AWK-3251A-RCC Series User Manual

Version 1.0, July 2023

www.moxa.com/products

AWK-3251A-RCC Series User Manual

Copyright Notice

Trademarks

Disclaimer

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About This Manual

Thank you for purchasing a Moxa's AWK-3251A-RCC Series product, referred to as 'AWK Series" in this manual. 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.

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 explain the instruction on how to initialize the configuration on Moxa's product. We provide three interfaces to access the configuration settings: RS-232 console interface, SSH/Telnet CLI (Command Line Interface), and web interface.

Chapter 3: Web Interface Configuration

In this chapter, we explain how to access the Moxa AWK-3251A-RCC's 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 AWK 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 AWK Series using the command line interface, refer to the AWK Series Command Line Interface User Manual.

Symbol Definition for Web Interface Configurations

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

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

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

About Note, Attention, and Warning

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

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

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

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

> **ATTENTION**
>
> When a different type of module has been inserted into the AWK 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:

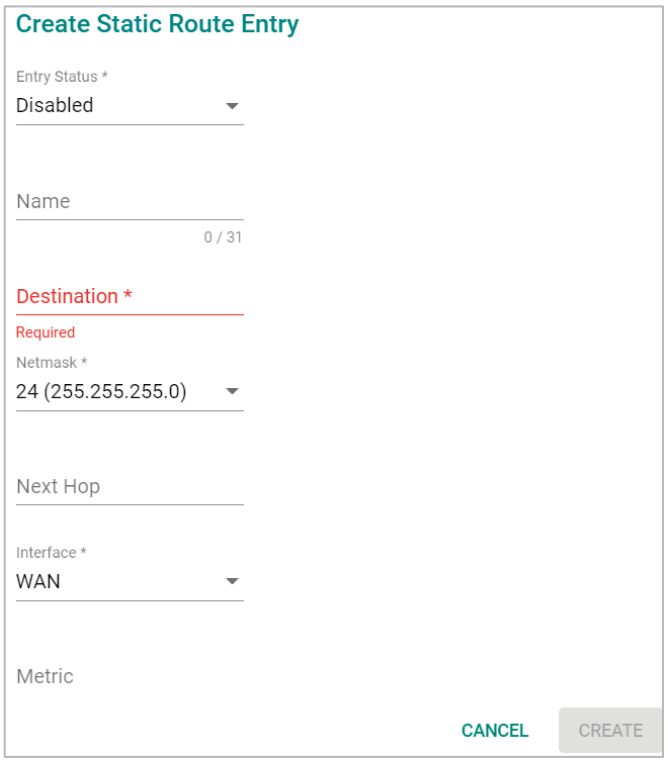
WARNING

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 AWK Series.

A: About Mandatory Parameters

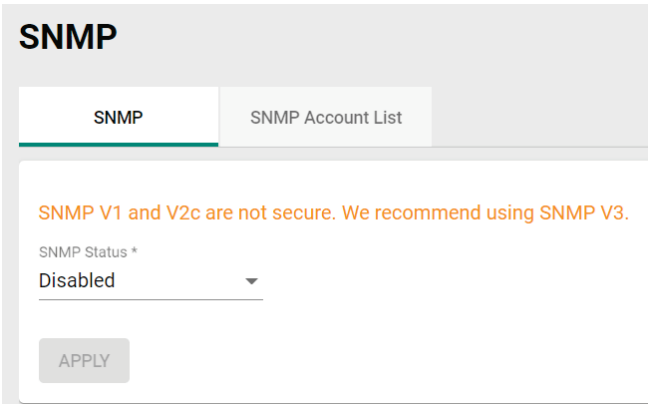


- The items with asterisks mean they are mandatory parameters that must be provided. In the figure above, the parameters for Entry Status, Destination, and Interface are required to be able to save or apply the configuration.
- If an item is marked in red means this item has been skipped. You need to fill in the parameters or you cannot apply or create the function.

In addition, some parameter values will be limited to a specific range. If the values exceed the range, it cannot be applied or created.

B: Preconfiguring Settings

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


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

2. Getting Started

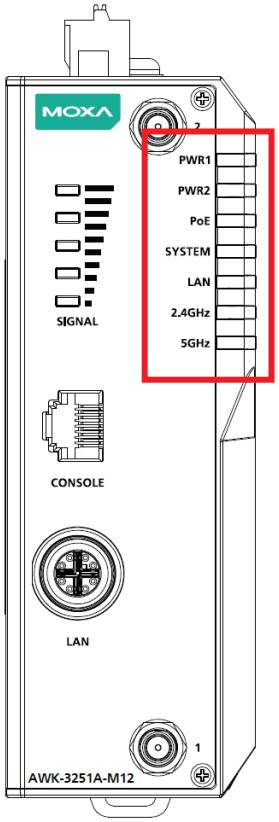
In this chapter, we provide an overview of the AWK Series, and explain how to log into the Moxa's AWK Series for the first time through the web-based interface.

Functional Design

LED Indicators

The LEDs on the front and right panels of the AWK Series provide a quick and easy means of determining the current operational status and wireless settings.

AWK-3251A-RCC Series



The following table summarizes how to read the device's wireless settings from the LED displays.

LED	Color	State	Description
PWR1	Green	On	Power is being supplied from power input 1.
		Off	Power is not being supplied from power input 1.
PWR2	Green	On	Power is being supplied from power input 2.
		Off	Power is not being supplied from power input 2.
PoE	Amber	On	Power is being supplied via PoE.
		Off	Power is not being supplied via PoE.
SYS	Red	On	System initialization failure, configuration error, or system error.
	Green	On	System startup completed and is operating normally.
LAN	Green	On	Link established on the LAN port at 1000 Mbps.
		Blinking (3 Hz)	Data is being transmitted at 1000 Mbps.
		Off	The LAN port's 1000 Mbps link is inactive.
	Amber	On	Link established on the LAN port at 10/100 Mbps.
		Blinking (3 Hz)	Data is being transmitted at 10/100 Mbps.
		Off	The LAN port's 10/100 Mbps link is inactive.
2.4GHz	Green	On	The device has established a Wi-Fi connection in a Client-related mode (Client/Client-Router/ACC Slave).
		Blinking	Data is being transmitted over the 2.4 GHz band in a Client-related mode.
	Amber	On	The device has established a Wi-Fi connection in an AP-related mode (Client/Client-Router/ACC Slave).
		Blinking	Data is being transmitted over the 2.4 GHz band in an AP-related mode.
	Green/ Amber	Off	The device is in Client/Slave/ACC Master/ACC Slave mode but no Wi-Fi connection is established, or WLAN is not working properly.
5G	Green	On	The device has established a Wi-Fi connection in a Client-related mode (Client/Client-Router/ACC Slave).
		Blinking	Data is being transmitted over the 5 GHz band in a Client-related mode.
		Off	The device has established a Wi-Fi connection in an AP-related mode (Client/Client-Router/ACC Slave).
	Amber	On	Data is being transmitted over the 5 GHz band in an AP-related mode.
		Blinking	The device is in Client/Slave/ACC Master/ACC Slave mode but no Wi-Fi connection is established, or WLAN is not working properly.
		Off	The device has established a Wi-Fi connection in a Client-related mode (Client/Client-Router/ACC Slave).
	Amber/ Green	Off	Data is being transmitted over the 2.4 GHz band in a Client-related mode.
Signal Strength (5 LEDs)	Green	On	The current signal strength (for Client/Slave/ACC Slave/ACC Master Only).
		Off	The device is in AP/Master/Sniffer mode, or no connection is established.

Beeper

The beeper emits two short beeps when the system is ready.

Reset Button

The Reset button is located on the top panel of the AWK-3251A-RCC Series. You can reboot the AWK 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 under 5 seconds and then release. The SYS LED will blink at 1 Hz.
- **Reset to factory default:** Hold down the Reset button for over 5 seconds until the SYS LED starts blinking green. Release the button to reset the AWK Series to its factory default settings. The SYS LED will blink at 4 Hz.
- **Abort the action:** Hold the Reset button down for longer than 10 seconds and then release to abort the reset action. The SYS LED will stop blinking and turn solid.

NOTE

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

Relay

The AWK-3251A-RCC Series has one relay output which is used to forward system failures and user-configured events.

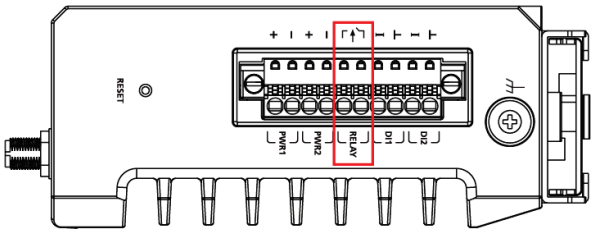
The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered.

If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the device is not powered up.

Summary of the AWK-3251A-RCC's Relay Status

Power Status	Event	Relay
Off	-	Open
On	Yes	Open
	No	Closed

The AWK-3251A-RCC relay is marked on the 2 terminal block contacts, as shown in the image below:



First-time Installation and Configuration

Before installing the AWK 3251A-RCC 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: Select the power source.

The AWK Series can be powered by a DC power input or PoE (Power over Ethernet) if applicable.

NOTE

For PoE-capable models, when both a DC and PoE power source is connected, the DC input will be the default primary power source while PoE will be secondary. Using both DC and PoE power sources at the same time does not provide seamless power redundancy. In the event the DC power source goes down, the AWK will perform a reboot to negotiate the PoE protocol before switching to the PoE source.

Step 2: Connect the AWK Series to a notebook or PC.

Since the AWK Series supports MDI/MDI-X auto-sensing, you can use either a straight-through or crossover cable to connect the AWK Series to the computer. The LED indicator on the AWK Series' LAN port will light up when a connection is established.

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

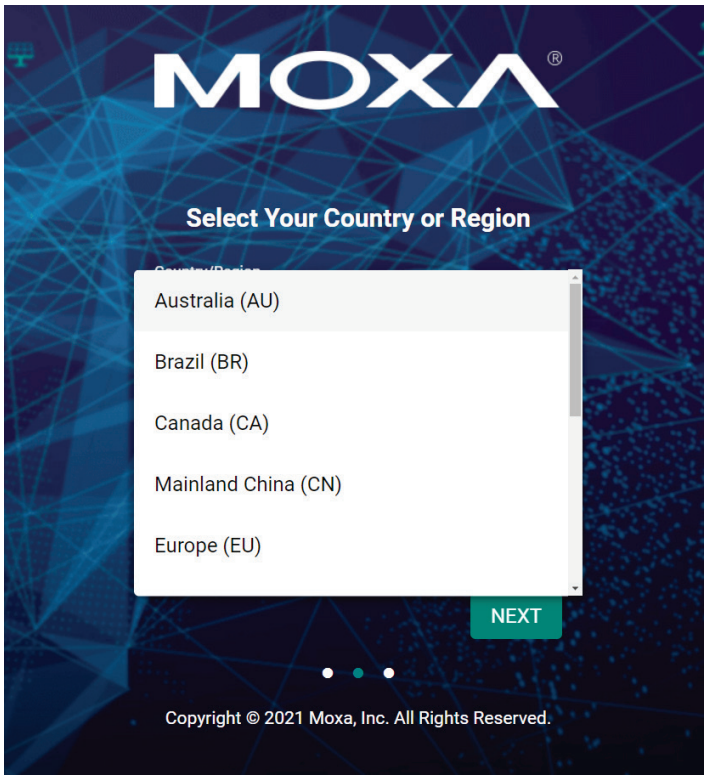
Choose an IP address on the same subnet as the AWK Series. Since the AWK Series' default IP address is **192.168.127.253**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**.

Step 4: Access the homepage of the AWK.

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

Step 5: Choose your country or region. (Not applicable to -US models)

Select your country or region from the drop-down list and click **NEXT**.

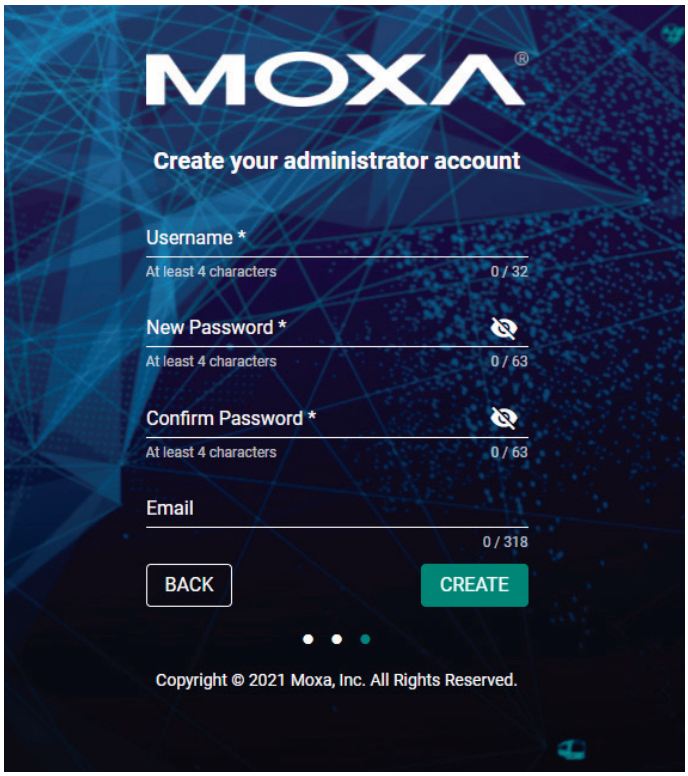


Step 6: Create a user account and password.

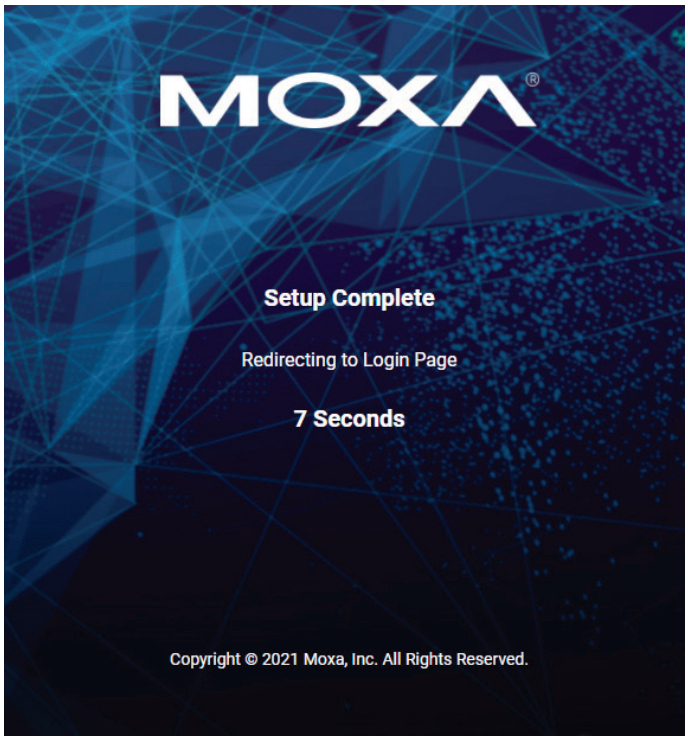
There is no default user account and password. Enter the username, password, and email address for your user account and click **CREATE**.

NOTE

The username and password are case-sensitive.



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



Step 7: Log in to the device.

Once the initialization message disappears (in red), enter your username and password and click **LOG IN**.

Communication Testing

After installing the AWK Series you can run a sample test to make sure the AWK Series and the wireless connection are functioning normally. Two testing methods are described below. Use the first method if you are using only one AWK Series device as an AP and use the second method if you are using AWK Series devices as Client and AP.

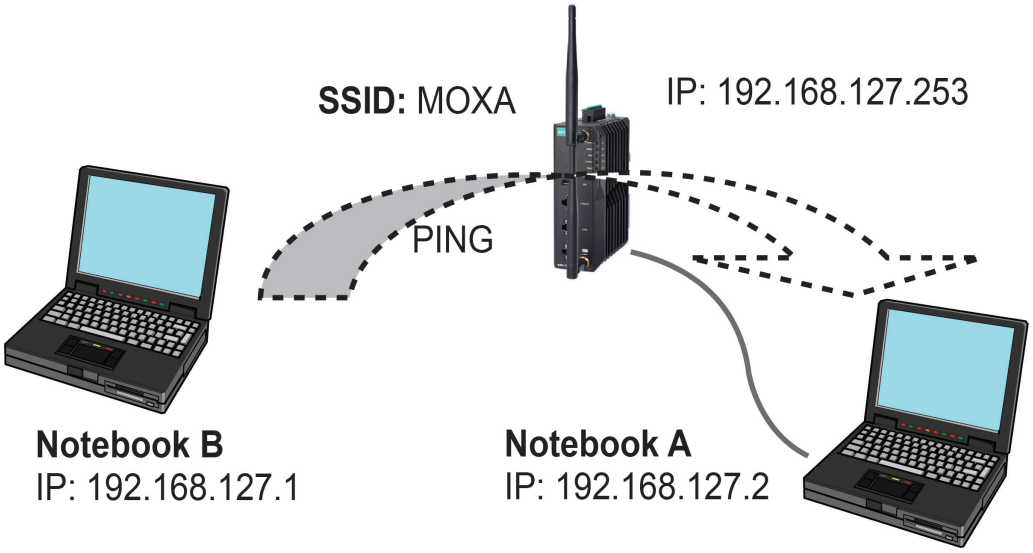
How to Test the AWK Series as an AP

If you are testing the AWK 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 AWK 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 AWK Series.

After configuring the WLAN card, establish a wireless connection with the AWK Series and open a DOS window on Notebook B. At the prompt, type

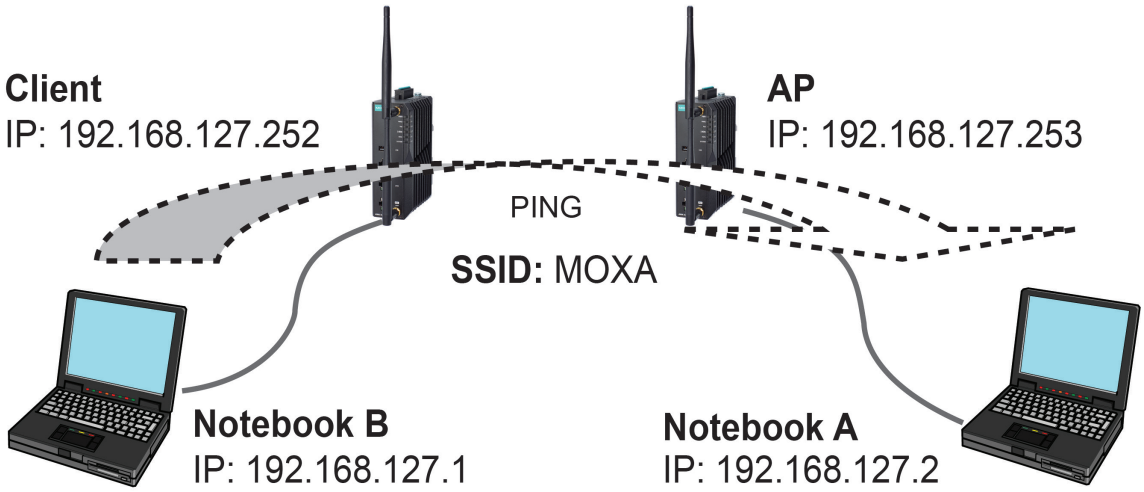
ping *<IP address of notebook A>*

and then press **Enter** (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 AWK Series as a Client

If you are testing the AWK 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 AWK Series connected to notebook B for Client mode with the correct SSID and credentials matching the target AP.



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

ping *<IP address of notebook A>*

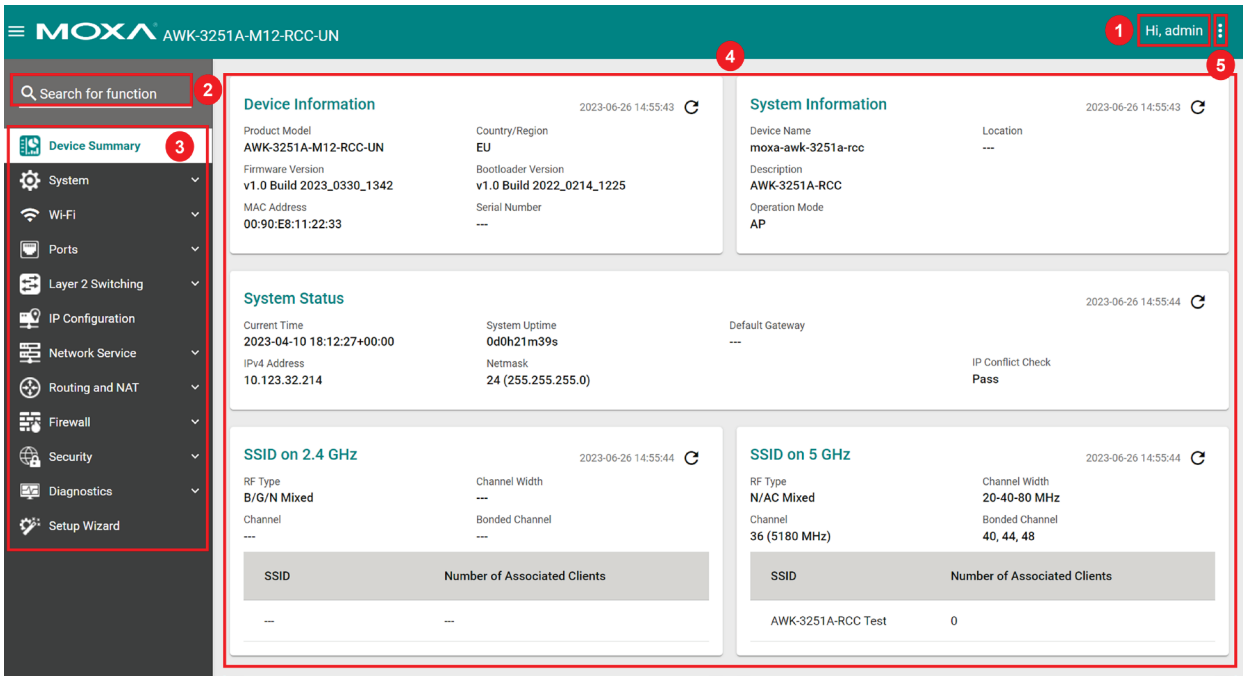
and then press **Enter**. A "Reply from IP address …" response means the communication was successful. A "Request timed out" response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.

3. Web Interface Configuration

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

Function Introduction

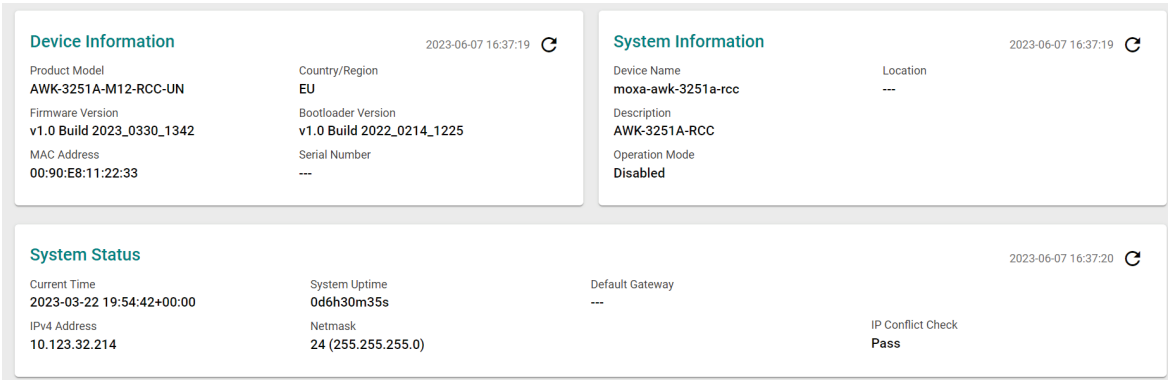
This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



1. **Login Name:** This shows the name of the user that is currently logged in.
2. **Search Bar:** Type the name of the function you want to search for in the function menu tree.
3. **Function Menu:** All functions of the AWK 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

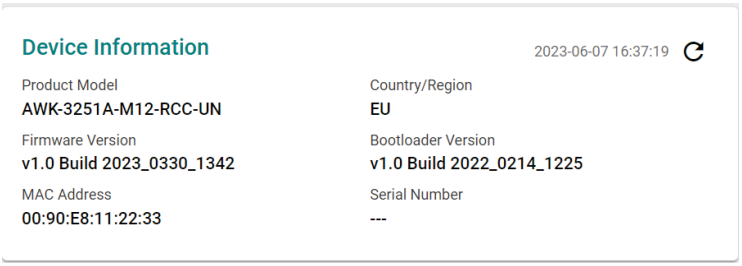
After successfully connecting to the AWK Series, the **Device Summary** will automatically appear. To view the device summary from anywhere in the interface, click **Device Summary** on the Function Menu.



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

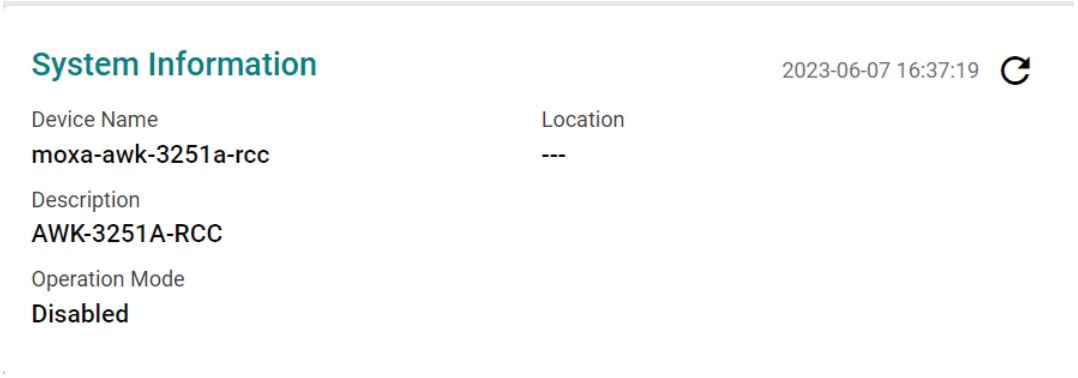
Device Information

This shows the model information, including product model name, the country or region where the device is located, and firmware version.



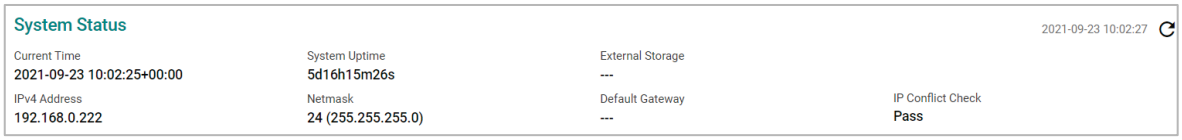
System Information

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



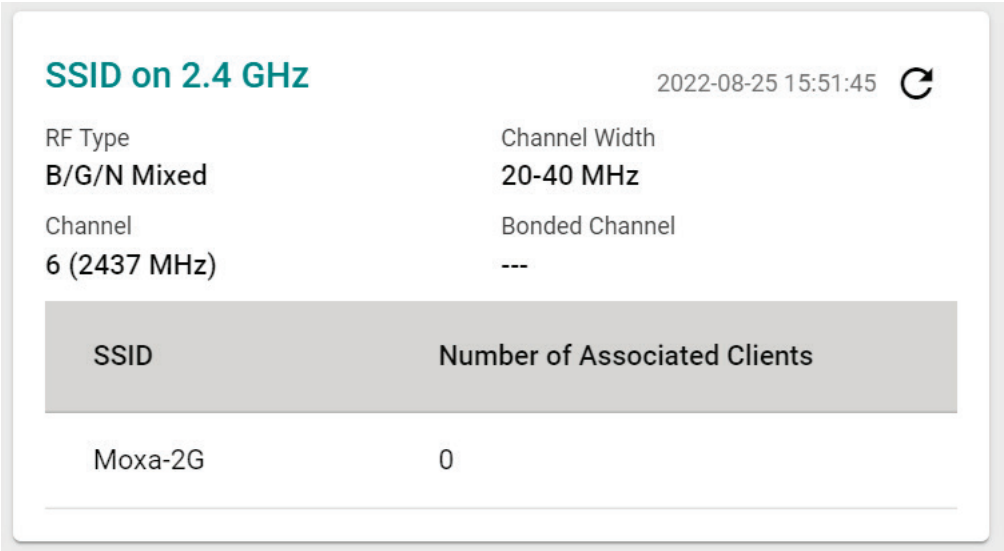
System Status

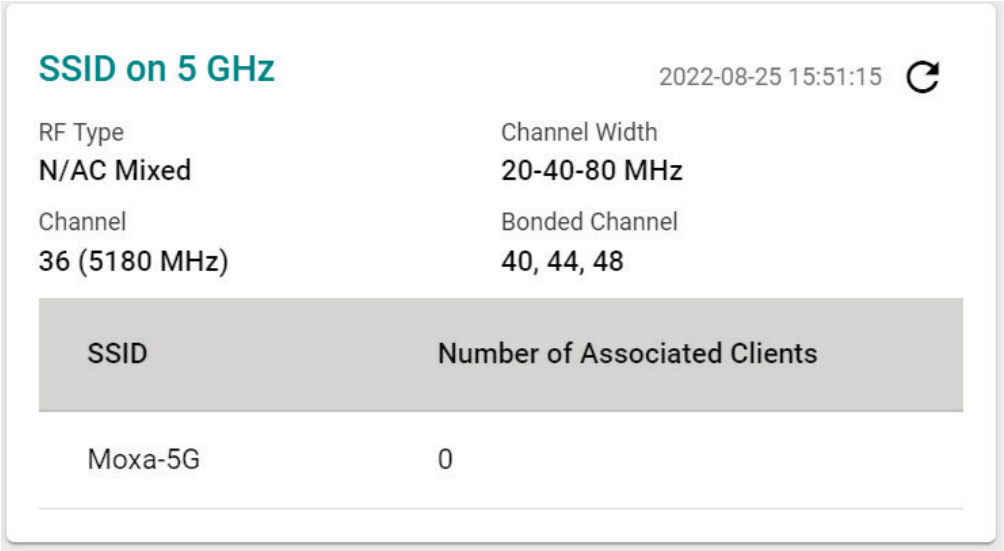
This shows the system status, including system time, system uptime, and IP address.



SSID

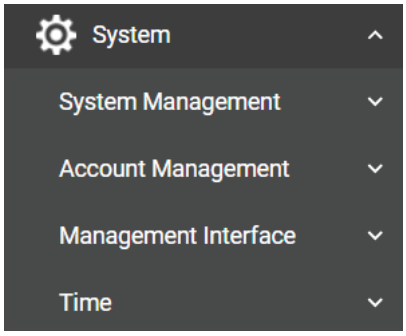
This shows information for the SSIDs configured on the AWK Series. This widget includes both the 2.4 GHz and 5 GHz bands.





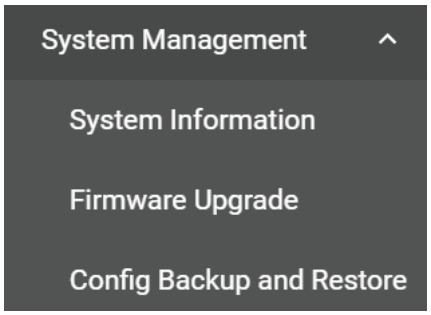
System

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.



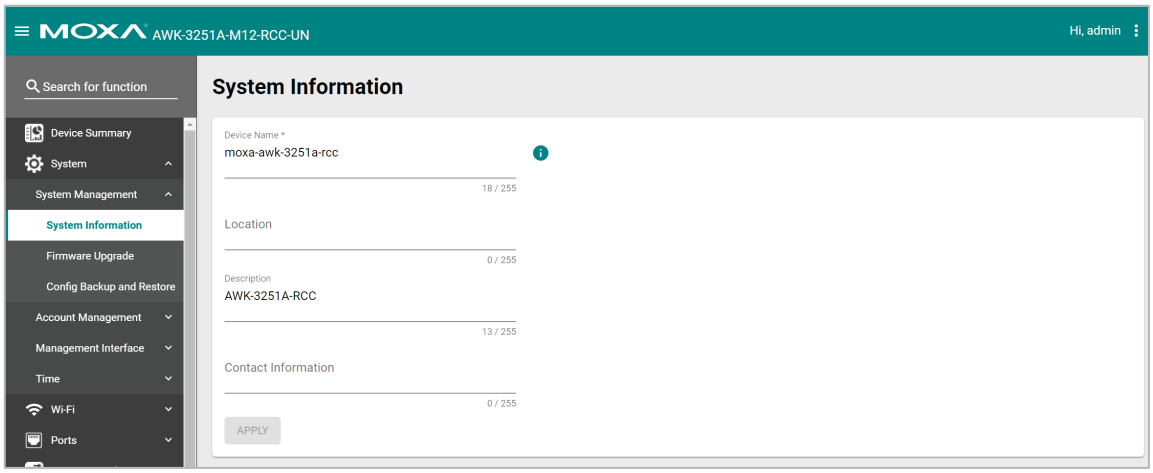
System Management

The **System Management** section houses three subsections: **System Information, Firmware Upgrade,** and **Configure Backup and Restore**.



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 AWKs that are connected to your network.



Device Name

Setting	Description	Factory Default
1 to 255 characters	Enter a name for the device. This is useful for differentiating between the roles or applications of different units. Note that the device name cannot be empty and must comply with the following naming rules: • Only supports letters (a-z), numbers (0-9), and special character dash (-) • Cannot contain spaces • Cannot start with dash (-) • Cannot end with dash (-) • When used in a PROFINET environment, cannot start with the prefix "port-x" where "x" equals 0 to 9. There is no validity to identify incorrect name formats.	moxa-awk-3251a-rcc

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.	AWK-3251A-RCC

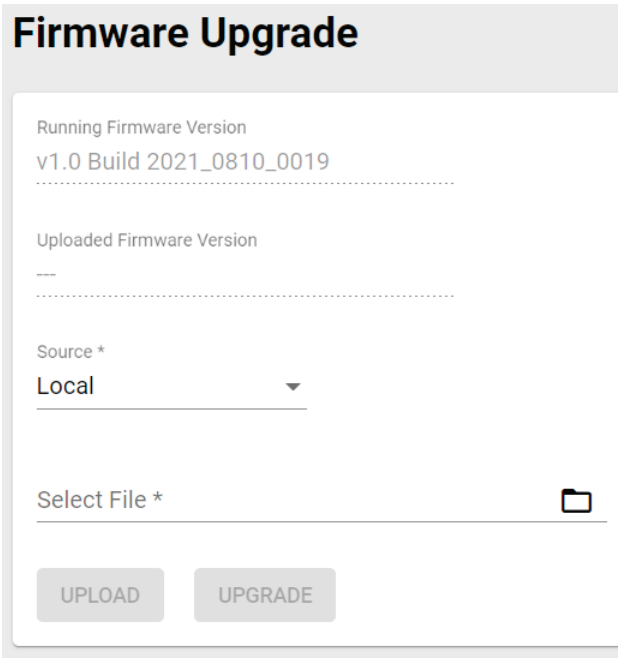
Contact Information

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.

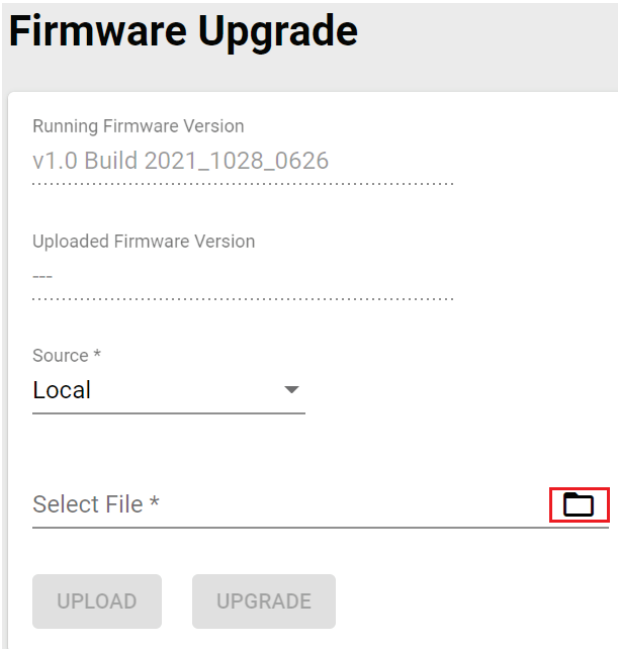
Firmware Upgrade

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



Local

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



Running Firmware Version

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

Uploaded Firmware Version

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

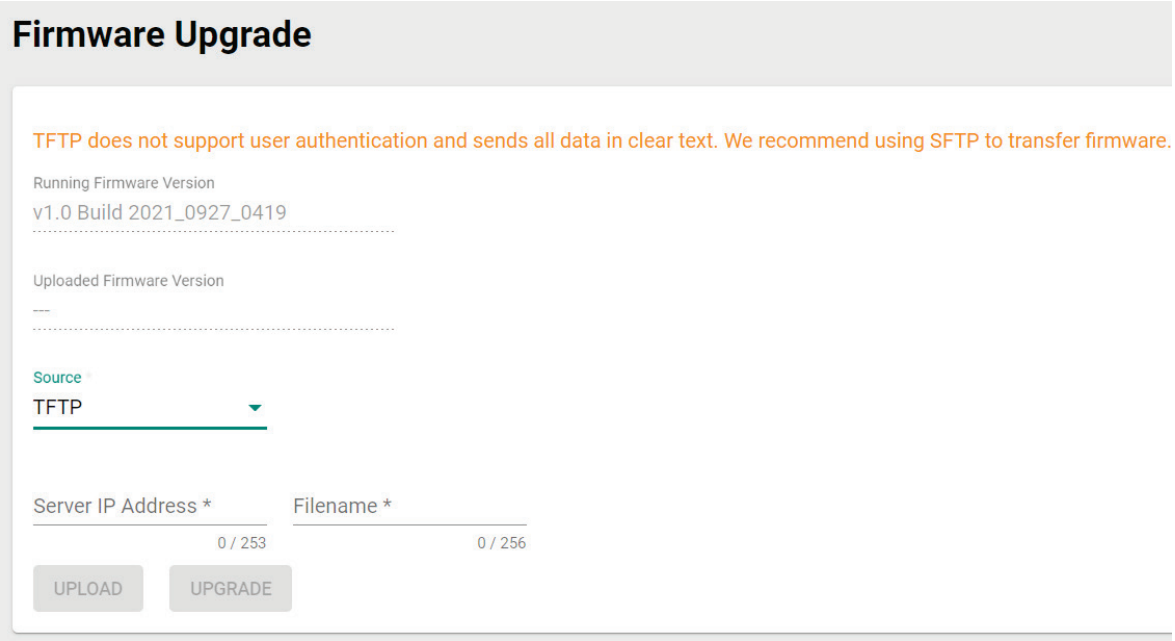
Select File

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

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

TFTP Server

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



Running Firmware Version

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

Uploaded Firmware Version

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

Server IP Address

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

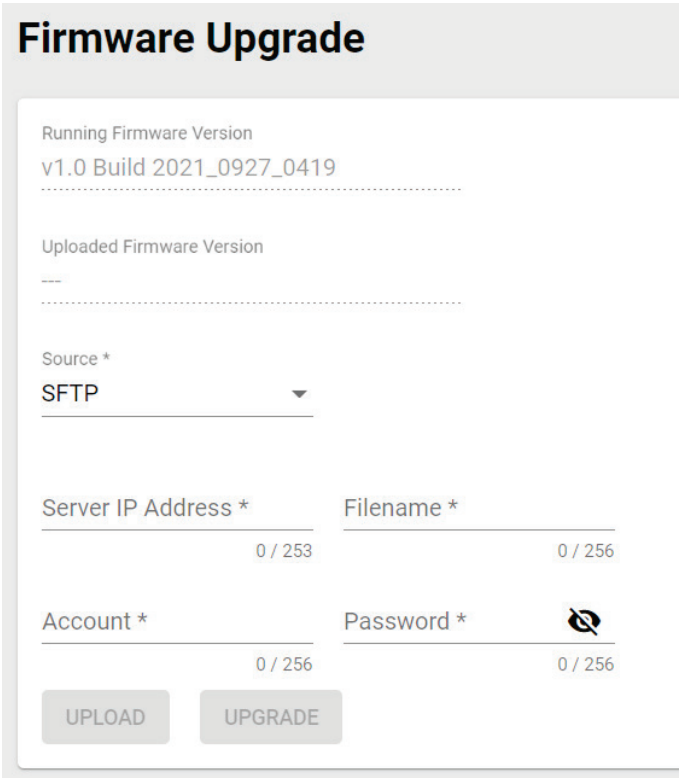
File Name

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

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

SFTP

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



Running Firmware Version

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

Uploaded Firmware Version

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

Server IP Address

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

File Name

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

Account

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

Password

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

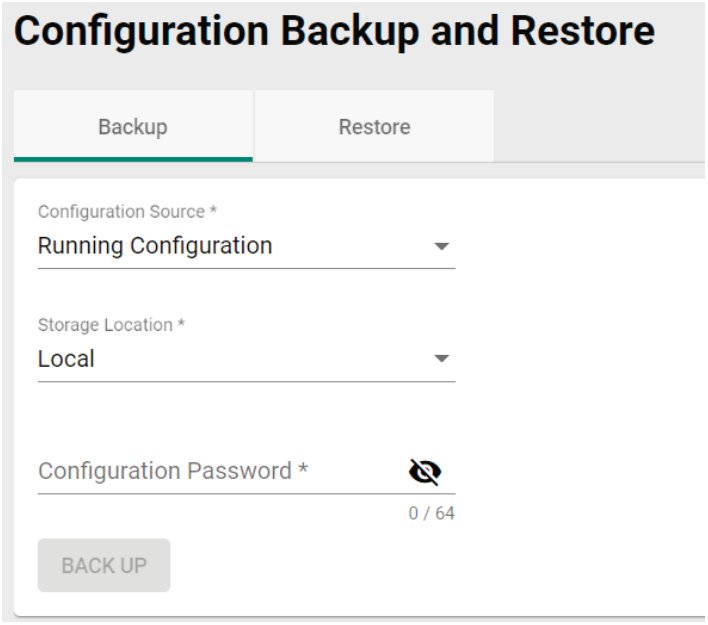
When finished, click **UPLOAD** to upload the file, then click **UPGRADE** to perform the firmware upgrade.

Configuration Backup and Restore

There are four ways to back up and restore your Moxa AWK's configuration: from a local configuration file, by remote TFTP server, remote SFTP server, or an ABC-01 backup and restoration tool.

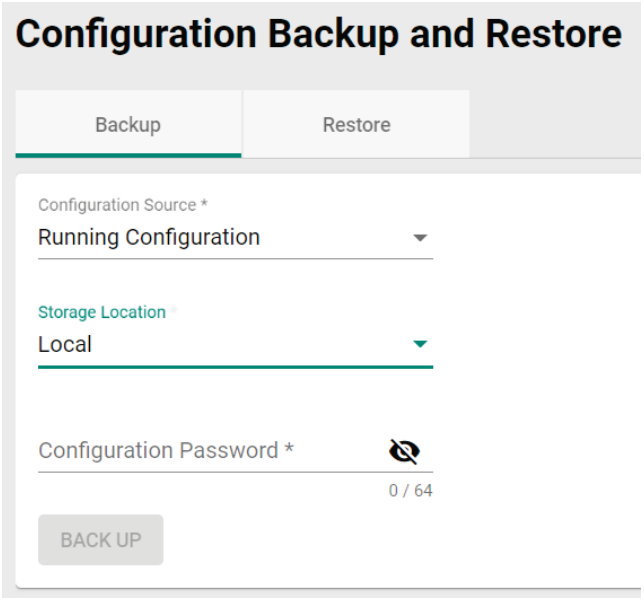
Backup

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 AWK Series devices.



Local

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



Configuration Source

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

Storage Location

Setting	Description	Factory Default
Local	Back up the configuration files to the local computer.	Local
TFTP	Back up the configuration files via TFTP.	
SFTP	Back up the configuration files via SFTP.	
ABC-01	Back up the configuration files via ABC-01 tool.	

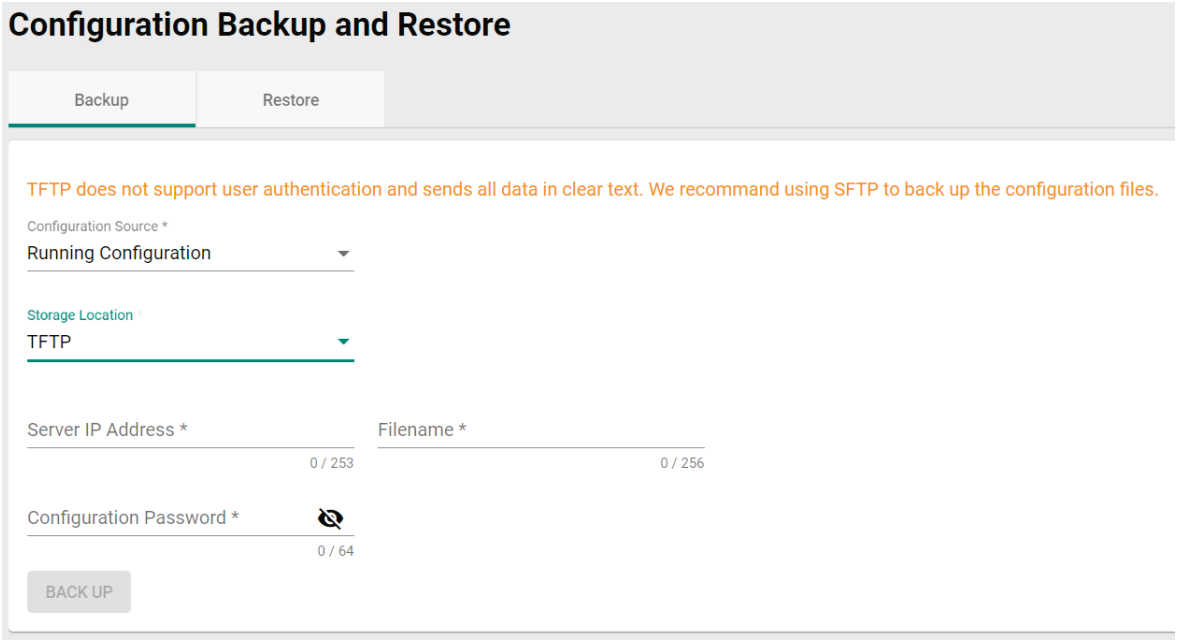
Configuration Password

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

When finished, click **BACK UP**.

TFTP Server

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



Configuration Source

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

Storage Location

Setting	Description	Factory Default
Local	Back up the configuration files to the local computer	Local
TFTP	Back up the configuration files via TFTP.	
SFTP	Back up the configuration files via SFTP.	
ABC-01	Back up the configuration files via ABC-01 tool.	

Server IP Address

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

File Name

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

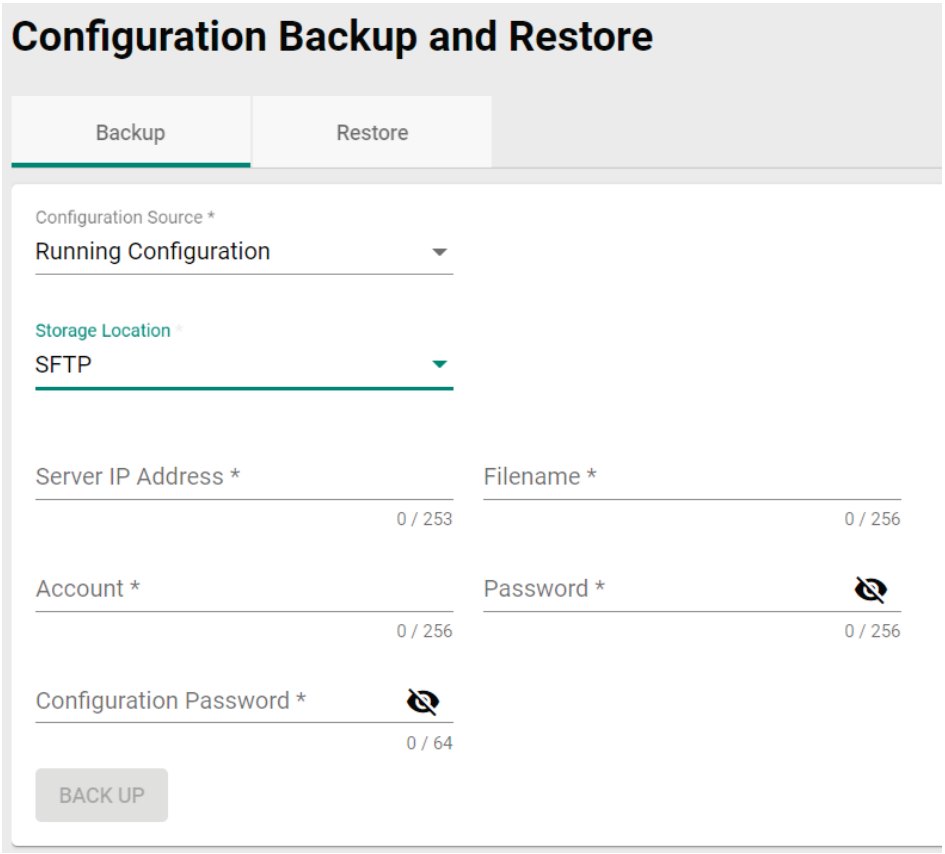
Configuration Password

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

When finished, click **BACK UP**.

SFTP Server

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



Configuration Source

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

Storage Location

Setting	Description	Factory Default
Local	Back up the configuration files to the local computer.	Local
TFTP	Back up the configuration files via TFTP.	
SFTP	Back up the configuration files via SFTP.	
ABC-01	Back up the configuration files via ABC-01 tool.	

Server IP Address

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

File Name

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

Account

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

Password

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

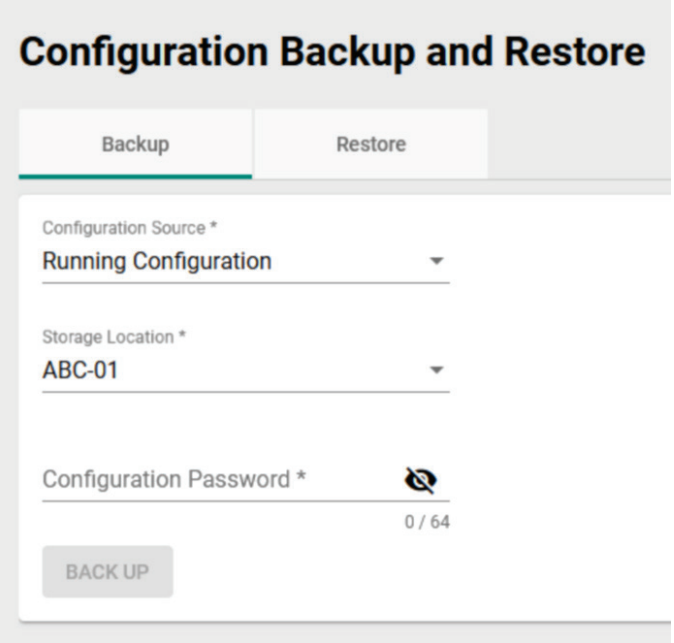
Configuration Password

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

When finished, click **BACK UP**.

ABC-01

Select **ABC-01** from the Storage Location drop-down list. This method requires a Moxa ABC-01 configuration backup and restore tool to be connected to the AWK Series.



Configuration Source

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

Storage Location

Setting	Description	Factory Default
Local	Back up the configuration files to the local computer.	Local
TFTP	Back up the configuration files via TFTP.	
SFTP	Back up the configuration files via SFTP.	
ABC-01	Back up the configuration files via ABC-01 tool.	

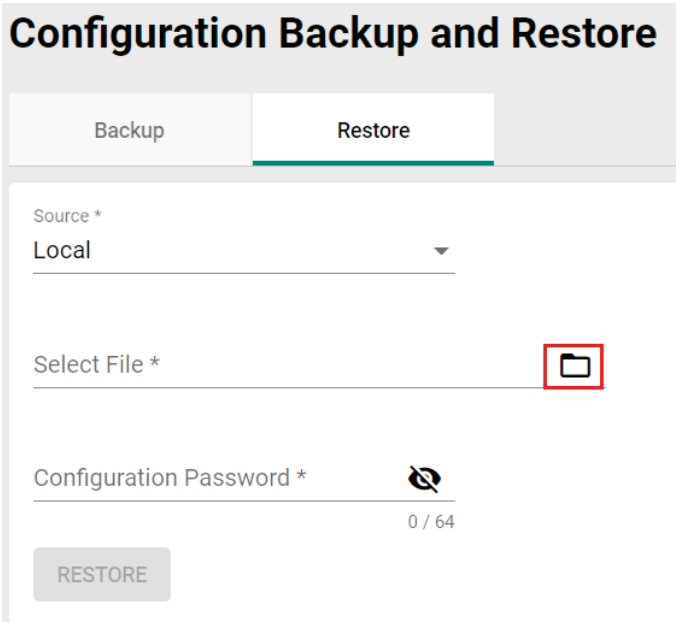
Configuration Password

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

When finished, click **BACK UP**.

Restore

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



Local

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

Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	Local
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	
ABC-01	Restore the configuration from a backup file on an ABC-01 tool.	

Select File

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

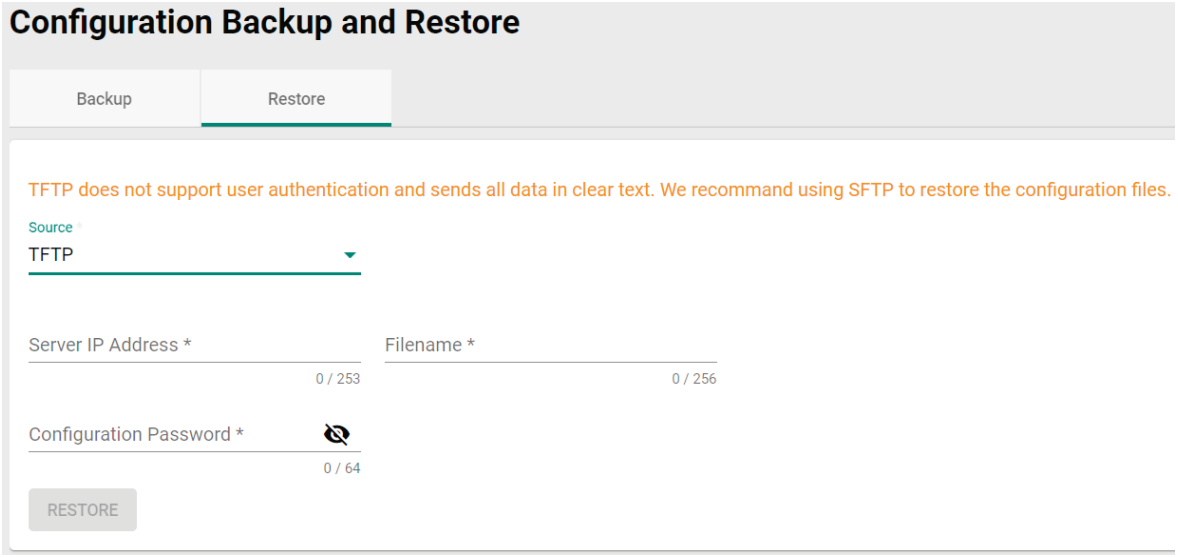
Configuration Password

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

When finished, click **RESTORE**.

TFTP Server

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



Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	Local
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	
ABC-01	Restore the configuration from a backup file on an ABC-01 tool.	

Server IP Address

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

File Name

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

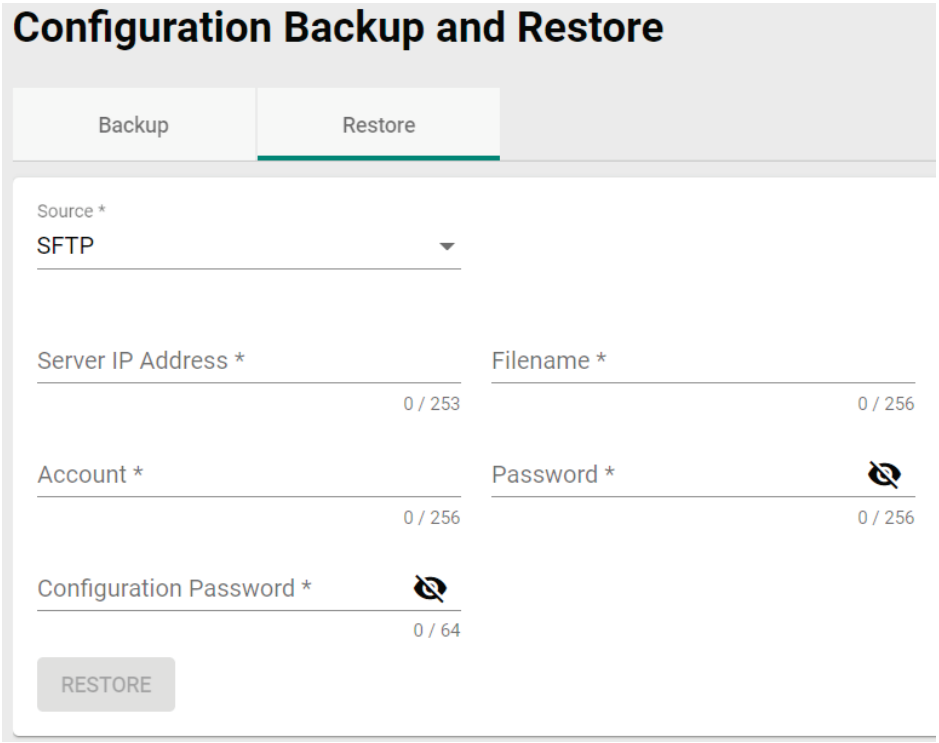
Configuration Password

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

When finished, click **RESTORE**.

SFTP Server

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



Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	Local
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	
ABC-01	Restore the configuration from a backup file on an ABC-01 tool.	

Server IP Address

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

File Name

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

Account

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

Password

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

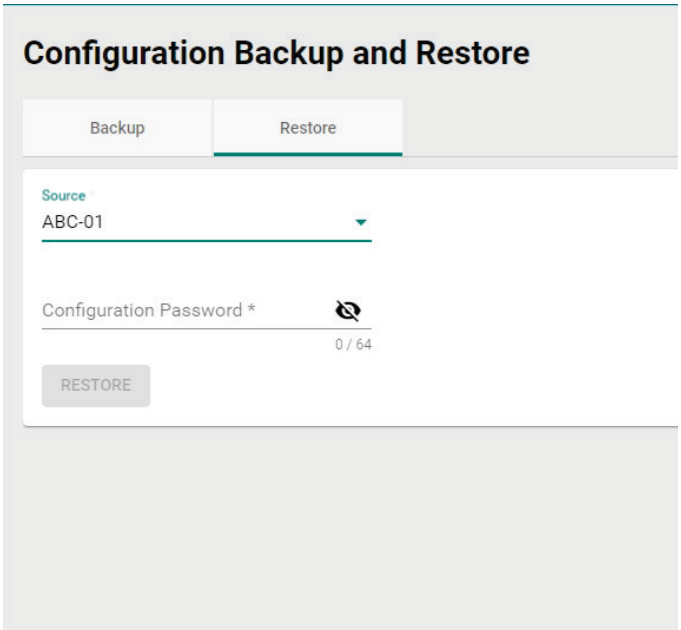
Configuration Password

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

When finished, click **RESTORE**.

ABC-01

Select **ABC-01** from the Source drop-down list.



Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	Local
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	
ABC-01	Restore the configuration from a backup file on an ABC-01 tool.	

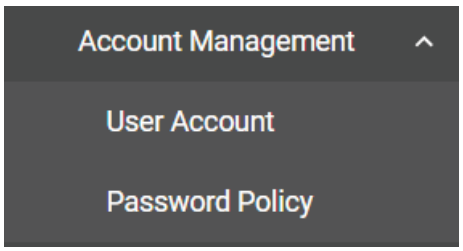
Configuration Password

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

When finished, click **RESTORE**.

Account Management

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

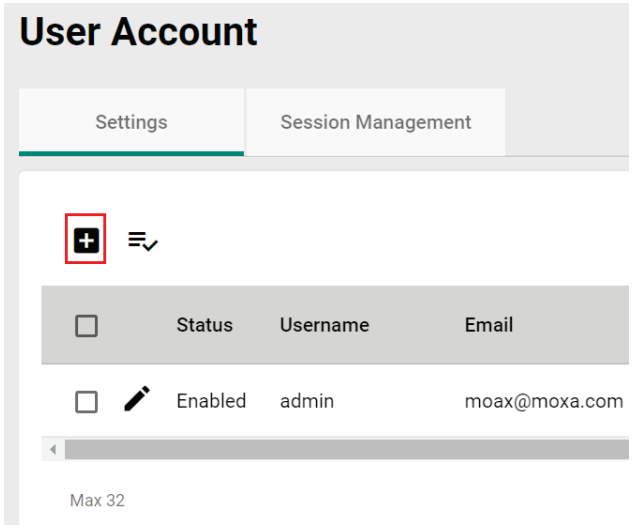


User Account

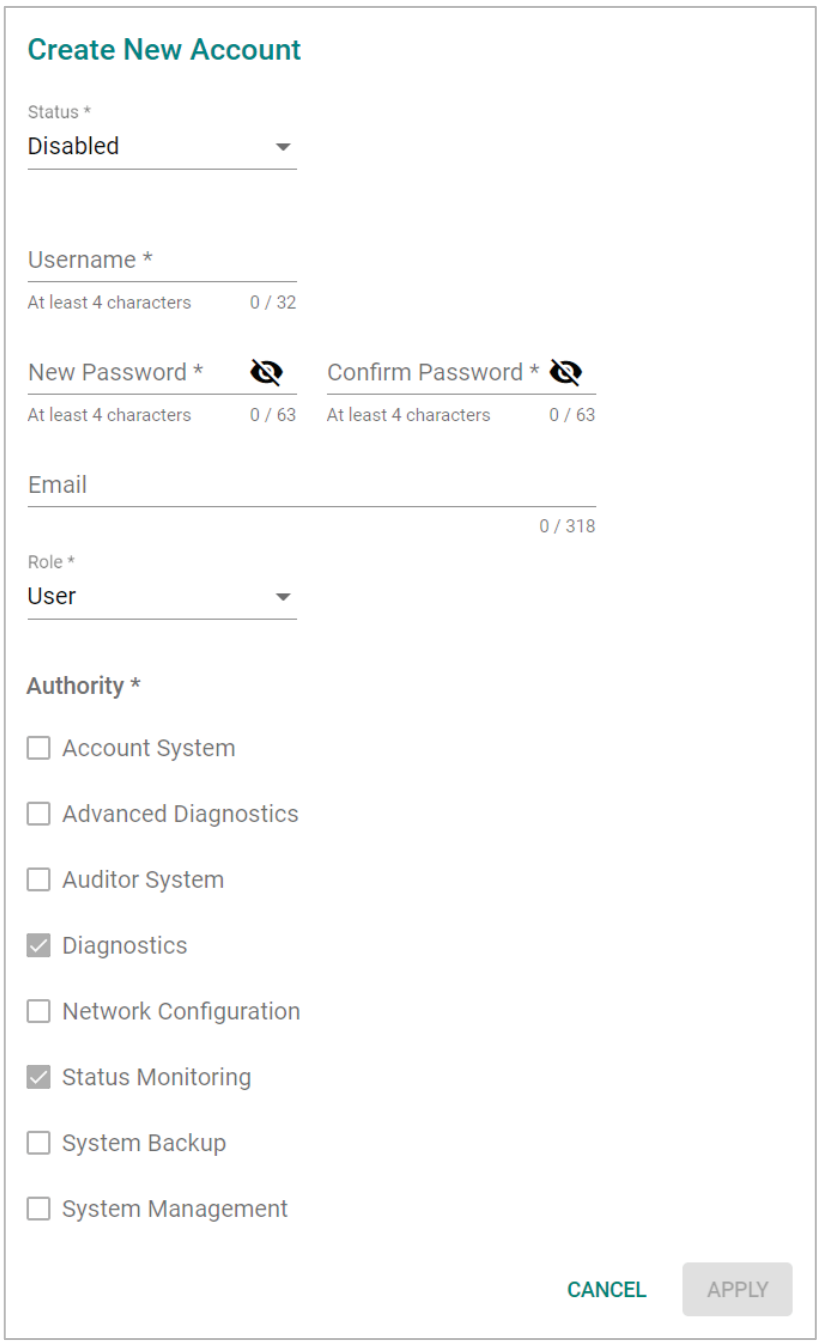
The **User Account** section lets you manage user accounts on the device, including setting user roles and privileges. Click **User Account** under **Account Management** to access this configuration screen.

Create a New Account

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



Edit the following settings:



Status

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

Username

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

New Password

Setting	Description	Factory Default
Min. 4 characters	Enter the password for this account.	None

Confirm Password

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

Email

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

Role

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

Authority

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

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

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

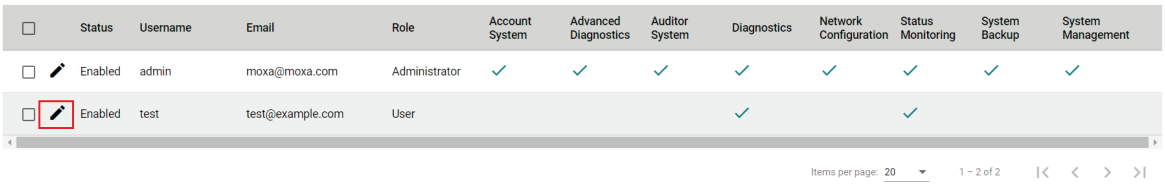
NOTE

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

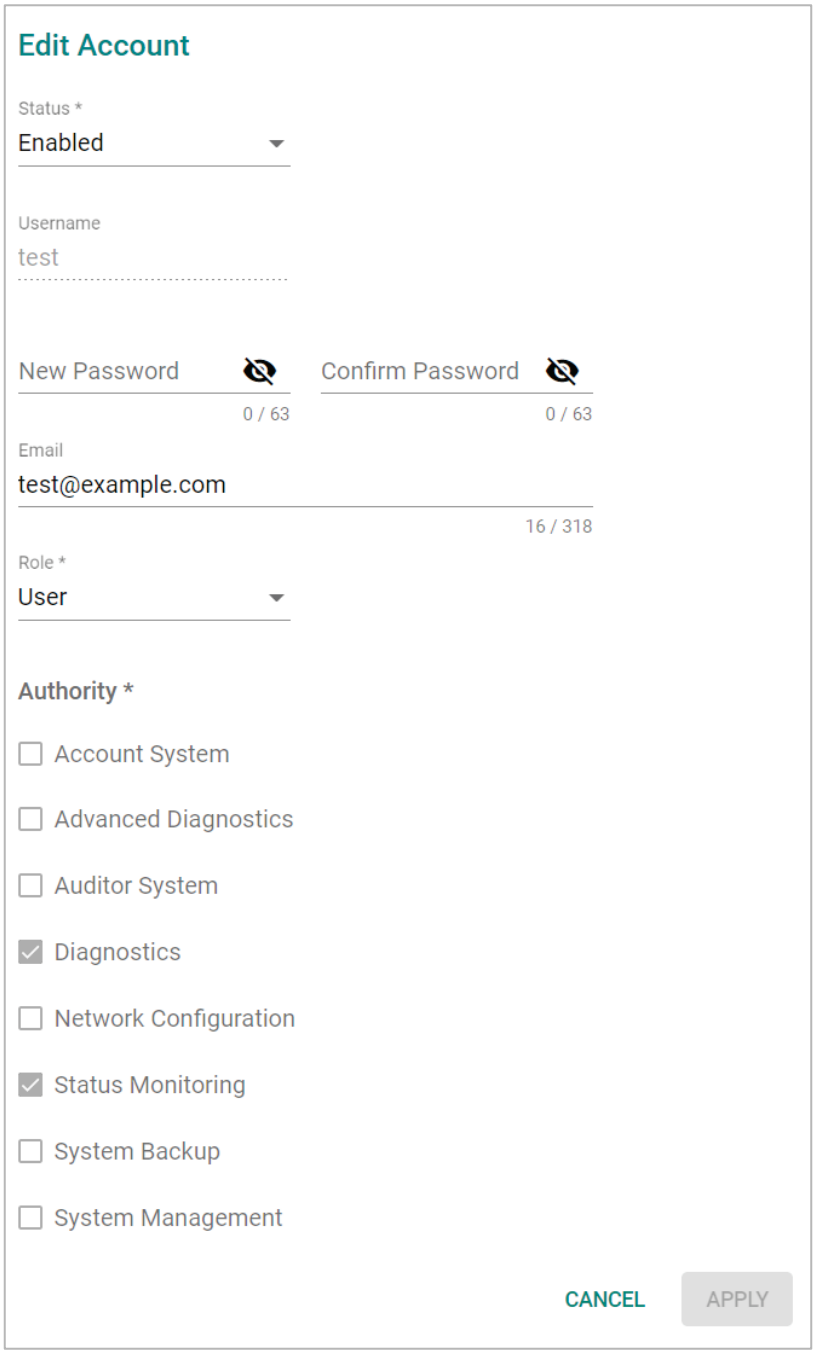
When finished, click **APPLY** to create a new account.

Edit an Existing Account

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



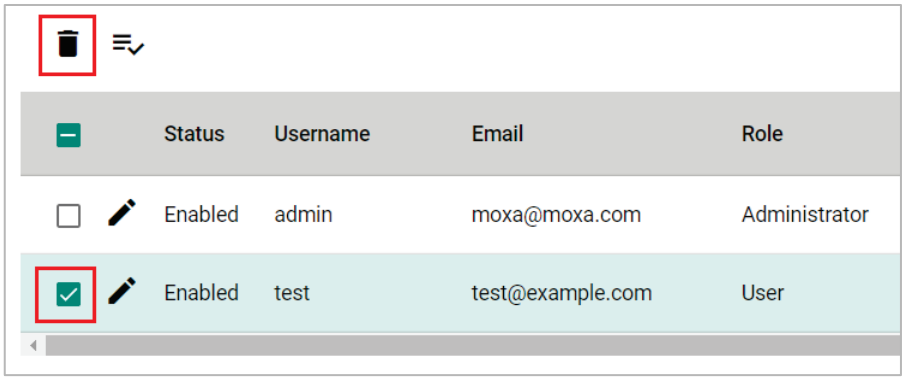
Edit the account settings. Refer to Create a New Account for a description of each setting.

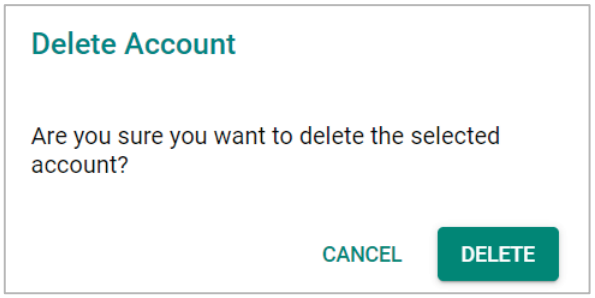


When finished, click **APPLY**.

Delete an Existing User

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



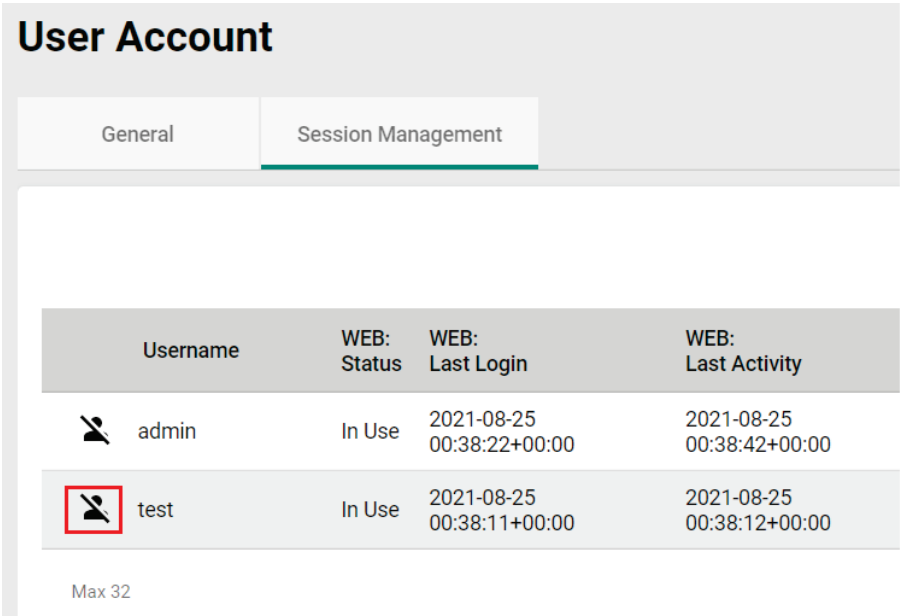


Click **DELETE** to delete the user.

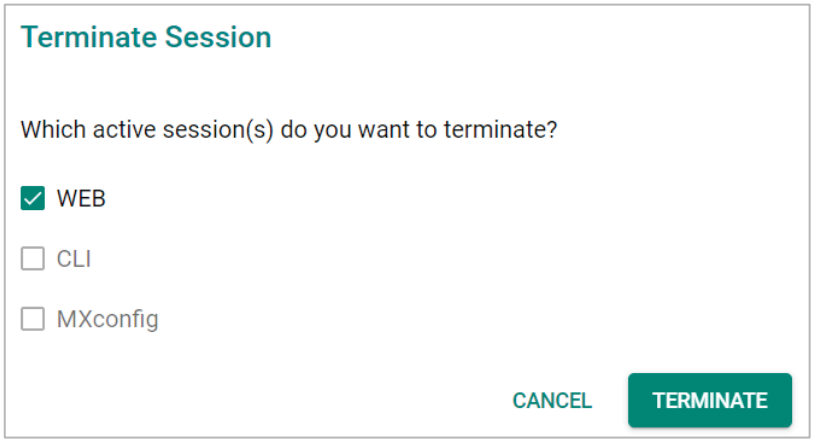
Terminate the Active Session of a User

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

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



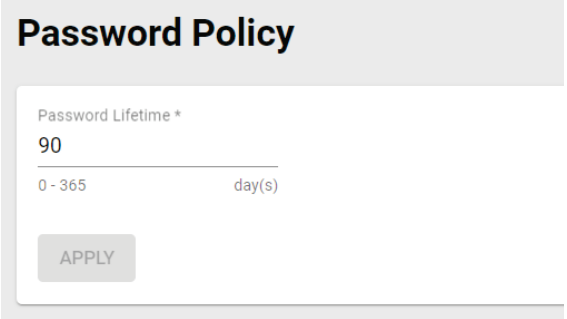
When prompted, select which active sessions you want to terminate.



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

Edit the Password Policy

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



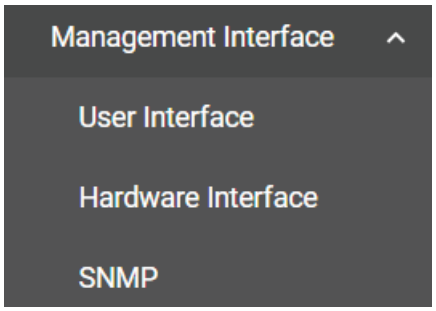
Password Lifetime

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. Every time this value is changed, users will be required to create a new password when logging in the next time.	90

When finished, click **APPLY**.

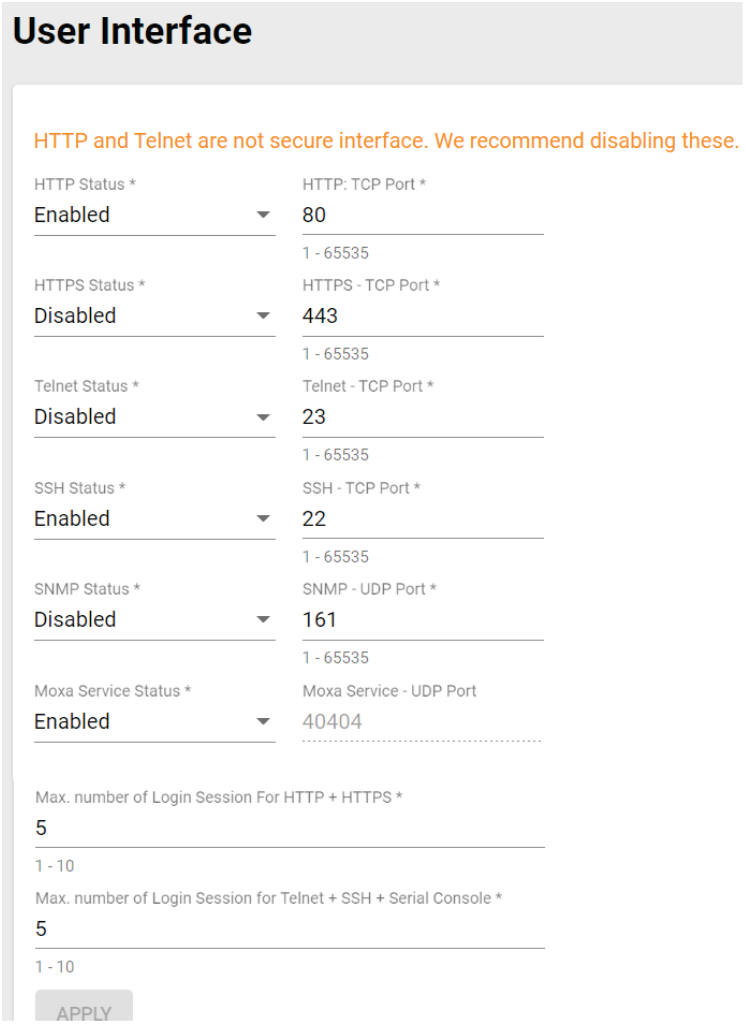
Management Interface

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.



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 65535	Specify the HTTP interface TCP port number.	80

HTTPS Status

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

HTTPS – TCP Port

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

Telnet Status

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

Telnet – TCP Port

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

SNMP Status

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

SNMP – Port

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

Moxa Service Status

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

NOTE

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

Moxa Service (Encrypted)

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

Maximum number of Login Sessions for HTTP + HTTPS

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

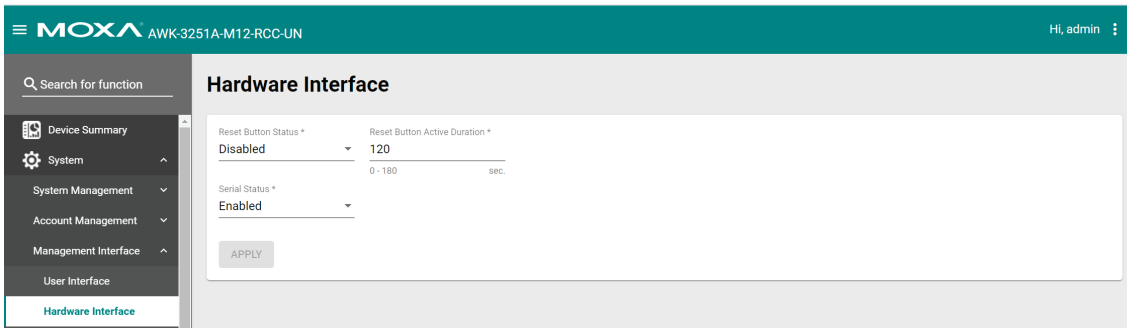
Maximum number of Login Sessions for Telnet + SSH + Serial Console

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

When finished, click **APPLY**.

Hardware Interface

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



Configure the following settings:

Reset Button Status

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

Reset Button Active Duration

Setting	Description	Factory Default
0 to 180 (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 RF LED indicator turns from amber to off after the boot up process. Specifically, the 2.4 GHz and 5 GHz LED on the AWK-3251A-RCC.	120

Serial Status

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

When finished, click **APPLY**.

SNMP

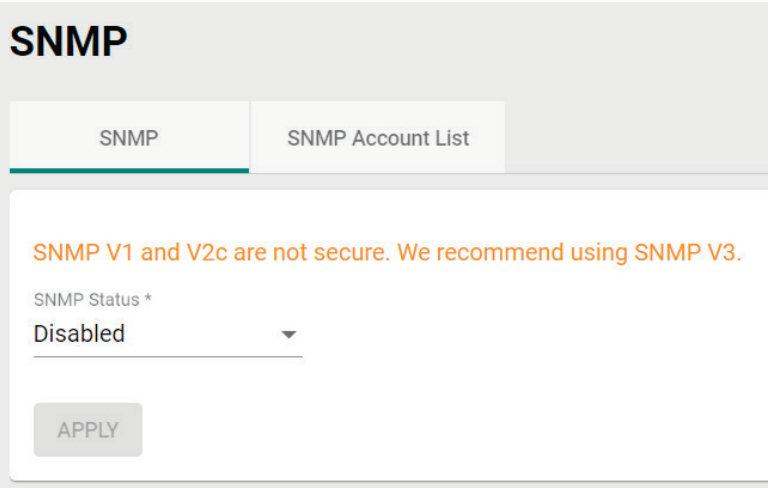
The Moxa AWK Series supports SNMP V1, V2c, and V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the default "public" and "private" community strings. SNMP V3 requires MD5 or SHA authentication.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

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

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

Configure SNMP Settings

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



SNMP Status

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

SNMP Version

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

Read Community (for V1/V2c Versions)

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

Read/Write Community (for V1/V2c Versions)

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

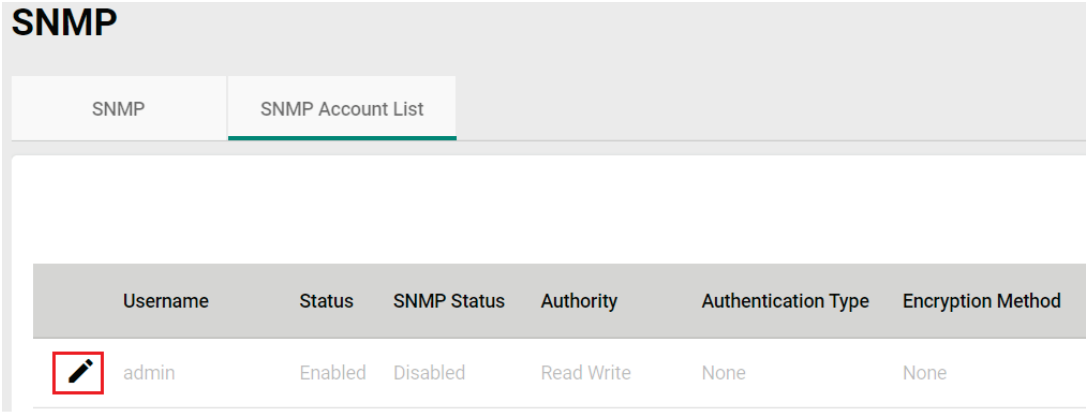
NOTE

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

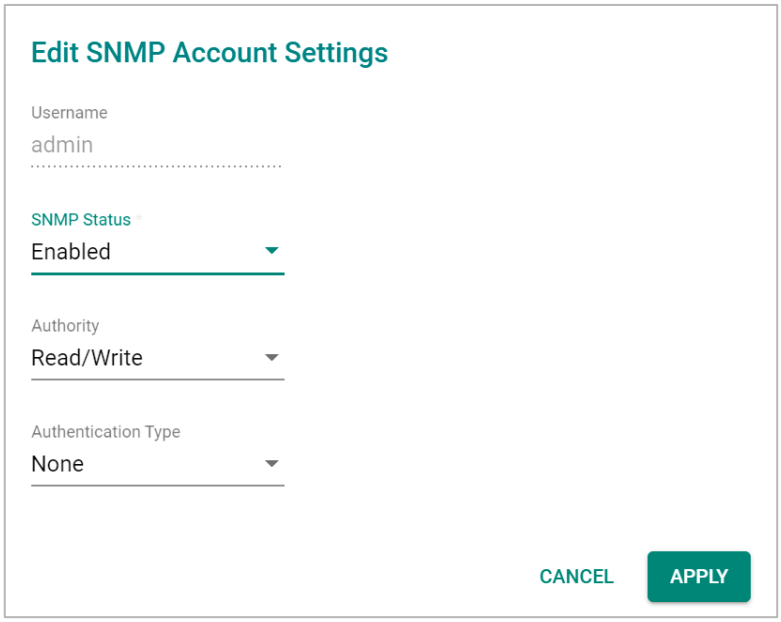
When finished, click **APPLY**.

Edit an SNMP Account

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



Configure the following settings:



Username

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

SNMP Status

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

Authority

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

Authentication Type

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

Authentication Password

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

Encryption Method

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

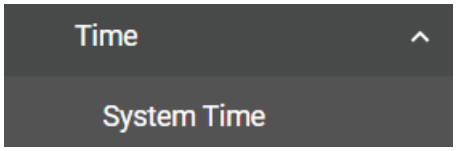
Encryption Key

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

When finished, click **APPLY**.

Time

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

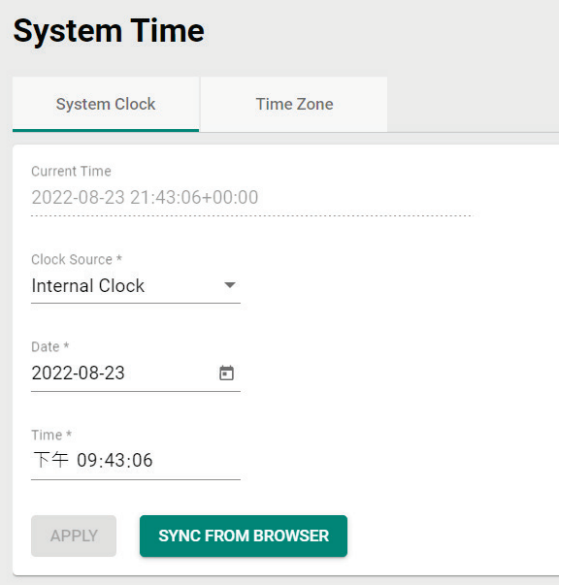


System Time

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

Edit the Clock

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



Configure the following settings:

ATTENTION

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

Current Time

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

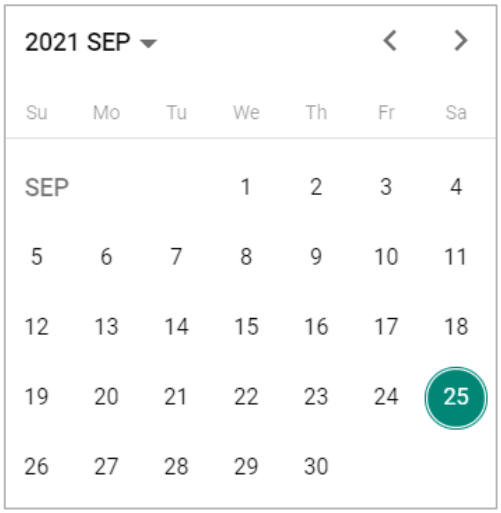
Clock Source

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

Configure the Time and Date (Internal Clock)

Date

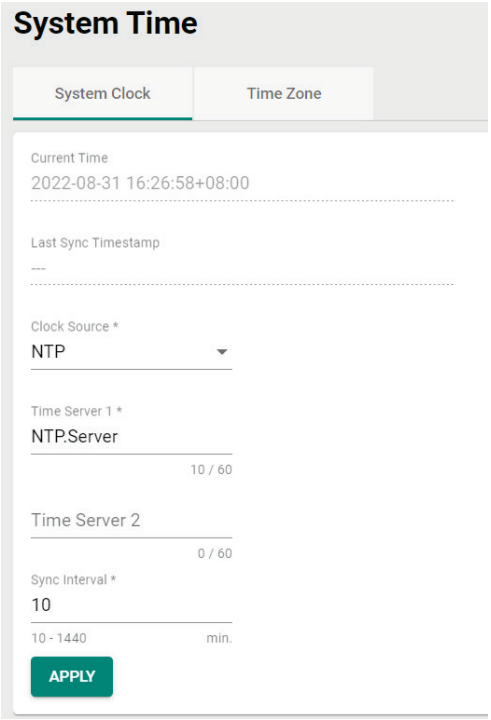
Setting	Description	Factory Default
Day of the month	Select the current date.	Local



Time

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

Configure Time Servers (NTP)



Time Server 1

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

Time Server 2

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

Sync Interval

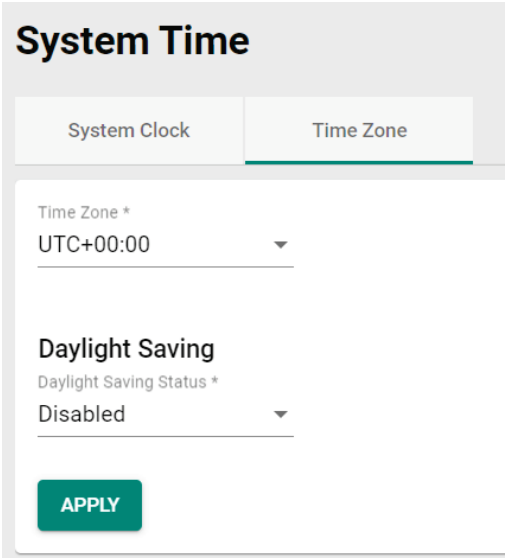
Setting	Description	Factory Default
10 to 1440 (sec.)	Specify the interval (in seconds) at which the system will sync the clock with the time server.	10

When finished, click **APPLY**.

Edit the Time Zone

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

Click the **Time Zone** tab.



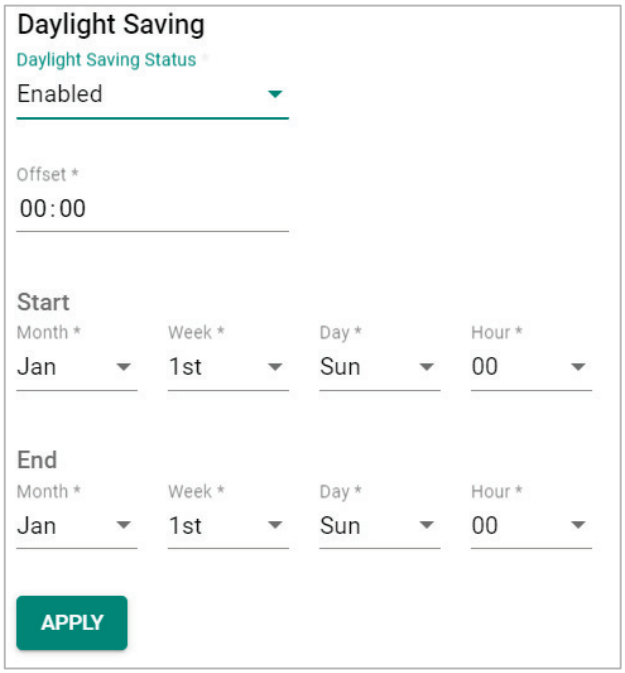
Configure the following settings:

Time Zone

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

Daylight Saving Time

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



Daylight Saving Status

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

Offset

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

Start

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

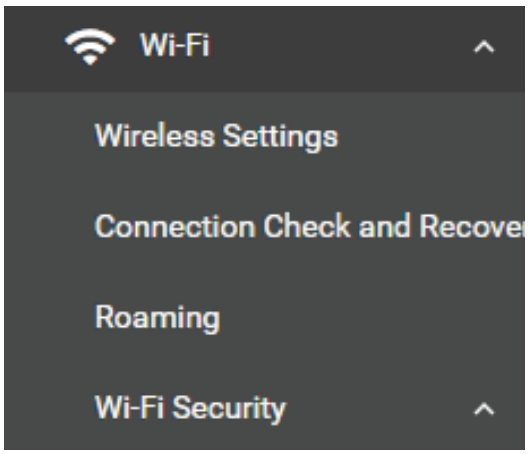
End

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

When finished, click **APPLY**.

Wi-Fi

From the Wi-Fi section, you can configure the Wireless Settings, Connection Check and Recovery, Roaming, and Wi-Fi Security.

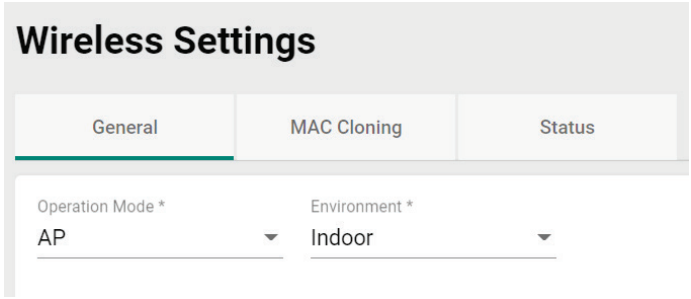


Wireless Settings

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 AWK's operation mode, creating SSIDs, and configuring RF settings. Click the **General** tab to access this screen.



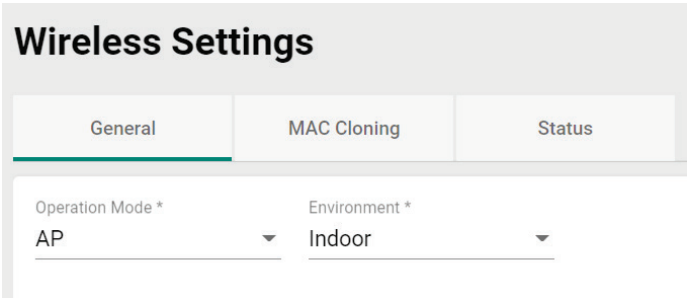
Configure the following settings:

Operation Mode

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

AP Mode Settings

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



Environment

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

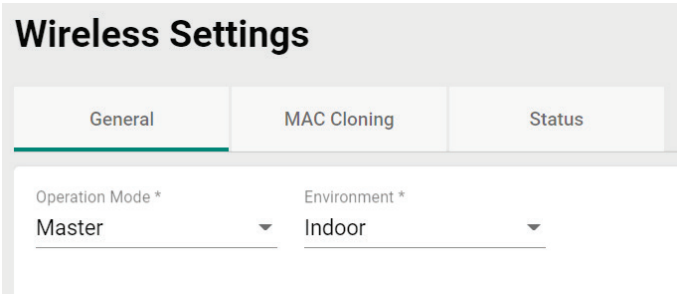
For SSID and security settings, refer to **Create a New SSID**.

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

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

Master Mode Settings

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



Environment

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

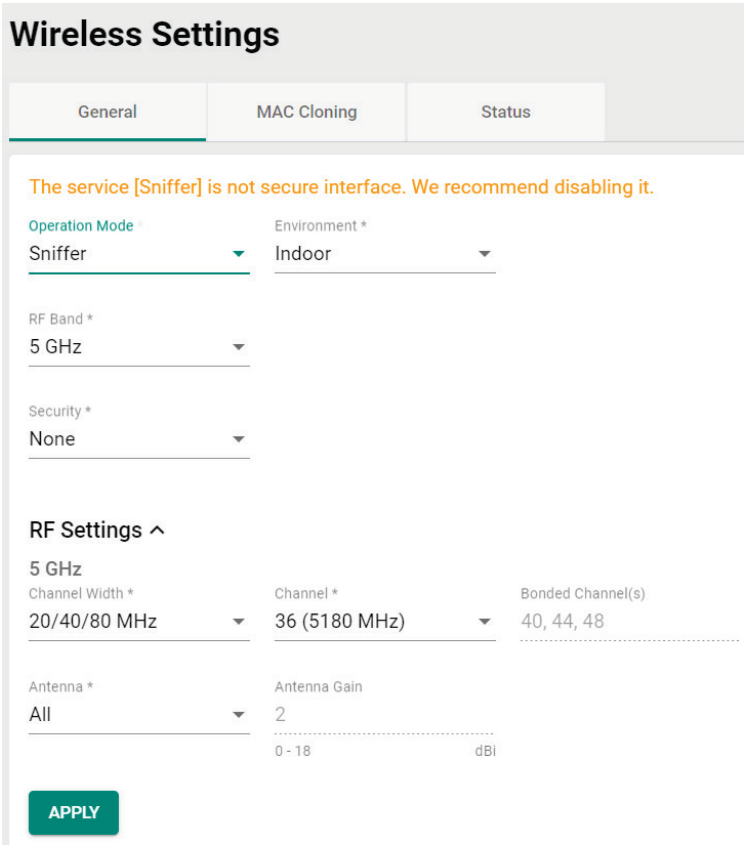
For SSID and security settings, refer to **Create a New SSID**.

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

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

Sniffer Mode Settings

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



Configure the following settings:

Environment

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

RF Band

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

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

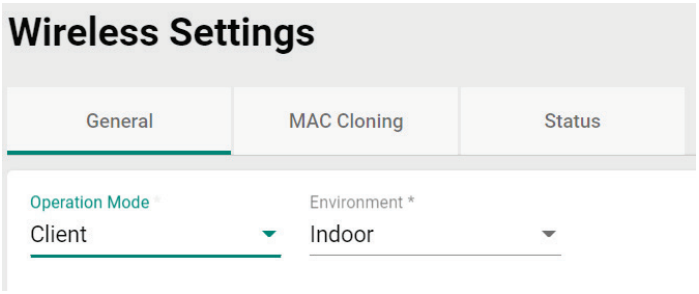
When finished, click **APPLY** to change the operation mode.

NOTE

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

Client Mode Settings

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



Configure the following settings:

Environment

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

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

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

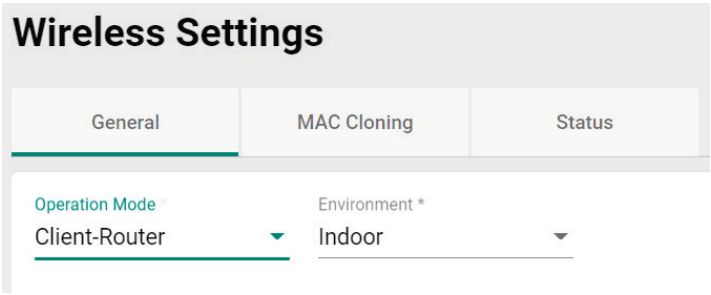
For configuring advanced settings, refer to **Advanced RF Settings**.

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

Client-Router Mode Settings

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

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



Configure the following settings:

Environment

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

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

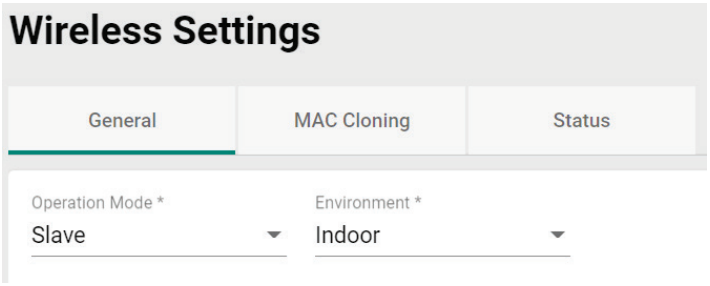
For configuring RF settings, refer to **RF Settings**.

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

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

Slave Mode Settings

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



Configure the following settings:

Environment

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

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

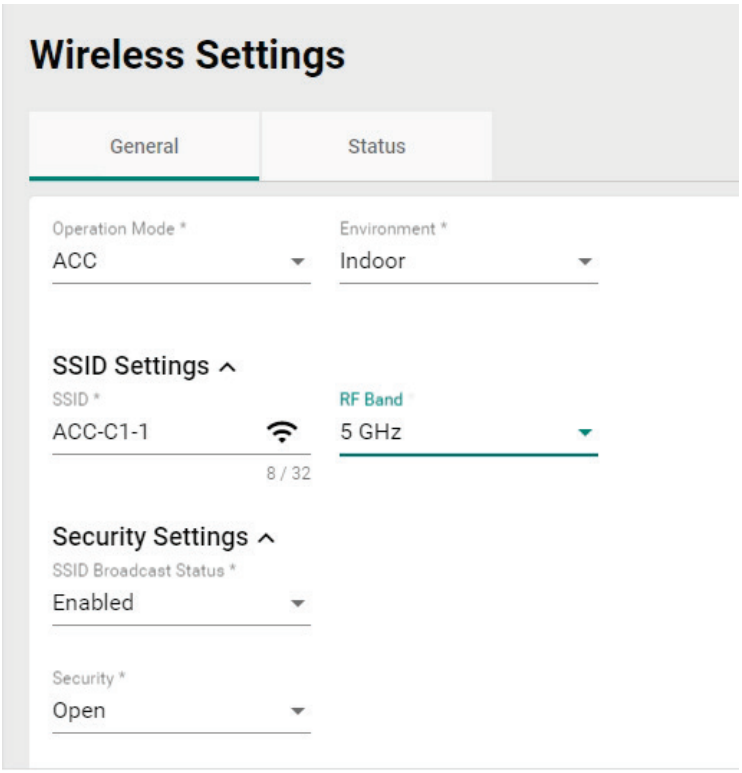
For configuring RF settings, refer to **RF Settings**.

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

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

ACC Mode Settings

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



Configure the following settings:

Environment

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

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

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

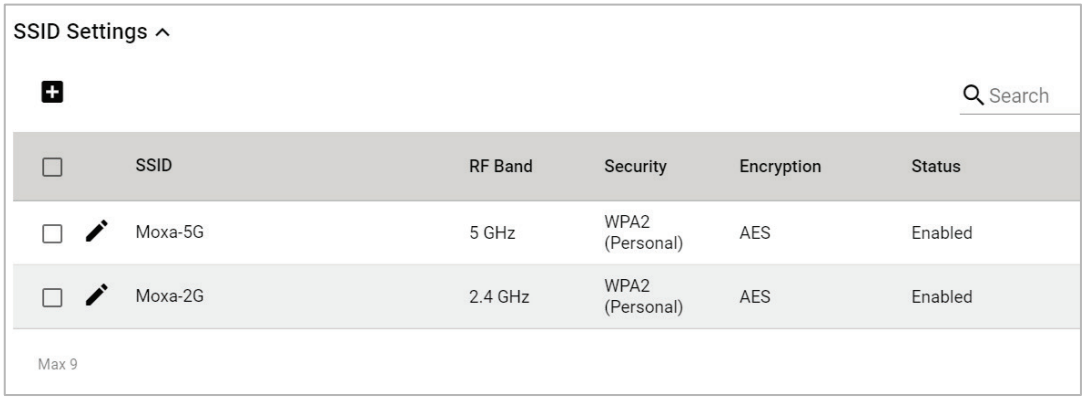
When finished, click **APPLY** to change the operation mode.

Add a New SSID (AP, Master, ACC Mode only)

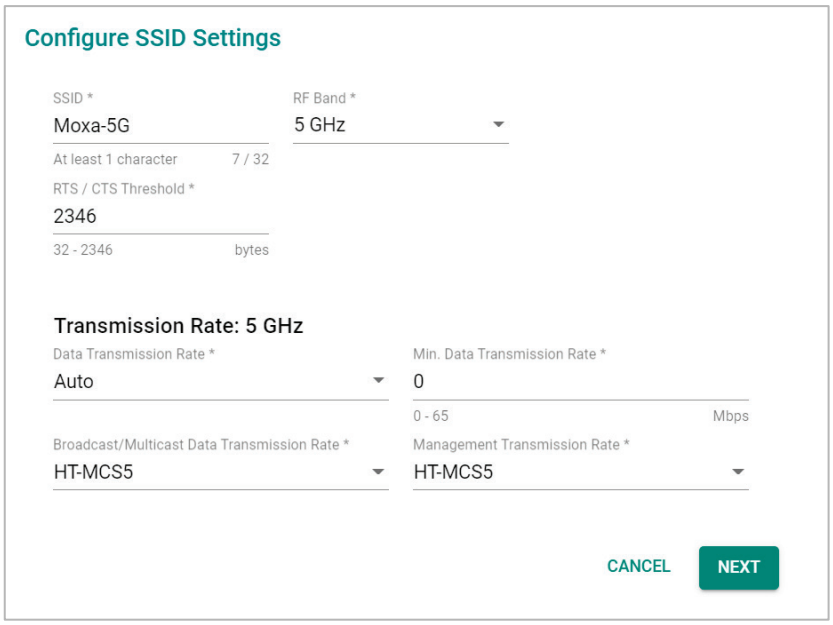
For AP and Master operation modes, configure and enable the SSID profile. There are no SSIDs on the device by default. To add a new SSID, click the **Add** icon.

NOTE

For more information about Client, Client-Router, and Slave Mode SSID settings, refer to the Wi-Fi Basic section.



Configure the following settings:



SSID Status

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

SSID

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

RF Band

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

RTS/CTS Threshold

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

Transmission Rate: 5 GHz/2.4 GHz

Data Transmission Rate

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

Minimum Data Transmission Rate

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

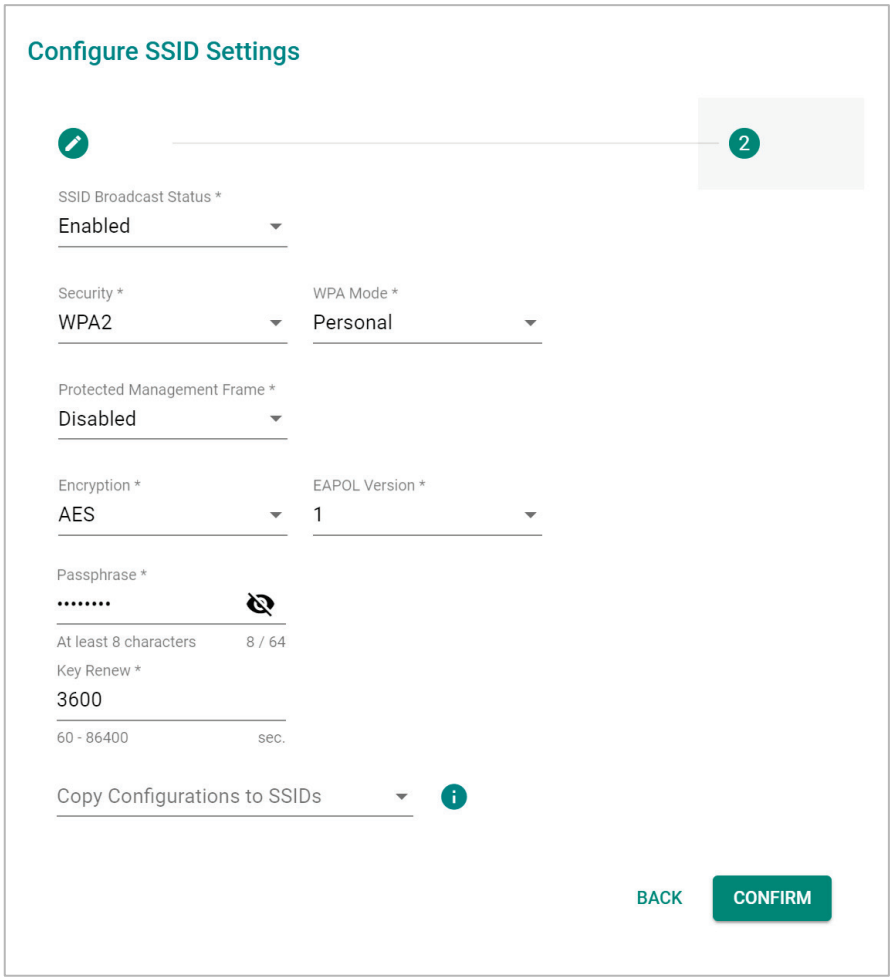
Broadcast/Multicast Data Transmission Rate

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

Management Transmission Rate

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

When finished, click **NEXT**.



SSID Broadcast Status

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

Security

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

The AWK 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 AWK supports WPA/WPA2 at the same time. The AWK is able to authenticate with both Wi-Fi clients that use WPA and WPA2.
- **WPA2/WPA3 Mixed:** The AWK supports WPA2/WPA3 at the same time. The AWK 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 WAP3.	Disabled
802.11w	Use 802.11w protocol as the protected management frame.	

WPA Mode

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

Encryption

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

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

EAPOL Version

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

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

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

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

Primary/Secondary RADIUS Port (for Enterprise mode only)

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

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

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

Passphrase (for Personal mode only)

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

Key Renew

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

Copy Configurations to SSIDs

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

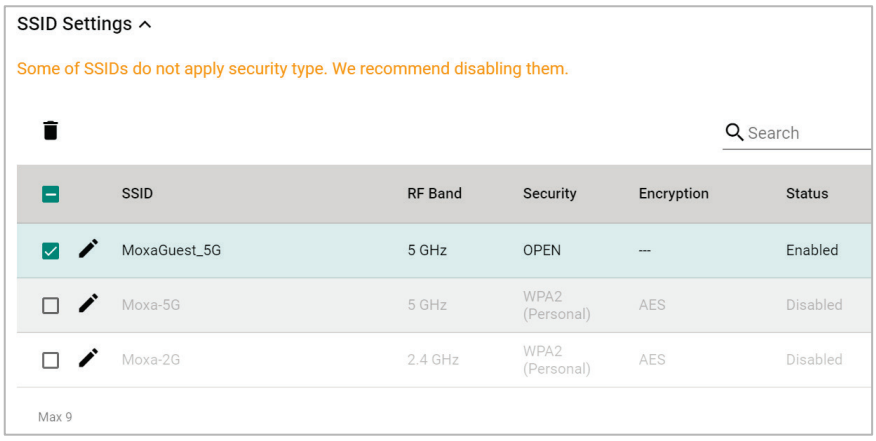
WARNING

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

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

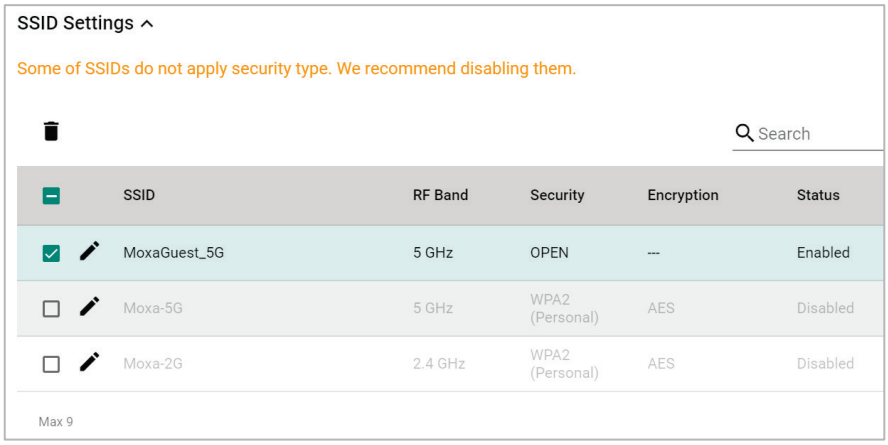
Edit an Existing SSID

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

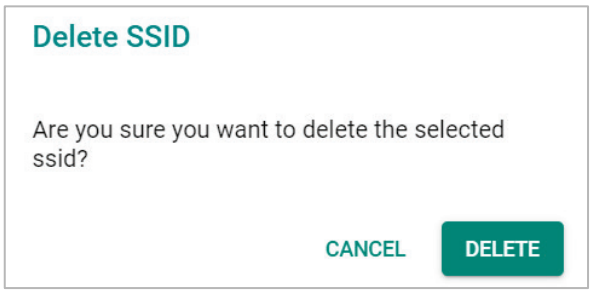


Delete an Existing SSID

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



When prompted, click **DELETE**.

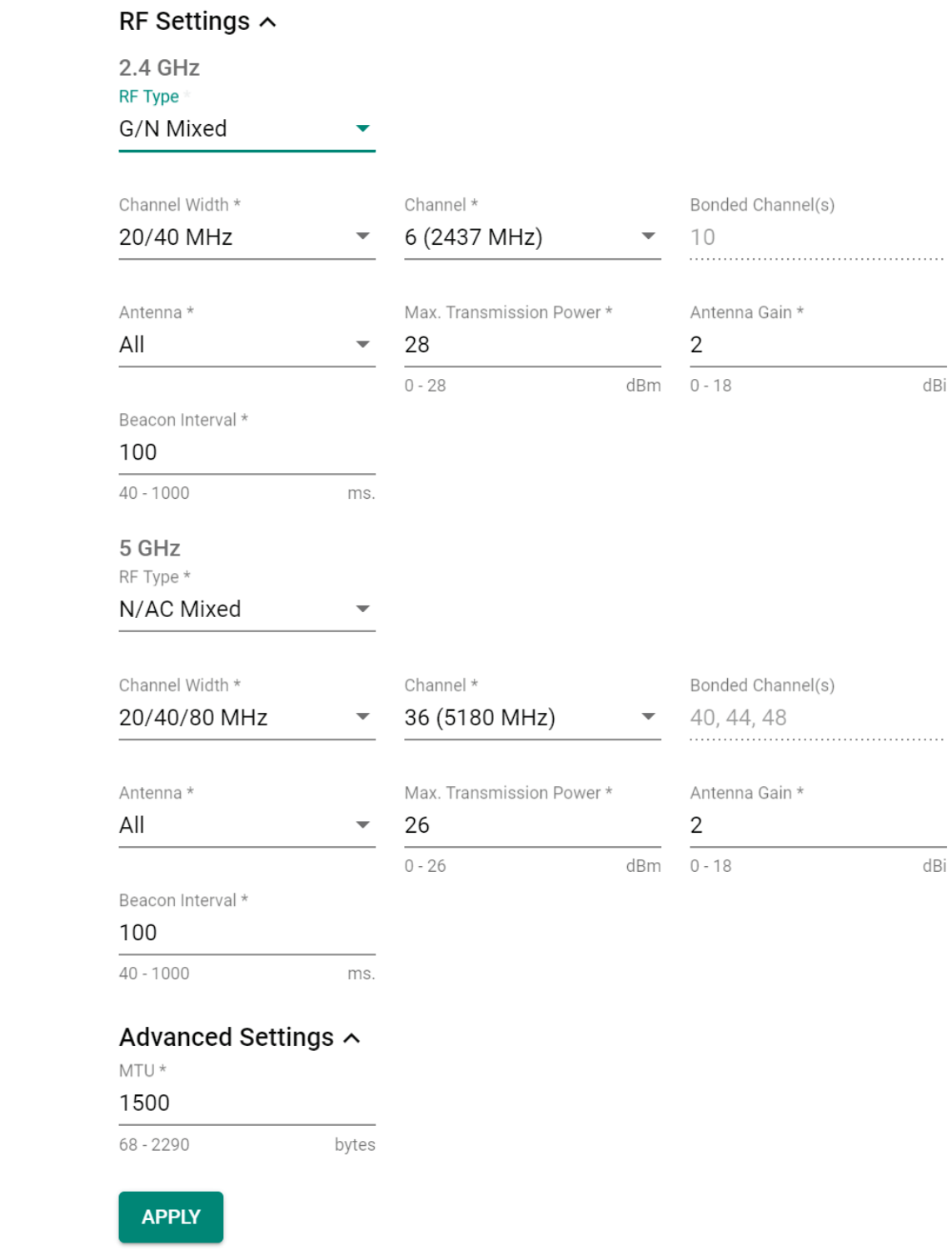


RF Settings

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

NOTE

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



For 2.4 GHz

Configure the following settings:

RF Type

Setting	Description	Factory Default
G/N Mixed	Enable IEEE 802.11g/n. 802.11n may operate at a slower speed if 802.11g clients are connected to the network.	B/G/N Mixed
B/G/N Mixed	Enable IEEE 802.11b/g/n. 802.11g/n may operate at a slower speed if 802.11b clients are on the network	
N Only (2.4 GHz)	Only enable IEEE 802.11n.	

Channel Width (for 802.11n RF types only)

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

Channel

Setting	Description	Factory Default
1 (2412 MHz) to 11 (2462 MHz)	Select the channel from the drop-down list. Each channel supports different frequencies. **Note**: Available channels depend on the selected country.	6 (2437 MHz)

Bonded Channel

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

Antenna

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

Maximum Transmission power

Setting	Description	Factory Default
dBm	Specify the maximum transmission power which acts as a hard ceiling for different transmission rates.	28 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)

For 5 GHz

Configure the following settings:

RF Type: 5 GHz

Setting	Description	Factory Default
AC Only (5 GHz)	Only enable IEEE 802.11ac.	A/N/AC Mixed
N/AC Mixed	Enable IEEE 802.11n/ac.	
A/N/AC Mixed	Enable IEEE 802.11a/n/ac.	

Channel Width (for any 11N RF type only)

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

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

Channel

Setting	Description	Factory Default
36 (5180 MHz) to 165 (5825 MHz)	Select the channel from the drop-down list. Each channel supports different frequencies.	36 (5180 MHz)

Bonded Channel

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

Antenna

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

Maximum Transmission power

Setting	Description	Factory Default
dBm	Specify the maximum transmission power which acts as a hard ceiling for different transmission rates. **Note**: The supported Maximum Transmission Power depends on the selected country code.	26 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)

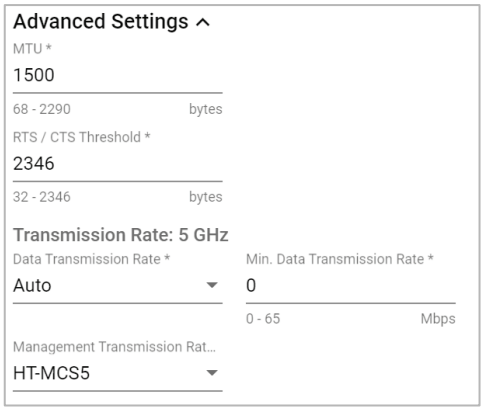
When finished, click **APPLY**.

Advanced RF Settings (Client, Client-Router, Slave, ACC Mode Only)

Some operation modes require additional advanced RF settings.

NOTE

Available RF settings depend on which Operation mode is active.



Configure the following settings:

RTS/CTS Threshold

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

Transmission Rate: 5 GHz/2.4 GHz

Data Transmission Rate

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

Minimum Data Transmission Rate

Setting	Description	Factory Default
0 to 64 Mbps (0 to disable)	Specify a minimum transmission rate. By setting a minimum transmission rate, the AWK Series will avoid communicating over weak signal wireless links to maintain better wireless performance and optimize the wireless frequency usage.	0 (Disabled)

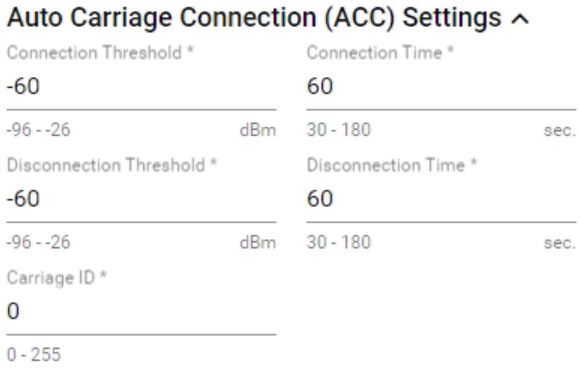
Management Transmission Rate

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

When finished, click **APPLY**.

Auto Carriage Connection (ACC) Settings

Auto Carriage Connection (ACC) is an operation mode specifically designed for inter-carriage wireless connections. In this mode, the AWK-3251A-RCC device is configured to form an ACC link with another AWK-3251A-RCC in ACC mode in an adjacent carriage. Both linked AWK-3251A-RCC Series devices must be configured to use the same settings, including SSID, RF, security, and other advanced settings.



Connection Threshold

Setting	Description	Factory Default
-96 to -26 dBm	Specify the connection threshold value. If the signal strength of an AWK-3251A-RCC device is above this value for the duration specified in the "Connection Time" field, this AWK-3251A-RCC device will be considered a candidate for the ACC connection.	-60 dBm

Connection Time

Setting	Description	Factory Default
30 to 180 sec	Specify the connection time value. If the signal strength of an AWK-3251A-RCC device is above the specified Connection Threshold value for the specified duration in this field, this AWK-3251A-RCC device will be considered a candidate for the ACC connection.	60 sec

Disconnection Threshold

Setting	Description	Factory Default
-96 to -26 dBm	Specify the disconnection threshold value. If the signal strength of the paired AWK-3251A-RCC device is below this value for the duration specified in the "Disconnection Time" field, the ACC link to this device will be dropped.	-60 dBm

Disconnection Time

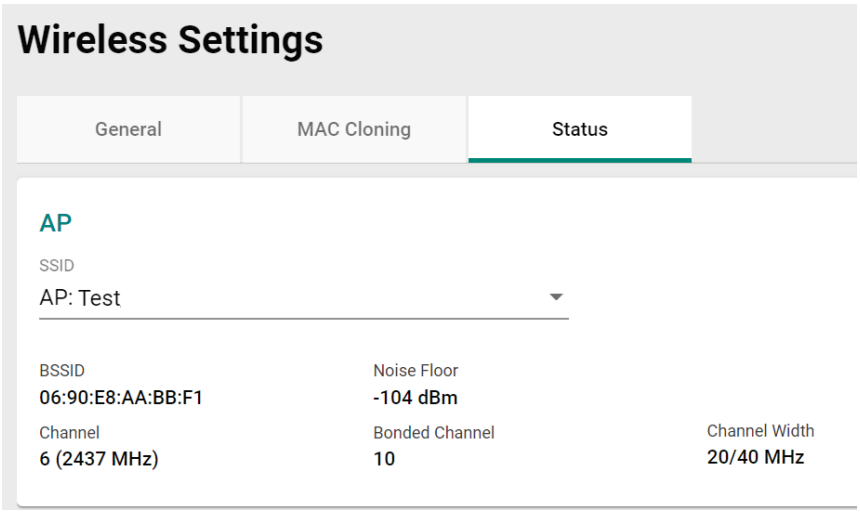
Setting	Description	Factory Default
30 to 180 seconds	Specify the disconnection time value. If the signal strength of the paired AWK-3251A-RCC device is below the specified Disconnection Threshold value for the specified duration in this field, the ACC link to this device will be dropped.	60 sec

Carriage ID

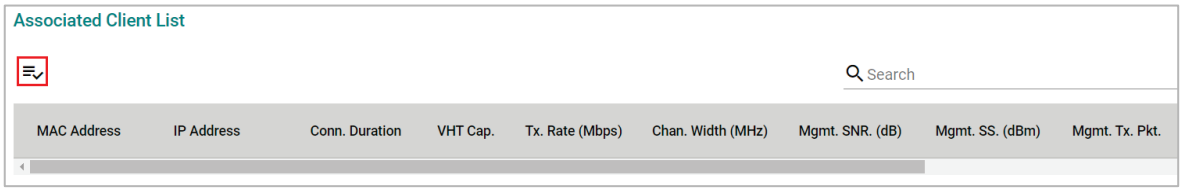
Setting	Description	Factory Default
0 to 255	Specify the Carriage ID. This value is used to identify in which carriage the AWK-3251A-RCC device is installed. If set to 0, the AWK-3251A-RCC will identify any potential ACC candidates matching the specified threshold and time values. If set to anything other than 0, this ID will be used to distinguish the location of the AWK-3251A-RCC when evaluating candidates. The device will then only associate with suitable ACC candidates that have a different Carriage ID.	0

Wi-Fi Connection Status

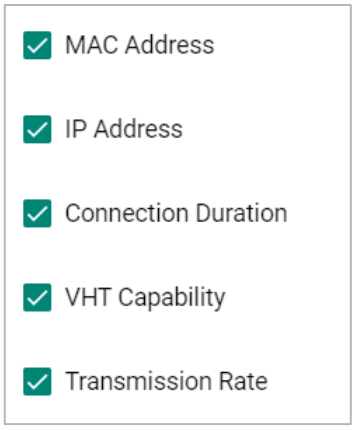
To view the Wi-Fi connection status, click **Status** tab. The information on this screen depends on the active operation mode. The following view is from AP Mode.



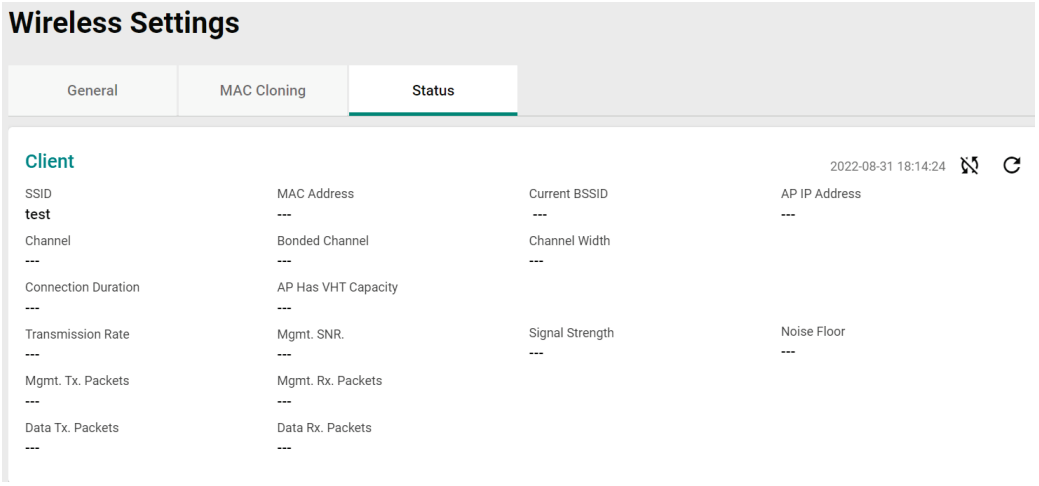
Select the SSID from the drop-down list to view its current status. In Client Mode, you can also view the client list to see all the connected client devices.



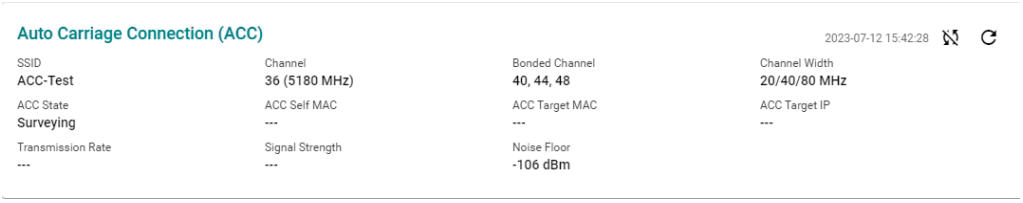
Click the **Filter** icon to select the information items that you want to show.



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

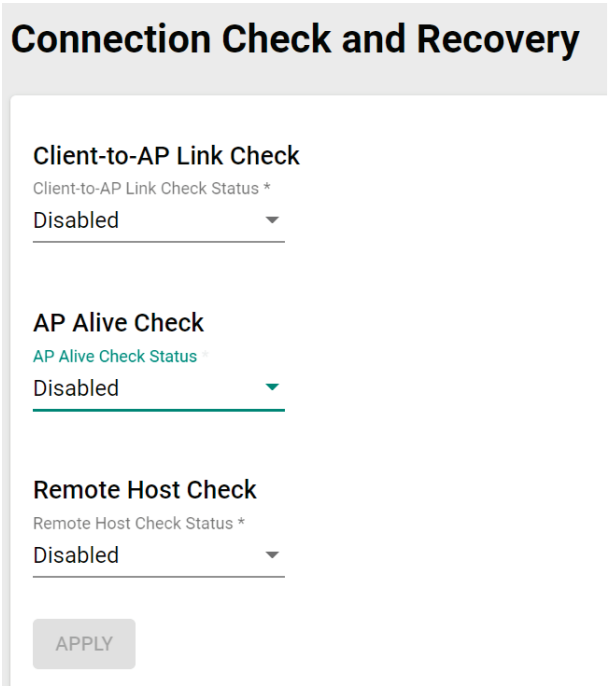


For the ACC operation mode, this view displays the properties of the ACC connection and paired devices.



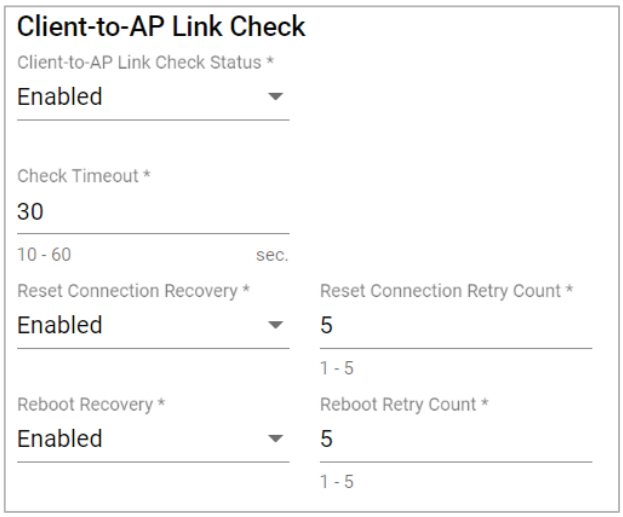
Connection Check and Recovery

The **Connection Check and Recovery** tab contains Wi-Fi troubleshooting tools. Click **Connection Check and Recovery** under **Wi-Fi** in the function tree to access this screen.



Client-to-AP Link Check

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



Configure the following settings:

Client-to-AP Link Check Status

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

Check Timeout

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

Reset Connection Recovery

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

Reset Connection Retry Count

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

Reboot Recovery

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

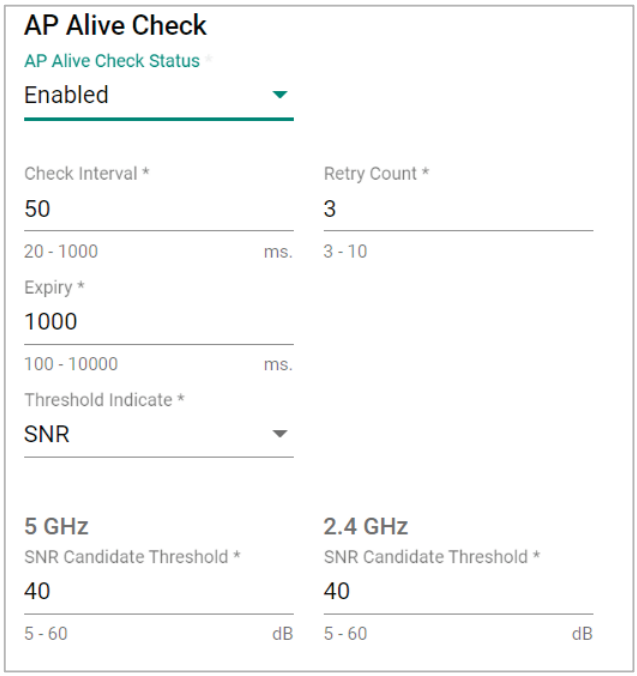
Reboot Retry Count

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

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

AP Alive Check

This is a recovery mechanism which checks whether it is still possible to receive data frame from the connected AP. When the timeout is triggered, the client will send a null data packet to probe the AP it is connected to. If the AP does not respond after the specified number of retries, the client will begin scan for other AP candidates in order to recover network communications as quickly as possible.



Configure the following settings:

AP Alive Check Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the AP Alive Check function.	Disabled

Check Interval

Setting	Description	Factory Default
20 to 1000 (ms)	Specify the interval at which the device will probe the AP.	50

Retry Count

Setting	Description	Factory Default
3 to 10	Specify the maximum number of times the device will probe the AP.	3

Expiry

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

Threshold Indicate

Setting	Description	Factory Default
SNR	Use SNR as the threshold indicator.	SNR
Signal Strength	Use signal strength as the threshold indicator.	

5 GHz: SNR Candidate Threshold (for SNR)

Setting	Description	Factory Default
5 to 60 (dB)	Specify the SNR roaming threshold.	40

2.4 GHz: SNR Candidate Threshold (for SNR)

Setting	Description	Factory Default
5 to 60 (dB)	Specify the SNR roaming threshold.	40

5 GHz: Signal Strength Candidate Threshold (for Signal Strength)

Setting	Description	Factory Default
-100 to -35 (dBm)	Specify the signal strength roaming threshold.	-65

2.4 GHz: Signal Strength Candidate Threshold (for Signal Strength)

Setting	Description	Factory Default
-100 to -35 (dBm)	Specify the signal strength roaming threshold.	-65

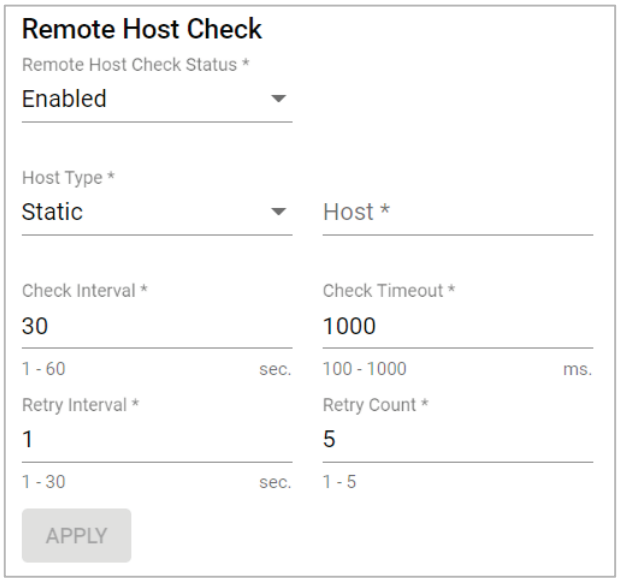
NOTE

The SNR and signal strength thresholds are used to determine when the AWK will start looking for a better AP to associate with. If the current connection quality to the AP (based on SNR or signal strength) is lower than the specified threshold value, the client will start looking for other suitable wireless devices.

When finished, click **APPLY**.

Remote Host Check

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



Configure the following settings.

Remote Host Check Status

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

Host Type

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

Host (for Static Host Type only)

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

Check Interval

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

Check Timeout

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

Retry Interval

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

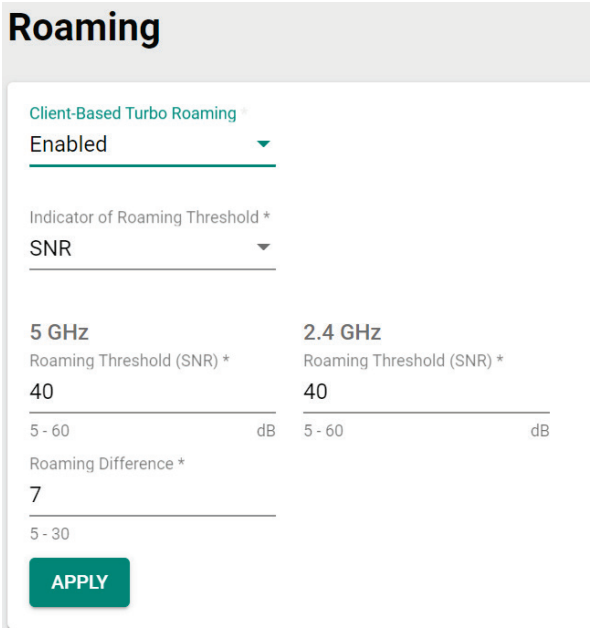
Retry Count

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

When finished, click **APPLY**.

Roaming

The **Roaming** page lets you enable or disable roaming functionality and configure roaming threshold settings. Click **Roaming** under **Wi-Fi** in the function tree to access this screen.



Configure the following settings:

Client-Based Turbo Roaming

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Client-based Turbo Roaming function.	Disabled

Indicator of Roaming Threshold

Setting	Description	Factory Default
SNR	Use SNR as the roaming threshold indicator.	SNR
Signal Strength	Use signal strength as the roaming threshold indicator.	

5 GHz: Roaming Threshold (for SNR)

Setting	Description	Factory Default
5 to 60 (dB)	Specify the SNR roaming threshold. If the current connection quality is below this threshold, the client will start looking better signal AP to associate with.	40

2.4 GHz: Roaming Threshold (for SNR)

Setting	Description	Factory Default
5 to 60 (dB)	Specify the SNR roaming threshold. If the current connection quality is below this threshold, the client will start looking better signal AP to associate with.	40

5 GHz: Roaming Threshold (for Signal Strength)

Setting	Description	Factory Default
-100 to -35 (dBm)	Specify the signal strength roaming threshold. If the current connection quality is below this threshold, the client will start looking better signal AP to associate with.	-65

2.4 GHz: Roaming Threshold (for Signal Strength)

Setting	Description	Factory Default
-100 to -35 (dBm)	Specify the signal strength roaming threshold. If the current connection quality is below this threshold, the client will start looking better signal AP to associate with.	-65

Roaming Difference

Setting	Description	Factory Default
5 to 30	Specify the roaming difference value.	7

NOTE

The Roaming Threshold determines when clients will start background scanning for other candidate APs with a stronger signal. Once the AWK starts background scanning, the client will compare the connection quality of the current and candidate AP. If the difference is larger than the specified Roaming Difference, the client will roam to the new AP.

NOTE

While the AWK is scanning the background, it will allocate 1/3 of its RF resources to search for candidate APs based on the channel plan configured on the Wi-Fi > Wireless Settings page. The maximum background scanning time required is proportional to the number of channels checked in channel plan.

NOTE

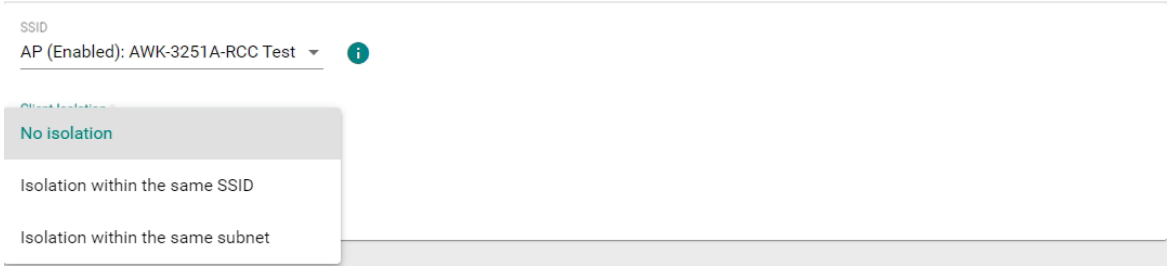
Once the background scan successfully identifies a candidate AP, the device will roam, The typical Turbo Roaming handover time of < 150 ms is an average of all documented test results, in optimized conditions, across APs configured with interference-free RF channels, and default Turbo Roaming parameters. The clients were configured with 3-channel roaming at 100 Kbps traffic load. Other conditions and factors may affect actual roaming performance.

When finished, click **APPLY**.

Wi-Fi Security

Client Isolation (AP Mode Only)

Available for AP mode only, Client isolation is used to isolate the associated wireless clients connected to one or more APs. Isolated clients cannot communicate with each other to increase the level of security. Depending on the type of client isolation used, you can specify exceptions (for clients) within the isolation network. This function can be useful in specific network environments where clients must be separated for security reasons, such as for enterprise server service.



SSID

Setting	Description	Factory Default
SSID	Select the SSID to configure client isolation for.	None

Client Isolation

Setting	Description	Factory Default
No isolation	Do not use client isolation.	None
Isolation within the same SSID	Only isolate clients connected to the same SSID.	

Setting	Description	Factory Default
Isolation within the same subnet	Isolate all clients in the specified subnet. The subnet is determined by the specified subnet mask and gateway.	

Subnet Type

Setting	Description	Factory Default
Static/DHCP	If **Isolate within the same subnet** is selected, select the subnet type. Select Static for applications that use a static IP address, such as for handheld devices that have a fixed AP in the same subnet as the AP. Select DHCP if clients receive their IP address from a DHCP server when connecting to the AP.	Static

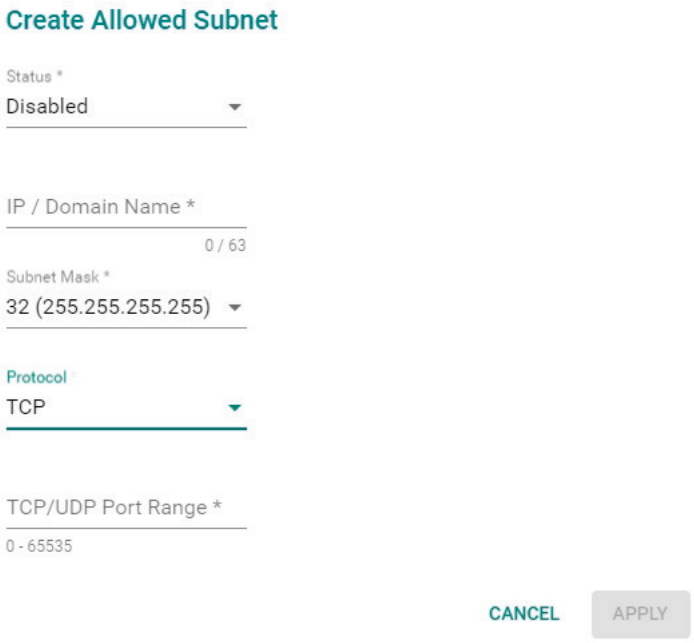
Subnet Mask

Setting	Description	Factory Default
Subnet Mask	If the **Subnet Type** is set to **Static**, specify the subnet mask. If using DHCP, leave this field blank.	24(255.255.255.0)

Gateway

Setting	Description	Factory Default
Gateway	If the **Subnet Type** is set to **Static**, specify the gateway address. If using DHCP, the DHCP server will automatically assign the gateway address.	None

The **Allowed subnet with TCP/UDP port** setting is used to specify the exceptions (subnets or hosts) when the **Isolated within the same subnet** option is selected. Up to eight subnets or hosts can be included in the list.



Status

Setting	Description	Factory Default
Enable/Disable	Enable or disable allowed subnet exception rules.	Disable

IP

Setting	Description	Factory Default
IP Address/Domain name	Specify the IP address of the subnet rule. Hosts in this subnet can be accessed by other hosts or wireless clients in the same subnet.	None

Subnet Mask

Setting	Description	Factory Default
Subnet Mask	Specify the netmask of the subnet rule. Hosts in this subnet can be accessed by other hosts or wireless clients in the same subnet.	32 (255.255.255.255)

Protocol

Setting	Description	Factory Default
All/ICMP/TCP/UDP	Select the protocol for this subnet rule. Hosts in this subnet can be accessed by other hosts or wireless clients in the same subnet.	A

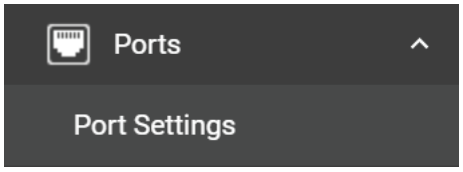
Port

Setting	Description	Factory Default
0 to 65535	Specify the port range for this subnet rule. Hosts in this subnet can be accessed by other hosts or wireless clients in the same subnet. Note: The port range only applies to the TCP and UDP protocols.	None

When finished, click **APPLY**.

Ports

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

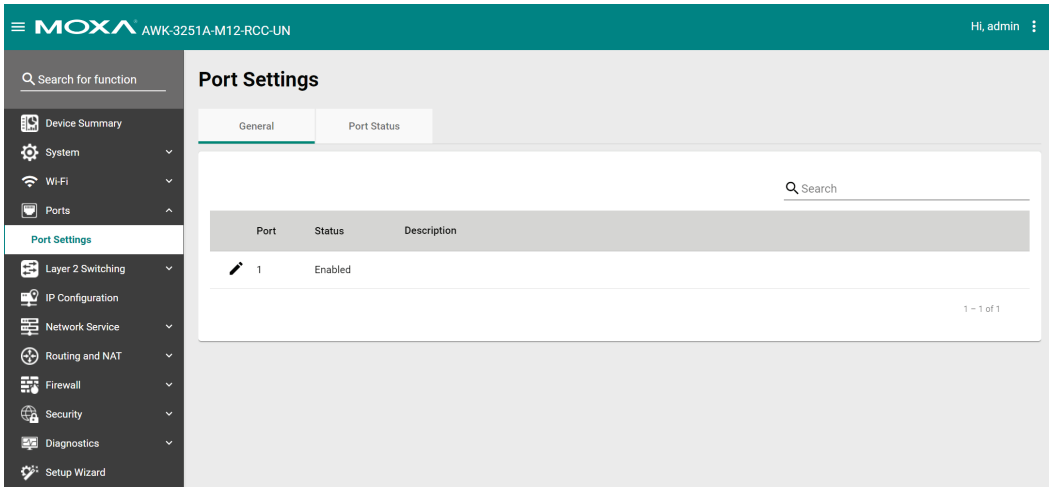


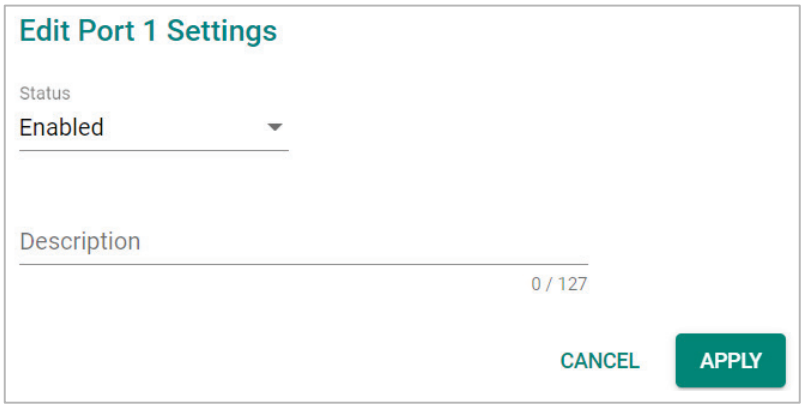
Port Settings

The **Ports Settings** page is used to configure the physical LAN 1 and LAN 2 network ports on the device. Click **Port Settings** under **Ports** in the function tree to access this screen.

General Settings

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





Configure the following settings:

Status

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

ATTENTION

The AWK-3251A-M12-RCC Series only has 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.

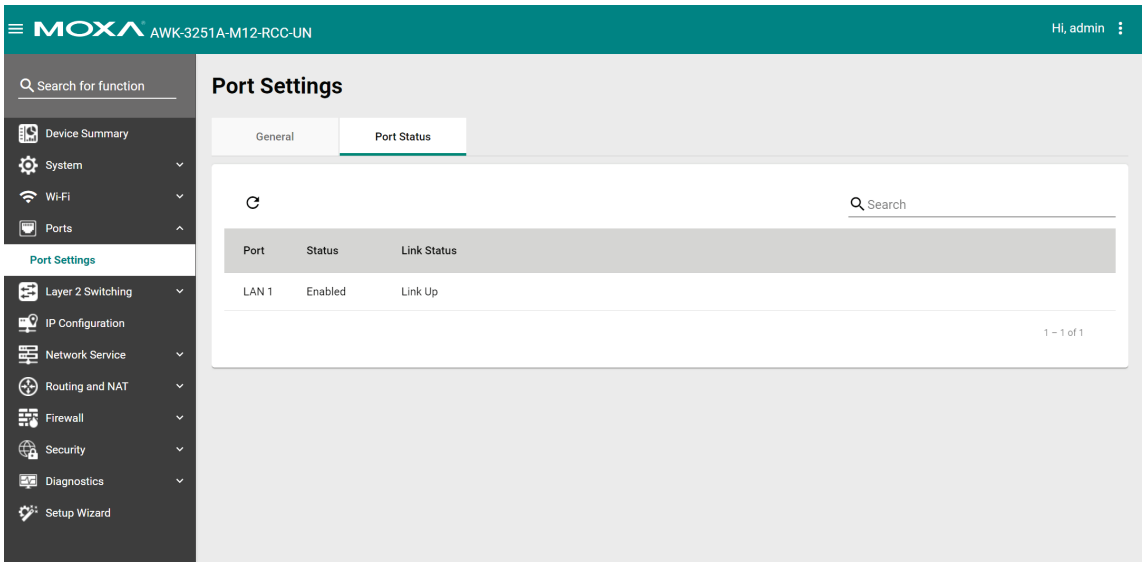
Description

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

When finished, click **APPLY**.

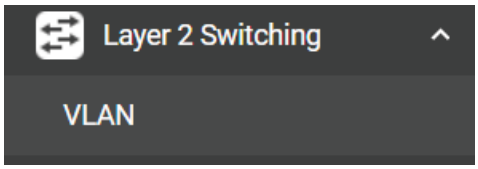
Status Check

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



Layer 2 Switching

This section describes how to configure the VLAN settings for the AWK.



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.

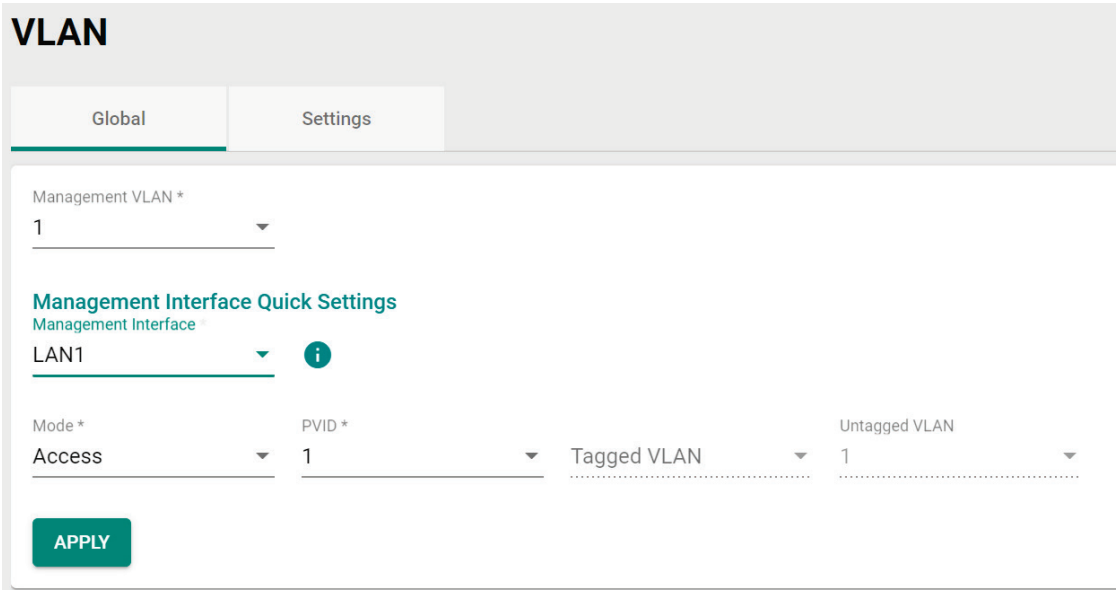
In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a department workgroup; for example, one VLAN could be used for a marketing department and the other for a human resource 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** paged is used to configure the management VLAN and interface. Click the **Global** tab to access this screen.



Configure the following settings:

Management VLAN ID

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

Management Interface Quick Settings

Management Interface

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

Mode

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

PVID

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

Tagged VLAN

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

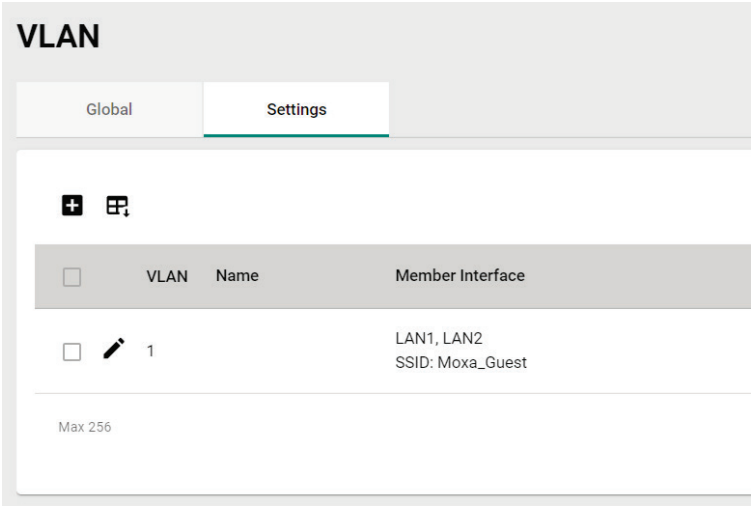
Untagged VLAN

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

When finished, click **APPLY**.

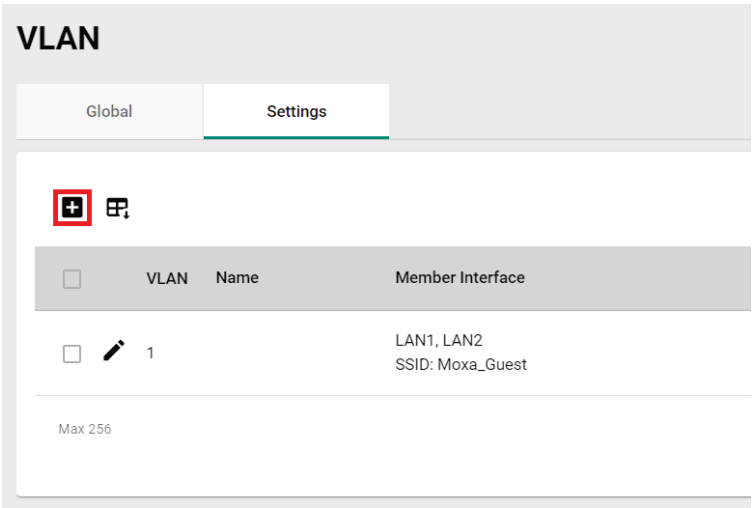
VLAN Settings

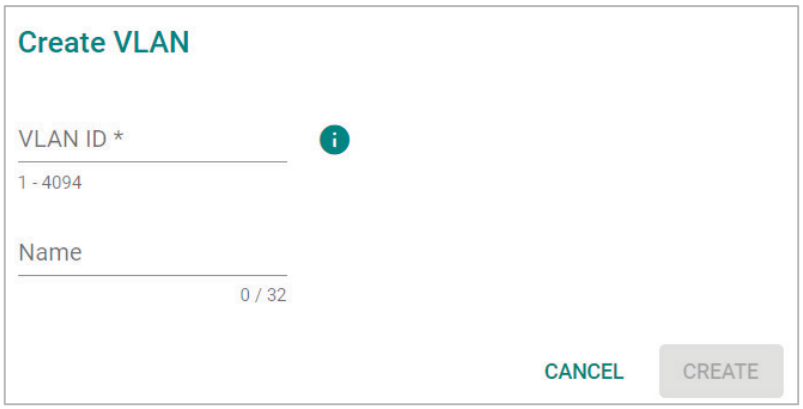
From the **Settings** tab, you can create, edit, and delete VLANs. Click the **Settings** tab to access this screen.



Create a New VLAN ID

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





Configure the following settings:

VLAN ID

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

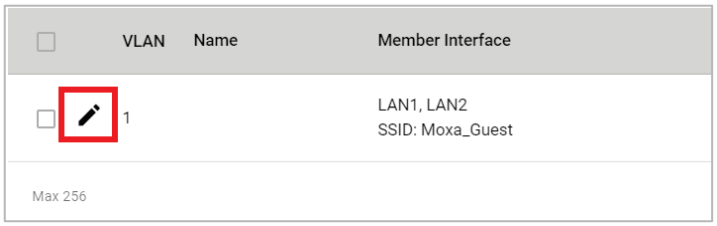
Name

Setting	Description	Factory Default
0 to 32 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.

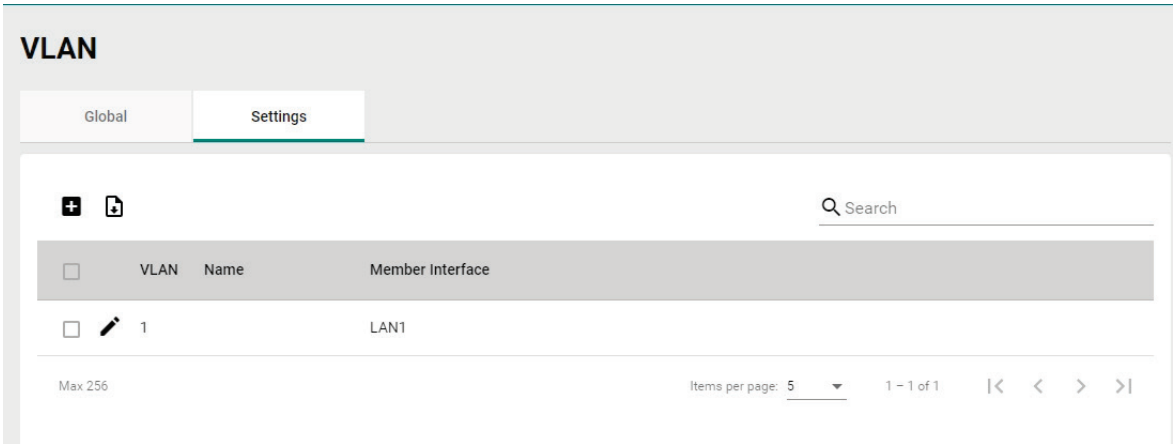
Name

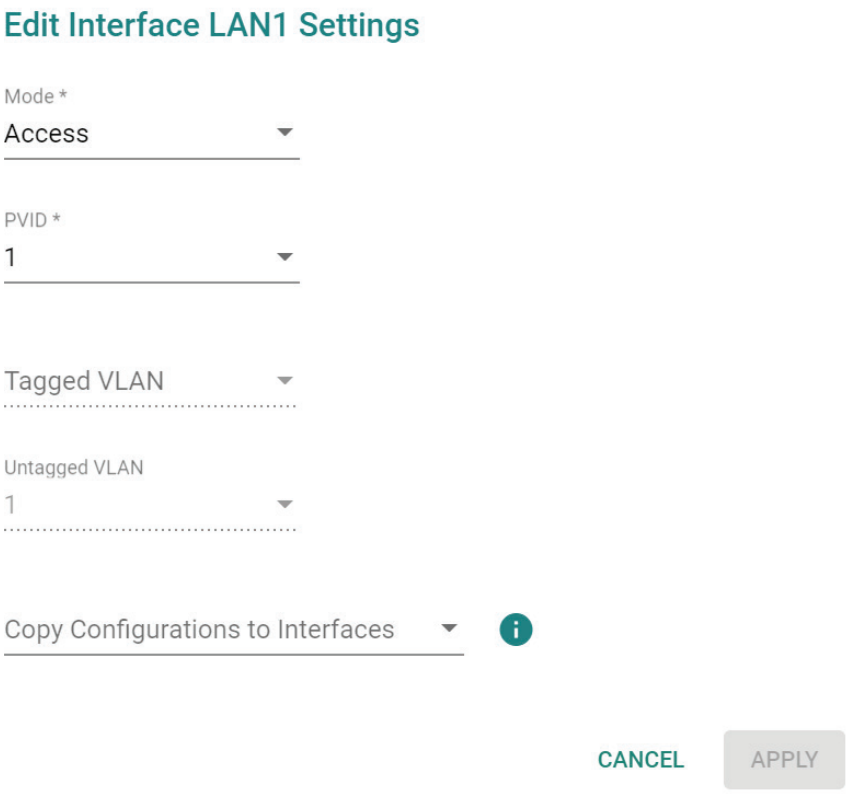
Setting	Description	Factory Default
0 to 32 characters	Enter a name for the VLAN ID.	None

When finished, click **APPLY**.

Edit VLAN Interface Settings

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





Configure the following settings.

Mode

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

PVID

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

Tagged VLAN

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

Untagged VLAN

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

Copy Configurations to Interfaces

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

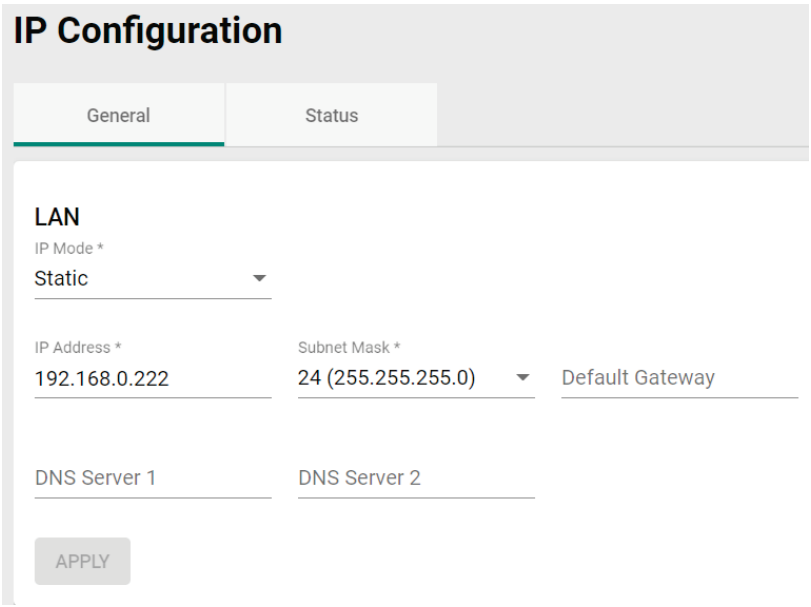
When finished, click **APPLY**.

IP Configuration

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

General Settings

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



Configure the following settings.

IP Mode

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

IP Address

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

Subnet mask

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

Default Gateway

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

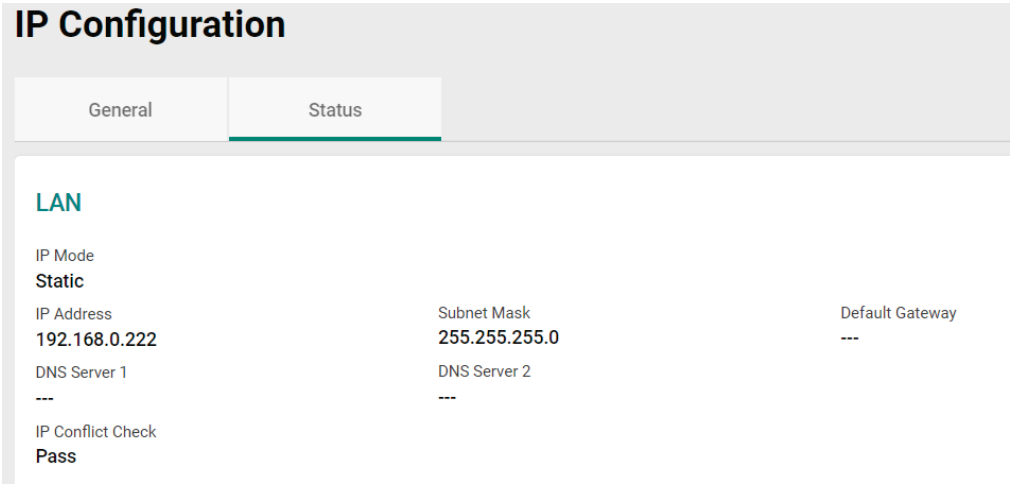
DNS Server 1 and DNS Server 2

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

When finished, click **APPLY**.

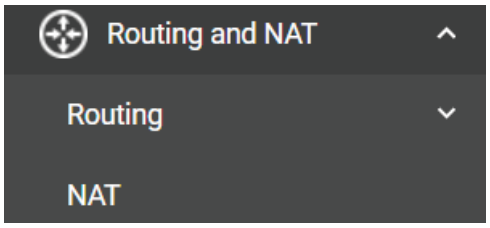
IP Configuration Status

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



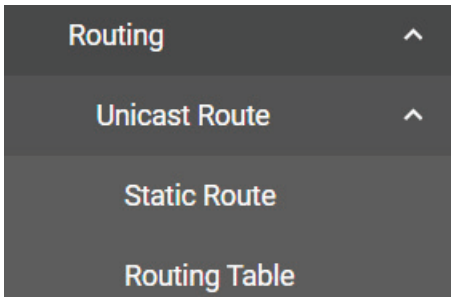
Routing and NAT

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



Routing

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



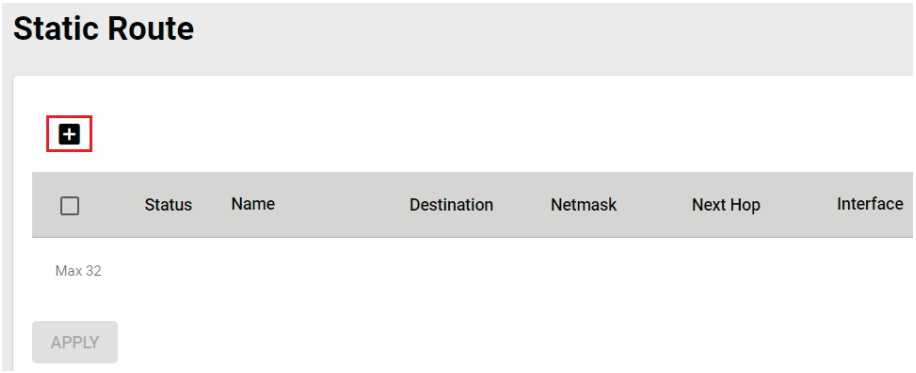
Unicast Route

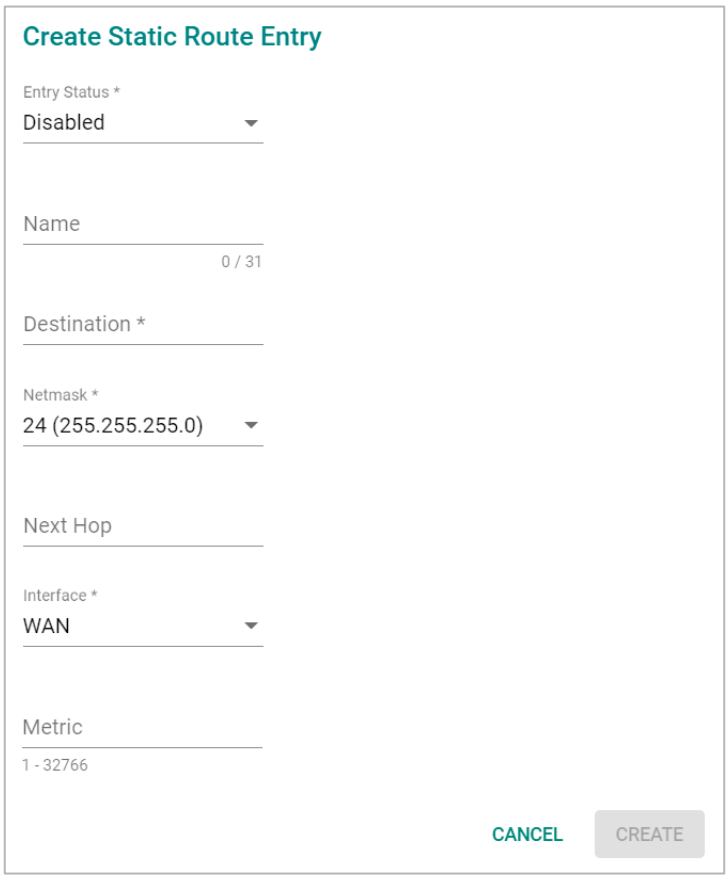
Static Route Settings

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

Create a New Static Route

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





Configure the following settings:

Entry Status

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

Name

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

Destination

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

Netmask

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

Next Hop

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

Interface

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

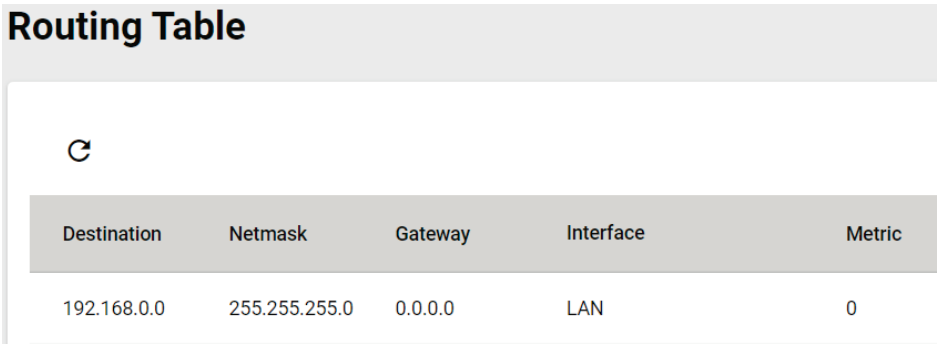
Metric

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

When finished, click **CREATE**.

Routing Table

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

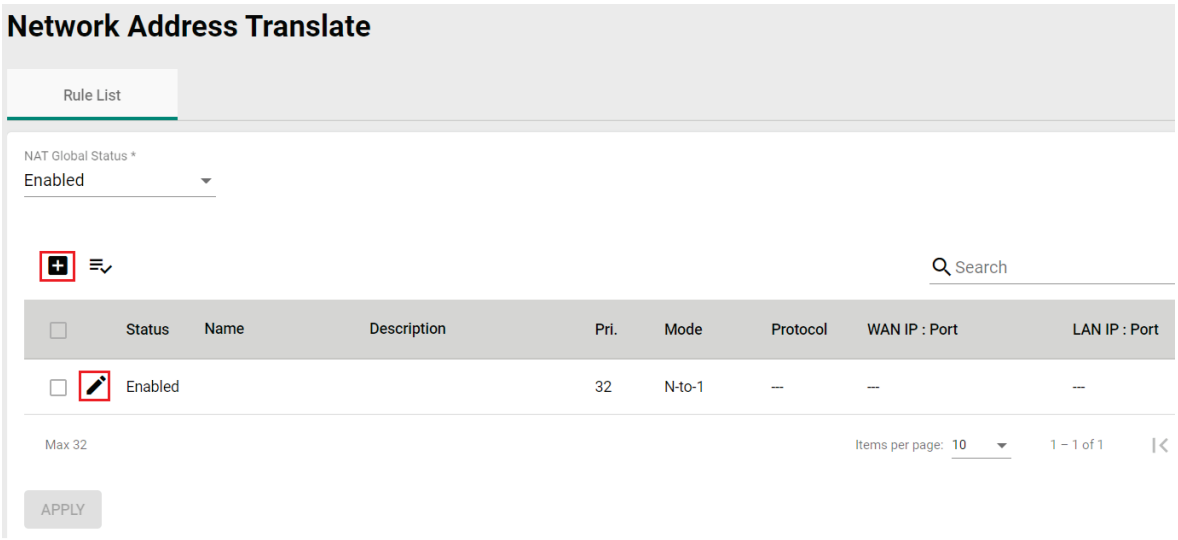


NAT

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

Network Address Translate

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



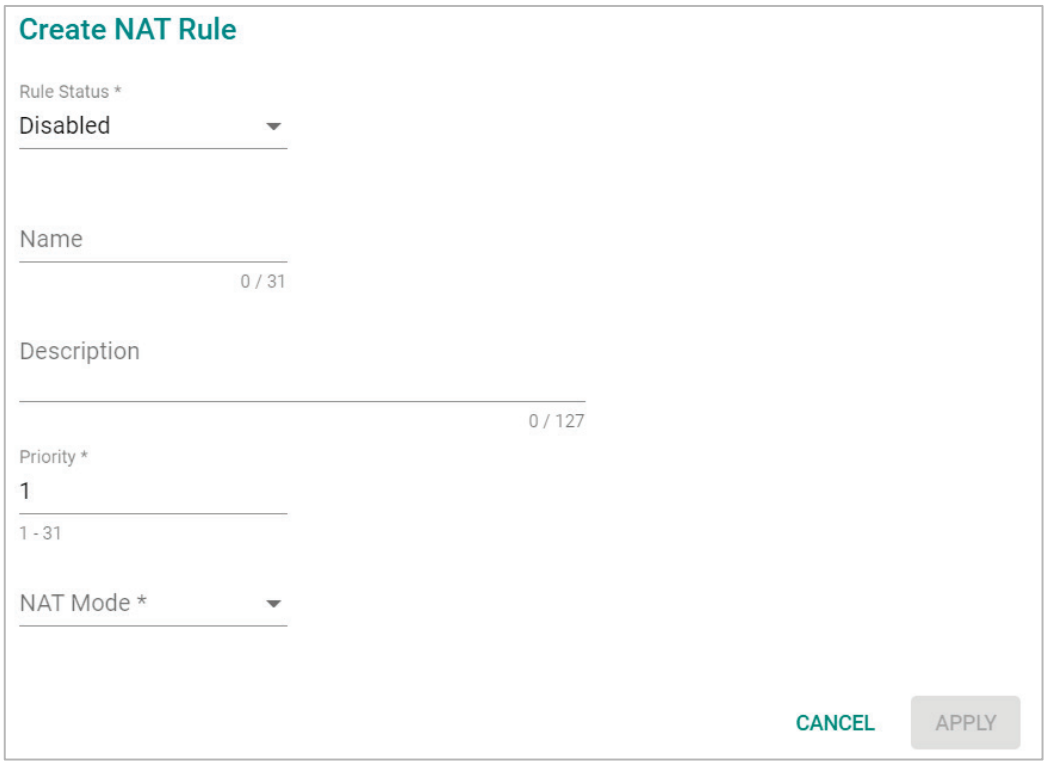
Configure the following setting:

NAT Global Status

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

Add a New NAT Rule

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



Configure the following settings:

Rule Status

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

Name

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

Description

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

Priority

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

NAT Mode

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

Mapping Type (1 to 1 Mode only)

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

Mapping Type (PAT Mode only)

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

Protocol (PAT Mode only)

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

WAN

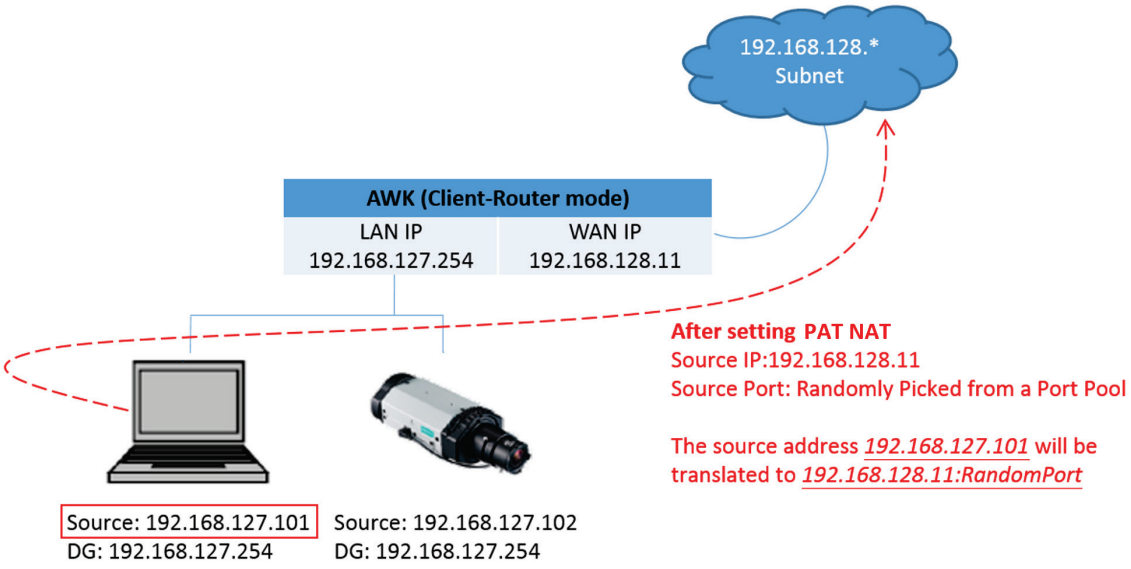
Setting	Description	Factory Default
IP address	For 1-to-1 mode only. Specify the IP address for the WAN.	None
0 to 65535	For PAT mode only. Specify the TCP or UDP port number for the WAN.	None

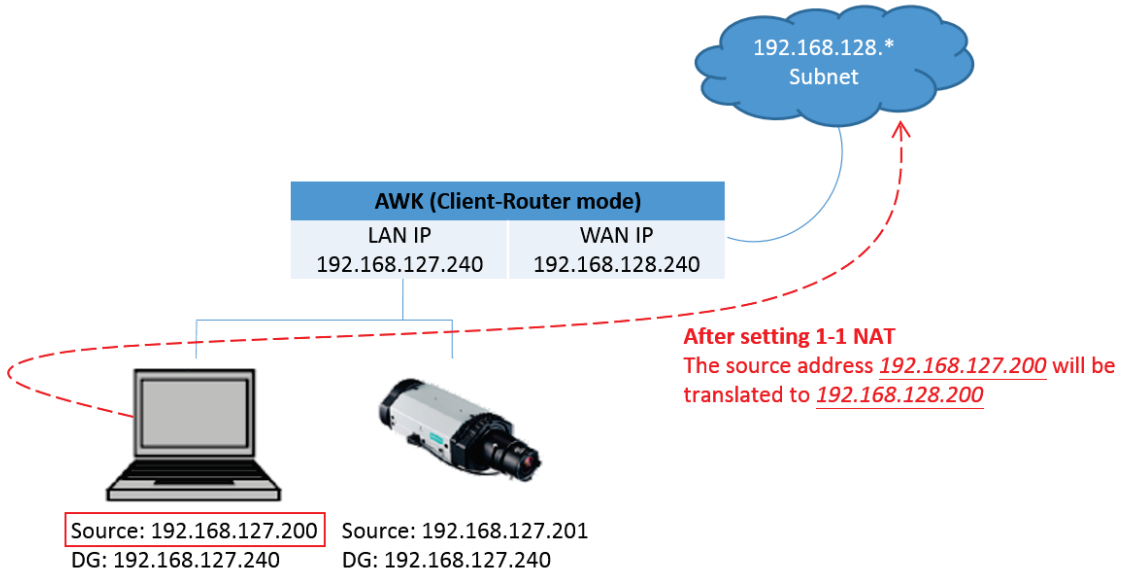
LAN

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

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

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

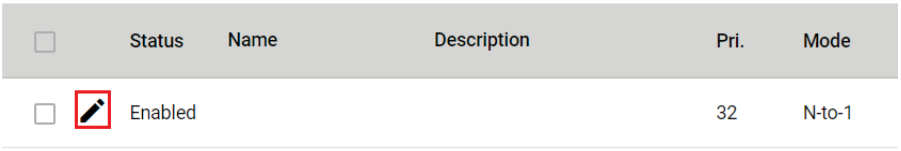


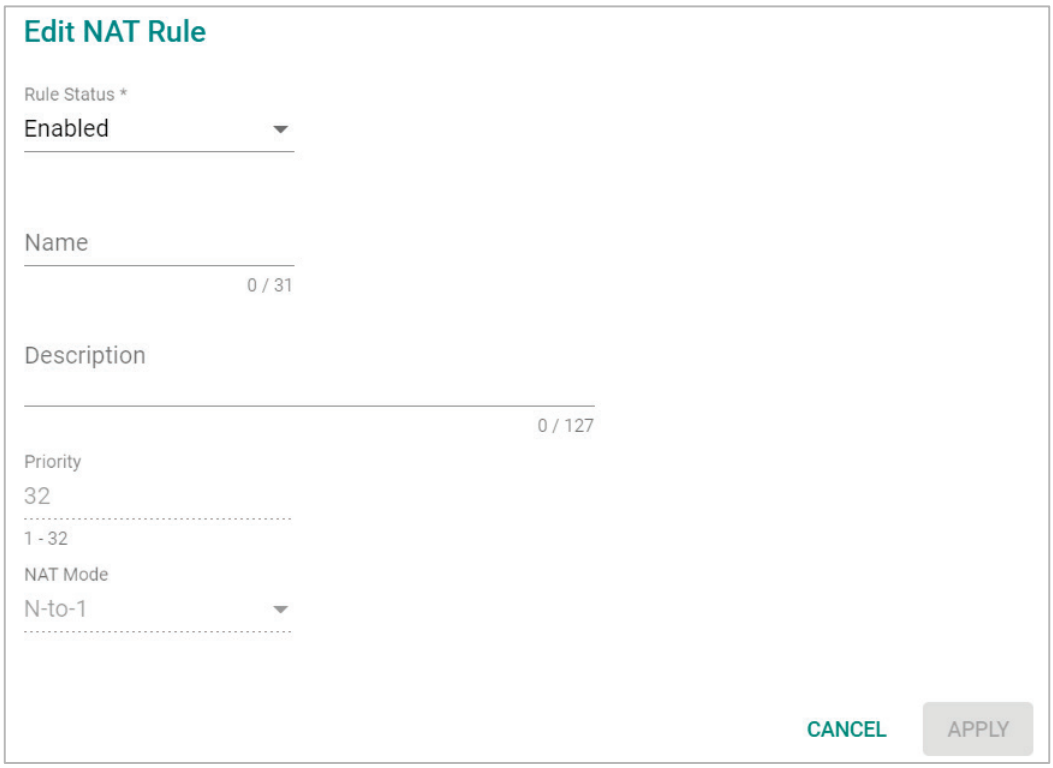


Edit an Existing NAT Rule

To edit an existing NAT rule, click the **Edit** icon next to the rule you want to edit.

Refer to **Create a New NAT Rule** for more information about each setting.

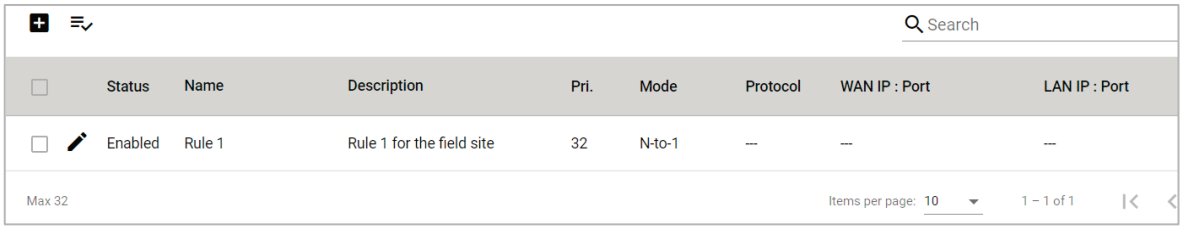




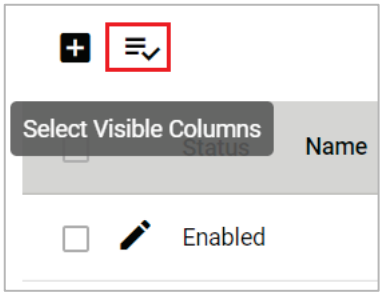
When finished, click **APPLY**.

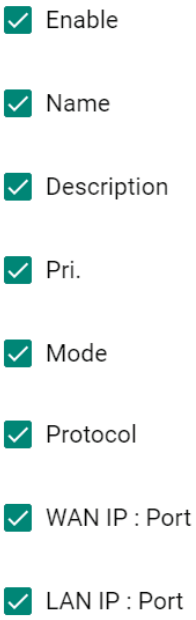
View the NAT Rule Status

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

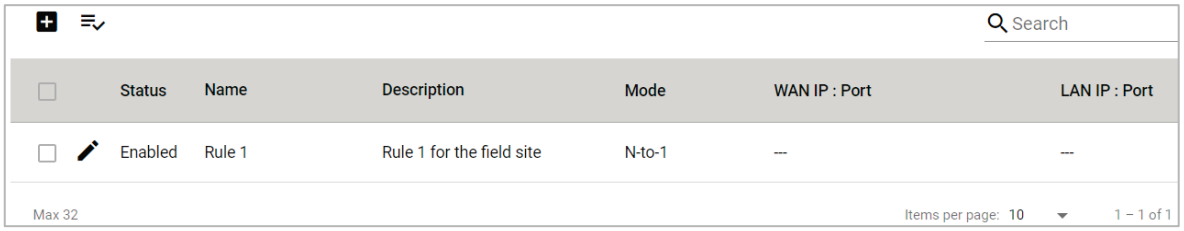


You select what information you want to view by clicking **Select Visible Columns** icon and checking the corresponding check boxes.



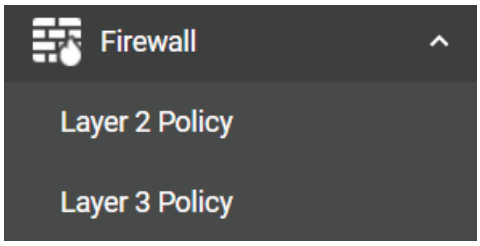


Only information for the selected items will be shown.



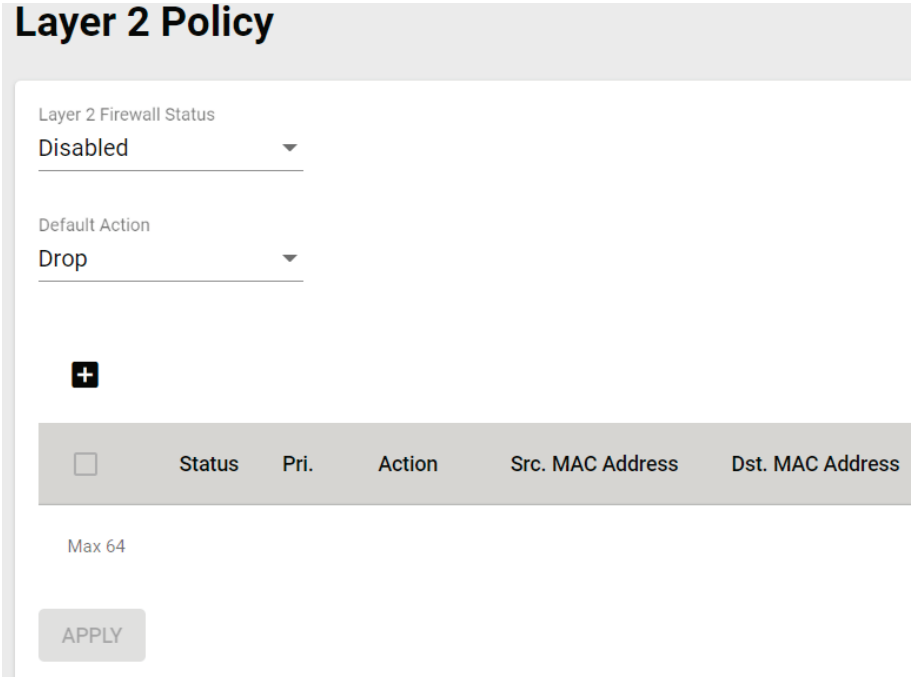
Firewall

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



Layer 2 Policy

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



Configure the following settings:

Layer 2 Firewall Status

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

Default Action

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

ATTENTION

Be careful when configuring the packet filtering function:

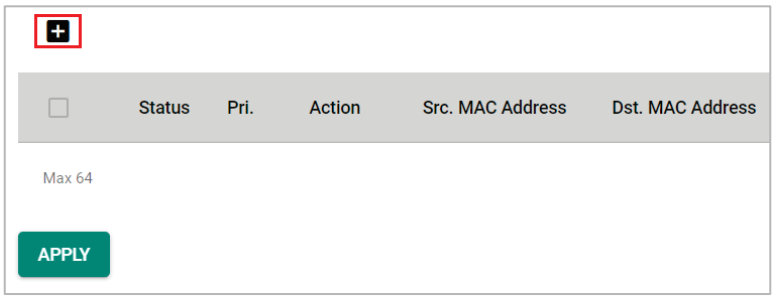
If the default action is set to **Drop** and **all rules are disabled, all packets will be allowed**.

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

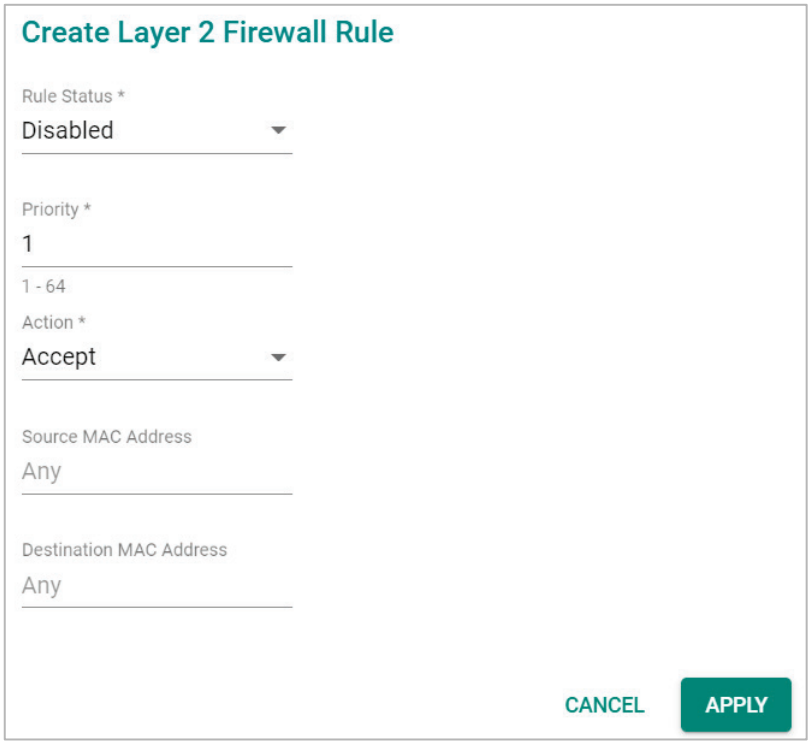
When finished, click **APPLY** to save your changes.

Add a New Layer 2 Firewall Rule

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



Configure the following settings:



Rule Status

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

Priority

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

Default Action

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

ATTENTION

Be careful when configuring the packet filtering function:

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

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

Source MAC Address

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

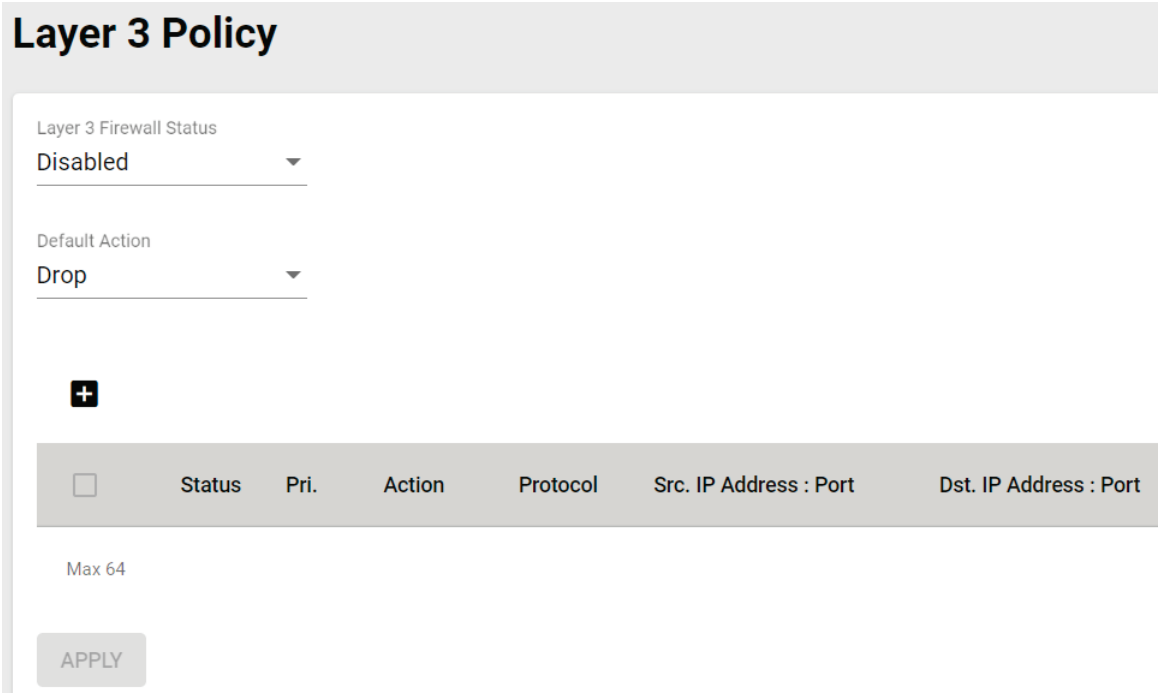
Destination MAC Address

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

When finished, click **APPLY**.

Layer 3 Policy

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



Configure the following settings.

Layer 3 Firewall Status

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

Default Action

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

ATTENTION

Be careful when configuring the packet filtering function:

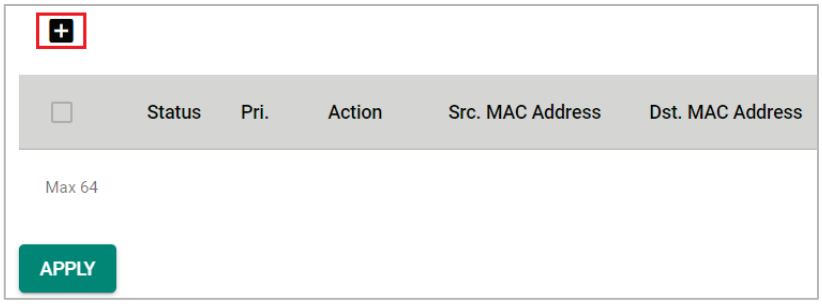
If the default action is set to **Drop** and **all rules are disabled, all packets will be allowed**.

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

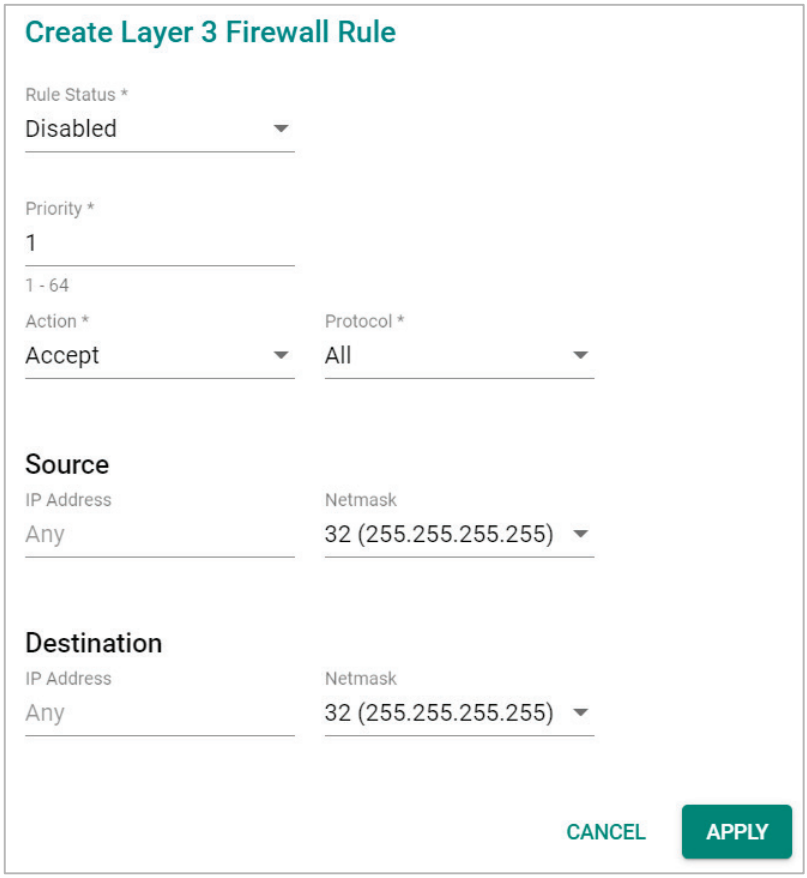
When finished, click **APPLY**.

Add a New Layer 3 Firewall Rule

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



Configure the following settings:



Rule Status

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

Priority

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

Default Action

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

Protocol

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

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

Source

IP Address

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

Netmask

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

Port Range

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

Destination

IP Address

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

Netmask

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

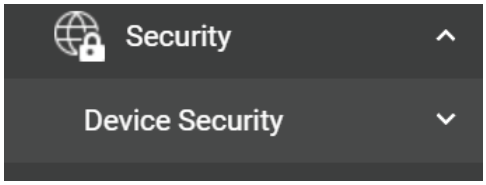
Port Range

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

When finished, click **APPLY**.

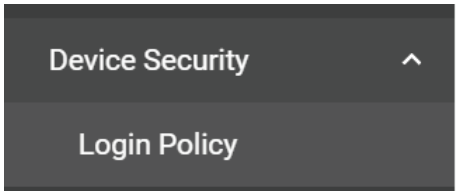
Security

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



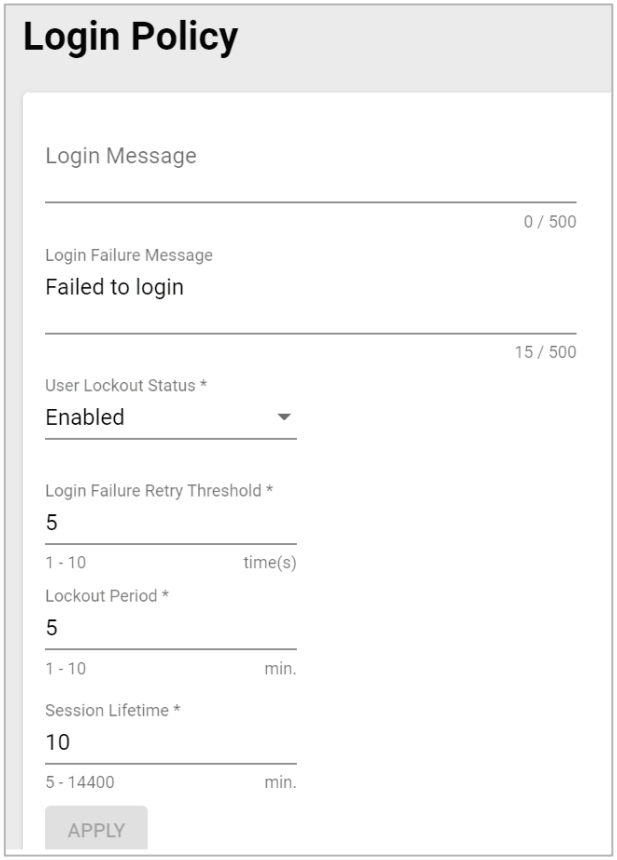
Device Security

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



Login Policy

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



Configure the following settings:

Login Message

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

Login Failure Message

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

User Lockout Status

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

Login Failure Retry Threshold

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

Lockout Period

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

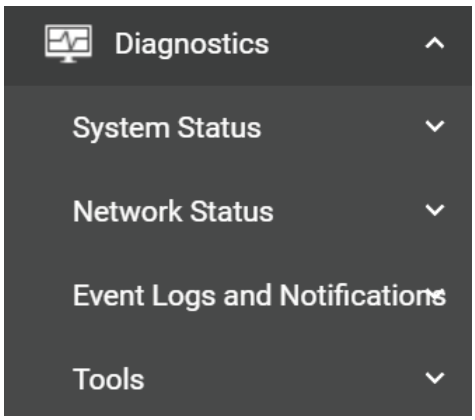
Session Lifetime

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

When finished, click **APPLY**.

Diagnostics

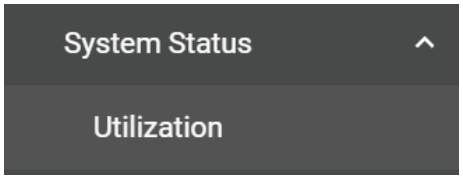
The **Diagnostics** section is used for monitoring and troubleshooting and includes the **System Status, Network Status, Event Logs and Notifications**, and **Tools** pages.



System Status

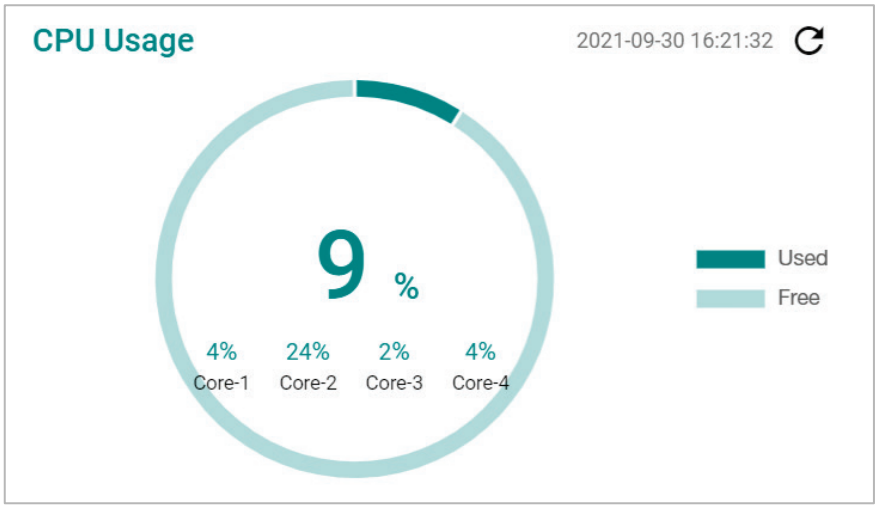
Utilization

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



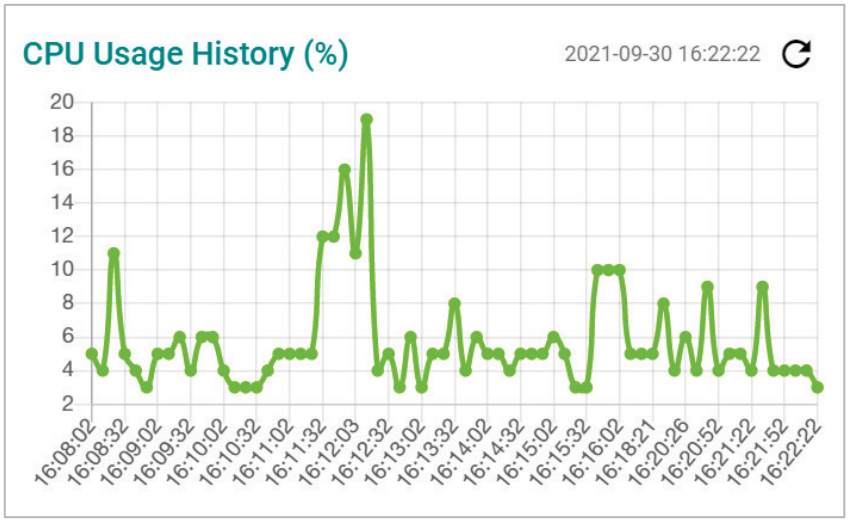
CPU Usage

This widget shows the current CPU usage.



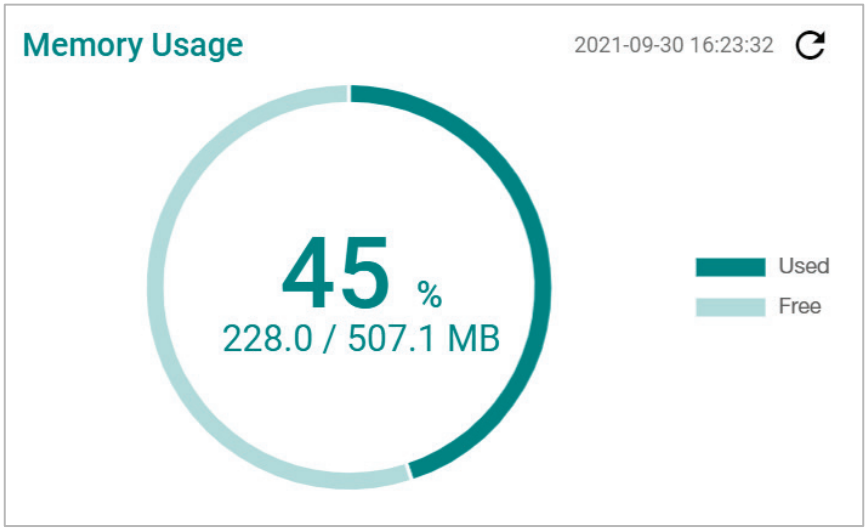
CPU Usage History

The graph shows the CPU usage history.



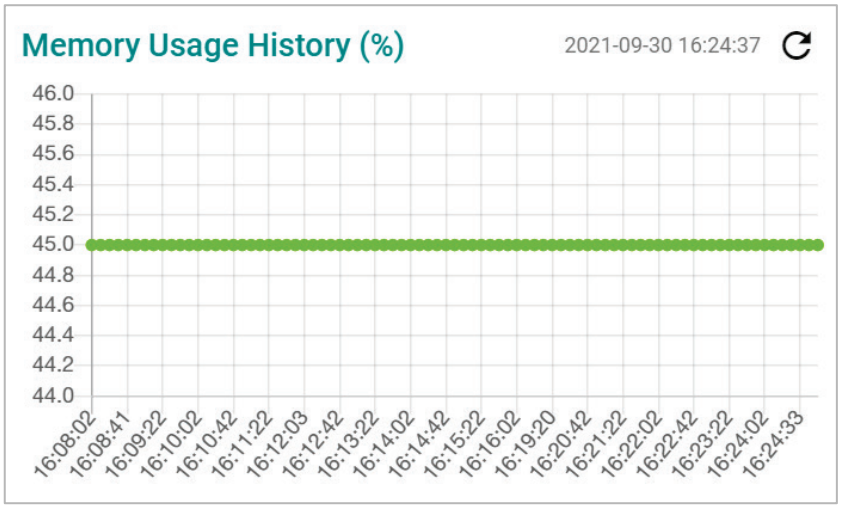
Memory Usage

This widget shows the current memory usage.



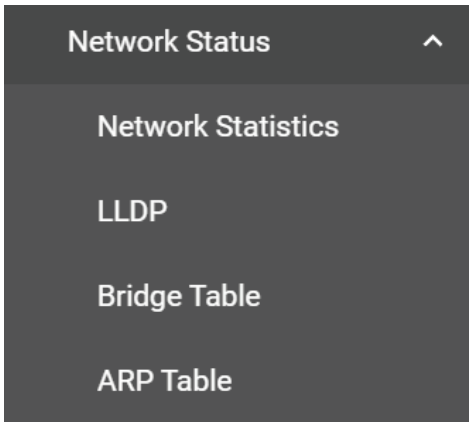
Memory Usage History

This graph shows the memory usage history.



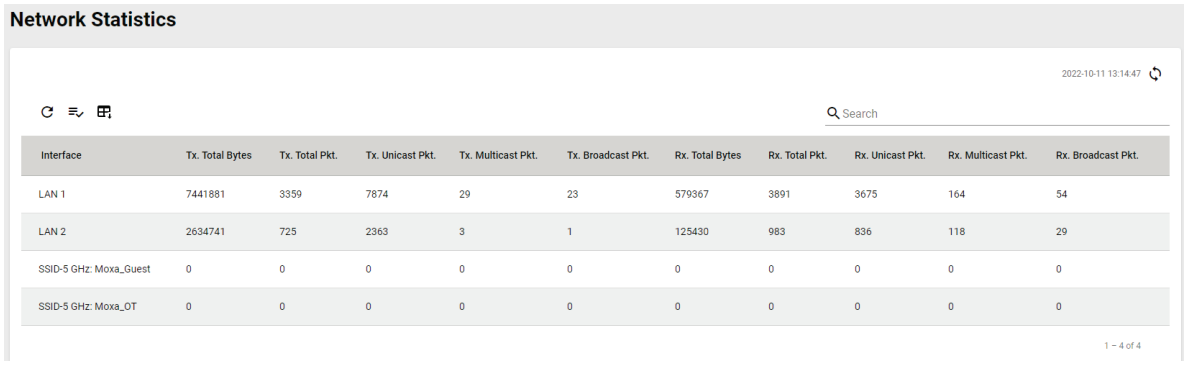
Network Status

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



Network Statistics

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



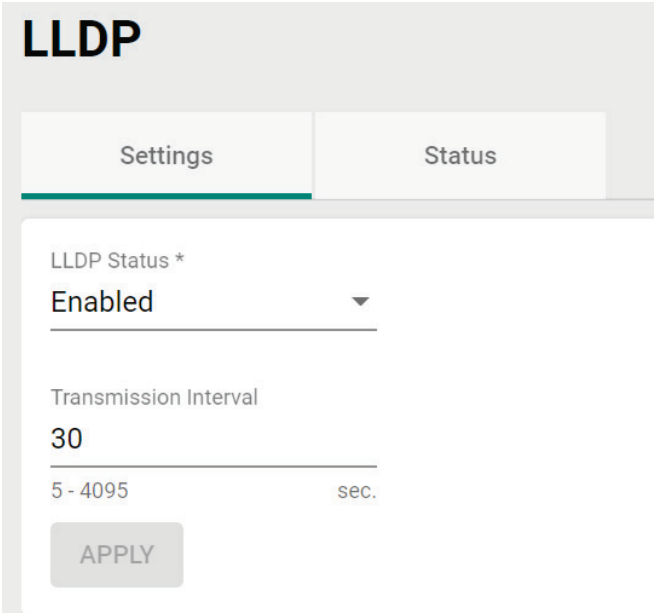
LLDP

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

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

LLDP Settings

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



Configure the following settings:

LLDP Status

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

Transmission Interval

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

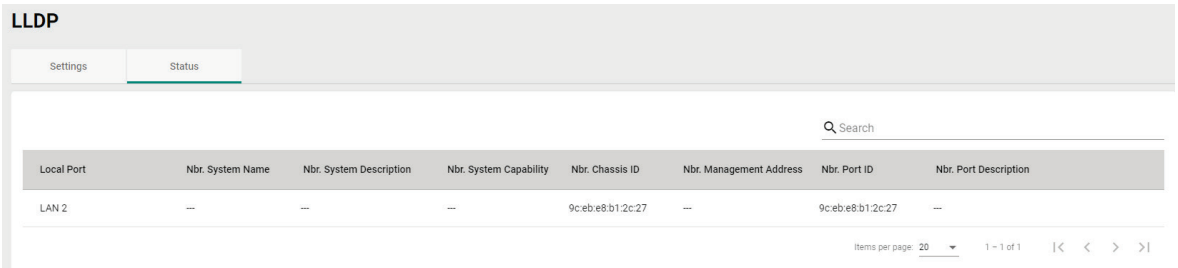
NOTE

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

When finished, click **APPLY**.

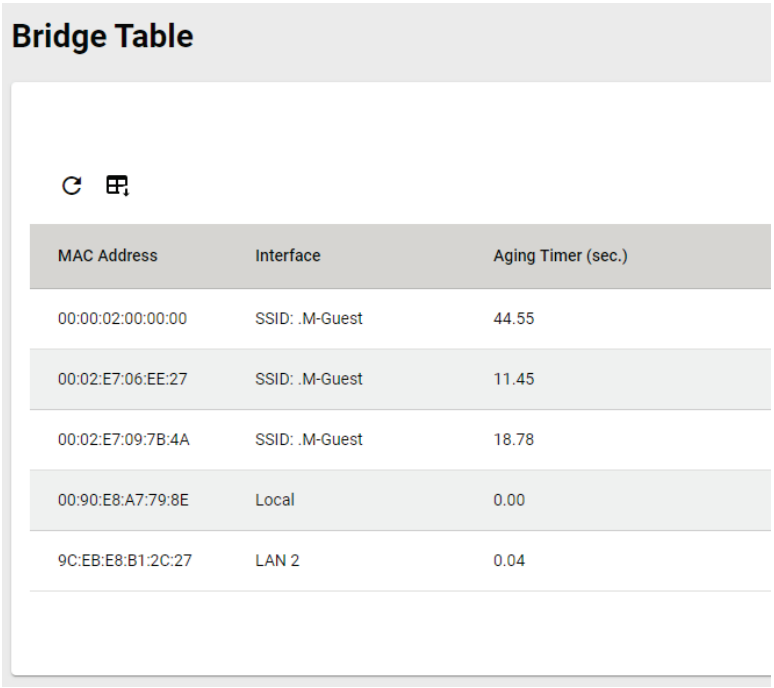
LLDP Status

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



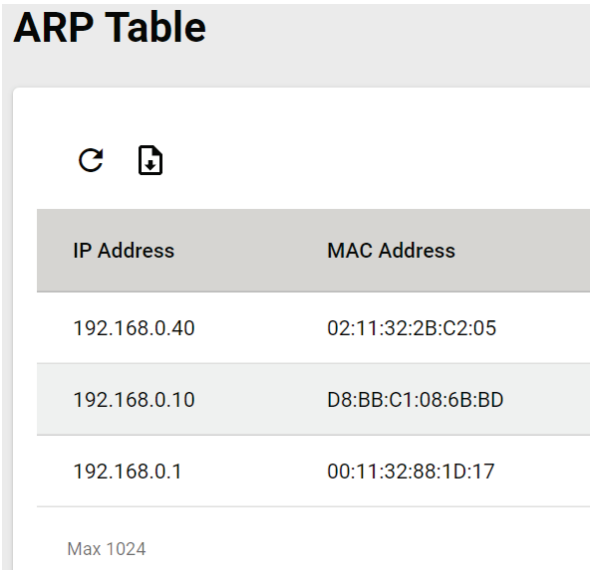
Bridge Table

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



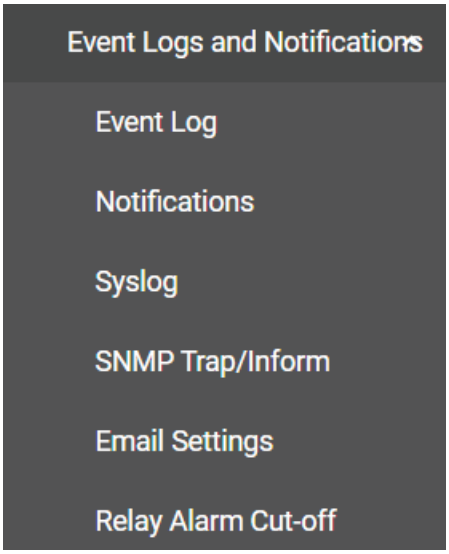
ARP Table

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



Event Logs and Notifications

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

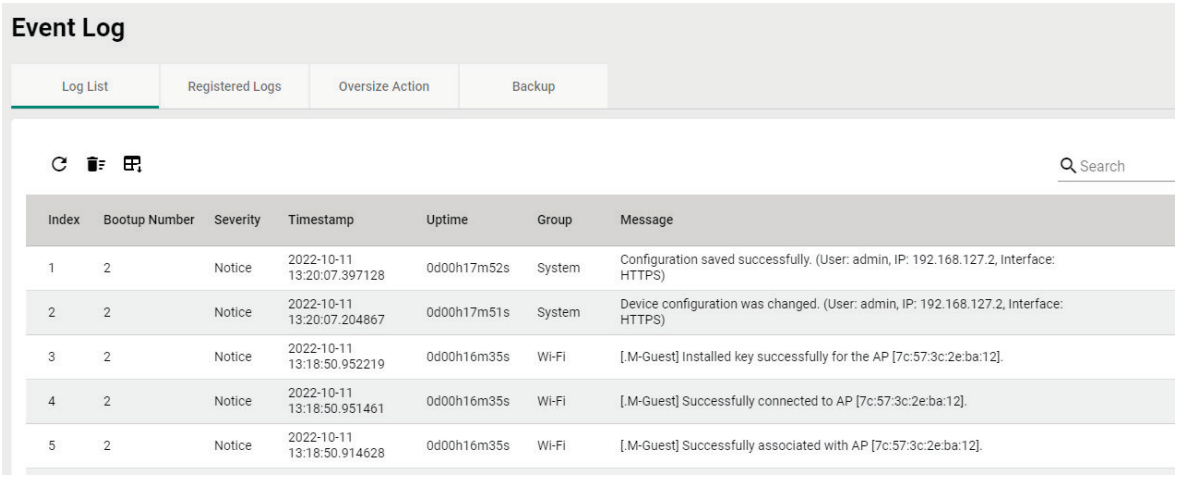


Event Log

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

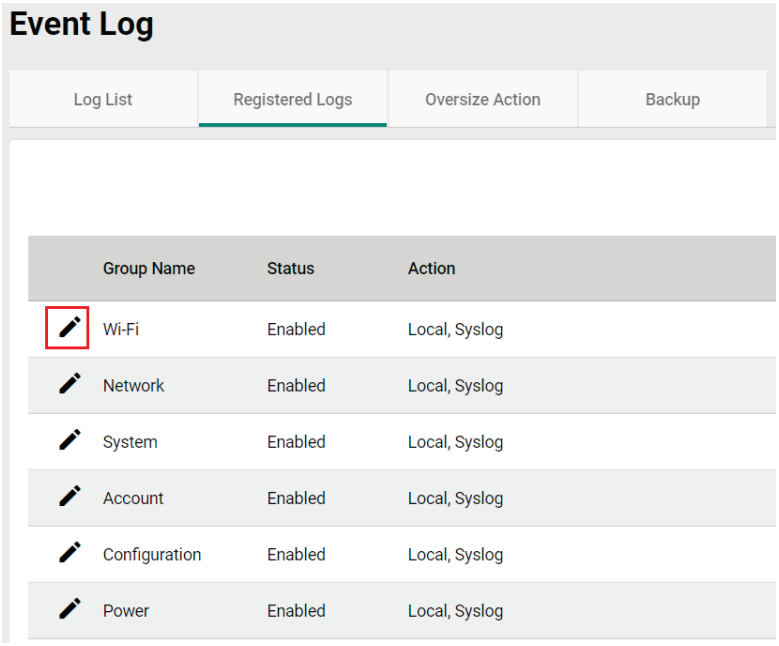
Log List

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

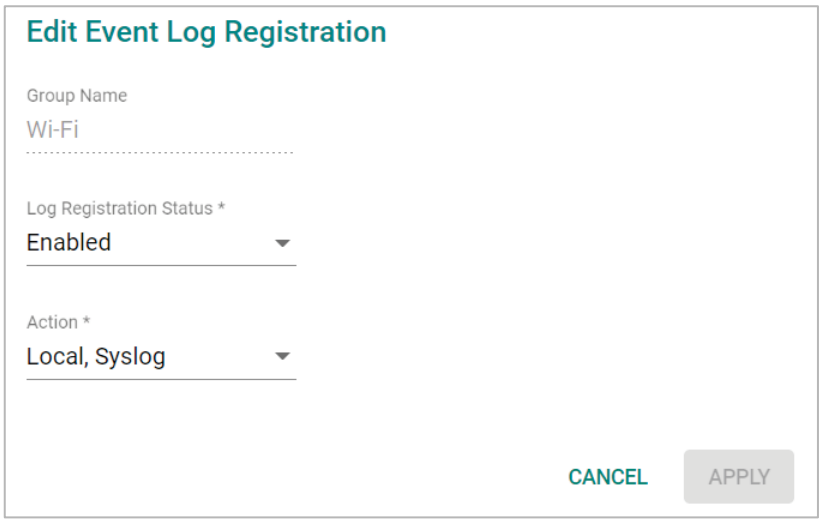


Registered Logs

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



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



Configure the following settings:

Log Registration Status

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

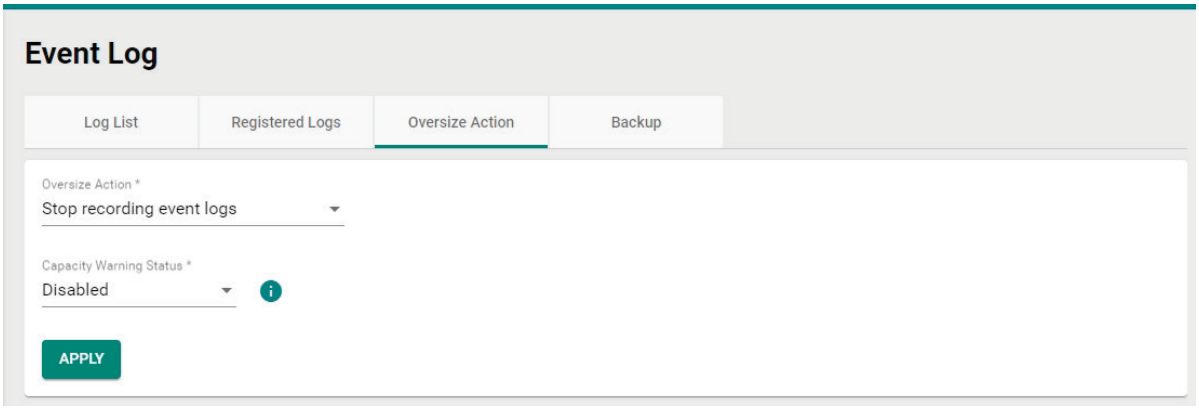
Action

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

When finished, click **APPLY**.

Oversize Action

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



Configure the following settings:

Oversize-Action

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

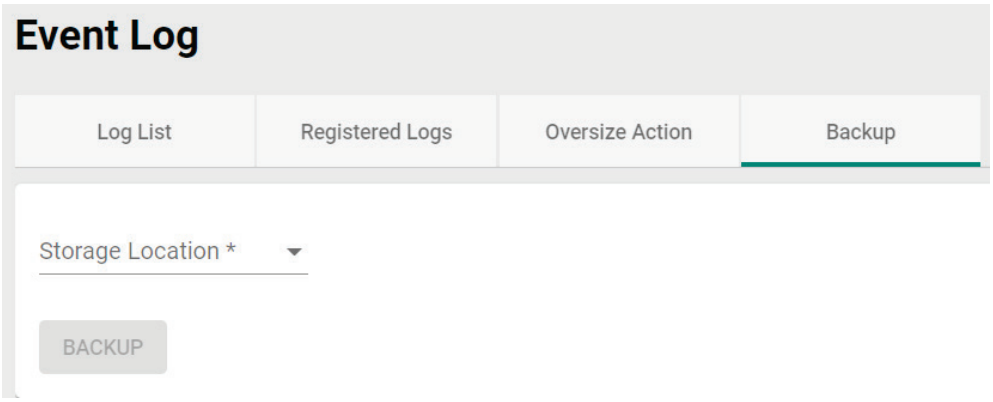
Capacity Warning

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

When finished, click **APPLY**.

Backup

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



Storage Location

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

Server IP Address (for TFTP only)

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

File Name (for TFTP only)

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

Server IP Address (for SFTP only)

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

Pathname (for SFTP only)

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

Account (for SFTP only)

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

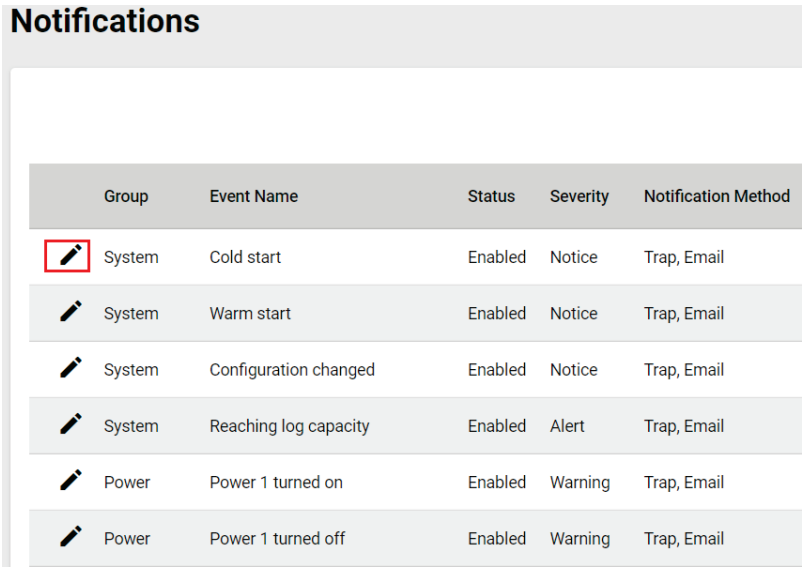
Password (for SFTP only)

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

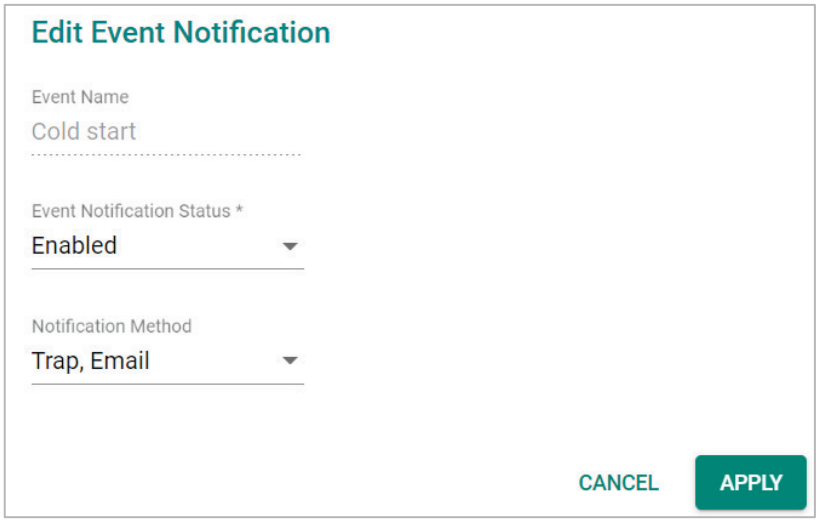
When finished, click **BACKUP**.

Notifications

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



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



Configure the following settings:

Event Notification Status

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

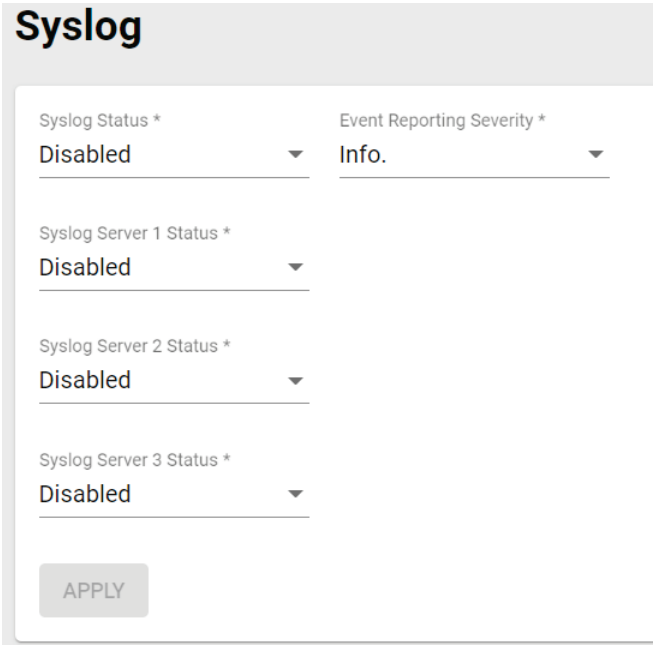
Notification Method

Setting	Description	Factory Default
Trap	Send notifications through SNMP Trap.	Trap/Email
Email	Send notifications through email.	
Relay	Use a relay for sending notifications. This option is only available for specific event groups.	

When finished, click **APPLY**.

Syslog

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



Configure the following settings:

Syslog Status

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

Event Reporting Severity

Setting	Description	Factory Default
Emerg.	Specify the syslog severity as Emergency.	Info.
Alert	Specify the syslog severity as Alert.	
Crit.	Specify the syslog severity as Critical.	
Error	Specify the syslog severity as Error.	
Warning	Specify the syslog severity as Warning	
Notice	Specify the syslog severity as Notice.	
Info.	Specify the syslog severity as Information.	

Syslog Server 1 Status

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

Syslog Server 2 Status

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

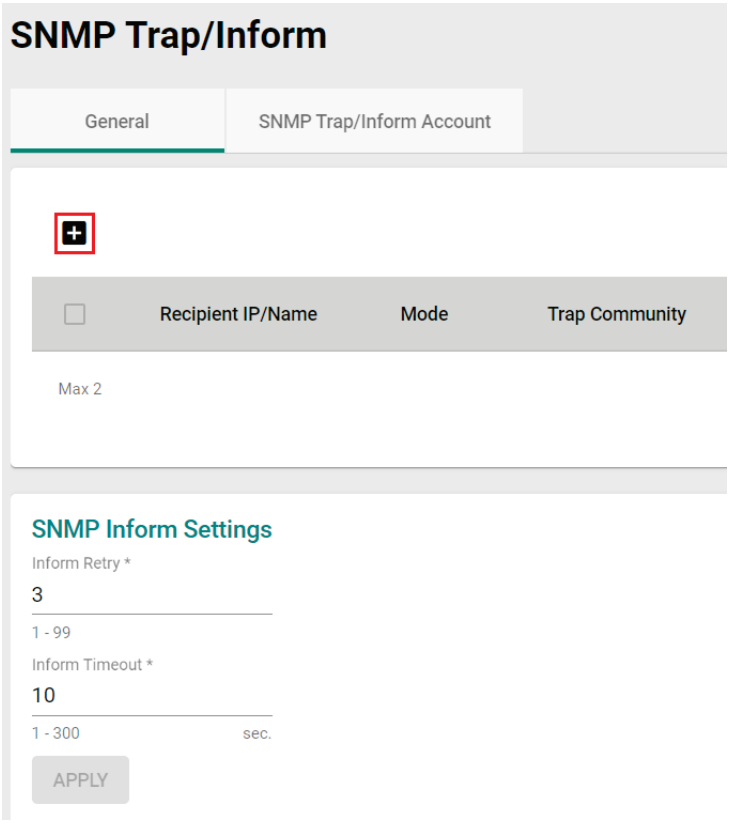
Syslog Server 3 Status

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

When finished, click **APPLY**.

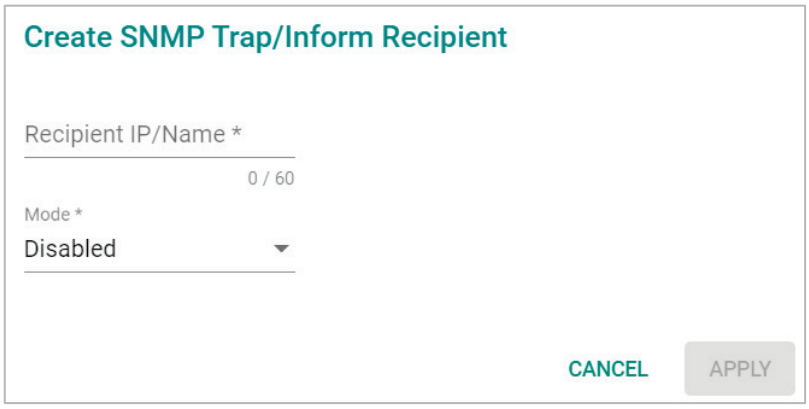
SNMP Trap/Inform

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.


SNMP Trap/Inform
General
SNMP Trap/Inform Account
Recipient IP/Name
Mode
Trap Community
Max 2
SNMP Inform Settings
Inform Retry *
3
1 - 99
Inform Timeout *
10
1 - 300
sec.
APPLY

General Settings

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



Configure the following settings:

Recipient IP/Name

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

Mode

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

When finished, click **APPLY**.

SNMP Inform Settings

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

Inform Retry

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

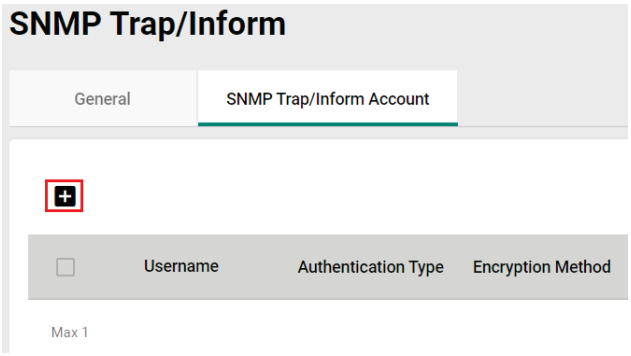
Timeout

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

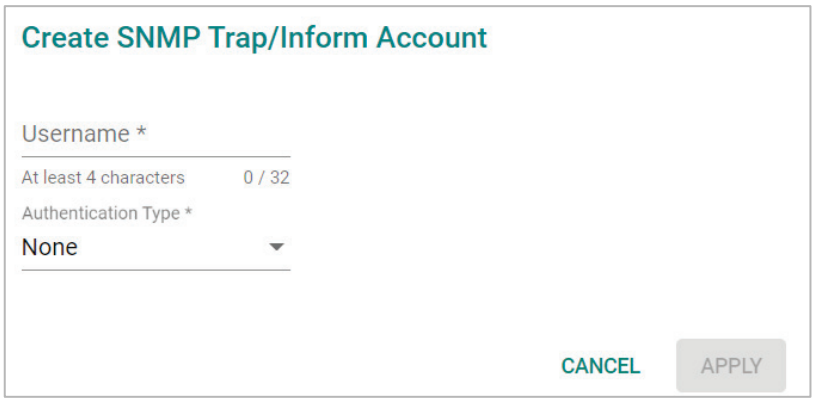
When finished, click **APPLY**.

SNMP Trap/Inform Account Settings

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



Configure the following settings:



Username

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

Authentication type

Setting	Description	Factory Default
None	Do not use any authentication mechanism.	None
MD5	Use MD5 as the authentication type.	
SHA	Use SHA as the authentication type.	

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

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

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

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

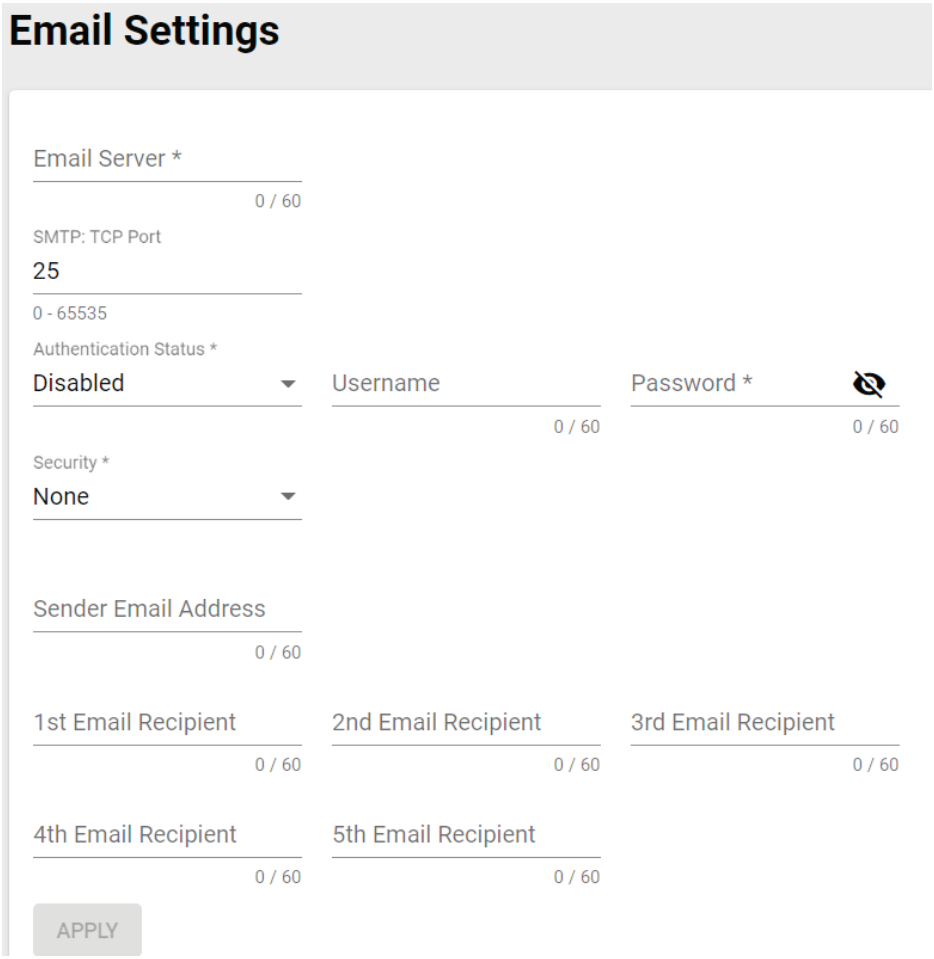
Encryption Key (when DES and AES is selected)

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

When finished, click **APPLY**.

Email Settings

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



Configure the following settings.

Email Server

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

SMTP: TCP Port

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

Authentication Status

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

Username

Setting	Description	Factory Default
Max. 60 characters	Enter the email user account.	None

Password

Setting	Description	Factory Default
Max. of 60 characters	Enter the email user password	None

Security

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

Sender Email Address

Setting	Description	Factory Default
Max. 60 characters	Enter the sender's email address.	None

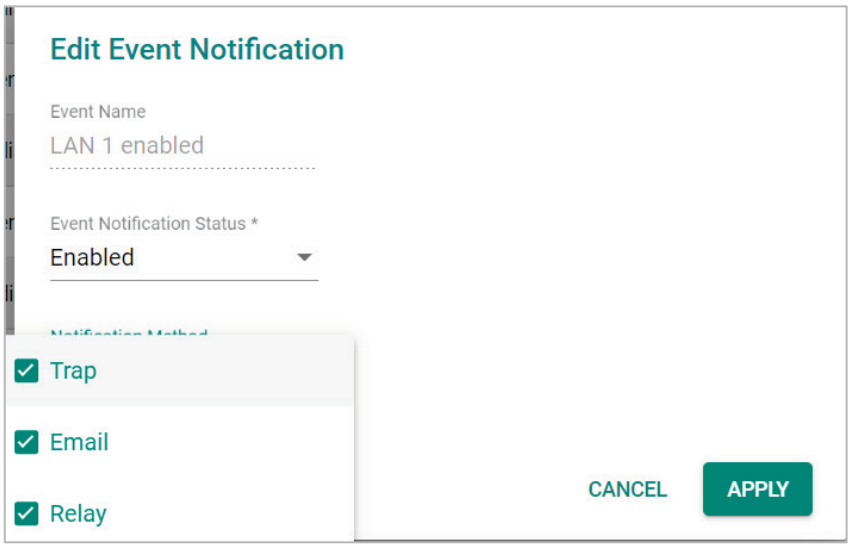
1st to 5th Email Addresses

Setting	Description	Factory Default
Max. 60 characters	Enter the recipient's email address. You can set up to five recipient email addresses to receive alert emails from the AWK device.	None

When finished, click **APPLY**.

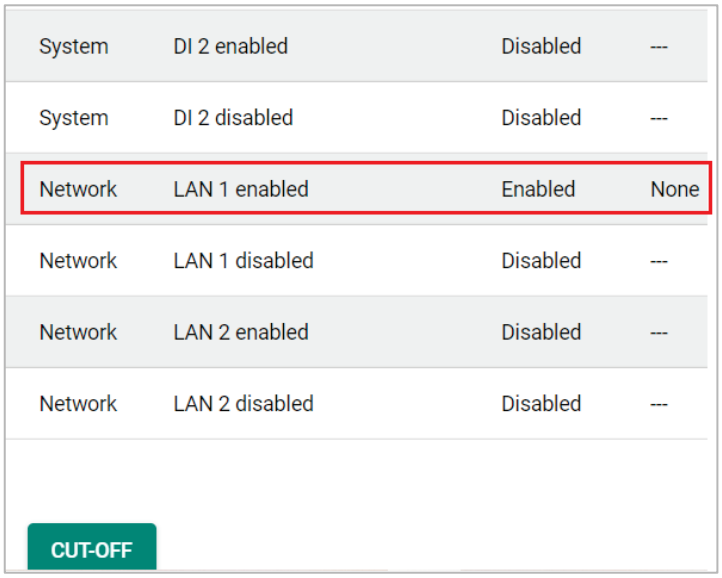
Relay Alarm Cut-off

Some events can be triggered by relay. If Relay is set as the notification method in the **Notifications** section, you will see the state for that event is **Triggered** when the corresponding event occurs. Once triggered, you can cut off the relay to deactivate the event. Click **Relay Alarm Cut-off** under **Diagnostics > Event Logs and Notifications** in the function menu to access this screen.



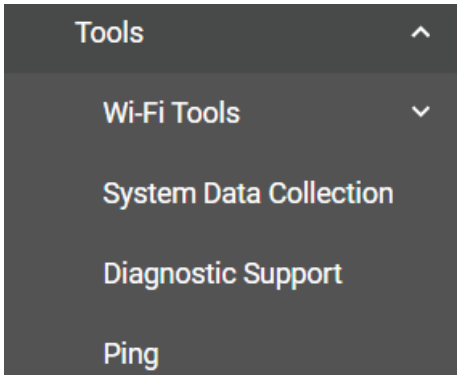
Group	Event Name	Status	State
System	Reaching log capacity	Disabled	---
Power	Power 1 turned off	Disabled	---
Power	Power 2 turned off	Disabled	---
System	DI 1 enabled	Disabled	---
System	DI 1 disabled	Disabled	---
System	DI 2 enabled	Disabled	---
System	DI 2 disabled	Disabled	---
Network	LAN 1 enabled	Enabled	Triggered
Network	LAN 1 disabled	Disabled	---
Network	LAN 2 enabled	Disabled	---
Network	LAN 2 disabled	Disabled	---

Click CUT-OFF to deactivate the event.



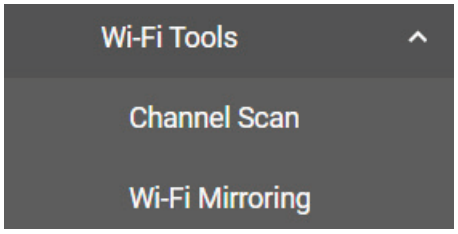
Tools

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



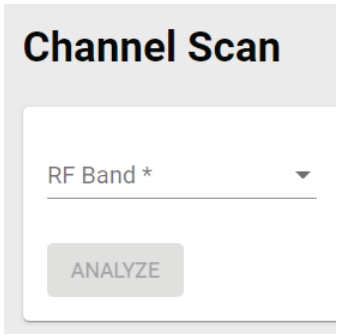
Wi-Fi Tools

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



Channel Scan

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



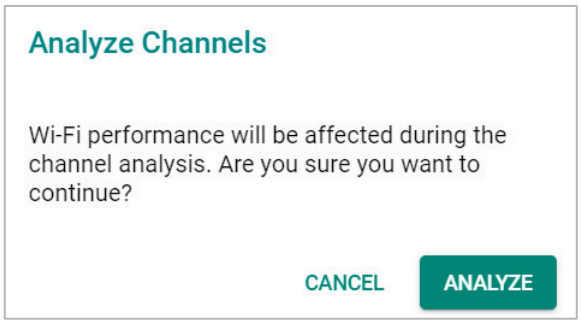
Configure the following setting:

RF Band

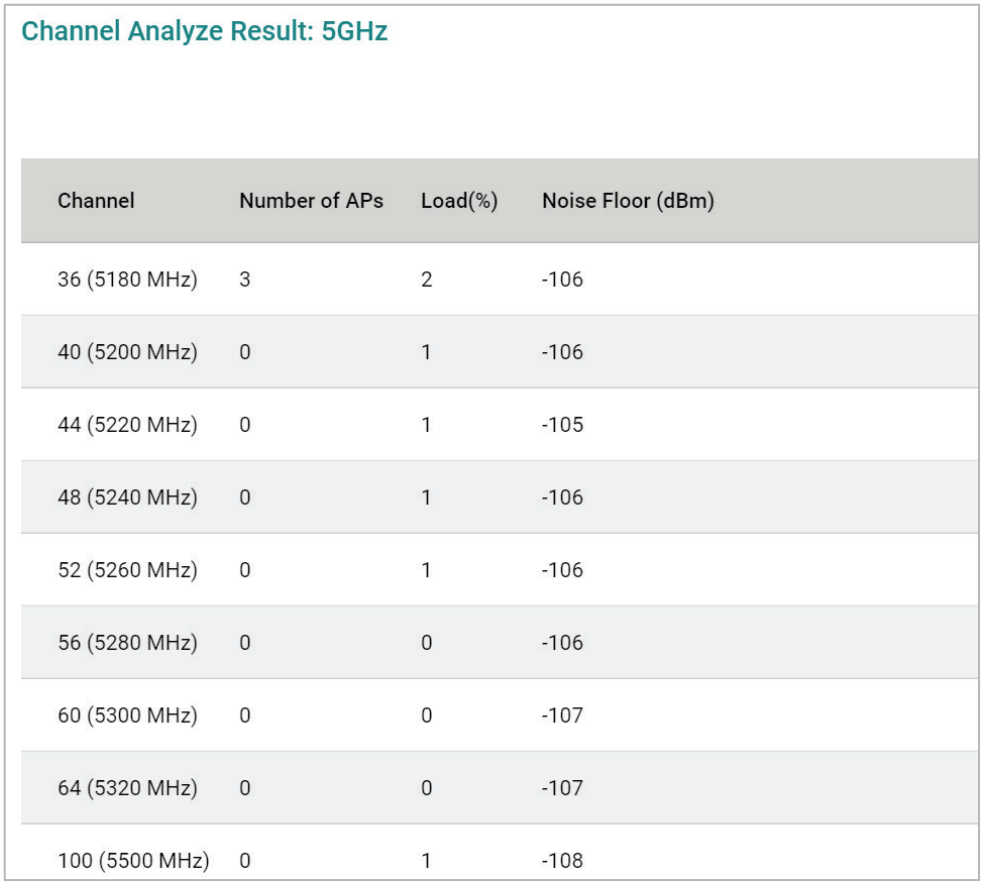
Setting	Description	Factory Default
5 GHz	Scan the 5 GHz RF band.	None
2.4 GHz	Scan the 2.4 GHz RF band.	
5 GHz & 2.4 GHz	Scan both 5 GHz and 2.4 GHz RF bands.	

When finished, click **ANALYZE**.

When prompted, click **ANALYZE** again.



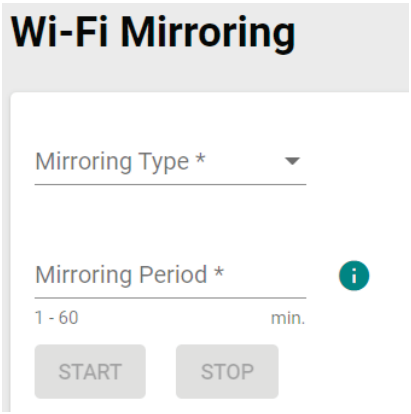
The result of the scan will be shown in the table at the bottom of the page.



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

Wi-Fi Mirroring

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



Configure the following settings.

Mirroring Type

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

Mirroring Period (Local Type only)

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

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

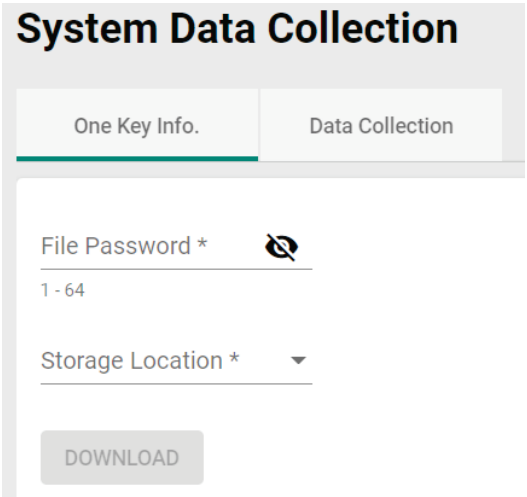
The result of the mirroring will be shown below. If you selected Local as the mirroring type, click **DOWNLOAD** to download the result to your local machine.

System Data Collection

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

Download One Key Information

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



Configure the following settings:

File Password

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

Storage Location

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

Server IP Address (for TFTP only)

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

Server IP Address (for SFTP only)

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

Server Account (for SFTP only)

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

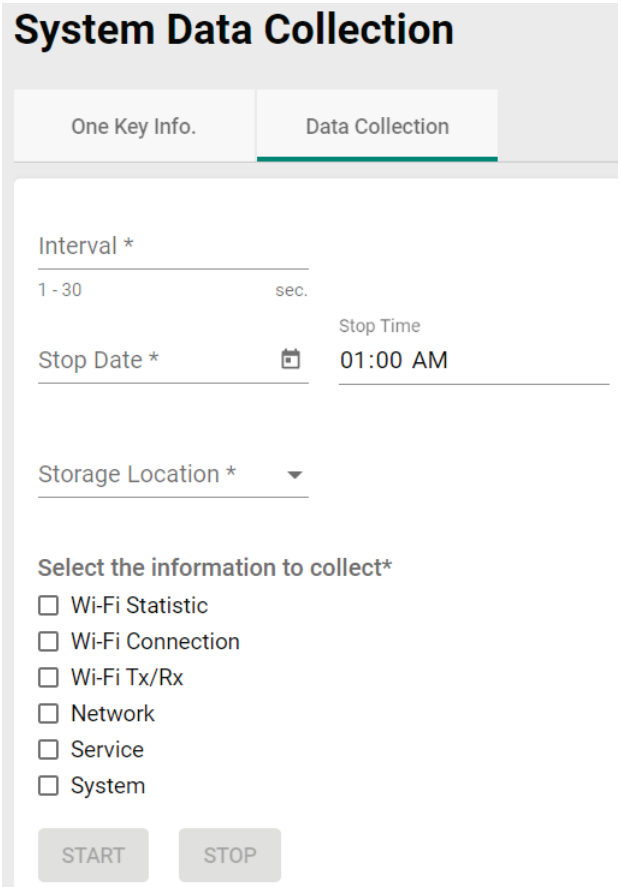
Server Password (for SFTP only)

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

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

Data Collection

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



Configure the following settings:

Interval

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

Stop Date

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

Stop Time

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

Storage Location

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

Server IP Address (for TFTP only)

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

Server IP Address (for SFTP only)

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

Server Account (for SFTP only)

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

Server Password (for SFTP only)

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

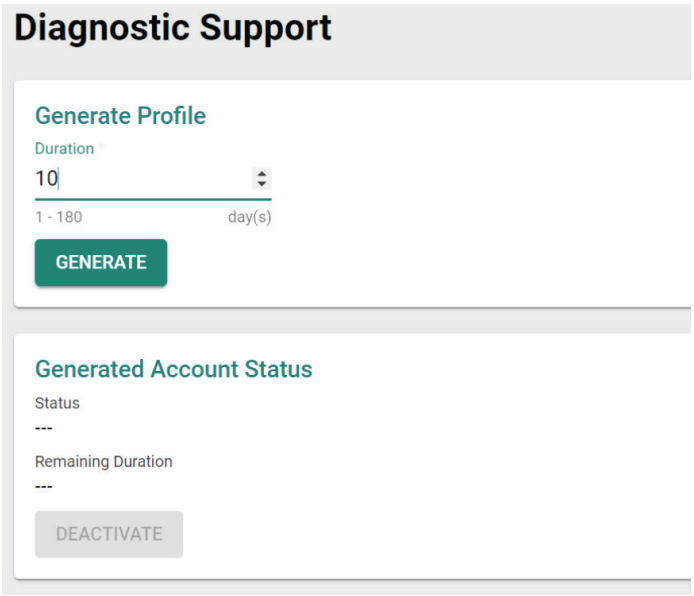
Select the information to collect

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

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

Diagnostic Support

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



Duration

Setting	Description	Factory Default
1 to 180 (days)	Specify how long the diagnostics account will be active for.	None

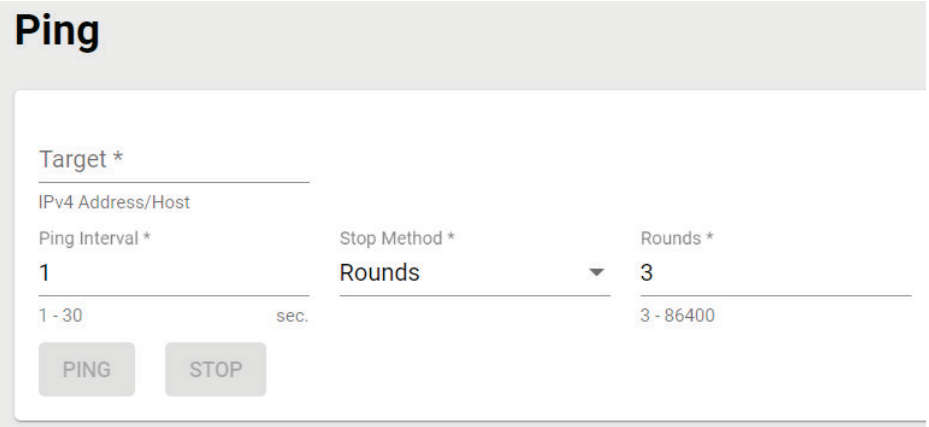
You can check the account status at any time in the bottom section of the screen. Click **DEACTIVATE** to immediately terminate a generated diagnostics account.

NOTE

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

Ping

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



Configure the following settings:

Target

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

Ping Interval

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

Stop Method

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

Rounds (for Rounds Method only)

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

End Date (for Timestamps Method only)

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

End Time (for Timestamps Method only)

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

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

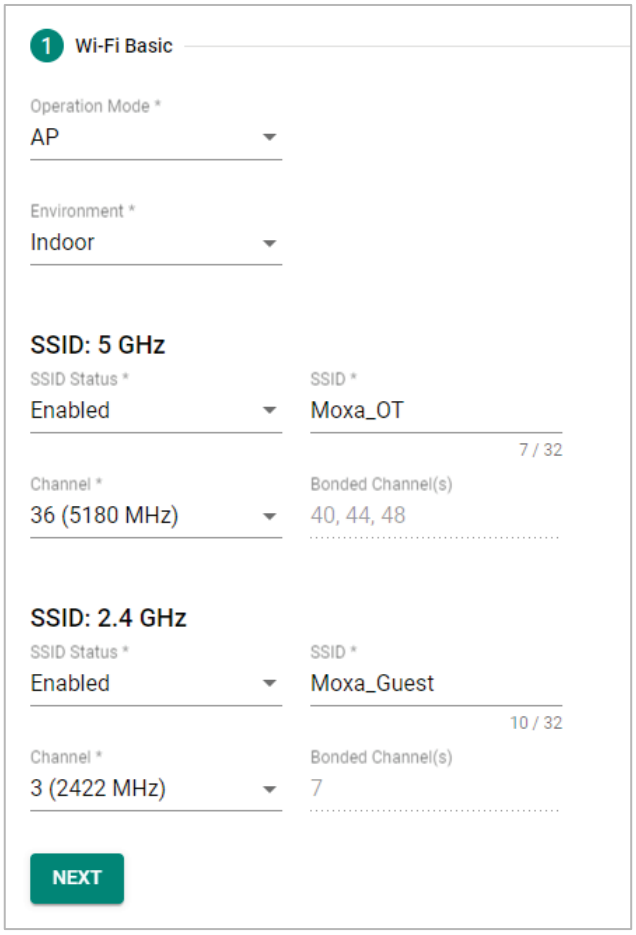
Setup Wizard

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

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

Wi-Fi Basic

Configure the following settings:



Operation Mode

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

Environment

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

SSID: 2.4 GHZ

SSID Status

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

SSID

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

Channel (available in AP and Master modes only)

Setting	Description	Factory Default
1 (2412 MHz) to 11 (2462 MHz)	Select the channel from the drop-down list. Each channel supports different frequencies.	6 (2437 MHz)

Bonded Channel (available in AP and Master modes only)

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

SSID: 5 GHZ

SSID Status

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

SSID

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

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

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

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

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

Channel (for AP and Master modes only)

Setting	Description	Factory Default
36 (5180 MHz) to 165 (5825 MHz)	Select the channel from the drop-down list. Each channel supports different frequencies.	36 (5180 MHz)

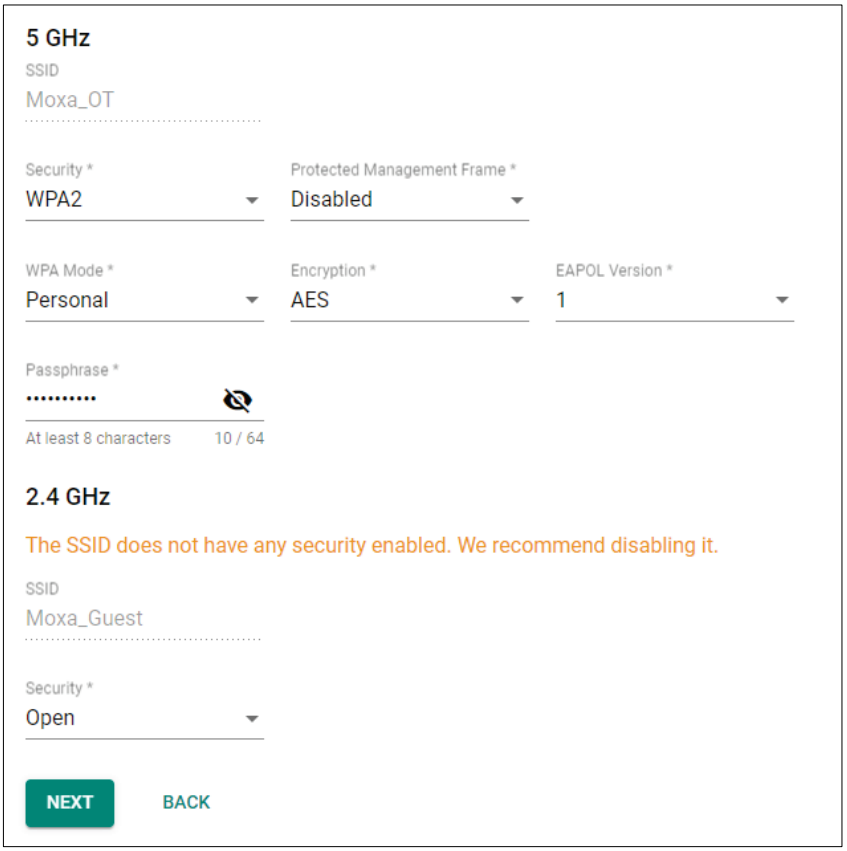
Bonded Channel (for AP and Master modes only)

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

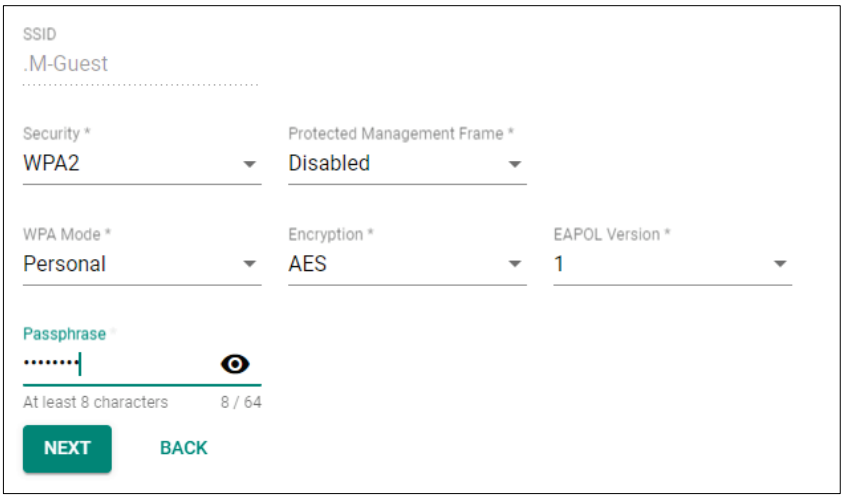
When finished, click **NEXT**.

Wi-Fi Security

AP/Master Mode



Client/Client-Router/Slave Mode



SSID

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

Security

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

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

Protected Management Frame

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

WPA type

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

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

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

Primary/Secondary RADIUS Port (for Enterprise mode only)

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

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

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

Encryption

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

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

EAPOL Version

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)

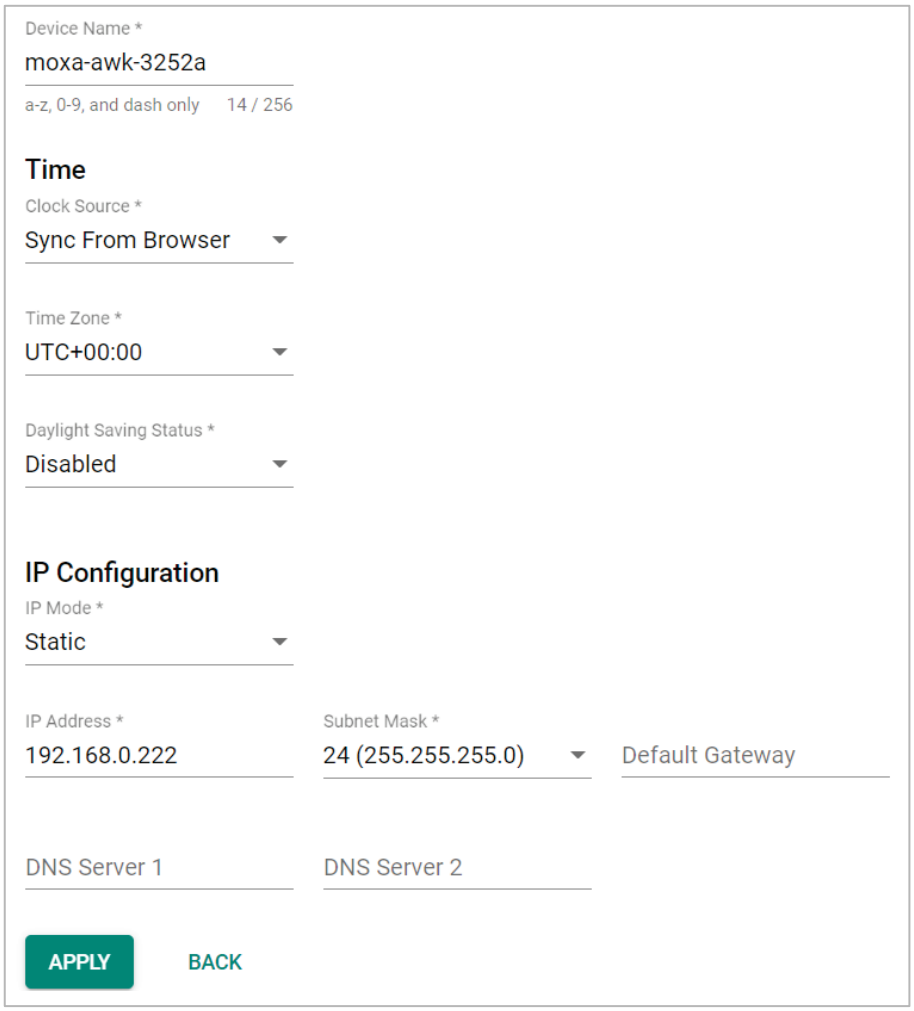
Setting	Description	Factory Default
8 to 63 characters	Enter the passphrase. This is the master key to generate keys for encryption and decryption. The passphrase cannot contain the following special characters: ` ' " | ; & $ Check **Show Password** to display the password in clear text.	None

EAP Protocol (for Enterprise mode only)

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

When finished, click **NEXT**.

System



Device Name

Setting	Description	Factory Default
1 to 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 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-awk-3251a

Time

Clock Source

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

Time Server 1 (for Clock Source is NTP)

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

Time Server 2 (for Clock Source is NTP)

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

Time Zone

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

Daylight Saving Time Status

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

Offset

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

Start

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

End

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

IP Configuration

IP Mode

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

IP Address (for Static mode only)

Setting	Description	Factory Default
IP address	Enter the AWK'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 AWK is connected to (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	24 (255.255.255.0)

Default Gateway (for Static mode only)

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

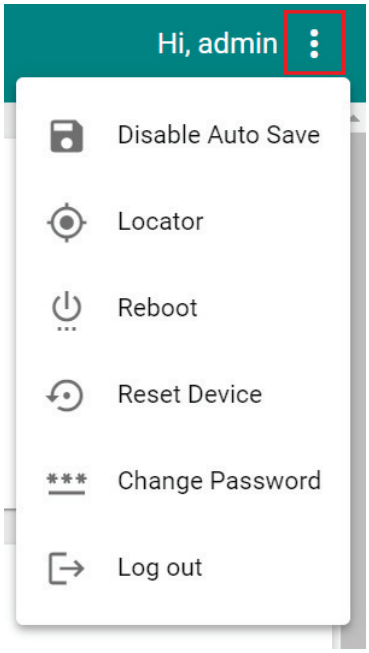
DNS Server 1 and DNS Server 2 (for Static mode only)

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

When finished, click **APPLY**.

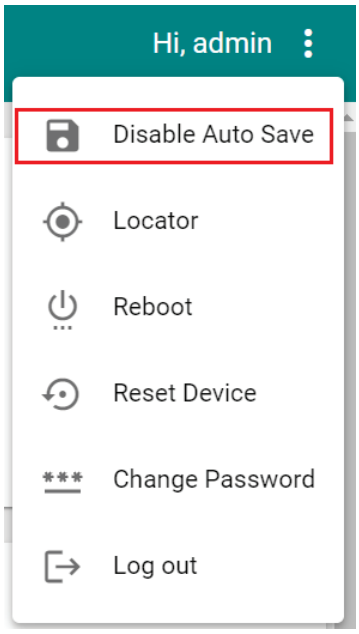
Maintenance and Tools

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.



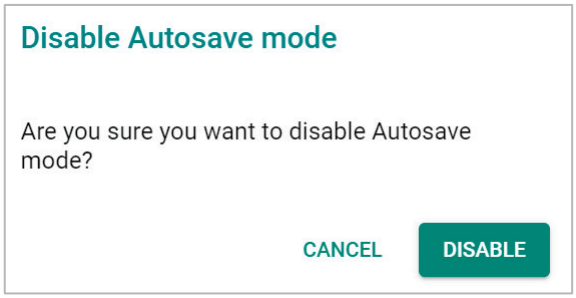
Disable Auto Save

Auto Save will automatically save the configuration changes to the startup configuration. All parameters will be effective immediately when applied, even if the AWK 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.



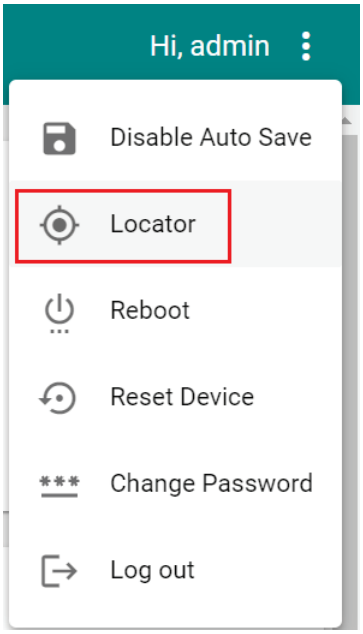
When **Disable Auto Save** is active, only the running configuration is saved. Disconnecting the power or performing a warm start will undo any running changes. When **Auto Save** is enabled, the startup configurations will be saved on the AWK.

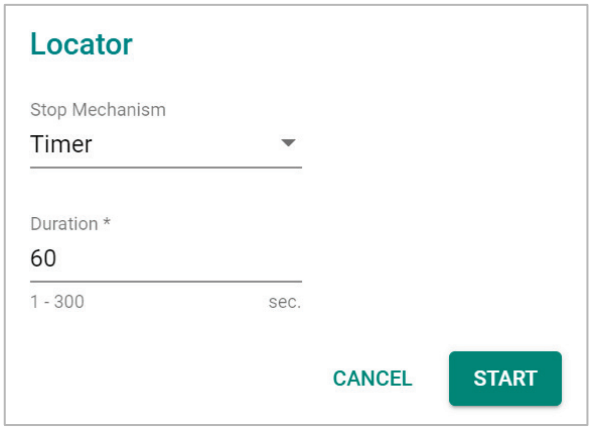
To disable the **Auto Save** function, click **Disable Auto Save** in the menu. When prompted, click **DISABLE** to disable the function.



Locator

Clicking **Locator** will trigger the wireless and SYSTEM LEDs to start flashing green at a 4 Hz interval for one minute (default) alongside an audible beeper. This feature is useful for locating the physical device in a field site.





Stop Mechanism

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

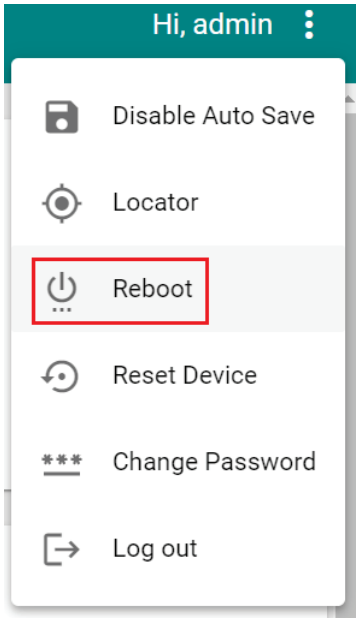
Duration

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

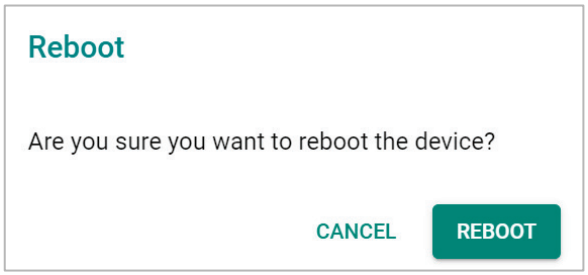
When finished, click **START** to activate the LEDs.

Reboot

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

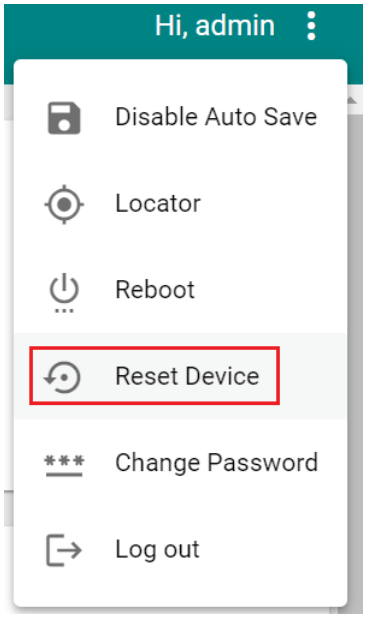


When prompted, click **REBOOT** to reboot the AWK.

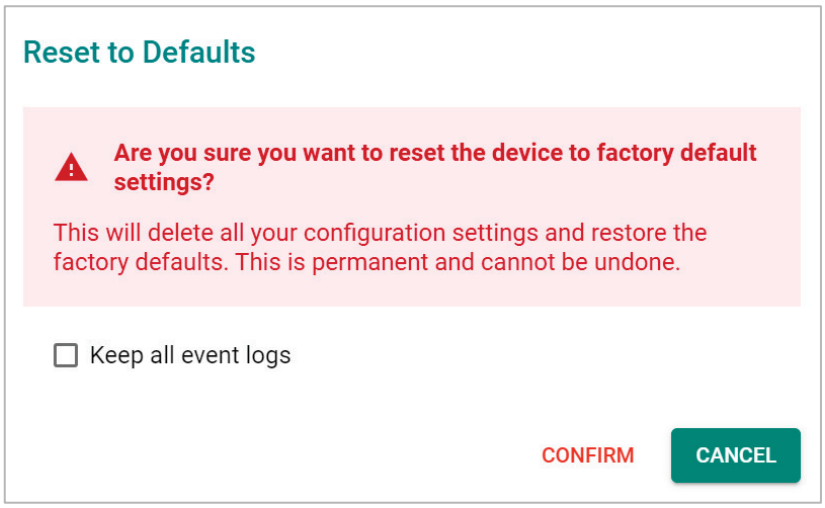


Reset Device

To reset the AWK to the factory default settings, click **Reset Device**.



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

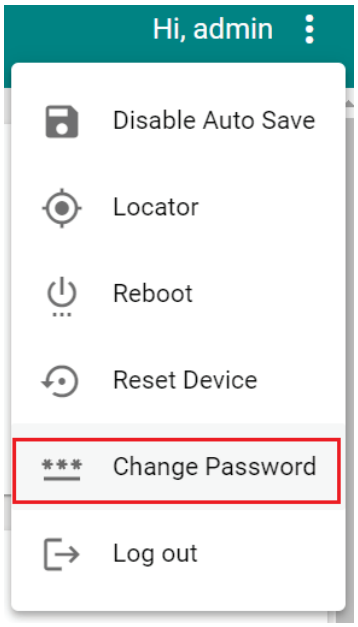


WARNING

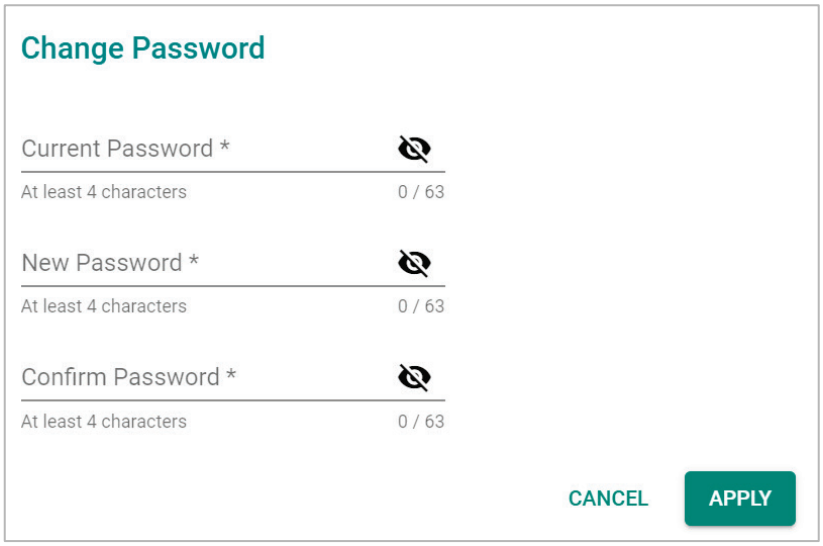
Resetting the AWK to the factory default settings will permanently delete all your configuration settings. This is permanent and cannot be undone.

Change Password

Click **Change Password** to change the password of the AWK.



Configure the following settings:



Current Password

Setting	Description	Factory Default
4 to 63 characters	Enter the current password.	None

New Password

Setting	Description	Factory Default
4 to 63 characters	Enter the new password.	None

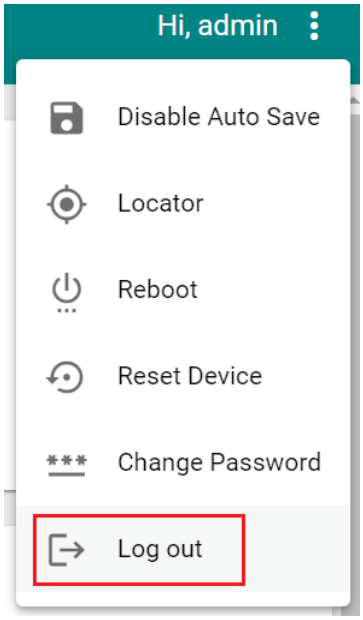
Confirm Password

Setting	Description	Factory Default
4 to 63 characters	Enter the new password again.	None

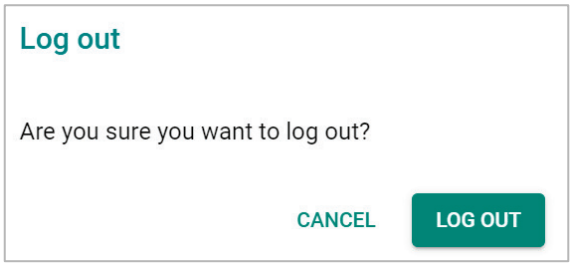
When finished, click **APPLY** to change the password.

Log Out

To log out of the AWK, click **Log out**.



When prompted, click **LOG OUT** to log out of the AWK.



A. Supporting Information

This chapter presents additional information about this product. You can also learn how to contact Moxa for technical support.

Device Recovery

In the 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 a power cycle does not solve the issue, the next step is to perform a reset to factory default setting. Refer to **Reset Device**.

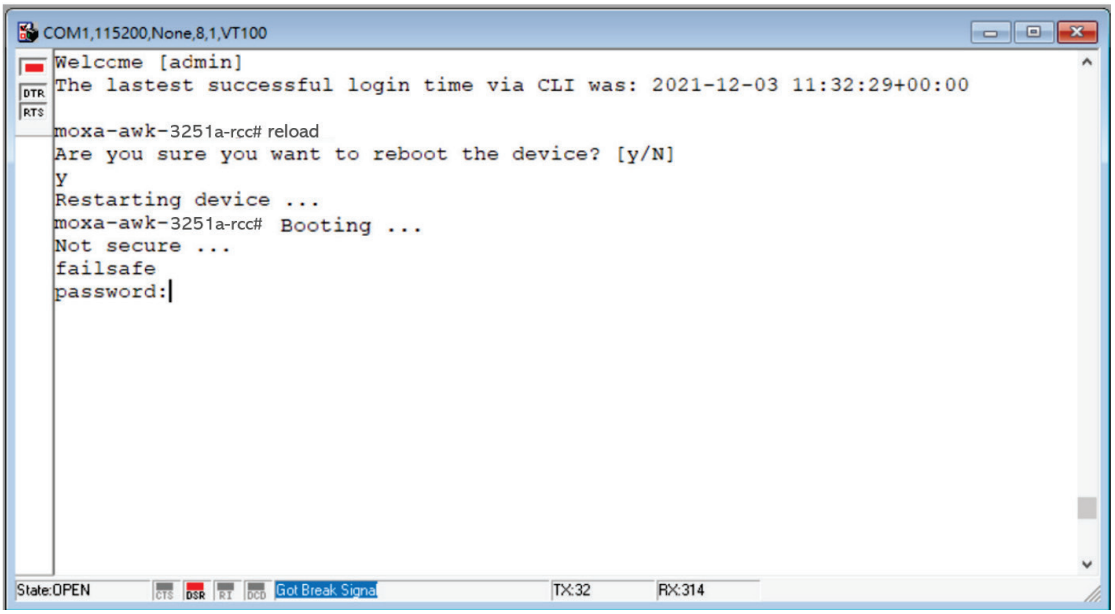
If you cannot access the web interface, and/or the Reset button is disabled, you can attempt to reset the device via the serial console's CLI FailSafe mode.

NOTE

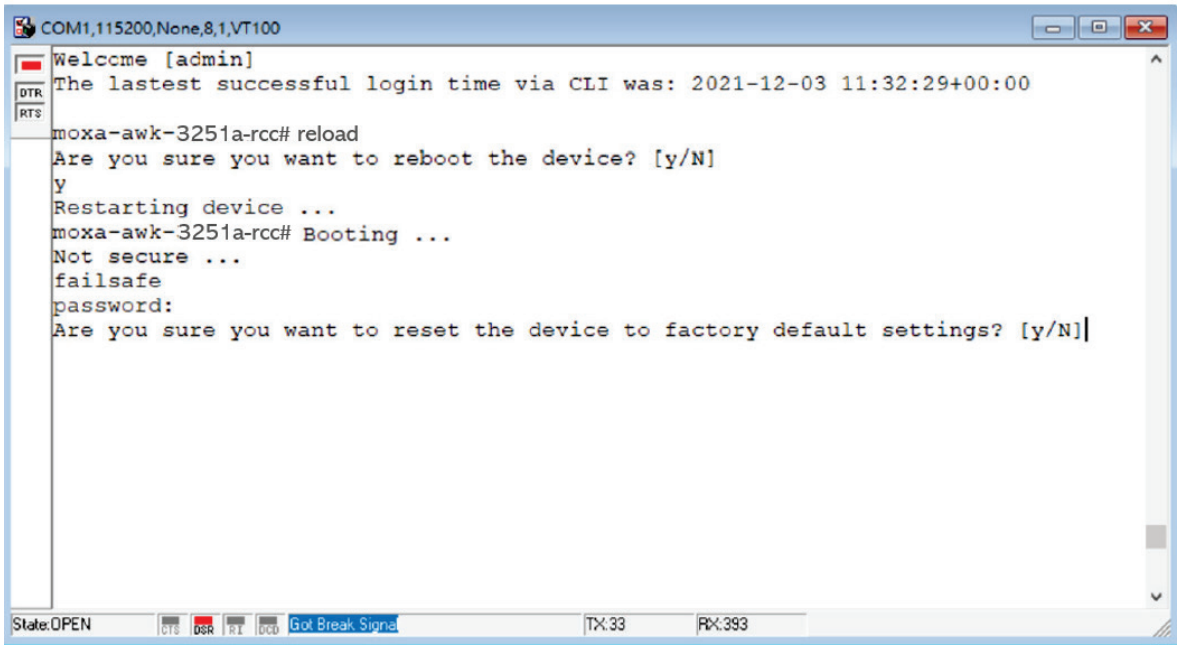
The admin password is required to authorize the FailSafe function.

Follow the instructions in the **Accessing the Serial Consoles** section to access the serial console CLI interface and enter the "reload" command to reboot the device.

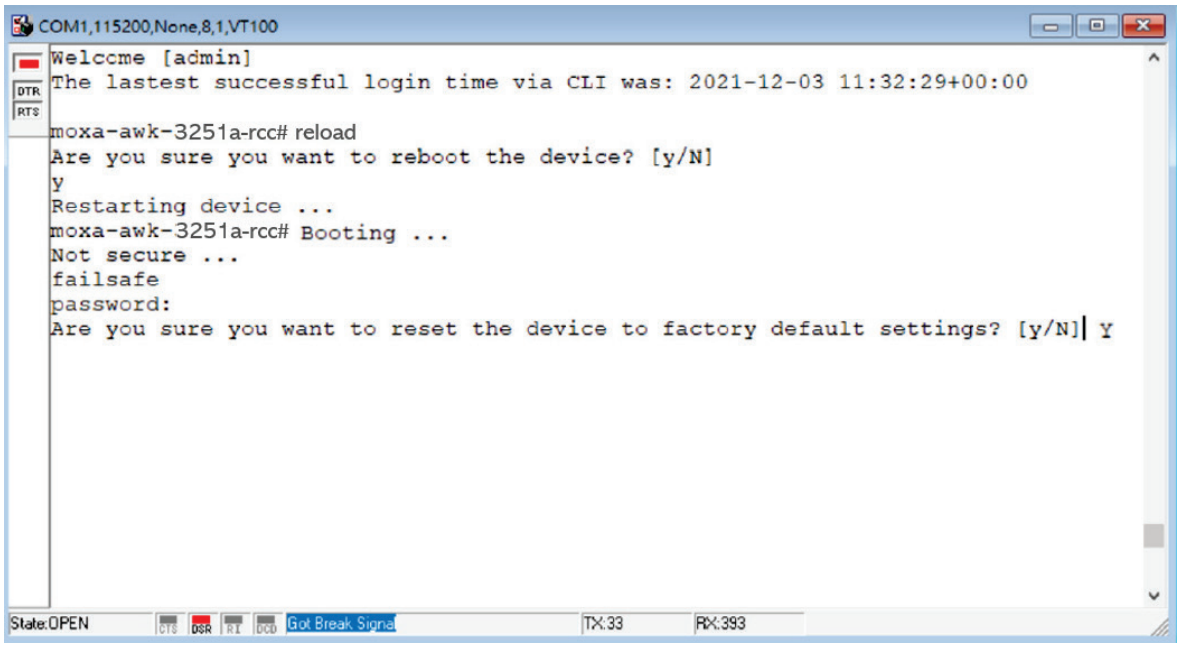
When the terminal is showing "Restarting device … [device]# Booting …", enter the "failsafe" command.



FailSafe mode will be triggered, and you will be prompted to confirm if you want to reset the device back to factory default settings.



Enter **Y** to make the device initiate a reset to factory default settings.



When the command line prompt displays the login prompt, it means the device was successfully reset to factory default settings.

B. Accessing the Serial Consoles

This chapter explains how to access the AWK Series. In addition to HTTP/HTTPS access, the AWK 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 AWK Series to a PC's COM port, can be used if you do not know the AWK Series' IP address. The other consoles can be used to access the AWK Series over an Ethernet LAN, or over the Internet.

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

The serial console connection method, which requires a serial cable to connect the AWK Series to a PC's COM port, can be used if you do not know the AWK Series' IP address. It is also convenient to use serial console configurations when you cannot access the AWK Series over Ethernet LAN.

ATTENTION

Do not use the RS-232 console manager when the AWK Series is powered at reversed voltage (ex. -48 VDC), even though reverse voltage protection is supported.

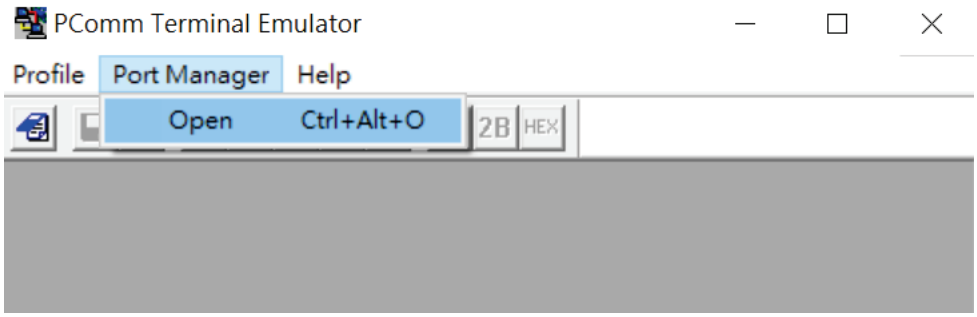
If you need to connect the RS-232 console at reversed voltage, we highly recommend using an isolator, such as the Moxa TCC-82 isolator.

NOTE

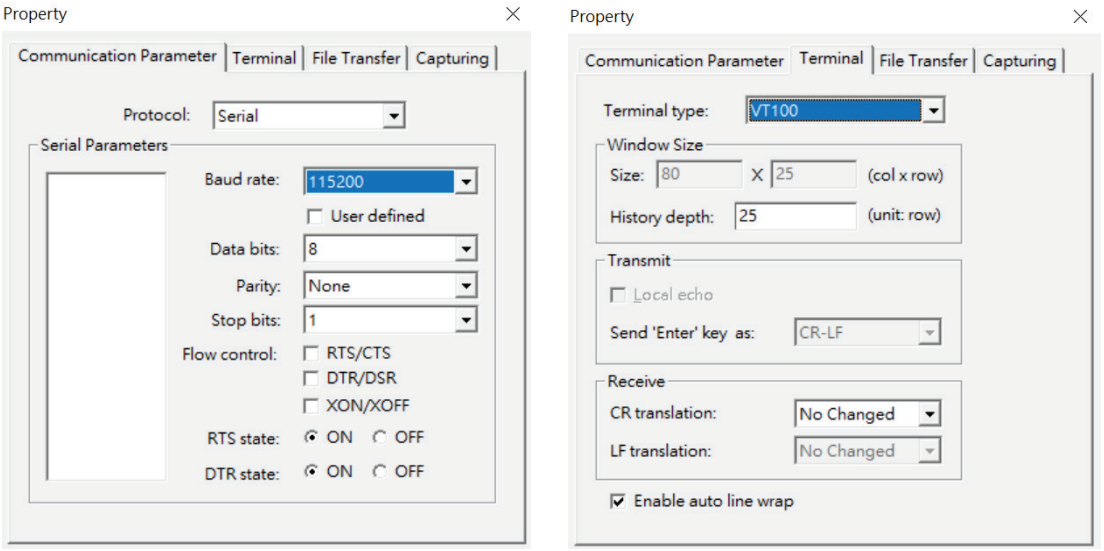
We recommend using **Moxa PComm (Lite)** Terminal Emulator, which can be downloaded free of charge from Moxa's website.

Before running PComm Terminal Emulator, use an RJ45-to-DB9-F (or RJ45-to-DB25-F) cable to connect the AWK Series' RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, perform the following steps to access the RS-232 console utility.

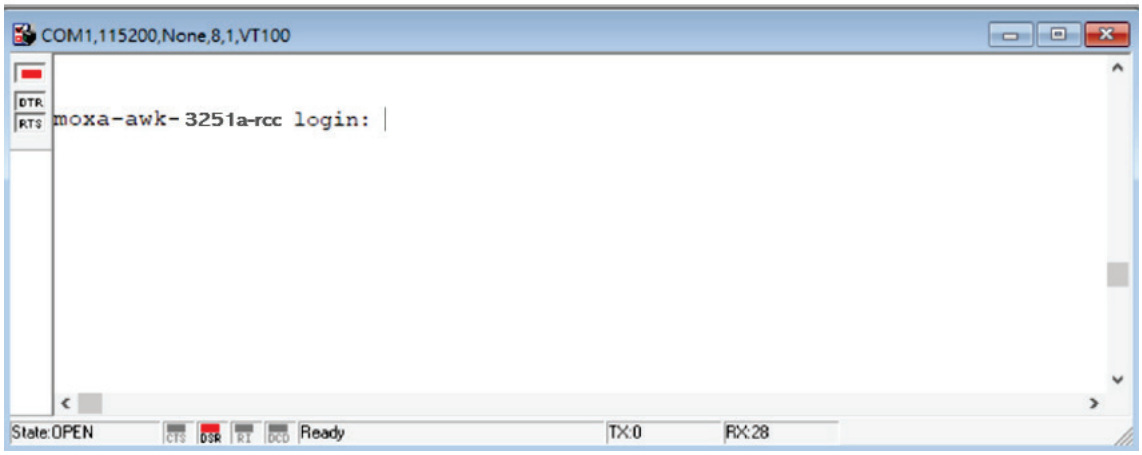
1. From Windows desktop, open the Start menu and run **PComm Terminal Emulator** in the PComm (Lite) group.
2. Select **Open** under **Port Manager** to open a new connection.



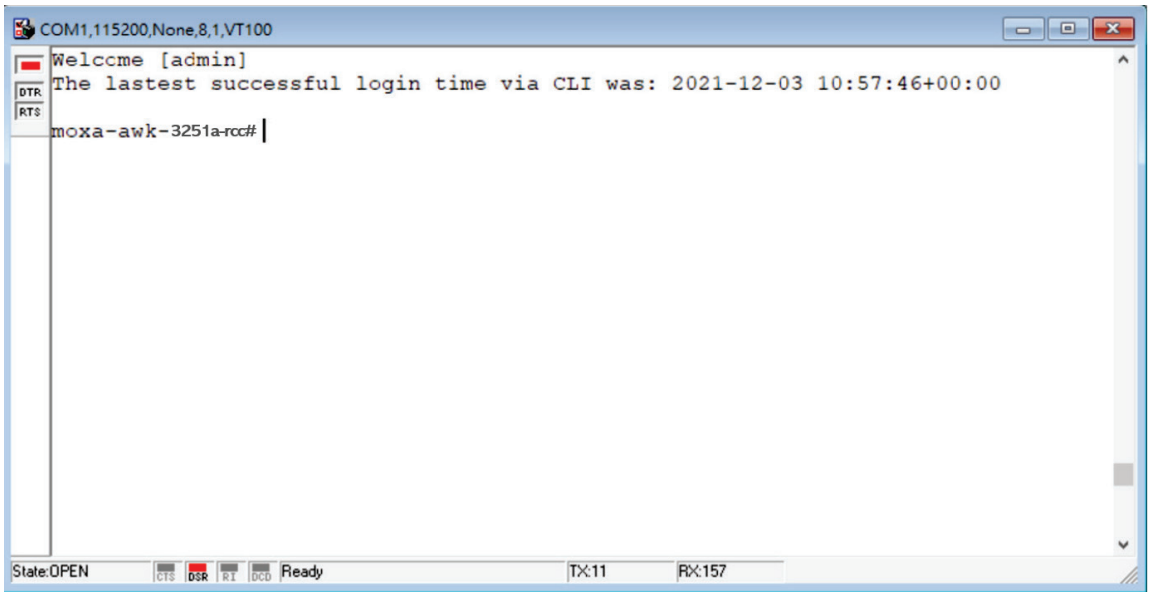
The **Communication Parameter** page of the Property window opens. Select the appropriate COM port for the Console Connection, **115200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits. Click on the **Terminal** tab and select **VT100 (or ANSI)** for Terminal Type. Click **OK** to continue.



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



4. The AWK Series device's CLI interface will be displayed. Refer to the device's CLI User's Manual for more information and instructions on how to use the command line interface.



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

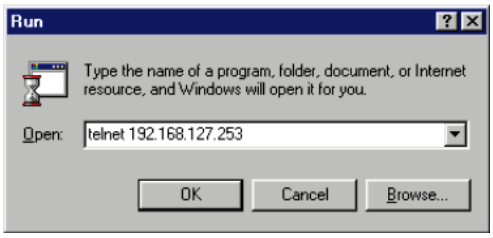
You can use a Telnet or SSH client to access the AWK Series and manage the console over a network. To access the AWK Series' functions over the network from a PC host that is connected to the same LAN as the AWK Series, you need to make sure that the PC host and the AWK Series are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

NOTE

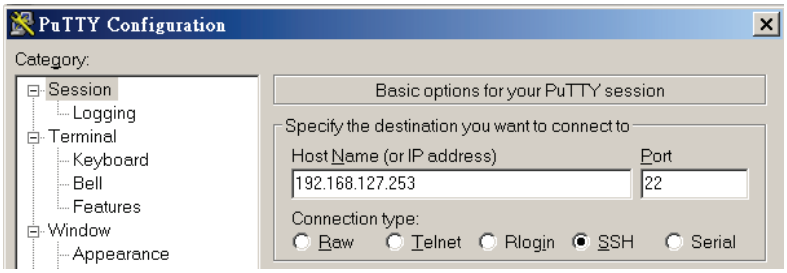
The AWK Series' default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). To configure the AWK Series remotely over a LAN network, set the PC host's IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

Follow the steps below to access the console utility via Telnet or SSH client:

1. From Windows Desktop, run **Start > Run**, and type *telnet (AWK IP address)* in the Run window and click **OK**. The AWK's default IP address is 192.168.127.253.



2. When using an SSH client (e.g. PuTTY), run the software and enter the AWK devce's IP address as the Host Name along with port **22**, and select **SSH** as the connection type.



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