# **AWK Series User Manual**

## Version 2.0, March 2023

www.moxa.com/products

**Models covered by this user manual:** AWK-1151C Series AWK-3252A Series AWK-4252A Series



### **AWK Series User Manual**

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

### **Copyright Notice**

© 2023 Moxa Inc. All rights reserved.

### Trademarks

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

### Disclaimer

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

### **Technical Support Contact Information**

www.moxa.com/support

## **Table of Contents**

1.	About This Manual	
	About Note, Attention, and Warning	
	Configuration Reminders	
	A: About Mandatory Parameters	
_	B: Preconfiguring Settings	
2.	Getting Started	
	Functional Design	
	LED Indicators	
	Event Indicators	
	Beeper	
	Reset Button	
	Relay (AWK-3252A and AWK-4252A Only)	
	First-time Installation and Configuration	
_	Communication Testing	
3.	Web Interface Configuration	
	Function Introduction	
	Device Summary	
	Device Information	
	System Information	
	System Status	22
	SSID	22
	System	23
	System Management	23
	Account Management	37
	Management Interface	44
	Time	51
	Wi-Fi	55
	Wireless Settings	55
	Connection Management	72
	Roaming	77
	Client Isolation	78
	Wi-Fi ACL	79
	Ports	80
	Port Settings	80
	Layer 2 Switching	82
	VLAN	82
	IP Configuration	88
	General Settings	88
	IP Configuration Status	89
	Networking Service	89
	DHCP Server	89
	Routing and NAT	90
	Routing	90
	NAT	93
	Firewall	98
	Layer 2 Policy	98
	Layer 3 Policy	100
	Certificate Management	102
	Device Certificate	103
	Server CA Certificate	104
	Security	105
	, Device Security	
	Diagnostics	
	System Status	
	Network Status	
	Event Logs and Notifications	
	Tools	

	Setup Wizard	133
	Wi-Fi Basic	134
	Wi-Fi Security	136
	System	138
	Maintenance and Tools	140
	Language	140
	Disable Auto Save	141
	Locator	142
	Reboot	144
	Reset to Defaults	145
	Renew Device Unique Key	146
	Change Password	146
	Log Out	
Α.	Supporting Information	149
	Device Recovery	149
в.	Accessing the Serial Consoles	151
	RS-232 Console Configuration (115200, None, 8, 1, VT100)	151
	Configuration by Telnet and SSH Consoles	153
С.	Security Guidelines	155
	Installation	155
	Physical Installation	155
	Account Management	156
	Vulnerable Protocols	156
	Operation	156
	Maintenance	157
	Decommission	157
D.	Service Authority Table	159

Thank you for purchasing a Moxa's AWK-3252A Series/AWK-4252A Series/AWK-1151C 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. Note that the web interface screenshots shown in this manual use the AWK-3252A Series for reference. Since all AWK Series use the same firmware image, the screenshots will be identical for all models, with the exception of the model name.

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

#### **Chapter 2: Getting Started**

In this chapter, we 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-3252A'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
lı	Clear all
≡~	Column selection
C	Refresh
8	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save the configuration.
<b>F</b>	Export
<b>/</b> `	Edit
((·	Perform a Wi-Fi site survey (Client mode only)
¢	Re-authentication
Î	Delete

Symbols	Meanings
K 3	Panel View
~	Expand
^	Collapse
•	Hint or additional information
타	Settings
→←	Data comparison
	Menu icon
\$	Change mode
۲	Locator
<u>ن</u>	Reboot
Ð	Reset to defaults
€	Logout
$\uparrow$	Increase
$\checkmark$	Decrease
+ + ■	Equal
	Menu
Q	Search
Ø	Hide text that is typed into a text box (usually used when typing a password)
Ο	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**

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

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

## **B: Preconfiguring Settings**

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

SNMP		
SNMP	SNMP Account List	
SNMP V1 and V2c a	re not secure. We recom	mend using SNMP V3.

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-4252A Series



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

LED	Color	State	Description			
		Fro	nt Panel LED Indicators (System)			
		On	Power is being supplied from DC to the PWR socket (power input 1			
PWR	Green	UII	or 2) or PoE.			
	Green	Off	Power is not being supplied from DC to the PWR socket (power input			
		On	1 or 2) or PoE.			
		On	Link established on the LAN port at 1000 Mbps.			
	Green Amber	Blinking	Data is being transmitted at 1000 Mbps.			
LAN 2		Off	The LAN port's 1000 Mbps link is inactive.			
		On	Link established on the LAN port at 10/100 Mbps.			
		Blinking	Data is being transmitted at 10/100 Mbps.			
		Off	The LAN port's 10/100 Mbps link is inactive.			
		On	Link established on the LAN port at 1000 Mbps.			
	Green	Blinking	Data is being transmitted at 1000 Mbps.			
LAN 1		Off	LAN port's 1000 Mbps link is inactive.			
	Amber	On	Link established on the LAN port at 10/100 Mbps.			
		Blinking	Data is being transmitted at 10/100 Mbps.			
		Off	The LAN port's 10/100 Mbps link is inactive.			

LED	Color	State	Description		
	Green	On	Client/Client-Router/Slave has established a Wi-Fi connection to an		
		OII	AP/Master with a SNR value of 35 or higher.		
2.4GHz		Blinking	Data is being transmitted over the 2.4 GHz band.		
2.40112		On	Client/Client-Router/Slave has established a Wi-Fi connection to an		
	Amber	On	AP/Master with a SNR value of less than 35.		
		Blinking	Data is being transmitted over the 2.4 GHz band.		
	Green	On	Client/Client-Router/Slave established a Wi-Fi connection to an		
		UII	AP/Master with a SNR value of 35 or higher.		
5GHz		Blinking	Data is being transmitted over the 5 GHz band.		
SGHZ	Amber	Z	ΠZ	On	Client/Client-Router/Slave has established a Wi-Fi connection to an
		On	AP/Master with a SNR value of less than 35.		
		Blinking	Data is being transmitted over the 5 GHz band.		
SYS	Red	On	System initialization failure, configuration error, or system error.		
515	Green On		System startup completed and is operating normally.		

#### AWK-3252A Series





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

LED	Color	State	Description				
Front Panel LED Indicators (System)							
PWR1	Croop	On	Power is being supplied from power input 1.				
PWKI	Green	Off	Power is not being supplied from power input 1.				
PWR2	Green	On	Power is being supplied from power input 2.				
FWKZ	Green	Off	Power is not being supplied from power input 2.				
PoE	Amber	On	Power is being supplied via PoE.				
POE	Ander	Off	Power is not being supplied via PoE.				
SYS	Red	On	System initialization failure, configuration error, or system error.				
515	Green	On	System startup completed and is operating normally.				
		On	Client/Client-Router/Slave has established a Wi-Fi connection to an				
	Green	OII	AP/Master with a SNR value of 35 or higher.				
2.4GHz		Blinking	Data is being transmitted over the 2.4 GHz band.				
2.4902		On	Client/Client-Router/Slave has established a Wi-Fi connection to an				
	Amber	ber	AP/Master with a SNR value of less than 35.				
		Blinking	Data is being transmitted over the 2.4 GHz band.				
		On	Client/Client-Router/Slave established a Wi-Fi connection to an				
	Green		AP/Master with a SNR value of 35 or higher.				
5GHz		Blinking	Data is being transmitted over the 5 GHz band.				
30112	HZ	On	Client/Client-Router/Slave has established a Wi-Fi connection to an				
	Amber	-	AP/Master with a SNR value of less than 35.				
		Blinking	Data is being transmitted over the 5 GHz band.				
		L	AN LED Indicators (RJ45 Port)				
		On	Link established on the LAN port at 1000 Mbps.				
	Green	Blinking	Data is being transmitted at 1000 Mbps.				
LAN 1		Off	The LAN port's 1000 Mbps link is inactive.				
		On	Link established on the LAN port at 10/100 Mbps.				
	Amber	Blinking	Data is being transmitted at 10/100 Mbps.				
		Off	The LAN port's 10/100 Mbps link is inactive.				
		On	Link established on the LAN port at 1000 Mbps.				
	Green	Blinking	Data is being transmitted at 1000 Mbps.				
LAN 2		Off	LAN port's 1000 Mbps link is inactive.				
		On	Link established on the LAN port at 10/100 Mbps.				
	Amber	Blinking	Data is being transmitted at 10/100 Mbps.				
		Off	The LAN port's 10/100 Mbps link is inactive.				

#### AWK-1151C Series



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

LED	Color	State	Description					
	Front Panel LED Indicators (System)							
PWR	Green	On	Power is being supplied from DC to the PWR socket.					
FWR	Green	Off	Power is not being supplied from DC to the PWR socket.					
		On	Client/Client-Router/Slave has established a Wi-Fi connection to an					
	Green	Oli	AP/Master with a SNR value of 35 or higher.					
	Green	Blinking	Data is being transmitted over the wireless interface (2.4 GHz or 5					
WLAN		Dilliking	GHz).					
WLAN		On	Client/Client-Router/Slave has established a Wi-Fi connection to an					
	Amber		AP/Master with a SNR value of less than 35.					
		Blinking	Data is being transmitted over the wireless interface (2.4 GHz or 5					
			GHz).					
SYSTEM	Red	On	System initialization failure, configuration error, or system error.					
STOTEM	Green	On	System startup completed and is operating normally.					
		L	AN LED Indicators (RJ45 Port)					
		On	Link established on the LAN port at 1000 Mbps.					
	Green	Blinking	Data is being transmitted at 1000 Mbps.					
LAN		Off	LAN port's 1000 Mbps link is inactive.					
LAN		On	Link established on the LAN port at 10/100 Mbps.					
	Amber	mber Blinking Data is being transmitted at 10/100 Mbps.						
		Off	The LAN port's 10/100 Mbps link is inactive.					

## **Event Indicators**

The device LEDs are also used to indicate specific device events or issues. Refer to the following table for more details.

Applicable Models	AWK-3252A AWK-4252A AWK-1151C		AWK-3252A AWK-4252A				AWK-1151C	
LED	SYS		2.4 GHz		5 GHz		WLAN	
LED	Red	Green	Amber	Green	Amber	Green	Amber	Green
IP address conflict	Blinks at 4 Hz	Off	-	-	_	-	-	-
Failed to get an IP from the DHCP server	Blinks at 4 Hz	Off	-	-	-	-	-	-
ABC-02 is connected	Off	Blinks at 4 Hz	-	-	-	-	-	-
Uploading/retrievi ng file(s) to/from ABC-02 (e.g., upgrading firmware, backup/restore configuration)	Off	Blinks at 4 Hz	Off	Blinks at 4 Hz	Off	Blinks at 4 Hz	Off	Blinks at 4 Hz
Failed to upload/retrieve file(s) to/from ABC-02. Possible reasons are: The file does not exist, failed to copy the file, or the ABC- 02 has insufficient space	Blinks at 4 Hz	Off	_	_	_	-	-	_
The device is being located.	Off	Blinks at 4 Hz	Off	Blinks at 4 Hz	Off	Blinks at 4 Hz	Off	Blinks at 4 Hz
The Reset button is being pressed for less than 5 seconds (system reboot)	Off	Blinks at 1 Hz	-	-	_	-		
The Reset button is being pressed for 5 to 10 seconds (System factory reset)	Off	Blinks at 4 Hz	-	-	-	-	-	-
The Reset button is being pressed for longer than 10 seconds (Abort reboot or reset)	Off	Solid on	-	-	-	-	-	-

### **Beeper**

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

## **Reset Button**

Depending on the AWK Series model, the Reset is located on the side panel (AWK-4252A), top panel (AWK-3252A), or bottom panel (AWK-1151C). 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 <u>Reset Button Active Duration</u> section for more detailed information.

## Relay (AWK-3252A and AWK-4252A Only)

The AWK-3252A and AWK-4252A Series have 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-3252A's Relay Status

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

The AWK-3252A relay is marked on the 2 terminal block contacts, as shown in the image below:



The AWK-4252A relay is integrated into the DI/DO connector (pins 1 and 2), as shown in the image below:



## **First-time Installation and Configuration**

Before installing the AWK 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.

## NOTE

The images in the instructions below use the AWK-3252A Series interface for reference. The instructions are identical for all supported AWK models.

#### Step 1: Select the power source.

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



### ΝΟΤΕ

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.

Create your administ	rator account
Username *	
At least 4 characters	0 / 32
New Password *	2
At least 4 characters	0 / 63
Confirm Password *	Ø
At least 4 characters	0 / 63
Email	
	0/318
BACK	CREATE

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

#### AWK-3252A/AWK-4252A

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

#### AWK-3252A/AWK-4252A/AWK-1151C

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.

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.

	AWK-325	52A-UN			4		Hi, admin
Q Search for function		Device Information	2022-01-11 1	5:58:51 <b>C</b>	System Information		2022-01-11 15:58:51 C
Device Summary	3	Product Model AWK-3252A-UN	Country/Region EU		Device Name moxa-awk-3252a	Location	
System	~	Firmware Version v1.0 Build 2022_0106_1056	Bootloader Version v1.0 Build 2021_1015_0548		Description AWK-3252A		
🗢 Wi-Fi	~	MAC Address 00:90:E8:9D:C5:1B	Serial Number TBAIB1116938		Operation Mode AP		
💟 Ports	~						
😫 Layer 2 Switching	~	System Status					2022-01-11 15:58:51
IP Configuration		Current Time	System Uptime		External Storage		
Routing and NAT	~	2022-01-11 15:58:50+00:00 IPv4 Address	OdOh6m54s Netmask		Default Gateway	IP Conflict Check	
Firewall	~	192.168.127.253	24 (255.255.255.0)			Pass	
Security	~						
Diagnostics	~	SSID on 2.4 GHz	2022-01-11 1	5:58:52 <b>C</b>	SSID on 5 GHz		2022-01-11 15:58:52
🕉 Setup Wizard		RF Type B/G/N Mixed	Channel Width		RF Type A/N/AC Mixed	Channel Width 20-40-80 MHz	
		Channel 	Bonded Channel		Channel 36 (5180 MHz)	Bonded Channel 40, 44, 48	
		SSID	Number of Associated Clients		SSID	Number of Associated Cl	ients
					Factory-Test	0	
						•	

- 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.

Device Information		2022-01-11 14:17:45 C	System Information		2022-01-11 14:17:45 (
Product Model AWK-3252A-UN	Country/Region EU		Device Name moxa-awk-3252a	Location	
irmware Version r1.0 Build 2022_0106_1056	Bootloader Version v1.0 Build 2021_1214_0620		Description AWK-3252A		
WAC Address 00:90:E8:9D:C5:31	Serial Number TBAIB1116960		Operation Mode AP		
System Status					2022-01-11 14:17:45 (
Current Time 2022-01-11 14:17:44+00:00	System Uptime 0d0h7m31s		External Storage		
Pv4 Address 192.168.127.253	Netmask 24 (255.255.255.0)		Default Gateway	IP Conflict Check Pass	
SSID on 2.4 GHz		2022-01-11 14:17:35 C	SSID on 5 GHz		2022-01-11 14:17:35 (
RF Type B/G/N Mixed	Channel Width		RF Type A/N/AC Mixed	Channel Width 20-40-80 MHz	
Channel	Bonded Channel		Channel 36 (5180 MHz)	Bonded Channel <b>40, 44, 48</b>	
SSID	Number of Associated Clients		SSID	Number of Associated Clients	
			Factory-Assembly	0	
			Factory-Test		

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.

<b>Device Information</b>	2022-01-11 11:44:38 C
Product Model AWK-3252A-UN	Country/Region EU
Firmware Version v1.0 Build 2022_0106_1056	Bootloader Version v1.0 Build 2021_1015_0548
MAC Address 00:90:E8:9D:C5:33	Serial Number TBAIB1116962

## **System Information**

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

System Information		2021-09-23 10:02:07	C
Device Name moxa-awk-3252a	Location		
Description AWK-3252A			
Operation Mode AP			

## **System Status**

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

System Status				2021-09-23 10:02:27 C
Current Time 2021-09-23 10:02:25+00:00	System Uptime 5d16h15m26s	External Storage		
IPv4 Address 192.168.0.222	Netmask 24 (255.255.255.0)	Default Gateway	IP Conflict Check Pass	

## SSID

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

SSID on 2.4 GHz RF Type B/G/N Mixed Channel 6 (2437 MHz)	2022-08-25 15:51:45 C Channel Width 20-40 MHz Bonded Channel
SSID	Number of Associated Clients
Moxa-2G	0
SSID on 5 GHz	2022-08-25 15:51:15 C
RF Type N/AC Mixed	Channel Width 20-40-80 MHz
Channel	Bonded Channel
36 (5180 MHz)	40, 44, 48
SSID	Number of Associated Clients
Moxa-5G	0

## 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.

system Information	
Device Name * moxa-awk-3252a	
	14 / 255
Location	
	0 / 255
Description AWK-3252A	
	9 / 255
Contact Information	
	0 / 255
APPLY	

#### Device Name

Setting	Description	Factory Default
1 to 255 characters	<ul> <li>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:</li> <li>Only supports letters (a-z), numbers (0-9), and special character dash (-)</li> <li>Cannot contain spaces</li> <li>Cannot start with dash (-)</li> <li>Cannot end with dash (-)</li> <li>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.</li> </ul>	moxa-awk-3252a

#### Location

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

#### Description

Setting	Description	Factory Default
Max. 255 characters	Enter a description for the device.	AWK-3252A

#### **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, remote SFTP server, or the ABC-02 tool.

Firmware Upgrade	
Running Firmware Version v1.0 Build 2021_0810_0019	
Uploaded Firmware Version 	
Source *	
Select File *	
UPLOAD UPGRADE	

#### Local

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

Firmware	U	lpg	ra	d	e
----------	---	-----	----	---	---

Running Firmware V v1.0 Build 2021		
Uploaded Firmware	Version	
Source *		
Local	<b>•</b>	
Select File *		
UPLOAD	UPGRADE	

#### Running Firmware Version

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

#### Uploaded Firmware Version

Setting	Description	Factory Default
New firmware version 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	None
Select the firmware file	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.

### **Firmware Upgrade**

TFTP does not support user authentication and sends all data in clear text. We recommend using SFTP to transfer firmware.

Uploaded Firmwa	are Version		
Source			
TETP	-		
TFTP	•		
TFTP	•		
	<b>•</b>	-	
TFTP Server IP Add	▼ dress *	Filename *	
	dress *	Filename *	0 / 25

#### Running Firmware Version

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

Uploaded Firmware Version		
Setting	Description	Factory Default
New firmware version 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.

	ersion		
v1.0 Build 2021		9	
Uploaded Firmware	Version		
Source *			
SFTP			
	2		
Server IP Addre	SS *	Filename *	
Server IP Addre	ess * 0 / 253	Filename *	0 / 256
	<u></u>	Filename * Password *	0 / 256
Server IP Addre Account *	<u></u>		0 / 256 & 0 / 256

#### Running Firmware Version

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

Uploaded Firmware V	ersion	
Setting	Description	Factory Default
New firmware version	This shows the new firmware version.	None
number		

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
ISEID convor 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
	Enter the SFTP user account password. This account must be	None
Si ir seivei passworu	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.

#### ABC-02

Select **ABC-02** from the Source drop-down. This method requires the Moxa ABC-02 USB configuration backup and restoration tool with the target firmware file is connected to the device. You can download the target firmware (\*.rom) file from Moxa's website (<u>www.moxa.com</u>). For more information about the Moxa ABC-02 Series USB tool, visit the <u>product page</u>.

## Firmware Upgrade

#### Running Firmware Version

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

#### **Uploaded Firmware Version**

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

#### Select File

Setting	Description	Factory Default
Salact the firmware file	Click the browse icon and navigate to the firmware file on the	Nono
Select the minimale file	Click the browse icon and navigate to the firmware file on the attached ABC-02 device.	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-02 USB 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.

## **Configuration Backup and Restore**

Backup	Restore
Configuration Source *	
Running Configuration	n 👻
Storage Location *	
Local	-
Configuration Passwe	ord *
Configuration Passwo	ord *
	0 / 64
BACK UP	

#### Local

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

Configuration	Backup	and	Restore
---------------	--------	-----	---------

Backup	Restore
Configuration Source * Running Configuration	Ţ
Storage Location  Local	•
Configuration Passwo	-
BACK UP	0 / 64

#### **Configuration Source**

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

Storage Locati	on	
Setting	Description	Factory Default
Local	Back up the configuration files for the local computer.	
TFTP	Back up the configuration files via TFTP.	Local
SFTP	Back up the configuration files via SFTP.	LUCAI
ABC-02	Back up the configuration files via ABC-02 USB 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. For firmware v2.0 and above, the password must be at least 8 characters long.	None

When finished, click **BACK UP**.

#### **TFTP Server**

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

## **Configuration Backup and Restore**

Backup	Restore	
TFTP does not support use	er authenticati	on and sends all data in clear text. We recommand using SFTP to back up the configuration
Configuration Source *		
Running Configuration	-	
Storage Location *		
TFTP	•	
Server IP Address *		Filename *
	0 / 253	0 / 256
Configuration Password *	Ø	
	0 / 64	

#### **Configuration Source**

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

#### Storage Location

Setting	Description	Factory Default
Local	Back up the configuration files for the local computer.	
TFTP	Back up the configuration files via TFTP.	Local
SFTP	Back up the configuration files via SFTP.	Local
ABC-02	Back up the configuration files via ABC-02 USB 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  $\ensuremath{\textbf{SFTP}}$  first from the Storage Location drop-down list.

## **Configuration Backup and Restore**

Backup	Restore		
Configuration Source *			
Configuration Source * Running Configuration	•		
Storage Location *			
SFTP	•		
Server IP Address *		Filename *	
	0 / 253		0 / 256
Account *		Password *	Ø
	0 / 256		0 / 256
Configuration Password	* 🖉		
	0 / 64		

#### **Configuration Source**

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

#### Storage Location

<b>j</b>		
Setting	Description	Factory Default
Local	Back up the configuration files for the local computer.	
TFTP	Back up the configuration files via TFTP.	Local
SFTP	Back up the configuration files via SFTP.	Local
ABC-02	Back up the configuration files via ABC-02 USB tool	

#### Server IP Address

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

#### File Name

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

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

#### 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-02

Select **ABC-02** from the Storage Location drop-down list. This method requires a Moxa ABC-02 configuration backup and restore USB tool to be connected to the AWK Series.

## **Configuration Backup and Restore**

Backup	Restore	
Configuration Source *		
Running Configuration	•	
Storage Location *		
ABC-02	•	
Backup for System Initialization *		
No	•	
Select Folder *		
Configuration Password *	Ø	
	0 / 64	
BACK UP		

#### **Configuration Source**

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

Storage Location		
Setting	Description	Factory Default
Local	Back up the configuration files for the local computer.	
TFTP	Back up the configuration files via TFTP.	Local
SFTP	Back up the configuration files via SFTP.	
ABC-02	Back up the configuration files via ABC-02 USB tool.	

#### Backup for System Initialization

Setting	Description	Factory Default
Yes	Back up the system initialization files.	No
No	Do not back up the system initialization files.	NO

#### Select Folder

Setting	Description	Factory Default
Folder path	Navigate to the folder path of the ABC-02 tool.	None

#### **Configuration Password**

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

When finished, click **BACK UP**.

### Automatic Backup to ABC-02

The AWK-Series also supports automatic configuration backups when using a Moxa ABC-02 backup and restore tool.

Automatically Back Up Configurations to ABC-02		
Auto Backup Status *		
Disabled	-	
APPLY		

#### Auto Backup Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable automatically backing up the device's configuration to the ABC-02.	Disabled

When finished, click **APPLY**.

#### Restore

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

Configuration	Backup and	Restore
Backup	Restore	
Source *		
Local	•	
Select File *		
Configuration Passwor	rd * 🔌	
	0 / 64	
RESTORE		

### Local

Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	Local
ABC-02	Restore the configuration from a backup file on an ABC-02 USB 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
	Enter the configuration password. You will need to enter this password when importing the backup file.	None

When finished, click **RESTORE**.

### **TFTP Server**

## **Configuration Backup and Restore**

Backup	Restore	
TFTP does not suppor	t user authenticatio	n and sends all data in clear text. We recommand using SFTP to restore the configuration file
Source *		
TFTP	•	
Server IP Address *		Filename *
	0 / 253	0 / 256
Configuration Passwo	rd * 🔌	
	0 / 64	
RESTORE		

#### Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	Local
ABC-02	Restore the configuration from a backup file on an ABC-02 USB 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

## Configuration Backup and Restore

Backup	Restore		
Source * SFTP	•		
Server IP Address *	0 / 253	Filename *	0 / 256
Account *	0 / 256	Password *	0/256
Configuration Password *	0 / 64		

#### Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	Local
ABC-02	Restore the configuration from a backup file on an ABC-02 USB tool.	

#### Server IP Address

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

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-02

## **Configuration Backup and Restore**

Backup	Restore	
Source * ABC-02	•	
Select File *		
Configuration Password *	Ø	
RESTORE	0 / 64	

#### Source

Setting	Description	Factory Default
Local	Restore the configuration from a local backup file.	
TFTP	Restore the configuration from a backup file via TFTP.	
SFTP	Restore the configuration from a backup file via SFTP.	Local
ABC-02	Restore the configuration from a backup file on an ABC-	
	02 USB tool.	

#### Select File

Setting	Description	Factory Default
Backup file	Click the browse icon and navigate to the backup file on the local host.	None
<b>Configuration Pass</b>	sword	

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

When finished, click **RESTORE**.
# **Automatic Restoration to ABC-02**

The AWK Series supports automatic configuration restoration when using a Moxa ABC-02 backup and restore tool.

Automatically Restore C	onfigurations from ABC-02
Auto Restore Status *	
Disabled	-
APPLY	

### Auto Restore Status

Setting	Description	Factory Default
Epobled (Disabled	Enable or disable automatically restoring the device's	
Enabled/Disabled	configuration from an ABC-02.	Disabled

When finished, click **APPLY** to change your setting.

# **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.

User Account							
Settings	5	Session Manageme	ent				
∎ =,							
	Status	Username	Email				
	Enabled	admin	moax@moxa.com				
Max 32							

Edit the following settings:

Create New Ac	count			
Status *				
Disabled	•			
Username *				
At least 4 characters	0 / 32			
New Password *	Ø	Confirm Passwore	d * 🐼	
At least 4 characters	0 / 63	At least 4 characters	0 / 63	
Email				
			0 / 318	
Role * User	-			
Authority *				
Account System	n			
Advanced Diag	nostics			
Auditor System				
Diagnostics				
Network Config	uration			
Status Monitori	ng			
System Backup				
System Manage	ement			
			CANCEL	APPLY

### Status

Setting	Description	Factory Default		
Enabled/Disabled	Disabled			
Username				
Setting	Description	Factory Default		

### New Password

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

### **Confirm Password**

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

### Email

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

### Role

KUle				
Setting	Description	Factory Default		
Administrator	authority)			
Engineer Set the user's role to Engineer. (pre-defined authority)		User		
User Set the user's role to User. (pre-defined authority)		User		
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	None
	authority privileges extend to all access interfaces, including	None
	CLI.	

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

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

# NOTE

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

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

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

# Edit an Existing Account

Click the Edit icon  $\checkmark$  of the account you want to edit.

	Status	Username	Email	Role	Account System	Advanced Diagnostics	Auditor System	Diagnostics	Network Configuration	Status Monitoring	System Backup	System Management
	Enabled	admin	moxa@moxa.com	Administrator	~	~	~	~	~	~	~	~
	Enabled	test	test@example.com	User				~		~		
4												•

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

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

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

When finished, click **APPLY**.

# **Delete an Existing User**

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

∎₹	,			
	Status	Username	Email	Role
	Enabled	admin	moxa@moxa.com	Administrator
	Enabled	test	test@example.com	User
4				
Delete A	Account			
Are you si account?	ure you war	nt to delete the s	selected	
		CANCEL	DELETE	

Click **DELETE** to delete the user.

### Terminate the Active Session of a User

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

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

User Account	t		
General	Session Man	agement	
Username	WEB: Status	WEB: Last Login	WEB: Last Activity
🔌 admin	In Use	2021-08-25 00:38:22+00:00	2021-08-25 00:38:42+00:00
<b>X</b> test	In Use	2021-08-25 00:38:11+00:00	2021-08-25 00:38:12+00:00
Max 32			

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

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

Minimum Length		
8		
8 - 63		
Password Va	dation Rules	
Must inclu	e at least one digit (0-9)	
Must inclu	le at least one uppercase letter (A-Z)	
Must inclu	le at least one lowercase letter (a-z)	
Must inclu	le at least one special character (~!@#\$%^&* :;,.<>{}[](	))
Password Lifetim	*	
90		
0 - 365	day(s)	
APPLY		

### Minimum Length

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

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

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

When finished, click **APPLY**.

# **Management Interface**

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



# **User Interface**

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

# **User Interface**

HTTP and Telnet are not secure interface. We recommend disabling these.

Enabled	▼ 80
	1 - 65535
HTTPS Status *	HTTPS - TCP Port *
Disabled	▼ 443
	1 - 65535
Telnet Status *	Telnet - TCP Port *
Disabled	<b>▼</b> 23
	1 - 65535
SSH Status *	SSH - TCP Port *
Enabled	<b>▼</b> 22
	1 - 65535
SNMP Status *	SNMP - UDP Port *
Disabled	<del>•</del> 161
	1 - 65535
Moxa Service Status *	Moxa Service - UDP Port
	▼ 40404

APPLY

# HTTP Status

NOTE

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

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
4 4 65505		
1 to 65535	Specify the HTTPS interface TCP port number.	443
Telnet Status	Specify the HTTPS Interface TCP port number.	443
	Description	443 Factory Default

pescription pecify the Telnet interface TCP port number. pescription	Factory Default 23
escription	
escription	En al anna Diafacult
	Factory Default
nable or disable SSH connections.	Enabled
escription	Factory Default
pecify the SSH interface TCP port number.	22
escription	Factory Default
nable or disable SNMP.	Disabled
escription	Factory Default
pecify the SNMP UDP port number.	161
escription	Factory Default
nable or disable Moxa Service.	Enabled
	escription escription pecify the SNMP. escription pecify the SNMP UDP port number. escription

# NOTE

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

Setting	Description	Factory Default
40404 (read only)	Specify the Moxa Service UDP port.	40404
Maximum number Setting	of Login Sessions for HTTP + HTTPS Description	Factory Default
Setting	Specify the maximum number of concurrent HTTP+HTTPS	

Setting	Description	Factory Default
	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.

# Hardware Interface

Reset Button Status * Disabled	-	Reset Button Activ	e Duration *
		0 - 180	sec.
Serial Status *			
Enabled	•		
USB Status *			
Enabled			

Configure the following settings:

### **Reset Button Status**

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

### **Reset Button Active Duration**

Setting	Description	Factory Default
0 to 180 (sec.)	<ul> <li>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.</li> <li>Note:</li> <li>If set to 0, the reset button will always be disabled.</li> <li>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-3252A and AWK-4252A Series; the WLAN LED on the AWK-1151C Series.</li> </ul>	120

### Serial Status

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

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

# **Configure SNMP Settings**

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

SNMP	SNMP Account List
NMP V1 and V	A are not secure. We recommend using SNM
NMP V1 and V	c are not secure. We recommend using SNM

### SNMP Status

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

### SNMP Version

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

### Read Community (for V1/V2c Versions)

Setting	Description	Factory Default
Public/Private	Specify the read community security authority level.	public
Read/Write Commun	ity (for V1/V2c Versions)	
Setting	Description	Factory Default

Specify the read/write community security authority level.

private

# •

## NOTE

Public/Private

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



# ΝΟΤΕ

While the AWK-3252A, AWK-4252A, and AWK-1151C Series use the same firmware and MIB structure, since the AWK-1151C Series only contains client feature sets and lacks DI/DO and Relay hardware interfaces, please be aware that SNMP read or write to non-applicable OIDs for the AWK-1151C Series will return "0 disabled" and "not support" messages.

When finished, click **APPLY**.

# Edit an SNMP Account

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

SNMP					
SNMP	SNMP Accour	nt List			
Username	Status	SNMP Status	Authority	Authentication Type	Encryption Method
admin	Enabled	Disabled	Read Write	None	None

Configure the following settings:

Edit SNMP Acco	ount S	ettings		
Username				
admin				
SNMP Status *				
Enabled	•			
Authority				
Read/Write	•			
Authentication Type				
None	•			
			CANCEL	APPLY

### Username

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

### SNMP Status

Shim 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.	Read/ write

### Authentication Type

Setting	Description	Factory Default
None	No authority type selected.	
MD5	Specify MD5 as the authority type.	None
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.	
DES	Specify DES as the Encryption Method.	None
AES	Specify AES as the Encryption Method.	

### **Encryption Key**

Setting	Description	Factory Default
	Depending on the selected Encryption Method, specify the 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.

System Clock	Time Zone	
Current Time		
2022-08-23 21:43:06	+00:00	
Clock Source *		
nternal Clock	-	
Date *		
2022-08-23		
Time *		
下午 09:43:06		

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.

Setting	Description	Factory Default
Current Time (read only)	Shows the current time.	Current Time
Clock Source		
Clock Source Setting	Description	Factory Default
Setting	<b>Description</b> Set the clock source to internal. This requires the date and	Factory Default
Setting	Set the clock source to internal. This requires the date and	Factory Default

# Configure the Time and Date (Internal Clock)

Date						
Settin	g			Descri	ption	
Day of	the n	nonth		Select 1	the cu	rrent da
2021	SEP	•			<	>
Su	Мо	Tu	We	Th	Fr	Sa
SEP			1	2	3	4
5	б	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

### 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 <b>Sync From</b> <b>Browser</b> to sync the time with your web browser.	Sync From Browser

# Configure Time Servers (NTP)

# System Time

Current Time 2022-08-31 16:26:58- Last Sync Timestamp  Clock Source * NTP Time Server 1 * NTP.Server 11 Time Server 2	-08:00	
Last Sync Timestamp  Clock Source * NTP Time Server 1 * NTP.Server 1	•08:00	
Clock Source * NTP Time Server 1 * NTP.Server	<b>•</b>	
NTP Time Server 1 * NTP.Server	•	
NTP Time Server 1 * NTP.Server	¥	
Time Server 1 * NTP.Server 1	•	
NTP.Server		
1		
Time Server 2	0 / 60	
TIME OCTVCT 2		
	0 / 60	
Sync Interval *		
10		
10 - 1440	min.	

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

When finished, click **APPLY**.

# **Edit the Time Zone**

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

Click the **Time Zone** tab.

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

Configure the following settings:

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

### **Daylight Saving Time**

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

Dayligh Daylight Sa							
Enabled			•				
Offset *							
00:00							
Start							
Month *		Week *		Day *		Hour *	
Jan	•	1st	•	Sun	*	00	•
End							
Month *		Week *		Day *		Hour *	
Jan	•	1st	•	Sun	•	00	
APPLY	r						

## Daylight Saving Status

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, and Roaming.



# **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.

Vireless Set	tings	
General	MAC Cloning	Status
Operation Mode *	Environment *	•

### **Operation Mode**



# NOTE

The AWK-1151C is a client device and does not support **AP** and **Master** mode.

Setting	Description	Factory Default
Disabled	Disable the operation mode.	
AP	Specify the operation mode as AP. Refer to AP Mode	
AF	Settings. (AWK-3252A, AWK-4252A only)	
Master	Specify the operation mode as Master. Refer to Master Mode	
Master	Settings. (AWK-3252A, AWK-4252A only)	
Sniffer	Specify the operation mode as Sniffer. Refer to Sniffer Mode	
Settings.		Disabled
Client	Specify the operation mode as Client. Refer to Client Mode	
Settings.		
Client-Router	Specify the operation mode as Client-Router. Refer to Client-	
Chefit-Rouler	Router Mode Settings.	
Slave	Specify the operation mode as Slave. Refer to Slave Mode	1
Slave	Settings.	

### **AP Mode Settings**

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



# NOTE

AP mode is only supported by the AWK-3252A and AWK-4252A Series.

Vireless Set	tings	
General	MAC Cloning	Status
Operation Mode * AP	Environment *	•

### Environment

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



### NOTE

Master mode is only supported by the AWK-3252A and AWK-4252A Series.

# Wireless Settings

Master	-	Indoor	-
Operation Mode *		Environment *	
General		MAC Cloning	Status

### Environment

Setting	Description	Factory Default	
Indoor	Set the application environment to indoor. Available channels		
	vary depending on the selection.	Indoor	
Outdoor	Set the application environment to outdoor. Available channels	1110001	
Outdoor	vary depending on the selection.		

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

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

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

### **Sniffer Mode Settings**

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

General	_	MAC Cloning	Sta	tus
he service [Sniffe	r] is not	secure interface. We	recomr	nend disabling i
peration Mode		Environment *		
niffer	•	Indoor	•	
F Band *				
5 GHz	•			
ecurity *				
lone	•			
RF Settings ^				
GHz				
Channel Width *		Channel *		Bonded Channel(s)
20/40/80 MHz	•	36 (5180 MHz)	•	40, 44, 48
.ntenna *		Antenna Gain		
dl	•	2		
		0 - 18	dBi	

Configure the following settings:

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels	
Indoor	vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels	1110001
Outdool	vary depending on the selection.	

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

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.

Wireless Sett	ings
---------------	------

General	MAC Cloning	Status
Operation Mode	Environment *	

### Configure the following settings:

### Environment

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

# **Wireless Settings**

MAC Cloning	Status
Environment *	
	Environment *

### Configure the following settings:

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

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

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

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.

Wireless Settings		
General	MAC Cloning	Status
Operation Mode *	Environment *	
Slave	<ul> <li>Indoor</li> </ul>	

Configure the following settings:

### Environment

Setting	Description	Factory Default
Indoor	Set the application environment to indoor. Available channels	
1110001	vary depending on the selection.	Indoor
Outdoor	Set the application environment to outdoor. Available channels	1110001
Outdoor	vary depending on the selection.	

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

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

For configuring advanced settings, refer to Advanced RF Settings.

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

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

For AP and Master operation modes, configure and enable the SSID profile. There are no SSIDs on the device by default. To add a new SSID, click the **Add** 1 icon.

# 

# NOTE

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

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

Configure the following settings:

SSID *		F Band *		
Moxa-5G	5	GHz	•	
At least 1 character	7/32			
RTS / CTS Threshold *				
2346				
32 - 2346	bytes			
Transmission Ra				
Data Transmission Rate		v	Min. Data Transmission Rate * 0	
Data Transmission Rate				Mbps
Data Transmission Rate Auto	*	•	0	Mbps
Transmission Ra Data Transmission Rate Auto Broadcast/Multicast Dat HT-MCS5	*	•	<b>0</b> 0 - 65	Mbps
Data Transmission Rate Auto Broadcast/Multicast Dat	*	• n Rate *	0 0 - 65 Management Transmission Rate *	

### 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	Auto
Auto	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**.

-				2
SSID Broadcast Status *				
Enabled	•			
Security *		WPA Mode *		
WPA2	•	Personal	•	
Protected Management	Frame *			
Disabled	•			
Encryption *		EAPOL Version *		
AES	•	1	•	
Passphrase *				
	Ø			
At least 8 characters	8 / 64			
Key Renew *				
3600				
60 - 86400	sec.			
Copy Configuration	ns to SSI	Ds 🗸 🚺		
Copy Configuration	ns to SSI	Ds 🔻 🚺		

### 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.	
WPA	Use WPA authentication.	7
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.	Open
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	7

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

and WPA3 clients to connect to the AWK.

- **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.

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.	

### Protected Management Frame

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

Encryption

Setting	Description	Factory Default		
AES	AES Use Advance Encryption System (AES) encryption.			
	Use TKIP/AES Mixed encryption. This option provides a TKIP			
TKIP/AES Mixed*	broadcast key and TKIP+AES unicast key to support legacy AP	TKIP/AES Mixed		
TRIP/ALS MIXEU	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.	1
Primary/Secon	dary RADIUS Server IP (for Enterprise mode only)	
Setting	Description	Factory Default
IP address	Specify the RADIUS authentication server for EAP.	None
Primary/Secon	dary 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
	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

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

### Copy Configurations to SSIDs

Setting	Description	Factory Default
ISSID	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**  $\checkmark$  icon next to the SSID you want to edit. Refer to **Create a New SSID** for more information about setting.

SID Settings ^						
Jile of C	SSIDS do not apply security typ	e. We recommend disa.	ning them.			
Î				Q	Search	
	SSID	RF Band	Security	Encryption	Status	
	MoxaGuest_5G	5 GHz	OPEN		Enabled	
•	Moxa-5G	5 GHz	WPA2 (Personal)	AES	Disabled	
•	Moxa-2G	2.4 GHz	WPA2 (Personal)	AES	Disabled	
Max 9						

# **Delete an Existing SSID**

To delete an existing SSID, check the SSID, then click the **Delete**  $\hat{\blacksquare}$  icon above the table.

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

When prompted, click **DELETE**.



# **RF Settings**

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



Í

# NOTE

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

2.4 GHz					
RF Type					
G/N Mixed					
Channel Width *		Channel *		Bonded Channel(s)	
20/40 MHz	•	6 (2437 MHz)	•	10	
Antenna *		Max. Transmission Power *		Antenna Gain *	
All	•	28		2	
		0 - 28	dBm	0 - 18	dBi
Beacon Interval *					
100					
40 - 1000	ms.				
5 GHz					
RF Type *					
N/AC Mixed	•				
Channel Width *		Channel *		Bonded Channel(s)	
20/40/80 MHz	•	36 (5180 MHz)	•	40, 44, 48	
Antenna *		Max. Transmission Power *		Antenna Gain *	
All	•	26		2	
		0 - 26	dBm	0 - 18	dBi
Beacon Interval *					
100					
40 - 1000	ms.				
Advanced Settin	00 A				
MTU *	ys A				
1500					
68 - 2290	bytes				

### For 2.4 GHz

Configure the following settings:

### RF Type

718 -		
Setting	Description	Factory Default
C/N Mixed	Enable IEEE 802.11g/n. 802.11n may operate at a slower	
G/N Mixed	speed if 802.11g clients are connected to the network.	
D/C/N Mixed	Enable IEEE 802.11b/g/n. 802.11g/n may operate at a slower	B/G/N Mixed
B/G/N Mixed	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	
20 MI12	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. <b>Note</b> : 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.	
2	Specify antenna 2 as the output antenna port.	All
ALL	Specify both antennas as the output antenna port.	

### Maximum Transmission power

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

71====		
Setting	Description	Factory Default
AC Only (5 GHz)	Only enable IEEE 802.11ac.	
N/AC Mixed	Enable IEEE 802.11n/ac.	A/N/AC Mixed
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	Select the channel from the drop-down list. Each channel	36 (5180 MHz)
(5825 MHz)	supports different frequencies.	50 (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.	
1	Specify antenna 1 as the output antenna port.	All
2	Specify antenna 2 as the output antenna port.	
Maximum Transmiss	ion power	
Setting	Description	Factory Default
	Specify the maximum transmission power which acts as a	
dBm	hard ceiling for different transmission rates.	26 dBm
	<b>Note</b> : The supported Maximum Transmission Power depends	
	on the selected country code.	
Antenna Gain (for Al	P/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

When finished, click **APPLY**.

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

Some operation modes require additional advanced RF settings.



# NOTE

Available RF settings depend on which Operation mode is active.

hutoo		
bytes		
bytes		
te: 5 GHz		
е*	Min. Data Transm	nission Rate *
-	0	
	0 - 65	Mbps
sion Rat		
-		
	bytes te: 5 GHz e *	te: 5 GHz e * Min. Data Transn • 0 0 - 65

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 Ti	ransmission Rate		
Setting	Description	Factory Default	
0 to 64 Mbps	Specify a minimum transmission rate. By setting a minimum transmission rate, the AWK Series will avoid communicating		

### Management Transmission Rate

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

over weak signal wireless links to maintain better wireless performance and optimize the wireless frequency usage.

When finished, click **APPLY**.

### **MAC Cloning Settings**

(0 to disable)

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

# **Wireless Settings**

General	MAC Cloning	Status
MAC Cloning Status *		
Enabled	<b>*</b>	
MAC Cloning Method *		
Auto	•	
MAC Cloning Interface *		
LAN 1	-	

Configure the following settings:

### MAC Cloning Status

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

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

0 (Disabled)

### MAC Cloning Interface

Setting	Description	Factory Default
LAN 1	Specify the static MAC address of LAN 1 that the connected AWK devices should copy.	-LAN 1
LAN 2	Specify the static MAC address of LAN 2 that the connected AWK devices should copy.	

When finished, click **APPLY**.

# **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.

Wireles	s Setti	ngs		
Gener	al	MAC Cloning	Status	
AP SSID AP: Test			•	
BSSID 06:90:E8:AA Channel 6 (2437 MH:		Noise Floor <b>-104 dBm</b> Bonded Char <b>10</b>	nnel	Channel Width 20/40 MHz

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.

Associated Clien	ıt List							
≡√						<b>Q</b> Search		
MAC Address	IP Address	Conn. Duration	VHT Cap.	Tx. Rate (Mbps)	Chan. Width (MHz)	Mgmt. SNR. (dB)	Mgmt. SS. (dBm)	Mgmt. Tx. Pkt.
•								

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

<b>~</b>	MAC Address
<b>~</b>	IP Address
<b>~</b>	Connection Duration
$\checkmark$	VHT Capability
$\checkmark$	Transmission Rate

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

# **Wireless Settings**

General	MAC Cloning	Status	_	
Client				2022-08-31 18:14:24 🕅 🕻
SSID	MAC Addres	s	Current BSSID	AP IP Address
test				
Channel	Bonded Cha	nnel	Channel Width	
Connection Duration	AP Has VHT	Capacity		
Transmission Rate	Mgmt. SNR.		Signal Strength	Noise Floor
Mgmt. Tx. Packets	Mgmt. Rx. P	ackets		
Data Tx. Packets	Data Rx. Pao	kets		

# **Connection Management**

# **Connection Check and Recovery**

.

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

Client-to-AP Link		
Disabled	▼	
AP Alive Check		
AP Alive Check Status *		
Disabled	•	
Demote Liest Ohe	.1.	
Remote Host Che Remote Host Check Status		
Disabled	-	

# **Client-to-AP Link Check**

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

Client-to-AP Link Ch Client-to-AP Link Check Status	
Enabled	▼
Check Timeout *	
30	
10 - 60 s	sec.
Reset Connection Recovery *	Reset Connection Retry Count *
Enabled	▼ 5
	1 - 5
Reboot Recovery *	Reboot Retry Count *
Enabled	<b>▼</b> 5
	1 - 5

### Configure the following settings:

### Client-to-AP Link Check Status

Setting	Description	Factory Default		
Enabled/Disabled	Enable or disable the Client-to-AP Link Check function.	Disabled		
Check Timeout				
------------------	-------------------------------------	-----------------	--	--
Setting	Description	Factory Default		
10 to 60 (sec.)	Specify the check timeout interval.	30		
Reset Connection	Recovery			

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

### Reset Connection Retry Count

Setting	Description	Factory Default
	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 Cour	nt			
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.

AP Alive Check			
AP Alive Check Status			
Enabled	•		
Check Interval *		Retry Count *	
50		3	
20 - 1000	ms.	3 - 10	
Expiry *			
1000			
100 - 10000	ms.		
Threshold Indicate *			
SNR	•		
5 GHz		2.4 GHz	
SNR Candidate Threshold *		SNR Candidate Threshold *	
40		40	
5 - 60	dB	5 - 60	dB

Configure the following settings:

### AP Alive Check Status

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

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 Signal Strength	Use SNR as the threshold indicator. Use signal strength as the threshold indicator.	SNR
5 GHz: SNR Candid	late Threshold (for SNR)	·
Setting	Description	Factory Default
5 to 60 (dB)	Specify the SNR roaming threshold.	40
2.4 GHz: SNR Cand	lidate Threshold (for SNR)	
Setting	Description	Factory Default
5 to 60 (dB)	Specify the SNR roaming threshold.	40

Setting	Description	Factory Default
-100 to -35 (dBm)	Specify the signal strength roaming threshold.	-65
2.4 GHz: Signal Stre	ength Candidate Threshold (for Signal Strength)	
2.4 GHz: Signal Stre Setting	ength Candidate Threshold (for Signal Strength) Description	Factory Default

# 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.

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

Configure the following settings.

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.	Static
Host (for Static Ho Setting	st Type only) 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		
Check Timeout Setting	Description	Factory Default

### Retry Interval

100 to 10000 (ms)

Setting	Setting Description		
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	

or unresponsive and will trigger the recovery mechanism.

exceeded, the client will consider the remote host unreachable 1000

When finished, click **APPLY**.

## **AP-based Disconnection**

The **AP-based Disconnection** tab contains Wi-Fi connectivity tools to configure the signal strength conditions for clients to meet normal operational communication requirements. Additionally, this screen

allows users to enable the AP-based disconnection mechanism to disconnect legacy clients without roaming logic in order to encourage these clients to automatically associate to another AP with a stronger signal when falling below the set threshold. Click the **AP-based Disconnection** tab under **Wi-Fi > Connection Management** in the function tree to access this screen.

Connection Manage	ment			
Connection Check and Recovery	AP-based Disconnecti	on		
AP-based Disconnection				
		<b>Q</b> Search		
SSID	SSID Stat	us AP-based Dis	sconn. Status Disc	conn. Threshold
5 GHz: AWK-3252A_ShopFlo	or Enabled	Enabled	SNR	R: 40 dB
Max 9				1 – 1 of 1
APPLY				

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

### **Edit AP-based Disconnection Settings**

5 GHz: AWK-3252A_ShopFloor S			
Enabled -			
Status *			
Enabled 🔹 🚺			
Attempts *			
3			
1 - 10			
Indicator of Disconnection Threshold *			
SNR	•		
5 GHz Disconnection Threshold (SNR) *			
40			
5 - 60	dB		
		CANCEL	APPLY

#### Status

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

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

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

When finished, click **APPLY**.

# 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.

# Roaming

Indicator of Roaming Thresho SNR	Id *		
5 GHz Roaming Threshold (SNR) * 40		2.4 GHz Roaming Threshold (SNR) * 40	
5 - 60 Roaming Difference * <b>7</b>	dB	5 - 60	dE

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.	SINK

### 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
	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



# ΝΟΤΕ

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.



# ΝΟΤΕ

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 <u>Wi-Fi > Wireless Settings</u> 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.



# NOTE

As key renewal is automatic for WPA3 encryption, using Turbo Roaming with WPA3 will result in a one-time increased handover time of approximately 200 ms during the roaming process when the key renewal takes place.

When finished, click **APPLY**.

# **Client Isolation**

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

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

By default, client isolation is not enforced.

# **Client Isolation**

SSID	
AP: moxa_guest	•
Oliant loolation *	
No isolation	
Isolation within the same SSID	
Isolation within the same subnet	

# Wi-Fi ACL

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

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

# **Automatic Wi-Fi ACL**

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

Automatic Wi-Fi ACL	
Automatic Wi-Fi ACL Status	Automatic Wi-Fi ACL Status
Wi-Fi Authentication Failure Retry Threshold	Enabled Disabled
1 - 10 time (s)	

### Automatic Wi-Fi ACL Status

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

### Wi-Fi Authentication Failure Retry Threshold

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

## NOTE

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

When finished, click **APPLY**.

## **Static Wi-Fi ACL**

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

Static Wi-Fi ACL Status	Wi-Fi ACL Mode	Wi-Fi ACL Status
Static Wi-Fi ACL List Mode	Block Accept	Enabled Disabled
0	<u>q</u>	Search
Status	MAC Address	
🗌 🧪 Enabled	00:90:E8:11:22:33	
Disabled		
Enabled	00:90:E8:AA:BB:CC	
Max 64	Items per page: 10 ▼ 1-3	3 of 3 I < < > >I
APPLY		

Static	Wi-Fi	ACL	Status

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

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

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.

Ρ	ort Se	ettings	5				
	Gene	ral	Port Status				
	Ρ	ort	Status	Descri	ption		
	1		Enabled				
	1 2		Enabled				
E	dit Port	1 Settir	ngs				
	atus nabled		•				
D	escription	1			0 /	127	
						CANCEL	APPLY

Configure the following settings:

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



## ATTENTION

The AWK-1151C 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.

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

When finished, click **APPLY**.



## ATTENTION

When both LAN1 and LAN2 are enabled, only one LAN port should be used as an uplink. The other LAN port may be used to connect other Ethernet based devices such as IP cameras. Be careful NOT to connect both LAN ports as uplinks to a switch simultaneously to prevent switching loops.

## **Status Check**

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

Port Settings					
	General		Port S	tatus	
c	;				
Po	rt	Status	L	ink Status	
LA	N 1	Enabled	L	ink Down	
LA	N 2	Enabled	L	ink Up	

# 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.

LAN					
Global		Settings			
Management VLAN *					
	-				
1					
I Management Inter Management Interface		ick Settings			
Management Inter		ick Settings			
Management Inter Management Interface				Untagged VLAN	

Configure the following settings:

### Management VLAN ID

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

## **Management Interface Quick Settings**

### Management Interface

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

#### Mode

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

### PVID

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

### Tagged VLAN

scription	Factory Default
he port type is set to Trunk or Hybrid, specify the VLAN ID tagged devices that connect to this port	None
h	e port type is set to Trunk or Hybrid specify the VLAN ID

### Untagged VLAN

Setting	Description	Factory Default
1 to 4094	Itagged devices that connect to this port and the tags that	Dependent on the selected PVID

When finished, click **APPLY**.

# **VLAN Settings**

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

V	LAN			
	Glo	obal	Settings	
	٥	₽.		
		VLAN	Name	Member Interface
		1		LAN1, LAN2 SSID: Moxa_Guest
	Max 25	6		

## **Create a New VLAN ID**

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

V	VLAN				
	Global		Settings		
	<b>.</b>				
		VLAN	Name	Member Interface	
		1		LAN1, LAN2 SSID: Moxa_Guest	
	Max 256				
_					
C	reate V	ΙΔΝ			

Create VLAN			
VLAN ID *	0		
1 - 4094			
Name			
0 / 32			
		CANCEL	CREATE

Configure the following settings:

### VLAN ID

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

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.

	VLAN	Name	Member Interface
	1		LAN1, LAN2 SSID: Moxa_Guest
Max 256			

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.

Interface	Mode	PVID	Untagged VLAN
IAN1	Access	1	1
/ LAN2	Access	1	1
SSID: .M-Guest	Access	1	1

# Edit Interface LAN1 Settings

Mode *				
Access	•			
PVID * 1	•			
Tagged VLAN				
Untagged VLAN 1	×			
Copy Configurati	ons to Interfaces	• 0		
			CANCEL	APPLY

### 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.	
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.	Access
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	None
	to.	

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.

IP Configurati	on		
General	Status		
LAN IP Mode * Static	<b>•</b>		
IP Address * 192.168.0.222	Subnet Mask * 24 (255.255.255.0)	•	Default Gateway
DNS Server 1	DNS Server 2		
APPLY			

Configure the following settings.

Setting	Description	Factory Default
DHCP	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	I 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.

IP Configurat	tion		
General	Status		
LAN IP Mode Static IP Address		Subnet Mask 255.255.255.0	Default Gateway
192.168.0.222 DNS Server 1  IP Conflict Check Pass	l	203.203.203.0 DNS Server 2 	

# **Networking Service**

From the Networking Service section, you can configure DHCP Server settings.



# **DHCP Server**

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

IP addresses can be assigned in one of two ways:

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

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



## NOTE

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

DHCP Pool Status * Enabled	^					
IP Address : Start		IP Address : End *				
192.168.127.	.59	192.168.127.77				
MAC-based	I IP Assignn				<b>Q</b> Search	
	Hostname	MAC Address	IP Address	Status	<b>Q</b> Search	
0	-		IP Address	Status	Q Search	0 of 0

# **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.

S	tatic R	oute							
	٠								
		Status	Name		Destination	Netm	ask	Next Hop	Interfac
	Max 32								
	APPLY								
C	Create St	atic Ro	ute Entr	y					
	ntry Status * Visabled		•						
Ν	lame								
D	estination	*	0 / 31						
	etmask * 4 (255.255	5.255.0)	•						
Ν	lext Hop								
	nterface * VAN		•						
_	1etric - 32766								
	- 32/00					CANCEL	CREATE		

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.

# **Routing Table**

G				
Destination	Netmask	Gateway	Interface	Metric
192.168.0.0	255.255.255.0	0.0.0.0	LAN	0

# 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.

ress Tran	slate					
•						
					<b>Q</b> , Search	
Name	Description	Pri.	Mode	Protocol	WAN IP : Port	LAN IP : Port
		32	N-to-1			
					Items per page: 10 👻	1 – 1 of 1 🛛 🗍
	Name	Name Description	Name Description Pri.	Name Description Pri. Mode	Name Description Pri. Mode Protocol	Name Description Pri. Mode Protocol WAN IP : Port 32 N-to-1

Configure the following setting:

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

## Add a New NAT Rule

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

Create NAT Rule
Rule Status *
Disabled 👻
Name
0 / 31
Description
Priority *
1
1 - 31
NAT Mode *

### Configure the following settings:

Setting	Description	Factory Default		
Enabled/Disabled	Enable or disable the NAT rule.	Disabled		
Name		·		
Setting	Description	Factory Default		
0 to 31 characters	Enter a name for this rule.	None		
Description				
Setting	Description	Factory Default		
0 to 127 characters	Enter a description for this rule.	None		
Priority				
Setting	Description	Factory Default		
1 to 31	Specify the priority for this rule.	1		
NAT Mode		·		
Setting	Description	Factory Default		
1 to 1	Set the NAT mode to 1-to-1.	None		
PAT	Set the NAT mode to PAT (Port Address Translation).	None		
Mapping Type (1 to	1 Mode only)			
Setting	Description	Factory Default		
Single to Single	Set the mapping type to Single to Single.			
Range to Range	Set the mapping type to Range to Range.	Single to Single		
Subnet to Subnet	Set the mapping type to Subnet to Subnet.			
Mapping Type (PA1	Mode only)			
Setting	Description	Factory Default		
Single Port	Set the mapping type to Single Port.	Single Port		
Multiple Ports	Set the manning type to Multiple Ports	Single Fort		

Set the mapping type to Multiple Ports.

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						
C - Him -		The second se				

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

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

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



# Edit an Existing NAT Rule

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

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

When finished, click **APPLY**.

## **View the NAT Rule Status**

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

Ð	0 ≡∕							<b>Q</b> Searc	h			
	\$	Status	Name	Description	Pri.	Mode	Protocol	WAN IP :	Port		LAN IP : Po	ort
	/	Enabled	Rule 1	Rule 1 for the field site	32	N-to-1						
Max 3	2							ltems per pa	ge: 10	• 1	– 1 of 1	< <

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

	₽ =,	
Sel	ect Visible Columns	Name
	Enabled	
$\checkmark$	Enable	
$\checkmark$	Name	
$\checkmark$	Description	
<b>~</b>	Pri.	
$\checkmark$	Mode	
$\checkmark$	Protocol	
<b>~</b>	WAN IP : Port	
$\checkmark$	LAN IP : Port	

Only information for the selected items will be shown.

÷	≡,					<b>Q</b> Sea	rch	
	Status	Name	Description	Mode	WAN IP : Port		LANI	P : Port
	✓ Enabled	Rule 1	Rule 1 for the field site	N-to-1				
Max 3	2					Items per page: 10	•	1 – 1 of 1

# **Firewall**

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



# **Layer 2 Policy**

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

Layer 2 I	Policy	/			
Layer 2 Firewall 3	Status	•			
Default Action Drop +		•			
	Status	Pri.	Action	Src. MAC Address	Dst. MAC Address
Max 64					
APPLY					

Configure the following settings:

Layer 2 Firewall St	atus	
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 all packets that do not match any policy rule.	—— Drop



## 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.

Ð					
	Status	Pri.	Action	Src. MAC Address	Dst. MAC Address
Max 64					
APPLY					



Create Layer	2 Firew
Rule Status *	
Disabled	•
Priority *	
1	
1 - 64	
Action *	
Accept	Ŧ
Source MAC Address	
Any	
Destination MAC Add	ress
Any	

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



## ATTENTION

Be careful when configuring the packet filtering function:

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

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

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

When finished, click **APPLY**.

# **Layer 3 Policy**

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

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

Configure the following settings.

Layer 3 Firewall St	atus	
Setting	Description	Factory Default
Enabled/Disabled	Enable or disable the Layer 3 firewall function.	Disabled
Default Action	Description	Fristern Defeuit
Setting	Description	Factory Default
Accept	Packets that match the policy rule will be allowed.	Duran



## **ATTENTION**

Drop

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.

Packets that match the policy rule will be denied.

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

When finished, click APPLY.

Drop

# Add a New Layer 3 Firewall Rule

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

	Status	Pri.	Action	Src. MAC Address	Dst. MAC Address
Max 64					
APPLY					

### Configure the following settings:

Create Layer 3 Fire	vall Rule
Rule Status *	
Disabled	F
Priority *	
1	
1 - 64	_
Action *	Protocol *
Accept	All
Source	
IP Address	Netmask
Any	32 (255.255.255.255) 💌
Destination	
IP Address	Netmask
Any	32 (255.255.255.255) 💌
	CANCEL APPLY

### Rule Status

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

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

### Protocol

Setting	Description	Factory Default
All	Filter all protocol traffic.	
ICMP	Only filter for ICMP protocol traffic.	All
ТСР	Only filter for TCP protocol traffic.	All
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 255.255.255.255.255" refers to the sole IP addresses from 192.168.1.1 to 192.168.255.

### Source

IP Address		
Setting	Description	Factory Default
IP address	Specify the source IP address.	Any
Netmask		
Setting	Description	Factory Default
Netmask	Select the subnet mask	32 (255.255.255.255)
Port Range		
Setting	Description	Factory Default
0 to 65535	If the Protocol is set to TCP or UDP, specify the port range.	None

### Destination

IP Address		
Setting	Description	Factory Default
IP address	Specify the destination IP address.	Any
Netmask		
Setting	Description	Factory Default
Netmask	Specify the subnet mask.	32 (255.255.255.255)
Port Range	· ·	·
Setting	Description	Factory Default
0 to 65535	If the Protocol is set to TCP or UDP, specify the port range.	None

When finished, click **APPLY**.

# **Certificate Management**

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

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

# **Basic Concept of SSL**



# **Device Certificate**

The **Device Certificate** table shows the current certificate for the listed functions. The AWK Series supports different certificates for different functions to increase security and minimize the potential risk in the event a certificate is compromised.

	te Management						
evice Cert	lificate						
æ.						Q Search	
	Function	Issue To	Issue By	Start Date	Expiration Date	Serial Number	
/ D	Data Transferring	moxa-awk-4252a	moxa-awk-4252a	Jun 10 11:35:54 2022 GMT	Jun 9 11:35:54 2027 GMT	1DAD0CC136A6B8DDBFAE9F23FD5E7A170E5C637A	
/ D	HTTPS	moxa-awk-4252a	moxa-awk-4252a	Jun 14 15:11:30 2022 GMT	Jun 13 15:11:30 2027 GMT	68E874CE1A7DD76482FDD4BBC2A92356C602CB73	
/ D	RSSI Report	moxa-awk-4252a	moxa-awk-4252a	Jun 10 11:36:20 2022 GMT	Jun 9 11:36:20 2027 GMT	17A4505C1B765433A2BE95A6021A820E418EAF31	
/ D	Syslog Server 1	moxa-awk-4252a	moxa-awk-4252a	Jun 14 15:15:23 2022 GMT	Jun 13 15:15:23 2027 GMT	260770B9701E5BA73694EE5FBD9EA48B0D5011AA	
/ D	Syslog Server 2	moxa-awk-4252a	moxa-awk-4252a	Jun 10 11:36:02 2022 GMT	Jun 9 11:36:02 2027 GMT	3470D83D8615E1259F693BA4E20AC62F07FF63E7	
/ D	Syslog Server 3	moxa-awk-4252a	moxa-awk-4252a	Jun 10 11:36:18 2022 GMT	Jun 9 11:36:18 2027 GMT	136CB52E4FE0CF16EE41222AA49F74CF2D6FC6FA	
/	Wi-Fi Client	moxa-awk-4252a	moxa-awk-4252a	Jun 10 11:36:23 2022 GMT	Jun 9 11:36:23 2027 GMT	18DD4729FAE2FB21F7A9CA72AC23D833F19B36DD	
/ D	Wi-Fi Sniffer and Wi-Fi Mirroring	moxa-awk-4252a	moxa-awk-4252a	Jun 10 11:36:31 2022 GMT	Jun 9 11:36:31 2027 GMT	02A8B18961592530FDEEC61C226CD81D14AD7BDE	
Max 8							1 – 8 c
able I	Field Name	Descript	ion				
unctio	n	The list o	f certificate	e-based authen	tication functio	ns:	
		Data Transferring					

	Data Transferring
	HTTPS
	RSSI Report
	Syslog Server 1/2/3
	Wi-Fi Client
	Wi-Fi Sniffer and Wi-Fi Mirroring

Table Field Name	Description
Issue To	The entity the certificate was issued to.
Issue By	The entity the certificate was issued by.
Start Date	The valid start date of the certificate.
Expiration Date	The expiration date of the certificate.
Serial Number	The unique serial number of the certificate.

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

	AWK-42	252A-UN									Hi, admin 🚦
Q Search for function		Certi	fica	te Manage	ment						
Device Summary		Device	e Cert	ificate							
🔅 System		₽;								Q Search	
Ports				Function		Issue To	Issue By	Start Date		Expiration Date	Serial Number
Layer 2 Switching		1	Ð	Data Transferring	In stall Da	uise Osstificato	and Kass		22 GMT	Jun 9 11:35:54 2027 GMT	1DAD0CC136A6B8DDBFA
P Configuration		$\mathbf{\mathcal{O}}$	G	HTTPS	Install De	vice Certificate	and Key		22 GMT	Jun 13 15:11:30 2027 GMT	68E874CE1A7DD76482FE
Routing and NAT		1		RSSI Report	Self-Signed				22 GMT	Jun 9 11:36:20 2027 GMT	17A4505C1B765433A2BE
Firewall	Ý	1		Syslog Server 1	Upload		CANCEL	GENERATE	22 GMT	Jun 13 15:15:23 2027 GMT	260770B9701E5BA73694
Certificate Managen	nent	1	J	Syslog Server 2		moxa-awk-4252a	moxa-awk-4252a	Jun 10 11:36:02	zu22 GMT	Jun 9 11:36:02 2027 GMT	3470D83D8615E1259F693
Diagnostics		1	Ð	Syslog Server 3		moxa-awk-4252a	moxa-awk-4252a	Jun 10 11:36:18	2022 GMT	Jun 9 11:36:18 2027 GMT	136CB52E4FE0CF16EE41
All one would						12 10000000					

# **Server CA Certificate**

Server CA Certificate

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

æ,					<b>Q</b> Search	
	Function	Issue To	Issue By	Start Date	Expiration Date	Serial Number
•	Data Transferring					
	Email Notification					
	RSSI Report					
•	Syslog Server 1					
•	Syslog Server 2					
•	Syslog Server 3					
- /	Wi-Fi Client					
Max 7						1 – 7 of 7



# ATTENTION

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

# Security

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



# **Device Security**

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



## **Login Policy**

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

ogin Poli.	су	
Login Message		
Login Wessage		
		0 / 500
Login Failure Messa	ge	
Failed to login		
		15 / 500
User Lockout Status	*	
User Lockout Status Enabled	*	
	*	
Enabled	•	
Enabled	•	
Enabled Login Failure Retry T 5	+reshold *	
Enabled Login Failure Retry T 5 1 - 10	•	
Enabled Login Failure Retry T 5 1 - 10 Lockout Period *	+reshold *	
Enabled Login Failure Retry T 5 1 - 10 Lockout Period * 5	hreshold * time(s)	
Enabled Login Failure Retry T 5 1 - 10 Lockout Period *	+reshold *	
Enabled Login Failure Retry T 5 1 - 10 Lockout Period * 5	hreshold * time(s)	
Enabled Login Failure Retry T 5 1 - 10 Lockout Period * 5 1 - 10	hreshold * time(s)	
Enabled Login Failure Retry T 5 1 - 10 Lockout Period * 5 1 - 10 Session Lifetime *	hreshold * time(s)	

### Configure the following settings:

### Login Message

Setting	Description	Factory Default
() 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
		ecces.

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**.

## **Security Status**

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

Feature Gro All C I	oup ▼	Q. Search
Status	Risk Level	Risk Description
A	HIGH	Enable HTTP to access this device.
$\checkmark$	HIGH	Enable Telnet to access this device.
	LOW	Firewall is not enabled to restrict network access.
Feature Gro	pup	
All (default) User Interfa Event Logs System Service Network		

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

## **Trusted Access**

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

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

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

nabled	•			Q Search
	IP Address	Netmask	Status	
	192.168.127.87	255.255.255.0	Enabled	
	192.168.128.55	255.255.0.0	Disabled	
lax 20 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 Statistics** under **Diagnostics > Network Status** in the function tree to access this page.

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

## LLDP

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

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

## **LLDP Settings**

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

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

Configure the following settings:

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

#### Transmission Interval

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.

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

# Bridge Table

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

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

## **ARP Table**

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

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

# **Event Logs and Notifications**

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

Event Logs and Notifications
Event Log
Notifications
Syslog
SNMP Trap/Inform
Email Settings
Relay Alarm Cut-off

## **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.

5	_ist Re	gistered Log	s Oversize Ac	ion B	ackup	
GI	i E.					Q Searc
Index	Bootup Number	Severity	Timestamp	Uptime	Group	Message
1	2	Notice	2022-10-11 13:20:07.397128	0d00h17m52s	System	Configuration saved successfully. (User: admin, IP: 192.168.127.2, Interface: HTTPS)
		Notice	2022-10-11	0d00h17m51s	System	Device configuration was changed. (User: admin, IP: 192.168.127.2, Interface: HTTPS)
2	2	Nouce	13:20:07.204867			ппез
	2	Notice	13:20:07.204867 2022-10-11 13:18:50.952219	0d00h16m35s	Wi-Fi	[.M-Guest] Installed key successfully for the AP [7c:57:3c:2e:ba:12].
2 3 4	10 <del>10</del>		2022-10-11	0d00h16m35s 0d00h16m35s	Wi-Fi Wi-Fi	

## **Registered Logs**

Click the  $\ensuremath{\textbf{Registered Logs}}$  tab to view and edit event log groups.

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

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

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

Configure the following settings:

Log Registration 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					
Syclog	Sand the event logs to a Sycleg server	Lucal, Syslog					

When finished, click **APPLY**.

## **Oversize Action**

Syslog

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

Send the event logs to a Syslog server.

Event Log			
Log List	Registered Logs	Oversize Action	Backup
Oversize Action Overwrite the oldest Capacity Warning Status * Disabled APPLY	event log 👻		
Auto Backup Status * Disabled	k Up Event Logs to /	ABC-02	

Configure the following settings:

#### **Oversize-Action**

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

#### Auto Backup Status

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable automatic event log backups to an ABC-02.	Disabled

When finished, click **APPLY**.

## Backup

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

Event Log			
Log List	Registered Logs	Oversize Action	Backup
Storage Location *	•		
BACKUP			

#### Storage Location

Setting	Description	Factory Default
Local	Back up the event log to the local storage on the AWK device.	
TFTP	Back up the event log via TFTP.	None
SFTP	Back up the event log via SFTP.	none
ABC-02	Back up the event log to an ABC-02 USB tool.	

#### 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	Enter the file name of the event log backup.	None
name	Line the hame 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 SF	TP only)	
Setting	Description	Factory Default
Password	Enter the SFTP server account password.	None
Select Folder (for	ABC-02 only)	
Setting	Description	Factory Default
Folder	Select the folder on the ABC-02 to store the event log backup in.	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.

Group Event Name Status Severity Notification	Method
System Cold start Enabled Notice Trap, Email	
System Warm start Enabled Notice Trap, Email	
System Configuration changed Enabled Notice Trap, Email	
System Reaching log capacity Enabled Alert Trap, Email	
Power Power 1 turned on Enabled Warning Trap, Email	
Power Power 1 turned off Enabled Warning Trap, Email	

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

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

Configure the following settings:

Event Notification Sta	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.				
Email	Trap/Email				
Relay	Use a relay for sending notifications. This option is only	rrap/ Linaii			
Relay	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.

Syslog Status * Disabled	•	Event Reporting Severity *
Syslog Server 1 Status *		
Disabled	•	
Syslog Server 2 Status *		
Disabled	•	
Syslog Server 3 Status *		
Disabled	•	

Configure the following settings:

Syslog Status		
Setting	Description	Factory Default
Enabled/Disabled	Enable or disable logging events to a syslog server.	Disabled
Event Reporting Se	verity	
Setting	Description	Factory Default
Emerg.	Specify the syslog severity as Emergency.	
Alert	Specify the syslog severity as Alert.	
Crit.	Specify the syslog severity as Critical.	
Error	Specify the syslog severity as Error.	Info.
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

Setting	Description	Factory Default
Enabled/Disabled	Disabled	
Svelog Server 3 Sta	tus	
Syslog Server 3 Sta		Factory Default
Syslog Server 3 Sta Setting Enabled/Disabled	<b>Description</b> Enable or disable the third syslog server.	Factory Default

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 Tra	ap/Inform		
General	SNMP Trap/	Inform Account	
•			
E F	Recipient IP/Name	Mode	Trap Community
Max 2			
SNMP Inform Inform Retry * 3	n Settings		
1 - 99 Inform Timeout * <b>10</b>			
1 - 300 APPLY	sec.		

## **General Settings**

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

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

Configure the following settings:

	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.	
Trap V1	Set the trap version to Trap V1.	
Trap V2c	Set the trap version to Trap v2c.	Disabled
Inform V2c	Set the inform version to Inform V2c.	Disabled
Trap V3	Set the trap version to Trap V3.	
Inform V3	Set the inform version to Inform V3.	

When finished, click **APPLY**.

## **SNMP Inform Settings**

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

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

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 E** icon to create a new entry.

SI	NMP T	rap/I	nform	1	
	General		SNMP 1	Frap/Inform Account	
		Userna	me	Authentication Type	Encryption Method
	Max 1				

#### Configure the following settings:

----

Create SNMP	Trap/In	form Account	
Username *			
At least 4 characters	0 / 32		
Authentication Type *			
None	-		

#### Username

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

type	
Description	Factory Default
Do not use any authentication mechanism.	
Use MD5 as the authentication type.	None
Use SHA as the authentication type.	
	Do not use any authentication mechanism. Use MD5 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.	
DES	DES is the encryption method.	None
AES	AES is the encryption method.	

#### Encryption Key (when DES and AES is selected)

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

When finished, click **APPLY**.

## **Email Settings**

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

Email Server *				
	0 / 60			
SMTP: TCP Port 25				
0 - 65535 Authentication Status *				
Disabled	-	Username	Password *	ø
		0 / 60		0 / 60
Security *				
None	•			
Sender Email Addre	SS			
	0 / 60			
1st Email Recipient		2nd Email Recipient	3rd Email Recipient	
	0 / 60	0 / 60		0 / 60
4th Email Recipient		5th Email Recipient		
			-	

#### 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 Stat	us	
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.	
STARTTLS	Use STARTTLS as the security method.	None
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
	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.



## NOTE

Relay Alarm Cut-off is only supported by the AWK-3252A and AWK-4252A Series.

CANCEL	APPLY
	CANCEL

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.

System	DI 2 enabled	Disabled	
System	DI 2 disabled	Disabled	
Network	LAN 1 enabled	Enabled	None
Network	LAN 1 disabled	Disabled	
Network	LAN 2 enabled	Disabled	
Network	LAN 2 disabled	Disabled	
CUT-OFF			

## 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, Wi-Fi Mirroring, and RSSI Reporting functions.



## **Channel Scan**

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

Channel Scan			
RF Band *			
ANALYZE			

Configure the following setting:

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

When finished, click **ANALYZE**.

When prompted, click **ANALYZE** again.



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

Channel Analyze	Result: 5GHz		
Channel	Number of APs	Load(%)	Noise Floor (dBm)
36 (5180 MHz)	3	2	-106
40 (5200 MHz)	0	1	-106
44 (5220 MHz)	0	1	-105
48 (5240 MHz)	0	1	-106
52 (5260 MHz)	0	1	-106
56 (5280 MHz)	0	0	-106
60 (5300 MHz)	0	0	-107
64 (5320 MHz)	0	0	-107
100 (5500 MHz)	0	1	-108

## **Wi-Fi Mirroring**

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

Wi-Fi Mi	rroriı	ng	
Mirroring Ty	pe *	•	
Mirroring Pe	riod *	min.	1

Configure the following settings.

Mirroring Type				
Setting	Description	Factory Default		
Local	Select Local to mirror traffic to the local storage on the device.			
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.	None		

#### Mirroring Period (Local Type only)

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

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

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

## **RSSI** Reporting

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

## **RSSI Reporting**

General	Authentication	1
Status *		
Disabled	•	
Recipient		
TCP/UDP Port		
514	•	
0 - 65535		
Reporting Interval *		
50		
50 - 500	ms.	
Security *		
None		

#### Status

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

#### Recipient

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

TCP/UDP Port		
Setting	Description	Factory Default
0 to 65535	Specify the designated Syslog server communication port to receive the RSSI report data on.	None

Setting	Description	Factory Default
50 to 500 ms	Specify the interval (in ms) at which RSSI report data is generated and sent to the Syslog server.	None

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

When finished, click **APPLY**.

## **System Data Collection**

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

## **Download One Key Information**

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

# **System Data Collection**

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

Configure the following settings:

Setting	Description	<b>Factory Default</b>		
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.			
TFTP	The file will be downloaded to a TFTP server.	None		
SFTP	The file will be downloaded to an SFTP server.	None		
ABC-02	The file will be downloaded to the connected ABC-02 USB.	1		
Server IP Address Setting	Description	Factory Default		
Setting	Description	Factory Default		
Setting		-		
_	Enter the IP address of the TFTP server.	None		
IP address	Enter the IP address of the TFTP server.	-		
IP address Server IP Address Setting	Enter the IP address of the TFTP server.	-		
IP address Server IP Address	Enter the IP address of the TFTP server. (for SFTP only)	None		
IP address Server IP Address Setting	Enter the IP address of the TFTP server. (for SFTP only) Description Enter the IP address of the SFTP server.	None Factory Default		
IP address Server IP Address Setting IP address	Enter the IP address of the TFTP server. (for SFTP only) Description Enter the IP address of the SFTP server.	None Factory Default None		
IP address Server IP Address Setting IP address Server Account (fo	Enter the IP address of the TFTP server. (for SFTP only) Description Enter the IP address of the SFTP server. r SFTP only)	None Factory Default		
IP address Server IP Address Setting IP address Server Account (fo Setting	Enter the IP address of the TFTP server. (for SFTP only) Description Enter the IP address of the SFTP server. r SFTP only) Description Enter the account name of the SFTP server.	None Factory Default None Factory Default		
IP address Server IP Address Setting IP address Server Account (fo Setting Account name	Enter the IP address of the TFTP server. (for SFTP only) Description Enter the IP address of the SFTP server. r SFTP only) Description Enter the account name of the SFTP server.	None Factory Default None Factory Default		

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

## **Data Collection**

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

System Data	Co	llection	
One Key Info.	D	ata Collection	
Interval *			
1 - 30	sec.		
		Stop Time	
Stop Date *		01:00 AM	
Storage Location *	-		
Select the information	on to c	collect*	
🔲 Wi-Fi Statistic			
Wi-Fi Connection			
🔲 Wi-Fi Tx/Rx			
Network			
Service			
System			
START	•		

Configure the following settings:

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	1		
Setting	Description	Factory Default	
Local	The file will be downloaded to the local storage on the AWK.		
TFTP	The file will be downloaded to a TFTP server.	None	
SFTP	The file will be downloaded to an SFTP server.		
ABC-02	The file will be downloaded to the connected ABC-02 USB.	7	

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 (fe	or SFTP only)	
Setting	Description	Factory Default
Account password	Enter the account password of the SFTP server.	None
Select the informati	ion to collect	
Setting	Description	Factory Default
Wi-Fi Statistic		
Wi-Fi Connection		
Wi-Fi Tx/Rx	Select the types of information you want to collect	None
Network	Select the types of information you want to collect.	NUTE
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.

Diagnos	tic Suppo	t	
Generate F	Profile		
<b>10</b> 1 - 180	¢ day(s)		
GENERATE			
Generated Status	Account Status		
Remaining Dura	tion		
DEACTIVA	ГЕ		

### Duration

Buración		
Setting	scription Factory Defa	
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.

Stop Method *		Rounds *
Rounds	•	3
		3 - 86400

Configure the following settings:

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 Timest	amps Method only)		
Setting	Description	Factory Default	
Setting	Specify the date when to stop pinging the IP address or	None	
Date	hostname.	None	
	hostname.	None	
Date	hostname.	Factory Default	

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

#### **Operation Mode**

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

#### Environment

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

## SSID: 2.4 GHZ

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

#### SSID

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

Channel (available in AP and Master modes only)

Setting	Description	Factory Default
· ·	Select the channel from the drop-down list. Each channel supports different frequencies.	6 (2437 MHz)

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

## SSID: 5 GHZ

SSID Status

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

### SSID

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

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

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

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

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

#### Channel (for AP and Master modes only)

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

#### Bonded Channel (for AP and Master modes only)

Setting	Description	Factory Default
14()/44/48 (read only)	The bonded channel used by the AP will be shown here if	None
	channel width is set to 36 (5180 GHz).	None

When finished, click **NEXT**.

# **Wi-Fi Security**

## AP/Master Mode

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

## Client/Client-Router/Slave Mode

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

#### SSID

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

Security		
Setting	Description	Factory Default
Open	Disable security on the SSID. This is not recommended.	
WPA	Use WPA authentication.	7
WPA2	Use WPA2 authentication. This mode supports IEEE 802.11i	7
WPAZ	with TKIP/AES + 802.1X encryption.	
WPA3	Use WPA3 authentication. This mode supports SAE	
	(Simultaneous Authentication of Equals) to avoid network	Open
	attacks, such as KRACK.	
WPA/WPA2 Mixed	Use WPA/WPA2 Mixed authentication. This allows both WPA	
WFAJ WFAZ MIXEU	and WPA2 clients to connect to the AWK.	
WPA2/WPA3 Mixed	Use WPA/WPA3 Mixed authentication. This allows both WPA2	
WFAZ/ WFAS MIXEU	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	
Disabled	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).	Dorconal
Enterprise	Use WPA, WPA2, and WPA3 with EAP security.	Personal

## 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*	Use TKIP/AES Mixed encryption. This option provides a TKIP broadcast key and TKIP+AES unicast key to support legacy AP clients. This option is rarely used and is not available when using WAP3.	TKIP/AES Mixed

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

# EAPOL VersionSettingDescriptionFactory Default1Use EAPOL Version 1 as the security authentication method.12Use EAPOL Version 2 as the security authentication method.1

#### 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 <b>Show Password</b> 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.	
TTLS	Use TTLS to validate the connection. This option requires users to also specify the Anonymous Name, Username, and Password.	TLS
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 *		
moxa-awk-3252a		
a-z, 0-9, and dash only 14 / 25	5	
Time		
Clock Source *		
Sync From Browser	-	
Time Zone *		
UTC+00:00	-	
Daylight Saving Status *		
Disabled -		
IP Configuration		
Static -	-	
IP Address *	Subnet Mask *	
192.168.0.222	24 (255.255.255.0)	Default Gateway
DNS Server 1	DNS Server 2	
_		
APPLY BACK		

## Device Name

Setting	Description	Factory Default
1 to 255 characters	<ul> <li>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:</li> <li>Only supports letters (a-z), numbers (0-9), and special character dash (-)</li> <li>Cannot contain any spaces</li> <li>Cannot start with dash (-)</li> <li>Cannot end with dash (-)</li> <li>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.</li> </ul>	Moxa-awk-3252a

#### Time

#### **Clock Source**

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

#### Time Server 1 (for Clock Source is NTP)

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

#### Time Server 2 (for Clock Source is NTP)

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

#### 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		
California	Description	Forstein Defeath

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	
DITCF	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	I DNS Server 2 (for Static mode only)		
Setting	Description	Factory Default	
Enter the primary and secondary DNS server address. After entering the DNS server's IP address, you can input the 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.



## Language

The AWK Series v2.0 firmware and above support language localization. Administrators can select the display language of the web interface from the drop-down menu. The AWK supports the following languages: English, Simplified Chinese, Traditional Chinese, and Japanese. The default is English.

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

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

# **Disable Auto Save**

NOTE

**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.

Disable Autosave mode		
Are you sure you want to disable Autosave mode?		
CANCEL	DISABLE	

## 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.

		Hi, admin 🚦
		Language
	8	Disable Auto Save
	(i)	Locator
[	Ϋ́	Reboot
	$\odot$	Reset to Defaults
	8,	Renew Device Unique Key
	***	Change Password
F	[→	Log out

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

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

## LEDs triggered:

AWK-3252A/AWK-4252A: 2.4GHz, 5GHz, SYSTEM (SYS)





AWK-1151C: WLAN, SYSTEM



## Reboot

To reboot the AWK, click Reboot.



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


## **Reset to Defaults**

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

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

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

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



#### WARNING

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

## **Renew Device Unique Key**

The AWK Series has a built-in device unique key. This unique key is used to encrypt the following sensitive information stored on the device:

- Configurations
- Certifications
- Encryption/decryption keys (for firmware decryption, diagnostic support encryption, etc.)

To improve device security, administrators can renew the device unique key from the maintenance list.

		Hi, admin 🚦
		Language
0C(	8	Disable Auto Save
-	۲	Locator
	Ü	Reboot
4	Ð	Reset to Defaults
1	8,	Renew Device Unique Key
	***	Change Password
on ss	[→	Log out



#### WARNING

When triggered, the system will take 12 to 15 seconds to renew the device unique key and will then reboot to activate the renewed device unique key. Please do not power off the device during this process.

## **Change Password**

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

		Hi, admin
		Language
	8	Disable Auto Save
	•••	Locator
	Ϋ́	Reboot
ļ	Ð	Reset to Defaults
l	8,	Renew Device Unique Key
	***	Change Password
II F	$[\rightarrow$	Log out

Configure the following settings:

Change Password			
Current Password *	ø		
At least 4 characters	0 / 63		
New Password *	Ø		
At least 4 characters	0 / 63		
Confirm Password *	Ø		
At least 4 characters	0 / 63		
		CANCEL	APPLY

#### Current Password

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.

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

# A. Supporting Information

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

# **Device Recovery**

In event the device is not working properly, including configuration changes not applying, the first troubleshooting action is to perform a power cycle. This is done by removing and reconnecting the power and verifying if the situation is resolved.

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

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



#### NOTE

The admin password is required to authorize the FailSafe function.

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

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



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



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



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

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.

μ

#### 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.

😼 PComm Terminal Emulator				—	$\times$
Profile	Port Manager	Help	-		
<b>a</b>	Open	Ctrl+Alt+O	2B HEX		

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

Property	×	Property ×
Communication Parameter Termina	I File Transfer Capturing	Communication Parameter Terminal   File Transfer   Capturing
Protocol: Serial	•	Terminal type: VT100
Baud rate:	115200 👻	Size: 80 X 25 (col x row)
	🖂 User defined	History depth: 25 (unit: row)
Data bits:	8 🗸	Transmit
Parity:	None	🗖 Local echo
Stop bits:	1	Send 'Enter' key as:
Flow control:	RTS/CTS	
	T XON/XOFF	CR translation: No Changed 💌
RTS state:	ON OFF	LF translation: No Changed 👻
DTR state:	○ ON ○ OFF	
		✓ Enable auto line wrap

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

Normal Emulator - COM1,115200,None,8,1,VT100	-	×
Pro <u>f</u> ile <u>E</u> dit <u>P</u> ort Manager <u>W</u> indow <u>H</u> elp		
B COM1,115200,None,8,1,VT100		
TR RTS moxa-awk-3252a login:	^	
	~	
C	>	
State: OPEN CTS DSR RT DCD Ready TX:0 RX:28	lie	

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.

聲 PComm Terminal Emulator - COM1,115200,None,8,1,VT100	-		×
Profile <u>E</u> dit <u>P</u> ort Manager <u>W</u> indow <u>H</u> elp			
GM1,115200,None,8,1,VT100	- • •		
Welcome [admin]		^	
The lastest successful login time via CLI was: 2021-12-03 10:57:46+00:00			
moxa-awk-3252a#			
		~	
State: OPEN CTS DSR RI DCD Ready TX:11 RX:157		//.	



#### NOTE

To modify the appearance of the PComm Terminal Emulator window, select **Edit > Font** and then choose the desired formatting options.



#### ATTENTION

If you unplug the RS-232 cable or trigger **DTR**, you will be disconnected and logged out for network security reasons. You will need to log in again to resume operations.

# **Configuration by Telnet and SSH Consoles**

You can use a Telnet or SSH client to access the 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.

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

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

🔀 PuTTY Configuration		×
Category:		
l⊟- Session	Basic options for your PuTTY s	ession
Logging - Terminal	Specify the destination you want to connect	to
- Keyboard	Host <u>N</u> ame (or IP address)	<u>P</u> ort
Bell	192.168.127.253	22
└── Features □- Window └── Appearance	Connection type: C_ <u>B</u> aw C_ <u>T</u> elnet C_Rlogin ● <u>S</u> §	SH O Serial

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

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

# Installation

## **Physical Installation**

- 1. To comply with IEC 62443 requirements, the AWK Series device MUST be installed within an accesscontrolled area, where only authorized personnel have physical access to the AWK Series device.
- 2. To comply with IEC 62443 requirements, the device MUST NOT be directly connected to the Internet, which means the AWK Series device MUST be installed within a security perimeter with firewall. Additionally, the various application service servers such as DHCP, NTP, RADIUS, ... etc. shall be securely configured with proper authentication within the security perimeter with firewall protection as illustrated in the image below:



- 3. Always configure the AWK Series device to comply with your organization's network and security requirements before physical installation. Do not physically install devices that are unconfigured or have an unknown configuration state to avoid unnecessary risks. Please follow the instructions in the Quick Installation Guide, which is included in the package, to ensure you install the device correctly in your environment.
- 4. The AWK Series has anti-tamper labels visible on the enclosures covering assembly screws. Any tampering to open the mechanical enclosure to access electrical circuit boards will result in the fracturing of anti-tamper labels. This allows an administrator to immediately tell if the device's hardware integrity has been compromised.
- 5. Ports that are not in use should be deactivated. Please refer to <u>Hardware Interface</u> and <u>Ports</u> to review the status of each I/O port and disable any unused ports.
- 6. The AWK Series devices are industrial WLAN infrastructure components serving as the underlying fabric to support automation processes. These devices are not an integral part of process automation logic and therefore do not support nor are they suitable for any deterministic process control outputs.

## Account Management

Follow these best practices when setting up an account:

- Each account should be assigned the correct privileges: Only allow the minimum number of people to have admin privilege so they can perform device configuration or modifications, while other users should only have the minimum required access privilege needed to fulfill their corresponding role. The AWK Series supports both local account authentication and remote centralized authentication mechanisms such as RADIUS.
- 2. Password protection has two means of enforcement: Password Lifetime and Password Complexity. We recommend to:
  - a. Review whether the password lifetime needs to be adjusted according to your organization's policies.
  - b. Review whether the configured password complexity options enabled on the AWK Series system (refer to <u>Create a New Account</u>) is sufficient according to your organization's policies. If not, modify the password complexity requirements to meet your organization's security guidelines.
- 3. Enforce regulations that ensure only trusted hosts can access the device. Refer to the <u>Trusted Access</u> section for more information and instructions.

## **Vulnerable Protocols**

 For network security reasons, we strongly recommend that you change the default port numbers, such as the TCP port number for HTTP, HTTPS, Telnet, and SSH, for protocols that are in use. Ports that are not in use but are still accessible, pose a security risk and should be disabled. Refer to the <u>Management</u> <u>Interface</u> section for more information and instructions.

Below is the list of default port numbers for each protocol used by all external interfaces.

Browser	Protocol Type	Default Port
TCD	HTTP	80
	HTTPS	443
ТСР	Telnet	23
	SSH	22
UDP	SNMP	161
Moxa Service		40404

- In order to avoid malicious actors from snooping confidential information, users should always apply encryption-based communication protocols such as HTTPS instead of HTTP, SSH instead of Telnet, SFTP instead of TFTP, SNMPv3 instead of SNMPv1/v2c etc. In addition, the maximum number of sessions should be kept to an absolute minimum. Refer to the <u>Management Interface</u> section for more information and instructions.
- 3. Users should generate the SSL certificate for the device before commissioning HTTPS or SSH applications. Please refer to the <u>Certificate Management</u> section for more information and instructions.
- 4. The HTTP, SNMPv1v2, and Telnet protocols are insecure and by default DISABLED. We recommend to always use secure alternatives such as HTTPS, SNMPv3, or SSL to protect your communications. If unsecure protocols need to be used with legacy devices, please consult a qualified security expert to evaluate and implement additional protection measures to prevent any potential security risks.
- 5. In order to ensure that the device configurations are adequately protected prior to deployment, it is recommended to review the security status of the device. Refer to the <u>Security Status</u> section for an overview of the device's current security conditions. If any of the identified risks require mitigating action, navigate to the corresponding setup page to address the issue, or consult a qualified security expert to evaluate and implement additional protection measures to prevent any potential security risks.

# Operation

1. The AWK Series supports the TLS v1.2 cryptographic algorithm to protect your HTTPS/SSH applications. Please ensure that your web browser is updated to a version that supports TLS v1.2:

Browser	Version
Microsoft Edge	All versions
Mozilla Firefox	V11 and above
Chrome	V38 and above
Apple Safari	V7 and above for OS X 10,9 (Mavericks) and above

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

- 2. The device supports event logs and syslog for SIEM integration:
  - a. Event log: Due to limited storage capacity, the event log can only accommodate a maximum of 10,000 entries. Administrators can set a warning for a pre-defined threshold. We recommend that users regularly back up system event logs. Please refer to the <u>Event Log</u> section for more information and instructions.
  - b. Syslog: The device supports syslog and advanced secure TLS-based syslog for centralized SIEM integration. Please refer to the <u>Syslog</u> section for more information and instructions.
- 3. The device can provide information for control system inventory:
  - a. SNMPv1, v2c, v3: We recommend administrators use SNMPv3 with authentication and encryption to manage the network. Please refer to the MIB file for the detailed OID structure.
  - b. Telnet/SSH: We recommend that administrators use SSH with authentication and encryption to retrieve device properties.
  - c. HTTP/HTTPS: We recommend that administrators use HTTPS with an internally renewed certificate or imported certificate that has been issued by a Certificate Authority (CA) to configure the device.
- 4. Denial of Service protection: We recommend enabling Trusted Access, Wi-Fi ACL, L2/L3 firewalls to mitigate the risk of DoS attack attempts.
- Periodically regenerate the SSH and SSL certificates: Even though the device supports up-to-date cipher suites to ensure sufficient complexity, we strongly recommend users to frequently renew their SSH key and SSL certificate in case the key is compromised. Please refer to the <u>Certificate Management</u> section for more information and instructions.

# Maintenance

- 1. Perform firmware upgrades frequently to enhance features, deploy security patches, or fix bugs. Periodically check the official product website or Moxa security advisory updates at https://www.moxa.com/en/support/product-support/security-advisory/security-advisories-all.
- Periodically, or after each maintenance session, back up the running system configuration to be able to restore the device back to the latest stable, secure state if necessary. The device supports password encryption and signature authentication for backup files to protect the system configuration files from being tampered with,
- 3. Examine event logs frequently to detect any anomalies.
- 4. Periodically, or after each maintenance session, check the <u>Security Status</u> overview to review and confirm the current device's security conditions.
- 5. To report vulnerabilities of Moxa products, please submit your findings on the following web page: <a href="https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability">https://www.moxa.com/en/support/product-support/security-advisory/report-a-vulnerability</a>.

## ATTENTION

**For AWK-1151C models**: Due to a console port hardware limitation on AWK-1151C models, disconnecting the console cable **WILL NOT** immediately auto-logout an active CLI session but rather auto-logout once the active session times out. To prevent exposure risks on the AWK-1151C's console connections, always log out each CLI session before disconnecting the console cable.

# Decommission

- 1. Power off the device to be decommissioned and unmount it from its physical installation location.
- 2. Identify the serial number or device name and locate (if applicable) any configuration backup files or certificates generated by the device to be decommissioned and ensure the deletion of these files.

3. To avoid any sensitive information such as the organization's information, account passwords, or certificates from being leaked, always reset the device to the factory default settings before decommissioning the device.

This appendix lists the required authority for each feature or service. The purpose of this table is to help administrators review and decide the appropriate account privileges and role to assign to user accounts.

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

Configuration Section	Authority Required
Device Summary	Status Monitoring
System	
System Management	
System Information	System Management
Firmware Upgrade	System Management
Configuration Backup and Restore	System Backup
Account Management	
User Account	(Refer to breakdown below)
Settings	Account System
Session Management	System Management
Password Policy	Account System
Management Interface	
User Interface	System Management
Hardware Interface	System Management
SNMP	(Refer to breakdown below)
SNMP	System Management
SNMP Account List	Account System
Time	
System Time	System Management
Wi-Fi	
Wireless Settings	(Refer to breakdown below)
General	Network
MAC Cloning	Network
Status	Status Monitoring
Connection Management	Network
Roaming	Network
Wi-Fi Security	Network
Ports	
Port Settings	(Refer to breakdown below)
General	Network
Port Status	Status Monitoring
Layer 2 Switching	
VLAN	Network
IP Configuration	
General	System Management
Status	Status Monitoring
Network Service	
DHCP Server	Network

Configuration Section	Authority Required
Routing and Nat	
Routing	
Unicast Route	
Static Route	Network
	Status Monitoring
Routing Table	
NAT	
Rule List	Network
Firewall	
Layer 2 Policy	Network
Layer 3 Policy	Network
Certificate Management	System Management, Auditor System, System Backup, Status Monitoring, Diagnostics, Advanced Diagnostic, or Network Configuration
Security	
Device Security	
Login Policy	System Management
Trusted Access	System Management
Diagnostics	
Security Status	Status Monitoring
Network Status	
Network Statistics	Status Monitoring
LLDP	(Refer to breakdown below)
Settings	Network
Status	Status Monitoring
Bridge Table	Status Monitoring
ARP Table	Status Monitoring
Event Logs and Notifications	
Event Log	(Refer to breakdown below)
Log List	Status Monitoring
Registered Logs	Auditor System
Oversize Action	
	Auditor System
Backup Event Notifications	Status Monitoring
	Auditor System
Syslog	Auditor System
General	Auditor System
Authentication	Auditor System
SNMP Trap/Inform	Auditor System
General	Auditor System
SNMP Trap/Inform Account	Auditor System
Email Settings	Auditor System
General	Auditor System
Authentication	Auditor System
Relay Alarm Cut-off	Auditor System
Tools	
Wi-Fi Tools	
Channel Scan	Advanced Diagnostic
Wi-Fi Mirroring	Diagnostic
General	Diagnostic
Authentication	Diagnostic
RSSI Reporting	Diagnostic
System Data Collection	Diagnostic
Diagnostic Support	Advanced Diagnostic
Ping	Diagnostic
Setup Wizard	Network and System Management
Maintenance Bar	· · · · · · · · · · · · · · · · · · ·
Language	Basic
Disable/Disable Auto Save	System Management
Locator	Diagnostic
	Biagriobuc

Configuration Section	Authority Required
Reboot	System Management
Reset Device	System Management
Renew Device Unique Key	System Management
Change Password	Basic
Log Out	Basic