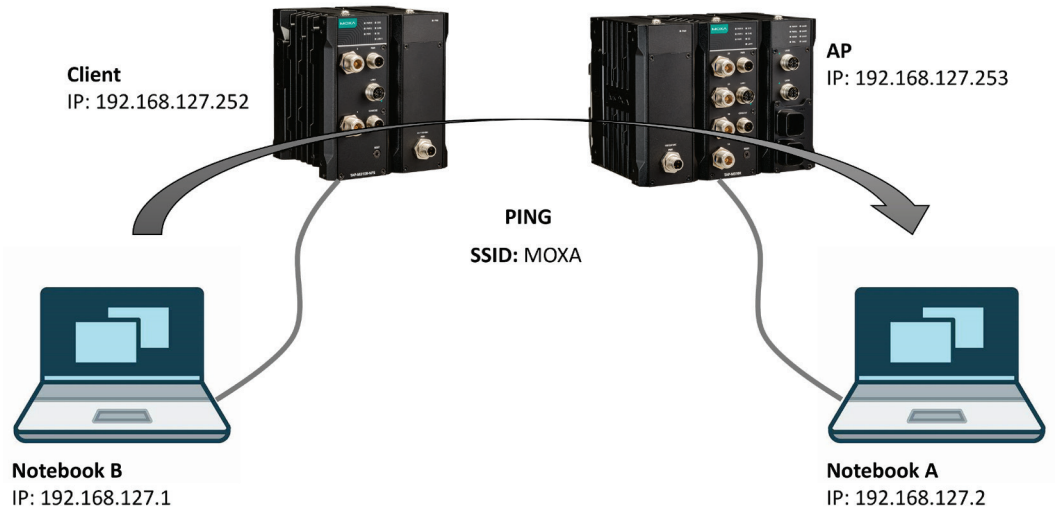
Press **Enter** to execute the command (see the figure below). A "Reply from IP address …" response means the communication was successful. A "Request timed out." response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.



How to Test the TAP-M310R Series as a Client

TAP-M310R-NPS-1R and -1P1R only

If you are testing the TAP-M310R Series as a Client, you will need a second notebook computer (Notebook B) equipped with an Ethernet port as well as an AP connected to notebook A. Configure the TAP-M310R Series connected to notebook B for Client mode with the correct SSID and credentials matching the target AP.



After setting up the testing environment, open a DOS window on notebook B. At the prompt, type:

ping *<IP address of notebook A>*

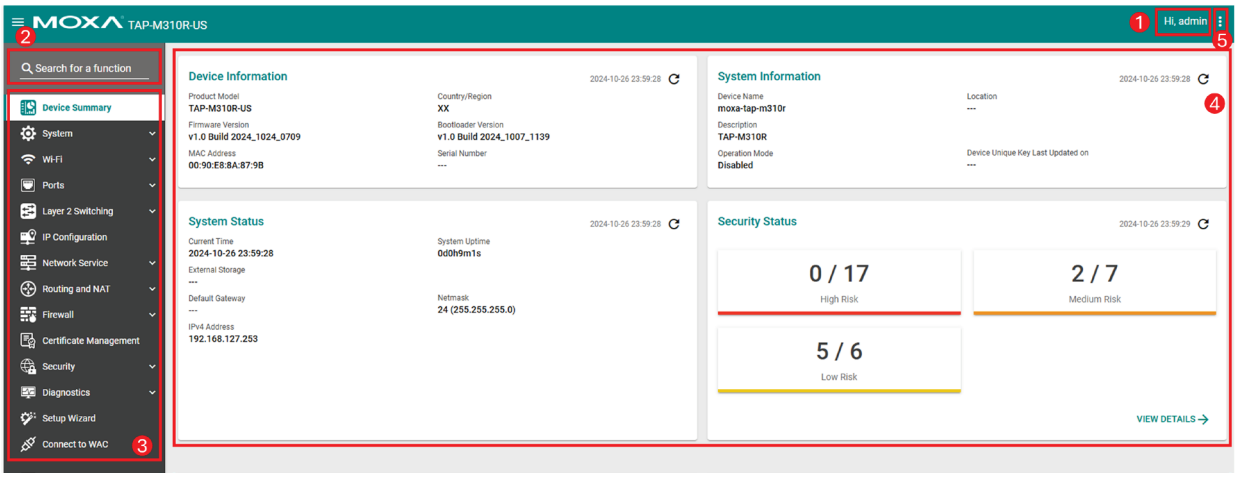
and then press **Enter**. A "Reply from IP address …" response means the communication was successful. A "Request timed out" response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.

3. Web Interface Configuration

Moxa's TAP-M310R Series offers a user-friendly web interface for easy configuration. All functions of the TAP-M310R Series can be configured via this web interface.

Function Introduction

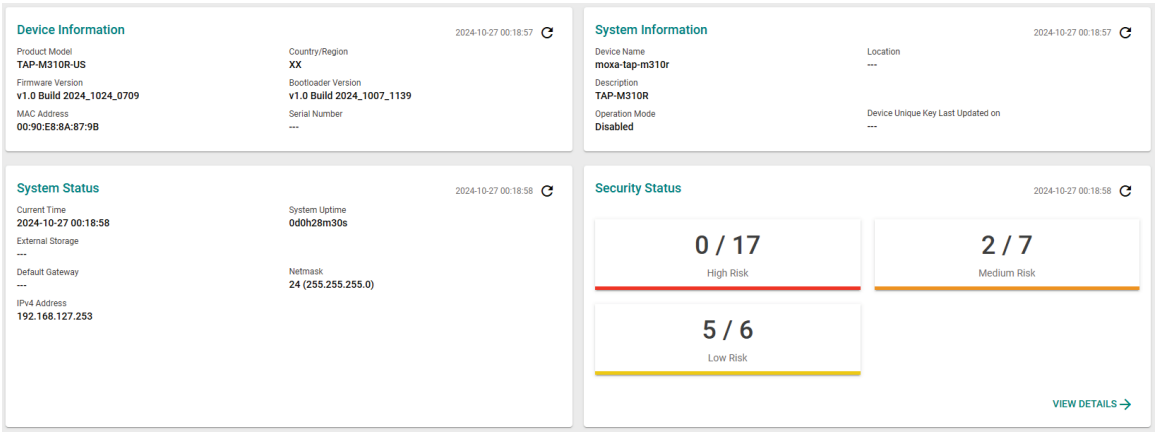
This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



1. **Login Name:** This shows the name of the user that is currently logged in.
2. **Search Bar:** Type the name of the function you want to search for in the function menu tree.
3. **Function Menu:** All functions of the TAP-M310R Series are shown here. Click the function you want to view or configure.
4. **Device Summary:** All important device information and statistics are shown here.
5. **Maintenance:** Functions for device maintenance are located here.

Device Summary

After successfully connecting to the TAP-M310R Series, the **Device Summary** will automatically appear. To view the device summary from anywhere in the interface, click **Device Summary** on the Function Menu.



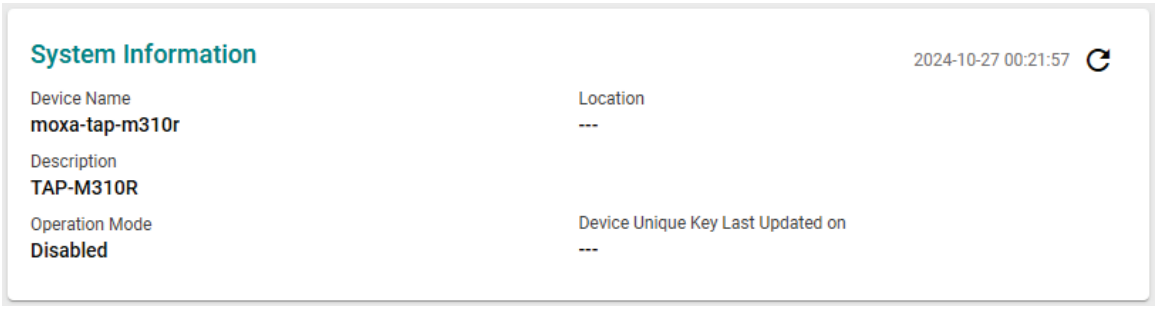
See the following sections for a detailed description of each widget.

Device Information

This shows the model information, including product model name, the country or region of RF compliance, and firmware version.

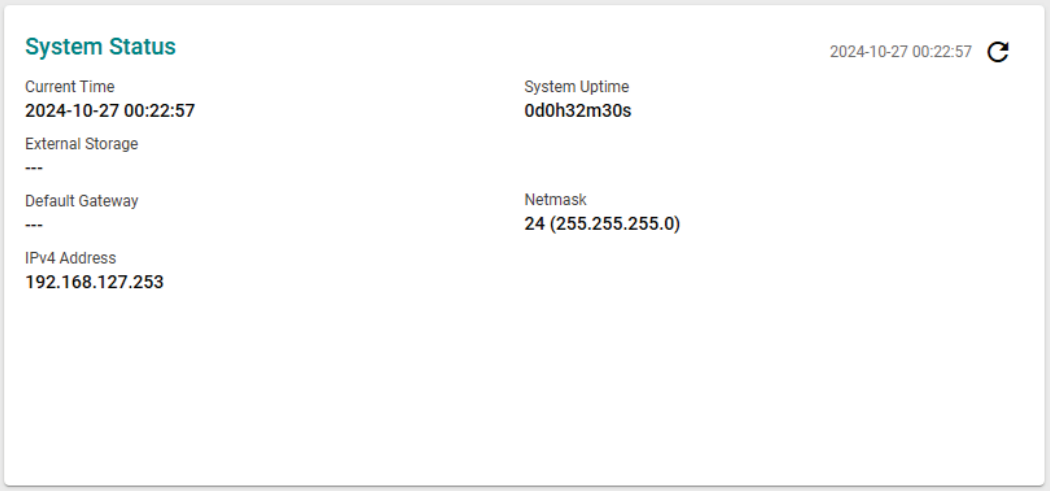
System Information

This shows system information including the device name, location, description, and current operation mode.



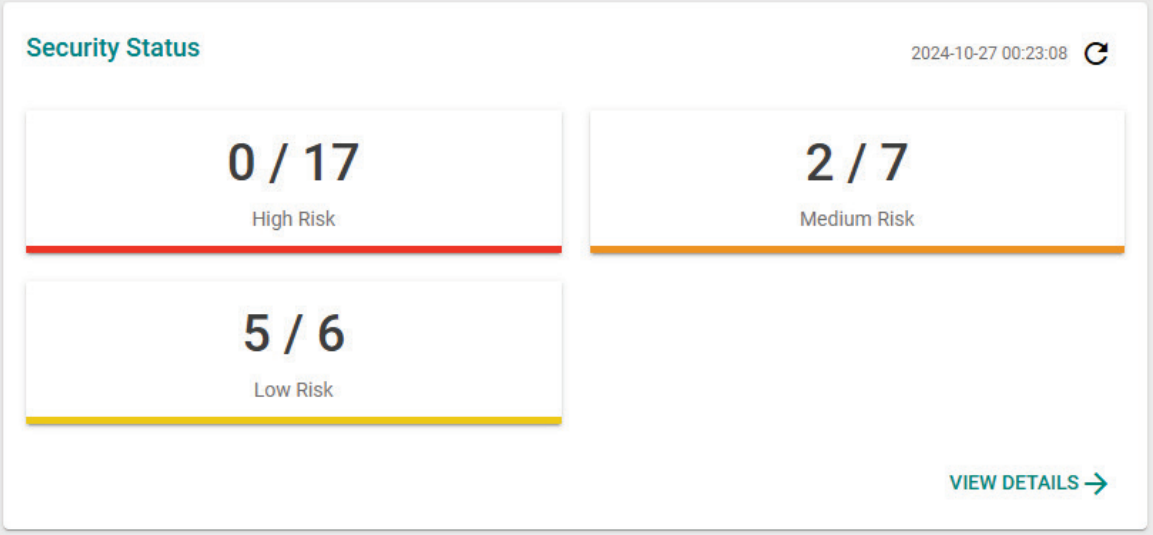
System Status

This shows the system status, including system time, system uptime, and IP address.



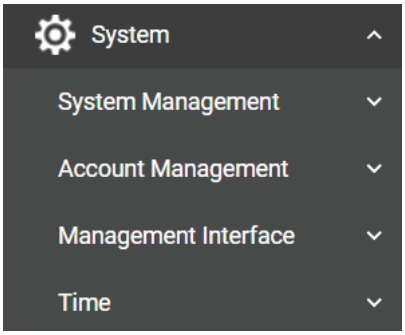
Security Status

This section reflects the overall device security status categorized into High, Medium, and Low risks. The accompanying link opens a detailed view of the risk entries to check the risk details at a glance. This allows administrators to evaluate and take mitigation action where necessary.



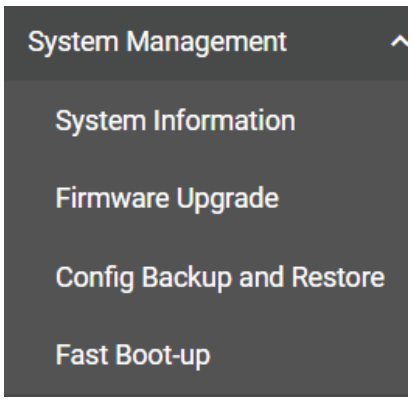
System

The **System** section houses all device and system configuration functions. From here, you can configure the **System Management, Account Management, Management Interface**, and **Time** settings.



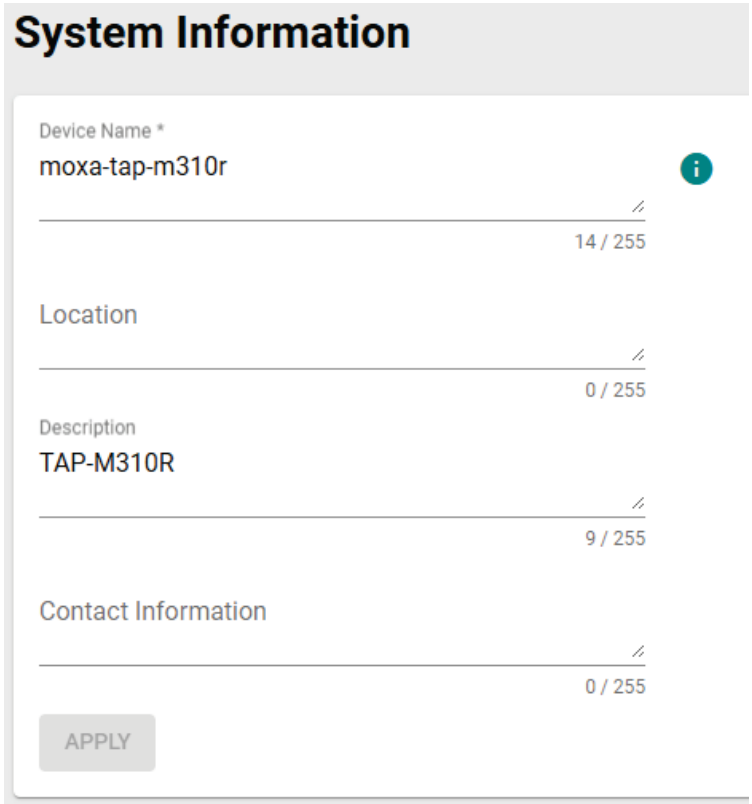
System Management

The **System Management** section houses four subsections: **System Information, Firmware Upgrade, Configure Backup and Restore**, and **Fast Boot-up**.



System Information

On the **System Information** screen, you can enter a device name, description, and location for the device. This makes it easier to identify different TAP devices that are connected to your network.



Device Name

Setting	Description	Factory Default
1 to 255 characters	Enter a name for the device. This is useful for differentiating between the roles or applications of different units. Note that the device name cannot be empty and must comply with the following naming rules: • Only supports letters (a-z), numbers (0-9), and special character dash (-) • Cannot contain spaces • Cannot start with dash (-) • Cannot end with dash (-) • When used in a PROFINET environment, cannot start with the prefix "port-x" where "x" equals 0 to 9. There is no validity to identify incorrect name formats.	moxa-tap-m310r

Location

Setting	Description	Factory Default
Max. 255 characters	Enter a location for the device. This is useful for identifying where the device is deployed. Example: production line 1.	None

Description

Setting	Description	Factory Default
Max. 255 characters	Enter a description for the device.	TAP-M310R

Contact Information

Setting	Description	Factory Default
Max. 255 characters	Enter the contact information of the person responsible for the device in case there is a problem with the device.	None

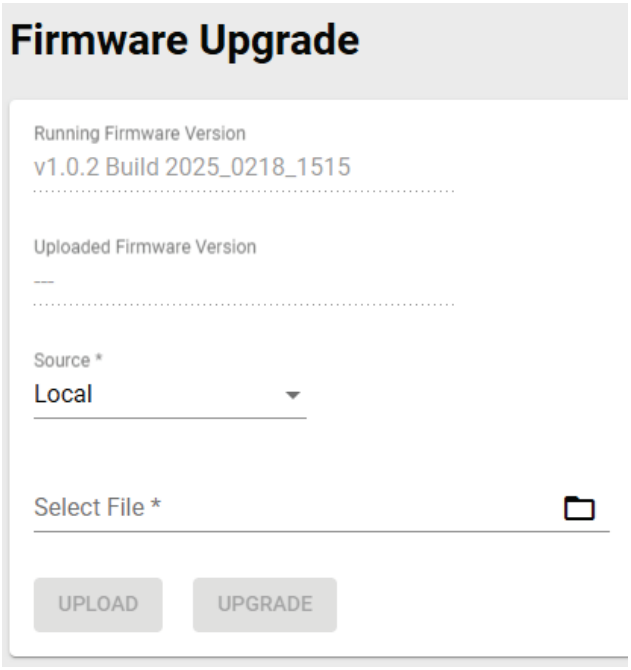
When finished, click **APPLY** to save your changes.

Firmware Upgrade

There are three ways to update your TAP-M310R's device firmware: from a local *.rom file, by remote TFTP server, or remote SFTP server.

Local

Select **Local** from the Source drop-down list. Before performing the firmware upgrade, download the target firmware (*.rom) file first from Moxa's website (www.moxa.com) to the local host.



Running Firmware Version

Setting	Description	Factory Default
Current firmware version number	This shows the current running firmware version.	Current running version

Uploaded Firmware Version

Setting	Description	Factory Default
New firmware version number	This shows the new firmware version.	None

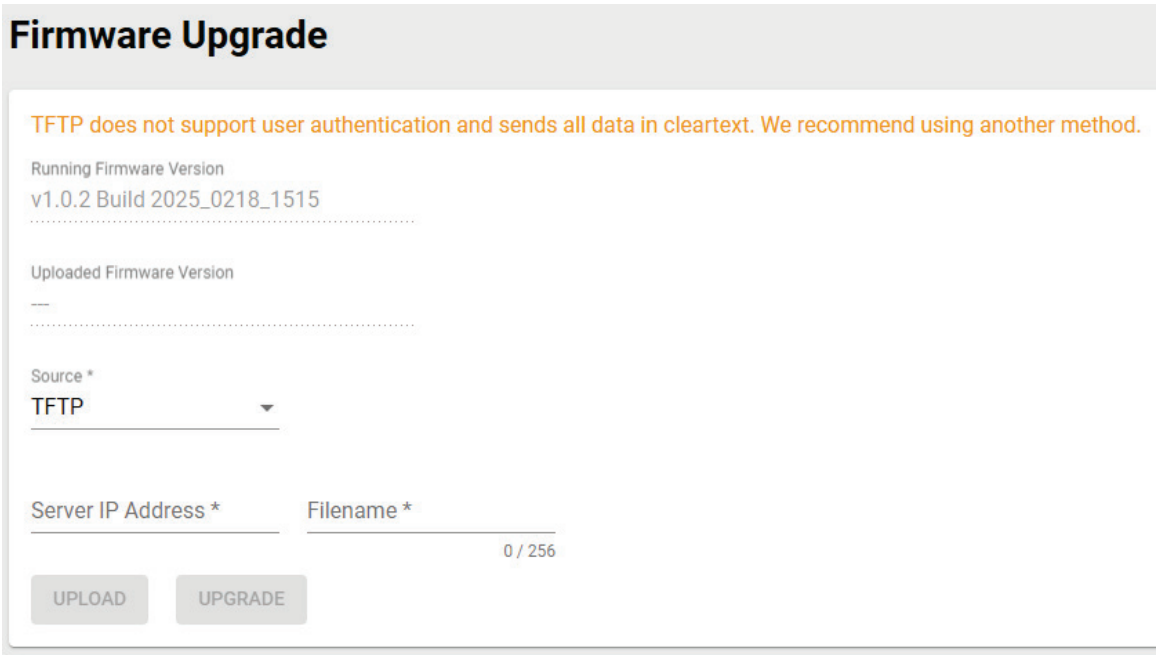
Select File

Setting	Description	Factory Default
Select the firmware file	Click the browse icon and navigate to the firmware file on the local host.	None

When finished, click **UPLOAD** to upload the file, then click **UPGRADE** to perform the firmware upgrade.

TFTP Server

Select **TFTP** from the Source drop-down list.



Running Firmware Version

Setting	Description	Factory Default
Current firmware version number	This shows the current running firmware version.	Current running version

Uploaded Firmware Version

Setting	Description	Factory Default
New firmware version number	This shows the new firmware version.	None

Server IP Address

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

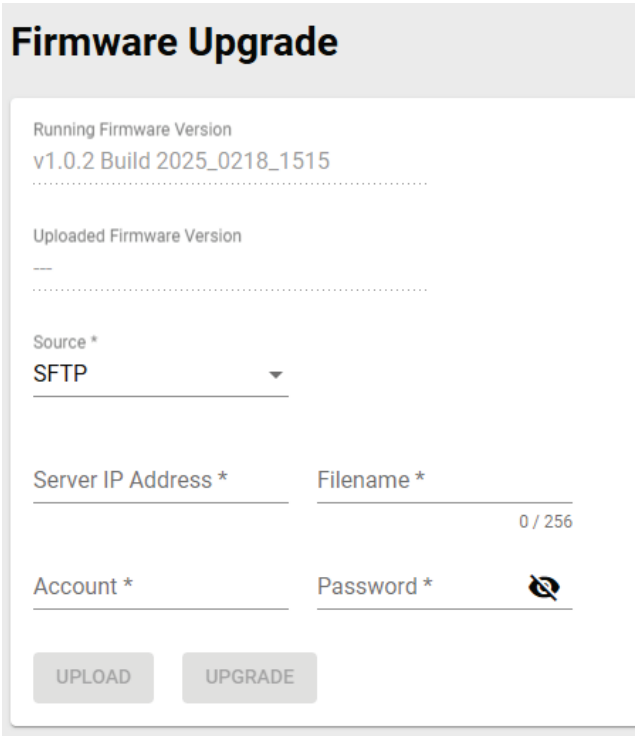
File Name

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

When finished, click **UPLOAD** to upload the file, then click **UPGRADE** to perform the firmware upgrade.

SFTP

Select **SFTP** from the Source drop-down list.



Running Firmware Version

Setting	Description	Factory Default
Current firmware version number	This shows the current running firmware version.	Current running version

Uploaded Firmware Version

Setting	Description	Factory Default
New firmware version number	This shows the new firmware version.	None

Server IP Address

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

File Name

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

Account

Setting	Description	Factory Default
SFTP server account	Enter the SFTP user account name. This account must be authorized to ensure a secure connection to the SFTP server.	None

Password

Setting	Description	Factory Default
SFTP server password	Enter the SFTP user account password. This account must be authorized to ensure a secure connection to the SFTP server.	None

When finished, click **UPLOAD** to upload the file, then click **UPGRADE** to perform the firmware upgrade.

Configuration Backup and Restore

There are three ways to back up and restore your Moxa TAP-M310R's configuration: from a local configuration file, by remote TFTP server, or remote SFTP server.

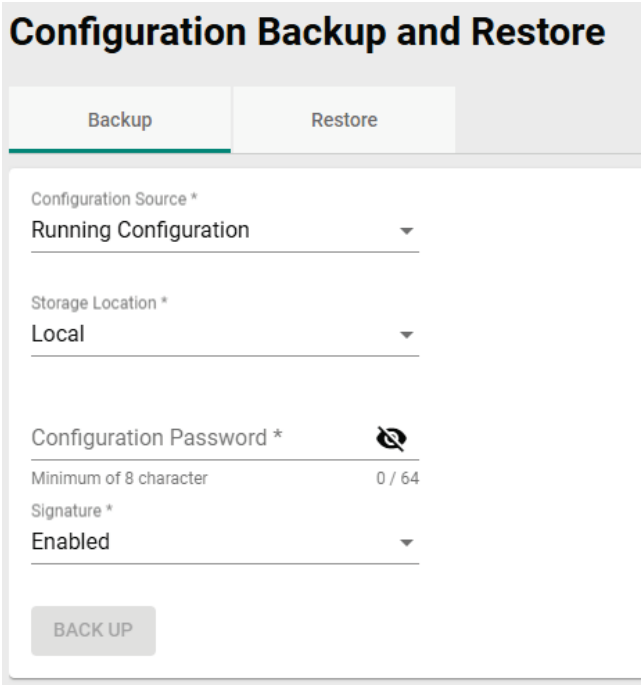
For all Backup and Restore methods, users can enable or disable CA signature. Enabling this function provides additional security by verifying the integrity of the configuration file.

Backup

The **Backup** tab is used to export a backup of the current configuration. This backup file can then be used to restore the device's configuration settings, or to import it to other TAP-M310R Series devices.

Local

Select **Local** first from the Storage Location drop-down list.



Configuration Source

Setting	Description	Factory Default
Running Configuration	Back up the running configuration.	Running Configuration
Startup Configuration	Back up the start-up configuration.	

Storage Location

Setting	Description	Factory Default
Local	**Back up the configuration files for the local computer.**	Local
TFTP	Back up the configuration files via TFTP.	
SFTP	Back up the configuration files via SFTP.	

Configuration Password

Setting	Description	Factory Default
Configuration password	Enter the configuration password. You will need to enter this password when importing the backup file. The password must be at least 8 characters long.	None

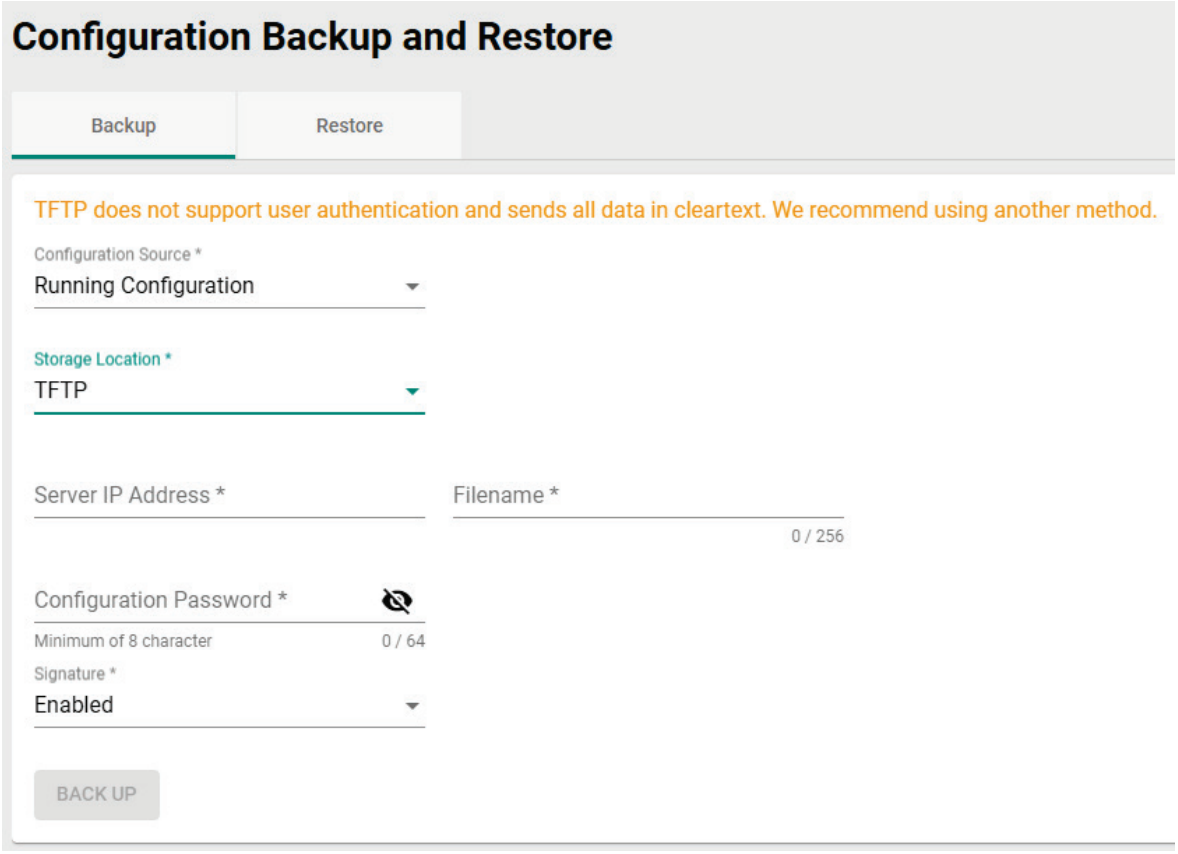
Signature

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the mechanism to verify the CA signature.	Enabled

When finished, click **BACK UP**.

TFTP Server

Select **TFTP** first from the Storage Location drop-down list.



Configuration Source

Setting	Description	Factory Default
Running Configuration	Back up the running configuration.	Running Configuration
Startup Configuration	Back up the start-up configuration.	

Storage Location

Setting	Description	Factory Default
Local	Back up the configuration files for the local computer.	Local
TFTP	**Back up the configuration files via TFTP.**	
SFTP	Back up the configuration files via SFTP.	

Server IP Address

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

File Name

Setting	Description	Factory Default
Max. 256 characters (including the .ini file extension).	Enter the configuration backup file name.	None

Configuration Password

Setting	Description	Factory Default
Configuration password	Enter the configuration password. You will need to enter this password when importing the backup file.	None

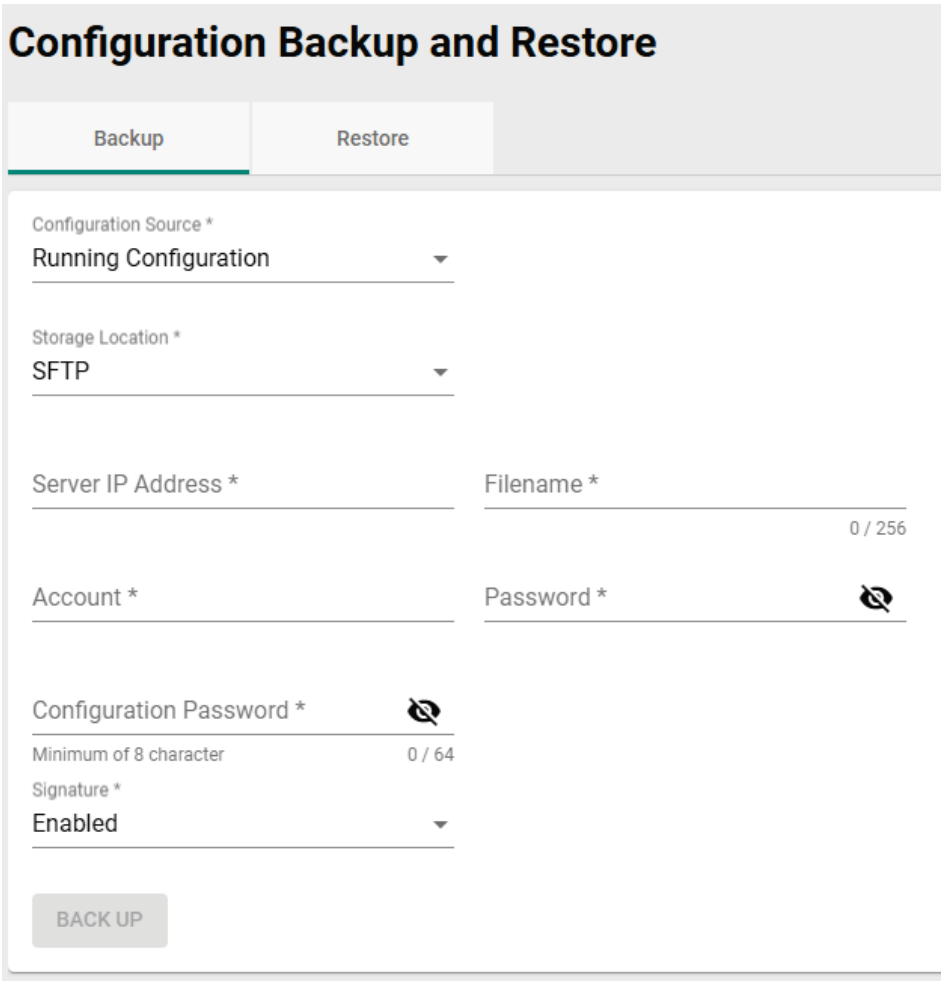
Signature

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the mechanism to verify the CA signature.	Enabled

When finished, click **BACK UP**.

SFTP Server

Select **SFTP** first from the Storage Location drop-down list.



Configuration Source

Setting	Description	Factory Default
Running Configuration	Back up the running configuration.	Running Configuration
Startup Configuration	Back up the start-up configuration.	

Storage Location

Setting	Description	Factory Default
Local	Back up the configuration files for the local computer.	Local
TFTP	Back up the configuration files via TFTP.	
SFTP	**Back up the configuration files via SFTP.**	

Server IP Address

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

File Name

Setting	Description	Factory Default
Max. 256 characters (including the .ini file extension).	Enter the configuration backup file name.	None

Account

Setting	Description	Factory Default
SFTP server account	Enter the SFTP user account name. This account must be authorized to ensure a secure connection to the SFTP server.	None

Password

Setting	Description	Factory Default
SFTP server password	Enter the SFTP user account password. This account must be authorized to ensure a secure connection to the SFTP server.	None

Configuration Password

Setting	Description	Factory Default
Configuration password	Enter the configuration password. You will need to enter this password when importing the backup file.	None

Signature

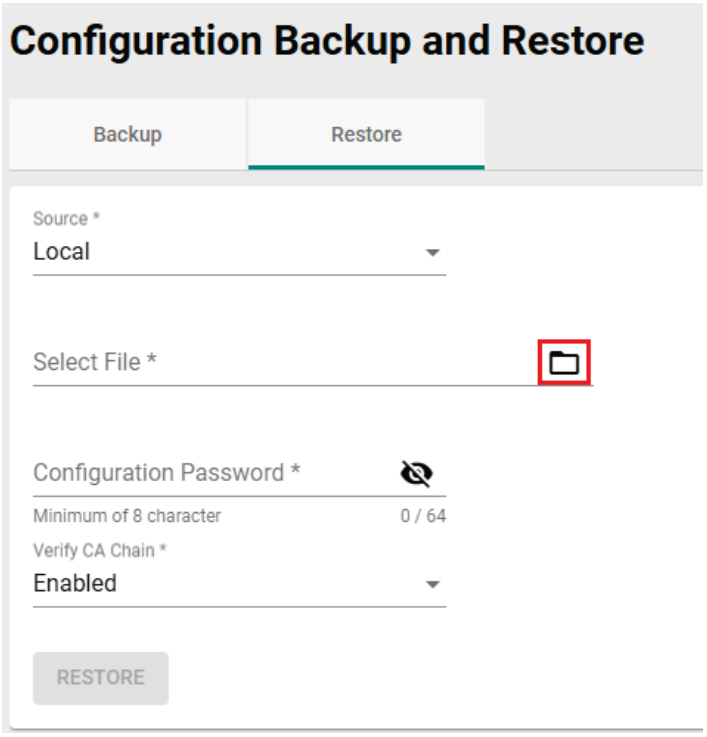
Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the mechanism to verify the CA signature.	Enabled

When finished, click **BACK UP**.

Restore

From the **Restore** tab you restore the device's configuration using a previously created backup file.

Local



Source

Setting	Description	Factory Default
Local	**Restore the configuration from a local backup file.**	Local
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	

Select File

Setting	Description	Factory Default
Backup file	Click the browse icon and navigate to the backup file on the local host.	None

Configuration Password

Setting	Description	Factory Default
Configuration password	Enter the configuration password. You will need to enter this password when importing the backup file.	None

Configuration Password

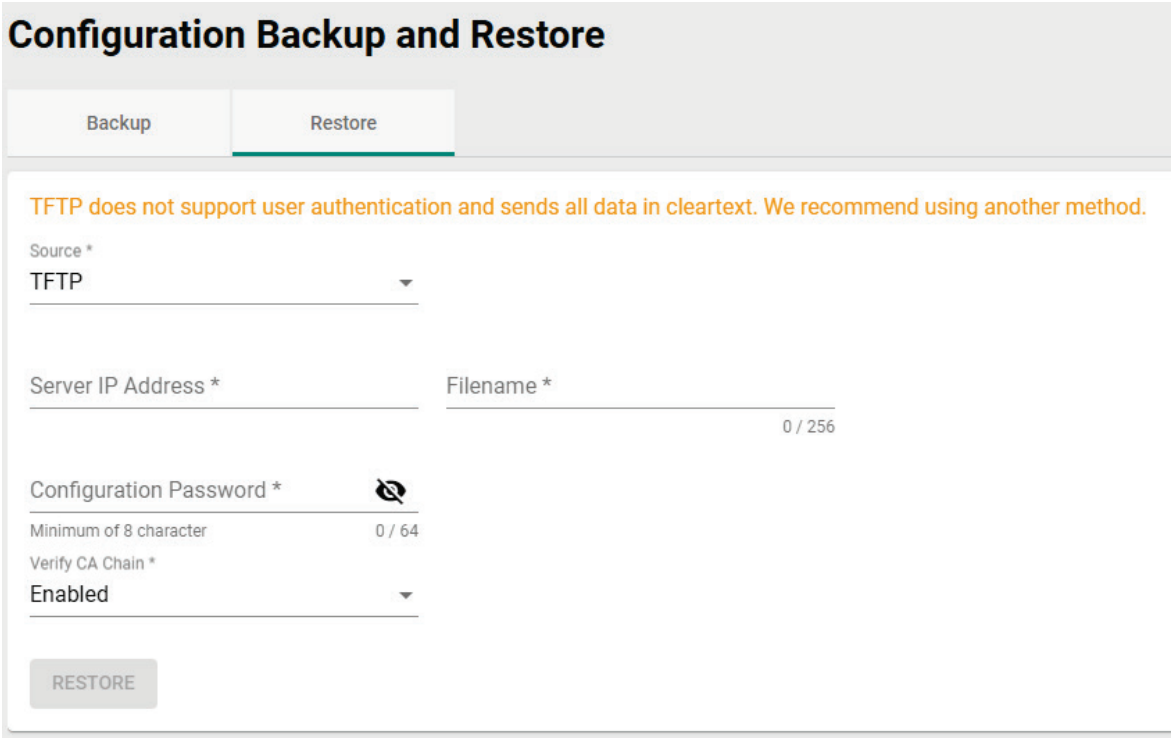
Setting	Description	Factory Default
Configuration password	Enter the configuration password. You will need to enter this password when importing the backup file.	None

Verify CA Chain

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the mechanism to verify the CA chain of the restored configuration.	Enabled

When finished, click **RESTORE**.

TFTP Server



Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	Local
TFTP	**Restore the configuration from a backup file via TFTP.**	
SFTP	Restore the configuration from a backup file via SFTP.	

Server IP Address

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

File Name

Setting	Description	Factory Default
Max. 256 characters (including the .ini file extension)	Enter the file name of the configuration backup file.	None

Configuration Password

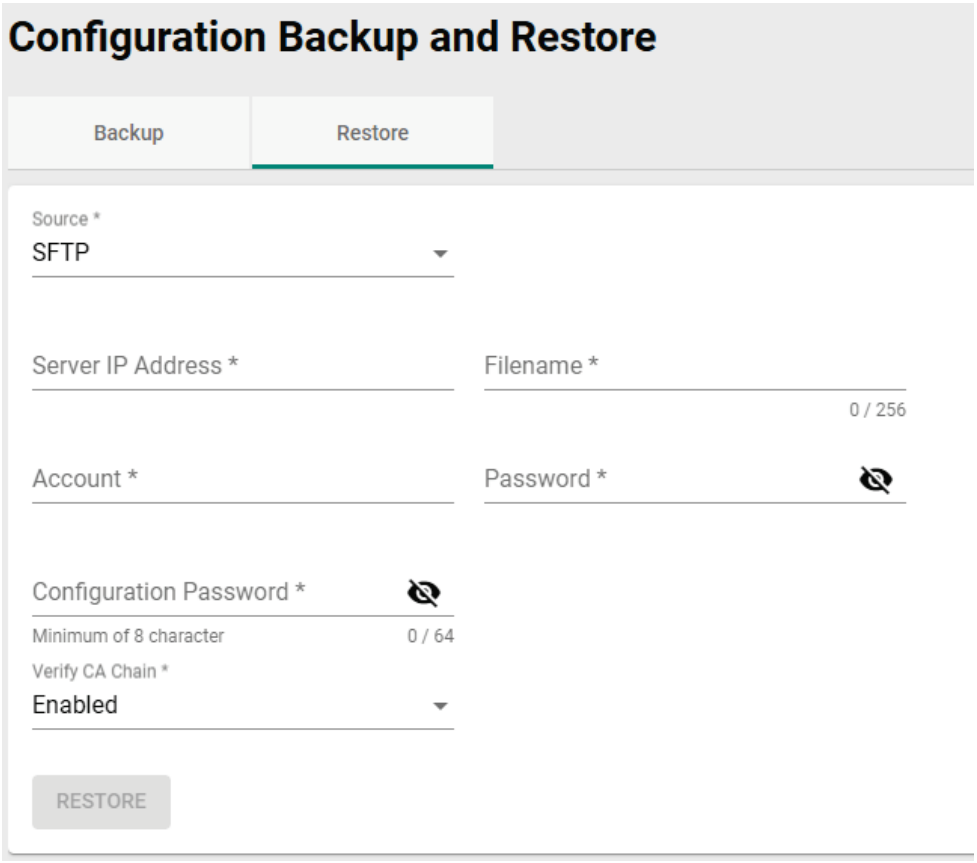
Setting	Description	Factory Default
Configuration password	Enter the configuration password. You will need to enter this password when importing the backup file.	None

Verify CA Chain

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the mechanism to verify the CA chain of the restored configuration.	Enabled

When finished, click **RESTORE**.

SFTP Server



Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	Local
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	**Restore the configuration from a backup file via SFTP.**	

Server IP Address

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

File Name

Setting	Description	Factory Default
Max. 256 characters (including the .ini file extension).	Enter the filename of the configuration restoration file.	None

Account

Setting	Description	Factory Default
SFTP server account	Enter the SFTP user account name. This account must be authorized to ensure a secure connection to the SFTP server.	None

Password

Setting	Description	Factory Default
SFTP server password	Enter the SFTP user account password. This account must be authorized to ensure a secure connection to the SFTP server.	None

Configuration Password

Setting	Description	Factory Default
Configuration password	Enter the configuration password. You will need to enter this password when importing the backup file.	None

Verify CA Chain

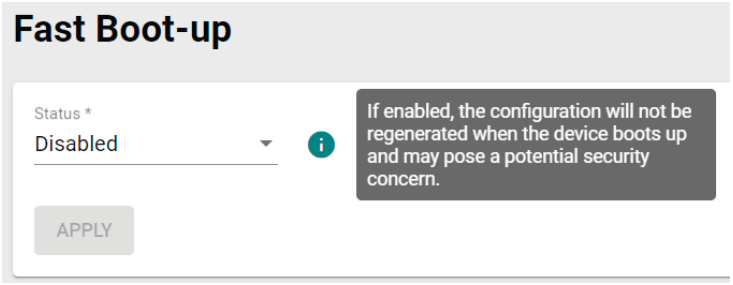
Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the mechanism to verify the CA chain of the restored configuration.	Enabled

When finished, click **RESTORE**.

Fast Boot-up

The TAP-M310R Series is designed with comprehensive security mechanisms to verify device integrity during boot-up. These security measures take time to process before the system is fully operational to provide wireless connectivity services. For applications that require fast connectivity services after a cold start, the Fast Boot-up feature skips some of the startup processes, including the configuration file verification and regeneration, to speed up the overall boot up time by around 30 seconds.

Please note that skipping the configuration file regeneration process to shorten the boot time implies that the device will be running the configuration file saved on the eMMC without prior verification. This could potentially be a security concern if the device has been physically accessed and the eMMC storage was tampered with.



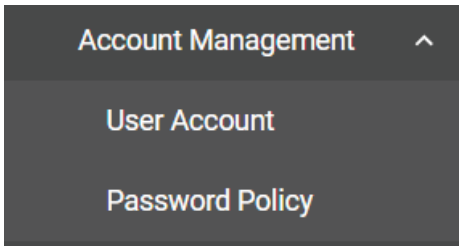
Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable fast boot-up.	Disabled

When finished, click **APPLY**.

Account Management

From this section, you can manage User Account settings and the Password Policy.

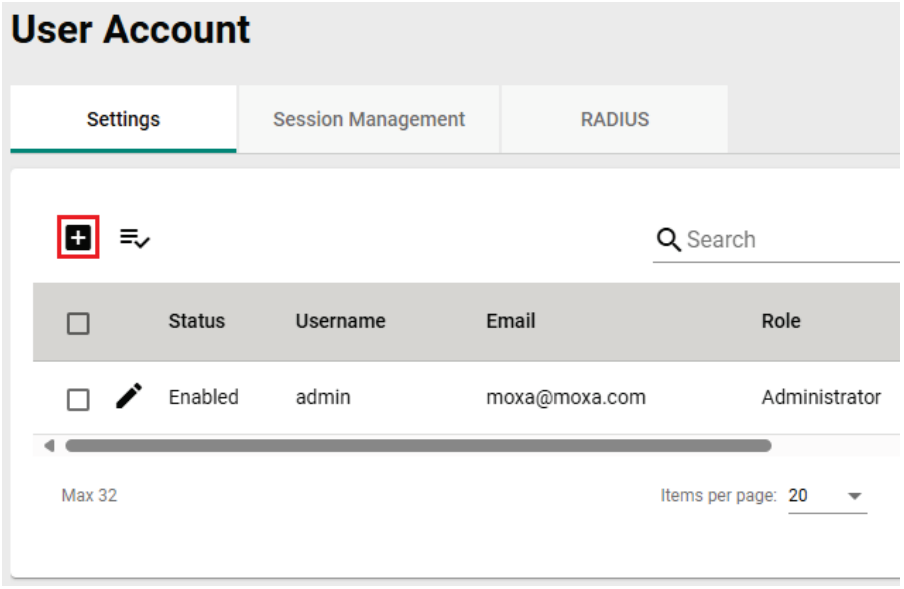


User Account

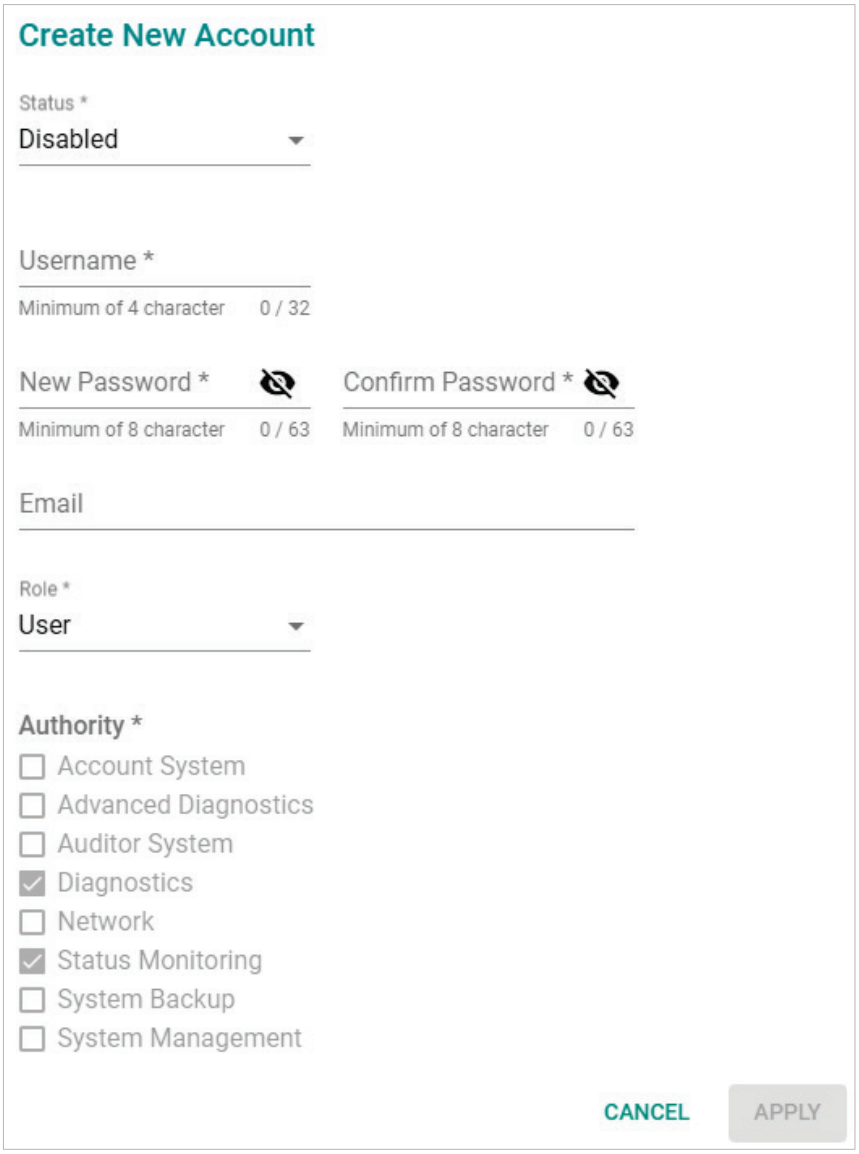
The **User Account** section lets you manage user accounts authorized to access this device and configure account privileges. You can choose to store user accounts on a RADIUS server or manage user accounts locally on the device. Click **User Account** under **Account Management** to access this configuration screen.

Create a New Local Account

To create a new user account, click the **Settings** tab, then click the Add icon.



Edit the following settings:



Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the user account.	Disabled

Username

Setting	Description	Factory Default
Min. 4 characters	Enter a username for this account.	None

New Password

Setting	Description	Factory Default
Min. 8 characters	Enter the password for this account. For better protection, it is recommended to enforce stronger password complexity by enabling the following Password Policy requirements: At least one digit (0-9) At least one upper case letter (A-Z) At least one lower case letter (a-z) At least one special character (~!@#$%^&*-_|:;,.<>{}[]())	None

Confirm Password

Setting	Description	Factory Default
Password	Enter the account password again for confirmation.	None

Email

Setting	Description	Factory Default
Email	Enter the email address for this account.	None

Role

Setting	Description	Factory Default
Administrator	Set the user's role to Administrator. This role provides full access to all configurations on the device. (pre-defined authority)	User
Engineer	Set the user's role to Engineer. (pre-defined authority)	
User	Set the user's role to User. (pre-defined authority)	
Custom	If a mix of authorities is necessary, create an account via the Custom option and manually select the necessary authorities for this account.	

Authority

Setting	Description	Factory Default
Checkbox	Checking authorities gives the user the ability to access configurations pages in the corresponding category. These authority privileges extend to all access interfaces, including CLI.	None

Refer to the table below for an overview of each role and corresponding authorities.

Authority	Admin	Engineer	User
Account System	Yes	No	No
Advanced Diagnostic	Yes	Yes	No
Auditor System	Yes	Yes	No
Diagnostic	Yes	Yes	Yes
Network	Yes	Yes	No
Status Monitoring	Yes	Yes	Yes
System Backup	Yes	No	No
System Management	Yes	Yes	No

NOTE

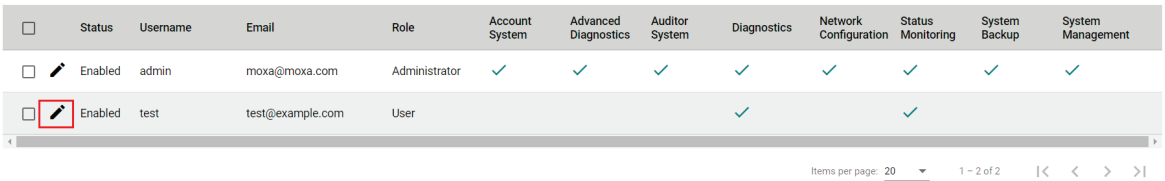
The Administrator, Engineer, and User roles have pre-defined authority options and cannot be changed. The Administrator has all authorities enabled by default. The Custom role allows you to select specific authorities for the user account.

Refer to Appendix D for a detailed overview of the required authority for each device feature or service to determine the privilege requirements when setting up an account.

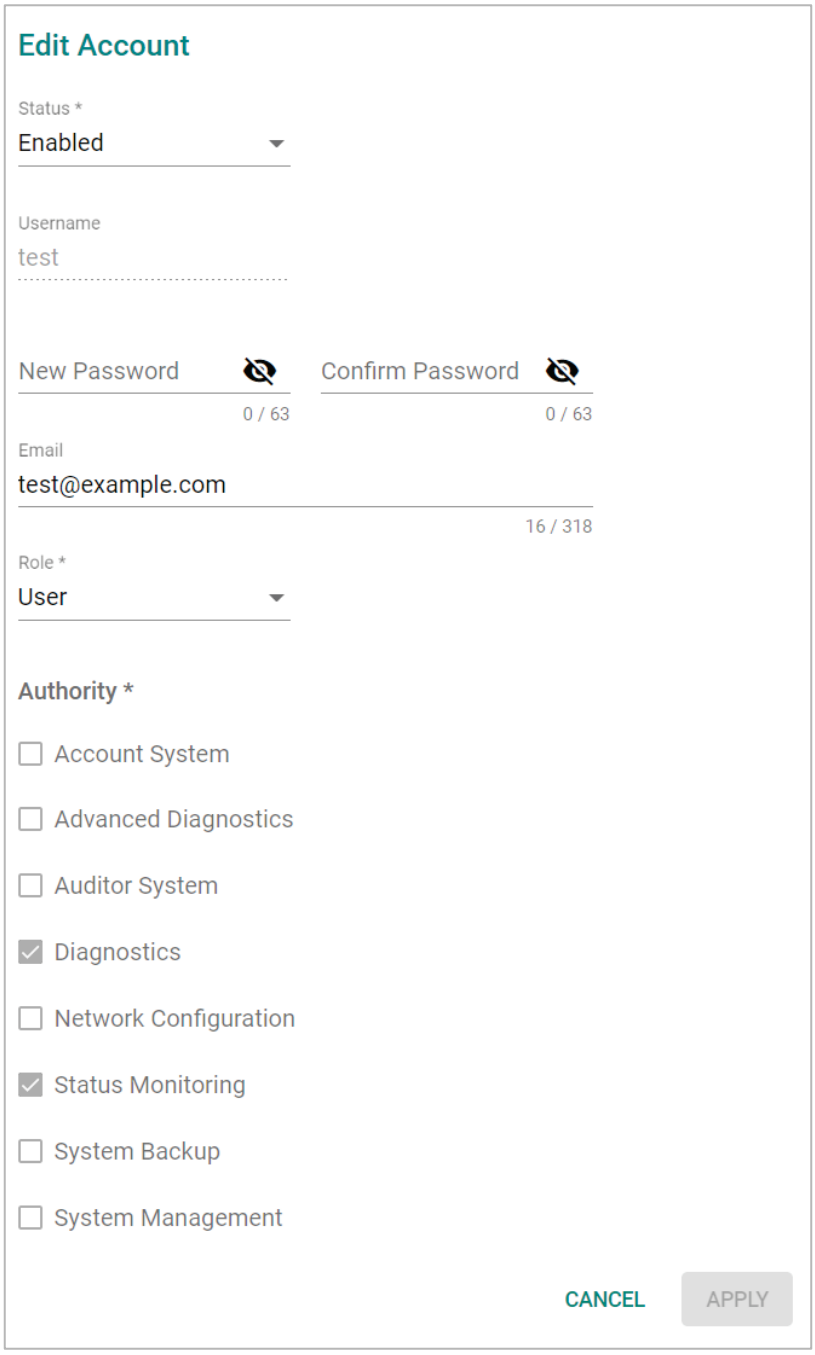
When finished, click **APPLY** to create a new account.

Edit an Existing Local Account

Click the Edit icon of the account you want to edit.



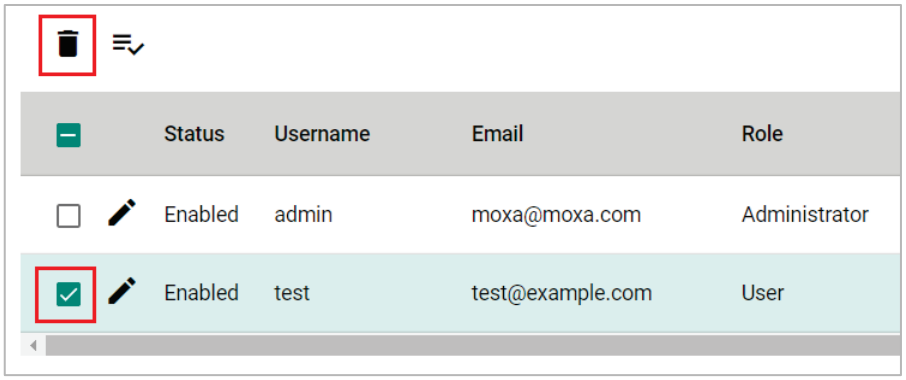
Edit the account settings. Refer to Create a New Account for a description of each setting.

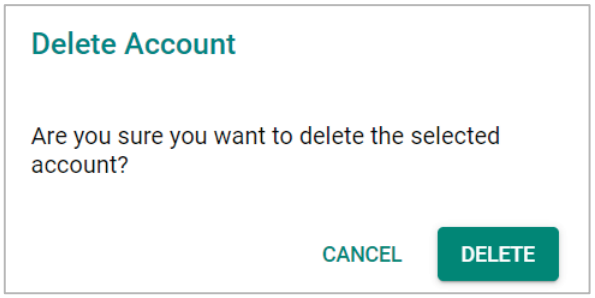


When finished, click **APPLY**.

Delete an Existing Local User

To delete one or more existing users, check the user(s) you want to delete and click the **Delete** icon on the top of the page.



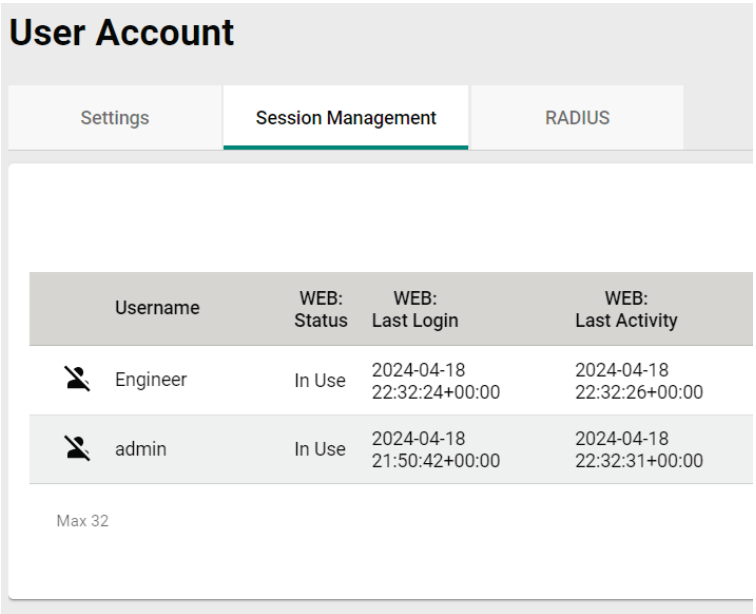


Click **DELETE** to delete the user.

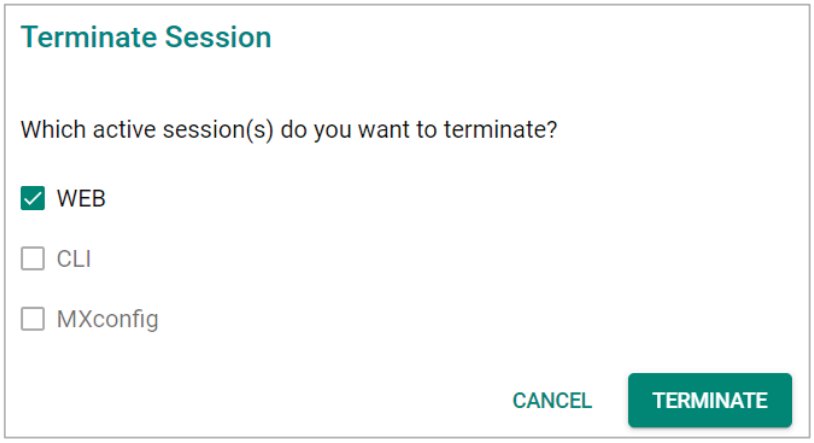
Terminate the Active Session of a User

If necessary, you can manually terminate a specific user's active session for a specific interface. This will also record an event log.

Click **Session Management** tab and click the **Terminate Session** icon next to the user.



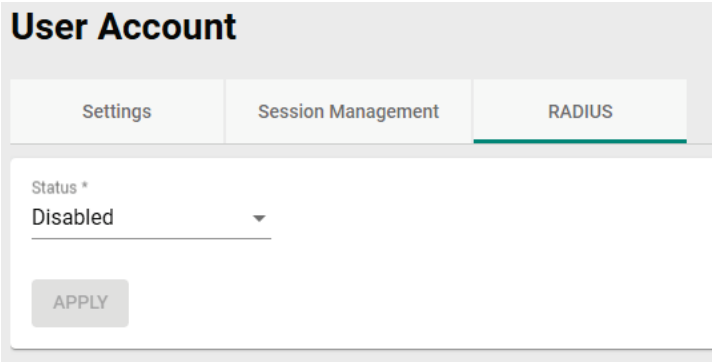
When prompted, select which active sessions you want to terminate.



Click **TERMINATE** to end the selected sessions. The user will be logged out of the corresponding interfaces immediately.

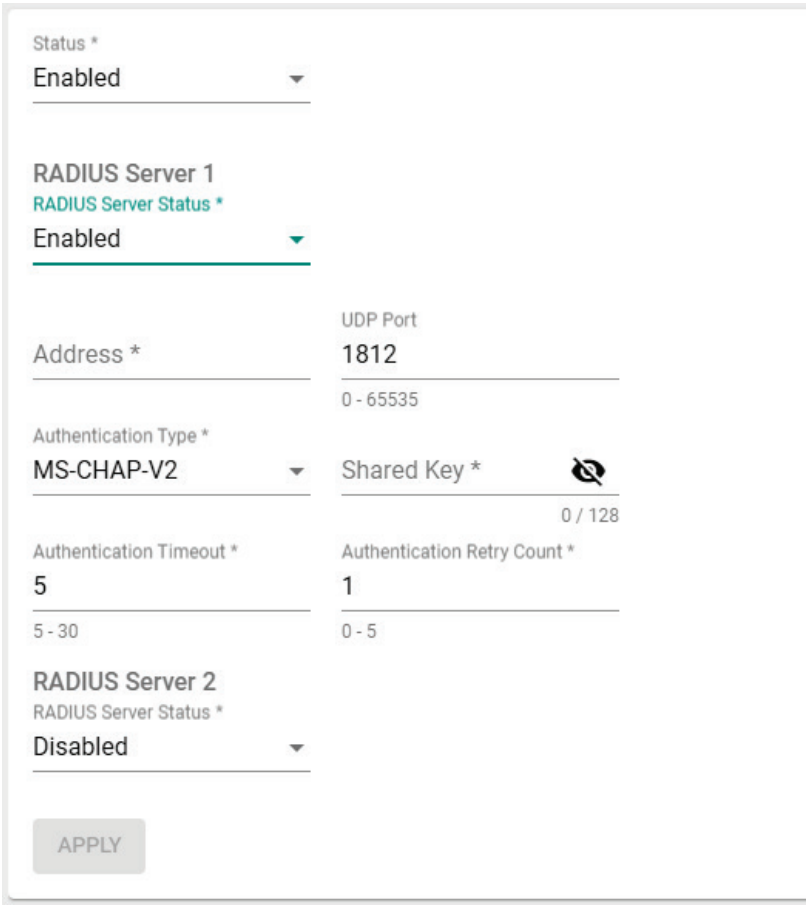
Remotely Authenticate and Authorize Users via RADIUS

Enabling RADIUS functionality allows the system to remotely authenticate and authorize users against an external RADIUS authentication server. If the system fails to authenticate the user via the configured RADIUS server(s), the device will authenticate the user against the local database instead.



Status

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



The following settings are identical for RADIUS server 1 and 2.

RADIUS Server Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the RADIUS server.	Disabled

Address

Setting	Description	Factory Default
IP address	Specify the IP address of the RADIUS server.	None

UDP Port

Setting	Description	Factory Default
0 to 65535	Specify the RADIUS server UDP port number.	1812

Authentication Type

Setting	Description	Factory Default
MS-CHAPv2	Set the RADIUS authentication type to MS-CHAPv2.	MS-CHAPv2
MS-CHAPv1	Set the RADIUS authentication type to MS-CHAPv1.	
CHAP	Set the RADIUS authentication type to CHAP.	
PAP	Set the RADIUS authentication type to PAP.	

Shared Key

Setting	Description	Factory Default
Password	Enter the password for this RADIUS server.	None

Authentication Timeout

Setting	Description	Factory Default
5 to 30	Specify the duration the device will wait for a response from the RADIUS authentication server.	5

Authentication Retry Count

Setting	Description	Factory Default
0 to 5	Specify the number of times the device will attempt to authenticate with the RADIUS server if no response is received.	1

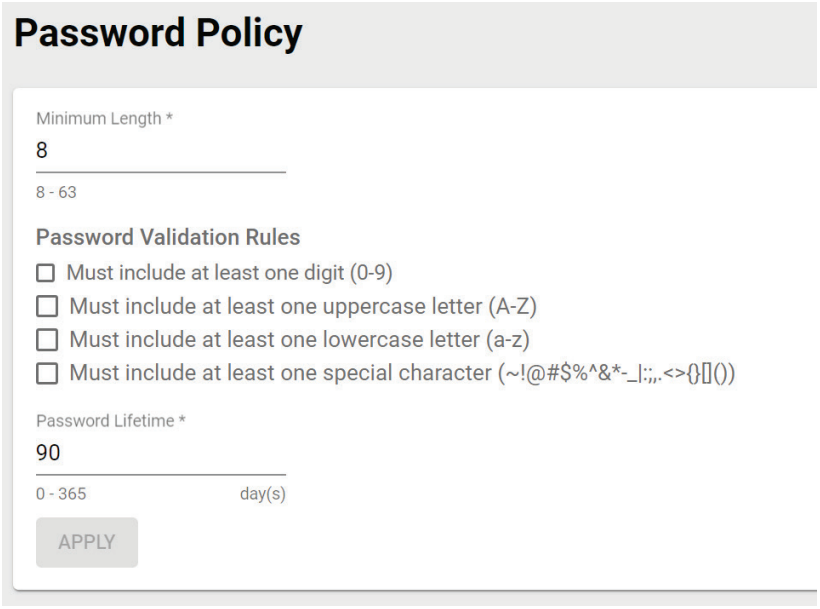
When finished, click **APPLY**.

NOTE

When both RADIUS servers are enabled and configured, RADIUS server 2 acts as a redundant server. If the device fails to authenticate the user via RADIUS server 1 after exhausting all retry attempts, the system will attempt to authenticate the user via the secondary RADIUS server.

Edit the Password Policy

To edit the password policy, click **Password Policy** under **Account Management** in the function menu tree.



Minimum Length

Setting	Description	Factory Default
8 to 63	Specify the required user account password length based on your organization's password length policy. To comply with IEC 62443 requirements, the minimum length starts at 8.	8

Password Validation Rules

Setting	Description	Factory Default
Selectable checkboxes	Select check box to enforce the required password complexity: At least one digit (0-9) At least one upper case letter (A-Z) At least one lower case letter (a-z) At least one special character (~!@#$%^&*-_|:;,.<>{}[]())	Unchecked

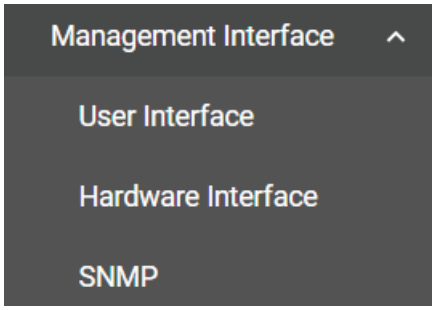
Password Lifetime

Setting	Description	Factory Default
0 to 365 day(s)	Specify the maximum password lifetime. At the end of this duration, the password will expire, and users will be requested to create a new password.	90

When finished, click **APPLY**.

Management Interface

The **Management Interface** section houses the **User Interface, Hardware Interface,** and **SNMP** configuration screens.

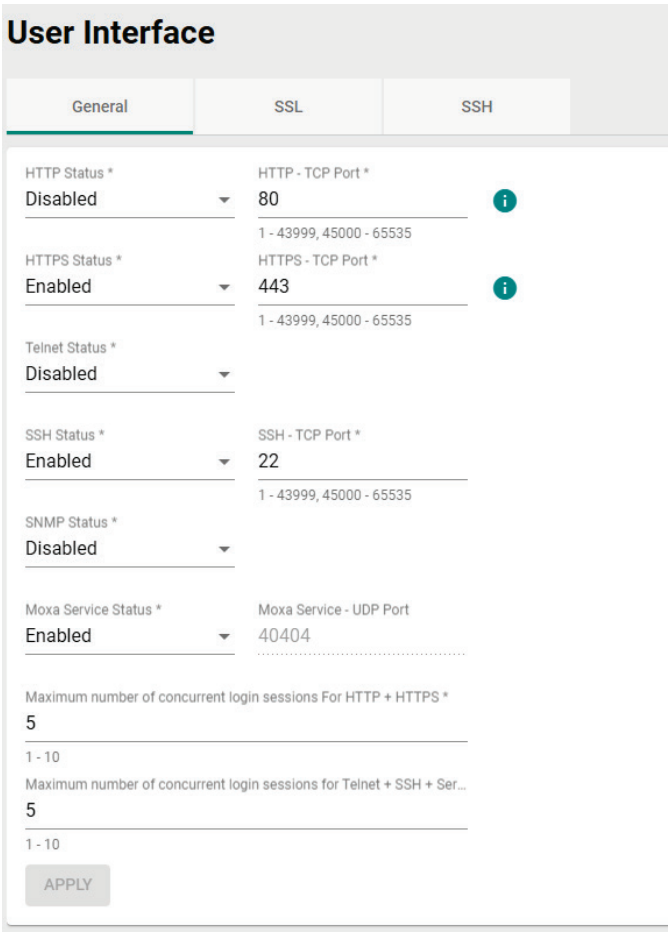


User Interface

The **User Interface** configuration screen lets you manage the interfaces available to users to access the device. Click **User Interface** under **Management Interface** to access this screen.

General

The **General** tab is used to configure the user interfaces and their respective TCP/UDP port.



HTTP Status

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

NOTE

If HTTP and HTTPS are both enabled, any HTTP session will automatically redirect to HTTPS.

HTTP – TCP Port

Setting	Description	Factory Default
1 to 43999, 45000 to 65535	Specify the HTTP interface TCP port number.	80

HTTPS Status

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

HTTPS – TCP Port

Setting	Description	Factory Default
1 to 43999, 45000 to 65535	Specify the HTTPS interface TCP port number.	443

Telnet Status

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

Telnet – TCP Port

Setting	Description	Factory Default
1 to 43999, 45000 to 65535	Specify the Telnet interface TCP port number.	23

SSH Status

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

SSH – TCP Port

Setting	Description	Factory Default
1 to 43999, 45000 to 65535	Specify the SSH interface TCP port number.	22

SNMP Status

Setting	Description	Factory Default
Disabled	Disable SNMP.	Disabled
Read Only	Enable and set SNMP to read-only.	
Read/Write	Enable and set SNMP to read/write.	

SNMP – UDP Port

Setting	Description	Factory Default
1 to 43999, 45000 to 65535	Specify the SNMP UDP port number.	161

Moxa Service Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Moxa Service.	Enabled

NOTE

Moxa Service is only for Moxa network management software such as MXconfig.

Moxa Service (Encrypted)

Setting	Description	Factory Default
40404 (read only)	Specify the Moxa Service UDP port.	40404

Maximum number of Concurrent Login Sessions for HTTP + HTTPS

Setting	Description	Factory Default
1 to 10	Specify the maximum number of concurrent HTTP+HTTPS login sessions allowed on the device.	5

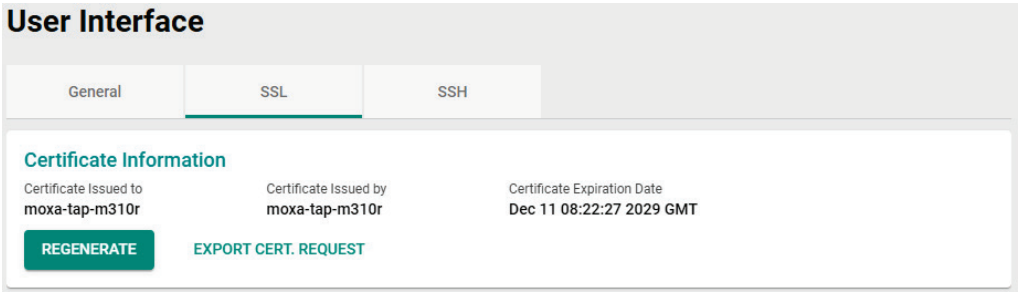
Maximum number of Concurrent Login Sessions for Telnet + SSH + Serial Console

Setting	Description	Factory Default
1 to 10	Specify the maximum number of concurrent Telnet, SSH, and Serial login sessions allowed on the device.	5

When finished, click **APPLY**.

SSL

The **SSL** tab is used to check SSL certificate information, regenerate the certificate, and export the certificate request.



To export the certificate request, click **EXPERT CERT. REQUEST.** This will download the certificate request file to the local host.

To regenerate the SSL certificate, click **REGENERATE**. The **Install Device Certificate and Key** window will appear.

Available options depend on the selected method.

Method

Setting	Description	Factory Default
Self-signed	Regenerate a self-signed SSL certificate.	Self-signed
Upload	Upload a local SSL certificate and key file.	

If you selected **Self-signed**, click **REGENERATE**.

If you selected **Upload**, configure the following settings:

Certificate

Setting	Description	Factory Default
Certificate file	Click the browse icon and navigate to the certificate file on the local host.	None

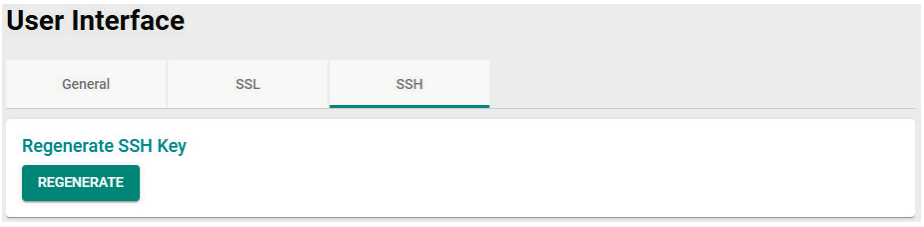
Key

Setting	Description	Factory Default
Key file	Click the browse icon and navigate to the key file on the local host.	None

With the files selected, click **UPLOAD**.

SSH

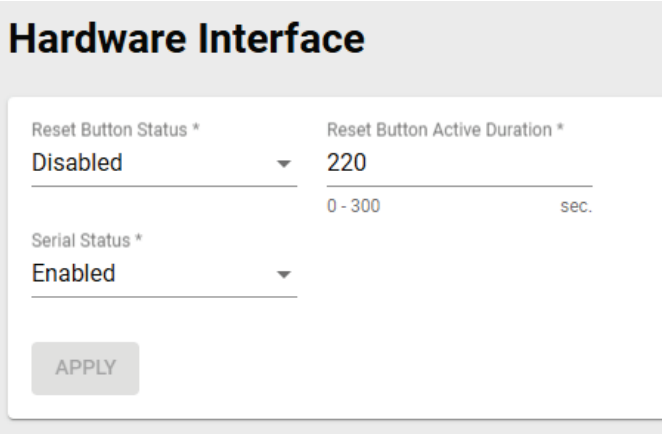
The **SSH** tab is used to regenerate the SSH key.



To generate the SSH key, click **REGENERATE**.

Hardware Interface

From the **Hardware Interface** screen, you can manage the physical interfaces on the device. Click **Hardware Interface** under **Management Interface** to access this screen.



Configure the following settings:

Reset Button Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the reset button.	Disabled

Reset Button Active Duration

Setting	Description	Factory Default
0 to 300 (sec.)	If the reset button is disabled, the "Active Duration" defines the grace period (in seconds) where the reset button will be active for after a system cold boot up. After the grace period, the reset button will be disabled. Note: • If set to 0, the reset button will always be disabled. • The Active Duration countdown begins as soon as the WLAN LED indicator turns from amber to off after the boot up process.	220

Serial Status

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

When finished, click **APPLY**.

SNMP

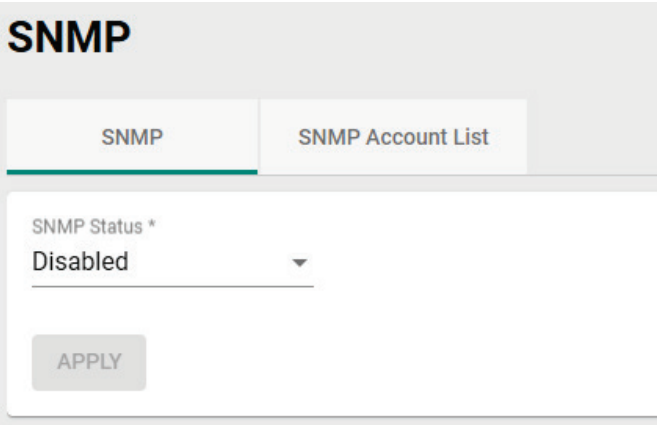
The Moxa TAP-M310R Series supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the default "public" and "private" community strings. SNMP V3 requires MD5 or SHA authentication. You can also enable data encryption to enhance data security.

The supported SNMP security modes and levels are shown in the table below. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	UI Setting	Authentication	Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	None	Uses a community string match for authentication.
	V1, V2c Write/Read Community	Community string	None	Uses a community string match for authentication.
SNMP V3	None	None	None	Uses an account with admin or user role to access objects.
	MD5 or SHA	Authentication based on MD5 or SHA	Disabled	Uses authentication based on HMAC-MD5, or HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.
	MD5 or SHA	Authentication based on MD5 or SHA	Data encryption key: DES, AES	Uses authentication based on HMAC-MD5 or HMAC-SHA algorithms, and a data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication .and encryption.

Configure SNMP Settings

From the **SNMP** screen you can configure the SNMP status and manage the SNMP account. Click **SNMP** from the function tree to access this screen.



SNMP Status

Setting	Description	Factory Default
Read/Write	Set SNMP to read-write.	Disabled
Read Only	Set SNMP as read-only.	
Disabled	Disable the SNMP.	

SNMP Version

Setting	Description	Factory Default
V1, V2c, V3	Enable SNMP V1, V2c, and V3.	V3 only
V1, V2c	Enable SNMP V1 and V2c.	
V3 only	Enable SNMP V3 only.	

Read Community (for V1/V2c Versions)

Setting	Description	Factory Default
Public/Private	Specify the read community security authority level.	public

Read/Write Community (for V1/V2c Versions)

Setting	Description	Factory Default
Public/Private	Specify the read/write community security authority level.	private

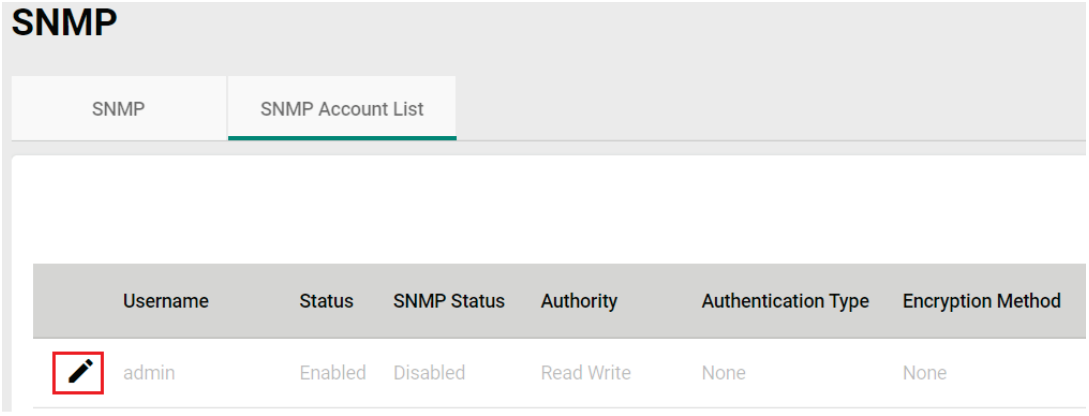
NOTE

SNMP V1 and V2c are not secure. We highly recommend using SNMP V3.

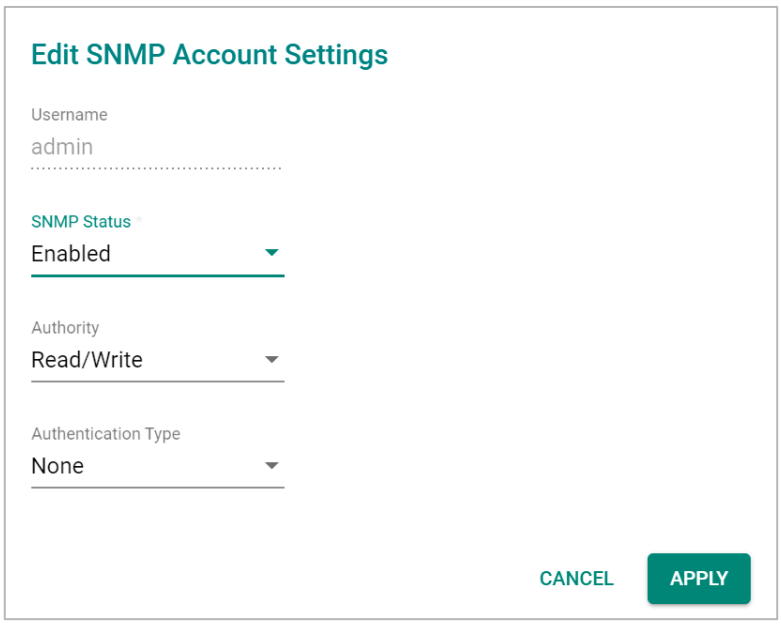
When finished, click **APPLY**.

Edit an SNMP Account

On the SNMP Account List tab, click the Edit icon of the account you want to edit.



Configure the following settings:



Username

Setting	Description	Factory Default
admin (read only)	Show the username. This cannot be changed.	Username for the current user

SNMP Status

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

Authority

Setting	Description	Factory Default
Read/Write	Give the SNMP account as Read/Write authority.	Read/Write
Read Only	Give the SNMP account Read Only authority.	

Authentication Type

Setting	Description	Factory Default
None	No authority type selected.	None
MD5	Specify MD5 as the authority type.	
SHA	Specify SHA as the authority type.	

Authentication Password

Setting	Description	Factory Default
8 to 63 characters	Depending on the selected Authentication Type, specify the Authentication Password. The password must be at least 8 characters long.	None

Encryption Method

Setting	Description	Factory Default
None	No encryption method selected.	None
DES	Specify DES as the Encryption Method.	
AES	Specify AES as the Encryption Method.	

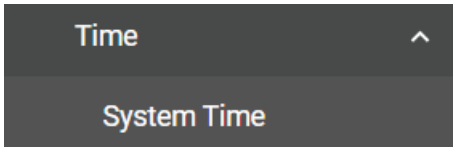
Encryption Key

Setting	Description	Factory Default
8 to 63 characters	Depending on the selected Encryption Method, specify the Encryption Key. The password must be at least 8 characters long.	None

When finished, click **APPLY**.

Time

From the **Time** section, you can configure the **System Time**.

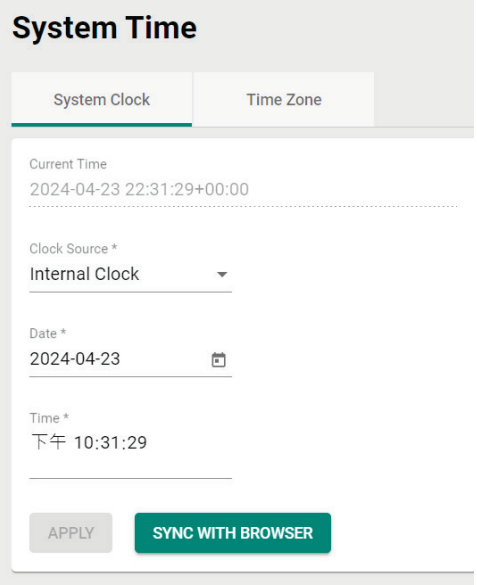


System Time

The **System Time** screen lets you configure the device time settings and specify the time zone. Click **System Time** under **Time** in the function tree to access this screen.

Edit the Clock

The system clock, time, and date can be set manually, or be synced to an external time server.



Configure the following settings:

ATTENTION

You must select the time zone first before configuring "System Clock" settings, as any changes made to the time zone after the system clock has been configured will shift the clock offset based on the deviation of the selected time zone.

Current Time

Setting	Description	Factory Default
Current Time (read only)	Shows the current time.	Current Time

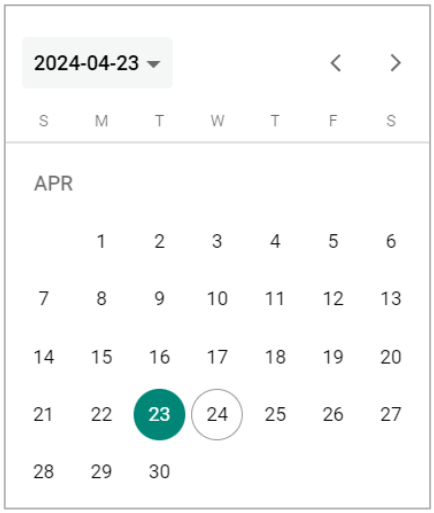
Clock Source

Setting	Description	Factory Default
Internal Clock	Set the clock source to internal. This requires the date and time to be specified manually.	Internal Clock
NTP	Set the clock source to NTP. This will sync the system clock with an external NTP server.	

Configure the Time and Date (Internal Clock)

Date

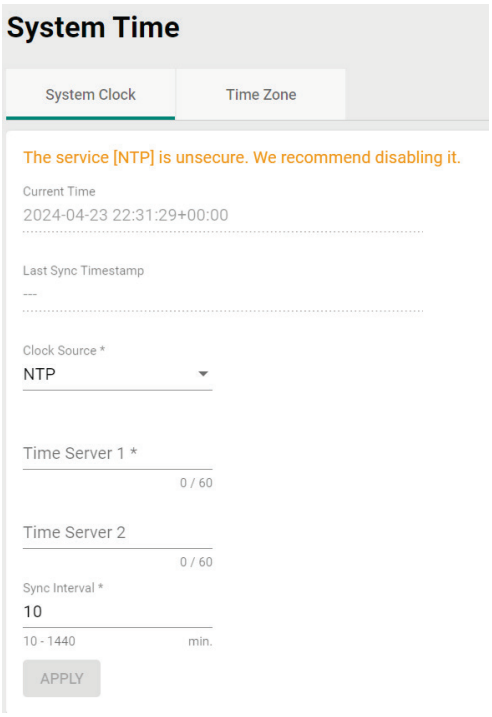
Setting	Description	Factory Default
Day of the month	Select the current date.	Local



Time

Setting	Description	Factory Default
hh, mm, ss	Specify the current time using the 12-hour AM/PM format. You can manually input the time, or you can click **Sync From Browser** to sync the time with your web browser.	Sync From Browser

Configure Time Servers (NTP)



Time Server 1

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

Time Server 2

Setting	Description	Factory Default
NTP time server	Specify the IP or domain address of the secondary NTP server. The secondary NTP server acts as a backup in case the device fails to connect to the first NTP server.	None

Sync Interval

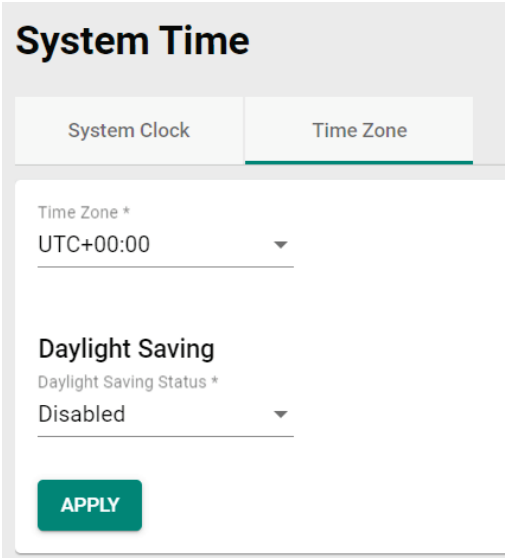
Setting	Description	Factory Default
10 to 1440 (sec.)	Specify the interval (in seconds) at which the system will sync the clock with the time server.	10

When finished, click **APPLY**.

Edit the Time Zone

You can specify the system clock time zone and apply daylight saving time.

Click the **Time Zone** tab.



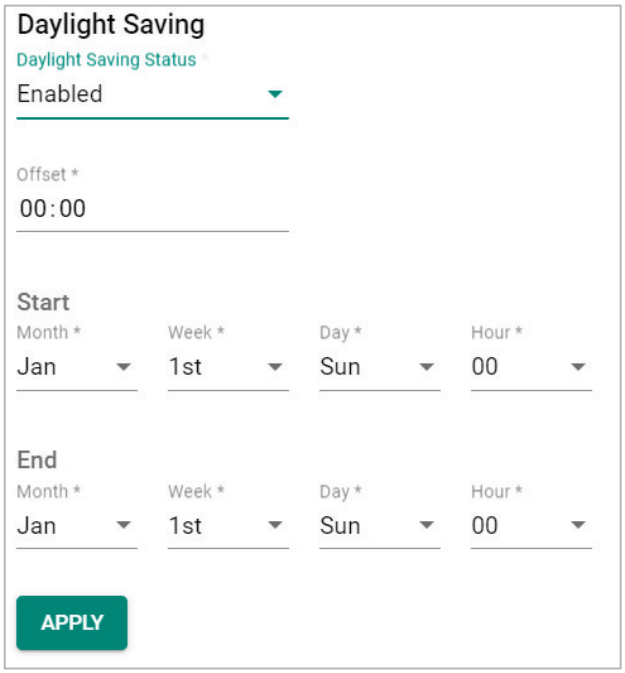
Configure the following settings:

Time Zone

Setting	Description	Factory Default
Time zone	Select a time zone.	GMT (Greenwich Mean Time)

Daylight Saving Time

The Daylight Saving Time settings are used to automatically adjust the time according to regional standards.



Daylight Saving Status

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

Offset

Setting	Description	Factory Default
User-specified value	Specify the offset value for Daylight Saving Time.	None

Start

Setting	Description	Factory Default
User-specified date	Specify the date that Daylight Saving Time begins.	Jan, 1st, Sun, 00.

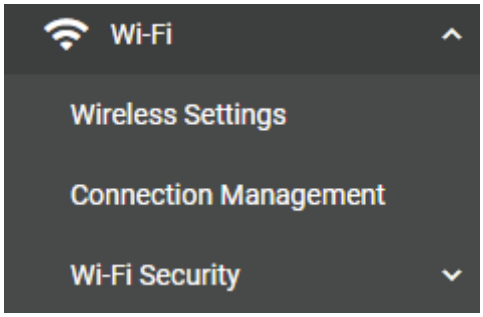
End

Setting	Description	Factory Default
User-specified date	Specify the date that Daylight Saving Time ends.	Jan, 1st, Sun, 00

When finished, click **APPLY**.

Wi-Fi

From the Wi-Fi section, you can configure the **Wireless Settings**, **Connection Management**, and **Wi-Fi Security**.

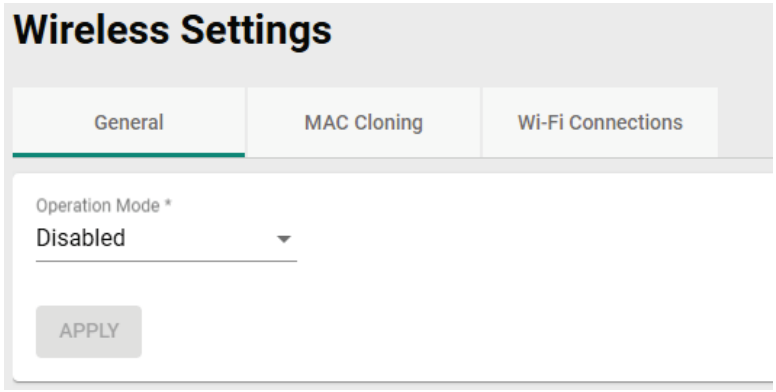


Wireless Settings

On the **Wireless Settings** page, you can configure the device's operating mode, SSID, MAC Cloning settings, as well as check the Wi-Fi connection status. Click **Wireless Settings** under **Wi-Fi** in the function tree to access this screen.

General Settings

The **General** section is used for setting the TAP-M310R's operation mode, creating SSIDs, and configuring RF settings. Click the **General** tab to access this screen.



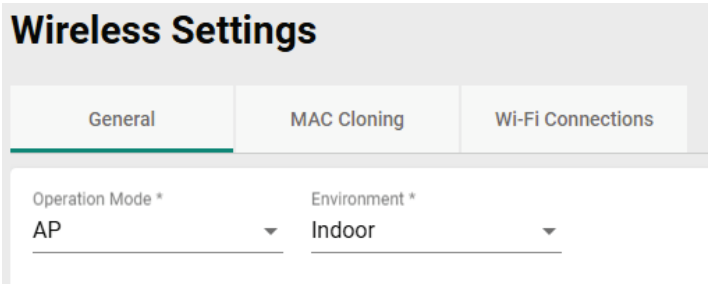
Configure the following settings:

Operation Mode

Setting	Description	Factory Default
Disabled	Disable the operation mode.	Disabled
AP	Specify the operation mode as AP. Refer to **AP Mode Settings**.	
Master	Specify the operation mode as Master. Refer to **Master Mode Settings**.	
Sniffer	Specify the operation mode as Sniffer. Refer to **Sniffer Mode Settings**.	
Client	Specify the operation mode as Client. Refer to **Client Mode Settings**.	
Client-Router	Specify the operation mode as Client-Router. Refer to **Client-Router Mode Settings**.	
Slave	Specify the operation mode as Slave. Refer to **Slave Mode Settings**.	

AP Mode Settings

Select **AP** from the drop-down list of **Operation Mode**. AP Mode requires at least one active SSID.



Environment

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels vary depending on the selection.	

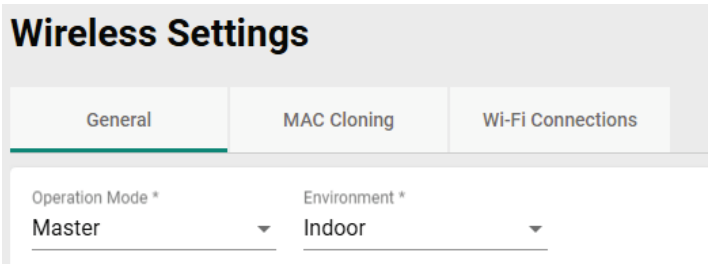
For SSID and security settings, refer to **Create a New SSID**.

For configuring RF settings, refer to **RF Settings**.

When finished, click **APPLY** to change the operation mode.

Master Mode Settings

Select **Master** from the drop-down list of **Operation Mode**. Master Mode requires at least one active SSID.



Environment

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels vary depending on the selection.	

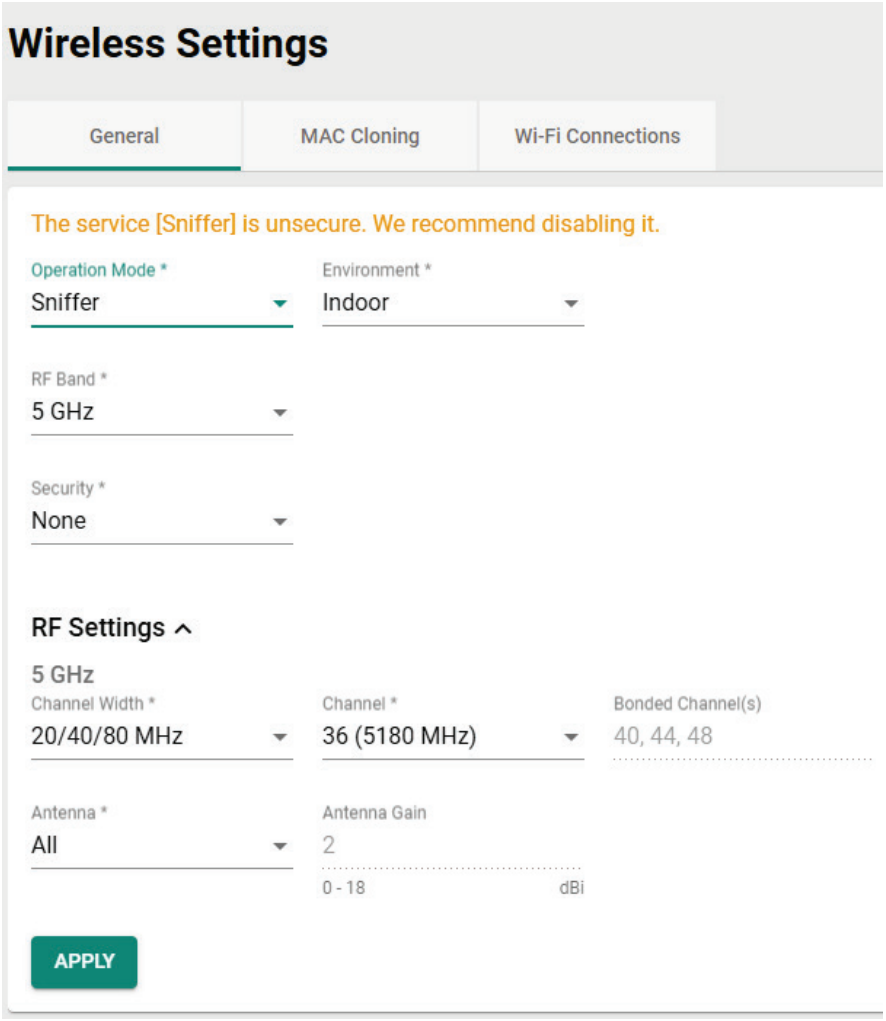
For SSID and security settings, refer to **Create a New SSID**.

For configuring RF settings, refer to **RF Settings**.

When finished, click **APPLY** to change the operation mode.

Sniffer Mode Settings

Select **Sniffer** from the drop-down list of **Operation Mode**.



Configure the following settings:

Environment

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels vary depending on the selection.	

RF Band

Setting	Description	Factory Default
5 GHz	Select 5 GHz as the RF band.	5 GHz
2.4 GHz	Select 2.4 GHz as the RF band.	
5 GHz & 2.4 GHz	Select both 5 GHz and 2.4 GHz as the RF bands.	

Security

Setting	Description	Factory Default
None	Do not use any authentication and encryption mechanism.	None
TLS	Set TLS as the authentication and encryption mechanism.	

For configuring RF settings, refer to **RF Settings**.

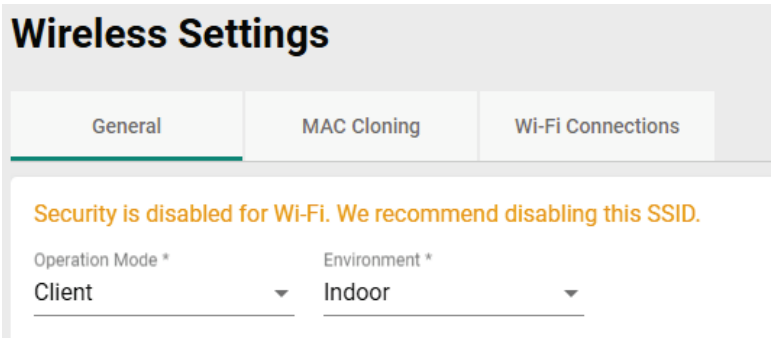
When finished, click **APPLY** to change the operation mode.

NOTE

Once Sniffer and RF settings have been configured, you can add the device's IP as an interface in your network capturing software (e.g. Wireshark) and start capturing packets using Sniffer mode.

Client Mode Settings

Select **Client** from the drop-down list of **Operation Mode**. Client Mode requires at least one active SSID.



Configure the following settings:

Environment

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels vary depending on the selection.	

For SSID and security settings, refer to **Wi-Fi Basic**.

For configuring RF settings, refer to **RF Settings**.

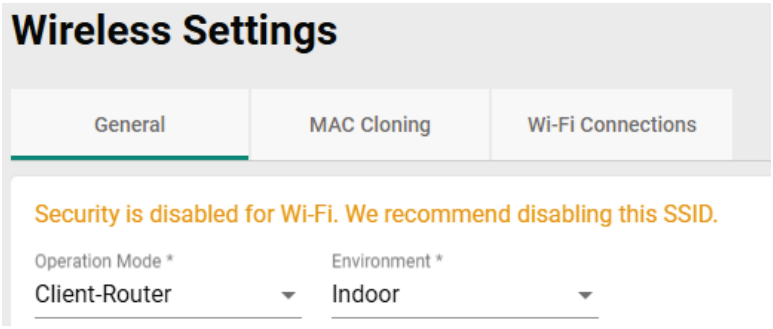
For configuring advanced settings, refer to **Advanced RF Settings**.

When finished, click **APPLY** to change the operation mode.

Client-Router Mode Settings

Client-Router mode allows you to enable Network Address Translation (NAT) functionality to forward data to LAN ports of connected devices.

Select **Client-Router** from the drop-down list of **Operation Mode**. Client-Router Mode requires at least one active SSID.



Configure the following settings:

Environment

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels vary depending on the selection.	

For SSID and security settings, refer to **Wi-Fi Basic**.

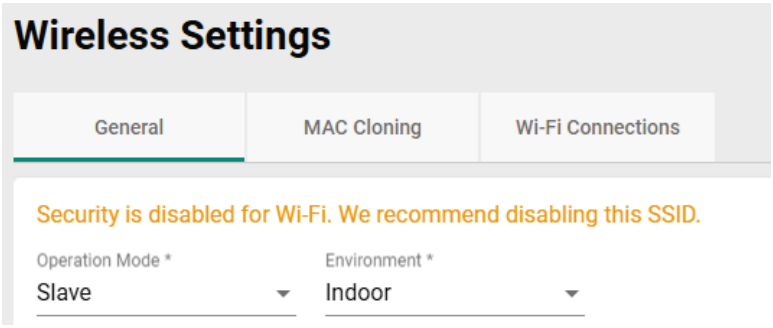
For configuring RF settings, refer to **RF Settings**.

For configuring advanced settings, refer to **Advanced RF Settings**.

When finished, click **APPLY** to change the operation mode.

Slave Mode Settings

Select **Slave** from the drop-down list of **Operation Mode**. Slave Mode requires at least one active SSID.



Configure the following settings:

Environment

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels vary depending on the selection.	

For SSID and security settings, refer to **Wi-Fi Basic**.

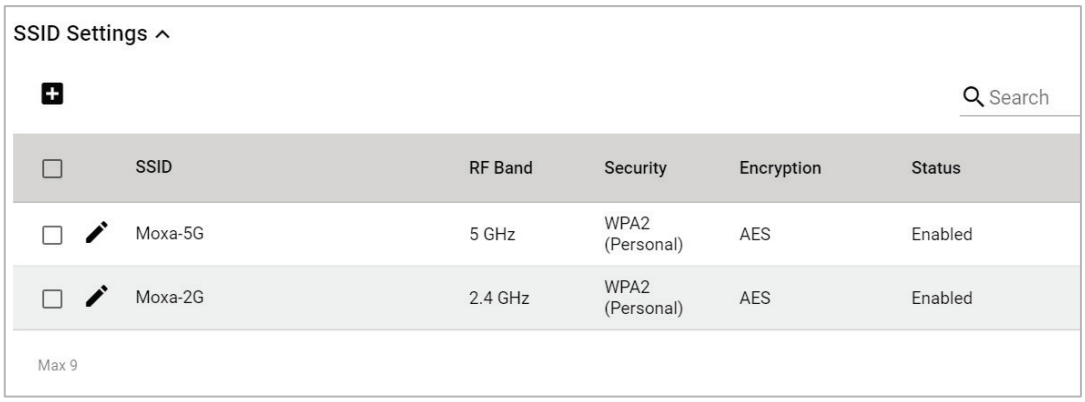
For configuring RF settings, refer to **RF Settings**.

For configuring advanced settings, refer to **Advanced RF Settings**.

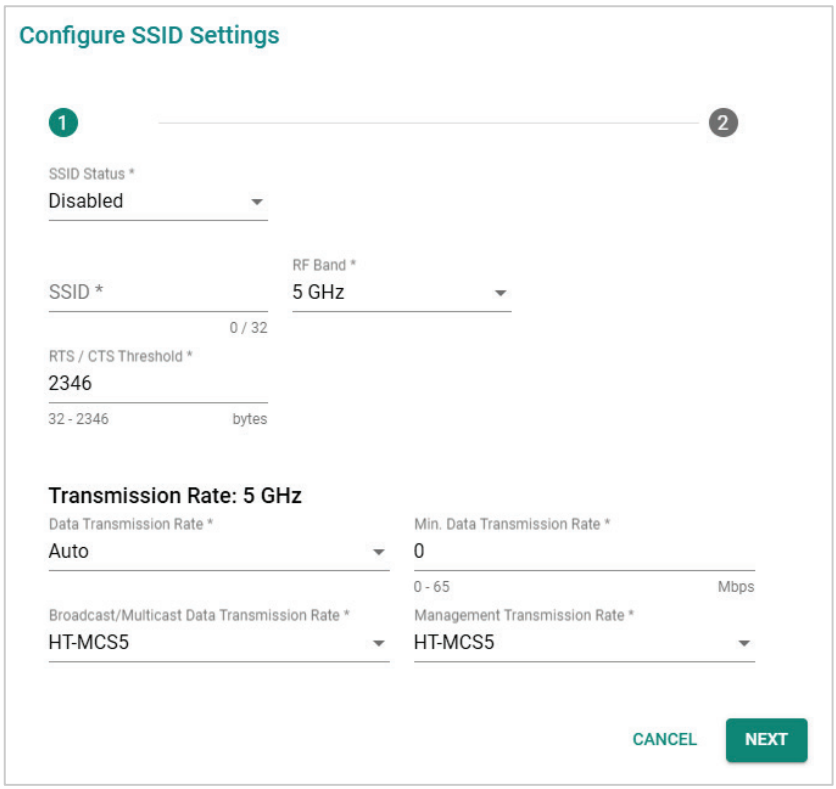
When finished, click **APPLY** to change the operation mode.

Add a New SSID (AP, Master Mode only)

For AP and Master operation modes, configure and enable the SSID profile. There are no SSIDs on the device by default. To add a new SSID, click the **Add (+)** icon.



Configure the following settings:



SSID Status

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

SSID

Setting	Description	Factory Default
1 to 32 characters	Enter a name for the SSID.	None

RF Band

Setting	Description	Factory Default
2.4 GHz	Use the 2.4 GHz RF band on this SSID.	5 GHz
5 GHz	Use the 5 GHz RF band on this SSID.	

RTS/CTS Threshold

Setting	Description	Factory Default
32 to 2346 bytes	Specify the RTS/CTS threshold for the SSID.	2346

Transmission Rate: 5 GHz/2.4 GHz

Data Transmission Rate

Setting	Description	Factory Default
Auto	The TAP-M310R Series will automatically sense the speed of the connected device(s) and adjust the data rate accordingly.	Auto

Minimum Data Transmission Rate

Setting	Description	Factory Default
0 to 65 Mbps (0 to disable)	Specify a minimum transmission rate. By setting a minimum transmission rate, the TAP-M310R Series will avoid communicating over weak signal wireless links to maintain better wireless performance and optimize the wireless frequency usage.	0 (Disabled)

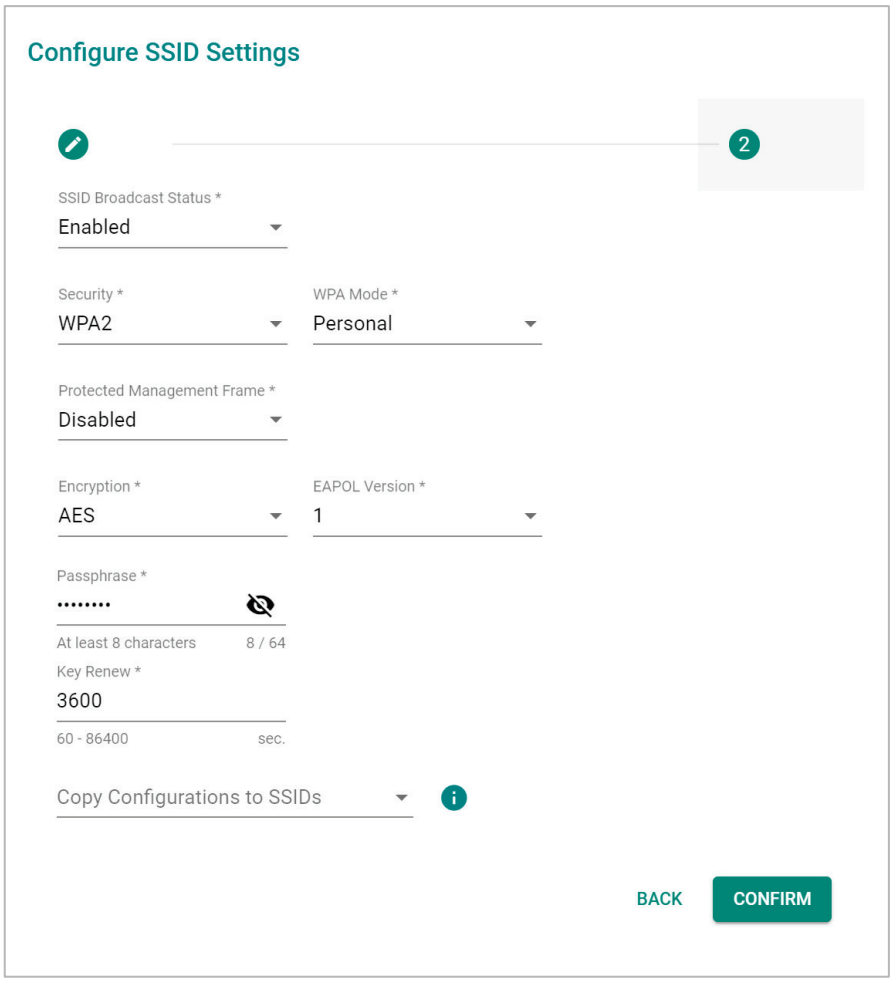
Broadcast/Multicast Data Transmission Rate

Setting	Description	Factory Default
HT-MCS0 to HT-MCS15	Set the broadcast/multicast data transmission rate for the TAP-M310R.	HT-MCS5

Management Transmission Rate

Setting	Description	Factory Default
HT-MCS0 to HT-MCS15	Set the management transmission rate for the TAP-M310R.	HT-MCS5

When finished, click **NEXT**.



SSID Broadcast Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable broadcasting the SSID. If enabled, wireless clients will be able to see and connect to this SSID.	Enabled (depending on the settings on the previous page)

Security

Setting	Description	Factory Default
Open	Disable security on the SSID. This is not recommended.	Open
WPA2	Use WPA2 authentication. This mode supports IEEE 802.11i with TKIP/AES + 802.1X encryption.	
WPA3	Use WPA3 authentication. This mode supports SAE (Simultaneous Authentication of Equals) to avoid network attacks, such as KRACK.	
WPA/WPA2 Mixed	Use WPA/WPA2 Mixed authentication. This allows both WPA and WPA2 clients to connect to the TAP-M310R.	
WPA2/WPA3 Mixed	Use WPA/WPA3 Mixed authentication. This allows both WPA2 and WPA3 clients to connect to the TAP-M310R.	

The TAP-M310R Series provides various standardized wireless security modes: **Open, WPA** (Wi-Fi Protected Access), **WPA2**, and **WPA3**.

- **Open:** No authentication, no data encryption.
- **WPA/WPA2-Personal:** Also known as WPA/WPA2-PSK. You will need to specify the Pre-Shared Key in the Passphrase field, which will be used by the TKIP or AES engine as a master key to generate keys that encrypt outgoing packets and decrypt incoming packets.
- **WPA3-Peronal:** Provide a more secured data connection than WPA2 by using SAE (Simultaneous Authentication of Equals).
- **WPA/WPA2-Enterprise:** Also called WPA/WPA2-EAP (Extensible Authentication Protocol). In addition to device-based authentication, WPA/WPA2-Enterprise enables user-based authentication via IEEE 802.1X. When the Enterprise is selected as the WPA Mode, an additional EAP protocol drop-down field will appear, allowing you to select TLS, TTLS, or PEAP. The EAP-TLS option supports TLS certificates and password upload interface.
- **WPA/WPA2 Mixed:** The TAP-M310R supports WPA/WPA2 at the same time. The TAP-M310R is able to authenticate with both Wi-Fi clients that use WPA and WPA2.
- **WPA2/WPA3 Mixed:** The TAP-M310R supports WPA2/WPA3 at the same time. The TAP-M310R is able to authenticate with both Wi-Fi clients that use WPA2 and WPA3.

When using any security mode except **Open**, Configure the following settings:

Protected Management Frame

Setting	Description	Factory Default
Disabled	Disable the protected management frame. This option is not available when using WPA3.	Disabled
802.11w	Use 802.11w protocol as the protected management frame.	

WPA Mode

Setting	Description	Factory Default
Personal	Authenticate WPA, WPA2, and WPA3 with a Pre-shared Key (PSK).	Personal
Enterprise	Authenticate WPA, WPA2, and WPA3 with EAP security protocol.	

Encryption

Setting	Description	Factory Default
AES	Use Advance Encryption System (AES) encryption.	TKIP/AES Mixed
TKIP/AES Mixed*	Use TKIP/AES Mixed encryption. This option provides a TKIP broadcast key and TKIP+AES unicast key to support legacy AP clients. This option is rarely used and is not available when using WAP3.	

**This option is available for legacy mode in AP/Master only and does not support AES-enabled clients.*

EAPOL Version

If you selected AES encryption in AP mode, select the EAPOL version.

Setting	Description	Factory Default
1	Use EAPOL Version 1 as the security authentication method.	1
2	Use EAPOL Version 2 as the security authentication method.	

Primary/Secondary RADIUS Server IP (for Enterprise mode only)

Setting	Description	Factory Default
IP address	Specify the RADIUS authentication server for EAP.	None

Primary/Secondary RADIUS Port (for Enterprise mode only)

Setting	Description	Factory Default
0 to 65535	Specify RADIUS server port number.	1812

Primary/Secondary RADIUS Shared Key (for Enterprise mode only)

Setting	Description	Factory Default
0 to 128 characters	Enter the secret key shared for communication between AP and the RADIUS server. The key cannot contain the following special characters: ` ' " | ; & $	None

Passphrase (for Personal mode only)

Setting	Description	Factory Default
8 to 63 characters	Enter the passphrase. This is the master key to generate keys for encryption and decryption. The passphrase cannot contain the following special characters: ` ' " | ; & $ Check Show Password to display the password in clear text.	None

Key Renew

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 day)	Specify the interval at which the group key is renewed.	3600 (seconds)

Copy Configurations to SSIDs

Setting	Description	Factory Default
SSID	Select a target SSID from the drop-down menu to copy the current configuration to.	None

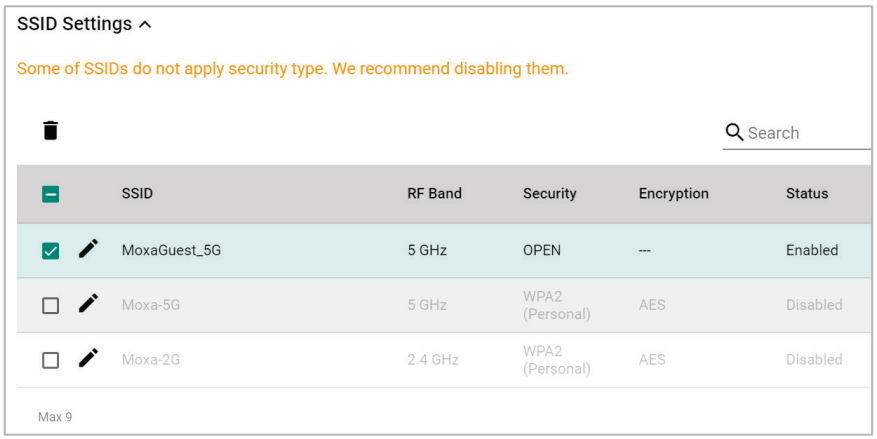
WARNING

The Open mode does not feature any form of authentication and data encryption. For security reasons, we highly recommend NOT to use Open as the security mode.

When finished, click **CREATE** to create a new SSID.

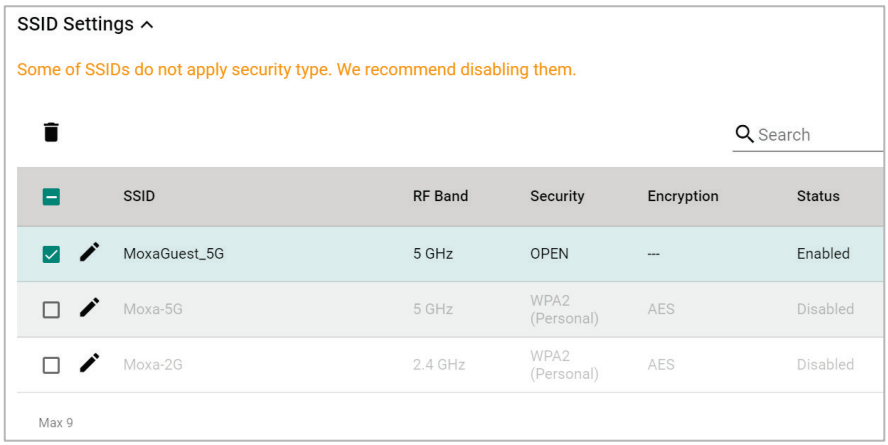
Edit an Existing SSID

To edit an existing SSID, click the **Edit** icon next to the SSID you want to edit. Refer to **Create a New SSID** for more information about setting.

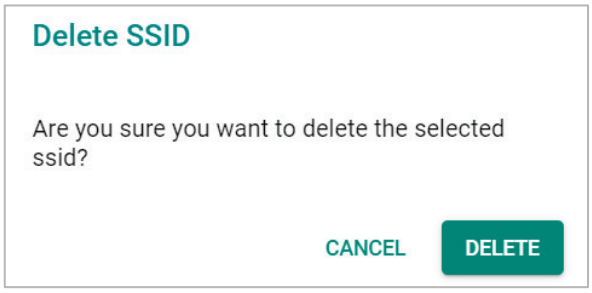


Delete an Existing SSID

To delete an existing SSID, check the SSID, then click the **Delete** icon above the table.



When prompted, click **DELETE**.



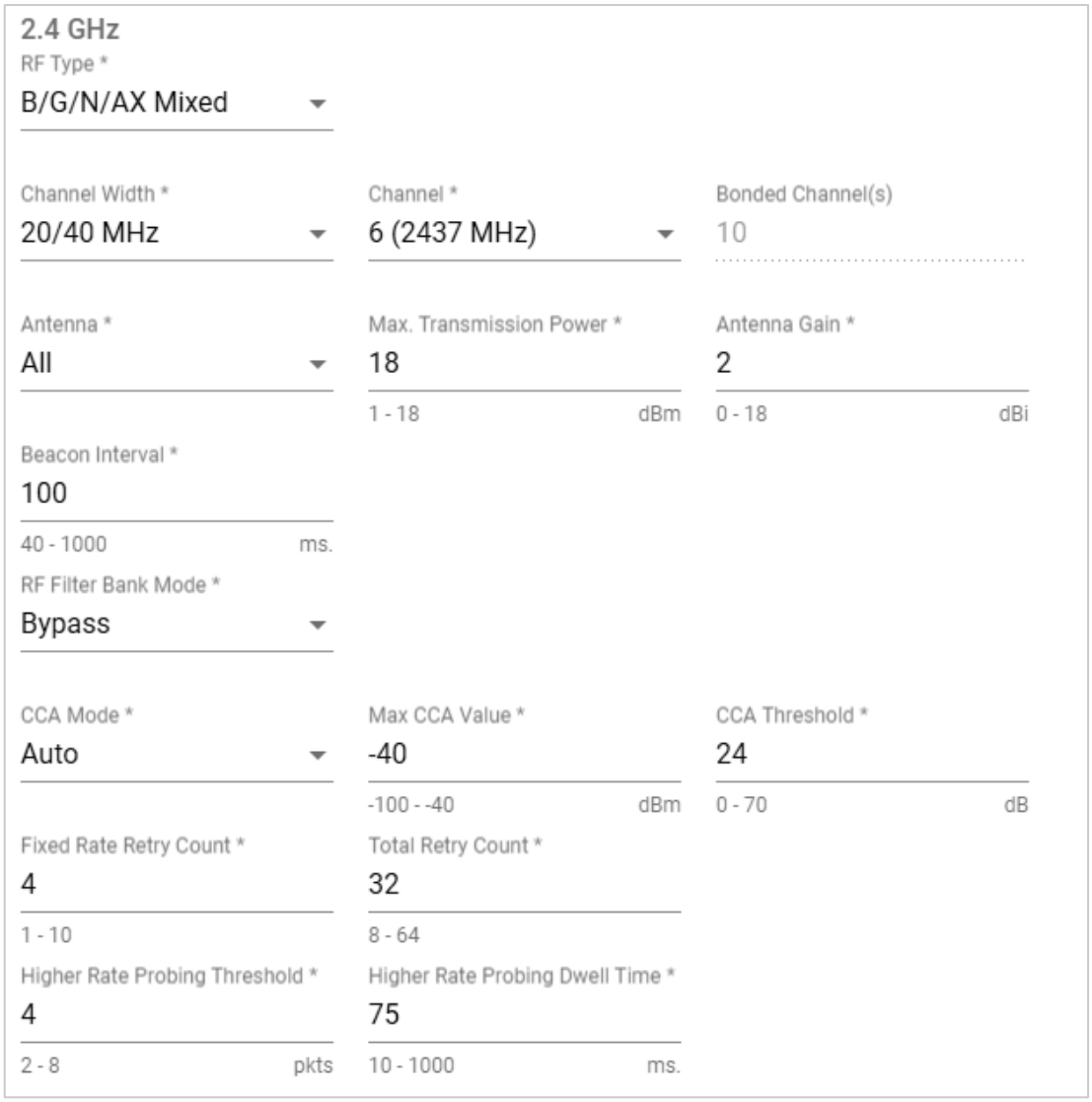
RF Settings

When selecting any operation mode, configure the following RF settings.

NOTE

Available RF settings depend on which Operation mode is active: AP, Master, Client, Client-Router, Sniffer, or Slave mode.

For 2.4 GHz



Configure the following settings:

RF Type

Setting	Description	Factory Default
G/N/AX Mixed	Enable IEEE 802.11g/n/ax. Higher speed Wi-Fi clients may operate at slower speed if legacy Wi-Fi clients are connected to the network.	B/G/N/AX Mixed
B/G/N/AX Mixed	Enable IEEE 802.11b/g/n/ax. Higher speed Wi-Fi clients may operate at slower speed if legacy Wi-Fi clients are connected to the network.	
N/AX Mixed	Enable IEEE 802.11n/ax. Higher speed Wi-Fi clients may operate at slower speed if legacy Wi-Fi clients are connected to the network.	

Setting	Description	Factory Default
AX Only	Only enable IEEE 802.11ax.	

Channel Width

Setting	Description	Factory Default
20 MHz	Set the channel width to 20 MHz. If you are not sure which option to use, select 20/40 MHz.	20/40 MHz
20/40 MHz	Set the channel width to 20/40 MHz. This is recommended.	

Channel

Setting	Description	Factory Default
1 (2412 MHz) to 13 (2472 MHz)	Select the channel from the drop-down list. Each channel supports different frequencies.	6 (2437 MHz)

Bonded Channel

Setting	Description	Factory Default
10 (read only)	The bonded channel used by the AP will be shown here if channel width is set to 20/40 MHz.	10

Antenna

Setting	Description	Factory Default
1	Specify antenna 1 as the output antenna port.	All
2	Specify antenna 2 as the output antenna port.	
ALL	Specify both antennas as the output antenna port.	

Maximum Transmission power

Setting	Description	Factory Default
dBm	Specify the maximum transmission power which acts as a hard ceiling for different transmission rates.	18 dBm

Antenna Gain

Setting	Description	Factory Default
0 to 18 (dBi)	Specify the antenna gain.	2

Beacon Interval

Setting	Description	Factory Default
40 to 1000 (ms.)	Specify the interval at which a beacon is sent.	100 (ms)

RF Filter Bank Mode

Setting	Description	Factory Default
Bypass	Set the RF filter bank mode to bypass. No filters will be used and all data will bypass the filters.	Bypass
Auto	Set the RF filter bank mode to auto. The system will automatically apply the appropriate filter based on the currently used channel.	

CCA Mode

Setting	Description	Factory Default
Auto	Set the Clear Channel Assessment (CCA) mode to Auto. In this mode, the system will automatically adjust the CCA value to the noise floor up until the specified max CCA value.	Auto
Fixed	Set the Clear Channel Assessment (CCA) mode to Fixed. In this mode, the CCA value is set to a fixed value and will not adjust to changes in the noise floor level.	

Max CCA Value

Setting	Description	Factory Default
dBm	When the CCA mode is set to Auto, configure the max CCA value. This value represents the upper limit the system can adjust to depending on the current noise floor.	-40

Fixed CCA Value

Setting	Description	Factory Default
dBm	When the CCA mode is set to Fixed, configure the fixed CCA value. This value represents the static CCA value disregarding the current noise floor.	-90

CCA Threshold

Setting	Description	Factory Default
0 to 70 (dB)	Specify the CCA threshold value. This value is used by the system to determine channel occupancy in relation to the current CCA value. If a signal exceeds the threshold ([signal] > ([CCA value]+[CCA threshold])), the system will consider the channel occupied.	24

Fixed Rate Retry Count

Setting	Description	Factory Default
1 to 10	Configure the fixed retry count used to transmit with the designated rate in fixed rate mode.	4

Total Retry Count

Setting	Description	Factory Default
8 to 64	Configure the total retry count.	32

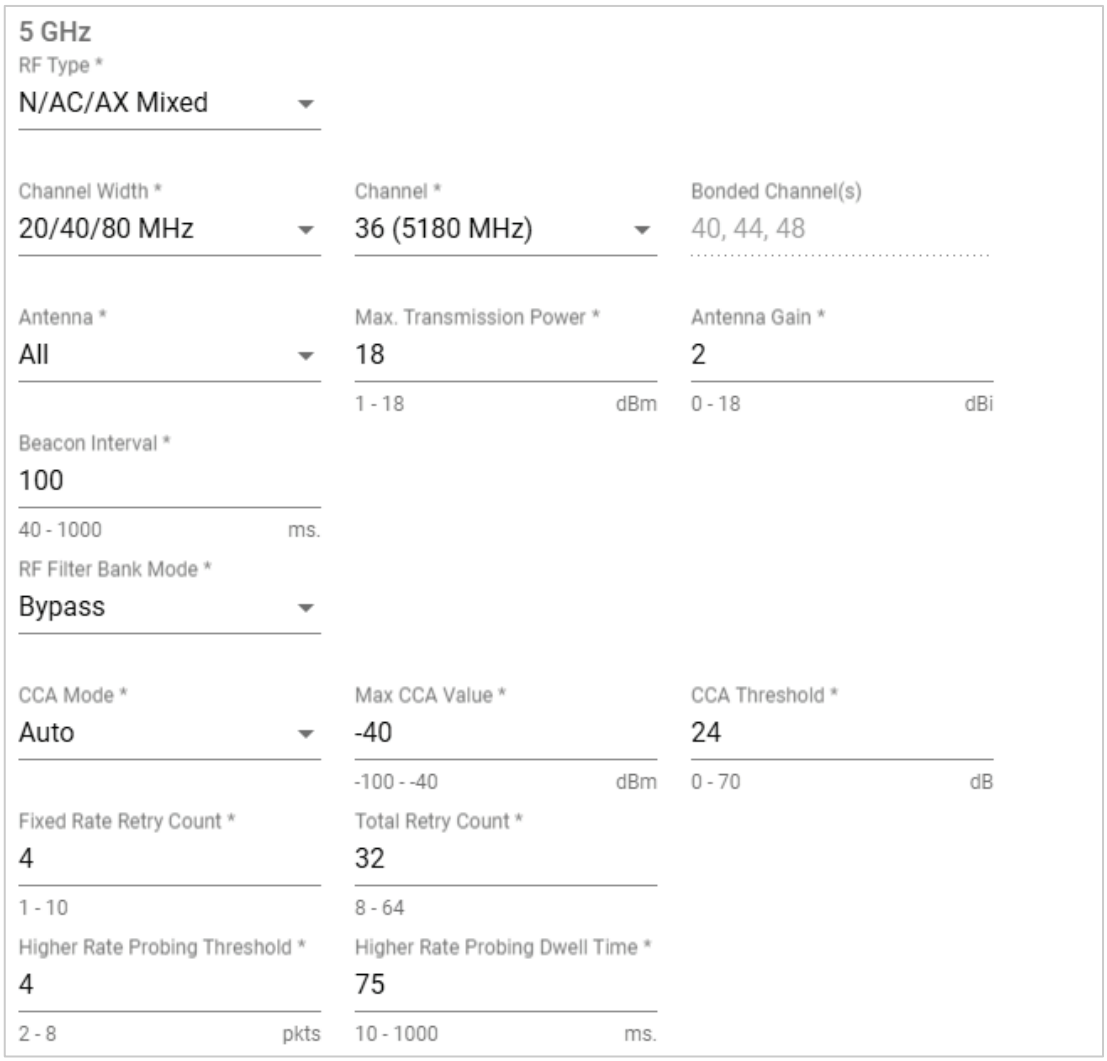
Higher Rate Probing Threshold

Setting	Description	Factory Default
2 to 8 (pkts)	Configure the threshold of consecutive successful transmitted packet count to probe higher rate.	4

Higher Rate Dwell Time

Setting	Description	Factory Default
10 to 1000 (ms)	Configure the minimum period to probe a higher transmission rate.	75

For 5 GHz



Configure the following settings:

RF Type

Setting	Description	Factory Default
AC/AX Mixed	Enable IEEE 802.11ac/ax. Higher speed Wi-Fi clients may operate at slower speed if legacy Wi-Fi clients are connected to the network.	N/AC/AX Mixed
N/AC/AX Mixed	Enable IEEE 802.11n/ac/ax. Higher speed Wi-Fi clients may operate at slower speed if legacy Wi-Fi clients are connected to the network.	
A/N/AC/AX Mixed	Enable IEEE 802.11a/n/ac/ax. Higher speed Wi-Fi clients may operate at slower speed if legacy Wi-Fi clients are connected to the network.	
AX Only	Only enable IEEE 802.11ax.	

Channel Width

Setting	Description	Factory Default
20 MHz	Set the channel width to 20 MHz. If you are not sure which option to use, select 20/40 MHz.	20/40/80 MHz
20/40 MHz	Set the channel width to 20/40 MHz. This is recommended.	
20/40/80 MHz	Set the channel width to 20/40/80 MHz. If you are not sure which option to use, select 20/40 MHz.	

Channel

Setting	Description	Factory Default
36 (5180 MHz) to 161 (5805 MHz)	Select the channel from the drop-down list. Each channel supports different frequencies.	36 (5180 MHz)

Bonded Channel

Setting	Description	Factory Default
40/44/48 (read only)	The bonded channel used by the AP will be shown here if channel width is set to 20/40/80 MHz.	40/44/48

Antenna

Setting	Description	Factory Default
ALL	Specify both antennas as the output antenna port.	All
1	Specify antenna 1 as the output antenna port.	
2	Specify antenna 2 as the output antenna port.	

Maximum Transmission power

Setting	Description	Factory Default
dBm	Specify the maximum transmission power which acts as a hard ceiling for different transmission rates.	18 dBm

Antenna Gain (for AP/Master mode only)

Setting	Description	Factory Default
0 to 18 (dBi)	Specify the antenna gain.	2

Beacon Interval (for AP/Master mode only)

Setting	Description	Factory Default
40 to 1000 (ms)	Specify the interval at which a beacon is sent.	100 (ms)

RF Filter Bank Mode

Setting	Description	Factory Default
Bypass	Set the RF filter bank mode to bypass. No filters will be used and all data will bypass the filters.	Bypass
Auto	Set the RF filter bank mode to auto. The system will automatically apply the appropriate filter based on the currently used channel.	

CCA Mode

Setting	Description	Factory Default
Auto	Set the Clear Channel Assessment (CCA) mode to Auto. In this mode, the system will automatically adjust the CCA value to the noise floor up until the specified max CCA value.	Auto
Fixed	Set the Clear Channel Assessment (CCA) mode to Fixed. In this mode, the CCA value is set to a fixed value and will not adjust to changes in the noise floor level.	

Max CCA Value

Setting	Description	Factory Default
dBm	When the CCA mode is set to Auto, configure the max CCA value. This value represents the upper limit the system can adjust to depending on the current noise floor.	-40

Fixed CCA Value

Setting	Description	Factory Default
dBm	When the CCA mode is set to Fixed, configure the fixed CCA value. This value represents the static CCA value disregarding the current noise floor.	-90

CCA Threshold

Setting	Description	Factory Default
0 to 70 (dB)	Specify the CCA threshold value. This value is used by the system to determine channel occupancy in relation to the current CCA value. If a signal exceeds the threshold ([signal] > ([CCA value]+[CCA threshold])), the system will consider the channel occupied.	24

Fixed Rate Retry Count

Setting	Description	Factory Default
1 to 10	Configure the fixed retry count used to transmit with the designated rate in fixed rate mode.	4

Total Retry Count

Setting	Description	Factory Default
8 to 64	Configure the total retry count.	32

Higher Rate Probing Threshold

Setting	Description	Factory Default
2 to 8 (pkts)	Configure the threshold of consecutive successful transmitted packet count to probe higher rate.	4

Higher Rate Dwell Time

Setting	Description	Factory Default
10 to 1000 (ms)	Configure the minimum period to probe a higher transmission rate.	75

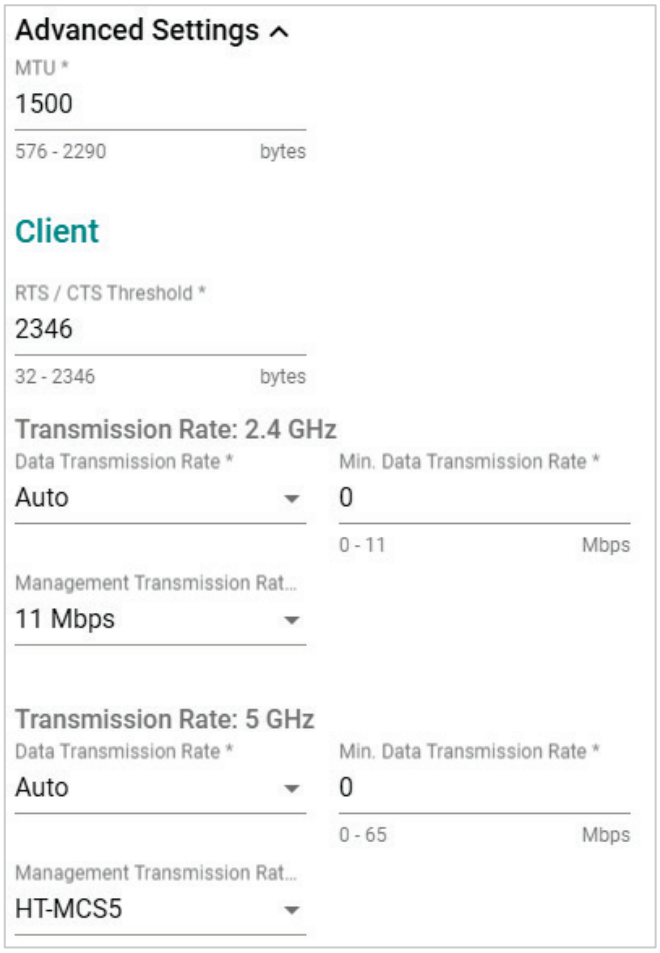
When finished, click **APPLY**.

Advanced RF Settings

Some operation modes require additional advanced RF settings.

NOTE

Available RF settings depend on which Operation mode is active.



Configure the following settings:

MTU

Setting	Description	Factory Default
576 to 2290 bytes	Configure the Maximum Transmission Unit (MTU) size (in bytes) depending on the application traffic type. Configuring a larger MTU value results in a lower packet count (less network congestion) over the wireless network when transmitting applications generate large data packets.	1500

RTS/CTS Threshold (Client, Client-Router, Slave Mode Only)

Setting	Description	Factory Default
32 to 2346 bytes	Specify the RTS/CTS threshold for the SSID.	2346

Transmission Rate: 5 GHz/2.4 GHz (Client, Client-Router, Slave Mode Only)

Data Transmission Rate

Setting	Description	Factory Default
Auto	The TAP-M310R Series will automatically sense the speed of the connected device(s) and adjust the data rate accordingly.	Auto

Minimum Data Transmission Rate

Setting	Description	Factory Default
0 to 65 Mbps (0 to disable)	Specify a minimum transmission rate. By setting a minimum transmission rate, the TAP-M310R Series will avoid communicating over weak signal wireless links to maintain better wireless performance and optimize the wireless frequency usage.	0 (Disabled)

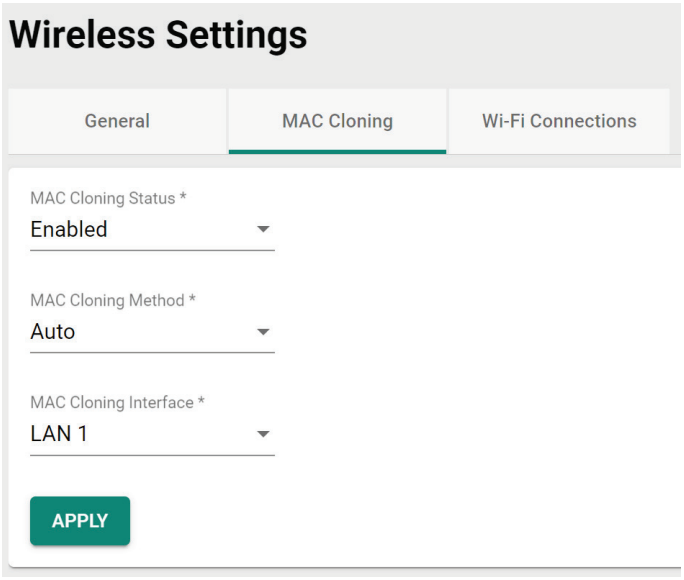
Management Transmission Rate

Setting	Description	Factory Default
HT-MCS0 to HT-MCS15	Set the management transmission rate for the TAP-M310R.	HT-MCS5

When finished, click **APPLY**.

MAC Cloning Settings (Client, Client-Router, Slave Mode Only)

Enabling this feature allows the TAP-M310R client to copy the MAC address of the equipment connected to the LAN. This overcomes the limitation of the IP-Bridged behavior in a MAC-sensitive network (MAC-based communication or MAC-authenticated network).



Configure the following settings:

MAC Cloning Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the MAC Cloning function.	Disabled

MAC Cloning Method

Setting	Description	Factory Default
Auto	The TAP client copies the MAC address of the device connected to the LAN if only one device is connected to TAP.	Auto
Static	The TAP client shares the assigned MAC address with multiple devices connected to the LAN. This allows for multiple devices to connect to the TAP via the LAN and only one of them needs to be assigned a MAC address.	

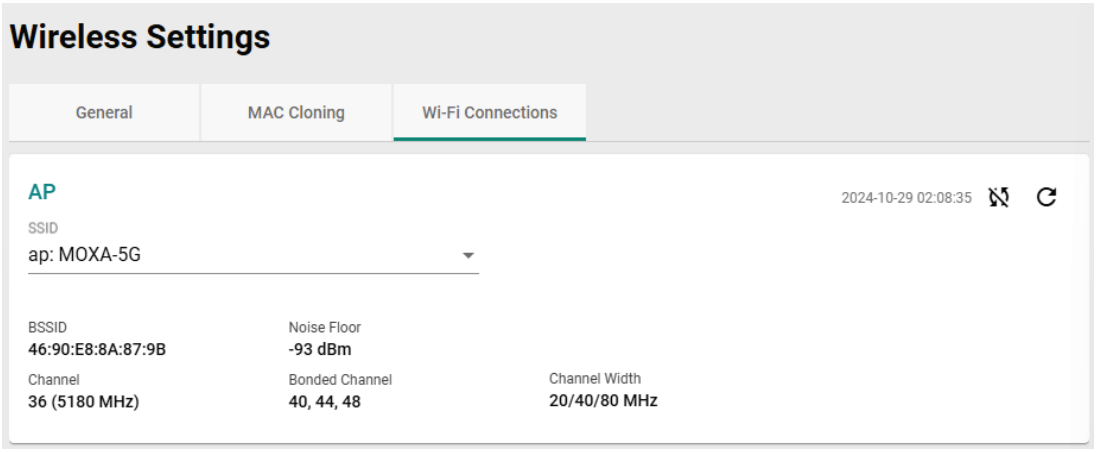
MAC Cloning Interface

Setting	Description	Factory Default
LAN 1 to 5	Specify the static MAC address of LAN port that the connected TAP devices should copy.	

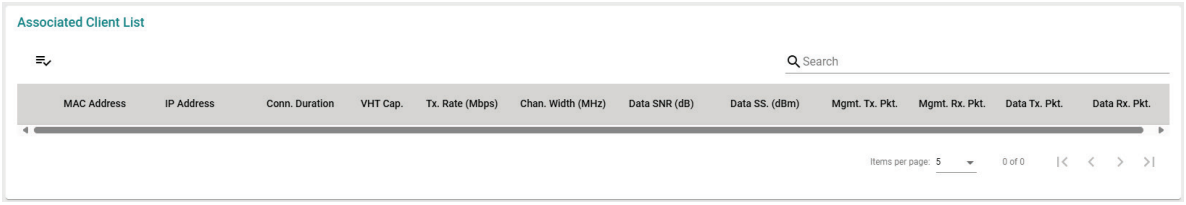
When finished, click **APPLY**.

Wi-Fi Connection Status

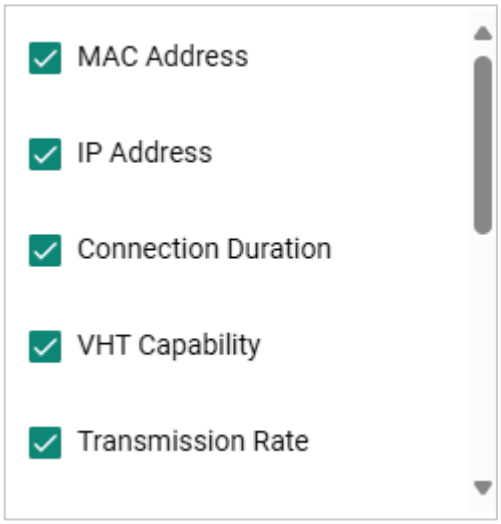
To view the Wi-Fi connection status, click **Wi-Fi Connections** tab. The information on this screen depends on the active operation mode. The following view is from AP Mode.



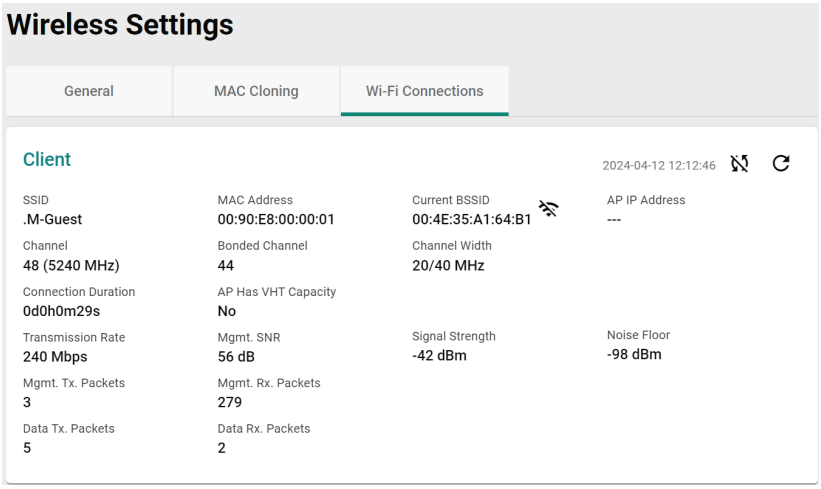
Select the SSID from the drop-down list to view its current status. In AP Mode, you can also view the client list to see all the connected client devices.



Click the **Filter** icon to select the information items that you want to show.



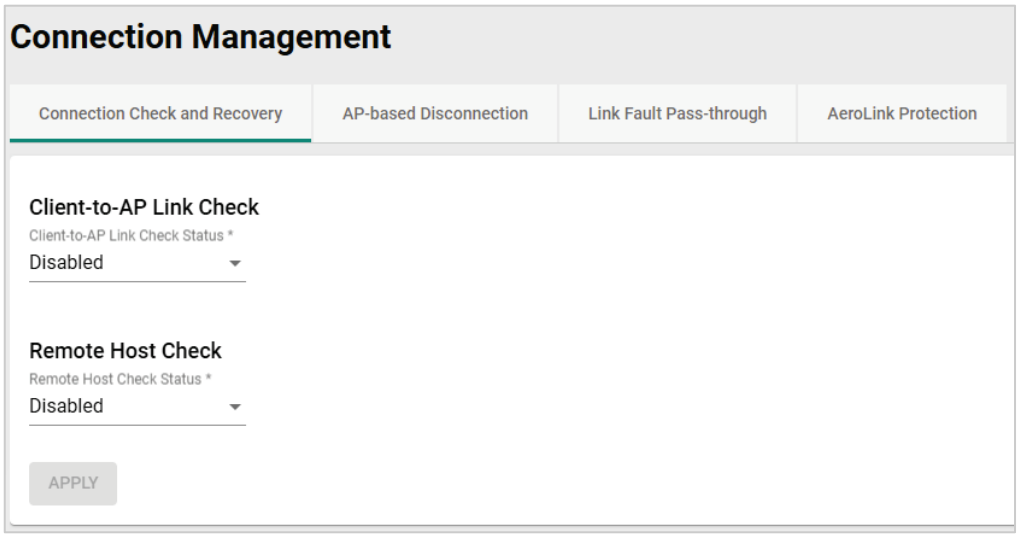
For the Client, Client-Router, and Slave operation modes, this view displays the SSID the device is associated with, and the properties of the connection.



Connection Management

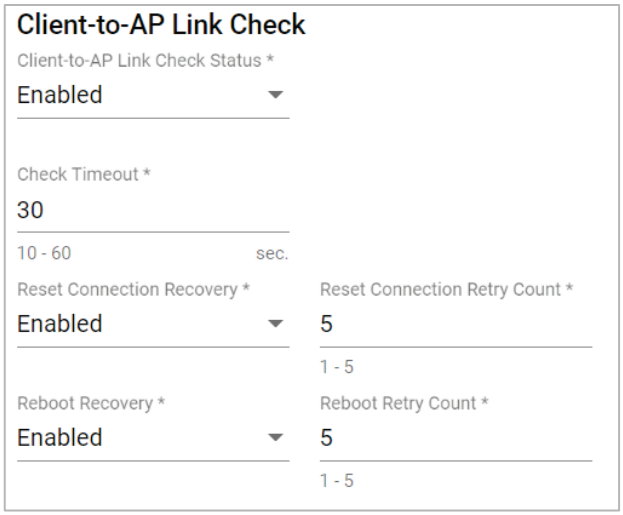
Connection Check and Recovery

The **Connection Check and Recovery** tab contains Wi-Fi connectivity tools to define conditions of normal operational criteria and enable recovery attempts without human intervention. Click **Connection Check and Recovery** under **Wi-Fi** in the function tree to access this screen.



Client-to-AP Link Check

When enabled, this recovery mechanism is triggered when the connection to the AP is lost. When disconnected, the device will reset the Wi-Fi interface in an attempt to recover the connection to the AP. If the connection can still not be recovered after the specified number of retries, the client will reboot and check the connectivity status again.



Configure the following settings:

Client-to-AP Link Check Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Client-to-AP Link Check function.	Disabled

Check Timeout

Setting	Description	Factory Default
10 to 60 (sec.)	Specify the check timeout interval.	30

Reset Connection Recovery

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Reset Connection Recovery function.	Enabled

Reset Connection Retry Count

Setting	Description	Factory Default
1 to 5	Specify the maximum number of times the device will reset the Wi-Fi interface to attempt to recover the connection.	5

Reboot Recovery

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Reboot Recovery function.	Disabled

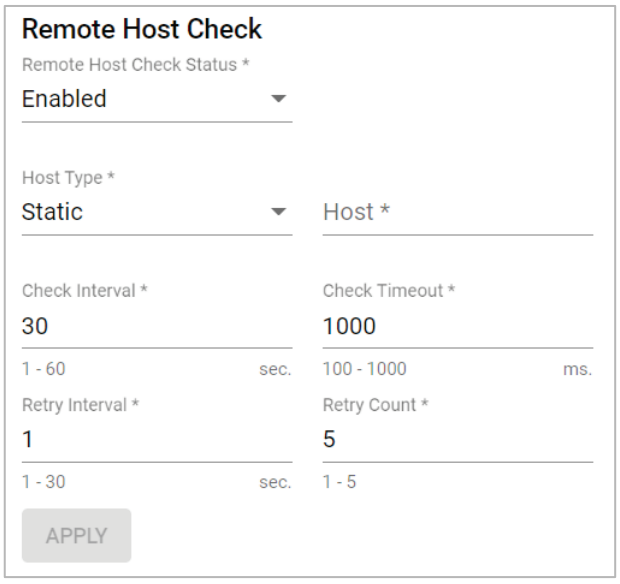
Reboot Retry Count

Setting	Description	Factory Default
1 to 5	Specify the maximum number of times the device will reboot to attempt to recover the connection.	5

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

Remote Host Check

When enabled, this recovery mechanism is triggered when IP traffic fails to reach the configured remote host. The mechanism works by checking if the remote host is reachable at the defined check interval. If the host is still unreachable after the specified number of retries, the client will disconnect from the current AP and will attempt to associate with another AP.



Configure the following settings:

Remote Host Check Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Remote Host Check function.	Disabled

Host Type

Setting	Description	Factory Default
Static	Use Static as the host type.	Static
Dynamic	Use Dynamic as the host type.	

Host (for Static Host Type only)

Setting	Description	Factory Default
Host name	Specify the host name.	None

Check Interval

Setting	Description	Factory Default
1 to 60 (sec.)	Specify the interval at which the client will check the connection to the host.	30

Check Timeout

Setting	Description	Factory Default
100 to 10000 (ms)	Specify the connection expiration interval (in ms). If exceeded, the client will consider the remote host unreachable or unresponsive and will trigger the recovery mechanism.	1000

Retry Interval

Setting	Description	Factory Default
1 to 30 (sec.)	Specify the interval at which the device will check the host again after a failed attempt.	1

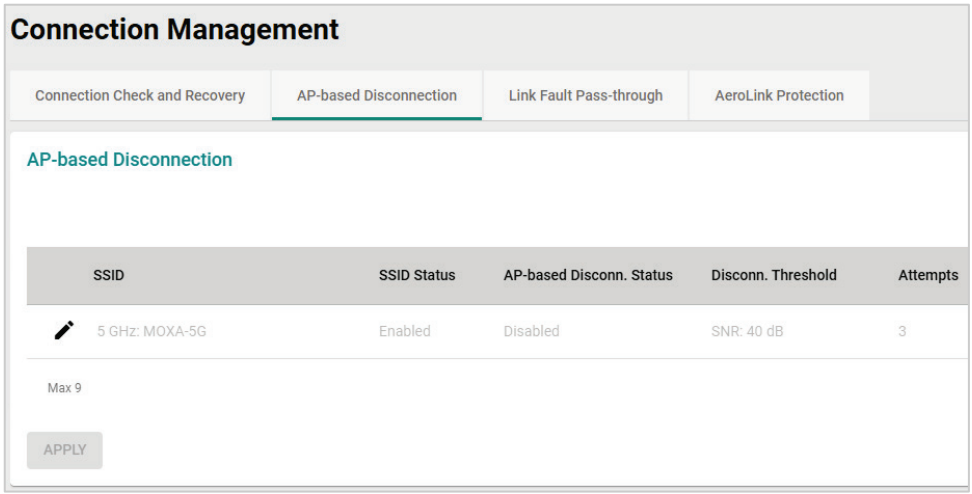
Retry Count

Setting	Description	Factory Default
1 to 5	Specify the maximum number of times the device will check the host.	5

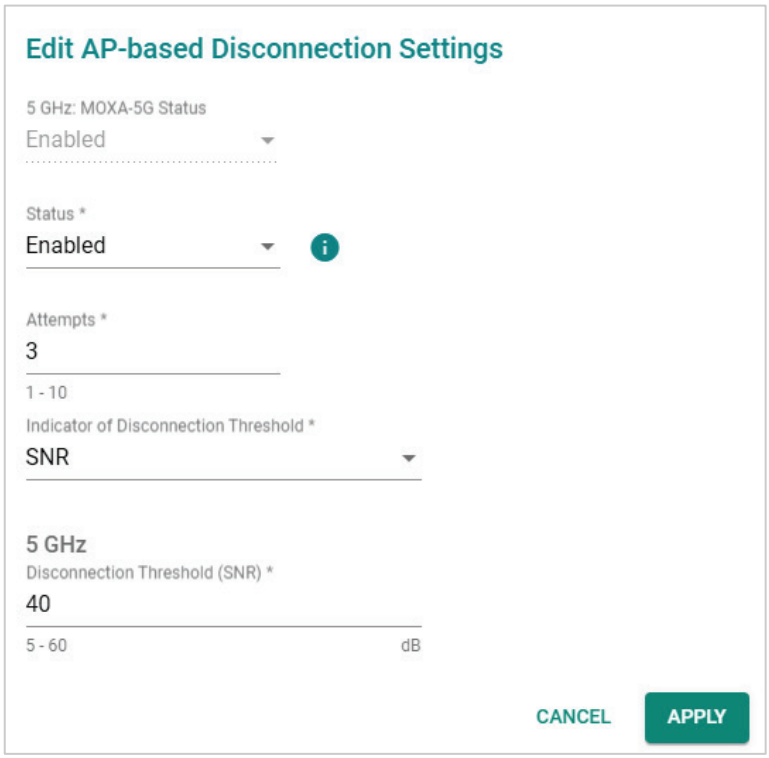
When finished, click **APPLY**.

AP-based Disconnection

The **AP-based Disconnection** tab contains Wi-Fi connectivity tools to configure the signal strength conditions for clients to meet normal operational communication requirements. Additionally, this screen allows users to enable the AP-based disconnection mechanism to disconnect legacy clients without roaming logic in order to encourage these clients to automatically associate to another AP with a stronger signal when falling below the set threshold. Click the **AP-based Disconnection** tab under **Wi-Fi > Connection Management** in the function tree to access this screen.



This tab displays all configured SSID profiles on the device. Click the pencil icon next to an SSID to edit the disconnection criteria for legacy clients.



Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the AP-based Disconnection mechanism.	Disabled

Attempts

Setting	Description	Factory Default
1 to 10	Specify the number of check attempts, with a 1 second interval between each check. If a client's SNR or signal strength falls below the set threshold consecutively for the specified number of attempts, the AP will disconnect the client.	3

Indicator of Disconnection Threshold

Setting	Description	Factory Default
SNR/Signal Strength	Select the threshold type for the disconnection mechanism.	SNR

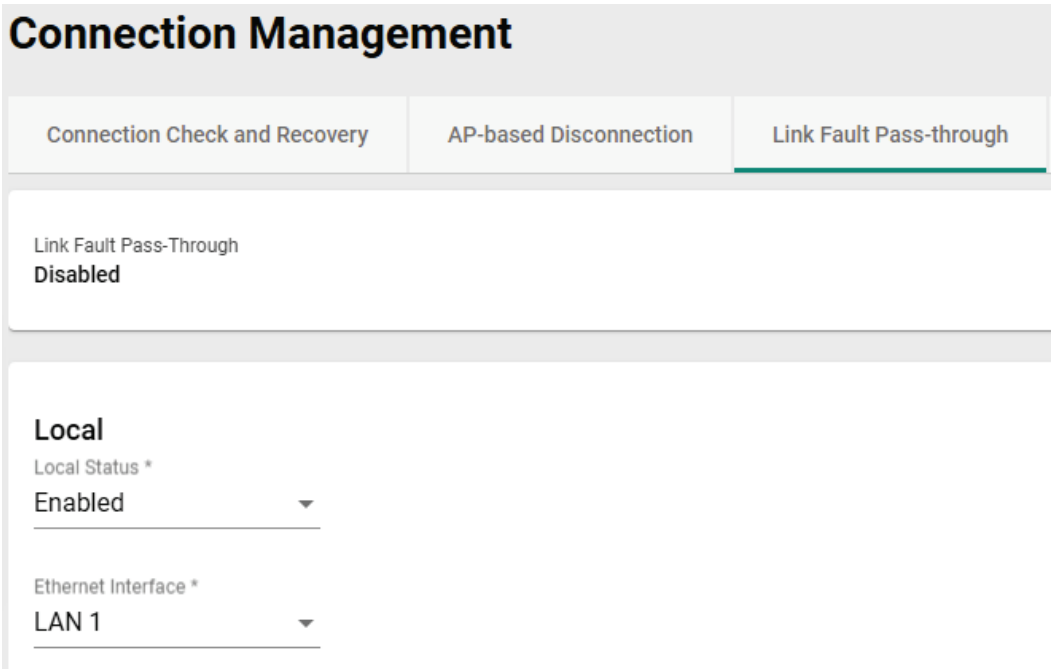
Disconnection Threshold

Setting	Description	Factory Default
5 to 60 dB for SNR/ -100 to -35 dBm for Signal Strength	Specify the threshold criteria for identifying poor client signal. When the client signal quality falls below the configured threshold, the AP will begin to check the client's signal. If a client's SNR or signal strength falls below the set threshold consecutively for the specified number of attempts, the AP will disconnect the client.	40 dB for SNR -65 dBm for Signal Strength

When finished, click **APPLY**.

Link Fault Pass-through

The Link Fault Pass-through feature helps detect wired link faults on the device's local Ethernet interface, or in uplink paths to a wired remote host. If a link fault is detected, the TAP AP will automatically disable its AP or Master SSID service to prevent wireless clients from associating and connecting to an AP that cannot successfully link to the designated application or service on the wired LAN network. Click the **Link Fault Pass-through** tab under **Wi-Fi > Connection Management** in the function tree to access this screen.



Local Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Link Fault Pass-through for local Ethernet interfaces.	Disabled

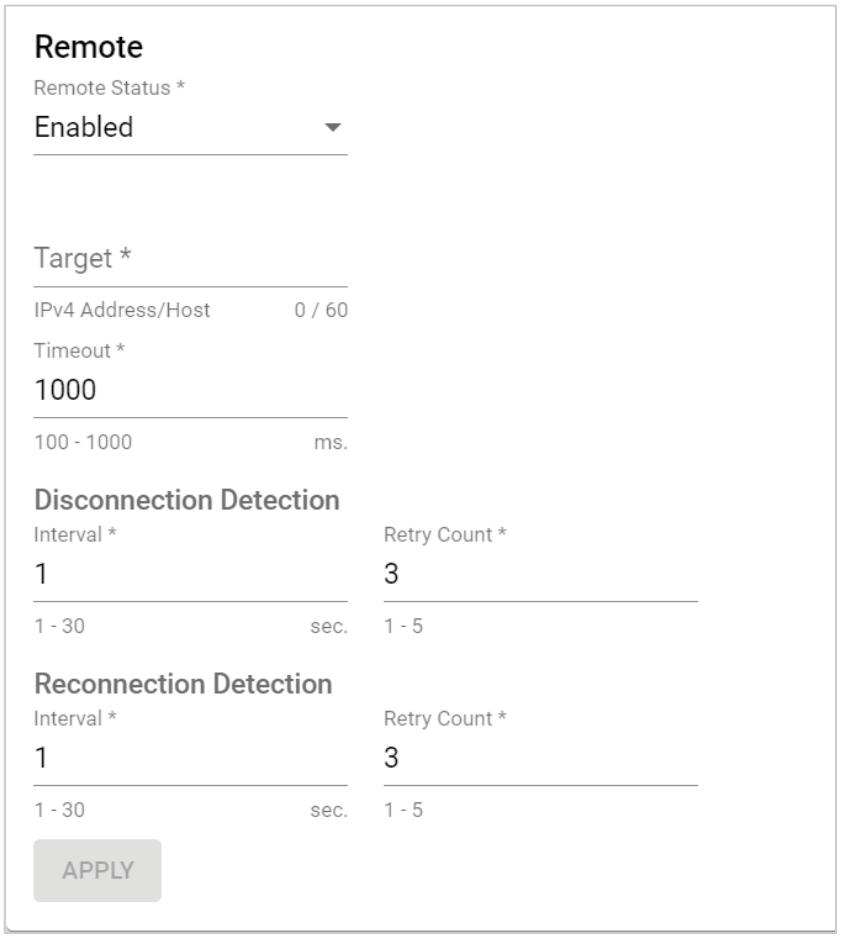
LAN Port

Setting	Description	Factory Default
LAN port	Select the LAN interface to monitor.	LAN 1

Remote Status

Enabling Link Fault Pass-through for remote links will cause the TAP to ping the target remote host at the specified interval to determine the status of the wired connection to the host.

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Link Fault Pass-through for links to remote hosts.	Disabled



Target

Setting	Description	Factory Default
IP address or hostname	Specify the IP address or hostname of the remote host to monitor.	None

Timeout

Setting	Description	Factory Default
100 to 1000 ms	Specify the duration (in ms) the TAP will wait before considering the host unresponsive.	1000

Disconnection Detection

The Disconnection Detection parameters determine the detection interval and retry count criteria for the TAP to deem the target remote host unreachable, triggering the shutdown of SSID service. The detection frequency may depend on the nature of the application and should be adjusted accordingly.

Interval

Setting	Description	Factory Default
1 to 30 sec	Specify the interval (in seconds) at which the TAP will ping the target host.	1

Retry Count

Setting	Description	Factory Default
3	Specify the number of times the TAP will retry to ping the host if no response is received.	3

Reconnection Detection

The Reconnection Detection parameters determine the detection interval and retry count criteria for the TAP to check if the link to the remote has been restored. If the link is deemed restored, the TAP will re-activate the SSID services for wireless clients attempting to connect to the AP.

Interval

Setting	Description	Factory Default
1 to 30 sec	Specify the interval (in seconds) at which the TAP will ping the target host.	1

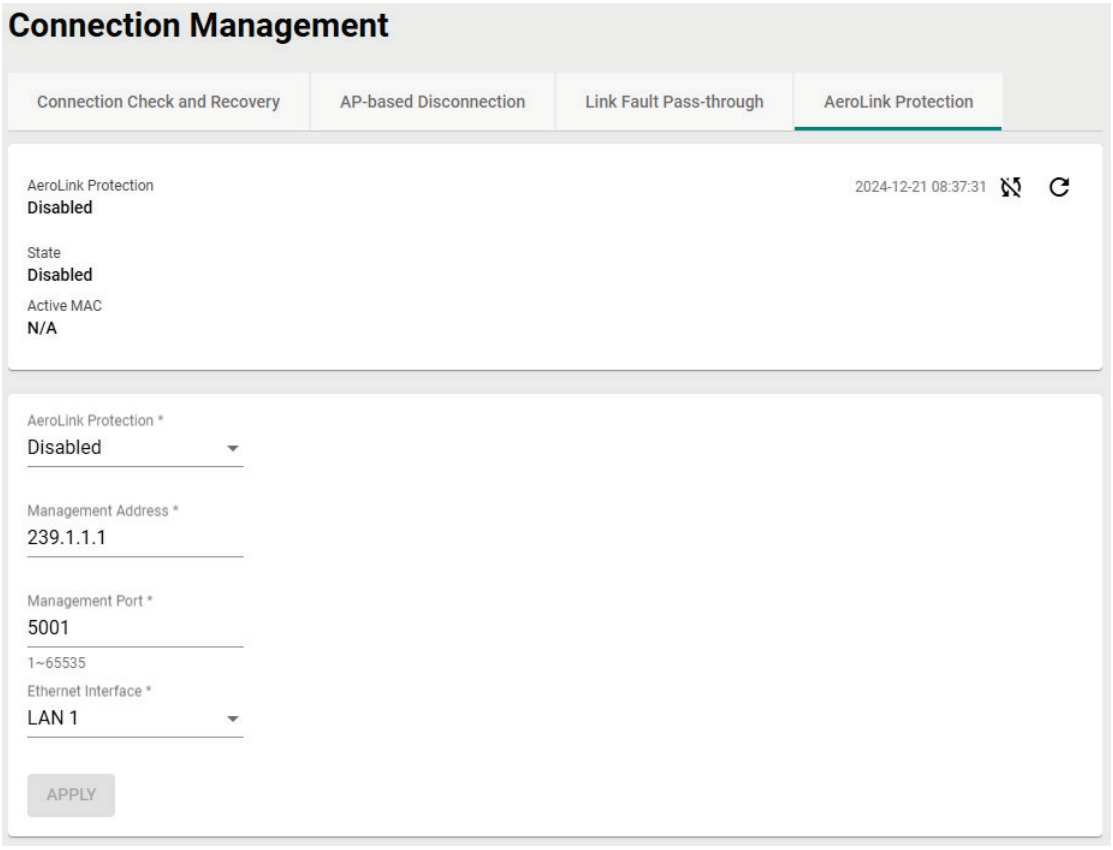
Retry Count

Setting	Description	Factory Default
3	Specify the number of times the TAP will retry to ping the host if no response is received.	3

When finished, click **APPLY**.

AeroLink Protection

The **AeroLink Protection** page lets you enable or disable AeroLink functionality and configure relevant settings. AeroLink Protection enables reliable train-to-ground communication with millisecond-fast client-based wireless redundancy that switches links between the backup devices once the active device or operating frequency is down. Click the **AeroLink Protection** tab under **Wi-Fi > Connection Management** in the function tree to access this screen.



AeroLink Protection

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable AeroLink Protection.	Disabled

Management Address

Setting	Description	Factory Default
IPv4 address	Specify the AeroLink Protection multicast management IPv4 address.	239.1.1.1

Management Port

Setting	Description	Factory Default
1 to 65535	Specify the AeroLink Protection management port.	5001

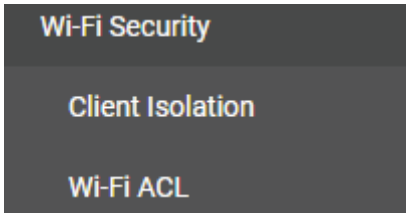
Ethernet Interface

Setting	Description	Factory Default
Interface	Specify the index of the Ethernet interface for AeroLink Protection.	LAN 1

When finished, click **APPLY**.

Wi-Fi Security

The **Wi-Fi Security** page lets you configure the Client Isolation and Wi-Fi Access Control List functions to manage access to the TAP device. Click **Wi-Fi Security** under **Wi-Fi** in the function tree to access this screen.

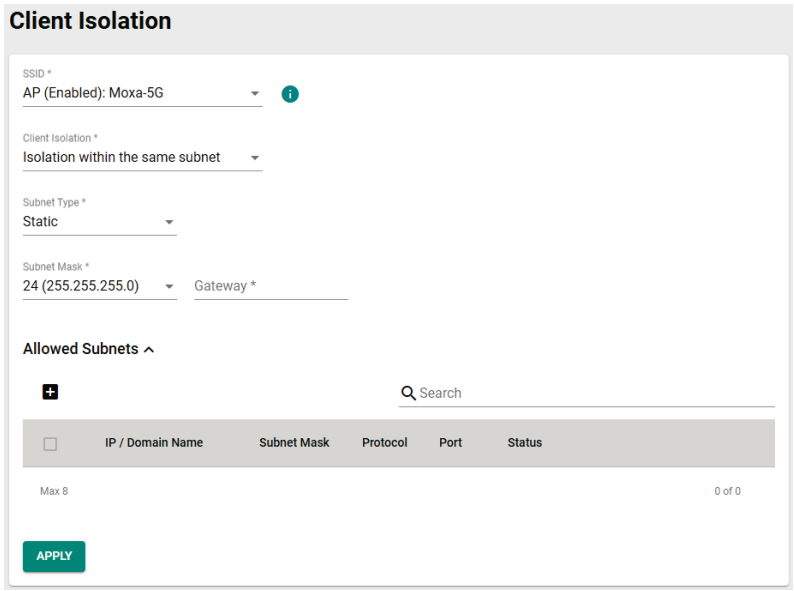


Client Isolation

The TAP-M310R Series supports client isolation functionality for AP-based operation modes to provide an additional layer of security for connected client devices.

For configured virtual access points, select the SSID you wish to enable client isolation for. Client isolation can be either enforced based on SSID where clients connecting to the same SSID on the AP are isolated from each other; or enforced by subnet where clients connecting to the same subnet as the configured SSID will be isolated from each other.

By default, client isolation is not enforced.



Client Isolation

Setting	Description	Factory Default
No isolation	Disable client isolation for the selected SSID.	No isolation
Isolation within the same BSSID	Enable client isolation for the selected SSID. Clients connected to this SSID cannot communicate with each other.	
Isolation within the same subnet	Enable client isolation for all within specific subnets. Depending on the selected subnet type, clients connected to either specified subnets or the same subnet as the SSID cannot communicate with each other.	

If the Client Isolation mode is set to **Isolation within the same subnet**, configure the following settings:

Subnet Type

Setting	Description	Factory Default
Static	Use a user-specified static subnet.	Static
DHCP	Use the DHCP server subnet	

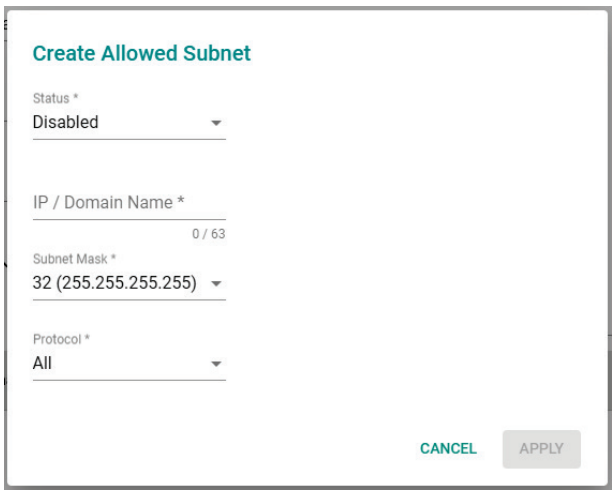
Subnet Mask

Setting	Description	Factory Default
1 (128.0.0.0) to 32 (255.255.255.255)	Specify the subnet mask.	24 (255.255.255.0)

Gateway

Setting	Description	Factory Default
IPv4 address	Specify the gateway address.	None

If Client Isolation is enabled, users can create allowed subnets where Client Isolation is not applied. To add a new allowed subnet, click the **Add** ( ) icon in the **Allowed Subnets** section.



Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the allowed subnet.	Disabled

IP / Domain Name

Setting	Description	Factory Default
Max. 63 characters	Specify the IP or domain name.	None

Subnet Mask

Setting	Description	Factory Default
1 (128.0.0.0) to 32 (255.255.255.255)	Specify the subnet mask.	32 (255.255.255.255)

Status

Setting	Description	Factory Default
All	The subnet allows all IP frames.	All
ICMP	The subnet only allows ICMP frames.	
TCP	The subnet only allows TCP frames.	
UDP	The subnet only allows UDP frames.	

TCP/UDP Port Range

Setting	Description	Factory Default
0 to 65535	Specify starting and ending port for the TCP/UDP port range.	None

When finished, click **APPLY**.

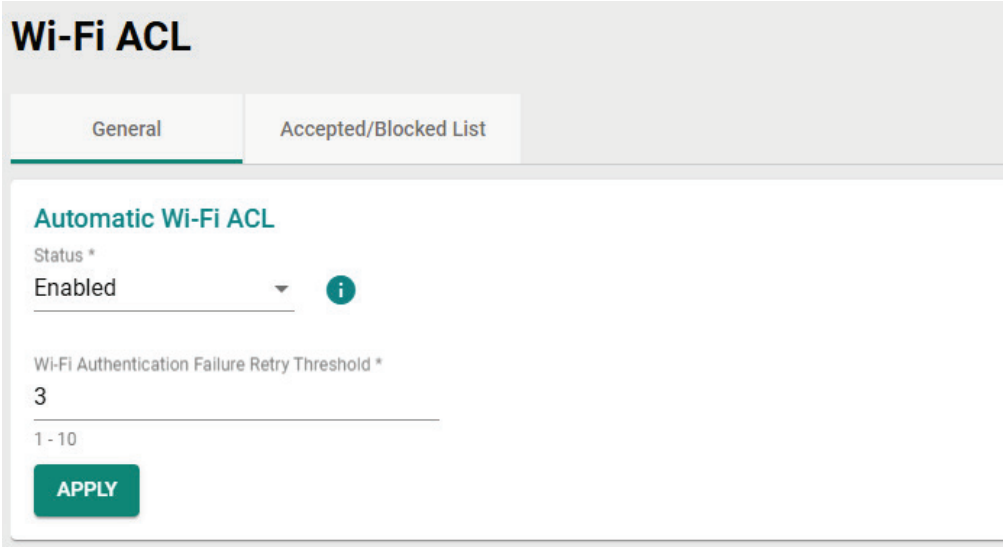
Wi-Fi ACL

The TAP-M310R Series supports Wi-Fi ACL filtering for both AP and client-based operation modes. Depending on the active operation mode, Wi-Fi ACL has two purposes. For AP-based operation modes, it blocks rogue client devices attempting to exhaust the Wi-Fi interface's resources. For client-based operation modes, it designates the list of authorized APs for the client to connect to.

There are two types of Wi-Fi ACL, Static or Automatic Wi-Fi ACL. Which type to use depends on the type of unwanted device to filter out through the Wi-Fi interface.

Automatic Wi-Fi ACL

Automatic Wi-Fi ACL will attempt to authenticate incoming device connections based on a specified number of tries. If the device fails all attempts, the TAP will automatically add this device to the list and block all future authentication requests from that device.



Automatic Wi-Fi ACL Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Automatic Wi-Fi ACL.	Disabled

Wi-Fi Authentication Failure Retry Threshold

Setting	Description	Factory Default
1 to 10	Specify the number of client authentication attempts. If the client consecutively fails the specified number of authentication checks, it will consider the client (client or AP) as a rogue device. Automatic Wi-Fi ACL will add the rogue device to the ACL and will block subsequent authentication attempts by this device in the future.	3

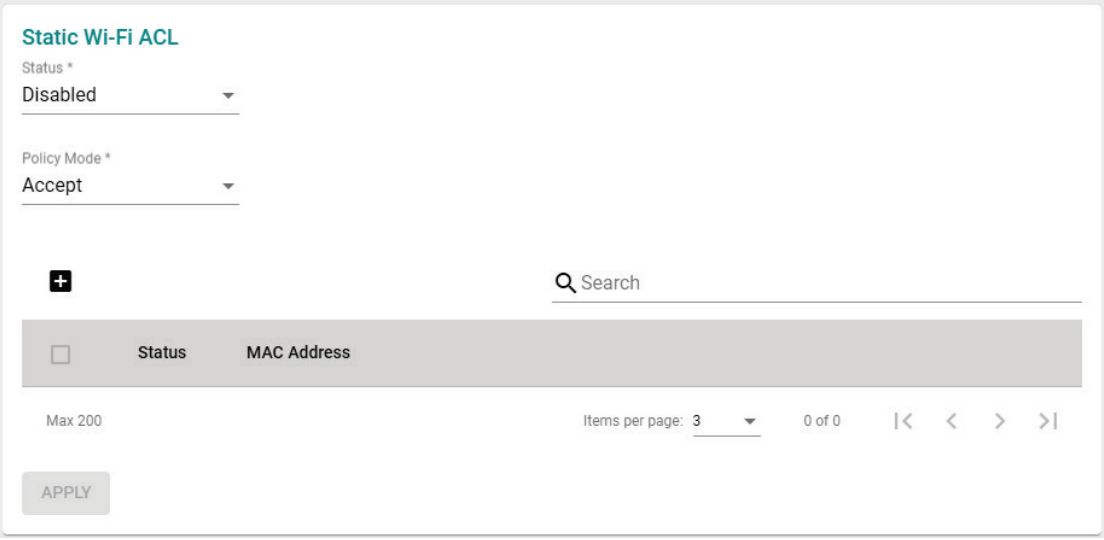
NOTE

Only management accounts with "Network" authority can manually remove or unlock devices blocked via Automatic Wi-Fi ACL.

When finished, click **APPLY**.

Static Wi-Fi ACL

Static Wi-Fi ACL allows users to manually add devices to the list by MAC address and set the access policy for all entries, either to allow or reject connections from the devices in the list.



Static Wi-Fi ACL Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Static Wi-Fi ACL.	Disabled

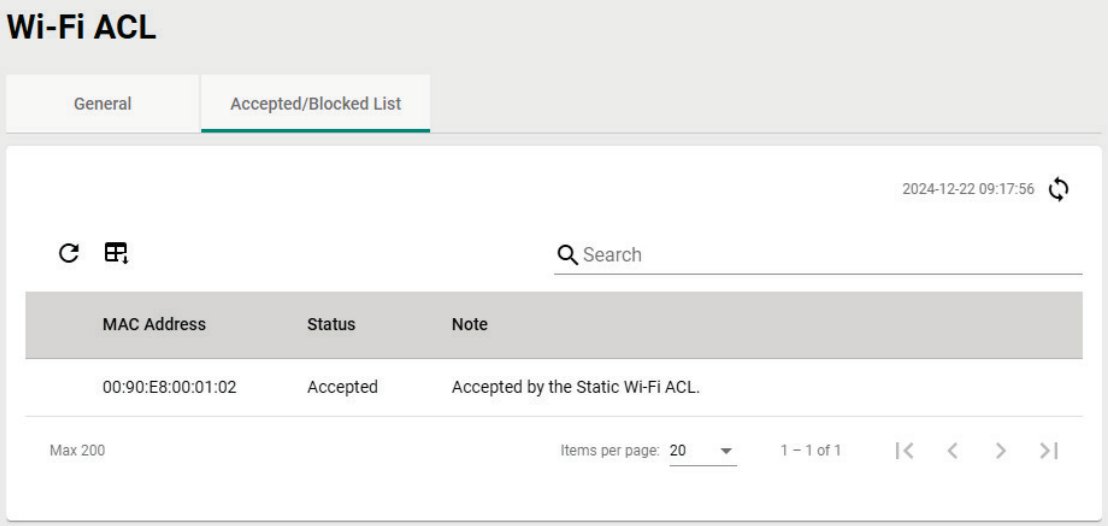
Static Wi-Fi ACL List Mode

Setting	Description	Factory Default
Block/Accept	Choose to either block or accept connections from the MAC addresses in the Static Wi-Fi ACL table.	Accept

When finished, click **APPLY**.

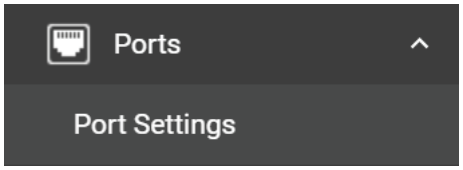
Accepted/Blocked List

The **Accepted/Blocked** List shows the list of devices accepted or blocked by Wi-Fi ACL. The list can be exported as CSV or PDF.



Ports

From the **Ports** section, you can configure **Port Settings**.

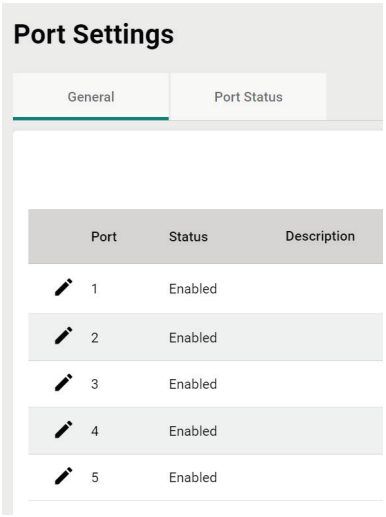


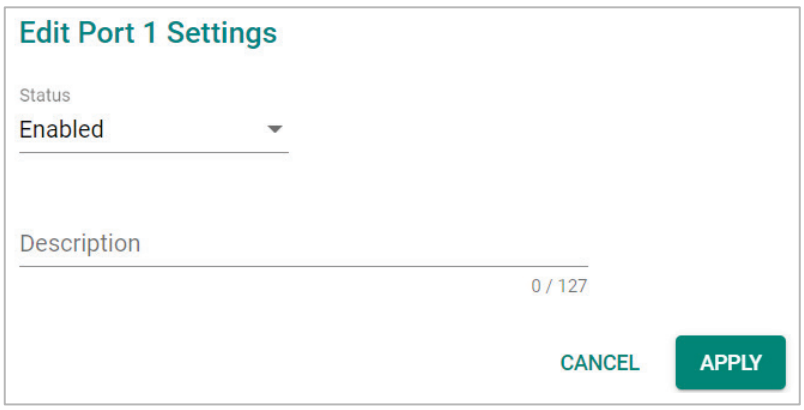
Port Settings

The **Ports Settings** page is used to configure the physical LAN 1 network ports on the device. Click **Port Settings** under **Ports** in the function tree to access this screen.

General Settings

Click **General** tab first, then click the **Edit** icon on the port you want to configure.





Configure the following settings:

Status

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

ATTENTION

The TAP-M310R-NPS-1R and -1P1R only have one LAN port (LAN1). If this port is disabled, the device will become inaccessible. The port can only be re-enabled via the console port or by resetting the device to factory default settings using the reset button.

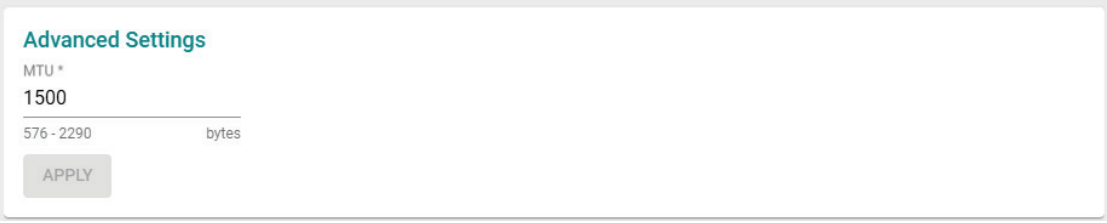
Description

Setting	Description	Factory Default
0 to 127 characters	Enter a description for the port.	None

ATTENTION

When more than one LAN ports is enabled, only one LAN port should be used as an uplink. The other LAN ports may be used to connect other Ethernet based devices such as IP cameras. Be careful NOT to connect more than one LAN port as uplinks to a switch simultaneously to prevent switching loops.

From the **Advanced Settings** section, users can configure the MTU size.



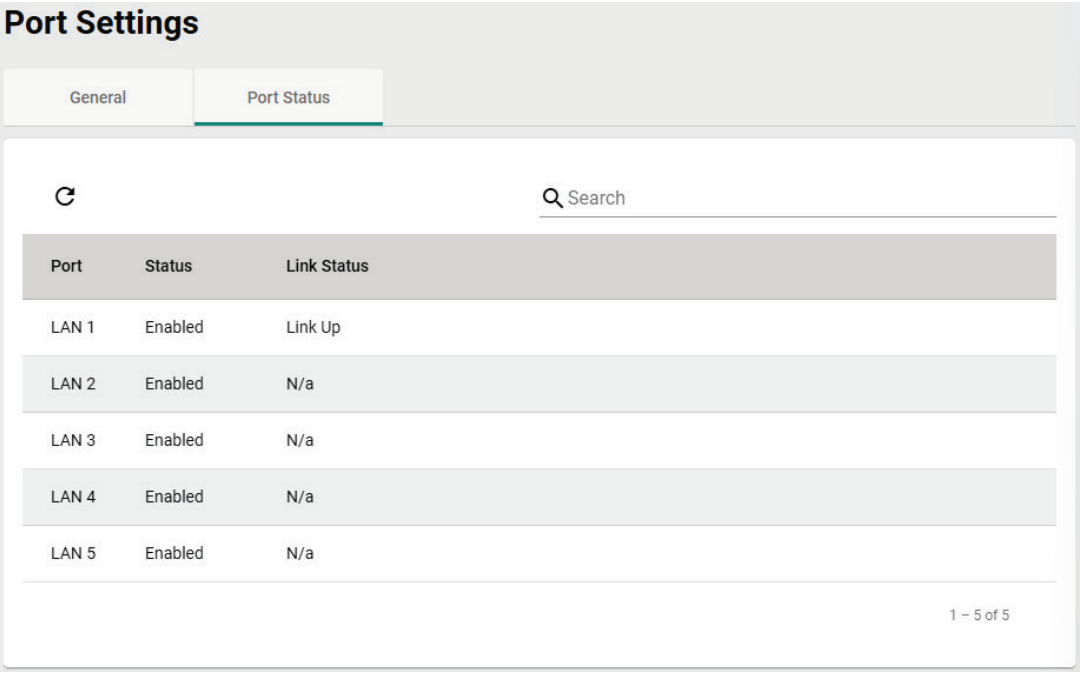
MTU

Setting	Description	Factory Default
576 to 2290 bytes	Configure the Maximum Transmission Unit (MTU) size (in bytes) depending on the application traffic type. Configuring a larger MTU value results in a lower packet count (less network congestion) over the wireless network when transmitting applications generate large data packets.	1500

When finished, click **APPLY**.

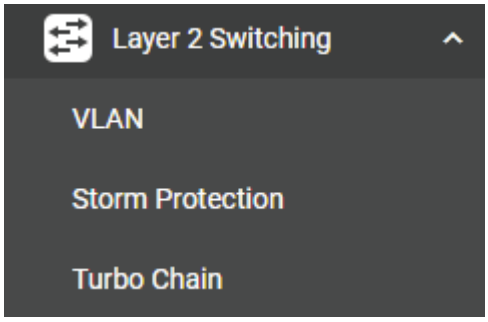
Status Check

Click the **Port Status** tab to check the current port and port link status.



Layer 2 Switching

This section describes how to configure the Layer 2 switching settings for the TAP.



VLAN

The Virtual LAN (VLAN) Concept

What is a VLAN?

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were connected to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows for end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks via SSID and VLAN assignment. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

Benefits of VLANs

VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage additions, relocations, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
- Improve network performance and reduce latency
- Increase security
- Secure network restricts members to resources on their own VLAN
- Clients roam without compromising security

VLAN Workgroups and Traffic Management

The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 9 SSIDs per radio interface, with a unique VLAN configurable per SSID.

The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

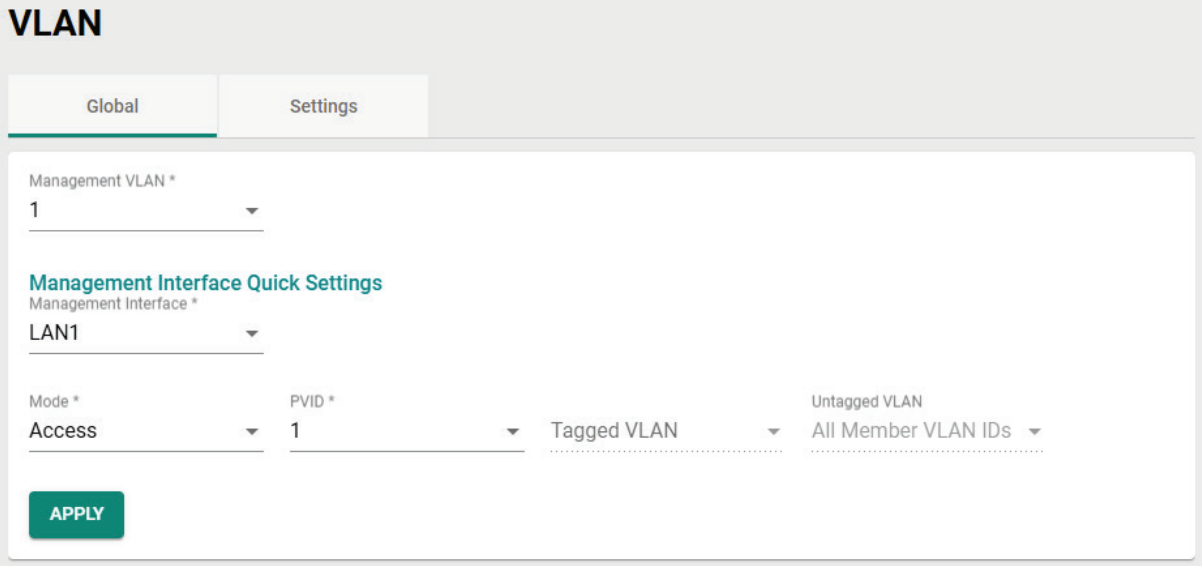
In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a department workgroup; for example, one VLAN could be used for a marketing department and the other for a human resource department.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as marketing or human resource, depending on which wireless client received it. The AP would insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resource department could be restricted to a gateway that allowed access to only the Internet. A member of the human resource department could send and receive e-mail and access the Internet but would be prevented from accessing servers or hosts on the local corporate network.

Global Settings

The **Global Settings** page is used to configure the management VLAN and interface. Click the **Global** tab to access this screen.



Configure the following settings:

Management VLAN ID

Setting	Description	Factory Default
1 to 4094	Specify the management VLAN of this TAP. By default, there is only VLAN ID 1. Additional VLAN IDs will need to be created first before they can be selected.	1

Management Interface Quick Settings

Management Interface

Setting	Description	Factory Default
Interface	Select the management VLAN interface.	None

Mode

Setting	Description	Factory Default
Access	Access mode is used if the port is connected to a single device, without tags.	Access
Hybrid	Hybrid mode is used if the port is connected to another Access 802.1Q VLAN-aware switch or another LAN that combines tagged and untagged devices.	

PVID

Setting	Description	Factory Default
1 to 4094	Set the default VLAN ID for untagged devices connected to the port.	1

Tagged VLAN

Setting	Description	Factory Default
1 to 4094	If the port type is set to Trunk or Hybrid, specify the VLAN ID for tagged devices that connect to this port.	None

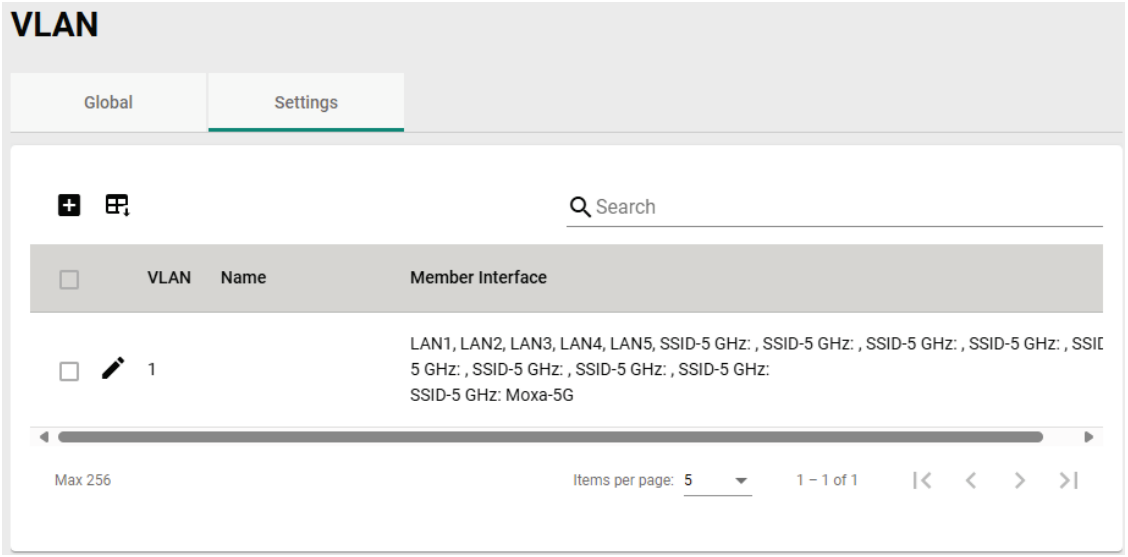
Untagged VLAN

Setting	Description	Factory Default
1 to 4094	If the port type is set to Hybrid, specify the VLAN ID for tagged devices that connect to this port and the tags that need to be removed in egress packets.	Dependent on the selected PVID

When finished, click **APPLY**.

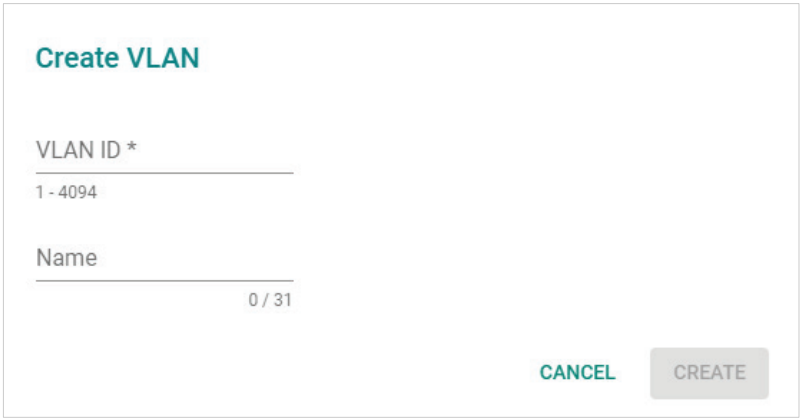
VLAN Settings

From the **Settings** tab, you can create, edit, and delete VLANs. Click the **Settings** tab to access this screen.



Create a New VLAN ID

To add a new VLAN ID, click the **Add** icon.



Configure the following settings:

VLAN ID

Setting	Description	Factory Default
1 to 4094	Enter the VLAN ID.	None

Name

Setting	Description	Factory Default
0 to 31 characters	Enter a name for the VLAN.	None

When finished, click **CREATE**.

Edit an Existing VLAN ID

To edit an existing VLAN ID, click the **Edit** icon next to the VLAN you want to edit.

Configure the following settings:

NOTE

Once created, the VLAN ID cannot be changed. Only the VLAN name can be edited.

To modify a VLAN ID and VLAN name combination, delete the entry and create a new entry with the desired VLAN ID and name.

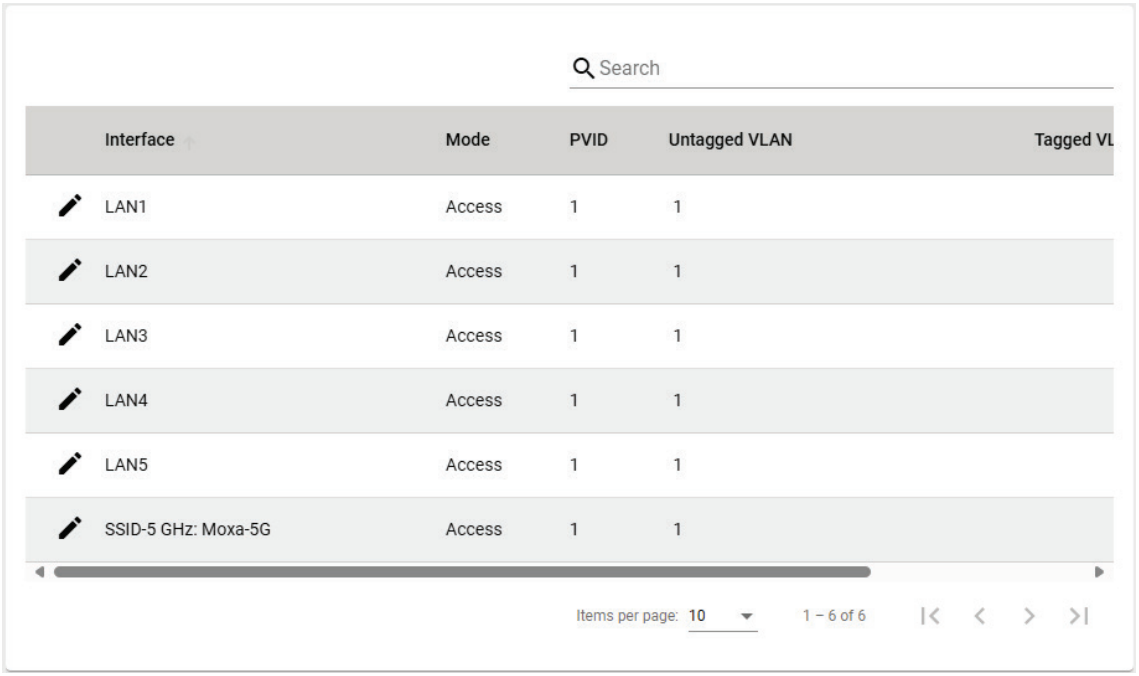
Name

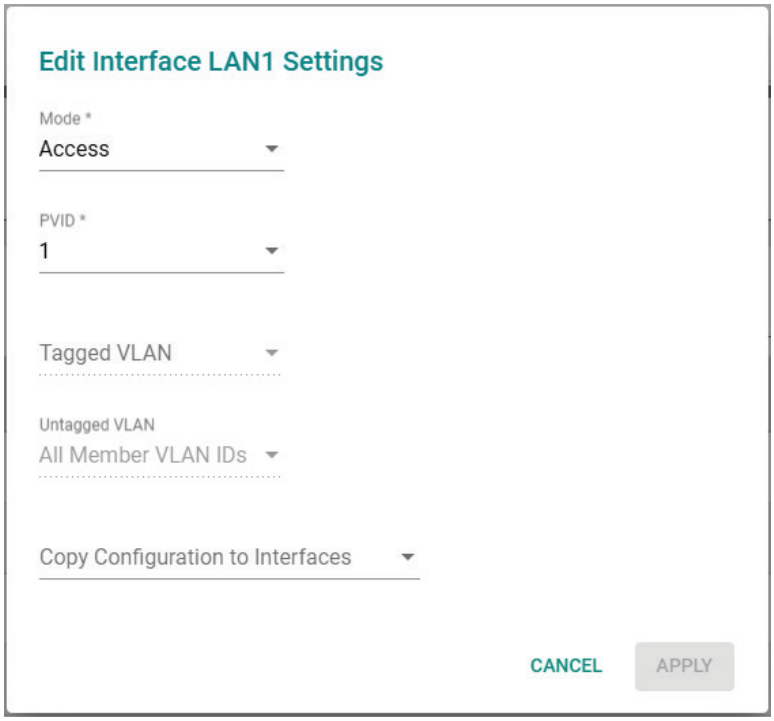
Setting	Description	Factory Default
0 to 31 characters	Enter a name for the VLAN ID.	None

When finished, click **APPLY**.

Edit VLAN Interface Settings

To edit the VLAN interface settings, click the **Edit** icon next to the interface you want to edit.





Configure the following settings:

Mode

Setting	Description	Factory Default
Access	Access mode is used if the port is connected to a single device, without tags.	Access
Hybrid	Hybrid mode is used if the port is connected to another Access 802.1Q VLAN-aware switch or another LAN that combines tagged and untagged devices.	

PVID

Setting	Description	Factory Default
1 to 4094	Set the default VLAN ID for untagged devices connected to the port.	1

Tagged VLAN

Setting	Description	Factory Default
1 to 4094	If the port type is set to Hybrid, specify the VLAN ID for tagged devices that connect to this port.	None

Untagged VLAN

Setting	Description	Factory Default
VID range from 1 to 4094	If the port type is set to Hybrid, specify the VLAN ID for tagged devices that connect to this port and the tags that need to be removed in egress packets.	Dependent on the selected PVID

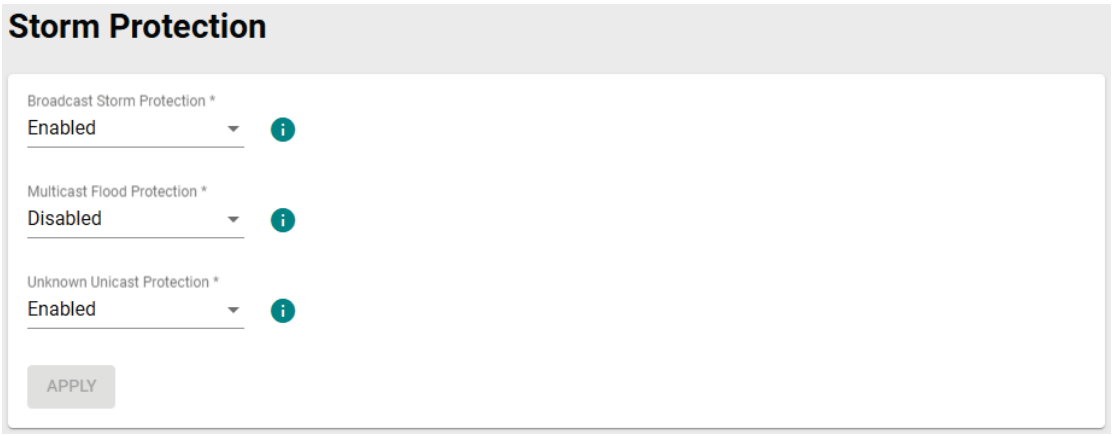
Copy Configurations to Interfaces

Setting	Description	Factory Default
Interface	Select the interface to copy the configuration of this interface to.	None

When finished, click **APPLY**.

Storm Protection (TAP-M310R-1P1R1S and -1P2R1S Only)

The TAP-M310R Series supports Storm Protection to protect the device against packet storms caused by wrong configurations or unexpected network device behavior.



Configure the following settings:

Broadcast Storm Protection

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Broadcast Storm Protection. If enabled, the switch component will limit the broadcast output bandwidth of each port to 1 Mbps.	Enabled

Multicast Flood Protection

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Multicast Flood Protection. If enabled, the switch component will limit the combined broadcast and multicast output bandwidth of each port to 1 Mbps.	Disabled

Unknown Unicast Protection

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable Unknown Unicast Protection. If enabled, the switch component will block CPU-bound unicast packets with an unknown destination.	Enabled

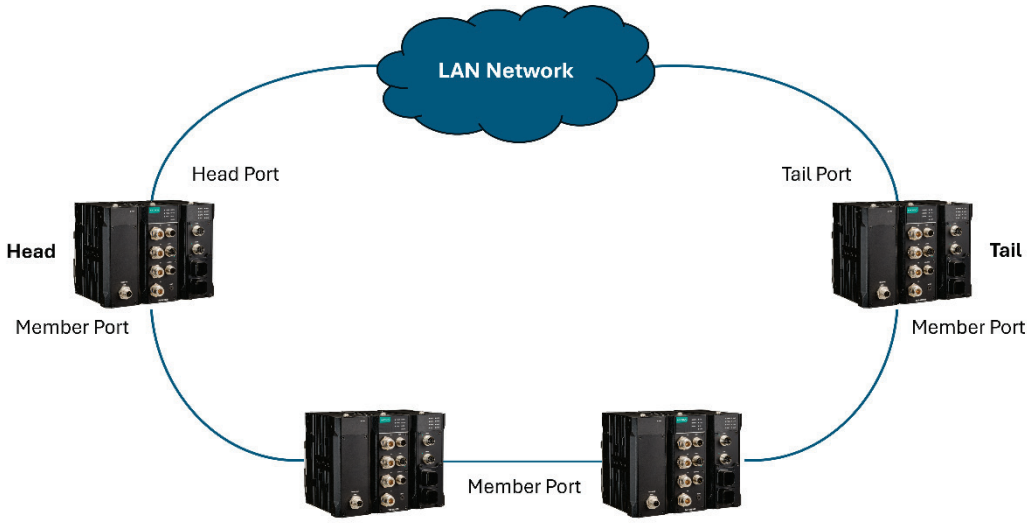
When finished, click **APPLY**.

Turbo Chain (TAP-M310R-1P1R1S and -1P2R1S Only)

What is Turbo Chain?

Moxa's Turbo Chain is an advanced software-technology that gives network administrators the flexibility of constructing any type of redundant network topology. When using the "chain" concept, you first connect the APs in a chain and then simply link the two ends of the chain to an Ethernet network, as illustrated in the following figure.

Turbo Chain can be used on industrial networks that have a complex topology. If the industrial network uses a multi-ring architecture, Turbo Chain can be used to create flexible and scalable topologies with a fast media-recovery time.



Setting up Turbo Chain

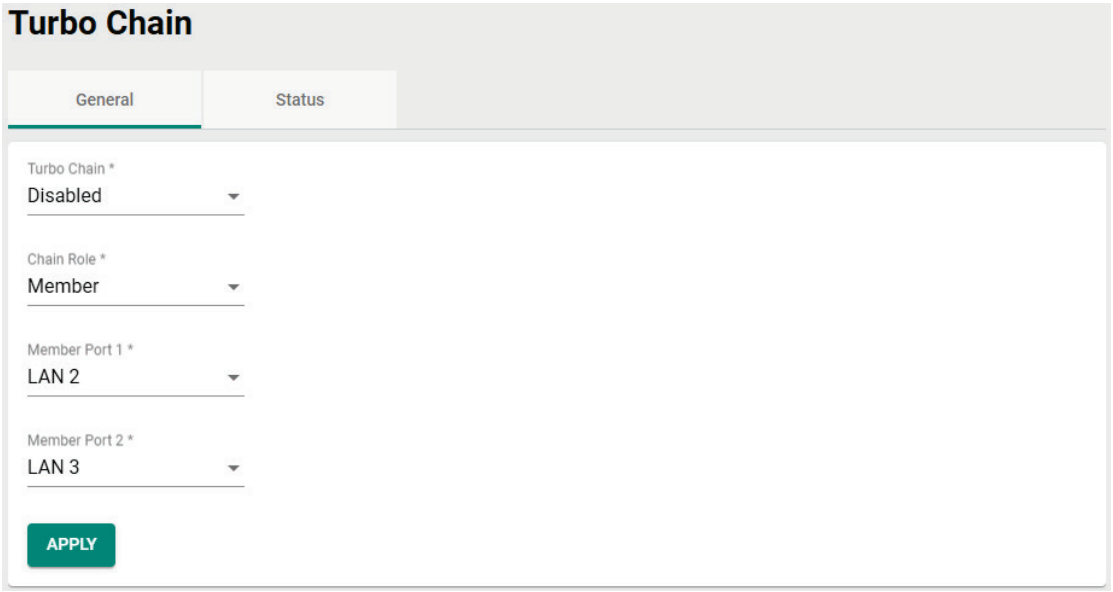
Configuring a Turbo Chain environment requires several key steps.

1. Designate the Head AP, Tail AP, and Member AP devices.
2. On the Head AP, configure one port as the Head port and another port as a Member port.
3. On the Tail AP, configure one port as the Tail port and another port as a Member port.
4. On each Member AP, configure two ports as Member ports.
5. Connect the Head AP, Tail AP, and Member APs as shown in the above diagram.

The path connecting to the Head port is the main path, and the path connecting to the Tail port is the backup path of the Turbo Chain. Under normal conditions, packets are transmitted through the Head Port to the LAN network. If the main Turbo Chain path is disconnected, the Tail Port backup path will be activated to make sure packet transmissions can continue.

General Settings

The **General Settings** page is used to configure Turbo Chain settings. Click the **General** tab to access this screen.



Configure the following settings:

Turbo Chain

Setting	Description	Factory Default
Enabled/Disabled	Enable or Disable Turbo Chain.	Disabled

Chain Role

Setting	Description	Factory Default
Head	Designate this AP as the Head AP.	Member
Member	Designate this AP as a Member AP.	
Tail	Designate this AP as the Tail AP.	

Head Port/Tail Port/Member Port 1/2 (Depending on the Selected Chain Role)

Setting	Description	Factory Default
LAN 2/LAN 3	Assign LAN 2 or LAN 3 as the Head, Tail, or a Member port.	Depends on the selected Chain Role

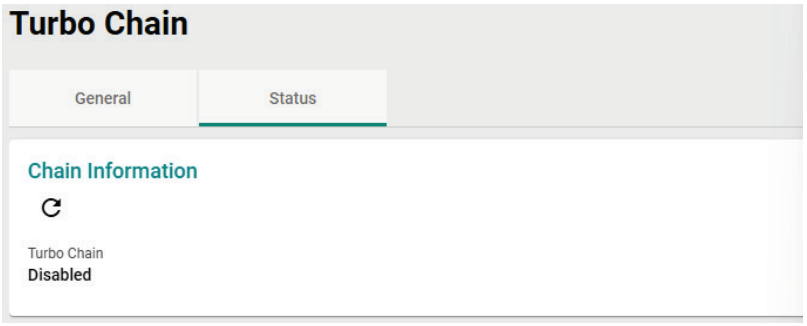
NOTE

Only fiber ports can be configured for Turbo Chain.

When finished, click **APPLY**.

Status

The **Status** shows the current Turbo Chain status. Click the **Status** tab to access this screen.

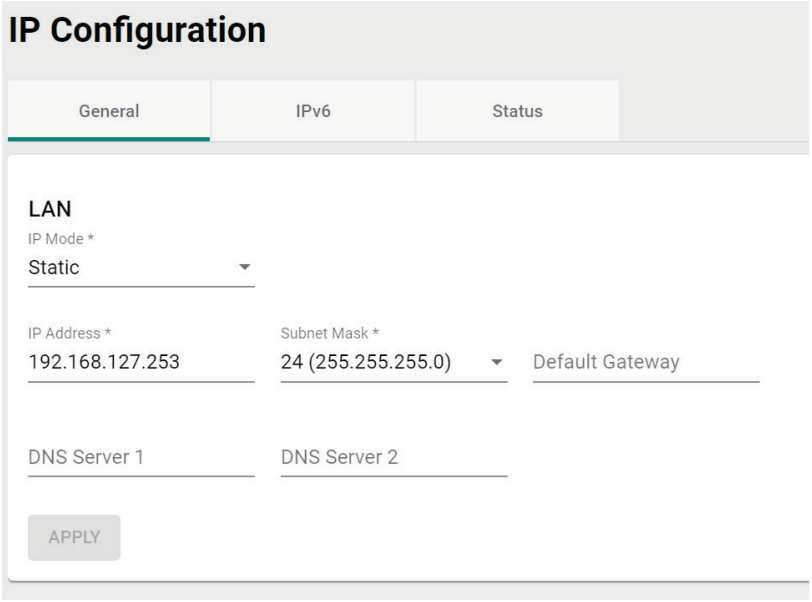


IP Configuration

The **IP Configuration** section is used to configure the device's basic IP configuration. Click **IP Configuration** in the function tree.

General Settings

The **General** tab lets you configure the device's basic network information. Click the **General** tab to access this screen.



Configure the following settings:

IP Mode

Setting	Description	Factory Default
DHCP	The TAP is assigned an IP address automatically by the network's DHCP server.	Static
Static	Manually configure up the TAP's IP address.	

IP Address

Setting	Description	Factory Default
IP address	Enter the TAP's IP address.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
Subnet mask	Select the subnet mask. This is used to identify the type of network the TAP is connected to (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	24 (255.255.255.0)

Default Gateway

Setting	Description	Factory Default
IP address	Enter the IP address of the router that connects the LAN to an outside network.	None

DNS Server 1 and DNS Server 2

Setting	Description	Factory Default
IP address	Enter the primary and secondary DNS server address. After entering the DNS server's IP address, you can input the TAP's URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

When finished, click **APPLY**.

IPv6

In addition to other benefits, IPv6 offers a significantly larger addressing pool compared to IPv4. IPv6 addresses are represented as eight groups of four hexadecimal digits each, separated by colons. The full representation may be shortened; for example, 2001:0db8:0000:0000:0000:8a2e:0370:7334 becomes 2001:db8::8a2e:370:7334.

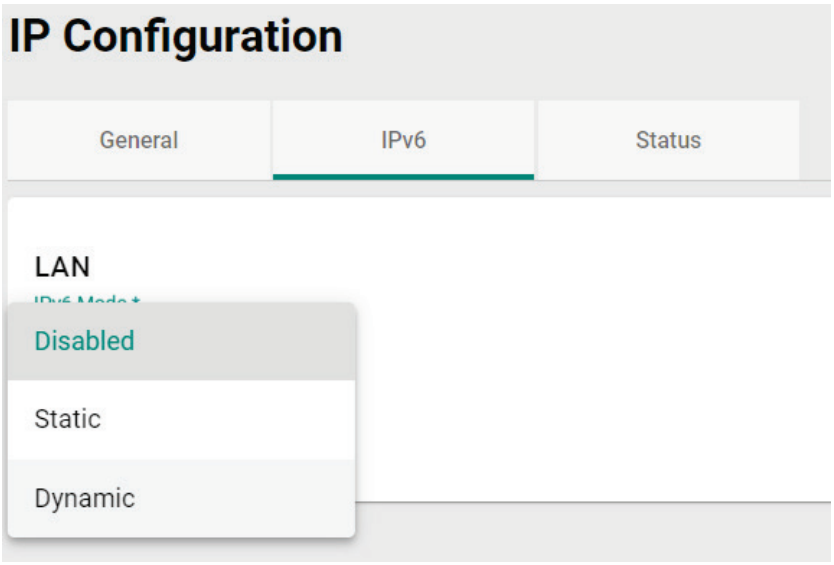
The TAP-M310R Series supports an IPv4 and IPv6 dual stack design, allowing the device to configure both an IPv4 and IPv6 address. This feature also allows the TAP to communicate with other nodes on the LAN or

the Internet using either IPv4 or IPv6. The DNS protocol is used by both IP protocols to resolve fully qualified domain names and IP addresses, but dual stack requires that the resolving DNS server can resolve both types of addresses.

Refer to the following sections for more information on the available modes for each option.

IPv6 LAN Options

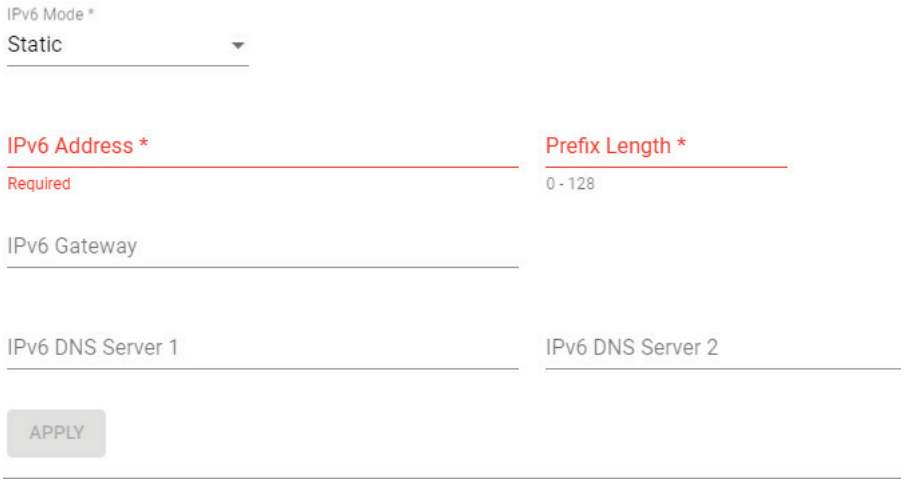
In all operation modes except Client-router mode, the TAP acts as a bridge device that receives and transmits data within the same network segment.



IPv6 Mode

Setting	Description	Factory Default
Disabled	Disable IPv6 functionality.	Disabled
Static	Manually configure the device's IPv6 address information. requires manual configuration.	
Dynamic	Automatically acquire the IPv6 address and DNS server information from an upstream IPv6 DHCP server on the network.	

If **IPv6 Mode** is set to **Static**, configure the following options:



IPv6 Address

Setting	Description	Factory Default
IPv6 address	Specify the IPv6 in the format of the eight groups of four hexadecimal digits, For example: 2001:b011:20e0:cb8:211:32ff:fe88:1d16	None

Prefix Length

Setting	Description	Factory Default
0 to 128 characters	Specify the IPv6 Prefix Length, between 0 to 128 characters. This is equivalent to the IPv4 subnet mask.	None

IPv6 Gateway

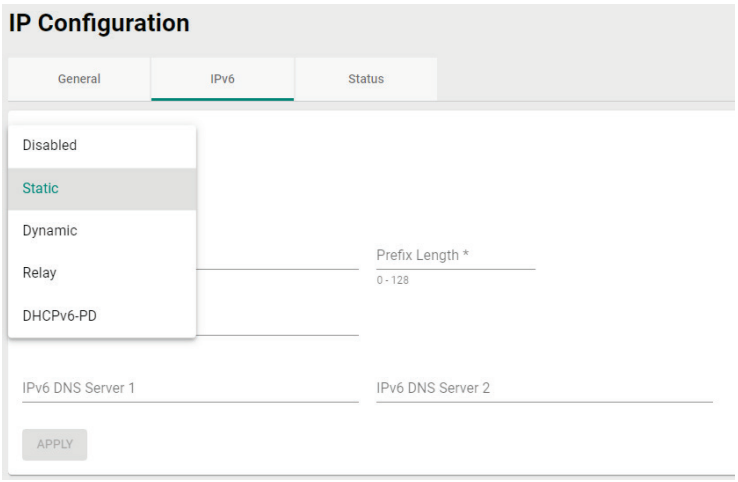
Setting	Description	Factory Default
IPv6 gateway address	Specify the IPv6 gateway address, if applicable.	None

IPv6 DNS Server 1/2

Setting	Description	Factory Default
DNS server address	Specify the address of the primary and secondary IPv6 DNS server.	None

IPv6 WAN Options

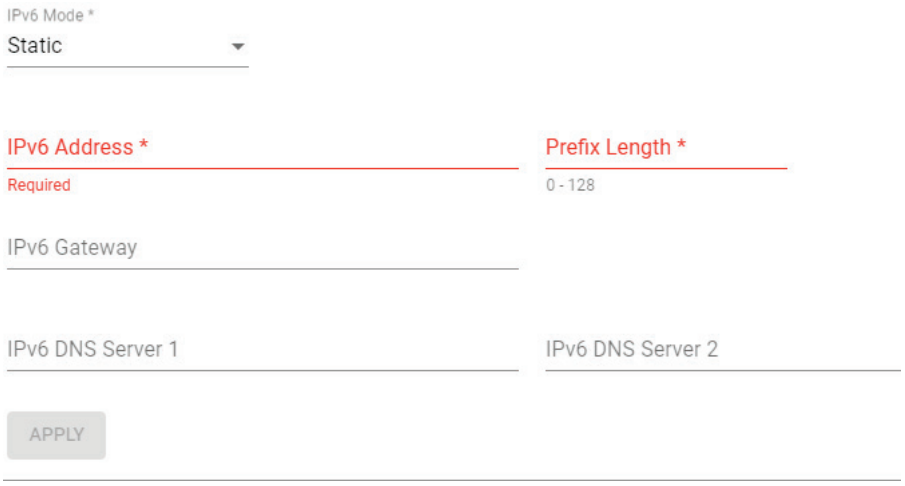
When operating in Client-router mode, the TAP acts as a router interfacing between two different network segments. Note that, except for Static, all WAN options require the admin to first configure the LAN IPv6 address in the Client operation mode and then switch back to Client-router mode in order to apply settings for the Dynamic, Relay, and DHCPv6-PD options.



IPv6 Mode

Setting	Description	Factory Default
Disabled	Disable IPv6 functionality.	Disabled
Static	Manually configure the device's IPv6 address information. requires manual configuration.	
Dynamic	Automatically acquire the IPv6 address and DNS server information from an upstream IPv6 DHCP server on the network.	
Relay	Configure the TAP as an IPv6 client and relay agent that can relay DHCPv6 requests from LAN-connected IPv6 clients to an upstream DHCPv6 Server. In this mode, the TAP automatically acquires its IPv6 address and DNS server information from an upstream IPv6 DHCP server on the network.	
DHCPv6-PD	Configure the TAP as an IPv6 client and prefix delegator that can automatically delegate IPv6 prefixes and assign IP addresses to connected devices based on the DHCPv6 Server configuration. In this mode, the TAP automatically acquires its IPv6 address and DNS server information from an upstream IPv6 DHCP server on the network.	

If **IPv6 Mode** is set to **Static**, configure the following options:



IPv6 Address

Setting	Description	Factory Default
IPv6 address	Specify the IPv6 in the format of the eight groups of four hexadecimal digits, For example: 2001:b011:20e0:cb8:211:32ff:fe88:1d16	None

Prefix Length

Setting	Description	Factory Default
0 to 128 characters	Specify the IPv6 Prefix Length, between 0 to 128 characters. This is equivalent to the IPv4 subnet mask.	None

IPv6 Gateway

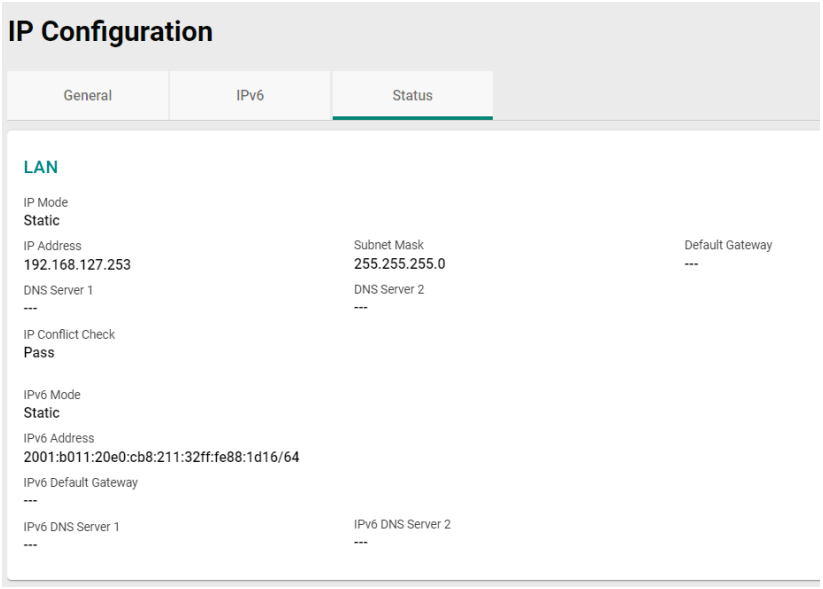
Setting	Description	Factory Default
IPv6 gateway address	Specify the IPv6 gateway address, if applicable.	None

IPv6 DNS Server 1/2

Setting	Description	Factory Default
DNS server address	Specify the address of the primary and secondary IPv6 DNS server.	None

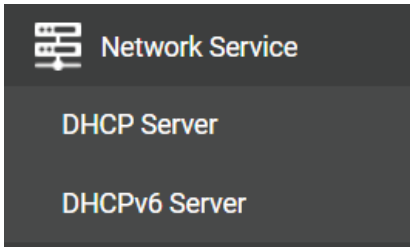
IP Configuration Status

To view the status of the current IP configuration, click the **Status** tab.



Network Service

From the **Network Service** section, you can configure **DHCP Server** and **DHCPv6 Server** settings.



DHCP Server

The **DHCP Server** section is used for configuring a local DHCP server for IP provisioning to connected devices. DHCP Server is only available for AP/Master/Client-Router operation modes. If the device is in Client-Router mode, the DHCP service applies to LAN interfaces for wired connected devices.

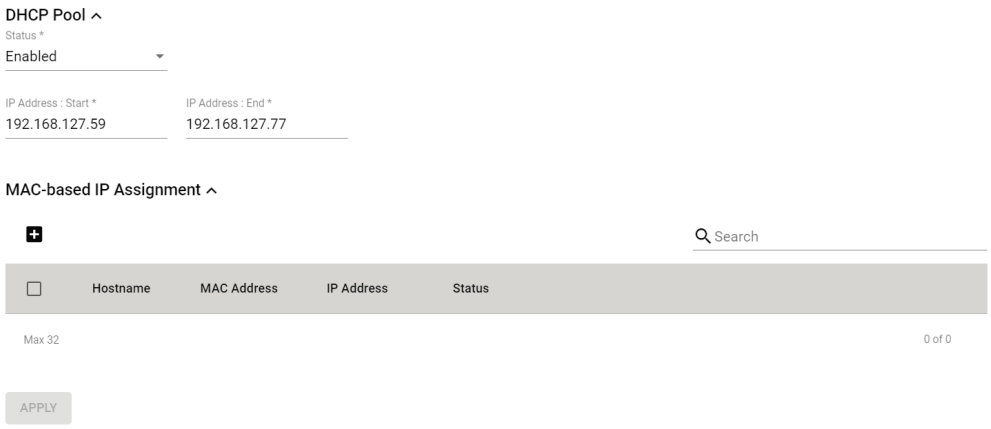
IP addresses can be assigned in one of two ways:

- Dynamic: The DHCP server automatically assigns IP addresses to devices from a configured IP address range.
- Static: Users manually map an IP address to a specific MAC address.

If necessary, users can use a mixed provisioning model with both dynamic DHCP pool and MAC-based IP assignment. In a mixed DHCP mode environment, the system will first check if the device is listed in the MAC-based IP assignment table. If no matching entry is found, the system will assign an IP address from the configured DHCP IP pool.

NOTE

Due to a functional limitation, if the device's own IP is acquired through DHCP, the DHCP Server feature cannot be enabled on the device.

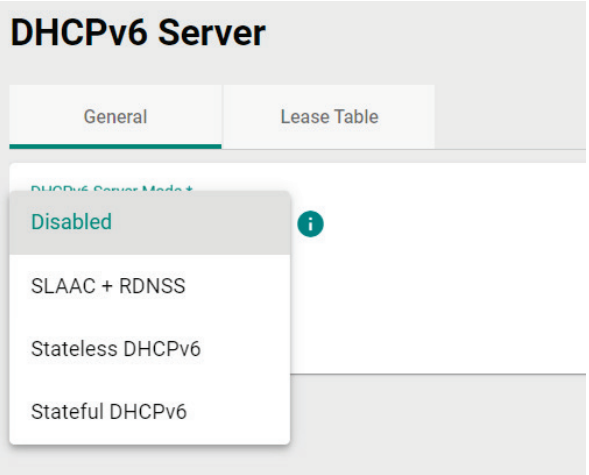


DHCPv6 Server

General

The DHCPv6 Server feature allows the device to assign IPv6 address to connected devices.

If the TAP's IPv6 settings were manually configured or obtained via DHCPv6-PD, the TAP can provision IPv6 addresses to connected devices downstream of the TAP's LAN ports in one of three supported modes.



DHCPv6 Server Mode

Setting	Description	Factory Default
Disabled	Disable the DHCPv6 server function.	Disabled
SLAAC + RDNSS	Connected devices or IPv6 clients issue a Router Solicitation (RS) and interpret the IPv6 Prefix, Default Gateway, DNS address from the Router Advertisement (RA) to compose their IPv6 address parameters by combining the prefix with a self-generated host ID.	
Stateless DHCPv6	Connected devices or IPv6 clients issue Router a Solicitation (RS) and interpret the IPv6 Prefix, Default Gateway from the Router Advertisement (RA) to compose their IPv6 address parameters by combining the prefix with a self-generated host ID. Subsequently it issues a DHCP Solicit and interprets the DHCPv6 Advertise to extract the DNS address.	
Stateful DHCPv6	Connected devices or IPv6 clients issue a Router Solicitation (RS) and interpret the Default Gateway address from the Router Advertisement (RA). Subsequently, it issues a DHCP Solicit / Request and interprets the DHCPv6 Advertise / Reply respectively to extract the DNS address and issued IPv6 address. The benefit of the Stateful DHCPv6 option is the state of all issued IPv6 address can be monitored and managed in the DHCPv6 Server.	

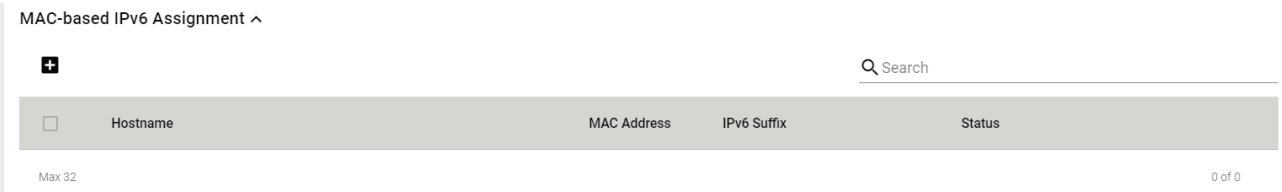
Lease Time

Setting	Description	Factory Default
2 to 14400	Specify the valid duration (in minutes) of issued IPv6 addresses.	1440

DNS Server 1/2

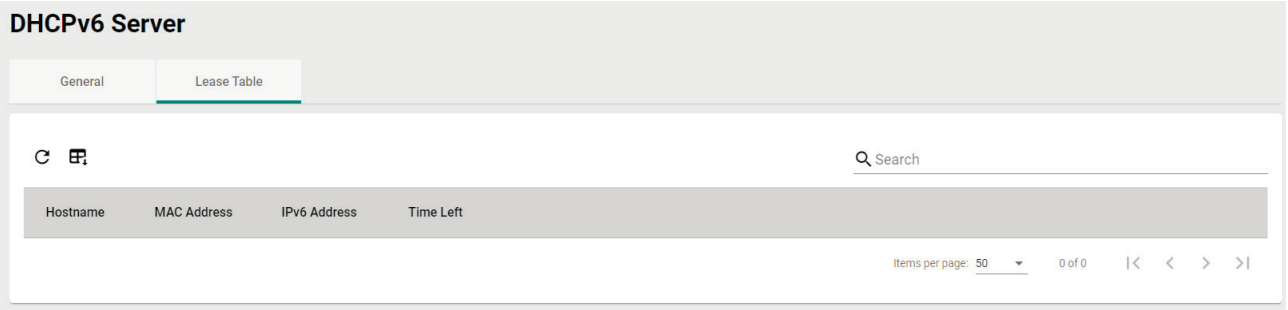
Setting	Description	Factory Default
IP address	Specify the IP address of the first and second DNS server.	None

If **Stateful DHCPv6** is selected, configure the IPv6-to-MAC mapping. Click the **Add** icon to add a new entry.



Lease Table

The **Lease Table** page shows the IPv6 addresses assigned by the DHCPv6 Server.

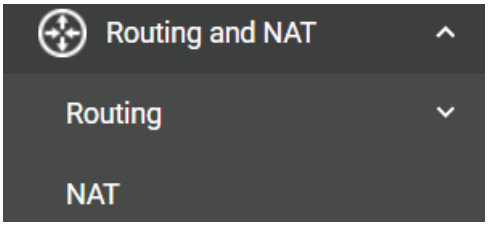


Click the **Refresh** icon to refresh the table.

Click the **Export** button to export the table.

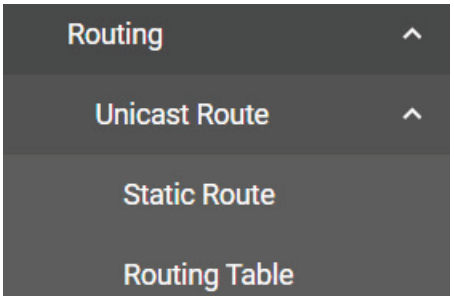
Routing and NAT

From the **Routing and NAT** section you can configure **Routing** and **NAT** settings.



Routing

The **Routing** section is used for managing static routes and checking the routing table.



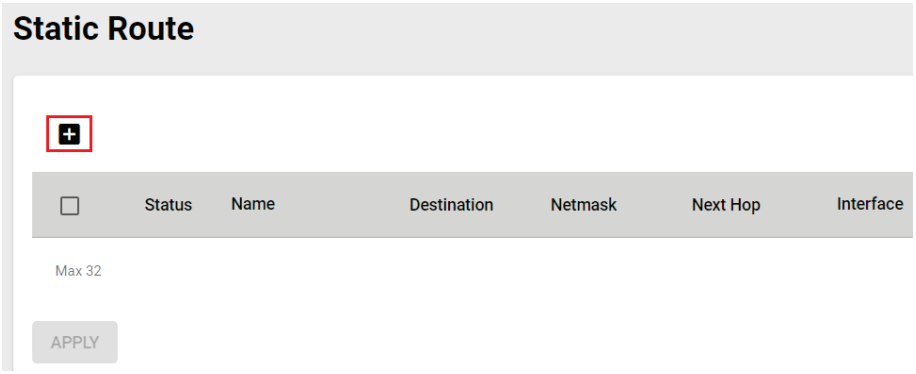
Unicast Route

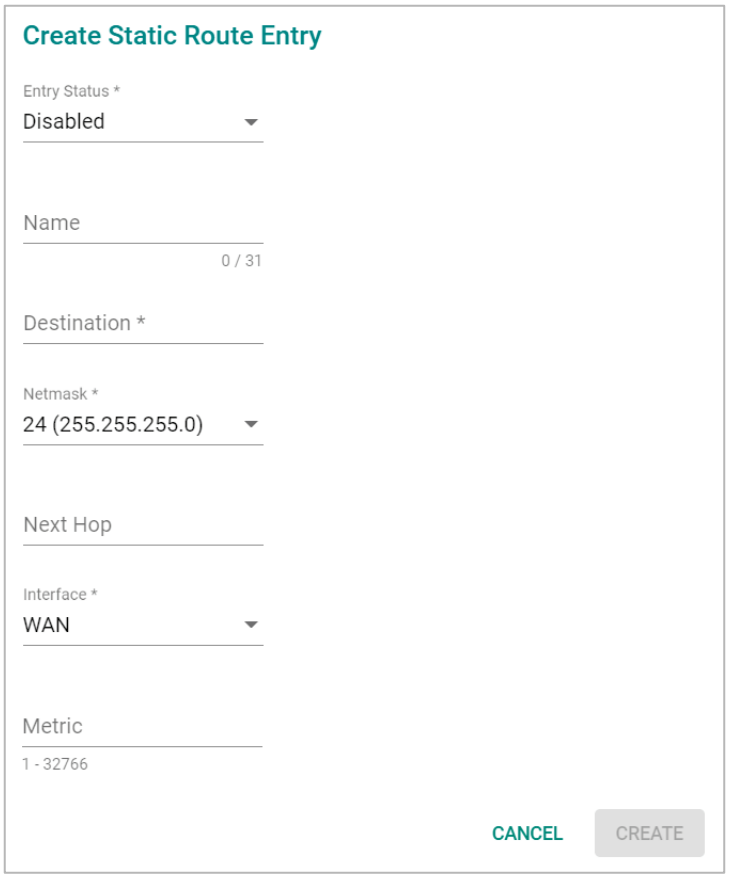
Static Route Settings

You can create, edit, and delete static route entries from the **Static Route** page. Click **Static Route** under **Routing > Unicast Route** in the function tree.

Create a New Static Route

Click the **Add** icon to create a new entry.





Configure the following settings:

Entry Status

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

Name

Setting	Description	Factory Default
0 to 31 characters	Enter a name for the static route entry.	None

Destination

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

Netmask

Setting	Description	Factory Default
IP address	Specify the subnet mask for this IP address.	24 (255.255.255.0)

Next Hop

Setting	Description	Factory Default
IP address	Specify the next gateway IP address. This IP address should be in the same subnet as the specified interface.	None

Interface

Setting	Description	Factory Default
Interface	Select the network interface for this route.	WAN

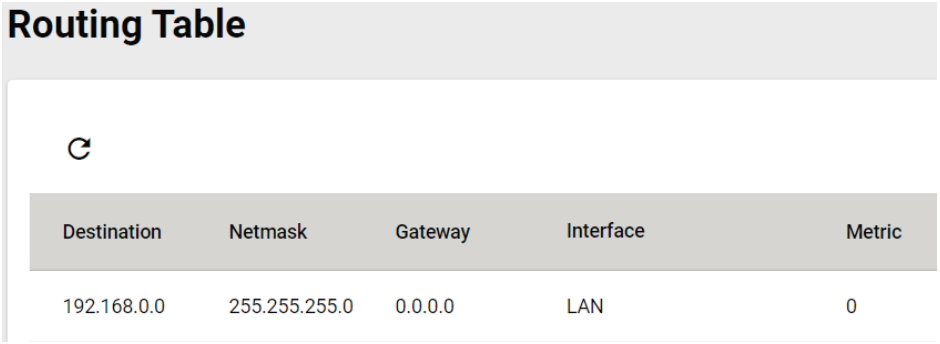
Metric

Setting	Description	Factory Default
1 to 32766	Specify the cost metric this route. Routes with a lower metric value take priority over routes with a higher cost.	None

When finished, click **CREATE**.

Routing Table

To view the current routing table, click **Routing Table** under **Routing > Unicast Route** in the function tree.

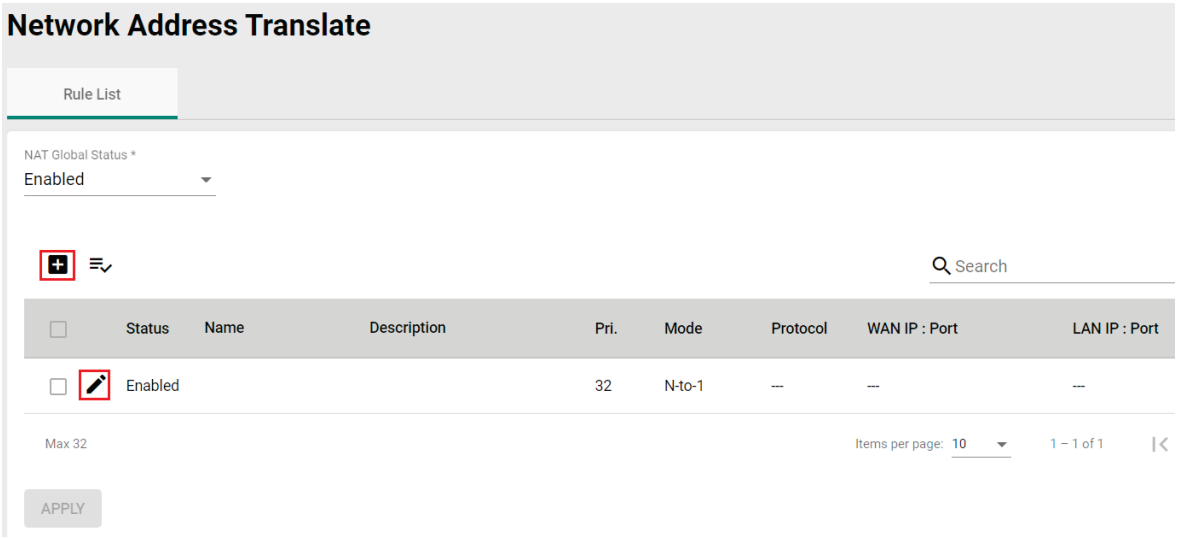


NAT

The TAP-M310R Series supports Network Address Translation (NAT) and Port Forwarding in Client-Router operation mode. This feature translates outgoing communication from private IPs to external IPs (WAN IP).

Network Address Translate

The **NAT** page lets you enable NAT functionality and manage NAT rules. Click **NAT** in the function tree.



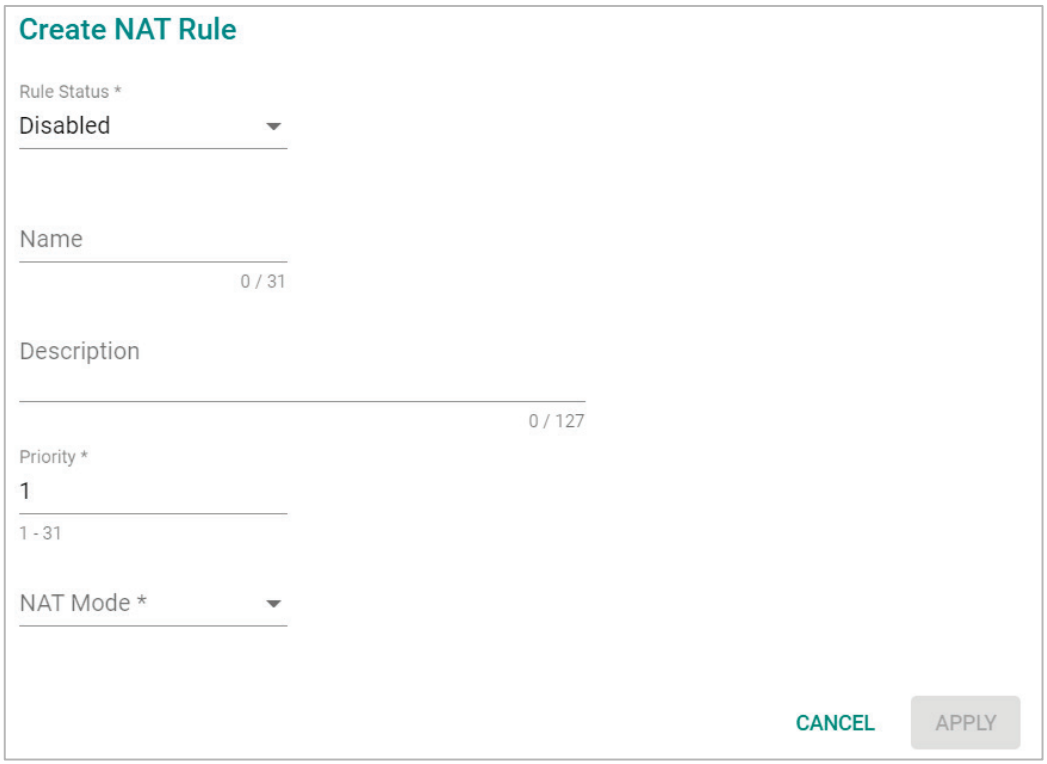
Configure the following setting:

NAT Global Status

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

Add a New NAT Rule

To add a new NAT rule, click the **Add** icon.



Configure the following settings:

Rule Status

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

Name

Setting	Description	Factory Default
0 to 31 characters	Enter a name for this rule.	None

Description

Setting	Description	Factory Default
0 to 127 characters	Enter a description for this rule.	None

Priority

Setting	Description	Factory Default
1 to 31	Specify the priority for this rule.	1

NAT Mode

Setting	Description	Factory Default
1 to 1	Set the NAT mode to 1-to-1.	None
PAT	Set the NAT mode to PAT (Port Address Translation).	

Mapping Type (1 to 1 Mode only)

Setting	Description	Factory Default
Single to Single	Set the mapping type to Single to Single.	Single to Single
Range to Range	Set the mapping type to Range to Range.	
Subnet to Subnet	Set the mapping type to Subnet to Subnet.	

Mapping Type (PAT Mode only)

Setting	Description	Factory Default
Single Port	Set the mapping type to Single Port.	Single Port
Multiple Ports	Set the mapping type to Multiple Ports.	

Protocol (PAT Mode only)

Setting	Description	Factory Default
TCP/UDP	Specify the protocol.	TCP, UDP

WAN

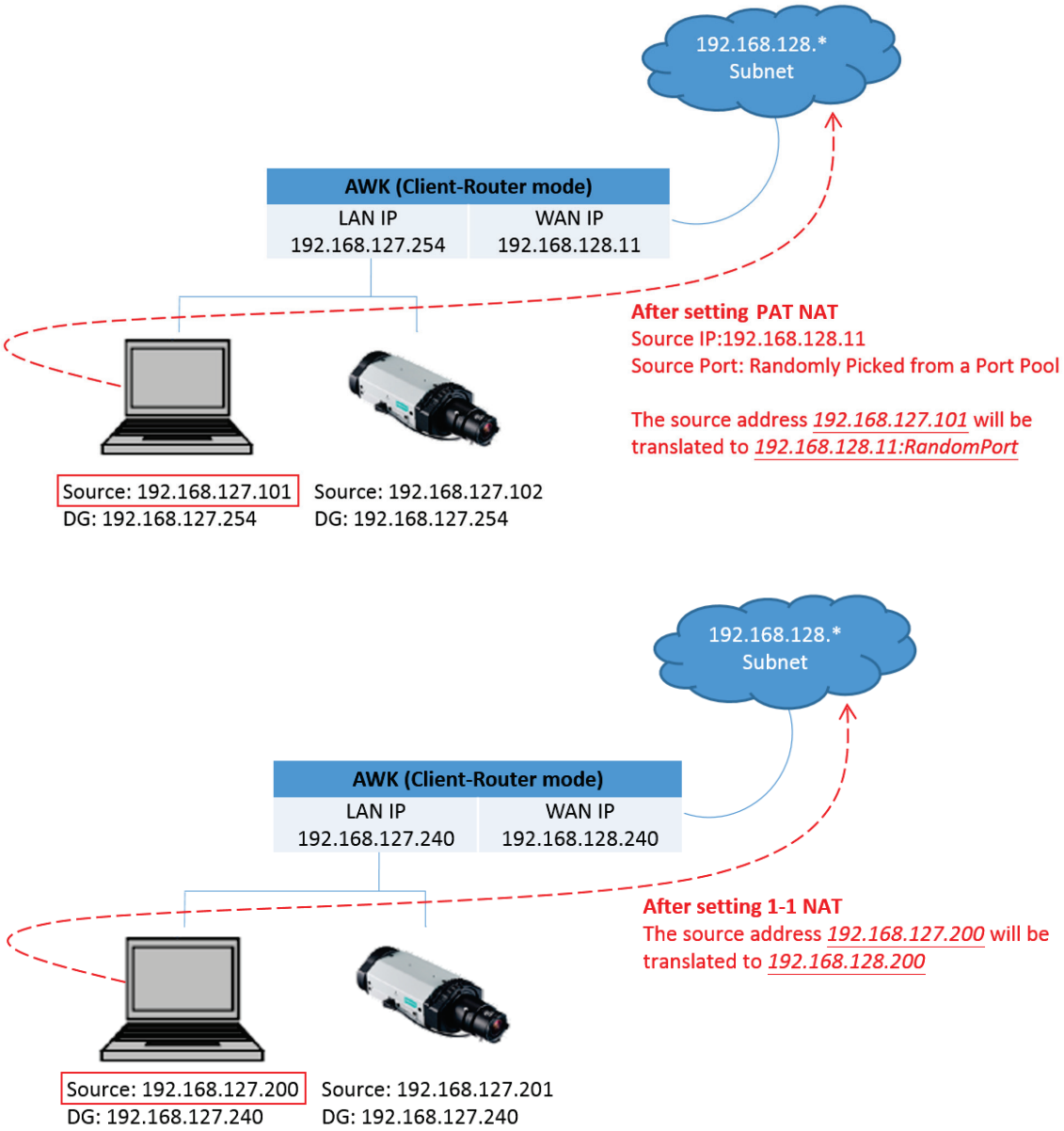
Setting	Description	Factory Default
IP address	For 1-to-1 mode only. Specify the IP address for the WAN.	None
0 to 65535	For PAT mode only. Specify the TCP or UDP port number for the WAN.	None

LAN

Setting	Description	Factory Default
IP address	Specify the LAN IP address.	None
0 to 65535	For PAT mode only. Specify the LAN TCP or UDP port number.	None

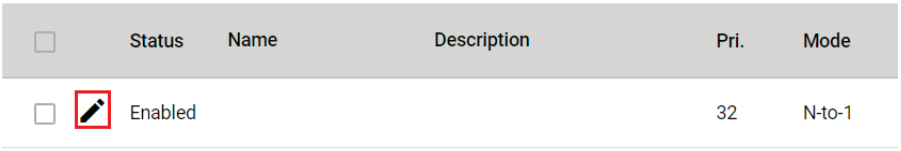
Click **APPLY** to create the new NAT rule.

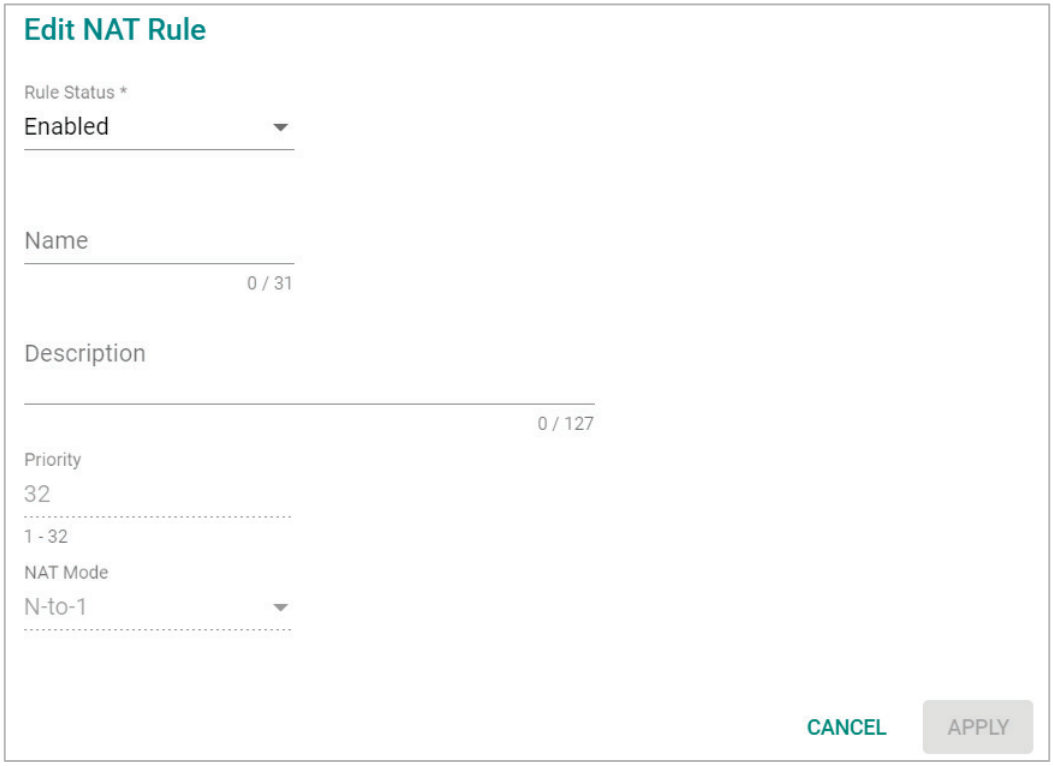
For **1 to 1 NAT Mode** and **PAT Mode**, refer to the following figure illustrations.



Edit an Existing NAT Rule

To edit an existing NAT rule, click the **Edit** icon next to the rule you want to edit.
Refer to **Create a New NAT Rule** for more information about each setting.

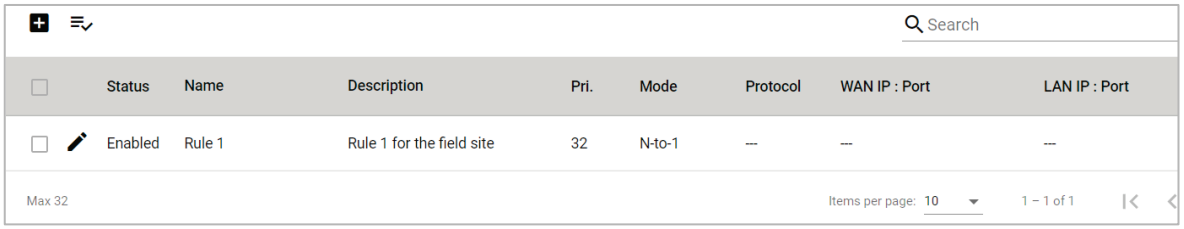




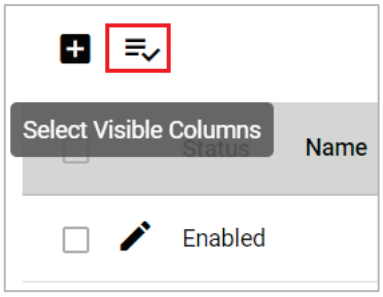
When finished, click **APPLY**.

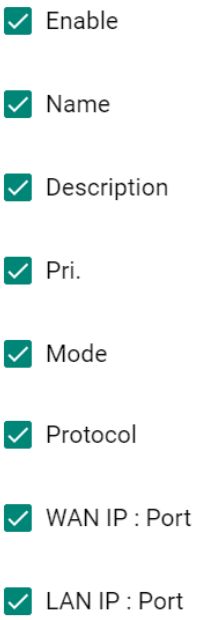
View the NAT Rule Status

You can view the status of all NAT rules from the NAT rule list page.



You select what information you want to view by clicking **Select Visible Columns** icon and checking the corresponding check boxes.

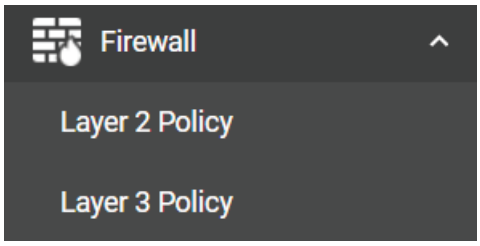




Only information for the selected items will be shown.

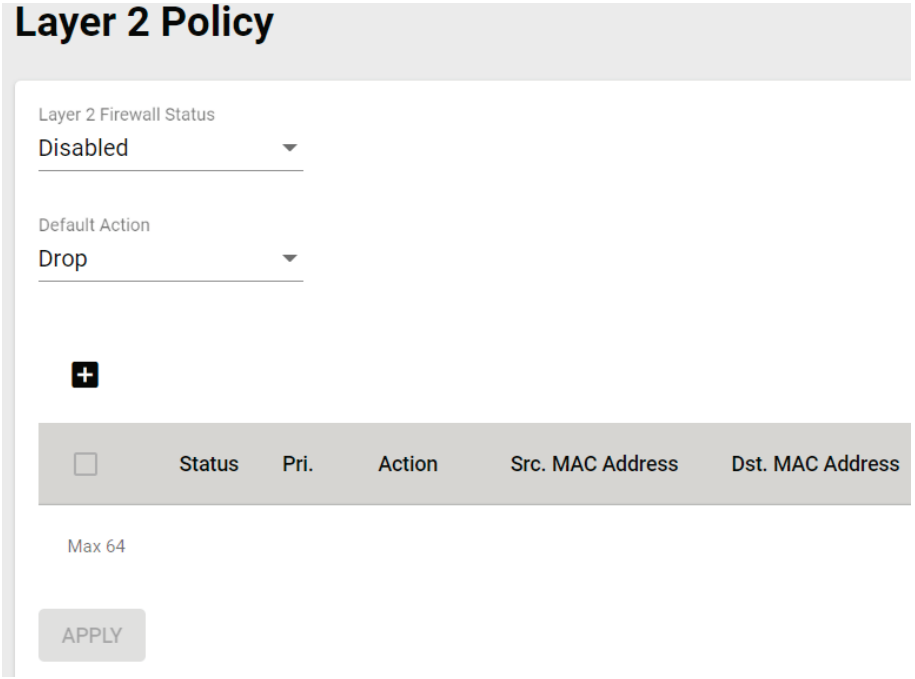
Firewall

The **Firewall** section contains the **Layer 2 Policy** and **Layer 3 Policy** configuration pages.



Layer 2 Policy

From the **Layer 2 Policy** screen, you can manage the L2 firewall policy and create, edit, and delete policy rules. Click **Layer 2 Policy** under **Firewall** in the function tree to access this screen.



Configure the following settings:

Layer 2 Firewall Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Layer 2 firewall function.	Disabled

Default Action

Setting	Description	Factory Default
Accept	Accept all packets that do not match any policy rule.	Drop
Drop	Drop all packets that do not match any policy rule.	

ATTENTION

Be careful when configuring the packet filtering function:

If the default action is set to **Drop** and **all rules are disabled, all packets will be denied**.

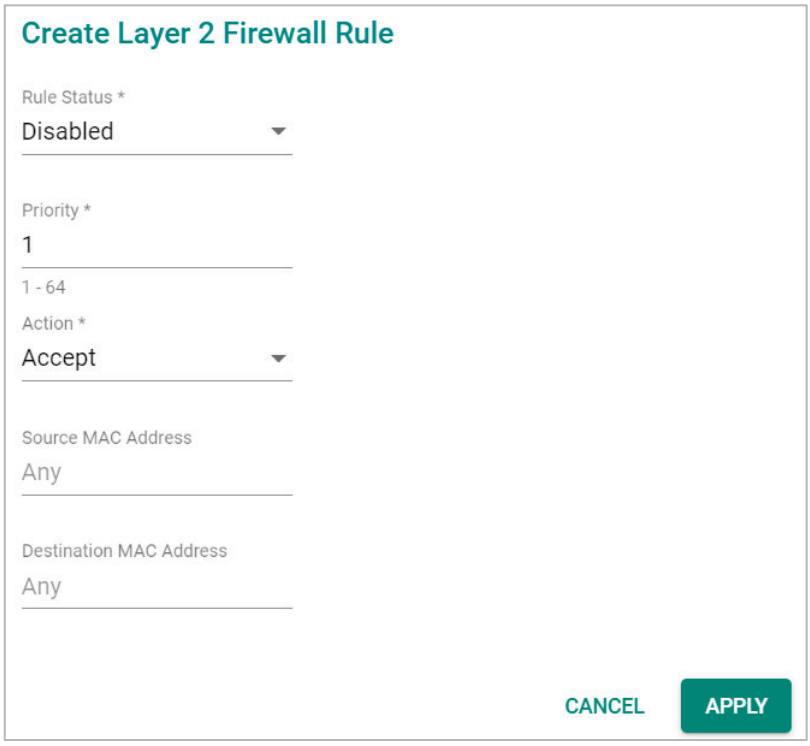
If the default action is set to **Accept** and **all rules are disabled, all packets will be allowed**.

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

Add a New Layer 2 Firewall Rule

To add a new Layer 2 firewall rule, click the **Add** icon.

Configure the following settings:



Rule Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Layer 2 firewall rule.	Disabled

Priority

Setting	Description	Factory Default
1 to 64	Specify the priority for this rule. A lower number represents a higher priority. Rules with a higher priority will be checked and enforced first.	1

Default Action

Setting	Description	Factory Default
Accept	Packets that match the policy rule will be allowed.	Accept
Drop	Packets that match the policy rule will be denied.	

ATTENTION

Be careful when configuring the packet filtering function:

If the default action is set to **Drop** and **all rules are disabled, all packets will be allowed**.

If the default action is set to **Accept** and **all rules are disabled, all packets will be denied**.

Source MAC Address

Setting	Description	Factory Default
MAC address	Enter the source MAC address.	Any

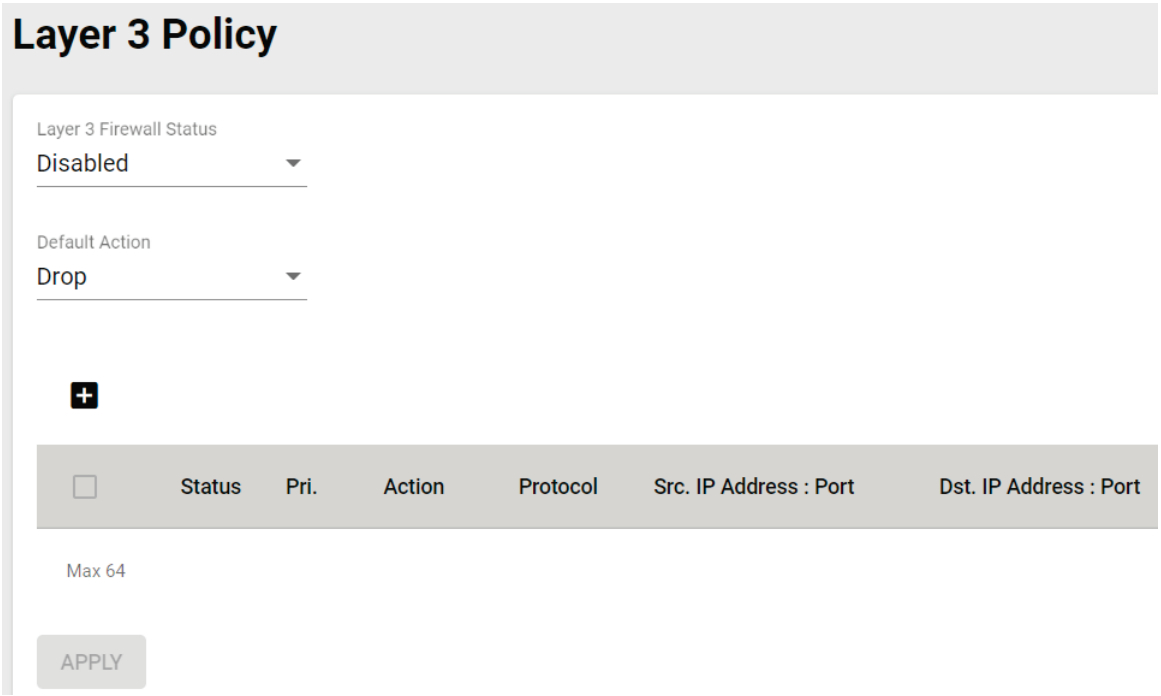
Destination MAC Address

Setting	Description	Factory Default
MAC address	Enter the destination MAC address.	Any

When finished, click **APPLY**.

Layer 3 Policy

From the **Layer 3 Policy** screen, you can manage the L3 firewall policy and create, edit, and delete policy rules. Click **Layer 3 Policy** under **Firewall** in the function tree to access this screen.



Configure the following settings:

Layer 3 Firewall Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Layer 3 firewall function.	Disabled

Default Action

Setting	Description	Factory Default
Accept	Packets that match the policy rule will be allowed.	Drop
Drop	Packets that match the policy rule will be denied.	

ATTENTION

Be careful when configuring the packet filtering function:

If the default action is set to **Drop** and **all rules are disabled, all packets will be allowed**.

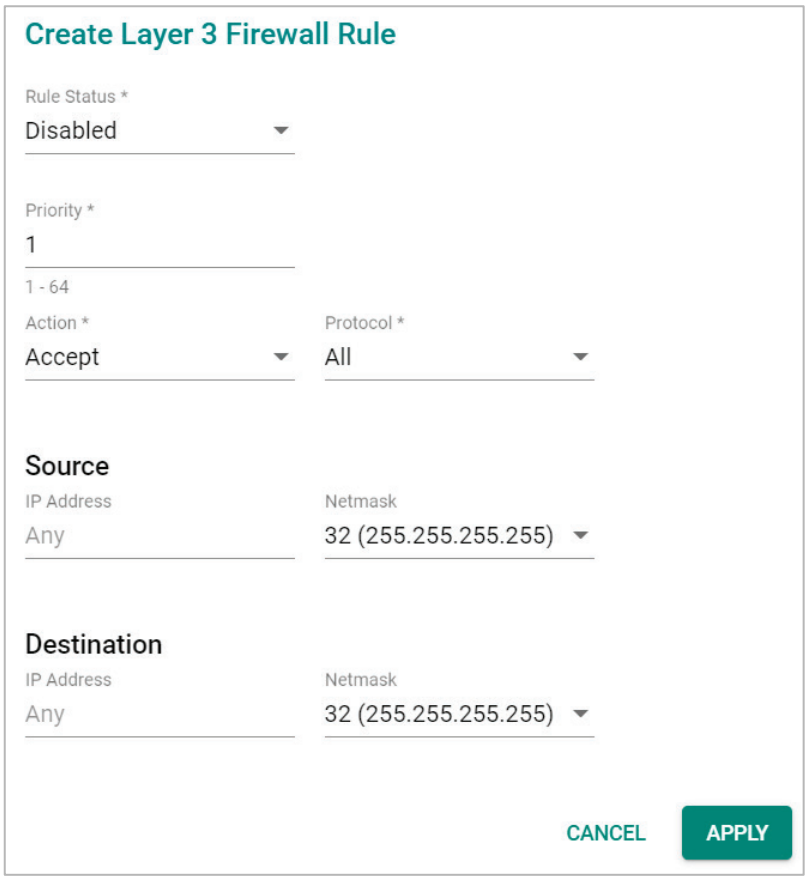
If the default action is set to **Accept** and **all rules are disabled, all packets will be denied**.

When finished, click **APPLY**.

Add a New Layer 3 Firewall Rule

To add a new Layer 3 firewall rule, click the **Add** icon.

Configure the following settings:



Rule Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Layer 3 firewall rule.	Disabled

Priority

Setting	Description	Factory Default
1 to 64	Specify the priority for this rule.	1

Default Action

Setting	Description	Factory Default
Accept	Packets that match the policy rule will be allowed.	Accept
Drop	Packets that match the policy rule will be denied.	

Protocol

Setting	Description	Factory Default
All	Filter all protocol traffic.	All
ICMP	Only filter for ICMP protocol traffic.	
TCP	Only filter for TCP protocol traffic.	
UDP	Only filter for UDP protocol traffic.	

The TAP's IP protocol filter is a policy-based filter that can allow or filter out IP-based packets with specified IP protocol and source/destination IP addresses.

The TAP provides 64 entities for setting IP protocol and source/destination IP addresses in your filtering policy. Four IP protocols are available: **All, ICMP, TCP,** and **UDP**. You must specify either the Source IP or the Destination IP. By combining IP addresses and netmasks, you can specify a single IP address or a range of IP addresses to accept or drop. For example, "IP address 192.168.1.1 and netmask 255.255.255.255" refers to the sole IP address 192.168.1.1. "IP address 192.168.1.1 and netmask 255.255.255.0" refers to the range of IP addresses from 192.168.1.1 to 192.168.255.

Source

IP Address

Setting	Description	Factory Default
IP address	Specify the source IP address.	Any

Netmask

Setting	Description	Factory Default
Netmask	Select the subnet mask	32 (255.255.255.255)

Port Range

Setting	Description	Factory Default
0 to 65535	If the Protocol is set to TCP or UDP, specify the port range.	None

Destination

IP Address

Setting	Description	Factory Default
IP address	Specify the destination IP address.	Any

Netmask

Setting	Description	Factory Default
Netmask	Specify the subnet mask.	32 (255.255.255.255)

Port Range

Setting	Description	Factory Default
0 to 65535	If the Protocol is set to TCP or UDP, specify the port range.	None

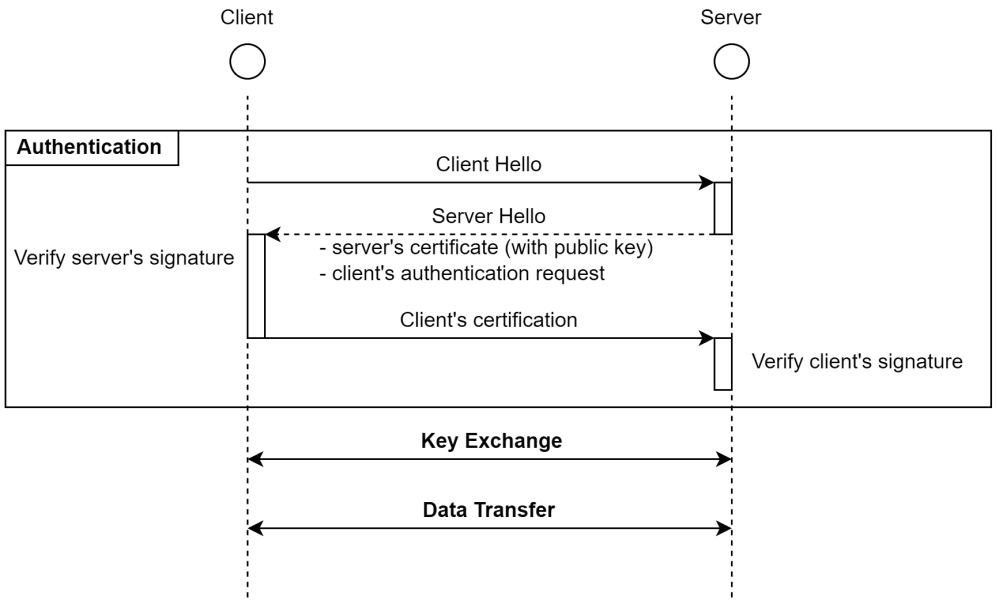
When finished, click **APPLY**.

Certificate Management

The **Certificate Management** page provides a holistic presentation of all the configuration features that support certificate-based authentication. From this dashboard table, administrators can easily review and edit device or Server CA certificates without having to navigate to the individual feature's configuration page, simplifying and speeding up certificate management tasks.

For example, administrators can update the certificate and key of Syslog Server 1 through the **Certificate Management** page, instead of having to navigate to **Diagnostics > Event Logs and Notifications > Syslog > Authentication** to perform the same task.

Basic Concept of SSL



Certificates

The **Certificates** table shows the current certificate for the listed functions. The TAP-M310R Series supports different certificates for different functions to increase security and minimize the potential risk in the event a certificate is compromised.

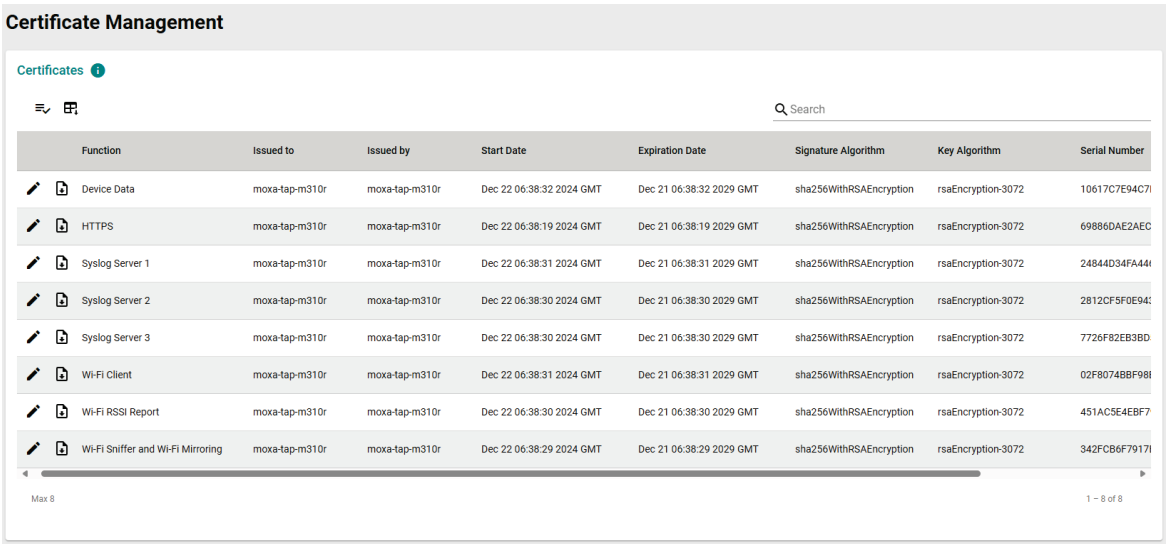
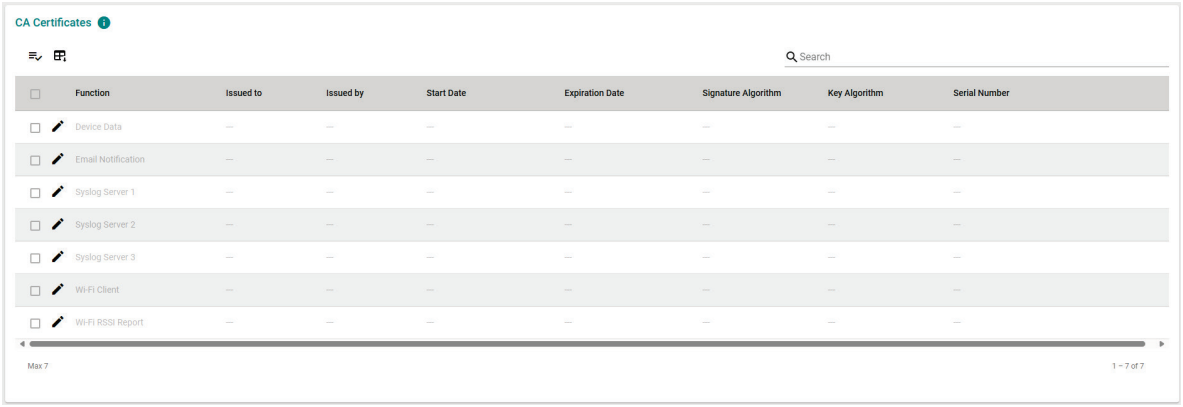


Table Field Name	Description
Function	The list of certificate-based authentication functions: Device Data HTTPS RSSI Report Syslog Server 1/2/3 Wi-Fi Client Wi-Fi Sniffer and Wi-Fi Mirroring
Issue To	The entity the certificate was issued to.
Issue By	The entity the certificate was issued by.
Start Date	The valid start date of the certificate.
Expiration Date	The expiration date of the certificate.
Signature Algorithm	The signature algorithm used by the certificate.
Key Algorithm	The key algorithm used by the certificate.
Serial Number	The unique serial number of the certificate.

By default, the certificates applied on the device are self-signed by the TAP device. It is recommended to update the self-signed certificate or upload a certificate issued by a trusted certificate authority (CA) for any functions that will be actively used.

CA Certificates

From the **CA Certificates** screen, administrators can upload third-party trusted CA certificates which are used to verify the authenticity of received server certificates during the signature verification process of the listed applications.

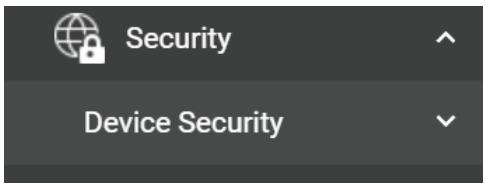


ATTENTION

The TAP-M310R Series device will automatically check and issue a warning message if the uploaded certificate has expired or was not issued by a trusted CA. Please note that the device will not automatically connect to public key infrastructure (PKI) to verify whether the uploaded certificate has been revoked or not. It is highly recommended to take additional measures to manually confirm the validity of the certificate (i.e. valid and not revoked) before uploading it to the device.

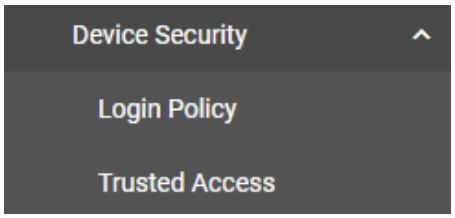
Security

The **Security** section lets you configure **Device Security** settings.



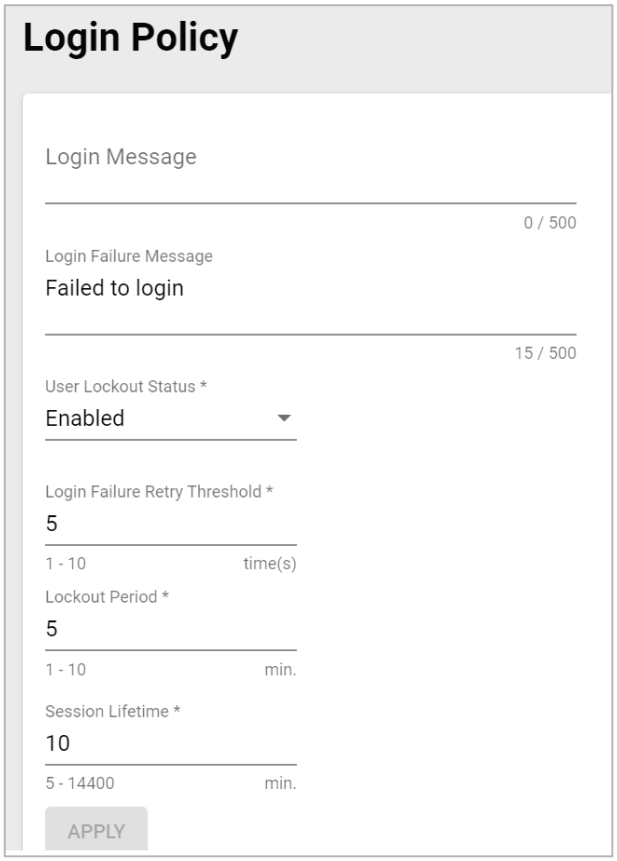
Device Security

This section describes how to configure the settings for **Login Policy** and **Trusted Access**.



Login Policy

On the **Login Policy** page, you can configure login messages and login security functions. Click **Login Policy** under **Security > Device Security** in the function tree to access this screen.



Configure the following settings:

Login Message

Setting	Description	Factory Default
0 to 500 characters	Enter the message that will be displayed on the login screen when accessing the device.	None

Login Failure Message

Setting	Description	Factory Default
0 to 500 characters	Enter the message that will be displayed when users fail to log in.	Failed to login

User Lockout Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the lockout function when a user fails to log in.	Enabled

Login Failure Retry Threshold

Setting	Description	Factory Default
1 to 10	Specify the maximum number of times a user can attempt to log in again after a failed attempt.	5

Lockout Period

Setting	Description	Factory Default
1 to 10 (min.)	Specify the duration (in minutes) the user will be unable to log in for after exceeding the number of allowed retries.	5

Session Lifetime

Setting	Description	Factory Default
5 to 1440 (min.)	Specify how long a user can be inactive for before being automatically logged out and be required to log in again.	10

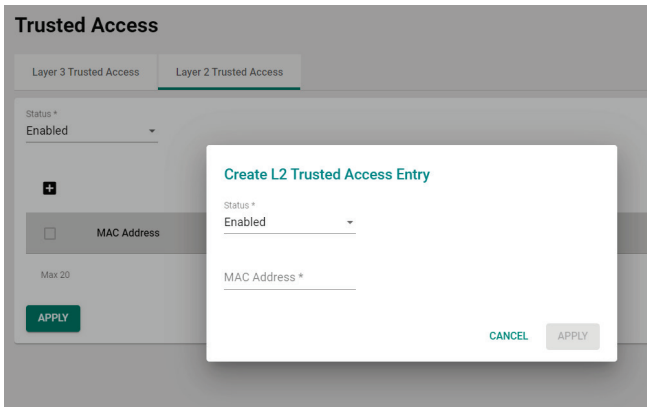
When finished, click **APPLY**.

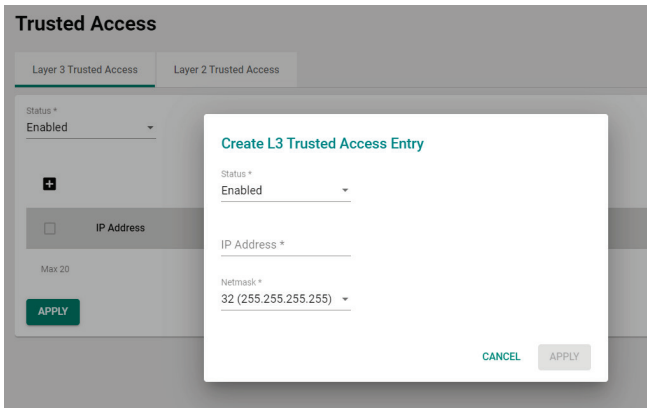
Trusted Access

In order to prevent DoS attacks, the Layer 2 and Layer 3 Trusted Access features allow authorized users to designate the MAC or IP addresses respectively that are allowed to access this device. When configured and enabled, the Trusted Access list will only allow the specified IP or MAC addresses access to the corresponding interfaces, databases, or services.

Trusted Access applies to the following interfaces, databases, and services:

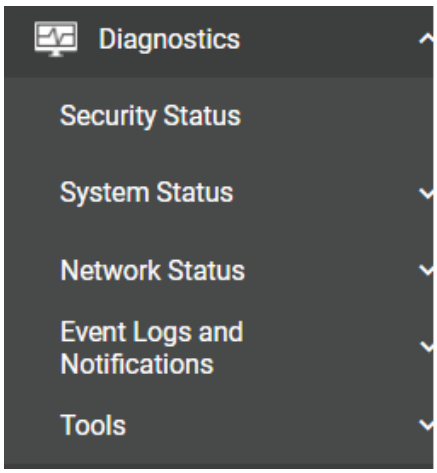
- User interfaces: HTTP/HTTPS, SSH/Telnet, SNMP, New Moxa Command.
- Event logs and notifications: Syslog, Email notifications, SNMP Trap/Inform.
- Services: DHCP Server, Wi-Fi Sniffer, Mirroring with Remote Type.





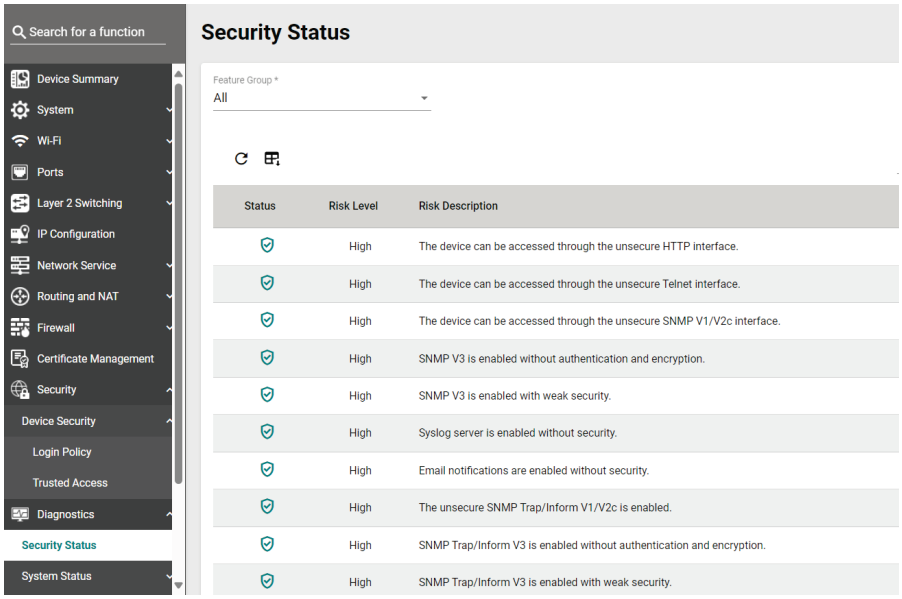
Diagnostics

The **Diagnostics** section is used for monitoring and troubleshooting and includes the **System Status, Network Status, Event Logs and Notifications**, and **Tools** pages.



Security Status

The Security Status screen consolidates the security status of all active interfaces of the device. This table serves as a review tool to ensure that the device’s configuration meets the desired IEC-62443 Security Level (SL) profile. If any of the configuration risks do not meet your organization's security policy, check the description, and navigate to the corresponding configuration page to address the issue. If the identified risk cannot be directly mitigated through the TAP-M310R Series' configuration, such as an active unsecure protocol to support legacy devices, consider consulting a qualified security expert to implement additional measures to mitigate the risk.

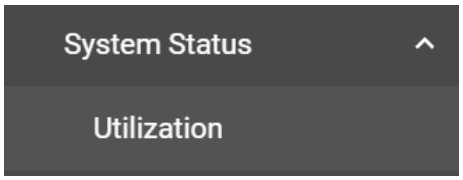


Field	Description
Status	The representative icons indicate if there are any risks that require mitigating action, and the corresponding severity of the risk. Risks that have been addressed will be marked with a checkmark.
Risk Level	The device categorizes risks into three tiers: **Low**: Risks vulnerable to exploitation per circumstances defined in SL3 and above. **Medium**: Risks vulnerable to exploitation per circumstances defined in SL2. **High**: Risks vulnerable to exploitation per circumstances defined in SL1.
Risk Description	Additional details describing the risk to provide administrators with context for taking the appropriate hardening action.

System Status

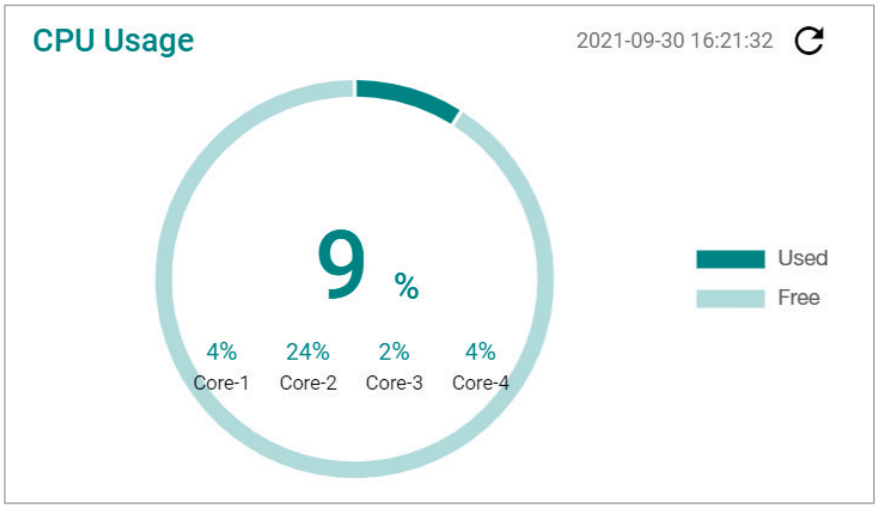
Utilization

The **Utilization** screen features widgets and charts showing the real-time resource usage of the TAP. Click **Utilization** under **Diagnostics > System** Status in the function tree to access this screen.



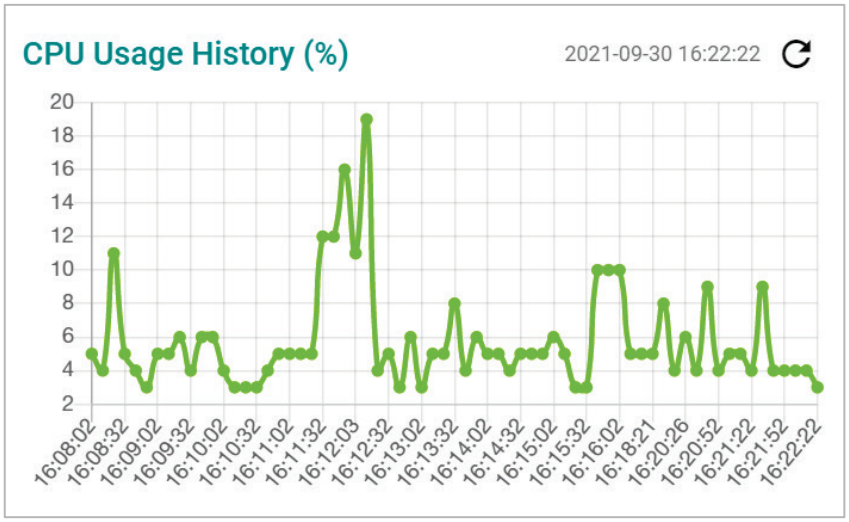
CPU Usage

This widget shows the current CPU usage.



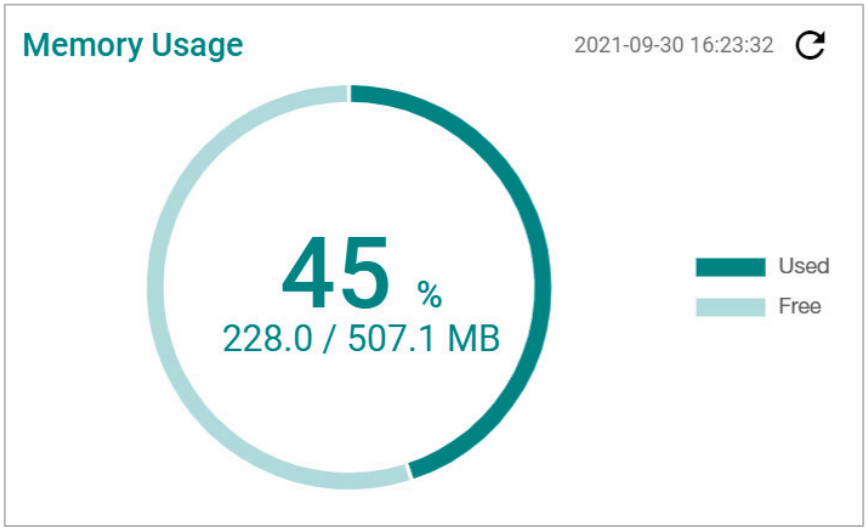
CPU Usage History

The graph shows the CPU usage history.



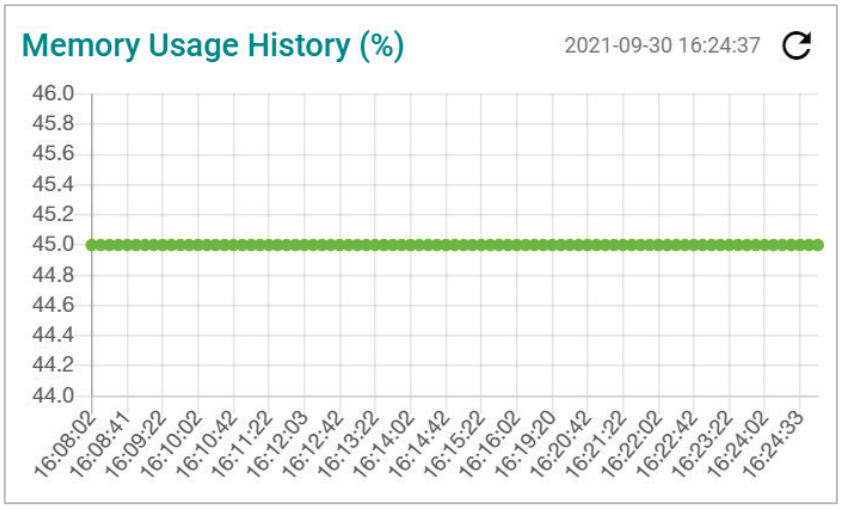
Memory Usage

This widget shows the current memory usage.



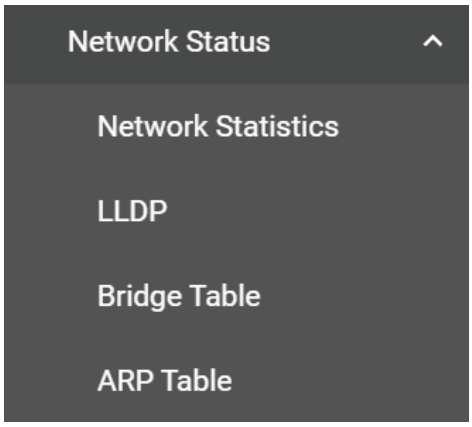
Memory Usage History

This graph shows the memory usage history.



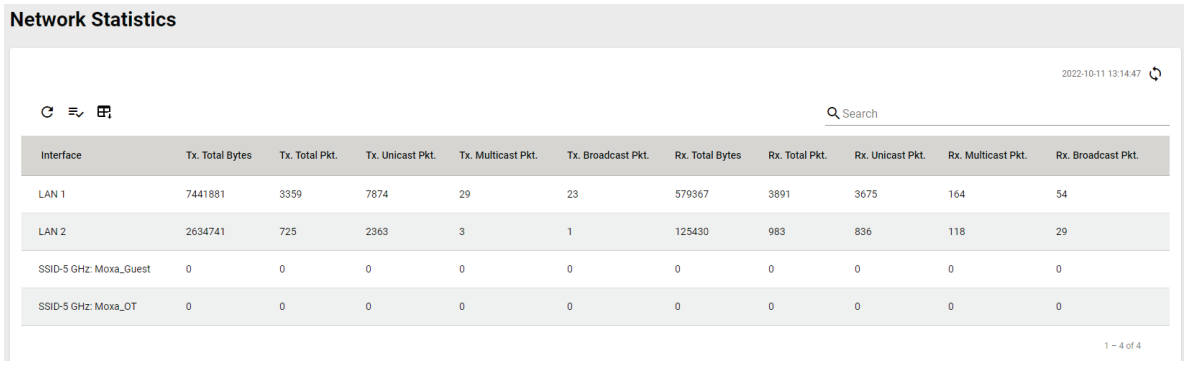
Network Status

The **Network Status** section contains the **Network Statistics, LLDP, Bridge Table,** and **ARP Table** pages.



Network Statistics

The **Network Statistics** page shows real-time data for all interfaces. Click **Network Statistic**s under **Diagnostics > Network Status** in the function tree to access this page.



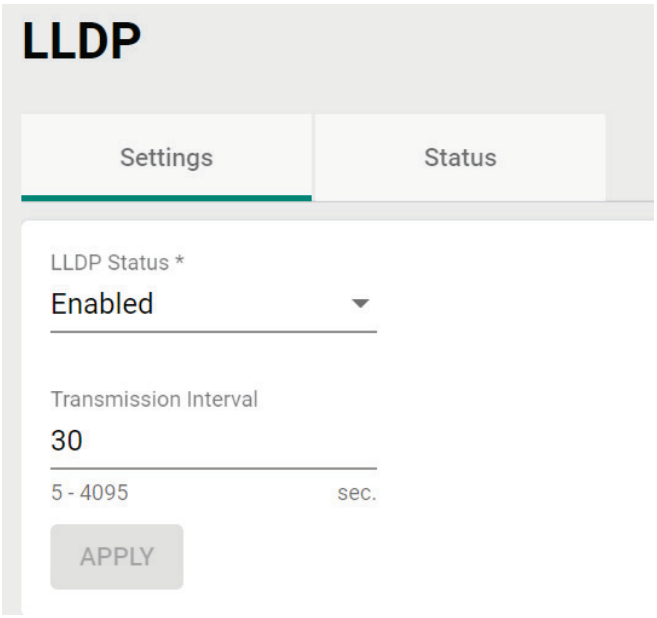
LLDP

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a Moxa managed switch or access point, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configurations. With SNMP, this information can be used to generate network visualization.

From the web interface, you can enable or disable LLDP, and set the LLDP transmit interval. In addition, you can view the neighbor-list, which is reported by its network neighbors.

LLDP Settings

Click the **Settings** tab to enable or disable LLDP and set the transmission interval.



Configure the following settings:

LLDP Status

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

Transmission Interval

Setting	Description	Factory Default
5 to 4095 (sec.)	Specify the transmission interval at which LLDP messages are sent.	30

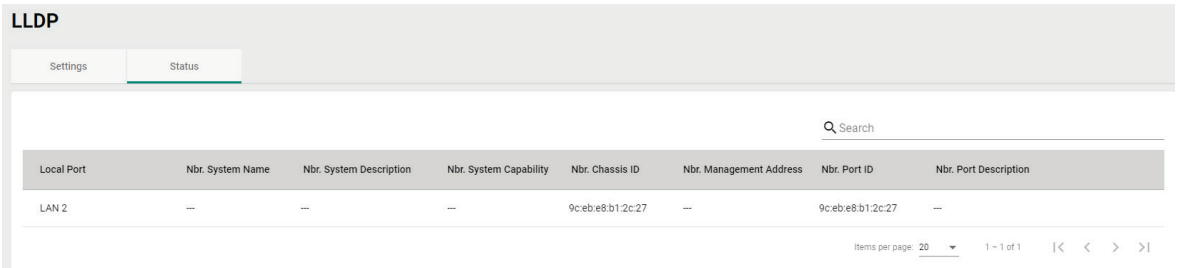
NOTE

The LLDP protocol transmits data in clear text and discloses the device model name.

When finished, click **APPLY**.

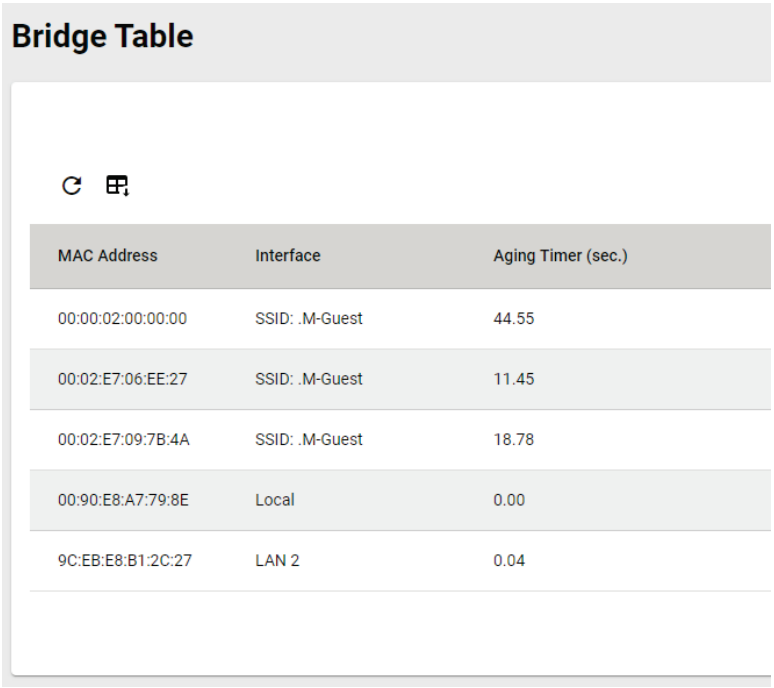
LLDP Status

Click the **Status** tab to view the LLDP status.



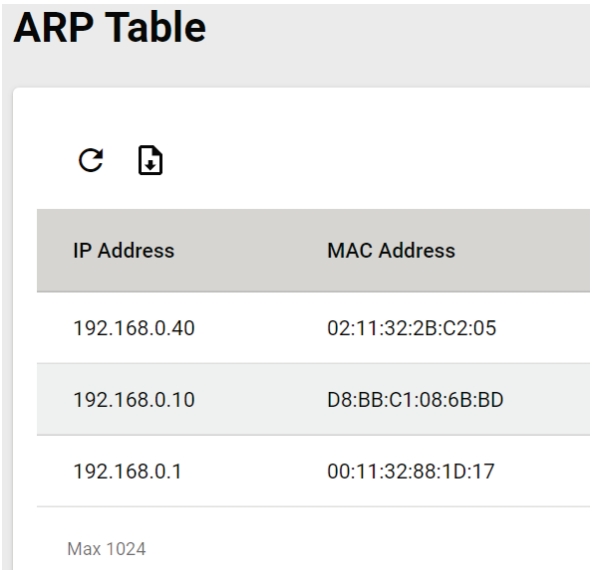
Bridge Table

The **Bridge Table** page provides more detailed bridging information. Click **Bridge Table** under **Diagnostics > Network Status** in the function tree to access this screen.



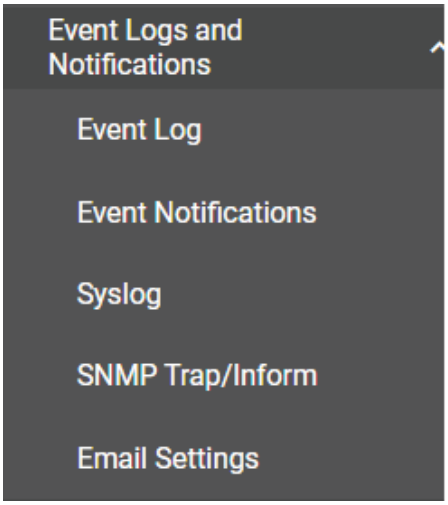
ARP Table

The **ARP Table** page shows all ARP entries. Click **ARP Table** under **Diagnostics > Network Status** in the function tree to access this screen.



Event Logs and Notifications

The **Event Logs and Notifications** section is used to configure event and notification settings and includes the **Event Log, Event Notifications, Syslog, SNMP Trap/Inform,** and **Email Settings**.

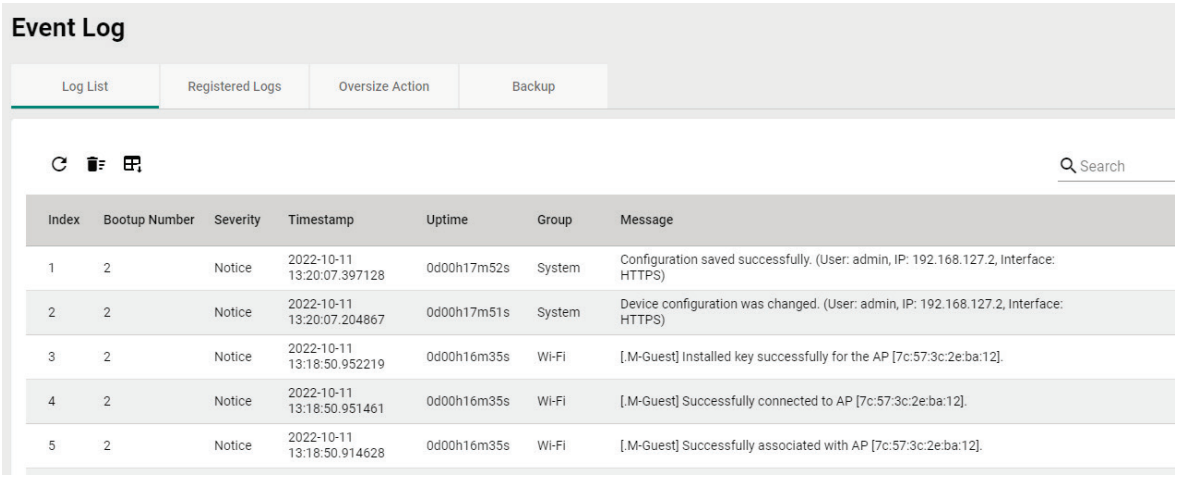


Event Log

From the **Event Log** page, you can view the current log list, configure the log oversize action, and back up the event log. Click **Event Log** under **Diagnostics > Event Logs** and Notifications in the function menu to access this page.

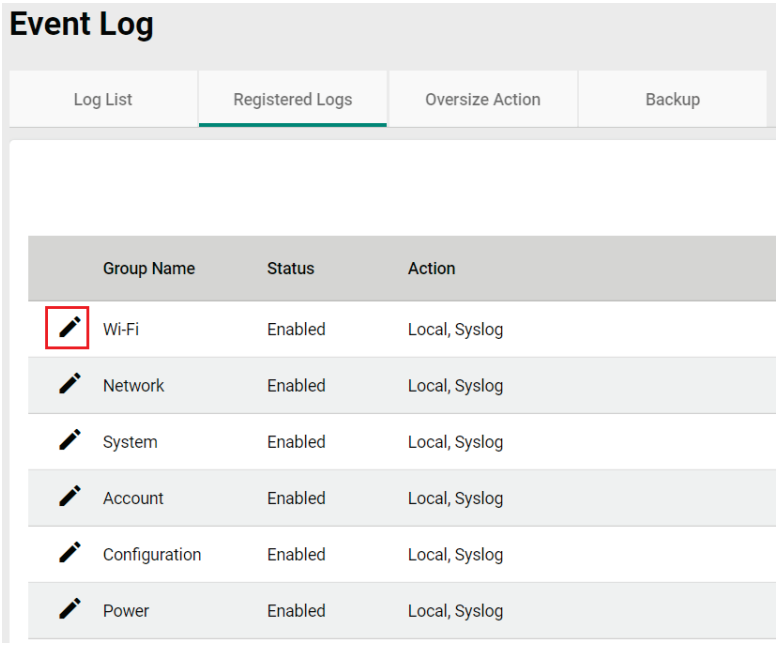
Log List

Click the **Log List** tab to view a list of all logged events.

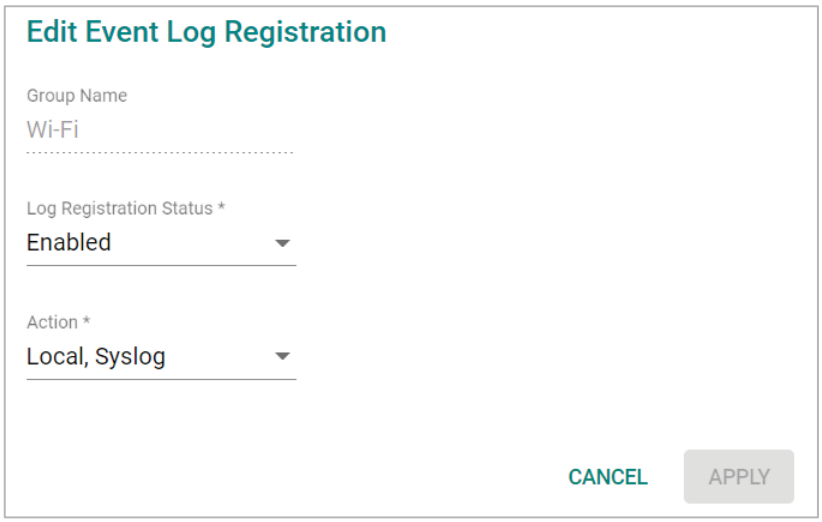


Registered Logs

Click the **Registered Logs** tab to view and edit event log groups.



To edit an event log group, click the **Edit** icon next to the group you want to edit.



Configure the following settings:

Log Registration Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the log group. If disabled, events associated with this group will not be logged.	Enabled

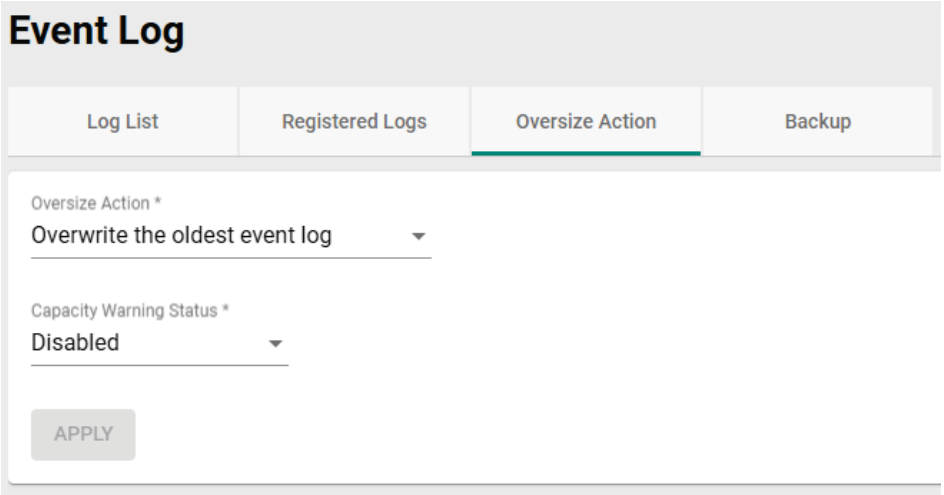
Action

Setting	Description	Factory Default
Local	Save the event logs locally.	Local, Syslog
Syslog	Send the event logs to a Syslog server.	

When finished, click **APPLY**.

Oversize Action

From the **Oversize Action** page, you can configure what happens when the log capacity has been reached. Click the **Oversize Action** tab to access this screen.



Configure the following settings:

Oversize-Action

Setting	Description	Factory Default
Overwrite the oldest event log	Overwrite the oldest event log.	Overwrite the oldest event log
Stop recording event log	Stop recording new event logs.	

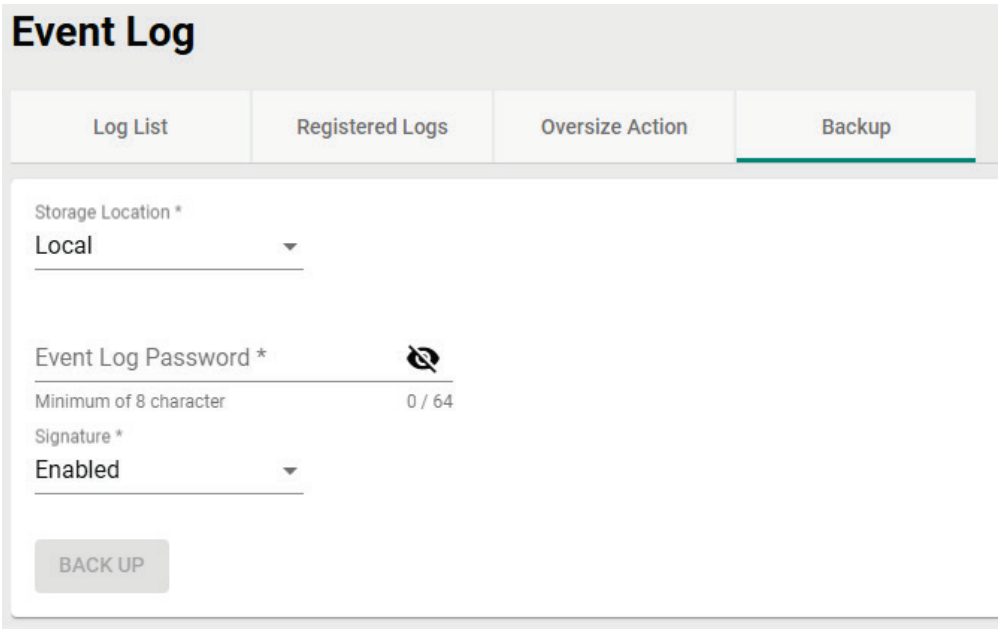
Capacity Warning

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable event log capacity warnings.	Disabled

When finished, click **APPLY**.

Backup

Click **Backup** tab to select the storage location.



Storage Location

Setting	Description	Factory Default
Local	Back up the event log to the local storage on the TAP device.	None
TFTP	Back up the event log via TFTP.	
SFTP	Back up the event log via SFTP.	

Server IP Address (for TFTP only)

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

File Name (for TFTP only)

Setting	Description	Factory Default
Input the backup file name	Enter the file name of the event log backup.	None

Server IP Address (for SFTP only)

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

Pathname (for SFTP only)

Setting	Description	Factory Default
Pathname	Specify the file path on the SFTP server for storing the event log backup.	None

Account (for SFTP only)

Setting	Description	Factory Default
Account name	Enter the SFTP server account name.	None

Password (for SFTP only)

Setting	Description	Factory Default
Password	Enter the SFTP server account password.	None

Event Log Password

Setting	Description	Factory Default
Min. 8 characters	Enter the encryption password for event log backups.	None

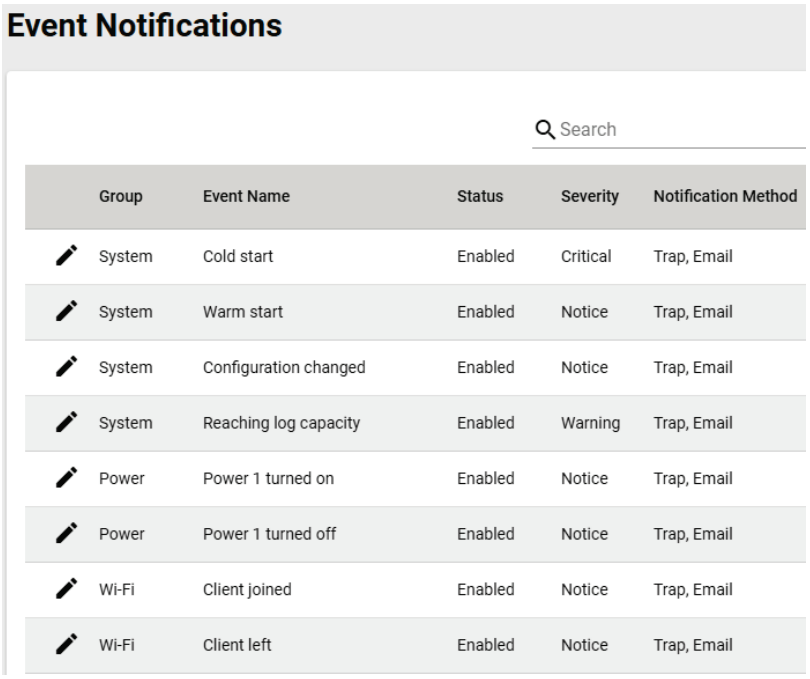
Signature

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable digital signature verification.	Enabled

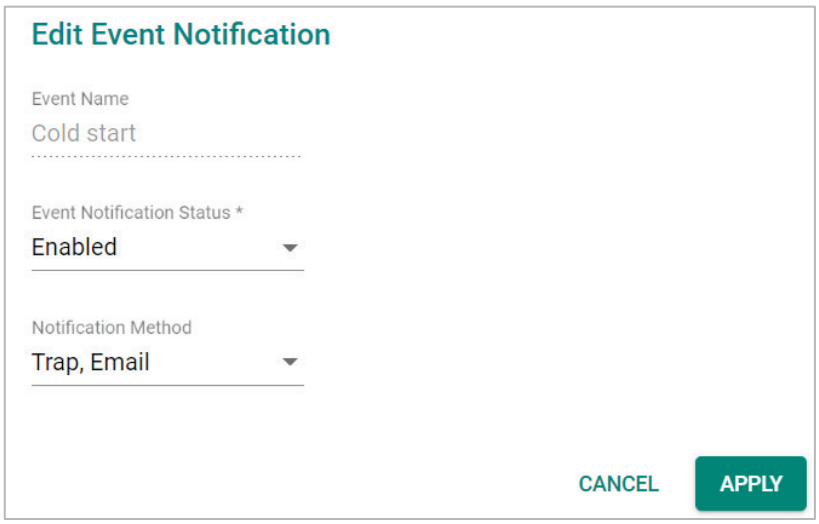
When finished, click **BACKUP**.

Event Notifications

You can configure the notification settings for individual event types. Click **Event Notifications** under **Diagnostics > Event Logs and Notifications** in the function tree to access this screen.



To edit the notification settings, click the **Edit** icon next to the event you want to edit.



Configure the following settings:

Event Notification Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable notifications for this event.	Enabled

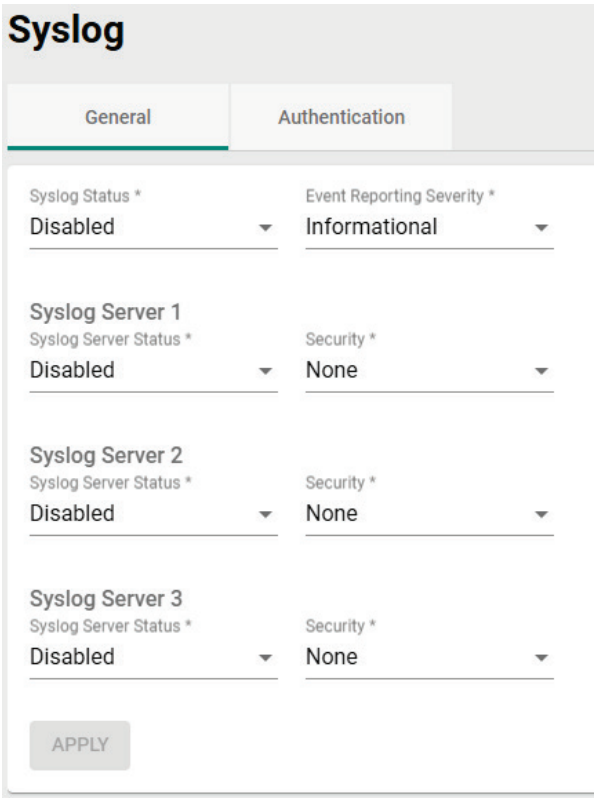
Notification Method

Setting	Description	Factory Default
Trap	Send notifications through SNMP Trap.	Trap/Email
Email	Send notifications through email.	

When finished, click **APPLY**.

Syslog

You can set up one or more Syslog servers to store event logs. Click **Syslog** under **Diagnostics > Event Logs and Notifications** in the function tree to access this screen.



Configure the following settings:

Syslog Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable logging events to a syslog server.	Disabled

Event Reporting Severity

Setting	Description	Factory Default
Emergency	Specify the syslog severity as Emergency.	Informational
Alert	Specify the syslog severity as Alert.	
Critical	Specify the syslog severity as Critical.	
Error	Specify the syslog severity as Error.	
Warning	Specify the syslog severity as Warning	
Notice	Specify the syslog severity as Notice.	
Informational	Specify the syslog severity as Informational.	

Syslog Server 1 Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the first syslog server.	Disabled

Syslog Server 2 Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the second syslog server.	Disabled

Syslog Server 3 Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the third syslog server.	Disabled

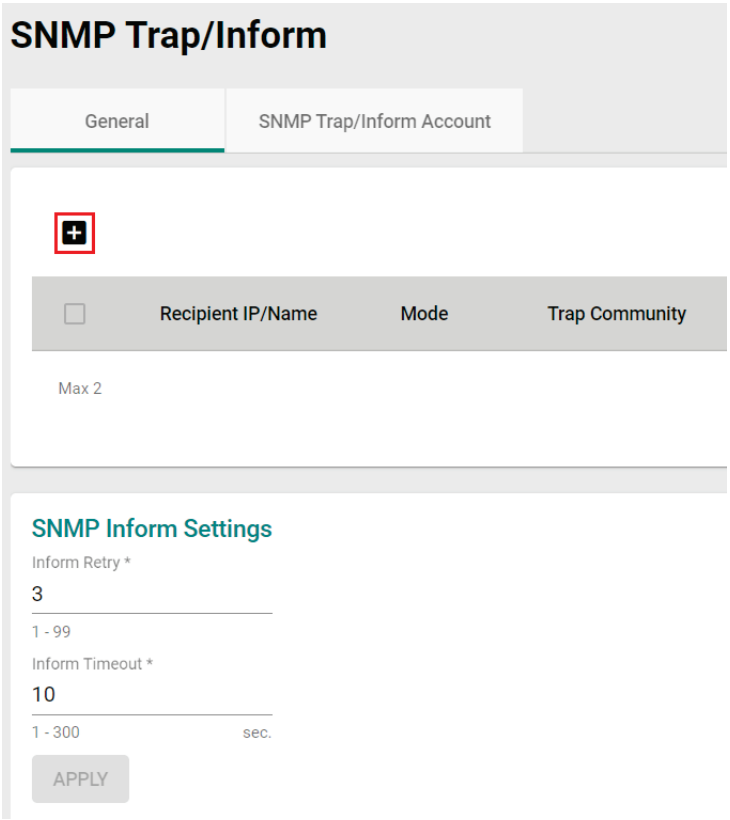
Security

Setting	Description	Factory Default
None	Do not use any security mechanism.	None
TLS	Use TLS encryption.	

When finished, click **APPLY**.

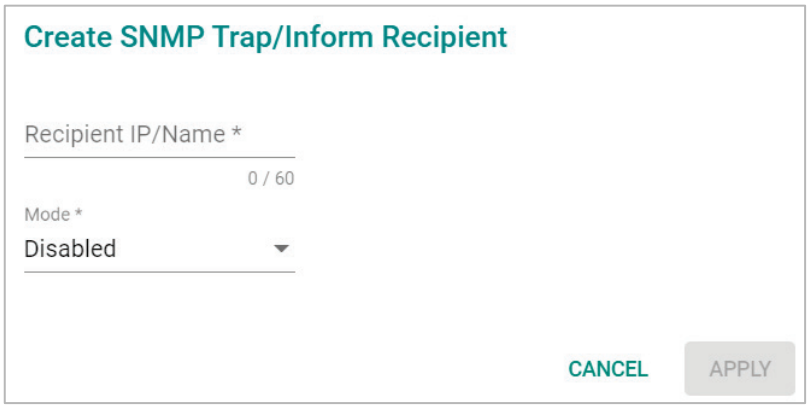
SNMP Trap/Inform

The **SNMP Trap/Inform** section is used for setting up SNMP Traps and Inform triggers for events. Click **SNM Trap/Inform** under **Diagnostics > Event Logs and Notifications** in the function tree to access this page.



General Settings

From the **General** tab, you can manage SNMP Trap/Inform recipients. Click the **General** tab to access this screen. Click the **Add** icon to create a new entry.



Configure the following settings:

Recipient IP/Name

Setting	Description	Factory Default
0 to 60 characters or IP address	Enter the name or IP of the recipient.	None

Mode

Setting	Description	Factory Default
Disabled	Disable the SNMP Trap/Inform function.	Disabled
Trap V1	Set the trap version to Trap V1.	
Trap V2c	Set the trap version to Trap v2c.	
Inform V2c	Set the inform version to Inform V2c.	
Trap V3	Set the trap version to Trap V3.	
Inform V3	Set the inform version to Inform V3.	

When finished, click **APPLY**.

SNMP Inform Settings

From the SNMP Inform Settings screen, users can make sure SNMP Inform notice packets are sent and received reliably. Users can specify the number of times the system will try to send an inform notice until receiving confirmation from the SNMP Server. Configure the following settings:

Inform Retry

Setting	Description	Factory Default
1 to 99	Specify the maximum number of Inform retries.	3

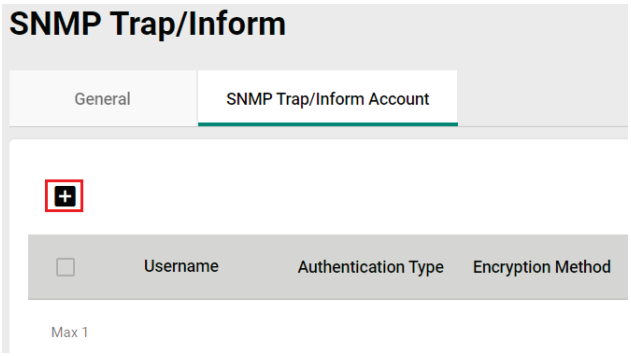
Timeout

Setting	Description	Factory Default
1 to 300	Specify the Inform timeout value.	10

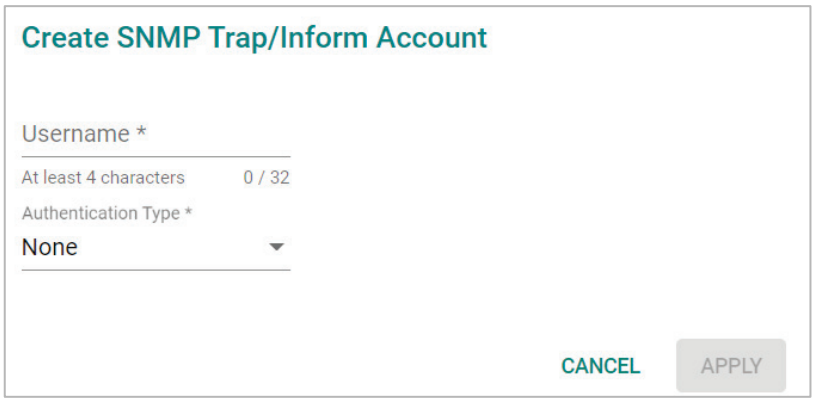
When finished, click **APPLY**.

SNMP Trap/Inform Account Settings

From the **SNMP Trap/Inform Account** tab, you can manage SNMP Trap/Inform accounts. Click the **SNMP Trap/Inform Account** tab to access this screen. Click the **Add** icon to create a new entry.



Configure the following settings:



Username

Setting	Description	Factory Default
At least 4 characters, (max. 32 characters)	Enter a username for the account.	None

Authentication type

Setting	Description	Factory Default
None	Do not use any authentication mechanism.	None
TLS	Use TLS as the authentication type.	
SHA-1	Use SHA-1 as the authentication type.	
SHA-256	Use SHA-256 as the authentication type.	
SHA-384	Use SHA-384 as the authentication type.	
SHA-512	Use SHA-512 as the authentication type.	

Authentication Password (when the Authentication type is set to MD5 or SHA)

Setting	Description	Factory Default
8 to 64 characters	Enter the authentication password.	None

Encryption Method (when the Authentication type is set to MD5 or SHA)

Setting	Description	Factory Default
None	Do not use any encryption.	None
DES	DES is the encryption method.	
AES	AES is the encryption method.	

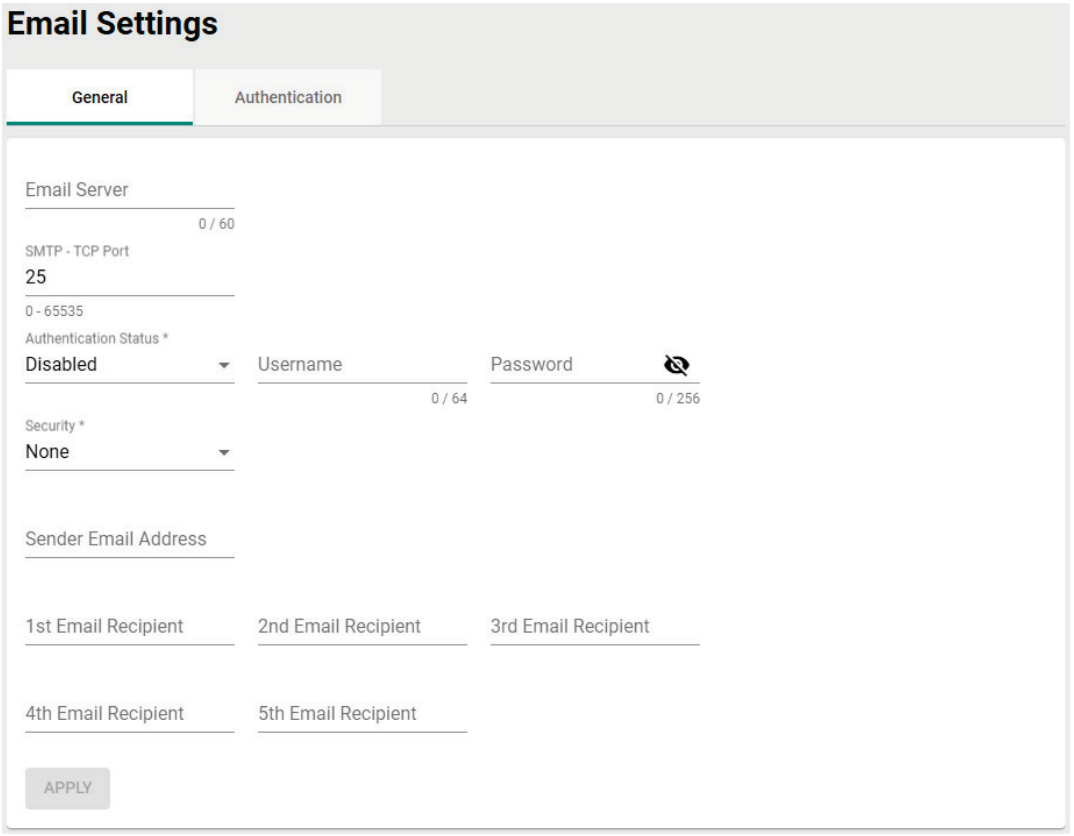
Encryption Key (when DES and AES is selected)

Setting	Description	Factory Default
8 to 64 characters	Enter the encryption key.	None

When finished, click **APPLY**.

Email Settings

The **Email Settings** page is used to configure email settings for notifications, including the email server, sender, and recipients. Click **Email Settings** under **Diagnostics > Event Logs and Notifications** in the function tree to access this screen.



Configure the following settings:

Email Server

Setting	Description	Factory Default
IP address or URL	The IP address or URL of the email server.	None

SMTP: TCP Port

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

Authentication Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable authentication for the email server.	Disabled

Username

Setting	Description	Factory Default
Max. 64 characters	Enter the email user account.	None

Password

Setting	Description	Factory Default
Max. 256 characters	Enter the email user password	None

Security

Setting	Description	Factory Default
None	Do not use any security method.	None
STARTTLS	Use STARTTLS as the security method.	
SSL/TLS	Use SSL/TLS as the security method.	

Sender Email Address

Setting	Description	Factory Default
Email address	Enter the sender's email address.	None

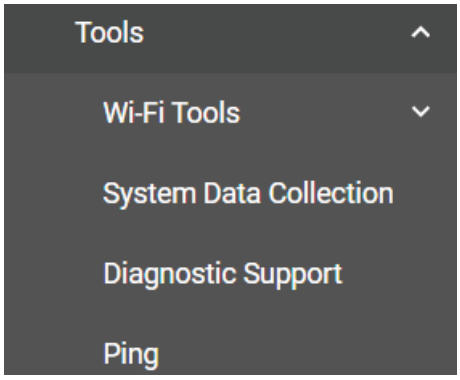
1st to 5th Email Addresses

Setting	Description	Factory Default
Email address	Enter the recipient's email address. You can set up to five recipient email addresses to receive alert emails from the TAP device.	None

When finished, click **APPLY**.

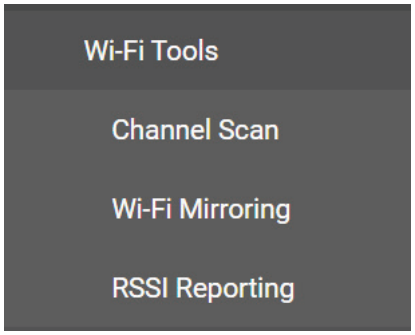
Tools

The Tools section contains several diagnostics and troubleshooting tools for the TAP, including **Wi-Fi Tools, System Data Collection, Diagnostic Support,** and **Ping**.



Wi-Fi Tools

Under **Wi-Fi Tools** are the **Channel Scan, Wi-Fi Mirroring**, and **RSSI Reporting** functions.



Channel Scan

The Channel Scan function is used to analyze the selected RF band for available channels. Click **Channel Scan** under **Diagnostics > Tools > Wi-Fi Tools** in the function tree to access this screen.

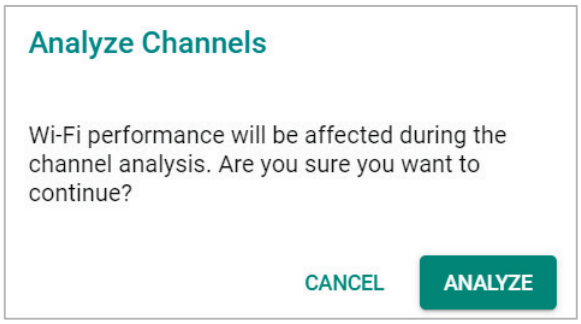
Configure the following setting:

RF Band

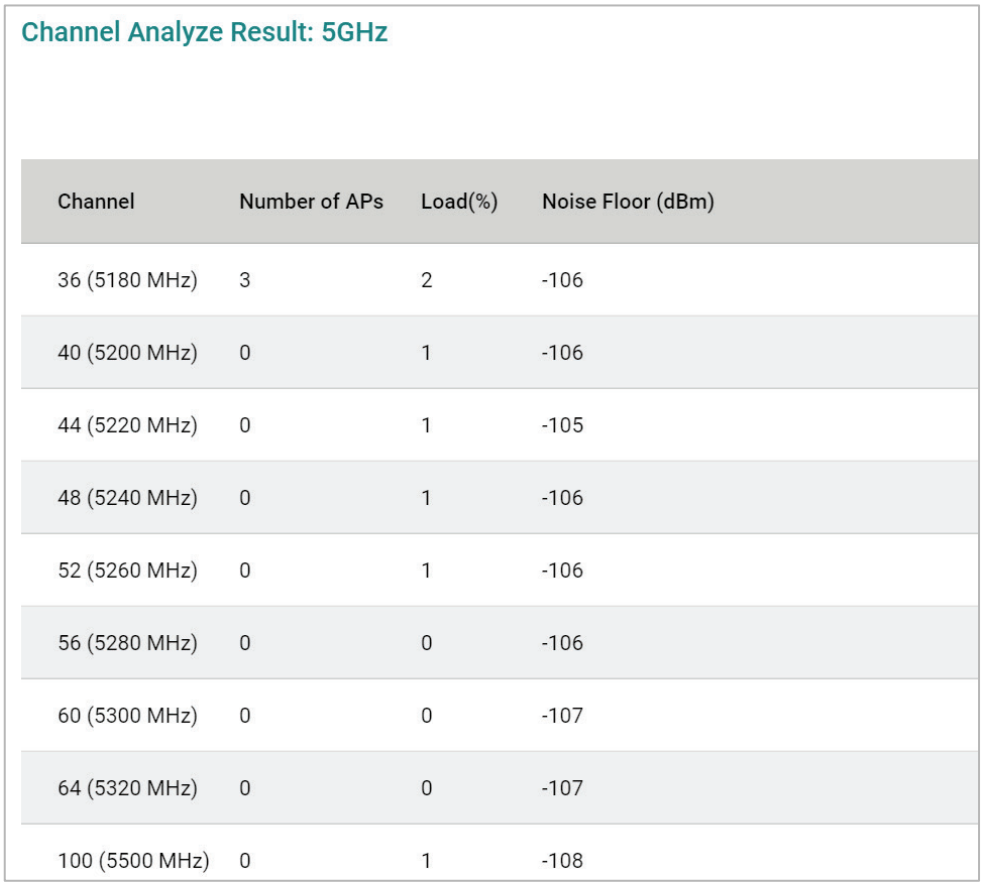
Setting	Description	Factory Default
5 GHz	Scan the 5 GHz RF band.	None
2.4 GHz	Scan the 2.4 GHz RF band.	
5 GHz & 2.4 GHz	Scan both 5 GHz and 2.4 GHz RF bands.	

When finished, click **ANALYZE**.

When prompted, click **ANALYZE** again.



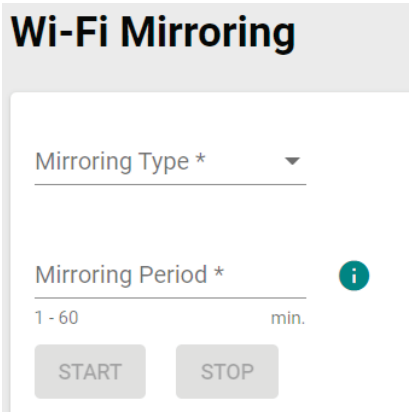
The result of the scan will be shown in the table at the bottom of the page. The Load(%) metric indicates the time the channel was used (in percentage) during the scan. The scan duration is approximately 330 ms for each channel.



Channel	Number of APs	Load(%)	Noise Floor (dBm)
36 (5180 MHz)	3	2	-106
40 (5200 MHz)	0	1	-106
44 (5220 MHz)	0	1	-105
48 (5240 MHz)	0	1	-106
52 (5260 MHz)	0	1	-106
56 (5280 MHz)	0	0	-106
60 (5300 MHz)	0	0	-107
64 (5320 MHz)	0	0	-107
100 (5500 MHz)	0	1	-108

Wi-Fi Mirroring

Wi-Fi Mirroring lets you copy the traffic of wireless traffic for analysis and troubleshooting purposes. Click **Wi-Fi Mirroring** under **Diagnostics > Tools > Wi-Fi Tools** in the function tree to access this screen.



Configure the following settings:

Mirroring Type

Setting	Description	Factory Default
Local	Select Local to mirror traffic to the local storage on the device.	None
Remote	Select Remote to have the TAP act as a server to be used with a capturing tool such as Wireshark to capture the mirror traffic.	

Mirroring Period (Local Type only)

Setting	Description	Factory Default
1 to 60 (min.)	Specify how long the device will mirror wireless traffic.	None

When finished, click **START** to start mirroring, and **STOP** to stop mirroring.

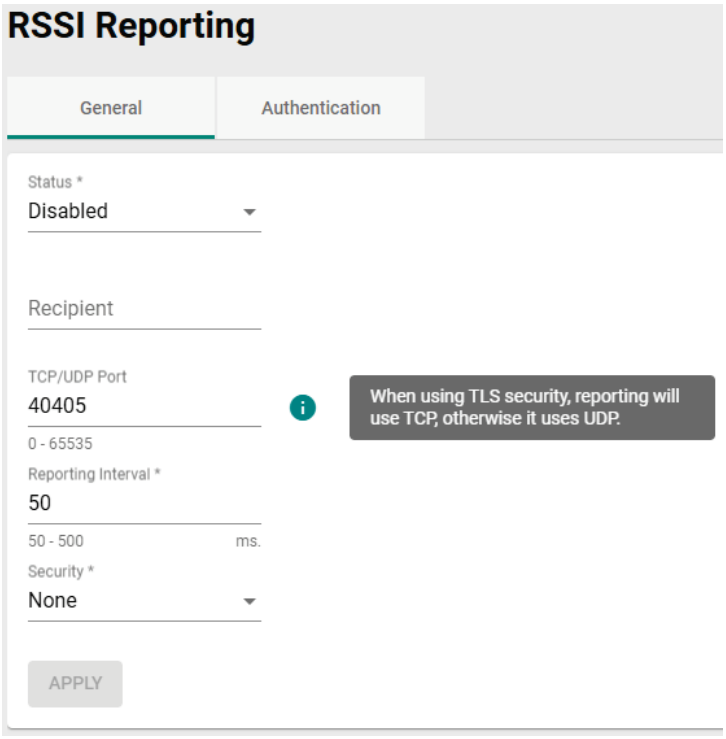
The result of the mirroring will be shown below. If you selected Local as the mirroring type, click **DOWNLOAD** to download the result to your local machine.

RSSI Reporting

RSSI Reporting sends out the AP's SNR or detected Signal Strength over Syslog to a designated recipient host for monitoring. This data is used to analyze if the configured Turbo Roaming Threshold and Roaming Difference values are suitable for the current network environment. Click **RSSI Reporting** under **Diagnostics > Tools > Wi-Fi Tools** in the function tree to access this screen.

General

From the **General** tab, you can enable or disable RSSI Reporting and configure basic settings.



Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable RSSI Reporting.	Disabled

Recipient

Setting	Description	Factory Default
Host IP/Domain name	Specify the Syslog server host IP or domain name that will receive the RSSI report data.	Empty

TCP/UDP Port

Setting	Description	Factory Default
0 to 65535	Specify the designated Syslog server communication port to receive the RSSI report data on.	40405

Reporting Interval

Setting	Description	Factory Default
50 to 500 ms	Specify the interval (in ms) at which RSSI report data is generated and sent to the Syslog server.	50

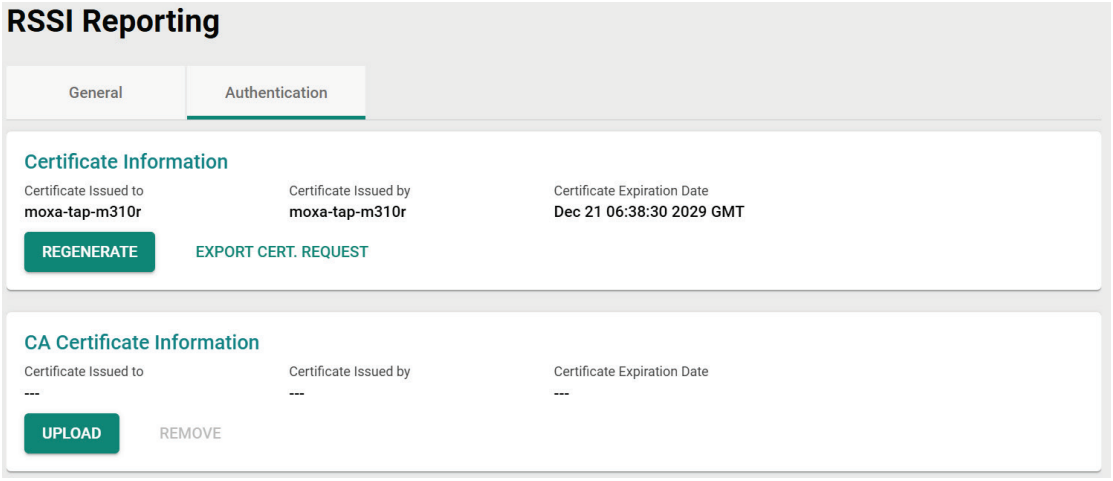
Security

Setting	Description	Factory Default
None/TLS	Specify whether the generated RSSI report data needs to be TLS encrypted or not.	None

When finished, click **APPLY**.

Authentication

From the **Authentication** tab, you can check and modify the RSSI reporting certificate and CA certificates.



To export the certificate request, click **EXPORT CERT. REQUEST**. This will download the certificate request file to the local host.

To regenerate the certificate, click **REGENERATE**. The **Install Device Certificate and Key** window will appear.

Available options depend on the selected method:

Method

Setting	Description	Factory Default
Self-signed	Regenerate a self-signed certificate.	Self-signed
Upload	Upload a local certificate and key file.	

If you selected **Self-signed**, click **REGENERATE**.

If you selected **Upload**, configure the following options:

Certificate

Setting	Description	Factory Default
Certificate file	Navigate to the certificate file on the local host to upload.	None

Method

Setting	Description	Factory Default
Key file	Navigate to the certificate key file on the local host to upload.	None

With the files selected, click **Upload**.

To upload the Server CA certificate, click **UPLOAD**. The **Upload Server CA Certificate** window will appear.

CA Certificate

Setting	Description	Factory Default
Certificate file	Navigate to the certificate file on the local host to upload.	None

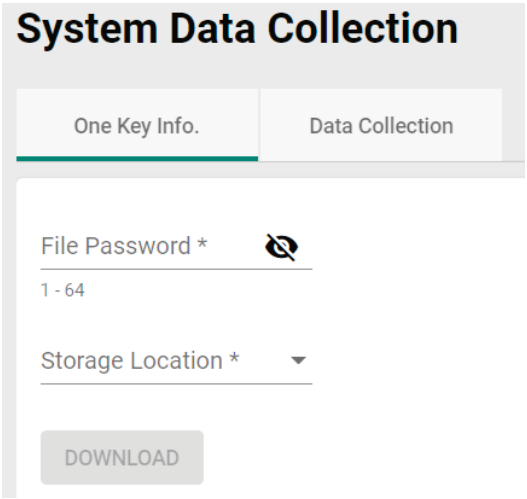
With the file selected, click **Upload**.

System Data Collection

The **System Data Collection** section contains the **One Key Information** and **Data Collection** functions.

Download One Key Information

Using the **One Key Info** function, all running configuration files, event logs, and CLI status will be saved as a compressed ZIP file and stored on the selected medium. Click the **One Key Info**. tab to access this screen.



Configure the following settings:

File Password

Setting	Description	Factory Default
1 to 64 characters	Enter the password for the file. This password will be required to open the compressed file.	None

Storage Location

Setting	Description	Factory Default
Local	The file will be downloaded to the local storage on the TAP.	None
TFTP	The file will be downloaded to a TFTP server.	
SFTP	The file will be downloaded to an SFTP server.	

Server IP Address (for TFTP only)

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

Server IP Address (for SFTP only)

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

Server Account (for SFTP only)

Setting	Description	Factory Default
Account name	Enter the account name of the SFTP server.	None

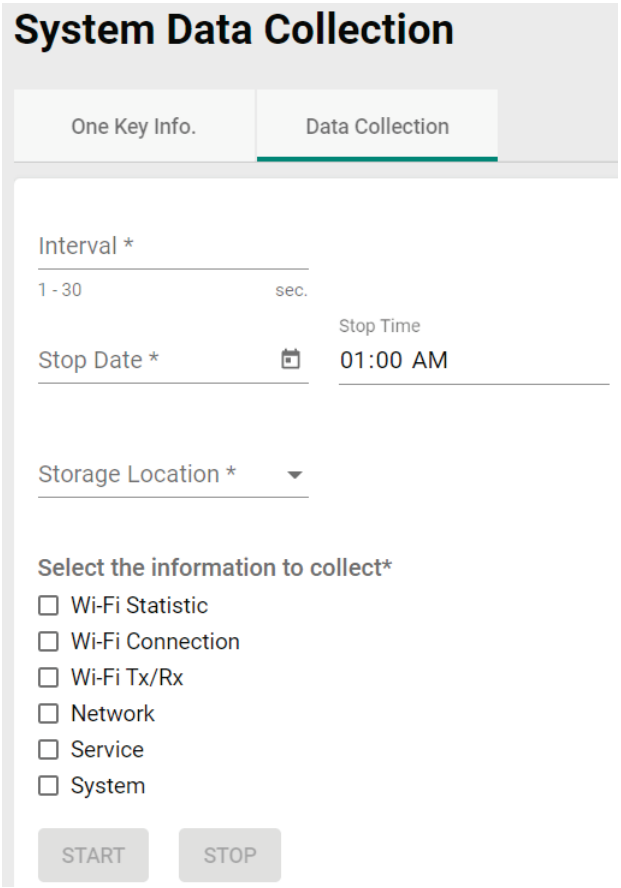
Server Password (for SFTP only)

Setting	Description	Factory Default
Account password	Enter the account password of the SFTP server.	None

When finished, click **DOWNLOAD** to download the file.

Data Collection

The **Data Collection** function is used to gather selected system information at specific intervals. Click the **Data Collection** tab to access this screen.



Configure the following settings:

Interval

Setting	Description	Factory Default
1 to 30 (sec.)	Specify the interval at which the TAP will collect information.	None

Stop Date

Setting	Description	Factory Default
Date	Specify the date the device will stop collecting information.	None

Stop Time

Setting	Description	Factory Default
Time	Specify the time the device will stop collecting information.	01:00 AM

Storage Location

Setting	Description	Factory Default
Local	The file will be downloaded to the local storage on the TAP.	None
TFTP	The file will be downloaded to a TFTP server.	
SFTP	The file will be downloaded to an SFTP server.	

Server IP Address (for TFTP only)

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

Server IP Address (for SFTP only)

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

Server Account (for SFTP only)

Setting	Description	Factory Default
Account name	Enter the account name of the SFTP server.	None

Server Password (for SFTP only)

Setting	Description	Factory Default
Account password	Enter the account password of the SFTP server.	None

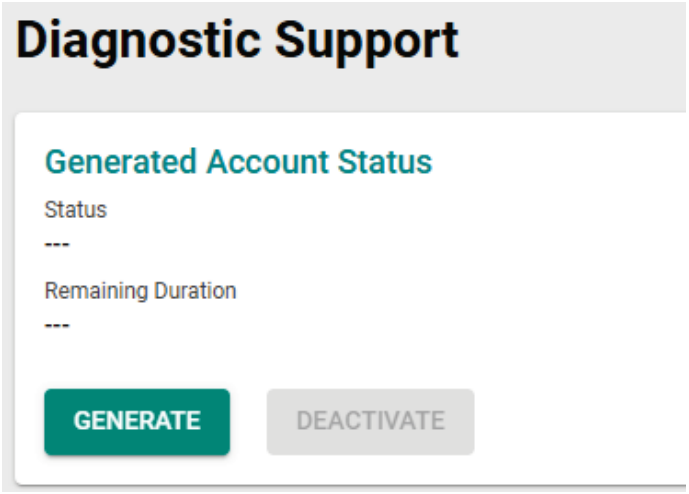
Select the information to collect

Setting	Description	Factory Default
Wi-Fi Statistic	Select the types of information you want to collect.	None
Wi-Fi Connection		
Wi-Fi Tx/Rx		
Network		
Service		
System		

When finished, click **START** to begin collecting information, and **STOP** to end.

Diagnostic Support

This feature allows an authorized user to generate an engineering account for Moxa support staff to access and troubleshoot the TAP-M310R Series. Click **Diagnostic Support** under **Diagnostics > Tools** in the function tree to access this screen.



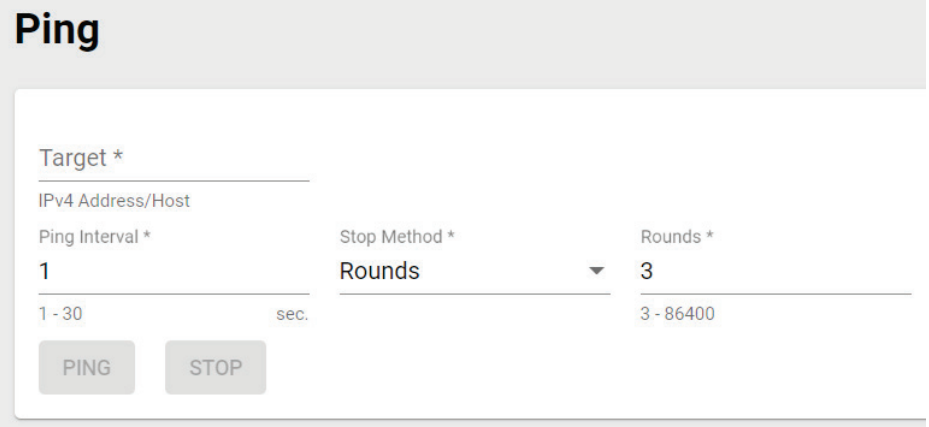
You can check the account status at any time in the bottom section of the screen. Click **DEACTIVATE** to immediately terminate a generated diagnostics account.

NOTE

Only provide generated diagnostics account credentials to authorized Moxa support personnel.

Ping

The **Ping** function is used to check the connection to a remote host. Click **Ping** under **Diagnostics > Tools** in the function tree to access this screen.



Configure the following settings:

Target

Setting	Description	Factory Default
IP address/hostname	Enter the IP address or hostname you want to ping.	None

Ping Interval

Setting	Description	Factory Default
1 to 30 (sec.)	Specify the interval at which the TAP will ping the host.	1

Stop Method

Setting	Description	Factory Default
Rounds	Specify Rounds as the stop method.	Rounds
Timestamps	Specify Timestamps as the stop method.	

Rounds (for Rounds Method only)

Setting	Description	Factory Default
3 to 86400	Specify the round value.	3

End Date (for Timestamps Method only)

Setting	Description	Factory Default
Date	Specify the date when to stop pinging the IP address or hostname.	None

End Time (for Timestamps Method only)

Setting	Description	Factory Default
Time	Specify the time to stop pinging the IP address or hostname.	01:00 AM

When finished, click **PING** to begin pinging, or **STOP** to send.

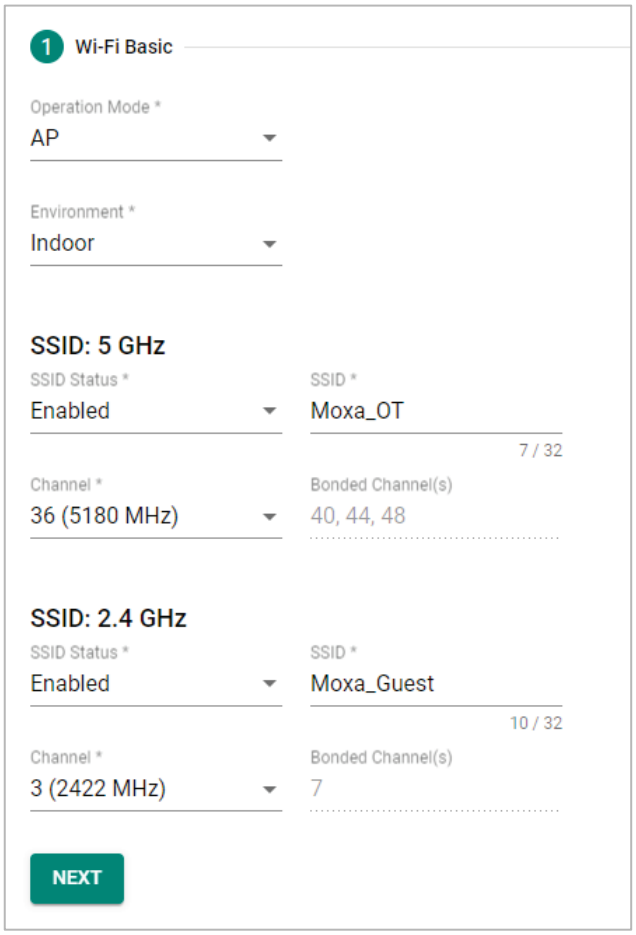
Setup Wizard

The **Setup Wizard** allows users to perform basic device configurations to get the TAP running quickly.

Click **Setup Wizard** in the function tree to start the Wizard, then follow the on-screen instructions. There are three configuration tabs: **Wi-Fi Basic, Wi-Fi Security,** and **System**. While the Wizard will start from the **Wi-Fi Basic** section by default, you can go to any other tab at any time.

Wi-Fi Basic

Configure the following settings:



Operation Mode

Setting	Description	Factory Default
Disabled	Disable the operation mode.	Disabled
AP	Specify the operation mode as AP. Refer to **AP Mode Settings**.	
Master	Specify the operation mode as Master. Refer to **Master Mode Settings**.	
Client	Specify the operation mode as Client. Refer to **Client Mode Settings**.	
Client-Router	Specify the operation mode as Client-Router. Refer to **Client-Router Mode Settings**.	
Slave	Specify the operation mode as Slave. Refer to **Slave Mode Settings**.	

Environment

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels vary depending on the selection.	

SSID: 2.4 GHZ

SSID Status

Setting	Description	Factory Default
Enabled/Disable	Enable or disable the SSID.	Disabled

SSID

Setting	Description	Factory Default
1 to 32 characters	Enter a name for the SSID.	None

Channel (available in AP and Master modes only)

Setting	Description	Factory Default
1 (2412 MHz) to 13 (2472 MHz)	Select the channel from the drop-down list. Each channel supports different frequencies.	6 (2437 MHz)

Bonded Channel (available in AP and Master modes only)

Setting	Description	Factory Default
10 (read only)	The bonded channel used by the AP will be shown here if channel width is set to 20/40 MHz.	None

SSID: 5 GHZ

SSID Status

Setting	Description	Factory Default
Enabled/Disable	Enable or disable the SSID.	Disabled

SSID

Setting	Description	Factory Default
1 to 32 characters	Enter a name for the SSID.	None

RF Band (for Client, Client-Router, and Slave modes only)

Setting	Description	Factory Default
5 GHz	Select 5 GHz as the RF band.	5 GHz
2.4 GHz	Select 2.4 GHz as the RF band.	
5 GHz & 2.4 GHz	Select both 5 GHz and 2.4 GHz as the RF bands.	

5 GHz Channel Plan (for Client, Client-Router, and Slave modes only)

Setting	Description	Factory Default
Channel	Select the channel for the 5 GHz band.	Any

Channel (for AP and Master modes only)

Setting	Description	Factory Default
36 (5180 MHz) to 161 (5805 MHz)	Select the channel from the drop-down list. Each channel supports different frequencies.	36 (5180 MHz)

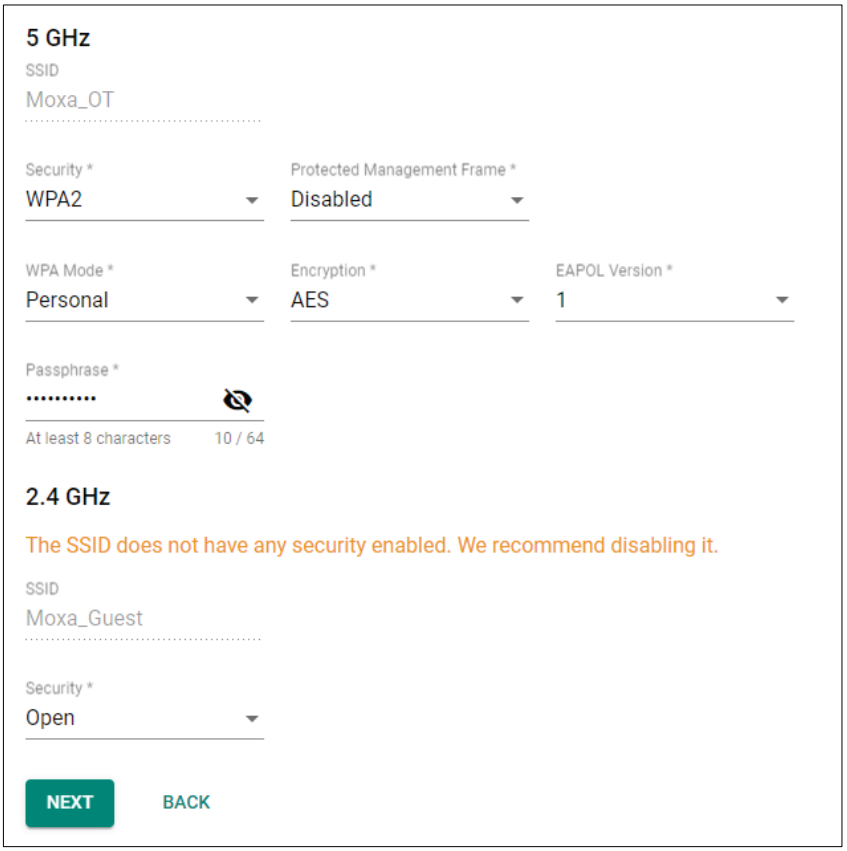
Bonded Channel (for AP and Master modes only)

Setting	Description	Factory Default
40/44/48 (read only)	The bonded channel used by the AP will be shown here if channel width is set to 36 (5180 GHz).	None

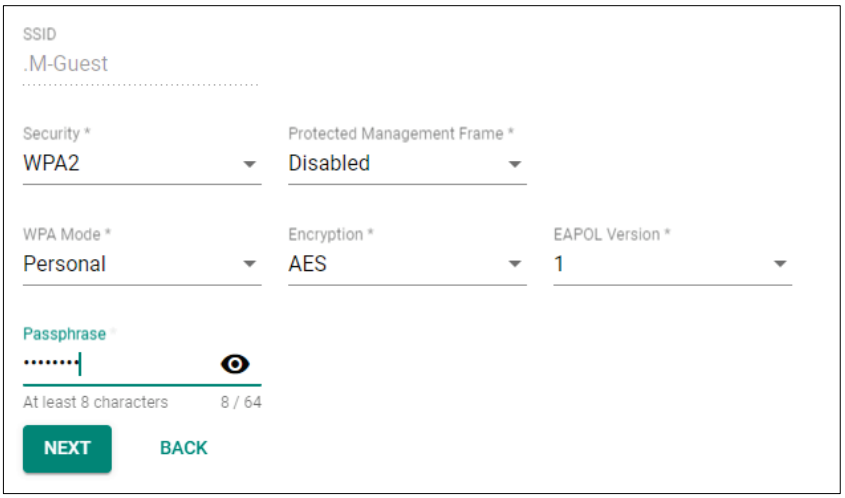
When finished, click **NEXT**.

Wi-Fi Security

AP/Master Mode



Client/Client-Router/Slave Mode



SSID

Setting	Description	Factory Default
SSID (read only)	Shows the name for the SSID.	None

Security

Setting	Description	Factory Default
Open	Disable security on the SSID. This is not recommended.	Open
WPA2	Use WPA2 authentication. This mode supports IEEE 802.11i with TKIP/AES + 802.1X encryption.	
WPA3	Use WPA3 authentication. This mode supports SAE (Simultaneous Authentication of Equals) to avoid network attacks, such as KRACK.	
WPA/WPA2 Mixed	Use WPA/WPA2 Mixed authentication. This allows both WPA and WPA2 clients to connect to the TAP.	
WPA2/WPA3 Mixed	Use WPA/WPA3 Mixed authentication. This allows both WPA2 and WPA3 clients to connect to the TAP.	

When using any security mode except **Open**, configure the following settings:

Protected Management Frame

Setting	Description	Factory Default
Disabled	Disable the protected management frame. This option is not available when using WAP3.	Disabled
802.11w	Use 802.11w protocol as the protected management frame.	

WPA type

Setting	Description	Factory Default
Personal	Use WPA, WPA2, and WPA3 with a Pre-shared Key (PSK).	Personal
Enterprise	Use WPA, WPA2, and WPA3 with EAP security.	

Primary/Secondary RADIUS Server IP (for Enterprise mode only)

Setting	Description	Factory Default
IP address	Specify the RADIUS authentication server for EAP.	None

Primary/Secondary RADIUS Port (for Enterprise mode only)

Setting	Description	Factory Default
0 to 65535	Specify RADIUS server port number.	1812

Primary/ Secondary RADIUS Shared Key (for Enterprise mode only)

Setting	Description	Factory Default
0 to 128 characters	Enter the secret key shared for communication between AP and the RADIUS server. The key cannot contain the following special characters: ` ' " | ; & $	None

Encryption

Setting	Description	Factory Default
AES	Use Advance Encryption System (AES) encryption.	TKIP/AES Mixed
TKIP/AES Mixed*	Use TKIP/AES Mixed encryption. This option provides a TKIP broadcast key and TKIP+AES unicast key to support legacy AP clients. This option is rarely used.	

**This option is available for legacy mode in AP/Master only and does not support AES-enabled clients.*

EAPOL Version

Setting	Description	Factory Default
1	Use EAPOL Version 1 as the security authentication method.	1
2	Use EAPOL Version 2 as the security authentication method.	

Passphrase (for Personal mode only)

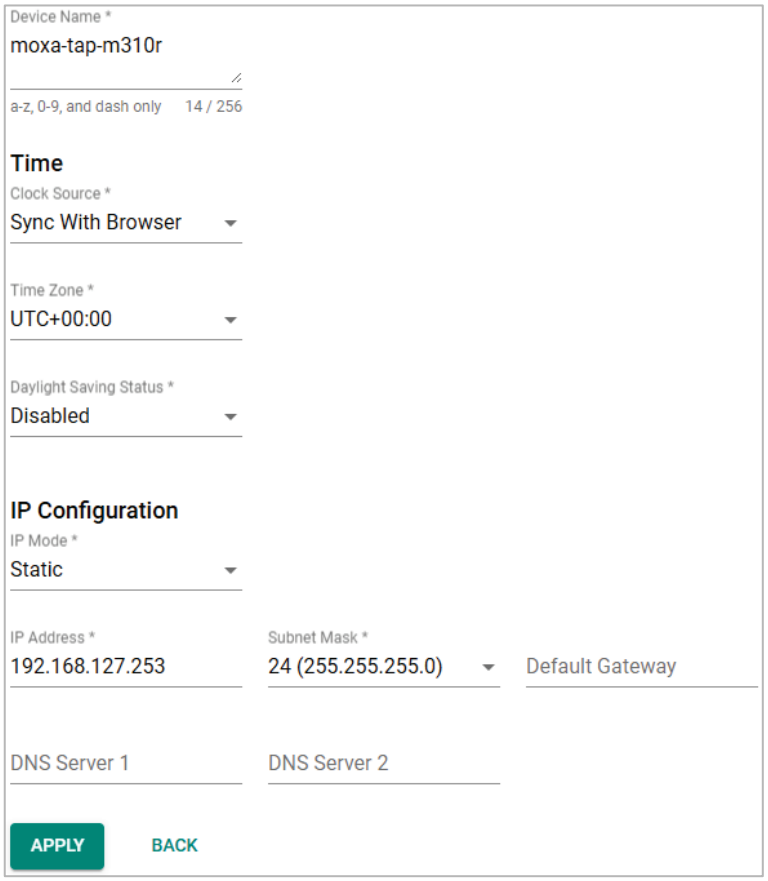
Setting	Description	Factory Default
8 to 64 characters	Enter the passphrase. This is the master key to generate keys for encryption and decryption. The passphrase cannot contain the following special characters: ` ' " | ; & $ Check **Show Password** to display the password in clear text.	None

EAP Protocol (for Enterprise mode only)

Setting	Description	Factory Default
TLS	Use EAP-TLS to validate the connection. This option allows the user to upload a TLS certificate to perform the identity check.	TLS
TTLS	Use TTLS to validate the connection. This option requires users to also specify the Anonymous Name, Username, and Password.	
PEAP	Use PEAP to validate the connection. This option requires users to also specify the Anonymous Name, Username, and Password.	

When finished, click **NEXT**.

System



Device Name

Setting	Description	Factory Default
1 to 256 characters	Enter a name for the device. This is useful for differentiating between the roles or applications of different units. Note that the device name cannot be empty and must comply with the following naming rules: • Only supports letters (a-z), numbers (0-9), and special character dash (-) • Cannot contain any spaces • Cannot start with dash (-) • Cannot end with dash (-) • When used in a PROFINET environment, cannot start with the prefix "port-x" where "x" equals 0 to 9. There is no validity check to identify incorrect name formats.	moxa-tap-m310r

Time

Clock Source

Setting	Description	Factory Default
Sync With Browser	Synchronize the system clock with the browser's clock.	Sync With Browser
NTP	Set the clock source to NTP. This will sync the system clock with an external NTP server.	

Time Server 1 (for Clock Source is NTP)

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

Time Server 2 (for Clock Source is NTP)

Setting	Description	Factory Default
NTP time server	Specify the IP or domain address of the secondary NTP server. The secondary NTP server acts as a backup in case the device fails to connect to the first NTP server.	None

Time Zone

Setting	Description	Factory Default
Time zone	Select a time zone.	UTC+00:00

Daylight Saving Time Status

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

Offset

Setting	Description	Factory Default
User-specified value	Specify the offset value for Daylight Saving Time.	00:00

Start

Setting	Description	Factory Default
User-specified date	Specify the date that Daylight Saving Time begins.	None

End

Setting	Description	Factory Default
User-specified date	Specify the date that Daylight Saving Time ends.	None

IP Configuration

IP Mode

Setting	Description	Factory Default
DHCP	The TAP is assigned an IP address automatically by the network's DHCP server.	Static
Static	Manually configure up the TAP's IP address.	

IP Address (for Static mode only)

Setting	Description	Factory Default
IP address	Enter the TAP's IP address.	192.168.127.253

Subnet Mask (for Static mode only)

Setting	Description	Factory Default
Subnet mask	Select the subnet mask. This is used to identify the type of network the TAP is connected to (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	24 (255.255.255.0)

Default Gateway (for Static mode only)

Setting	Description	Factory Default
IP address	Enter the IP address of the router that connects the LAN to an outside network.	None

DNS Server 1 and DNS Server 2 (for Static mode only)

Setting	Description	Factory Default
IP address	Enter the primary and secondary DNS server address. After entering the DNS server's IP address, you can input the TAP's URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

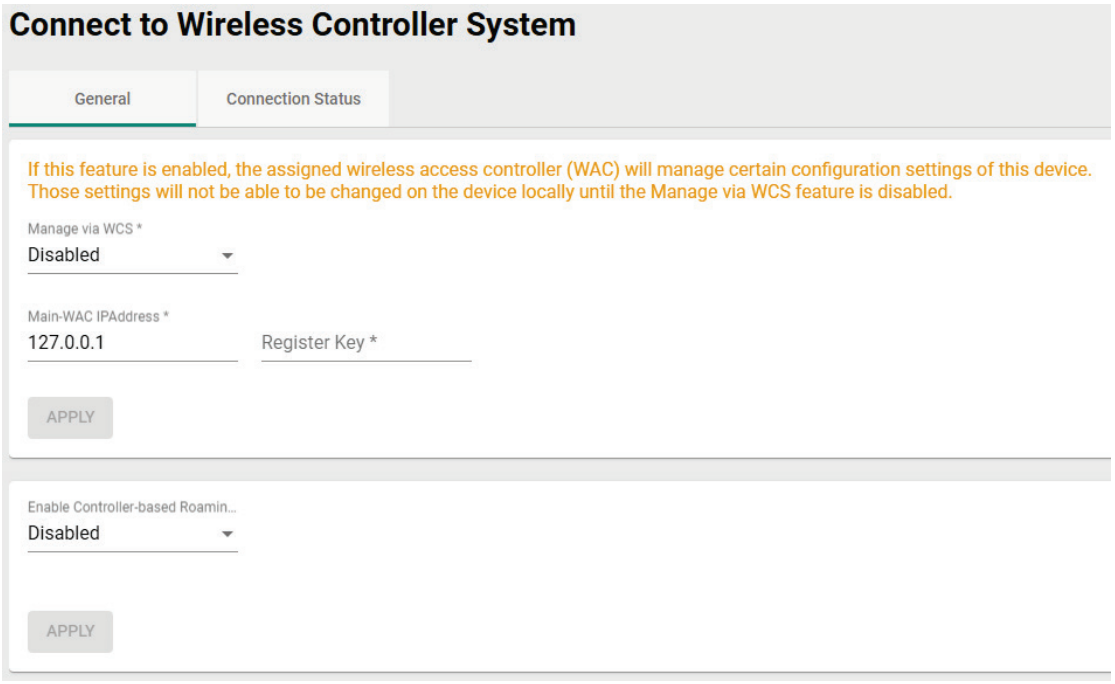
When finished, click **APPLY**.

Connect to Wireless Controller System (WCS)

The **Connect to WCS** section is used to configure the remote management of the TAP device via a WAC-M300 Series wireless access controller (WAC). When enabling this feature, certain settings on the device, including wireless and roaming settings, will be managed via the associated wireless access controller. Click **Connect to WCS** in the function tree.

General Settings

The **General** tab is used to configure the required parameters to connect the TAP to a WAC Series access controller. Click the **General** tab to access this screen.



Configure the following settings:

Manage via WCS

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable managing this TAP device via a WAC-M300 Series wireless access controller. If enabled, the assigned WAC will manage certain configuration settings of this device. Those settings will not be able to be changed on the device locally until the **Manage via WCS** feature is disabled.	Disabled

Main-WAC IP Address

Setting	Description	Factory Default
IP address	Specify the IP address of the main WAC to associate this TAP device with.	127.0.0.1

Register Key

Setting	Description	Factory Default
Register key	Enter the registration key of the specified main WAC.	None

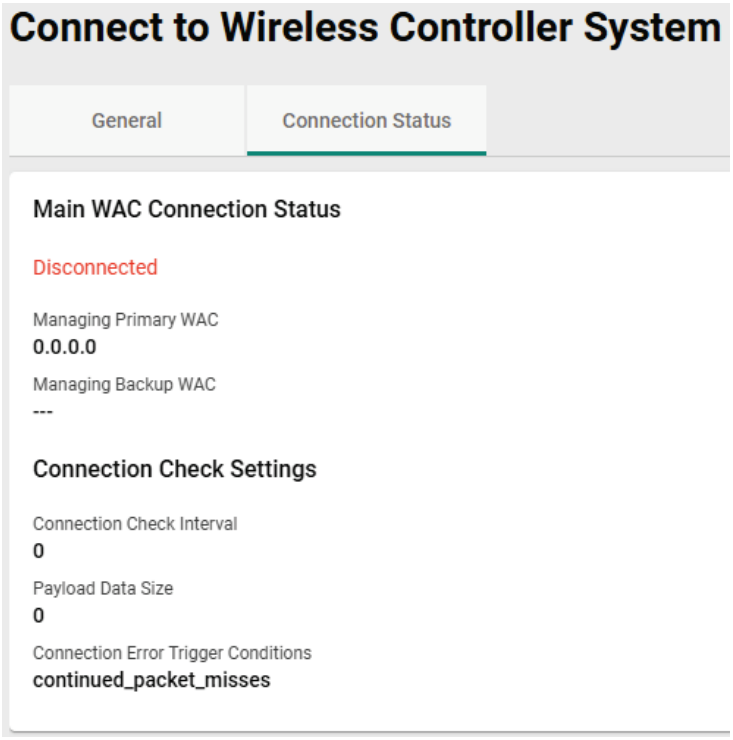
Enable Controller-based Roaming

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable controller-based roaming. If enabled, the TAP device's roaming behavior will be managed via the wireless access controller.	Disabled

When finished, click **APPLY**.

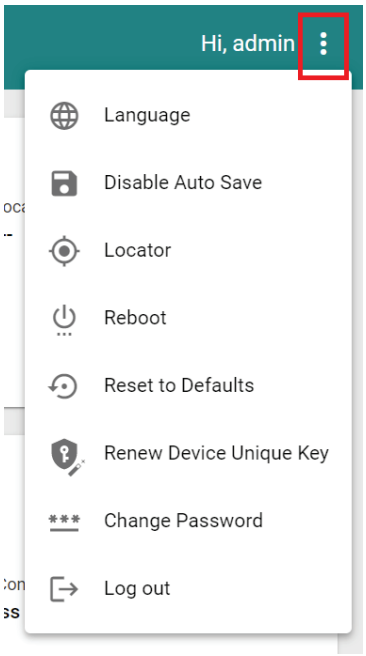
Connection Status

The **Connection Status** page shows the status of the connection to the WAC. Click the **Connection Status** tab to access this screen.



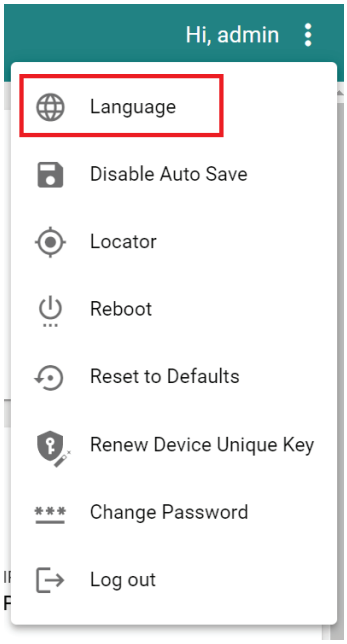
Maintenance and Tools

The user tools and functions are located at the top-right of the interface. Click the three-dot icon in the upper right corner of the page to open the user menu.



Language

The TAP-M310R Series v1.0 firmware and above support language localization. Administrators can select the display language of the web interface from the drop-down menu. The TAP-M310R supports the following languages: English, Simplified Chinese, Traditional Chinese, and Japanese. The default is English.

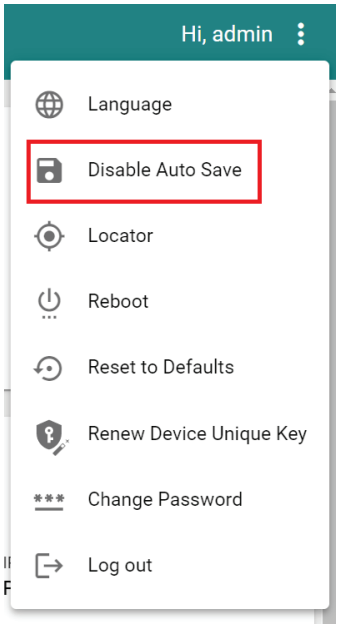


NOTE

Language options are only available for the web interface. The CLI only supports English.

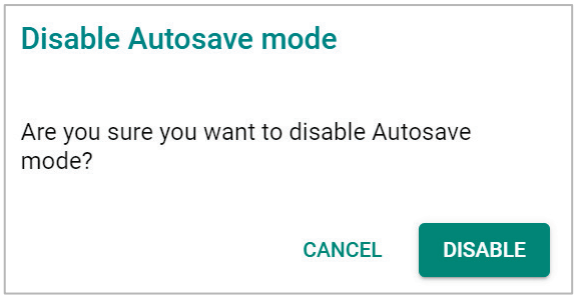
Disable Auto Save

Auto Save will automatically save the configuration changes to the startup configuration. All parameters will be effective immediately when applied, even if the TAP is restarted. If **Auto Save** is disabled, all parameters will be temporarily stored in the running configuration (memory). To make any changes take effect, you will need to save the running configuration to the startup configuration after applying the changes.



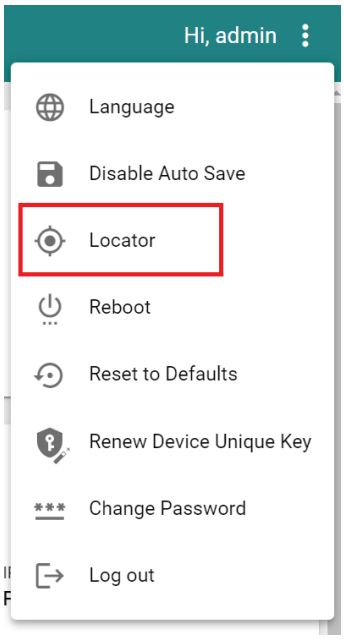
When **Disable Auto Save** is active, only the running configuration is saved. Disconnecting the power or performing a warm start will undo any running changes. When **Auto Save** is enabled, the startup configurations will be saved on the TAP.

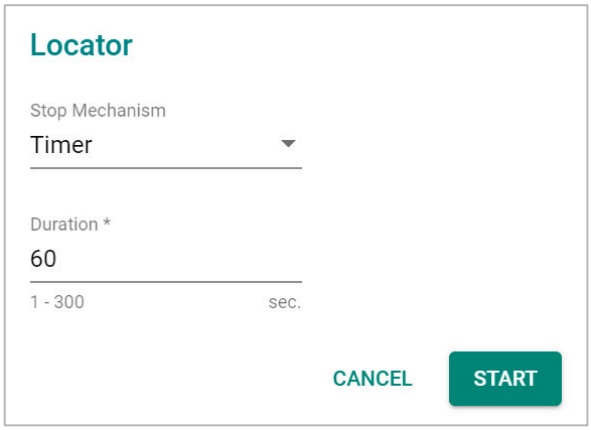
To disable the **Auto Save** function, click **Disable Auto Save** in the menu. When prompted, click **DISABLE** to disable the function.



Locator

Clicking **Locator** will trigger the SYS, 2.4G, and 5G LEDs to start flashing green at a 4 Hz interval for one minute (default) alongside an audible beeper. This feature is useful for locating the physical device in a field site.





Stop Mechanism

Setting	Description	Factory Default
Timer	Use a timer to stop the locator LEDs from blinking.	Timer
Manually	Stop the locator LEDs manually.	

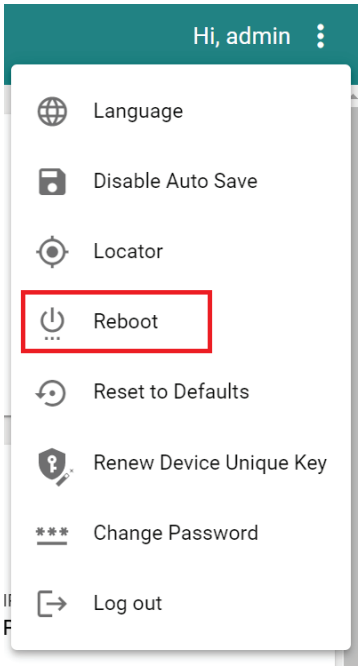
Duration

Setting	Description	Factory Default
1 to 300 (sec.)	Specify the duration the LEDs will be blinking for.	60

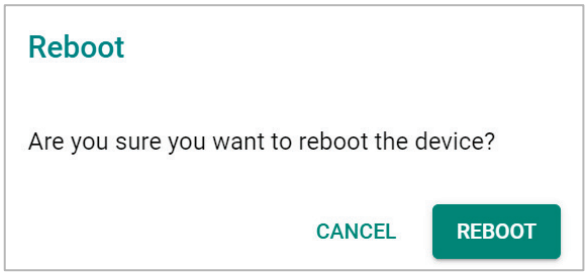
When finished, click **START** to activate the LEDs.

Reboot

To reboot the TAP, click **Reboot**.

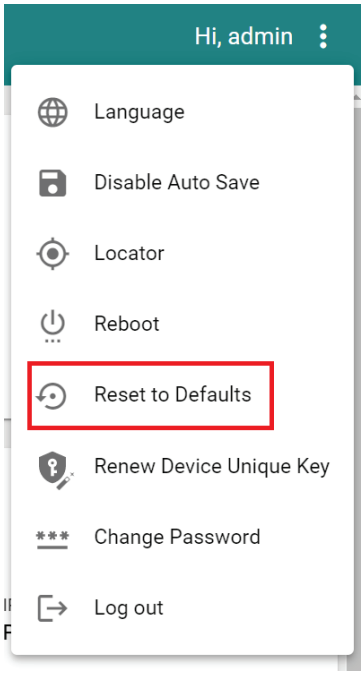


When prompted, click **REBOOT** to reboot the TAP.

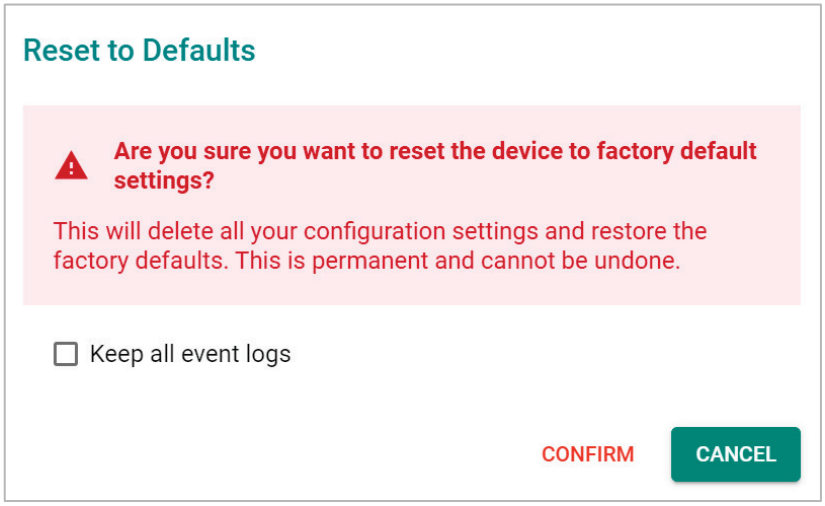


Reset to Defaults

To reset the TAP to the factory default settings, click **Reset to Defaults**.



When prompted, check **Keep all event logs** if you want to keep the event history, then click **CONFIRM**.



WARNING

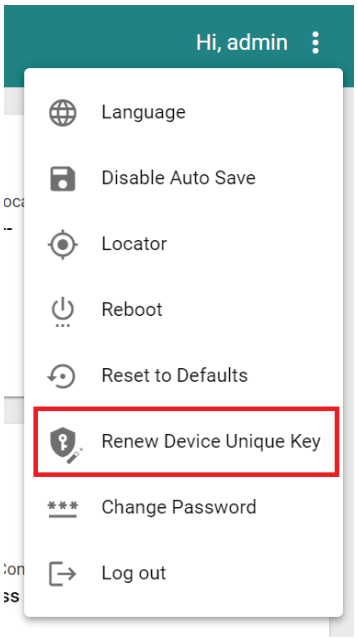
Resetting the TAP to the factory default settings will permanently delete all your configuration settings. This is permanent and cannot be undone.

Renew Device Unique Key

The TAP-M310R Series has a built-in device unique key. This unique key is used to encrypt the following sensitive information stored on the device:

- Configurations
- Certifications
- Encryption/decryption keys (for firmware decryption, diagnostic support encryption, etc.)

To improve device security, administrators can renew the device unique key from the maintenance list.

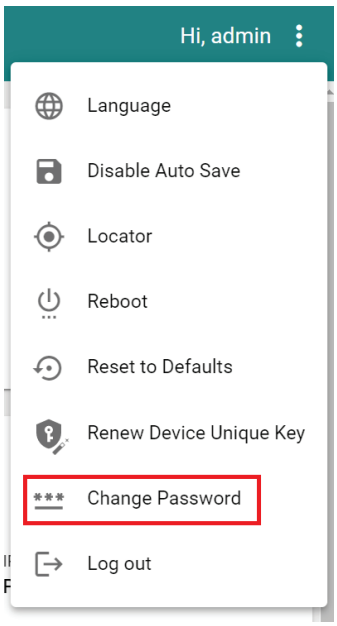


WARNING

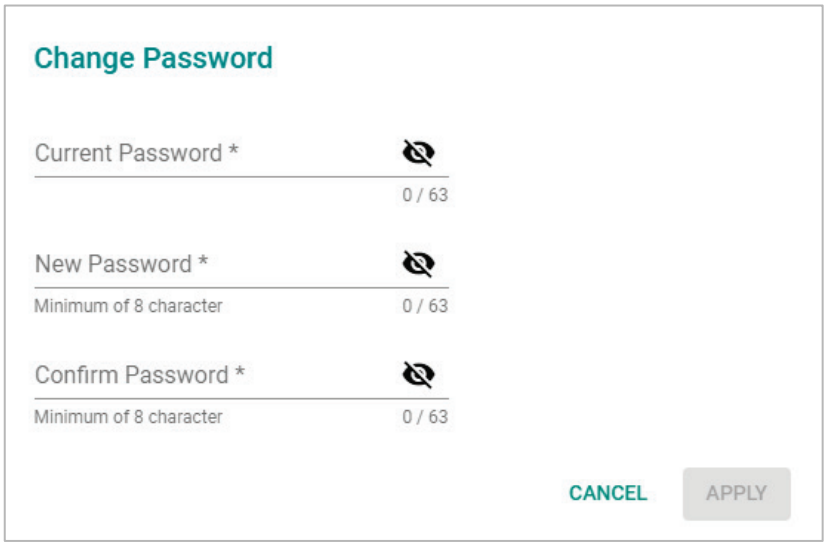
When triggered, the system will take 12 to 15 seconds to renew the device unique key and will then reboot to activate the renewed device unique key. Please do not power off the device during this process.

Change Password

Click **Change Password** to change the password of the TAP.



Configure the following settings:



Current Password

Setting	Description	Factory Default
8 to 63 characters	Enter the current password.	None

New Password

Setting	Description	Factory Default
8 to 63 characters	Enter the new password.	None

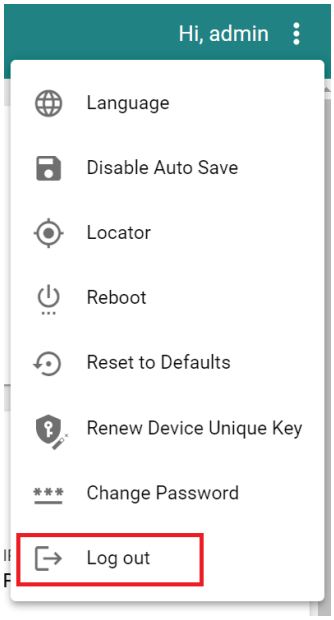
Confirm Password

Setting	Description	Factory Default
8 to 63 characters	Enter the new password again.	None

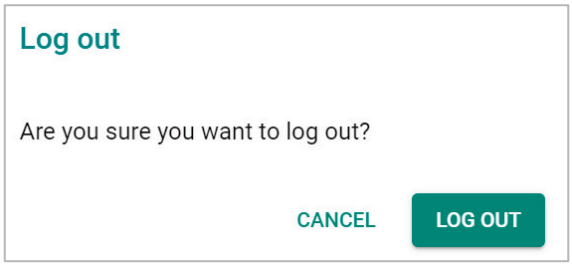
When finished, click **APPLY** to change the password.

Log Out

To log out of the TAP, click **Log out**.



When prompted, click **LOG OUT** to log out of the TAP.



A. Supporting Information

This chapter presents additional information about this product. You can also learn how to contact Moxa for technical support.

Device Recovery

In event the device is not working properly, including configuration changes not applying, the first troubleshooting action is to perform a power cycle. This is done by removing and reconnecting the power and verifying if the situation is resolved.

If power cycle does not solve the issue, the next step is to perform a reset to factory default setting. Refer to **Reset Device**.

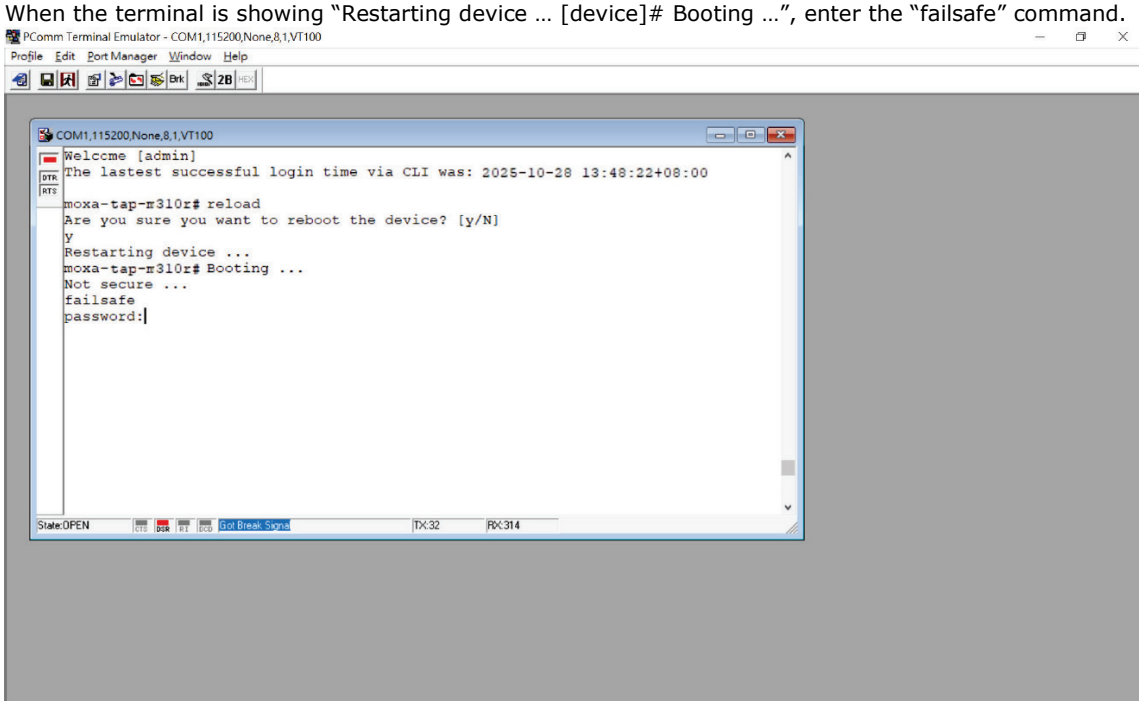
If you cannot access the web interface, and/or the Reset button is disabled, you can attempt to reset the device via the serial console's CLI FailSafe mode.

NOTE

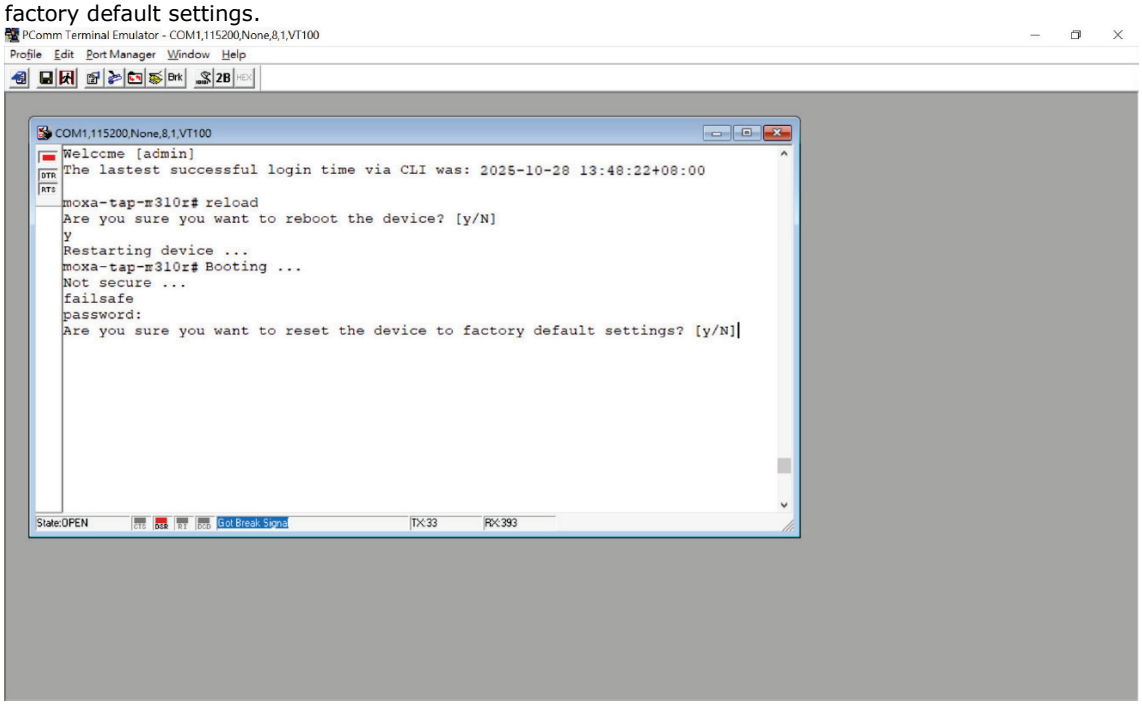
The admin password is required to authorize the FailSafe function.

Follow the instructions in the **Accessing the Serial Consoles** section to access the serial console CLI interface and enter the "reload" command to reboot the device.

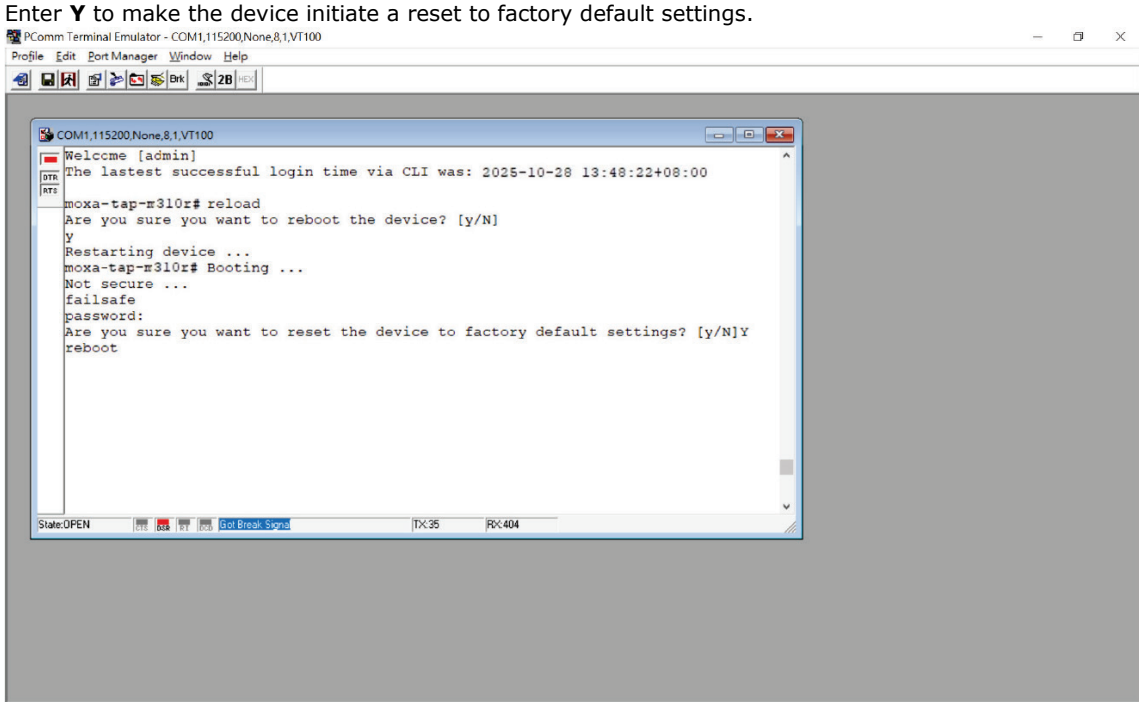
When the terminal is showing "Restarting device … [device]# Booting …", enter the "failsafe" command.



FailSafe mode will be triggered, and you will be prompted to confirm if you want to reset the device back to factory default settings.



Enter **Y** to make the device initiate a reset to factory default settings.



When the command line prompt displays the login prompt, it means the device was successfully reset to factory default settings.

B. Accessing the Serial Consoles

This chapter explains how to access the TAP-M310R Series. In addition to HTTP/HTTPS access, the TAP-M310R Series can also be accessed through the serial console and Telnet/SSH console. The serial console connection method, which requires a serial cable to connect the TAP-M310R Series to a PC's COM port, can be used if you do not know the TAP-M310R Series' IP address. The other consoles can be used to access the TAP-M310R Series over an Ethernet LAN, or over the Internet.

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

ATTENTION

Do not use the RS-232 console manager when the TAP-M310R Series is powered at reversed voltage (ex. -48 VDC), even though reverse voltage protection is supported.

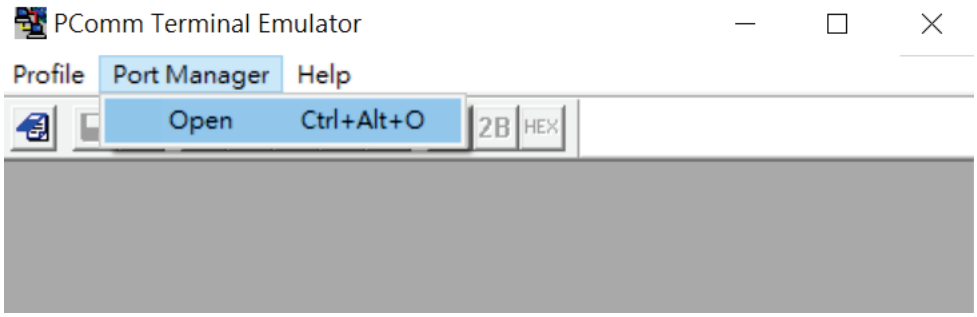
If you need to connect the RS-232 console at reversed voltage, we highly recommend using an isolator, such as the Moxa TCC-82 isolator.

NOTE

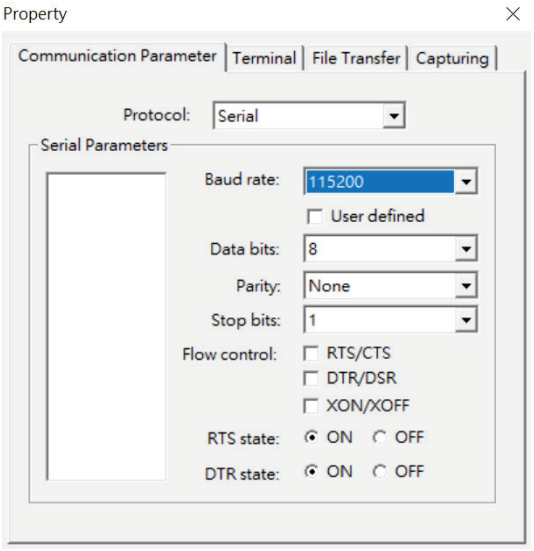
We recommend using **Moxa PComm (Lite)** Terminal Emulator, which can be downloaded free of charge from Moxa's website.

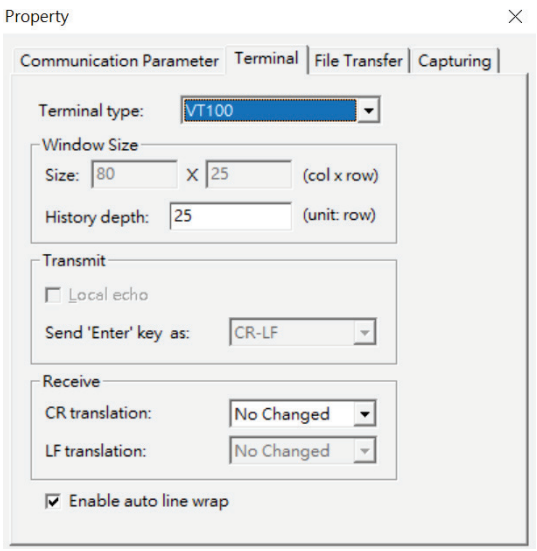
Before running PComm Terminal Emulator, use an A-coded female M12-to-5-pin DB9 console cable to connect the TAP-M310R Series' RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, perform the following steps to access the RS-232 console utility.

1. From Windows desktop, open the Start menu and run **PComm Terminal Emulator** in the PComm (Lite) group.
2. Select **Open** under **Port Manager** to open a new connection.

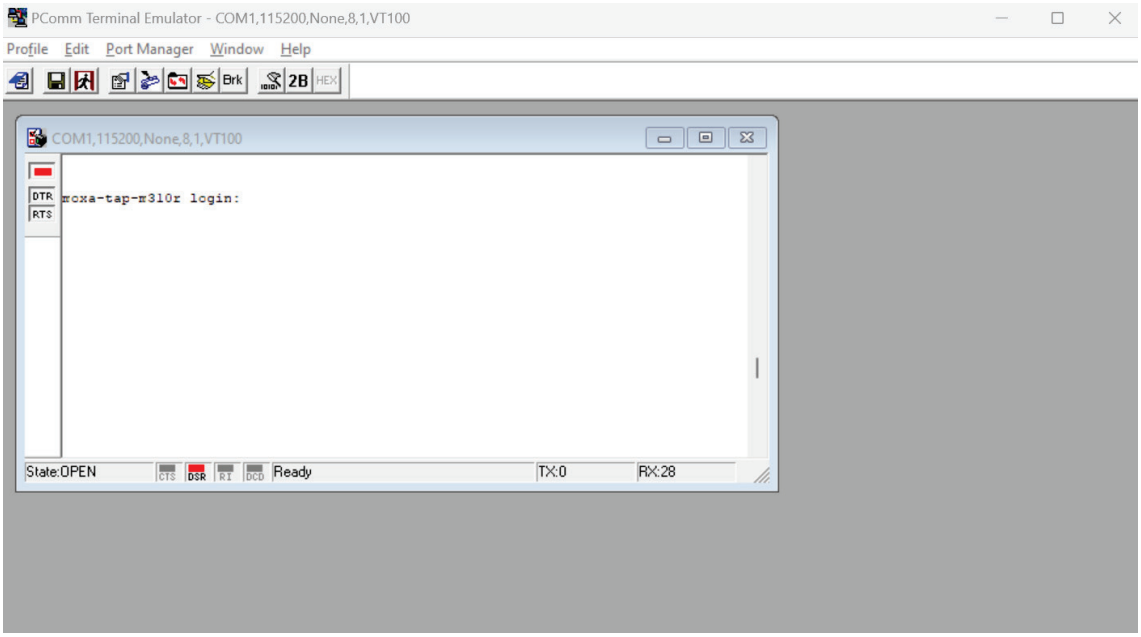


The **Communication Parameter** page of the Property window opens. Select the appropriate COM port for the Console Connection, **115200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits. Click on the **Terminal** tab and select **VT100 (or ANSI)** for Terminal Type. Click **OK** to continue.

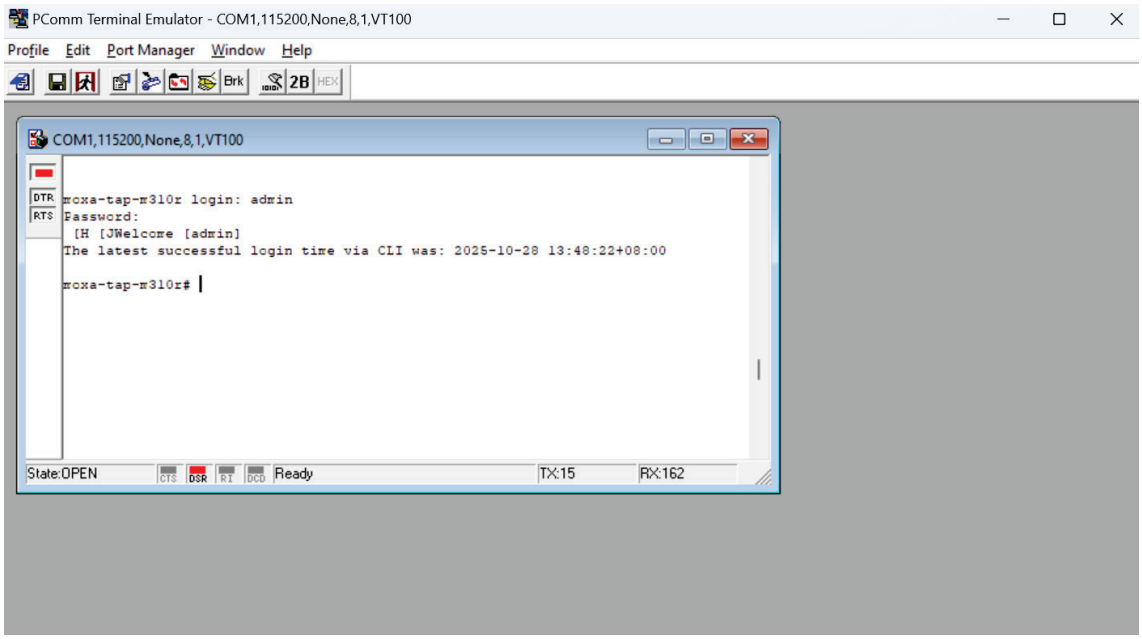




3. The Console login screen will appear. Log into the RS-232 console with the device's account and password.



4. The TAP-M310R Series device's CLI interface will be displayed.



NOTE

To modify the appearance of the PComm Terminal Emulator window, select **Edit > Font** and then choose the desired formatting options.

ATTENTION

If you unplug the RS-232 cable or trigger **DTR**, you will be disconnected and logged out for network security reasons. You will need to log in again to resume operations.

Configuration by Telnet and SSH Consoles

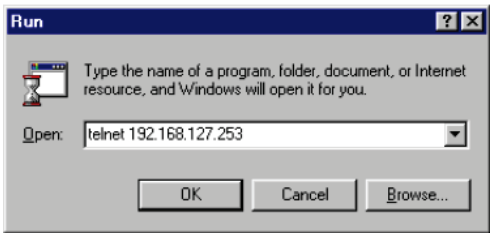
You can use a Telnet or SSH client to access the TAP-M310R Series and manage the console over a network. To access the TAP-M310R Series' functions over the network from a PC host that is connected to the same LAN as the TAP-M310R Series, you need to make sure that the PC host and the TAP-M310R Series are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

NOTE

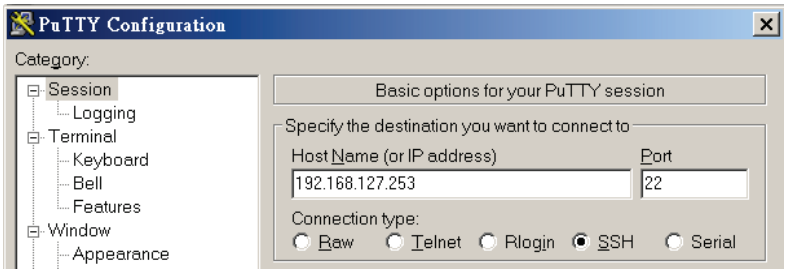
The TAP-M310R Series' default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). To configure the TAP-M310R Series remotely over a LAN network, set the PC host's IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

Follow the steps below to access the console utility via Telnet or SSH client:

1. From Windows Desktop, run **Start > Run**, and type *telnet (TAP IP address)* in the Run window and click **OK**. The TAP's default IP address is 192.168.127.253.



2. When using an SSH client (e.g. PuTTY), run the software and enter the TAP device's IP address as the Host Name along with port **22**, and select **SSH** as the connection type.



3. The Console login screen will appear. Please refer to the previous paragraph "RS-232 Console Configuration" and for login and administration.

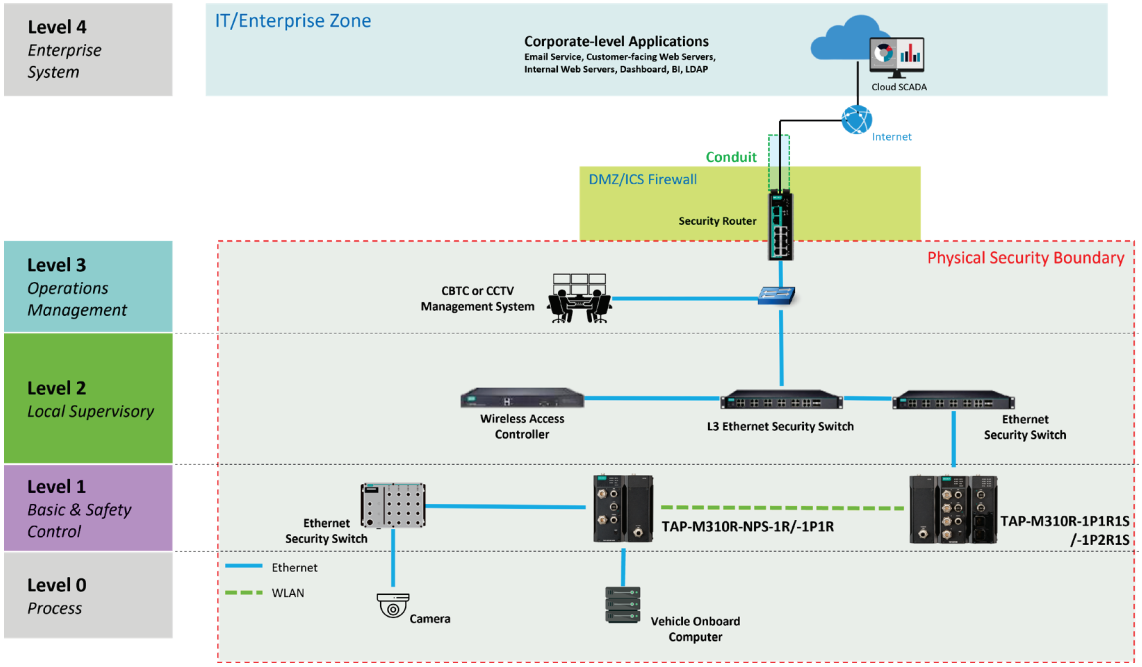
C. Security Guidelines

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

Installation

Physical Installation

1. To comply with IEC 62443 requirements, the TAP-M310R Series device MUST be installed within an access-controlled area, where only authorized personnel have physical access to the TAP-M310R Series device.
2. To comply with IEC 62443 requirements, the device MUST NOT be directly connected to the Internet, which means the TAP-M310R Series device MUST be installed within a security perimeter with firewall. Additionally, the various application service servers such as DHCP, NTP, RADIUS, … etc. shall be securely configured with proper authentication within the security perimeter with firewall protection as illustrated in the image below:



3. Always configure the TAP-M310R Series device to comply with your organization's network and security requirements before physical installation. Do not physically install devices that are unconfigured or have an unknown configuration state to avoid unnecessary risks. Please follow the instructions in the Quick Installation Guide, which is included in the package, to ensure you install the device correctly in your environment.
4. The TAP-M310R Series has anti-tamper labels visible on the enclosures covering assembly screws. Any tampering to open the mechanical enclosure to access electrical circuit boards will result in the fracturing of anti-tamper labels. This allows an administrator to immediately tell if the device's hardware integrity has been compromised.
5. Ports that are not in use should be deactivated. Please refer to Hardware Interface and Ports to review the status of each I/O port and disable any unused ports.

6. The TAP-M310R Series devices are industrial WLAN infrastructure components serving as the underlying fabric to support automation processes. These devices are not an integral part of process automation logic and therefore do not support nor are they suitable for any deterministic process control outputs.

Account Management

Follow these best practices when setting up an account:

1. Each account should be assigned the correct privileges: Only allow the minimum number of people to have admin privilege so they can perform device configuration or modifications, while other users should only have the minimum required access privilege needed to fulfill their corresponding role. The TAP-M310R Series supports both local account authentication and remote centralized authentication mechanisms such as RADIUS.
2. Password protection has two means of enforcement: Password Lifetime and Password Complexity. We recommend to:
   a. Review whether the password lifetime needs to be adjusted according to your organization's policies.
   b. Review whether the configured password complexity options enabled on the TAP-M310R Series system (refer to Create a New Local Account) is sufficient according to your organization's policies. If not, modify the password complexity requirements to meet your organization's security guidelines.
3. Enforce regulations that ensure only trusted hosts can access the device. Refer to the Trusted Access section for more information and instructions.

Vulnerable Protocols

1. For network security reasons, we strongly recommend that you change the default port numbers, such as the TCP port number for HTTP, HTTPS, Telnet, and SSH, for protocols that are in use. Ports that are not in use but are still accessible, pose a security risk and should be disabled. Refer to the Management Interface section for more information and instructions.
   Below is the list of default port numbers for each protocol used by all external interfaces.

Browser	Protocol Type	Default Port
TCP	HTTP	80
	HTTPS	443
	Telnet	23
	SSH	22
UDP	SNMP	161
	Moxa Service	40404

2. In order to avoid malicious actors from snooping confidential information, users should always apply encryption-based communication protocols such as HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, SNMPv3 instead of SNMPv1/v2c etc. In addition, the maximum number of sessions should be kept to an absolute minimum. Refer to the Management Interface section for more information and instructions.
3. Users should generate the SSL certificate for the device before commissioning HTTPS or SSH applications. Please refer to the Certificate Management section for more information and instructions.
4. The HTTP, SNMPv1v2, and Telnet protocols are insecure and by default DISABLED. We recommend always using secure alternatives such as HTTPS, SNMPv3, or SSL to protect your communications. If unsecure protocols need to be used with legacy devices, please consult a qualified security expert to evaluate and implement additional protection measures to prevent any potential security risks.
5. In order to ensure that the device configurations are adequately protected prior to deployment, it is recommended to review the security status of the device. Refer to the Security Status section for an overview of the device's current security conditions. If any of the identified risks require mitigating action, navigate to the corresponding setup page to address the issue, or consult a qualified security expert to evaluate and implement additional protection measures to prevent any potential security risks.

Operation

1. For security reasons, The TAP-M310R Series does not support TLS v1.0/ v1.1. The TAP-M310R Series supports the TLS v1.2 cryptographic algorithm to protect your HTTPS/SSH applications. Please ensure that your web browser is updated to a version that supports TLS v1.2:

Browser	Version
Microsoft Edge	All versions
Mozilla Firefox	V11 and above
Chrome	V38 and above
Apple Safari	V7 and above for OS X 10,9 (Mavericks) and above

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

2. The device supports event logs and syslog for SIEM integration:
   a. Event log: Due to limited storage capacity, the event log can only accommodate a maximum of 10,000 entries. Administrators can set a warning for a pre-defined threshold. We recommend that users regularly back up system event logs. Please refer to the Event Log section for more information and instructions.
   b. Syslog: The device supports syslog and advanced secure TLS-based syslog for centralized SIEM integration. Please refer to the Syslog section for more information and instructions.
3. The device can provide information for control system inventory:
   a. SNMPv1, v2c, v3: We recommend administrators use SNMPv3 with authentication and encryption to manage the network. Please refer to the MIB file for the detailed OID structure.
   b. Telnet/SSH: We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
   c. HTTP/HTTPS: We recommend that administrators use HTTPS with an internally renewed certificate or imported certificate that has been issued by a Certificate Authority (CA) to configure the device.
4. Denial of Service protection: We recommend enabling Trusted Access, Wi-Fi ACL, L2/L3 firewalls to mitigate the risk of DoS attack attempts.
5. Periodically regenerate the SSH and SSL certificates: Even though the device supports up-to-date cipher suites to ensure sufficient complexity, we strongly recommend users to frequently renew their SSH key and SSL certificate in case the key is compromised. Please refer to the Certificate Management section for more information and instructions.

Defense-in-depth Strategy

1. The defense-in-depth strategy is a security approach to protect systems from various types of attacks by using multiple independent defense mechanisms. This strategy involves incorporating multiple layers of security to protect the product against potential attacks and vulnerabilities at various stages of its design, development, and use.
2. It is important to understand that no single protection measure can guarantee complete security. That's why the defense-in-depth approach makes it difficult for attackers to exploit one weakness to attack the product or the network as a whole. By implementing a defense-in-depth approach, attackers must overcome multiple security layers undetected, making breaches increasingly difficult.
3. Refer to the following table for measures you can leverage to create a defense-in-depth security environment on the TAP-M310R Series.

Security Function	Description	Type	Implementation
Account Management	Reduces human error by enforcing access privileges	Administrative Control	Admin/User role settings
Syslog Logging	Logs operations and anomalies	Administrative Control	Supports remote syslog server
Web/CLI Login Authentication	Prevents unauthorized user access to the device	Administrative Control	Web/CLI Login Authentication
Device Certificate & Authentication	Prevent man-in-the-middle (MITM) attacks	Logical/Technical Control	Supports TLS v1.2, SNMPv3

Security Function	Description	Type	Implementation
Signed Firmware Validation	Prevents unauthorized firmware uploads	Logical/Technical Control	Signature verification ensures firmware validity
Critical Service Access Control	Restricts internal services such as DHCP/NTP	Logical/Technical Control	Configuration is restricted to authorized internal users, external access is blocked
Wireless Security Mechanisms	Controls AP/Client behavior and access	Logical/Technical Control	WPA2/WPA3, 802.1X, MAC filter
Trusted Access	Limits access by IP/Port/Protocol	Logical/Technical Control	Layer 2/3 ACL to manage device access
Physical Security	Prevents unauthorized physical access	Physical Control	Install the device in cabinets with strict access control and surveillance

Maintenance

1. Perform firmware upgrades frequently to enhance features, deploy security patches, or fix bugs. Periodically check the official product website or Moxa security advisory updates at https://www.moxa.com/en/support/product-support/security-advisory/security-advisories-all.
2. Periodically, or after each maintenance session, back up the running system configuration to be able to restore the device back to the latest stable, secure state if necessary. The device supports password encryption and signature authentication for backup files to protect the system configuration files from being tampered with,
3. Examine event logs frequently to detect any anomalies.
4. Periodically, or after each maintenance session, check the Security Status overview to review and confirm the current device's security conditions.
5. To report vulnerabilities for Moxa products, please email your findings to PSIRT@moxa.com.

Decommission

1. Power off the device to be decommissioned and dismount it from its physical installation location.
2. Identify the serial number or device name and locate (if applicable) any configuration backup files or certificates generated by the device to be decommissioned and ensure the deletion of these files.
3. To avoid any sensitive information such as the organization's information, account passwords, or certificates from being leaked, always reset the device to the factory default settings before decommissioning the device. If the reset function via the web console or the physical button is unavailable, it is recommended to securely dispose of the hard drive using specialized hard drive shredding equipment or services.

D. Service Authority Table

This appendix lists the required authority for each feature or service. The purpose of this table is to help administrators review and decide the appropriate account privileges and role to assign to user accounts.

Authority	Admin	Engineer	User
Account System	Yes	No	No
Auditor System	Yes	Yes	No
Advanced Diagnostics	Yes	Yes	No
Diagnostics	Yes	Yes	Yes
Network Configuration	Yes	Yes	No
Status Monitoring	Yes	Yes	Yes
System Backup	Yes	No	No
System Management	Yes	Yes	No

Configuration Section	Authority Required
Device Summary	Status Monitoring
System	
System Management	
System Information	System Management
Firmware Upgrade	System Management
Configuration Backup and Restore	System Backup
Fast Boot-up	System Management
Account Management	
User Account	(Refer to breakdown below)
Settings	Account System
Session Management	System Management
RADIUS	Account System
Password Policy	Account System
Management Interface	
User Interface	System Management
Hardware Interface	System Management
SNMP	(Refer to breakdown below)
SNMP	System Management
SNMP Account List	Account System
Time	
System Time	System Management
Wi-Fi	
Wireless Settings	(Refer to breakdown below)
General	Network
MAC Cloning	Network
Wi-Fi Connections	Network
Connection Management	Network
Wi-Fi Security	Network
Ports	
Port Settings	(Refer to breakdown below)
General	Network
Port Status	Status Monitoring
Layer 2 Switching	
VLAN	Network
Storm Protection	Network
Turbo Chain	Network
IP Configuration	
General	System Management

Configuration Section	Authority Required
IPv6	System Management
Status	Status Monitoring
Network Service	
DHCP Server	Network
DHCPv6 Server	Network
Routing and Nat	
Routing	
Unicast Route	
Static Route	Network
Routing	Status Monitoring
NAT	
Network Address Translation	Network
Firewall	
Layer 2 Policy	Network
Layer 3 Policy	Network
Certificate Management	System Management, Auditor System, System Backup, Status Monitoring, Diagnostics, Advanced Diagnostic, or Network Configuration
Security	
Device Security	
Login Policy	System Management
Trusted Access	System Management
Diagnostics	
Security Status	Status Monitoring
System Status	Status Monitoring
Network Status	
Network Statistics	Status Monitoring
LLDP	(Refer to breakdown below)
Settings	Network
Bridge Table	Status Monitoring
ARP Table	Status Monitoring
Event Logs and Notifications	
Event Log	(Refer to breakdown below)
Log List	Status Monitoring
Registered Logs	Auditor System
Oversize Action	Auditor System
Backup	Status Monitoring
Event Notifications	Auditor System
Syslog	Auditor System
SNMP Trap/Inform	Auditor System
Email Settings	Auditor System
Tools	
Wi-Fi Tools	
Channel Scan	Advanced Diagnostic
Wi-Fi Mirroring	Diagnostic
RSSI Reporting	Diagnostic
System Data Collection	Diagnostic
Diagnostic Support	Advanced Diagnostic
Ping	Diagnostic
Setup Wizard	Network and System Management
Connect to WCS	Network and System Management
Maintenance Bar	
Language	Basic
Disable Auto Save	System Management
Locator	Diagnostic
Reboot	System Management
Reset to Defaults	System Management
Renew Device Unique Key	System Management

Configuration Section	Authority Required
Change Password	Basic
Log Out	Basic