TAP-M310R Series User Manual

Version 1.0, May 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

© 2025 Moxa Inc. All rights reserved.

Trademarks

The MOXA logo is a registered trademark of Moxa Inc. All other trademarks or registered marks in this manual belong to their respective manufacturers.

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

About This Manual	
About Note, Attention, and Warning	
Configuration Reminders	
A: About Mandatory Parameters	
B: Preconfiguring Settings Getting Started	
-	
Functional Design	
LED Indicators	
Reset Button	
First-time Installation and Configuration	
Communication Testing	
Web Interface Configuration	
Function Introduction	
Device Summary	
Device Information	
System Information	
System Status	
Security Status	
System	
System Management	
Account Management	30
Management Interface	39
Time	46
Wi-Fi	51
Wireless Settings	51
Connection Management	71
AeroLink Protection	
Wi-Fi Security	
Ports	
Port Settings	
Layer 2 Switching	
VLAN	
Storm Protection (TAP-M310R-1P1R1S and -1P2R1S Only)	
Turbo Chain (TAP-M310R-1P1R1S and -1P2R1S Only)	
IP Configuration	
General Settings	
IP Configuration Status	
Network Service	
DHCP Server	
DHCPv6 Server	
Routing and NAT	
Routing	
NAT	100
Firewall	106
Layer 2 Policy	106
Layer 3 Policy	108
Certificate Management	110
Certificates	11:
CA Certificates	112
Security	112
Device Security	
, Diagnostics	
Security Status	
System Status	
Network Status	
Event Logs and Notifications	

	Tools	132
	Setup Wizard	140
	Wi-Fi Basic	140
	Wi-Fi Security	143
	System	145
	Connect to Wireless Controller System (WCS)	147
	General Settings	147
	Connection Status	148
	Maintenance and Tools	148
	Language	149
	Disable Auto Save	150
	Locator	150
	Reboot	151
	Reset to Defaults	152
	Renew Device Unique Key	154
	Change Password	154
	Log Out	156
Α.	Supporting Information	
	Device Recovery	157
В.	Accessing the Serial Consoles	159
	RS-232 Console Configuration (115200, None, 8, 1, VT100)	159
	Configuration by Telnet and SSH Consoles	161

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
C	Refresh
8	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save the configuration.
J	Export
<i>`</i>	Edit
(ŕ	Perform a Wi-Fi site survey (Client mode only)
\$	Re-authentication
Î	Delete
к X К X	Panel View

Symbols	Meanings
~	Expand
^	Collapse
•	Hint or additional information
타	Settings
→←	Data comparison
:	Menu icon
\$	Change mode
۲	Locator
Ģ	Reboot
Ð	Reset to defaults
€	Logout
\uparrow	Increase
\checkmark	Decrease
+ + ■	Equal
≡	Menu
Q	Search
Ø	Hide text that is typed into a text box (usually used when typing a password)
0	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

Create Static Ro	ute E
Entry Status *	
Disabled	•
Name	
	0 / 31
Destination *	
Required	
Netmask *	
24 (255.255.255.0)	•
Next Hop	
Interface *	
WAN	•
Metric	

- 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 a SNMP Status * Disabled	re not secure. We recom	mend using SNMP V3.

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.		
		On	Power is being supplied to the 24 VDC input of the radio module.		
PWR	PWR Green	Green Off	Green	Off	Power is not being supplied via the 24 VDC input of the radio
			UII	module, or the switch module is present.	
		On	Indicates a system initialization failure, configuration error, or		
SYS	Green	On	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.		
	Red	On	The LAN port's 2500 Mbps link is active.		
	Reu	Blinking	Data is being transmitted at 2500 Mbps.		
LAN1	Green	On	The LAN port's 10/100/1000 Mbps link is active.		
LANI	Green	Blinking	Data is being transmitted at 10/100/1000 Mbps		
	Green/ Amber	Off	The LAN port is inactive.		

LED	Color	State	Description
	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.
	Green	Blinking	Traffic is being transmitted in Client(-router) or Slave mode over the 2.4 GHz band.
2.4G	Amber	On	The device is in AP, Master, Sniffer mode and the 2.4 GHz band is active.
	Amber	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.
	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.
	Green	Blinking	Traffic is being transmitted in Client(-router) or Slave mode over the 5 GHz band.
5G	Amber	On	The device is in AP, Master, or Sniffer mode and the 5 GHz band is active.
	Amber	Blinking	Traffic is being transmitted in AP or Master mode over the 5 GHz band.
	Green/Amb er	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	
			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.	
		Blinking	- the switch module is the Member switch, and Member port 1 is not	
		5	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.	
			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	
		Off	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.	
		On	Turbo Chain redundancy is enabled, and the Tail port is in the Link	
		On	Up Forward (LUF) state.	
			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.	
			Blinking	- the switch module is the Member switch, and Member Port 2 is not
TAIL	Green		- the switch module is the Tail switch, and the Member Port is not in	
			the Link Up Forward (LUF) state.	
			Turbo Chain redundancy is disabled or	
			Turbo Chain redundancy is enabled, and	
		Off	- the switch module is the Head switch, and the Member Port is in	
		Oli	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.	
	Green	On	The LAN port's 2500 Mbps link is active.	
		Blinking	Data is being transmitted at 2500 Mbps.	
LAN2/3	Amber	On	The LAN port's 10/100/1000 Mbps link is active.	
(SFP)		Blinking	Data is being transmitted at 10/100/1000 Mbps	
	Green/	Off	The LAN port is inactive, the SFP module or SFP cabling is attached	
	Amber		properly.	
	Green	On	The LAN port's 2500 Mbps link is active.	
	0.001	Blinking	Data is being transmitted at 2500 Mbps.	
LAN4/5	Amber	On	The LAN port's 10/100/1000 Mbps link is active.	
		Blinking	Data is being transmitted at 10/100/1000 Mbps	
	Green/	Off	The LAN port is inactive.	
	Amber	2	- P	

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.
PWK	Green	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.

ΝΟΤΕ

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 <u>Reset Button Active Duration</u> 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.

0/3
0/3
8
0/6
8
0 / 63
1

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.

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.

ch for a function Device Information		2024-10-26 23:59:28 C	System Information	2024-10-26
ice Summary Product Model TAP-M310R-US	Country/Region		Device Name moxa-tap-m310r	Location
tem Yirmware Version v1.0 Build 2024_1024_0709	Bootloader Version v1.0 Build 2024_1007_1139		Description TAP-M310R	
FI MAC Address 00:90:E8:8A:87:9B	Serial Number		Operation Mode Disabled	Device Unique Key Last Updated on
ts 🗸 🗸				
er 2 Switching		2024-10-26 23:59:28 C	Security Status	2024-10-26
onfiguration Current Time	System Uptime			
work Service	0d0h9m1s		0 / 17	2/7
ting and NAT V Default Gateway	Netmask		High Risk	Medium Risk
wall V IPv4 Address	24 (255.255.255.0)			
tificate Management 192.168.127.253			5/6	
urity 🗸			J / O	
pnostics 🗸 🗸			LOW MUR	

- 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.

2024-10-27 00:18:57	System Information	2024-10-27 00:18:57 C		Device Information
Location	Device Name moxa-tap-m310r		Country/Region XX	Product Model TAP-M310R-US
	Description TAP-M310R		Bootloader Version v1.0 Build 2024_1007_1139	Firmware Version v1.0 Build 2024_1024_0709
Device Unique Key Last Updated on	Operation Mode Disabled		Serial Number	MAC Address 00:90:E8:8A:87:9B
2024-10-27 00:18:58	Security Status	2024-10-27 00:18:58 C		System Status
			System Uptime 0d0h28m30s	Current Time 2024-10-27 00:18:58
2/7	0 / 17			External Storage
Medium Risk	High Risk		Netmask 24 (255.255.255.0)	Default Gateway
	5/6			IPv4 Address 192.168.127.253
	Low Risk			
_				
VIEW DETAILS				

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.

Device Information	2024-10-27 00:21:07 C
Product Model TAP-M310R-US	Country/Region XX
Firmware Version v1.0 Build 2024_1024_0709	Bootloader Version v1.0 Build 2024_1007_1139
MAC Address 00:90:E8:8A:87:9B	Serial Number

System Information

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

System Information	2024-10-27 00:21:57 C
Device Name moxa-tap-m310r	Location
Description TAP-M310R	
Operation Mode Disabled	Device Unique Key Last Updated on

System Status

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

System Status		2024-10-27 00:22:57 C
Current Time 2024-10-27 00:22:57	System Uptime 0d0h32m30s	
External Storage		
Default Gateway 	Netmask 24 (255.255.255.0)	
Pv4 Address 192.168.127.253		

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.

Security Status	2024-10-27 00:23:08 C
0 / 17 High Risk	2/7 Medium Risk
5 / 6 Low Risk	
	VIEW DETAILS ->

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.

evice Name *	
noxa-tap-m310r	
	/
	14 / 255
ocation	
	0 / 255
escription	
AP-M310R	
	1
	9 / 255
Contact Information	
	0 / 255

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 (<u>www.moxa.com</u>) to the local host.

Firmware Upgrade

Running Firmware Version v1.0.2 Build 2025_0218_1515	
Uploaded Firmware Version	
Source *	
Select File *	
UPLOAD UPGRADE	

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

Uploaded Firmware Version

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

Select File

Setting	Description	Factory Default
Soloct the firmware file	Click the browse icon and navigate to the firmware file on the	Nono
Select the firmware file	local host.	NULLE

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.

Firmware Upgrade

TFTP does not support user authentication and sends all data in cleartext. We recommend using another method.

Running Firmware	e Version		
v1.0.2 Build 2	025_0218_15	15	
Uploaded Firmwa	re Version		
Source *			
TFTP	*		
Server IP Add	ress *	Filename *	
-		-	0/256
UPLOAD	UPGRADE		

Running Firmware Version

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

Uploaded Firmware Version

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

irmware Upgra	de	
Running Firmware Version v1.0.2 Build 2025_0218_1	515	
Uploaded Firmware Version		
Source * SFTP		
Server IP Address *	Filename *	0 / 256
Account *	Password *	ø
UPLOAD UPGRADE		

Running Firmware Version

Setting	Description	Factory Default
Current firmware version number	This shows the current running firmware version.	Current running version
Uploaded Firmware V	'ersion	
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 Backup and Restore

Backup	Restore
Configuration Source *	
Running Configuration	•
Storage Location *	
Local	•
Local Configuration Password *	۔ ک
	0 / 64
Configuration Password *	

Configuration Source

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

Storage Location

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

Configuration Password

Setting	Description	Factory Default
	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 Ba	ackup an	nd Restore	
Backup	Restore		
TFTP does not support use	er authenticatio	on and sends all data in cleartext. We recommend usi	ng another meth
Configuration Source * Running Configuration	Ŧ		
Storage Location *			
TFTP	×		
Server IP Address *		Filename *	
Configuration Password *	Ø		
Minimum of 8 character Signature *	0 / 64		
Enabled	•		
BACK UP			
onfiguration Source			
etting Do	escription		Factory Defau
	· ·		Running

Running Configuration	Back up the running configuration.	Running
Startup Configuration	Back up the start-up configuration.	Configuration
Storage Location		

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

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

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.

Backup	Restore		
Configuration Source * Running Configuration	Ŧ		
Storage Location *			
SFTP	-		
Server IP Address *		Filename *	
			0 / 256
Account *		Password *	Ø
Configuration Password	ø *		
Minimum of 8 character	0 / 64		
Signature *			
Enabled	-		

Configuration Source

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

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

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

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

Signature

bigilatare				
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

Configuration Backup and Restore

Backup	Restore	
Source *		
Local	•	
Select File *		
Configuration Password *	ø	
Minimum of 8 character	0 / 64	
Verify CA Chain *		
Enabled	*	
RESTORE		

Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	
TFTP	Restore the configuration from a backup file via TFTP.	Local
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
	Enter the configuration password. You will need to enter this password when importing the backup file.	None
Configuration Passwo	rd	Eastory Default

Setting	Description	Factory Default
Configuration password	Enter the configuration password. You will need to enter this	None
configuration password	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	Enabled
Lindbled/Disabled	restored configuration.	LIIdbieu

When finished, click **RESTORE**.

TFTP Server

Configuration Backup and Restore Backup Restore TFTP does not support user authentication and sends all data in cleartext. We recommend using another method.

Source *			
TFTP	•		
Server IP Address *		Filename *	
			0 / 256
Configuration Password *	8		
Minimum of 8 character	0/64		
Verify CA Chain *			
Enabled			

Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	
TFTP	Restore the configuration from a backup file via TFTP.	Local
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	Factory Default	
Configuration passwo	Enter the configuration password. You will need to enter this	None
configuration passwe	password when importing the backup file.	None
Verify CA Chain		
Setting	Description	En atoms Defecult
Setting	Description	Factory Default

When finished, click **RESTORE**.

SFTP Server

Backup	Restore		
Source *			
SFTP	•		
Server IP Address *		Filename *	
			0 / 256
Account *		Password *	Ø
Configuration Passw	vord * 🔌		
Minimum of 8 character	0 / 64		
Verify CA Chain * Enabled	•		

restored configuration.

Source

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

Server IP Address

Setting	Description	Factory Default
SETP server address	Enter the IP address of the SFTP server where the new	None
	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	None				
Password					
Setting	Description	Factory Default			
SFTP server password	None				
Configuration Passwo	rd				
Setting	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.

ast Boot-u	р		
Status * Disabled	•	0	If enabled, the configuration will not be regenerated when the device boots up and may pose a potential security concern.
APPLY			
atus			

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.

U	ser Ac	count				
	Settings	S	Session Management	RADIUS	;	
	∎ =,				Q Sear	ch
		Status	Username	Email		Role
	□ ∕	Enabled	admin	moxa@moxa.com		Administrator

Edit the following settings:

Create New Acc	count			
Status * Disabled	*			
Username *				
Minimum of 4 character	0/32			
New Password *	Ø	Confirm Password *	8	
Minimum of 8 character	0 / 63	Minimum of 8 character	0 / 63	
Email				
Role *				
User	*			
Authority * Account System Advanced Diagn Advitor System Diagnostics Network Status Monitorir System Backup System Manage	nostics			
			CANCEL	APPLY

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	ng Description			
Min. 8 characters	Enter the password for this account. For better protection, it is recommended to enforce stronger password complexity by enabling the following <u>Password</u> <u>Policy</u> 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	nail Enter the email address for this account.				
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)				
Engineer	Set the user's role to Engineer. (pre-defined authority)	User			
User	Set the user's role to User. (pre-defined authority)	USEI			
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
	Checking authorities giv

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 \checkmark of the account you want to edit.

Status	Username	Email	Role	Account System	Advanced Diagnostics	Auditor System	Diagnostics	Network Configuration	Status Monitoring	System Backup	System Management
Enabled	admin	moxa@moxa.com	Administrator	~	~	~	~	~	~	~	~
Enabled	test	test@example.com	User				~		~		
											÷

Items per page: 20 ▼ 1 − 2 of 2 |< < > >|

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

Edit Account			
Status * Enabled			
Username test			
New Password 🔇 🗞	Confirm Password	8	
0 / 63 Email		0 / 63	
test@example.com			
	1	6 / 318	
Role *			
Authority *			
🗌 Account System			
Advanced Diagnostics			
Auditor System			
Diagnostics			
Network Configuration			
Status Monitoring			
System Backup			
System Management			
		CANCEL	APPLY

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** \mathbf{I} icon on the top of the page.

∎₹				
	Status	Username	Email	Role
	Enabled	admin	moxa@moxa.com	Administrator
	Enabled	test	test@example.com	User
•				
Delete A	ccount			
Are you su account?	re you war	nt to delete the se	lected	
		CANCEL	DELETE	

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.

User Account								
Settings	Session Mar	nagement	RADIUS					
Username	WEB: Status	WEB: Last Login	WEB: Last Activity					
Lngineer	In Use	2024-04-18 22:32:24+00:0	2024-04-18 22:32:26+00:	00				
🗙 admin	In Use	2024-04-18 21:50:42+00:0	2024-04-18 22:32:31+00:	00				
Max 32								

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

Terminate Session				
Which active session(s) do you want to terminate?				
WEB				
MXconfig				
CANCEL 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.

User Account				
Settings	Session Management	RADIUS		
Status * Disabled	•			
APPLY				

Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable RADIUS server functionality.	Disabled
Status * Enabled	-	
---	---	--------------------------------
RADIUS Server 1 RADIUS Server Status *		
Enabled	•	
Address *		UDP Port 1812
Address		0 - 65535
Authentication Type *		0 00000
MS-CHAP-V2	•	Shared Key * 🛛 🔌
		0 / 128
Authentication Timeout * 5		Authentication Retry Count * 1
5 - 30		0 - 5
RADIUS Server 2 RADIUS Server Status *		
Disabled	-	

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

RADIUS Server Sta	tus	
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 Typ	e	
Setting	Description	Factory Default
MS-CHAPv2	Set the RADIUS authentication type to MS-CHAPv2.	
MS-CHAPv1	Set the RADIUS authentication type to MS-CHAPv1.	MS-CHAPv2
CHAP	Set the RADIUS authentication type to CHAP.	M3-CHAPV2
PAP	Set the RADIUS authentication type to PAP.	
Shared Key		
Setting	Description	Factory Default
Password	Enter the password for this RADIUS server.	None
Authentication Tim	eout	
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
	Specify the number of times the device will attempt to	
0 to 5	authenticate with the RADIUS server if no response is	1
	received.	

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.

Password Policy

Minimum Length *		
8		
8 - 63		
Password Vali	dation Rules	
Must includ	e at least one dig	jit (0-9)
Must inclue	de at least one	uppercase letter (A-Z)
Must inclue	de at least one l	owercase letter (a-z)
Must inclue	de at least one s	special character (~!@#\$%^&*l:;,.<>{[]())
Password Lifetime	*	
90		
0 - 365	day(s)	
APPLY		

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.

User	Interface

General		SSL	SSH
HTTP Status *		HTTP - TCP Port *	
Disabled	-	80	0
		1 - 43999, 45000 - 65	535
HTTPS Status *		HTTPS - TCP Port *	
Enabled	•	443	0
		1 - 43999, 45000 - 65	535
Telnet Status *			
Disabled	-		
SSH Status *		SSH - TCP Port *	
Enabled	-	22	
		1 - 43999, 45000 - 65	535
SNMP Status *			
Disabled	•		
Moxa Service Status *		Moxa Service - UDP F	Port
Enabled	-	40404	
Maximum number of concu 5	urrent lo	gin sessions For HTTP ·	+ HTTPS *
1 - 10			
Maximum number of concu 5	urrent lo	gin sessions for Telnet ·	+ SSH + Ser
1 - 10			

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

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.	
Read Only	Enable and set SNMP to read-only.	Disabled
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	5	
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 o	f 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 o	f Concurrent Login Sessions for Telnet + SSH + Serial Cons	ole	
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 ${\bf SSL}$ tab is used to check SSL certificate information, regenerate the certificate, and export the certificate request.

User Interfac	e			
General	SSL	SSH		
Certificate Inform	ation			
Certificate Issued to moxa-tap-m310r	Certificate Issue moxa-tap-m31		Certificate Expiration Date Dec 11 08:22:27 2029 GMT	
REGENERATE	EXPORT CERT. 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.	Sell-Signed

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 $\ensuremath{\textbf{SSH}}$ tab is used to regenerate the SSH key.

User Interfac	e			
General	SSL	SSH		
Regenerate SSH REGENERATE	(ey			

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.

eset Button Status * Visabled		Reset Button Activ	e Duration *
		0 - 300	sec.
Serial Status *			
Enabled	-		

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,	V1, V2c Read Community	Community string	None	Uses a community string match for authentication.
V2c	V1, V2c Write/Read Community	Community string	None	Uses a community string match for authentication.
	None	None	None	Uses an account with admin or user role to access objects.
SNMP V3	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.	
Read Only	Set SNMP as read-only.	Disabled
Disabled	Disable the SNMP.	

SNMP Version

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

Read Community (for V1/V2c Versions)

Setting	Description	Factory Default
Public/Private	public	
Read/Write Comr	nunity (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 \checkmark of the account you want to edit.

S	NMP					
	SNMP	SNMP Accoun	t List			
Ι.						
	Username	Status	SNMP Status	Authority	Authentication Type	Encryption Method
	admin	Enabled	Disabled	Read Write	None	None

Configure the following settings:

Edit SNMP Acc	ount Settings		
Username			
admin			
SNMP Status *			
Enabled	•		
Authority			
Read/Write	•		
Authentication Type			

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.	Redu/ White	
Authentication Type			
Setting	Description	Factory Default	
None	No authority type selected.		
MD5	Specify MD5 as the authority type. None Specify SHA as the authority type. Image: Comparison of the second secon		
SHA			
Authentication Pass	sword		
Setting	Description	Factory Default	
	Depending on the selected Authentication Type, specify the		
8 to 63 characters	Authentication Password. The password must be at least 8	None	
	characters long.		
Encryption Method			
Setting	Description	Factory Default	
None	No encryption method selected.		
DES	Specify DES as the Encryption Method.	None	
AES	Specify AES as the Encryption Method.		
Encryption Key			
Setting	Description	Factory Default	
	Depending on the selected Encryption Method, specify the		
8 to 63 characters	Encryption Key. The password must be at least 8 characters	None	
	long.		

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.

System Clock		Time Zor	ne	
Current Time				
2024-04-23 22:31:29	+00:0	0		
Clock Source *				
Internal Clock	•			
Date *				
2024-04-23				
Time *				
下午 10:31:29				

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	
	Set the clock source to NTP. This will sync the system clock		
NTP	with an external NTD conver		

Configure the Time and Date (Internal Clock)

with an external NTP server.

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



Time

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

Configure Time Servers (NTP)

System Time

System Clock	Time Z	one	
The service [NTP] is	unsecure. We	e recomm	end disabling it.
Current Time			
2024-04-23 22:31:29	+00:00		
Last Sync Timestamp			
Clock Source *			
NTP	•		
Time Server 1 *			
	0 / 60		
Time Server 2			
	0 / 60		
Sync Interval *			
10			
10 - 1440	min.		
APPLY			

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

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.

System Time			
System Clock	Time Zone		
Time Zone *			
UTC+00:00	▼		
Daylight Saving Daylight Saving Status *			
Disabled	•		
APPLY			

Configure the following settings:

Time	Zone
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	20116

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.

Enabled \checkmark Offset * $00:00$ Start Month *Week *Jan \checkmark 1st \checkmark Sun \checkmark 00 \checkmark End Month *Week *Jan \checkmark 1st \checkmark Sun \checkmark 00 \checkmark	Daylight Savin	-					
00:00 Start Month* Jan Ist Sun O0 End Month* Week* Day* Hour* Hour* Hour* Hour* Hour*			•				
Start Day* Hour* Jan Ist Sun 00 End Month* Week* Day*	Offset *						
Month *Week *Day *Hour *JanIstSun00End Month *Week *Day *Hour *	00:00						
Jan Ist Sun 00 End Month* Week* Day* Hour*	Start						
End Month * Week * Day * Hour *	Month *	Week *		Day *		Hour *	
Month * Week * Day * Hour *	Jan 👻	1st	•	Sun	*	00	*
	End						
Jan 🔻 1st 💌 Sun 💌 00 💌	Month *	Week *		Day *		Hour *	
	Jan 🔻	1st	•	Sun	•	00	•
	APPLY						

Daylight Saving Status

us	
Description	Factory Default
Enable or disable Daylight Saving Time.	Disabled
Description	Factory Default
Specify the offset value for Daylight Saving Time.	None
Description	Factory Default
Specify the date that Daylight Saving Time begins.	Jan, 1st, Sun, 00.
Description	Factory Default
Specify the date that Daylight Saving Time ends.	Jan, 1st, Sun, 00
	Description Enable or disable Daylight Saving Time. Description Specify the offset value for Daylight Saving Time. Description Specify the date that Daylight Saving Time begins. Description

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.

Wireless Settings					
General	MAC Cloning	Wi-Fi Connections			
Operation Mode * Disabled	•				

Configure the following settings:

Operation Mode			
Setting	Description	Factory Default	
Disabled	Disable the operation mode.		
AP	Specify the operation mode as AP. Refer to AP Mode		
Ar	Settings.		
Master	Specify the operation mode as Master. Refer to Master Mode		
Master	Settings.	Disabled	
Sniffer	Specify the operation mode as Sniffer. Refer to Sniffer Mode		
Shine	Settings.		
Client	Specify the operation mode as Client. Refer to Client Mode		
Chefit	Settings.		
Client-Router	Specify the operation mode as Client-Router. Refer to Client-		
Chefit-Roulei	Router Mode Settings.		
Slave	Specify the operation mode as Slave. Refer to Slave Mode]	
Slave	Settings.		

AP Mode Settings

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

Wireless Set	tings	
General	MAC Cloning	Wi-Fi Connections
Operation Mode * AP	Environment *	•

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.	Indoor

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.

Wireless Settings

General	MAC Cloning	Wi-Fi Connections
Operation Mode * Master	Environment *	•

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	1110001
Outdoor	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**.

General	_	MAC Cloning	Wi-Fi Co	nnections
The service [Sniffer] is uns	ecure. We recomm	end disat	bling it.
Operation Mode *		Environment *		
Sniffer	•	Indoor	•	
RF Band *				
5 GHz	•			
Security *				
None	•			
RF Settings 🔨				
5 GHz				
Channel Width *		Channel *		Bonded Channel(s)
20/40/80 MHz	*	36 (5180 MHz)	*	40, 44, 48
Antenna *		Antenna Gain		
All	-	2		
		0 - 18	dBi	

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	110001
Outdoor	vary depending on the selection.	

RF Band

Setting	Description	Factory Default
5 GHz	Select 5 GHz as the RF band.	
2.4 GHz	Select 2.4 GHz as the RF band.	5 GHz
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.	None	

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.

Vireless Set	ting	S	
General	1	MAC Cloning	Wi-Fi Connections
Security is disabled Operation Mode *	for Wi-	Fi. We recomme	end disabling this SSID.
Client	-	Indoor	•

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.	110001

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.

Vireless Settings					
General	MAC Cloning	Wi-Fi Connections			
Security is disabled f	for Wi-Fi. We recommer	nd disabling this SSID.			

Indoor

Configure the following settings:

Environment

Client-Router

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	110001	
Outdoor	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.

Vireless Se	tting	S	
General	P	MAC Cloning	Wi-Fi Connections
	_	-	
Security is disabled	d for Wi-	Fi. We recomme	nd disabling this 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.	Indoor

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 (E) icon.

SSID Setti	ngs ^				
Ð					Q Search
	SSID	RF Band	Security	Encryption	Status
□ /	Moxa-5G	5 GHz	WPA2 (Personal)	AES	Enabled
	Moxa-2G	2.4 GHz	WPA2 (Personal)	AES	Enabled
Max 9					

Configure the following settings:

0				2
SSID Status *				
Disabled	-			
		RF Band *		
SSID *		5 GHz	•	
	0/32			
RTS / CTS Threshold *				
2346				
32 - 2346	bytes			
Transmission Ra	to E C	U -		
Data Transmission Rate '		ΠZ	Min. Data Transmission Rate *	
Auto			- 0	
			0 - 65	Mbps
Broadcast/Multicast Data	a Transmis	sion Rate *	Management Transmission Rate *	
HT-MCS5			 HT-MCS5 	-

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

Minimum Data Transmission Rate

Setting	Description	Factory Default
0 to 65 Mbps	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 Transmis	ssion Rate	

	ılt
HT-MCS0 to HT-MCS15 Set the management transmission rate for the TAP-M310R. HT-MCS5	

When finished, click **NEXT**.

onfigure SSID Setting	S			
0				2
SSID Broadcast Status *				
Security * WPA2	WPA Mode * Personal	•		
Protected Management Frame * Disabled				
Encryption * AES -	EAPOL Version * 1	▼		
Passphrase *				
At least 8 characters 8 / 64 Key Renew * 3600				
60 - 86400 sec. Copy Configurations to SS	SIDs 🗸 👔			
			BACK	CONFIRM

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.		
WPA2	Use WPA2 authentication. This mode supports IEEE 802.11i		
WPAZ	with TKIP/AES + 802.1X encryption.		
WPA3	Use WPA3 authentication. This mode supports SAE		
	(Simultaneous Authentication of Equals) to avoid network	Onon	
	attacks, such as KRACK.	Open	
WPA/WPA2 Mixed	Use WPA/WPA2 Mixed authentication. This allows both WPA	7	
WPA/ WPAZ MIXEU	and WPA2 clients to connect to the TAP-M310R.		
WPA2/WPA3 Mixed	Use WPA/WPA3 Mixed authentication. This allows both WPA2	1	
WFAZ/ WFAS MIXEU	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.	
	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.	TKIP/AES Mixed

*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.	T

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

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
Kev Renew		I

		Factory Default
60 to 86400 seconds (1	Specify the interval at which the group key is renewed.	3600 (seconds)
minute to 1 day)	Specify the interval at which the group key is renewed.	Sooo (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** \checkmark icon next to the SSID you want to edit. Refer to **Create a New SSID** for more information about setting.

SID Set	tings ^				
ome of S	SIDs do not apply security type	e. We recommend disab	ling them.		
Î				م	Search
	SSID	RF Band	Security	Encryption	Status
	MoxaGuest_5G	5 GHz	OPEN		Enabled
•	• Moxa-5G	5 GHz	WPA2 (Personal)	AES	Disabled
•	Moxa-2G	2.4 GHz	WPA2 (Personal)	AES	Disabled
Max 9					

Delete an Existing SSID

To delete an existing SSID, check the SSID, then click the **Delete** \mathbf{I} icon above the table.

SID Set	ttings ^				
ome of S	SSIDs do not apply security typ	e. We recommend disab	ling them.		
Î				Q	Search
	SSID	RF Band	Security	Encryption	Status
	MoxaGuest_5G	5 GHz	OPEN		Enabled
•	Moxa-5G	5 GHz	WPA2 (Personal)	AES	Disabled
	Moxa-2G	2.4 GHz	WPA2 (Personal)	AES	Disabled
Max 9					

When prompted, click **DELETE**.

Delete SSID	
Are you sure you want to delete the s ssid?	elected
CANCEL	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.

2.4 GHz RF Type * B/G/N/AX Mixed	Ŧ			
Ohannal Width *		Observal #		Bonded Obernel/e
Channel Width * 20/40 MHz	-	Channel * 6 (2437 MHz)	•	Bonded Channel(s 10
Antenna *		Max. Transmission Power *		Antenna Gain *
All	-	18		2
Beacon Interval * 100		1 - 18	dBm	0 - 18
40 - 1000	ms.			
RF Filter Bank Mode *				
Bypass	•			
CCA Mode *		Max CCA Value *		CCA Threshold *

CCA Mode *		Max CCA Value *		CCA Threshold *	
Auto	-	-40		24	
		-10040	dBm	0 - 70	dB
Fixed Rate Retry Count *		Total Retry Count *			
4		32			
1 - 10		8 - 64			
Higher Rate Probing Thre	shold *	Higher Rate Probin	g Dwell Time *		
4		75			
2 - 8	pkts	10 - 1000	ms.		

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	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.	B/G/N/AX Mixed
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.	

dBi

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

Channel	Width
Channel	TTGUI

enamer mach		
Setting	Description	Factory Default
20 MHz	Set the channel width to 20 MHz. If you are not sure which	20/40 MHz
20 14112	option to use, select 20/40 MHz.	
20/40 MHz	Set the channel width to 20/40 MHz. This is recommended.	

Channel

Setting	Description	Factory Default
• •	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	10
IO (Tead Offy)	channel width is set to 20/40 MHz.	10

Antenna

Setting	Description	Factory Default
1	Specify antenna 1 as the output antenna port.	
2	Specify antenna 2 as the output antenna port.	All
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
Bypacc	Set the RF filter bank mode to bypass. No filters will be used	
Bypass	and all data will bypass the filters.	
	Set the RF filter bank mode to auto. The system will	Bypass
Auto	automatically apply the appropriate filter based on the	
	currently used channel.	

CCA Mode

Setting	Description	Factory Default
	Set the Clear Channel Assessment (CCA) mode to Auto. In	
Auto	this mode, the system will automatically adjust the CCA value	
	to the noise floor up until the specified max CCA value.	Auto
	Set the Clear Channel Assessment (CCA) mode to Fixed. In	Auto
Fixed	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 Probi	ng 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	l Time	
Setting	Description	Factory Default
10 to 1000 (ms)	Configure the minimum period to probe a higher transmission rate.	75

For 5 GHz

5 GHz RF Type * N/AC/AX Mixed	•				
Channel Width *		Channel *		Bonded Channel(s)	
20/40/80 MHz	•	36 (5180 MHz)	*	40, 44, 48	
Antenna * All	_	Max. Transmission Powe	er *	Antenna Gain * 2	
	•				
Beacon Interval * 100		1 - 18	dBm	0 - 18	dBi
40 - 1000	ms.				
RF Filter Bank Mode *					
Bypass	•				
CCA Mode *		Max CCA Value *		CCA Threshold *	
Auto	-	-40		24	
		-10040	dBm	0 - 70	dB
Fixed Rate Retry Count *		Total Retry Count *			
4		32			
1 - 10		8 - 64			
Higher Rate Probing Thres 4	hold *	Higher Rate Probing Dwe 75	II Time *		
2 - 8	pkts	10 - 1000	ms.		

Configure the following settings:

RF Type

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

Channel Width

endimen mach		
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	Set the channel width to 20/40 MHz. This is recommended.	20/40/80 MHz
20/40/90 MH-	Set the channel width to 20/40/80 MHz. If you are not sure]
20/40/80 MHz	which option to use, select 20/40 MHz.	

Setting	Description	Factory Default
36 (5180 MHz) to 161	Select the channel from the drop-down list. Each channel	36 (5180 MHz)
5805 MHz)	supports different frequencies.	30 (3180 MHZ)
Sonded 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.	
1	Specify antenna 1 as the output antenna port.	All
2	Specify antenna 2 as the output antenna port.	
Maximum Transmissi	on power	
Setting	Description	Factory Default
	Specify the maximum transmission power which acts as a	
dBm	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
Setting	Set the RF filter bank mode to bypass. No filters will be used	Tactory Delaute
Bypass	and all data will bypass the filters.	
	Set the RF filter bank mode to auto. The system will	Bypass
Auto	automatically apply the appropriate filter based on the	Dypuss
	currently used channel.	
CCA Mode		
Setting	Description	Factory Default
	Set the Clear Channel Assessment (CCA) mode to Auto. In	
Auto	this mode, the system will automatically adjust the CCA value	
	to the noise floor up until the specified max CCA value.	
	Set the Clear Channel Assessment (CCA) mode to Fixed. In	Auto
Fixed	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
	When the CCA mode is set to Auto, configure the max CCA	
dBm	value. This value represents the upper limit the system can	-40
	adjust to depending on the current noise floor.	-
Fixed CCA Value		
Setting	Description	Factory Default
	When the CCA mode is set to Fixed, configure the fixed CCA	
	value. This value represents the static CCA value disregarding	-90
dBm		

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

Setting	Description	Factory Default
	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		
		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.

Advanced Set MTU *	tings ^		
1500			
576 - 2290	bytes		
Client			
RTS / CTS Threshold 2346	*		
32 - 2346	bytes		
Transmission R Data Transmission R		Z Min. Data Transm	nission Rate *
Auto	-	0	
		0 - 11	Mbps
	niceion Pat		
Management Transn	lission Rat		
Management Transn 11 Mbps	▼		
11 Mbps	•		
11 Mbps	• ate: 5 GHz	Min. Data Transm	nission Rate *
11 Mbps Transmission R Data Transmission R	• ate: 5 GHz	Min. Data Transm 0	nission Rate *
11 Mbps Transmission R	• ate: 5 GHz		nission Rate * Mbps
11 Mbps Transmission R Data Transmission R	ate: 5 GHz	0	

Configure the following settings:

МТИ		
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
	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
	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).

Wireless Settings

General	MAC Cloning	Wi-Fi Connections
MAC Cloning Status *		
Enabled	•	
MAC Cloning Method *		
Auto	•	
MAC Cloning Interface *		
LAN 1		

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.					
Static	The TAP client shares the assigned MAC address with multiple	Auto				
	devices connected to the LAN. This allows for multiple devices	Auto				
	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.

Wireless Settings General MAC Cloning Wi-Fi Connections AP 2024-10-29 02:08:35 🕅 C SSID ap: MOXA-5G * Noise Floor BSSID -93 dBm 46:90:E8:8A:87:9B Channel Width Channel Bonded Channel 36 (5180 MHz) 20/40/80 MHz 40, 44, 48

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.

Assoc	ciated Client List											
=,∕								Q Se	arch			
	MAC Address	IP Address	Conn. Duration	VHT Cap.	Tx. Rate (Mbps)	Chan. Width (MHz)	Data SNR (dB)	Data SS. (dBm)	Mgmt. Tx. Pkt.	Mgmt. Rx. Pkt.	Data Tx. Pkt.	Data Rx. Pkt.
									Items per	page: 5 💌	0 of 0 <	$\langle \rangle \rangle$

Click the **Filter** \equiv 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.

Wireless Settings

General	MAC Cloning	Wi-Fi Connections	
lient			2024-04-12 12:12:46
ssid M-Guest	MAC Address 00:90:E8:00:00:01	Current BSSID 00:4E:35:A1:64:B1	AP IP Address
^{Channel} 48 (5240 MHz)	Bonded Channel 44	Channel Width 20/40 MHz	
Connection Duration Dd0h0m29s	AP Has VHT Capacity No		
Transmission Rate 240 Mbps	Mgmt. SNR 56 dB	Signal Strength -42 dBm	Noise Floor -98 dBm
Mgmt. Tx. Packets 3	Mgmt. Rx. Packets 279		
Data Tx. Packets 5	Data Rx. Packets 2		

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.

Connection Management							
Connection Check and Recovery	AP-based Disconnection	Link Fault Pass-through	AeroLink Protection				
Client-to-AP Link Check Client-to-AP Link Check Status * Disabled • Remote Host Check Remote Host Check Status * Disabled •							
APPLY							

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.

Client-to-AP Link Che	ck
Client-to-AP Link Check Status *	
Enabled	r
Check Timeout *	
30	
10 - 60 se	 c.
Reset Connection Recovery *	Reset Connection Retry Count *
Enabled	- 5
	1 - 5
Reboot Recovery *	Reboot Retry Count *
Enabled	5
	1 - 5

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 R	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 Coun	t		
Setting	Description	Factory Default	
1 to 5	Specify the maximum number of times the device will reboot	5	

to attempt to recover the connection. 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.

Remote Host Check			
Enabled	•		
Host Type *			
Static	•	Host *	
Check Interval *		Check Timeout *	
30		1000	
1 - 60	sec.	100 - 1000	ms.
Retry Interval *		Retry Count *	
1		5	
1 - 30	sec.	1 - 5	
APPLY			

Configure the following settings:

Remote Host Check Status

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

Host	Туре

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

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.				
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.

Connection Manage	ment			
Connection Check and Recovery	AP-based Disconnection	Link Fault Pass-through	AeroLink Protection	
AP-based Disconnection				
SSID	SSID Status	AP-based Disconn. Status	Disconn. Threshold	Attempts
5 GHz: MOXA-5G	Enabled	Disabled	SNR: 40 dB	3
Max 9				
APPLY				

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.

Edit AP-based Disconnec	tion Setting	js	
5 GHz: MOXA-5G Status			
Enabled 👻			
Status *			
Enabled 🔹 🚺			
Attempts *			
3			
1 - 10			
Indicator of Disconnection Threshold *			
SNR	*		
5 GHz			
Disconnection Threshold (SNR) *			
40			
5 - 60	dB		
		CANCEL	APPLY

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.

Connection Management					
Connection Check and Recover	AP-based Disconnection	Link Fault Pass-through			
Link Fault Pass-Through Disabled					
Local					
Enabled -					
Ethernet Interface *					
LAN 1 👻					

Local Status

Setting	Description	Factory Default			
Enabled/Disabled	Enable or disable Link Fault Pass-through for local Ethernet interfaces.	Disabled			
LAN Port	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	
Enabled/Disabled	Enable or disable Link Fault Pass-through for links to remote	Disabled
Lilabled/Disabled	hosts.	Disabled

Remote			
Remote Status *			
Enabled	-		
orgot *			
Target *			
IPv4 Address/Host	0 / 60		
Timeout *			
1000			
100 - 1000	ms.		
Disconnection De	tection		
Interval *		Retry Count *	
1		3	
1 - 30	sec.	1 - 5	
Reconnection Det	ection		
Interval *		Retry Count *	
1		3	
1 - 30	sec.	1 - 5	

Target

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

Setting	Description	Factory Default
	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.

Connection Check and Recovery	AP-based Disconnection	Link Fault Pass-through	AeroLink Protection	
AeroLink Protection Disabled			2024-12-21 08:37:31	é c
State Disabled				
Active MAC N/A				
AeroLink Protection *				
Disabled 👻				
Management Address * 239.1.1.1				
Management Port * 5001				
1~65535				
Ethernet Interface *				
LAN 1				

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable AeroLink Protection.	Disabled
Management Addre	255	
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 Interf	ace	
Setting	Description	Factory Default
Interface	Specify the index of the Ethernet interface for AeroLink	LAN 1
	Protection.	

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			
SSID *			
AP (Enabled): Moxa-5G 🔹 🚺			
Client Isolation *			
Isolation within the same subnet			
Subnet Type *			
Static •			
Subnet Mask *			
24 (255.255.255.0) Gateway *	_		
Allowed Subnets A			
Allowed Subliets A			
Ð	Q Search		
IP / Domain Name Subnet Mask	Protocol Port	Status	
Max 8			0 of 0
APPLY			

Client Isolation

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

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 * Disabled	•		
IP / Domain Nam	e *		
Subnet Mask *	0 / 63		
32 (255.255.255.	255) 👻		
Protocol *			
All	*		

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	Specify the subnet mask.	32
(255.255.255.255)		(255.255.255.255)

Status

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

Wi-Fi ACL	
General	Accepted/Blocked List
Automatic Wi-	Fi ACL
Enabled	· 0
Wi-Fi Authentication F	Failure Retry Threshold *
1 - 10	
APPLY	

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 * Disabled	¥	
Policy Mode * Accept	Y	
٥		Q Search
+ Status	MAC Address	Q Search
	MAC Address	Q Search Items per page: 3 0 of 0 <

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			
	Choose to either block or accept connections from the MAC		

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.

CL									
eral	Accept	ed/Blocked List							
						202	4-12-22	. 09:17:	56 (
Ŧ,				Q Search					
MAC Address		Status	Note						
0:90:E8:00:01	02	Accepted	Accepted	by the Static Wi-Fi ACL.					
				Items per page: 20 💌	1 – 1 of 1	<	<	>	>
	eral MAC Address 00:90:E8:00:01:	Accept Accept	Accepted/Blocked List Accepted/Blocked List Accepted List Accepted List Accepted List Accepted List Accepted List	eral Accepted/Blocked List Accepted/Blocked List MAC Address Status Note 00:90:E8:00:01:02 Accepted Accepted	eral Accepted/Blocked List C Search MAC Address Status Note D0:90:E8:00:01:02 Accepted Accepted by the Static Wi-Fi ACL.	eral Accepted/Blocked List C Search MAC Address Status Note 00:90:E8:00:01:02 Accepted by the Static Wi-Fi ACL.	eral Accepted/Blocked List 202 202 Q Search MAC Address Status Note 202 202 <td>eral Accepted/Blocked List 2024-12-22 Q Search MAC Address Status Note D0:90:E8:00:01:02 Accepted Accepted by the Static Wi-Fi ACL.</td> <td>eral Accepted/Blocked List 2024-12-22 09:17: 2024-12-22 09:17: Q Search MAC Address Status Note 20:90:E8:00:01:02 Accepted by the Static Wi-Fi ACL.</td>	eral Accepted/Blocked List 2024-12-22 Q Search MAC Address Status Note D0:90:E8:00:01:02 Accepted Accepted by the Static Wi-Fi ACL.	eral Accepted/Blocked List 2024-12-22 09:17: 2024-12-22 09:17: Q Search MAC Address Status Note 20:90:E8:00:01:02 Accepted by the Static Wi-Fi ACL.

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** \checkmark icon on the port you want to configure.

General Port Status Port Status Port Status Description 1 Enabled 2 Enabled 3 Enabled 4 Enabled 5 Enabled	Port S	Setting	S				
1 Enabled 2 Enabled 3 Enabled 4 Enabled	Ge	eneral	Port Statu	IS			
1 Enabled 2 Enabled 3 Enabled 4 Enabled							
1 Enabled 2 Enabled 3 Enabled 4 Enabled	_						
2 Enabled 3 Enabled 4 Enabled		Port	Status	Description			
 3 Enabled 4 Enabled 	1	1	Enabled				
4 Enabled	1	2	Enabled				
	1	3	Enabled				
▶ 5 Enabled	1	4	Enabled				
	1	5	Enabled				
	Status						
Status	Enable	ed		-			
Status Enabled							
	Descr	iption					
					0/12	.7	
Enabled					C	ANCEL	APPI

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.

Advanced Settings				
MTU *				
1500				
576 - 2290	bytes			
APPLY				

мти

Setting	Description	Factory Default
,	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.

ort Set	ttings		
Genera	al	Port Status	
G			Q Search
Port	Status	Link Status	
LAN 1	Enabled	Link Up	
LAN 2	Enabled	N/a	
LAN 3	Enabled	N/a	
LAN 4	Enabled	N/a	
LAN 5	Enabled	N/a	
			1 – 5 of 5

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.

AN			
Global	Settings		
Management VLAN *			
1	rface Quick Settings		
1 Management Inte	rface Quick Settings		
1 Management Inter Management Interface LAN1	rface Quick Settings		
1 Management Inter Management Interface	rface Quick Settings	✓ Tagged VLAN	Untagged VLAN

Configure the following settings:

Management	VI AN TD
rianayement	

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	
ACCESS	device, without tags.	
	Hybrid mode is used if the port is connected to another Access	Access
Hybrid	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
11 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	Itagged devices that connect to this port and the tags that	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.

VL	AN			
	Global		Settings	
	₽ ₽,			Q Search
		VLAN	Name	Member Interface
	. /	1		LAN1, LAN2, LAN3, LAN4, LAN5, SSID-5 GHz: , SSID-5 GHz: SSID-5 GHz: Moxa-5G
	Max 256			Items per page: 5 1 − 1 of 1 < < > >

Create a New VLAN ID

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

CANCEL	CREATE
	CANCEL

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.

	Interface	Mode	PVID	Untagged VLAN	Tagged V
/	LAN1	Access	1	1	
/	LAN2	Access	1	1	
1	LAN3	Access	1	1	
ľ	LAN4	Access	1	1	
1	LAN5	Access	1	1	
1	SSID-5 GHz: Moxa-5G	Access	1	1	

Mode *		
Access	•	
PVID *		
1	Ŧ	
Tagged VLAN	.	
Untagged VLAN		
All Member VLAN		
Copy Configuratio	n to Interfaces 🔹	

Configure the following settings:

Mode

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

PVID

Setting	Description	Factory Default
1 to 4004	Set the default VLAN ID for untagged devices connected to the	1
1 to 4094	port.	T

Tagged VLAN

Setting	Description	Factory Default
11 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	None
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.

Storm Protection

Broadcast Storm Protectio Enabled	on *		
Multicast Flood Protection	۱*		
Disabled	• 1		
Unknown Unicast Protectio	on *		
Enabled	- ()		

Configure the following settings:

Broadcast Storm Protection

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

switch component will block CPU-bound unicast packets with

When finished, click **APPLY**.

Enabled/Disabled

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

an unknown destination.

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.

Enabled



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.

Turbo Chain

General		Status
	-	
Turbo Chain *		
Disabled	*	
Chain Role *		
Member	•	
Member Port 1 *		
LAN 2	*	
Member Port 2 *		
LAN 3	•	
APPLY		

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	Designate this AP as a Member AP.	Member	
Tail	Designate this AP as the Tail AP.		
Head Port/Tail Po	rt/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	



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.

Turbo Chain				
General	Status			
Chain Information				
C Turbo Chain				
Disabled				

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.

selected Chain Role

IP Configuration

General	IPv6	Status
LAN IP Mode * Static	*	
IP Address * 192.168.127.253	Subnet Mask * 24 (255.255.25	5.0) 💌 Default Gateway
DNS Server 1	DNS Server 2	

Configure the following settings:

IP Mode		
Setting	Description	Factory Default
DHCP	The TAP is assigned an IP address automatically by the	
DITCI	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
	Select the subnet mask. This is used to identify the type of	
Subnet mask	network the TAP is connected to (e.g., 255.255.0.0 for a Class	24 (255.255.255.0)
	B network, or 255.255.255.0 for a Class C network).	
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
	Enter the primary and secondary DNS server address. After	
	entering the DNS server's IP address, you can input the TAP's	
IP address	URL (e.g., http://ap11.abc.com) in your browser's address	None
	field instead of entering the IP address. The Secondary DNS	
	server will be used if the Primary DNS server fails to connect.	

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.

IP Configuration			
General	IPv6	Status	
LAN Disabled			
Static			
Dynamic			

IPv6 Mode

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

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

IPv6 Mode * Static -

IPv6 Address *	Prefix Length *
Required	0 - 128
IPv6 Gateway	
IPv6 DNS Server 1	IPv6 DNS Server 2
APPLY	

IPv6 Address

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

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.

IP Configuration

General	IPv6	Status
Disabled		
Static		
Dynamic		
Relay		Prefix Ler
DHCPv6-PD		
IPv6 DNS Server 1		IPv6 DNS
APPLY		

IPv6 Mode

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

Static •	
IPv6 Address *	Prefix Length *
Required	0 - 128
IPv6 Gateway	
IPv6 DNS Server 1	IPv6 DNS Server 2

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.

IP Configurat	tion		
General	IPv6	Status	
LAN IP Mode			
Static IP Address 192.168.127.253		Subnet Mask 255.255.255.0	Default Gateway
DNS Server 1 IP Conflict Check		DNS Server 2	
Pass IPv6 Mode Static			
IPv6 Address 2001:b011:20e0:cb8:21	11:32ff:fe88:1d16/64		
IPv6 Default Gateway		IPv6 DNS Server 2	
IPv6 DNS Server 1		IPvo DNS Server 2	

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.

Ø	

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.

Enabled	*				
IP Address : Start *	IP Address : End *				
192.168.127.59	192.168.127.77				
MAC-based IP As	signment ^				
MAC-based IP As	signment A			Q Search	
0				Q Search	
		IP Address	Status	Q Search	
0		IP Address	Status	Q Search	0 of 0

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

General	Lease Table
DHODus Conver Mode +	
Disabled	0
SLAAC + RDNSS	
Stateless DHCPv6	
Stateful DHCPv6	

DHCPv6 Server Mode

Setting	Description	Factory Default
Disabled	Disable the DHCPv6 server function.	
	Connected devices or IPv6 clients issue a Router Solicitation	
	(RS) and interpret the IPv6 Prefix, Default Gateway, DNS	
SLAAC + RDNSS	address from the Router Advertisement (RA) to compose their	
	IPv6 address parameters by combining the prefix with a self-	
	generated host ID.	
	Connected devices or IPv6 clients issue Router a Solicitation	
	(RS) and interpret the IPv6 Prefix, Default Gateway from the	
Stateless DHCPv6	Router Advertisement (RA) to compose their IPv6 address	
	parameters by combining the prefix with a self-generated host	Disabled
	ID. Subsequently it issues a DHCP Solicit and interprets the	Disablea
	DHCPv6 Advertise to extract the DNS address.	
	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	
Stateful DHCPv6	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 Somer 1/2		

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 D** icon to add a new entry.

MAC-based IPv6 Assignment

 Image: Mac Address
 Image: Q_Search

 Image: Mac Address
 IPv6 Suffix

 Max 32
 Status

Lease Table

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

DHCPv6 Se	rver	
General	Lease Table	
С ₽		Q Search
Hostname	MAC Address IPv6 Address Time Left	
		ttems per page: <u>50</u>

Click the **Refresh** $^{\mathbf{C}}$ icon to refresh the table.

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

Routing and NAT

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

Routing and NAT	^
Routing	~
NAT	

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.

Static Route

•						
	Status	Name	Destination	Netmask	Next Hop	Interface
Max 32						
APPLY						

Create Static R	oute
Entry Status *	
Disabled	-
Name	
	0 / 31
Destination *	
Netmask *	
24 (255.255.255.0)	•
Next Hop	
Interface *	
WAN	•
Metric	
1 - 32766	

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.

Ro	outing Tal	ble			
	G				
	Destination	Netmask	Gateway	Interface	Metric
	192.168.0.0	255.255.255.0	0.0.0.0	LAN	0

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.

Network Address Tra	nslate					
Rule List						
NAT Global Status * Enabled -						
					Q Search	
Status Name	Description	Pri.	Mode	Protocol	WAN IP : Port	LAN IP : Port
Enabled		32	N-to-1			
Max 32					Items per page: 10 💌	1−1of1 <
APPLY						

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.

Create NAT R	ule	
Rule Status *		
Disabled	•	
Name		
	0 / 31	
Description		
		0 / 107
Priority *		0 / 127
1		
1 - 31		
NAT Mode *	•	

Configure the following settings:

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	
РАТ	Set the NAT mode to PAT (Port Address Translation).	None	
Mapping Type (1 to	1 Mode only)		
Setting	Description	Factory Default	
Single to Single	Set the mapping type to Single to Single.		
Range to Range	Set the mapping type to Range to Range.	Single to Single	
Subnet to Subnet	Set the mapping type to Subnet to Subnet.		
Mapping Type (PA1	Mode only)		
Setting	Description	Factory Default	
Single Port	Set the mapping type to Single Port.		
Multiple Ports	Set the manning type to Multiple Ports	Single Port	

Set the mapping type to Multiple Ports.

Multiple Ports

Protocol (PAT M	ode 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		
C - Him -		The second se

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** \checkmark icon next to the rule you want to edit. Refer to **Create a New NAT Rule** for more information about each setting.

	Status	Name	Description	Pri.	Mode	
	Enabled			32	N-to-1	
Edit N	AT Rule					
Rule Statu	s *					
Enabled		•				
Name						
		0 / 31				
Descrip	tion					
			0 / 127			
Priority						
32						
1 - 32						
NAT Mode						
N-to-1		-				
					CANCEL	APPLY

When finished, click **APPLY**.

View the NAT Rule Status

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

÷	=,∕							Q Search	
		Status	Name	Description	Pri.	Mode	Protocol	WAN IP : Port	LAN IP : Port
	/	Enabled	Rule 1	Rule 1 for the field site	32	N-to-1			
Max 3	2							Items per page: 10 💌	1 – 1 of 1 🛛 🛛 🕹 🔨

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

	~	
Select Visibl	le Columns	Name
	Enabled	
🗸 Enable		
🗸 Name		
🗸 Descrip	tion	
🗸 Pri.		
🖌 Mode		
V Protoco)I	
🔽 WAN IP	: Port	
LAN IP :	: Port	

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.

Layer 2 Pol	icy			
Layer 2 Firewall Status Disabled	•			
Default Action Drop	•			
Statu	ıs Pri.	Action	Src. MAC Address	Dst. MAC Address
Max 64				
APPLY				

Configure the following settings:

Layer 2 Firewall Sta	atus	
Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Layer 2 firewall function.	Disabled
Default Action		
Setting	Description	Factory Default
Setting Accept	Description Accept all packets that do not match any policy rule.	Factory Default



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:

Create Layer 2 Fi	rewall
Rule Status *	
Disabled	•
Priority *	
1	
1 - 64	
Action *	
Accept	•
Source MAC Address	
Any	
Destination MAC Address	
Any	

Rule Status

Nulle Blatus		
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 1	
	enforced first.	

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



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**.

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

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.

Layer 3	Polic	у				
Layer 3 Firewall Disabled	Status	•				
Default Action Drop		•				
+	Status	Pri.	Action	Protocol	Src. IP Address : Port	Dst. IP Address : Port
Max 64						
APPLY						

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					
Delault Action					
Setting	Description	Factory Default			
Setting Accept	Description Packets that match the policy rule will be allowed.	Factory Default			



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:
Create Layer 3 Firew	all Rule		
Rule Status *			
Disabled •			
Priority *			
1			
1 - 64			
Action *	Protocol *		
Accept -	All		
Source IP Address Any	Netmask 32 (255.255.255.255)	•	
Destination			
IP Address	Netmask		
Any	32 (255.255.255.255)	•	
		CANCEL	APPLY

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.	Accont
Drop	Packets that match the policy rule will be denied.	Accept

Protocol

Setting	Description	Factory Default
All	Filter all protocol traffic.	
ICMP	Only filter for ICMP protocol traffic.	A11
ТСР	Only filter for TCP protocol traffic.	All
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 255.255.255.255.255" refers to the sole IP addresses 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

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		
Destination		
Destination IP Address	Description	Factory Default
Destination IP Address Setting		Factory Default
Destination IP Address Setting IP address	Description	_
Destination IP Address Setting IP address Netmask	Description	_
	Description Specify the destination IP address.	Any Factory Default 32
Destination IP Address Setting IP address Netmask Setting	Description Specify the destination IP address. Description	Any Factory Default
Destination IP Address Setting IP address Netmask Setting Netmask	Description Specify the destination IP address. Description	Any Factory Default 32

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.

Certifi	cate Management							
Certificates 👔								
=,	≂v EL Q Search							
	Function	Issued to	Issued by	Start Date	Expiration Date	Signature Algorithm	Key Algorithm	Serial Number
/ 🖸	Device Data	moxa-tap-m310r	moxa-tap-m310r	Dec 22 06:38:32 2024 GMT	Dec 21 06:38:32 2029 GMT	sha256WithRSAEncryption	rsaEncryption-3072	10617C7E94C7
/ 6	HTTPS	moxa-tap-m310r	moxa-tap-m310r	Dec 22 06:38:19 2024 GMT	Dec 21 06:38:19 2029 GMT	sha256WithRSAEncryption	rsaEncryption-3072	69886DAE2AEC
/ [Syslog Server 1	moxa-tap-m310r	moxa-tap-m310r	Dec 22 06:38:31 2024 GMT	Dec 21 06:38:31 2029 GMT	sha256WithRSAEncryption	rsaEncryption-3072	24844D34FA44
/ 6	Syslog Server 2	moxa-tap-m310r	moxa-tap-m310r	Dec 22 06:38:30 2024 GMT	Dec 21 06:38:30 2029 GMT	sha256WithRSAEncryption	rsaEncryption-3072	2812CF5F0E943
/ G	Syslog Server 3	moxa-tap-m310r	moxa-tap-m310r	Dec 22 06:38:30 2024 GMT	Dec 21 06:38:30 2029 GMT	sha256WithRSAEncryption	rsaEncryption-3072	7726F82EB3BD
/ 6	Wi-Fi Client	moxa-tap-m310r	moxa-tap-m310r	Dec 22 06:38:31 2024 GMT	Dec 21 06:38:31 2029 GMT	sha256WithRSAEncryption	rsaEncryption-3072	02F8074BBF98i
/ G	Wi-Fi RSSI Report	moxa-tap-m310r	moxa-tap-m310r	Dec 22 06:38:30 2024 GMT	Dec 21 06:38:30 2029 GMT	sha256WithRSAEncryption	rsaEncryption-3072	451AC5E4EBF7
/ 6	Wi-Fi Sniffer and Wi-Fi Mirroring	moxa-tap-m310r	moxa-tap-m310r	Dec 22 06:38:29 2024 GMT	Dec 21 06:38:29 2029 GMT	sha256WithRSAEncryption	rsaEncryption-3072	342FCB6F7917I
Max 8								▶ 1 - 8 of 8

Table Field Name	Description
	The list of certificate-based authentication functions:
	Device Data
	HTTPS
Function	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.

.					Q	Search		
Function	Issued to	Issued by	Start Date	Expiration Date	Signature Algorithm	Key Algorithm	Serial Number	
Email Notification								
Syslog Server 1								
Syslog Server 2								
Syslog Server 3								
🖋 Wi-Fi Client								
🖋 WI-FI RSSI Report								



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**.

Device Security	^
Login Policy	
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.

ogin Polio.	су (
Login Message		
Login Failure Message Failed to login	2	0 / 500
User Lockout Status * Enabled Login Failure Retry Th	reshold *	15 / 500
5		
1 - 10 Lockout Period * 5	time(s)	
1 - 10	min.	
Session Lifetime * 10		
5 - 14400 APPLY	min.	

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 Th	reshold	
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.

Trusted Access		
Layer 3 Trusted Access	Layer 2 Trusted Access	
Status * Enabled •		_
MAC Address	Create L2 Trusted Access Entry Status * Enabled	
Max 20	MAC Address *	
APPLY		CANCEL APPLY

Layer 3 Trusted Access	yer 2 Trusted Access	
Status * Enabled -	Create L3 Trusted Access Entry	
٥	Status * Enabled *	
IP Address	IP Address *	
Max 20	Netmask * 32 (255.255.255.255) *	
_		CANCEL APPLY

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.

Q Search for a function	Security St	atus	
Device Summary	Feature Group * All		·
r oyuuni	C E		
😫 Layer 2 Switching 🛛 🗸	Status	Risk Level	Risk Description
IP Configuration	Ø	High	The device can be accessed through the unsecure HTTP interface.
➡ Network Service ~ ↔ Routing and NAT ~	Ø	High	The device can be accessed through the unsecure Telnet interface.
Firewall	Ø	High	The device can be accessed through the unsecure SNMP V1/V2c interface.
ିଙ୍କୁ Certificate Management	Ø	High	SNMP V3 is enabled without authentication and encryption.
🛱 Security 🔷 🗙	Ø	High	SNMP V3 is enabled with weak security.
Device Security ^	Ø	High	Syslog server is enabled without security.
Login Policy Trusted Access	Ø	High	Email notifications are enabled without security.
Trusted Access	Ø	High	The unsecure SNMP Trap/Inform V1/V2c is enabled.
Security Status	Ø	High	SNMP Trap/Inform V3 is enabled without authentication and encryption.
System Status	Ø	High	SNMP Trap/Inform V3 is enabled with weak security.

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.
	The device categorizes risks into three tiers:
Risk Level	Low: Risks vulnerable to exploitation per circumstances defined in SL3 and above.
RISK Level	Medium: Risks vulnerable to exploitation per circumstances defined in SL2.
	High: Risks vulnerable to exploitation per circumstances defined in SL1.
Riel, Descuintion	Additional details describing the risk to provide administrators with context for taking
Risk Description	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 Statistics** under **Diagnostics > Network Status** in the function tree to access this page.

twork Statistic	s									
										2022-10-11 13:14:47 🕻
C ≕∕ E.							Q	Search		
Interface	Tx. Total Bytes	Tx. Total Pkt.	Tx. Unicast Pkt.	Tx. Multicast Pkt.	Tx. Broadcast Pkt.	Rx. Total Bytes	Rx. Total Pkt.	Rx. Unicast Pkt.	Rx. Multicast Pkt.	Rx. Broadcast Pkt.
LAN 1	7441881	3359	7874	29	23	579367	3891	3675	164	54
LAN 2	2634741	725	2363	3	1	125430	983	836	118	29
SSID-5 GHz: Moxa_Guest	0	0	0	0	0	0	0	0	0	0
SSID-5 GHz: Moxa_OT	0	0	0	0	0	0	0	0	0	0
										1 - 4 of 4

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.

LDP		
Settings		Status
LLDP Status * Enabled	•	
Transmission Interval		
5 - 4095 APPLY	Sec.	

Configure the following settings:

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

Transmission Interval

		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.

Settings	Status						
						Q Search	
Local Port	Nbr. System Name	Nbr. System Description	Nbr. System Capability	Nbr. Chassis ID	Nbr. Management Address	Nbr. Port ID	Nbr. Port Description
LAN 2		-	()	9c:eb:e8:b1:2c:27		9c:eb:e8:b1:2c:27	

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.

Bridge Table					
C E					
MAC Address	Interface	Aging Timer (sec.)			
00:00:02:00:00:00	SSID: .M-Guest	44.55			
00:02:E7:06:EE:27	SSID: .M-Guest	11.45			
00:02:E7:09:7B:4A	SSID: .M-Guest	18.78			
00:90:E8:A7:79:8E	Local	0.00			
9C:EB:E8:B1:2C:27	LAN 2	0.04			

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.

ARP Table	
C I	
IP Address	MAC Address
192.168.0.40	02:11:32:2B:C2:05
192.168.0.10	D8:BB:C1:08:6B:BD
192.168.0.1	00:11:32:88:1D:17
Max 1024	

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.

C 1	if ER					
						Q Searc
Index	Bootup Number	Severity	Timestamp	Uptime	Group	Message
1	2	Notice	2022-10-11 13:20:07.397128	0d00h17m52s	System	Configuration saved successfully. (User: admin, IP: 192.168.127.2, Interface: HTTPS)
2	2	Notice	2022-10-11 13:20:07.204867	0d00h17m51s	System	Device configuration was changed. (User: admin, IP: 192.168.127.2, Interface: HTTPS)
3	2	Notice	2022-10-11 13:18:50.952219	0d00h16m35s	Wi-Fi	[.M-Guest] Installed key successfully for the AP [7c:57:3c:2e:ba:12].
4	2	Notice	2022-10-11 13:18:50.951461	0d00h16m35s	Wi-Fi	[.M-Guest] Successfully connected to AP [7c:57:3c:2e:ba:12].
5	2	Notice Notice		0d00h16m35s 0d00h16m35s	Wi-Fi Wi-Fi	[.M-Guest] Successfully connected to AP [7c:57:3c:2e:ba:12].

Registered Logs

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

Event Log			
Log List	Registered Logs	Oversize Action	Backup
Group Name	Status	Action	
🖍 Wi-Fi	Enabled	Local, Syslog	
Network	Enabled	Local, Syslog	
🖍 System	Enabled	Local, Syslog	
Account	Enabled	Local, Syslog	
Configuration	Enabled	Local, Syslog	
Power	Enabled	Local, Syslog	

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

Edit Event Log Registration	
Group Name	
Wi-Fi	
Log Registration Status *	
Enabled	
Action *	
Local, Syslog 👻	
	CANCEL APPLY

Configure the following settings:

Log Registration St	tatus		
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	ocal Save the event logs locally.		

When finished, click **APPLY**.

Oversize Action

Syslog

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.

Event Log			
Log List	Registered Logs	Oversize Action	Backup
Oversize Action * Overwrite the oldest Capacity Warning Status * Disabled	event log 👻		

Send the event logs to a Syslog server.

Configure the following settings:

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

Local, Syslog

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.

Log List	Registered Logs	Oversize Action	Backup
prage Location *			
ocal	* &		
ocal			
ocal	* &		

Storage Location

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

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 (f	or SFTP only)	
Setting	Description	Factory Default
IP address	Enter the IP address of the SFTP server.	None
		None
Pathname (for SFTP		None
Pathname (for SFTP Setting		Factory Default
•	only)	
Setting Pathname	only) Description Specify the file path on the SFTP server for storing the event log backup.	Factory Default
Setting Pathname Account (for SFTP on	only) Description Specify the file path on the SFTP server for storing the event log backup.	Factory Default
Setting	only) Description Specify the file path on the SFTP server for storing the event log backup.	Factory Default
Setting Pathname Account (for SFTP on Setting	only) Description Specify the file path on the SFTP server for storing the event log backup. hy) Description Enter the SFTP server account name.	Factory Default None Factory Default
Setting Pathname Account (for SFTP on Setting Account name	only) Description Specify the file path on the SFTP server for storing the event log backup. hy) Description Enter the SFTP server account name.	Factory Default None Factory Default

d	
Description	Factory Default
Enter the encryption password for event log backups.	None
Description	Factory Default
Enable or disable digital signature verification.	Enabled
	Description Enter the encryption password for event log backups. Description

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.

Event Notifications

		(Q Search	
Group	Event Name	Status	Severity	Notification Method
🖍 System	Cold start	Enabled	Critical	Trap, Email
🖍 System	Warm start	Enabled	Notice	Trap, Email
🖍 System	Configuration changed	Enabled	Notice	Trap, Email
🖍 System	Reaching log capacity	Enabled	Warning	Trap, Email
Power	Power 1 turned on	Enabled	Notice	Trap, Email
Power	Power 1 turned off	Enabled	Notice	Trap, Email
🖍 Wi-Fi	Client joined	Enabled	Notice	Trap, Email
🖍 Wi-Fi	Client left	Enabled	Notice	Trap, Email

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

Edit Event Noti	fication	
Event Name		
Cold start		
Event Notification Status	*	
Enabled	•	
Notification Method		
Trap, Email	•	

Configure the following settings:

Event Notification Status				
Setting	Description	Factory Default		
Enabled/Disabled	Enable or disable notifications for this event.	Enabled		
Notification Metho				
	-			
Setting	Description	Factory Default		
	-	Factory Default		

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.

General	A	uthentication	
Syslog Status *		Event Reporting Severity *	
Disabled	•	Informational	•
Syslog Server 1			
Syslog Server Status *		Security *	
Disabled	•	None	•
Syslog Server 2			
Syslog Server Status *		Security *	
Disabled	•	None	•
Syslog Server 3			
Syslog Server Status *		Security *	
Disabled	-	None	-

Configure the following settings:

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

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

Syslog Server 1 Sta	tus	
Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the first syslog server.	Disabled

Syslog Server 2 Sta	ntus	
Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the second syslog server.	Disabled
Syslog Server 3 Sta	itus	
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.	None

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.

NMP Tr	ap/Inform		
General	SNMP Trap	/Inform Account	
Ð			
	Recipient IP/Name	Mode	Trap Community
Max 2			
	m Cottingo		
SNMP Infor Inform Retry *	m settings		
3			
1 - 99			
Inform Timeout *			
10			
1 - 300	sec.		

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.

Create SNM	IP Trap/Info	orm Recipier	nt	
Recipient IP/N	lame *			
	0 / 60			
Mode *				
Disabled	-			
			CANCEL	APPLY

Configure the following settings:

Recipient IP/Name		
		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.	
Trap V1	Set the trap version to Trap V1.	
Trap V2c	Set the trap version to Trap v2c.	Disabled
Inform V2c	Set the inform version to Inform V2c.	Disabled
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	Description	ractory berault

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 I** icon to create a new entry.

SI	SNMP Trap/Inform						
	General		SNMP 1	Frap/Inform Account			
		Usernar	ne	Authentication Type	Encryption Method		
	Max 1						

Configure the following settings:

0/32			
•			
	0 / 32	0/32	0/32

Username

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

Authentication type				
Setting	Description	Factory Default		
None	Do not use any authentication mechanism.			
TLS	Use TLS as the authentication type.			
SHA-1	Use SHA-1 as the authentication type.	Neze		
SHA-256	Use SHA-256 as the authentication type.	None		
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) Description **Factory Default** Setting Enter the authentication password. 8 to 64 characters None

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

Setting	Description	Factory Default
None	Do not use any encryption.	
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.

Email Settings

General	А	uthentication			
Email Server					
Email Server	0/60				
SMTP - TCP Port 25	0700				
0 - 65535 Authentication Status *					
Disabled	•	Username		Password	Ø
Security *			0 / 64		0 / 256
None	-				
Sender Email Address					
1st Email Recipient		2nd Email Recip	pient	3rd Email Recip	pient
4th Email Recipient		5th Email Recip	ient		
		-			
APPLY					

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 Statu	IS	
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

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

Sender Email Address

Setting	Description	Factory Default
Email address	None	
1st to 5th Email Ad		
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.

Channel Scan

RF Band *	•
ANALYZE	

Configure the following setting:

RF Band

Setting	Description	Factory Default
5 GHz	Scan the 5 GHz RF band.	
2.4 GHz	Scan the 2.4 GHz RF band.	None
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 Analyze	Result: 5GHz		
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.

Wi-Fi Mi	rrorir	ng	
Mirroring Typ	pe *	•	
Mirroring Pe	riod *	min.	1

Configure the following settings:

Mirroring Type		
Setting	Description	Factory Default
Local	Select Local to mirror traffic to the local storage on the device.	
	Select Remote to have the TAP act as a server to be used with	None
Remote	a capturing tool such as Wireshark to capture the mirror	None
	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	Authentication	
Status *		
Disabled	*	
Recipient		
TCP/UDP Port 40405	1	Vhen using TLS security, reporting will se TCP, otherwise it uses UDP.
0 - 65535		
Reporting Interval * 50		
50 - 500	ms.	
Security *		
None	*	

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
10 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**.

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.

System Data Collection

One Key Info.	Data Collection
File Password *	Ø
1 - 64	
Storage Location *	•
DOWNLOAD	

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.		
TFTP	The file will be downloaded to a TFTP server.	None	
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 (fo	or 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.

system Data Collection				
One Key Info.	D	ata Collection		
Interval *				
1 - 30	sec.			
		Stop Time		
Stop Date *	Ē	01:00 AM		
Select the informatio	on to c	collect*		
Wi-Fi Connection				
Wi-Fi Tx/Rx				
System				
START STOP	0			

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 Locatior	1		
Setting	Description	Factory Default	
Local	The file will be downloaded to the local storage on the TAP.		
TFTP	P The file will be downloaded to a TFTP server.		
SFTP	The file will be downloaded to an SFTP server.		
Server IP Addres	ss (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 informat	ion to collect				
Setting	Description	Factory Default			
Wi-Fi Statistic					
Wi-Fi Connection					
Wi-Fi Tx/Rx	Calact the types of information you want to callect	None			
Network	Select the types of information you want to collect.	none			
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.

Diagnostic Support			
Generated Acc Status Remaining Duration 	count Status		
GENERATE	DEACTIVATE		

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.

Ping

Target *					
IPv4 Address/Host					
Ping Interval *		Stop Method *		Rounds *	
1		Rounds	-	3	
1 - 30	sec.			3 - 86400	

Configure the following settings:

Description	Factory Default	
ne Enter the IP address or hostname you want to ping.	None	
Description	Factory Default	
Specify the interval at which the TAP will ping the host.	1	
Description	Factory Default	
Specify Rounds as the stop method.	Rounds	
Specify Timestamps as the stop method.		
nds Method only)		
Description	Factory Default	
Specify the round value.	3	
nestamps Method only)		
Description	Factory Default	
Specify the date when to stop pinging the IP address or hostname.	None	
	Description Specify the interval at which the TAP will ping the host. Description Specify Rounds as the stop method. Specify Timestamps as the stop method. Specify the round value. Description Specify the round value. Description Specify the round value. Specify the round value. Specify the round value.	

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 * AP	-		
Environment *			
Indoor	*		
SSID: 5 GHz			
SSID Status *		SSID *	
Enabled	-	Moxa_OT	
			7/32
Channel *		Bonded Channel(s)	
36 (5180 MHz)	*	40, 44, 48	
SSID: 2.4 GHz			
SSID Status *		SSID *	
Enabled	-	Moxa_Guest	
			10 / 32
Channel *		Bonded Channel(s)	
3 (2422 MHz)	-	7	

Operation Mode

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

Environment

Setting	Description	Factory Default
lindoor	Set the application environment to indoor. Available channels vary depending on the selection.	Indoor
luitaoor	Set the application environment to outdoor. Available channels vary depending on the selection.	110001

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
• •	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 Defa		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.	
2.4 GHz	Select 2.4 GHz as the RF band.	5 GHz
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
· · · · ·	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	None
+0/++/+0 (read only)	channel width is set to 36 (5180 GHz).	NULLE

When finished, click **NEXT**.

Wi-Fi Security

AP/Master Mode

5 GHz		
Moxa_OT		
Security * WPA2 -	Protected Management Frame * Disabled	
WPA Mode *	Encryption *	EAPOL Version *
Personal 🔹	AES 👻	1 •
Passphrase *		
At least 8 characters 10 / 64		
2.4 GHz		
The SSID does not have an	y security enabled. We reco	ommend disabling it.
ssid Moxa_Guest		
Security * Open -		
NEXT BACK		

Client/Client-Router/Slave Mode

ssid .M-Guest					
Security * WPA2	•	Protected Managemer Disabled	nt Frame * ▼		
WPA Mode * Personal	•	Encryption * AES	•	EAPOL Version * 1	•
Passphrase	Ø				
At least 8 characters	8 / 64				

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.			
WPA2	Use WPA2 authentication. This mode supports IEEE 802.11i with TKIP/AES + 802.1X encryption.	i		
WPA3	Use WPA3 authentication. This mode supports SAE (Simultaneous Authentication of Equals) to avoid network attacks, such as KRACK.	Open		
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.	
	Use TKIP/AES Mixed encryption. This option provides a TKIP	TKIP/AES Mixed
TKIP/AES Mixed*	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
TIC	Use EAP-TLS to validate the connection. This option allows the	
TLS	user to upload a TLS certificate to perform the identity check.	
	Use TTLS to validate the connection. This option requires	
TTLS	users to also specify the Anonymous Name, Username, and	TLS
	Password.	TL3
	Use PEAP to validate the connection. This option requires	
PEAP	users to also specify the Anonymous Name, Username, and	
	Password.	

When finished, click **NEXT**.

System

Device Name *			
moxa-tap-m310r			
	h		
a-z, 0-9, and dash only 14 / 2	56		
Time			
Clock Source *			
Sync With Browser	-		
Time Zone *			
UTC+00:00	-		
Daylight Saving Status *			
Disabled			
IP Configuration			
IP Mode *			
Static	-		
IP Address *	Subnet Mask *		
192.168.127.253	24 (255.255.255.0)	-	Default Gateway
DNO 0 1	DNO October 0		
DNS Server 1	DNS Server 2		
APPLY BACK			
APPLY BACK			

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

Setting	Description	Factory Default
Sync With Browser	Synchronize the system clock with the browser's clock.	
NTP	Set the clock source to NTP. This will sync the system clock with an external NTP server.	Sync With Browser
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
, j	Specify the IP or domain address of the secondary NTP server.	
NTP time server	The secondary NTP server acts as a backup in case the device fails to connect to the first NTP server.	None
Time Zone		1
Setting	Description	Factory Default
	Select a time zone.	
Time zone	Select a time zone.	UTC+00:00
		01C+00:00
Daylight Saving Tim	ne Status	
Daylight Saving Tim Setting		Factory Default
Daylight Saving Tim Setting Enabled/Disabled	Description	Factory Default
Daylight Saving Tim Setting	Description Enable or disable Daylight Saving Time.	Factory Default Disabled
Daylight Saving Tim Setting Enabled/Disabled Offset	Description	Factory Default
Daylight Saving Tim Setting Enabled/Disabled Offset Setting	Description Enable or disable Daylight Saving Time.	Factory Default Disabled Factory Default
Daylight Saving Tim Setting Enabled/Disabled Offset Setting User-specified value	Description Enable or disable Daylight Saving Time.	Factory Default Disabled Factory Default
Daylight Saving Tim Setting Enabled/Disabled Offset Setting User-specified value Start	Description Enable or disable Daylight Saving Time. Description Specify the offset value for Daylight Saving Time.	Factory Default Disabled Factory Default 00:00

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)
	B network, or 255.255.255.0 for a Class C network).	

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

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.

	Connection Status d, the assigned wireless access controller (WAC) will manage certain configuration settings of this devic be able to be changed on the device locally until the Manage via WCS feature is disabled.
mose settings will not i	be able to be changed on the device locally until the manage via wos reature is disabled.
Manage via WCS *	
Disabled	*
	—
Main-WAC IPAddress * 127.0.0.1	Register Key *
APPLY	
nable Controller-based Roamii	n
Disabled	*
APPLY	

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
IIP 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-L 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.

Connect to Wireless Controller System		
General	Connection Status	
Main WAC Connecti	on Status	
Disconnected		
Managing Primary WAC 0.0.0.0		
Managing Backup WAC		
Connection Check S	ettings	
Connection Check Interval 0		
Payload Data Size 0		
Connection Error Trigger Co continued_packet_mise		

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.

 Language Disable Auto Save Locator Reboot Reset to Defaults Renew Device Unique Key Change Password Log out 		Hi, admin 🚦
 Locator Reboot Reset to Defaults Renew Device Unique Key Change Password 		Language
 Reboot Reset to Defaults Renew Device Unique Key Change Password 	8	Disable Auto Save
 Reset to Defaults Renew Device Unique Key Change Password 	۲	Locator
Renew Device Unique Key **** Change Password	Ü.	Reboot
*** Change Password	\odot	Reset to Defaults
_	P,	Renew Device Unique Key
⊢→ Log out	***	Change Password
	[→	Log out

Locator			
Stop Mechanism			
Timer	•		
Duration *			
60			
1 - 300	sec.		
		CANCEL	START

Stop Mechanism

Setting	Description	Factory Default
Timer	Use a timer to stop the locator LEDs from blinking.	Timer
Manually	Stop the locator LEDs manually.	Timer

Duration

Setting	Description	Factory Default
1 to 300 (sec.)	Specify the duration the LEDs will be blinking for.	60

When finished, click $\ensuremath{\textbf{START}}$ to activate the LEDs.

Reboot

To reboot the TAP, click **Reboot**.

Hi, admin 🚦
Language
Disable Auto Save
Locator
Reboot
Reset to Defaults
Renew Device Unique Key
Change Password
Log out

When prompted, click **REBOOT** to reboot the TAP.

Reboot	
Are you sure you want to reboot the c	levice?
CANCEL	REBOOT

Reset to Defaults

To reset the TAP to the factory default settings, click **Reset to Defaults**.

		Hi, admin 🚦
		Language
	8	Disable Auto Save
	•	Locator
	Ü	Reboot
Į.	Ð	Reset to Defaults
l	P,	Renew Device Unique Key
	***	Change Password
IF F	[→	Log out

When prompted, check **Keep all event logs** if you want to keep the event history, then click **CONFIRM**.

Reset to Defaults	
Are you sure you want to reset the device to factory default settings?	
This will delete all your configuration settings and restore the factory defaults. This is permanent and cannot be undone.	
☐ Keep all event logs	
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.

		Hi, admin
		Language
oca	8	Disable Auto Save
-	•	Locator
	Ü	Reboot
_	\odot	Reset to Defaults
1	P,	Renew Device Unique Key
	***	Change Password
on SS	$[\rightarrow$	Log out



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 *	Ø		
	0 / 63		
New Password *	ø		
Minimum of 8 character	0 / 63		
Confirm Password *	ø		
Minimum of 8 character	0 / 63		
		CANCEL	APPLY

Current Password

Current Passworu		
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.

Log out	
Are you sure you want to log out?	
CANCEL	LOG OUT

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.

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.

Ø	

 Λ

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.

- 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.

🔁 PCo	mm Terminal En	nulator		_	\times
Profile	Port Manager	Help			
-	Open	Ctrl+Alt+O	2B HEX		

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.

Property	× Property ×
Communication Parameter Terminal File Transfer Capturing	Communication Parameter Terminal File Transfer Capturing
Protocol: Serial 💌	Terminal type: VT100 Vindow Size
Baud rate: 115200 -	Size: 80 X 25 (col x row)
User defined	History depth: 25 (unit: row)
Data bits: 8	_ Transmit
Parity: None 💌	☐ Local echo
Stop bits: 1	Send 'Enter' key as: CR-LF 👻
Flow control: TRTS/CTS TDTR/DSR XON/XOFF	Receive CR translation: No Changed
RTS state: ON COFF	LF translation: No Changed V
DTR state: ON OFF	
	Enable auto line wrap

3. The Console login screen will appear. Log into the RS-232 console with the device's account and password.

PComm Terminal Emulator - COM1,115200,None,8,1,VT100	_	×
Pro <u>f</u> ile <u>E</u> dit <u>P</u> ort Manager <u>W</u> indow <u>H</u> elp		
B COM1,115200,None,8,1,VT100		
TR RTS moxa-awk-3252a login:	^	
	~	
State:OPEN TX:0 RX:28	>	

4. The TAP-M310R Series device's CLI interface will be displayed.

PComm Terminal Emulator - COM1,115200,None,8,1,VT100	_		×
Pro <u>f</u> ile <u>E</u> dit <u>P</u> ort Manager <u>W</u> indow <u>H</u> elp			
COM1,115200,None,8,1,VT100	- • •		
Welcome [admin] The lastest successful login time via CLI was: 2021-12-03 10:57:46+00:00 moxa-awk-3252a#		^	
		~	
State: OPEN DER RT DEC Ready TX:11 RX:157		//.	



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:

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.

Run	? ×
2	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
<u>O</u> pen:	telnet 192.168.127.253
	OK Cancel Browse

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.

🞇 PuTTY Configuration		×
Category:		
E Session	Basic options for your PuTTY sess	ion
Logging — Terminal	$_{\!$	
- Keyboard	Host <u>N</u> ame (or IP address)	<u>P</u> ort
Bell	192.168.127.253	22
Features ⊡-Window Appearance	Connection type: ◯ <u>R</u> aw ◯ <u>T</u> elnet ◯ Rlogin ⓒ <u>S</u> SH	C Serial

3. The Console login screen will appear. Please refer to the previous paragraph "RS-232 Console Configuration" and for login and administration.