AirWorks AWK-4131A User's Manual

Version 9.1, November 2020

www.moxa.com/product

© 2020 Moxa Inc. All rights reserved.

AirWorks AWK-4131A User's 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

© 2020 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

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

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

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

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

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

Table of Contents

1. Introduction 1-1
- Overview 1-2
- Package Checklist 1-2
- Product Features 1-2
- Functional Design 1-3
  - LED Indicators 1-3
  - Beeper 1-4
  - Reset Button 1-4
  - Relay (Digital Output) 1-5

2. Getting Started 2-1
- First-time Installation and Configuration 2-2
- Communication Testing 2-3
- Function Guide 2-4

3. Web Console Configuration 3-1
- Configuration by Web Browser 3-2
- Overview 3-4
- Quick Setup 3-6
- General Setup 3-8
  - System Information 3-8
  - Interface On/Off 3-9
  - Network Settings 3-10
  - System Time 3-12
- Wireless LAN Setup 3-13
  - AeroMag 3-14
  - Operation Mode 3-19
  - Basic WLAN Setup 3-20
  - WLAN Security Settings 3-25
  - Advanced WLAN Settings 3-32
  - WLAN Certificate Settings (for EAP-TLS in Client/Client-router/Slave mode only) 3-37
- Advanced Setup 3-38
- Using Virtual LAN 3-38
  - The Virtual LAN (VLAN) Concept 3-38
  - Configuring Virtual LAN 3-39
  - DHCP Server (for AP/Client-router mode only) 3-40
  - Packet Filters 3-42
  - RSTP Settings (Master/Slave mode only) 3-45
  - Static Route (Client-Router mode only) 3-46
  - NAT Settings/Port Forwarding (for Client-router mode only) 3-47
  - SNMP Agent 3-50
  - Link Fault Pass-through (Client/Slave mode only) 3-52
- Logs and Notifications 3-52
  - System Logs 3-52
  - Syslog 3-54
  - E-mail Notifications 3-55
  - Relay 3-56
  - Trap 3-56
- Status 3-58
  - Wireless LAN Status 3-58
  - Associated Client List (for AP/Master mode only) 3-58
  - DHCP Client List (for AP mode only) 3-59
  - System Logs 3-60
  - Relay Status 3-60
  - DI and Power Status 3-61
  - AeroLink Protection Status (Client/Slave mode only) 3-61
  - System Status 3-62
  - Network Status 3-62
- Maintenance 3-63
  - Console Settings 3-63
  - Ping 3-64
  - Firmware Upgrade 3-64
  - Configuration Import and Export 3-65
  - Load Factory Default 3-67
  - Account Settings 3-67
  - Misc. Settings 3-68
  - Changing the Password 3-69
  - Troubleshooting 3-69
- Save Configuration 3-72
- Restart 3-73

Logout 3-74
4. Software Installation/Configuration 4-1
Overview 4-2
Wireless Search Utility 4-2
Installing Wireless Search Utility 4-2
Configuring Wireless Search Utility 4-5
5. Other Console Configurations 5-1
RS-232 Console Configuration (115200, None, 8, 1, VT100) 5-2
Configuration by Telnet and SSH Consoles 5-3
Configuration by Web Browser with HTTPS/SSL 5-4
Disabling Telnet and Browser Access 5-5
A. References A-1
AeroLink Protection A-2
Wireless Distribution System (WDS) A-3
Beacon A-4
DTIM A-5
Fragment A-5
RTS Threshold A-5
STP and RSTP A-5
The STP/RSTP Concept A-5
Differences between RSTP and STP A-5
B. Supporting Information B-1
About This User's Manual B-2
Firmware Recovery B-3
DoC (Declaration of Conformity) B-4
Federal Communication Commission Interference Statement B-4
RED Compliance Statement B-5

1

Introduction

The AWK-4131A industrial a/b/g/n high-speed wireless access point (AP) products are ideal wireless solutions for hard-to-wire applications that use mobile equipment connected over a TCP/IP network. The AWK-4131A is rated to operate at temperatures ranging from -40 to 75°C and is rugged enough for any harsh industrial environment.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Functional Design**
  - LED Indicators
  - Beeper
  - Reset Button
  - Relay (Digital Output)

Overview

The AWK-4131A outdoor wireless access point is an ideal solution for industrial applications that are hard to wire, too expensive to wire, or use mobile equipment that connect to a TCP/IP network. The AWK-4131A is rated to operate at temperatures ranging from -40 to 75°C, and its dust-tight and weatherproof design is IP68-rated. An IP68 rating means that the device is completely protected from the ingress of dust and is protected against the effects of immersion in water at depths of 15 cm and 1 m. You can use the AWK-4131A to set up a WLAN or extend existing wired networks to outdoor locations and still maintain a reliable connection. The AWK-4131A has two redundant DC power inputs for increased reliability, can be powered via PoE, and is easy to deploy.

Package Checklist

Moxa's AWK-4131A is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- AWK-4131A wireless AP/bridge/client
- 2 2.4/5 GHz antennas: ANT-WDB-ANM-0306
- Wall mounting kit (includes 2 supports)
- Field-installable power plug
- Field-installable RJ45 plug (LAN)
- Metal cap to cover RJ45 connector (RS-232 Console)
- Metal cap to cover M12 female connector
- Transparent plastic sticks for field-installable plugs
- Quick installation guide (printed)
- Warranty card

NOTE The above items come with the AWK-4131A standard version. The package contents may vary in different customized versions.

Product Features

- IEEE802.11a/b/g/n compliant
- Advanced wireless security:
  - 64-bit and 128-bit WEP/WPA/WPA2 encryption
  - SSID Hiding/IEEE 802.1X/RADIUS
  - Packet access control and filtering
- STP/RSTP support for network system redundancy (master and slave mode only)
- Long-distance transmission support (5 GHz channel only)
- Turbo Roaming enables rapid handover (Client/Client-Router/Slave mode)
- ABC-01 for configuration import/export
- Selectable antenna output
- RS-232 console management
- 2DI + 1DO for on-site monitoring and warnings
- Wide -40 to 75°C operating temperature range (-T model)
- Redundant 12 to 48 VDC power inputs or IEEE 802.3af Power over Ethernet
- DIN-rail or wall mounting ability
- IP68-rated metal housing
- Waterproof RJ45 connectors and M12 connectors

NOTE The latest specifications for Moxa's products can be found at https://www.moxa.com.

ATTENTION

- The AWK-4131A is NOT a portable mobile device and should be located at least 20 cm away from the human body.
- The AWK-4131A is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of these units, and to establish a wireless network.

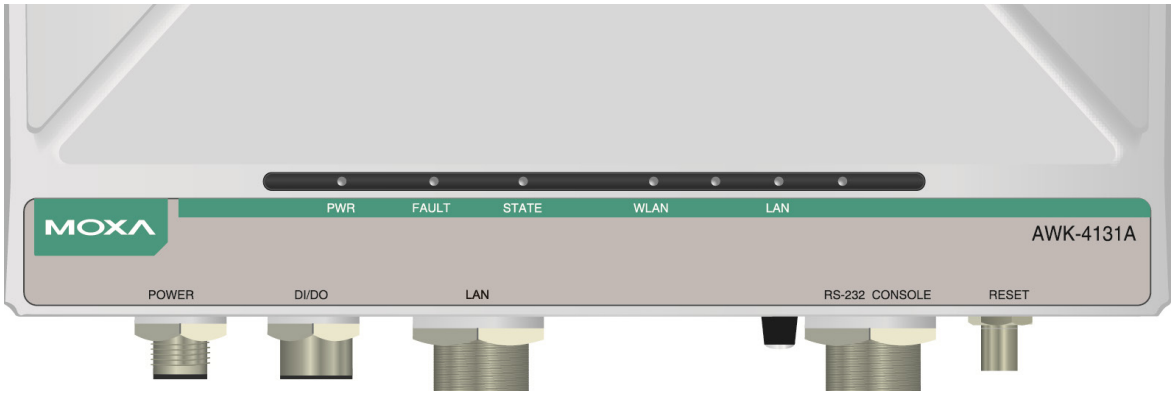
Patent http://www.moxa.com/doc/operations/Moxa_Patent_Marking.pdf

Functional Design

LED Indicators

The LEDs on the front panel of AWK-4131A allow you to identity the status and wireless settings quickly.

The LED for **FAULT** indicates the system failure and user-configured events. If the AWK-4131A cannot retrieve the IP address from a DHCP server, the **FAULT** LED will blink at an interval of one second.



The following table is a summary for the wireless settings and LED displays. You can check the status of the AWK-4131A by reading these LEDs. More information about "Basic Wireless Settings" is presented in Chapter 3.

LED	Color	State	Description
Front Panel LED Indicators (System)			
PWR	Green	On	Power is being supplied (from power input 1 or 2, or PoE)
		Off	Power is **not** being supplied
FAULT	Red	Blinking (slow at 1-sec intervals)	Cannot get an IP address from the DHCP server
		Blinking (fast at 0.5-sec intervals)	IP address conflict
		Off	No error condition exist
STATE	Green	On	System startup is complete and the system is in operation
		Blinking (slow at 1-second intervals)	Device has been located by the Wireless Utility
		Blinking (fast at 0.5-second intervals)	AeroLink Protection is enabled and is currently in "Backup" state
	Red	On	System is booting up

LED	Color	State	Description
WLAN	Green	On	WLAN function is in Client/Client-Router/Slave mode
		Blinking	WLAN's data communication is in Client/Client-Router/Slave mode
		Off	WLAN is not in operation
	Amber	On	WLAN function is in AP/Master mode
		Blinking	WLAN's data communication is in AP/Master mode
		Off	WLAN is not in operation
LAN	Green	On	LAN port's 1000 Mbps link is **active**
		Blinking	Data is being transmitted at 1000 Mbps
		Off	LAN port's 1000 Mbps link is **inactive**
	Amber	On	LAN port's 10/100 Mbps link is **active**
		Blinking	Data is being transmitted at 10/100 Mbps
		Off	LAN port's 10/100 Mbps link is **inactive**

ATTENTION

When the LEDs for STATE (Green), FAULT, and WLAN all light up simultaneously and blink at one-second intervals, it means the system failed to boot. This may be due to improper operation or issues such as an unexpected shutdown during firmware update. To recover the firmware, refer to "Firmware Recovery" in Chapter 6.

Beeper

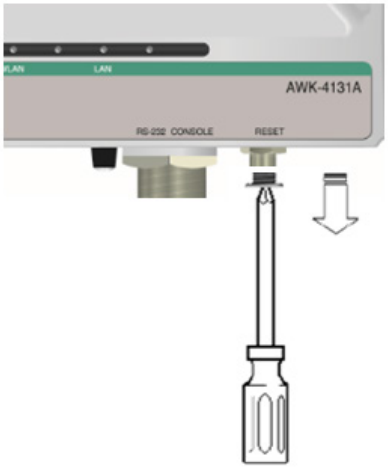
The beeper signals that the system is ready with two short beeps.

Reset Button

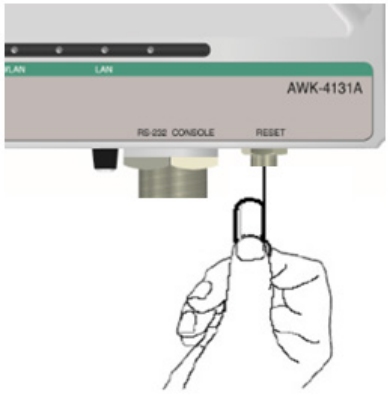
The **RESET** button is located on the bottom panel of the AWK-4131A. You can reboot the AWK-4131A or reset it to factory default settings by pressing the **RESET** button with a pointed object such as an unfolded paper clip.

- **System reboot:** Hold the RESET button down for under 5 seconds and then release.
- **Reset to factory default:** Hold the RESET button down for over 5 seconds until the **STATE** LED starts blinking green. Release the button to reset the AWK-4131A.

STEP 1:
Remove the reset button cover.



STEP 2:
Using a pointed object, press and hold the reset button.



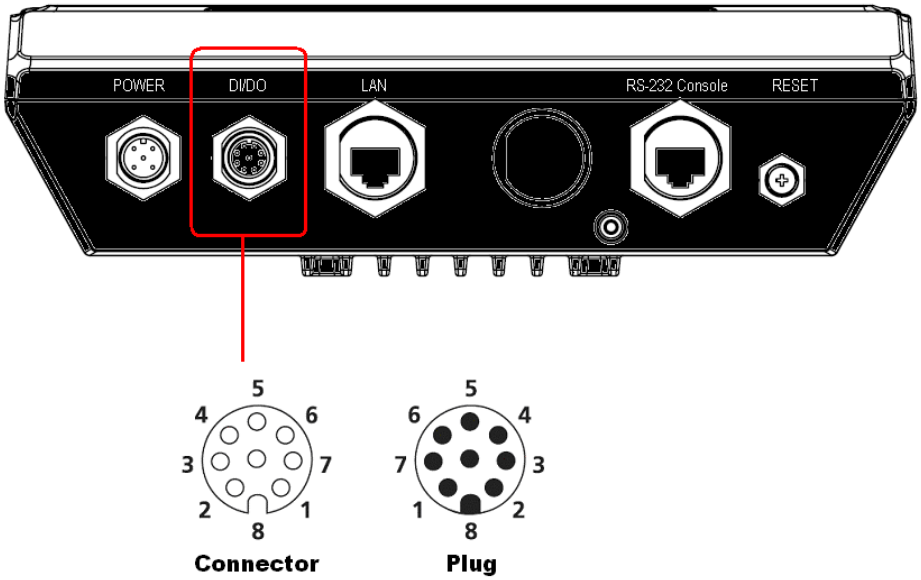
Relay (Digital Output)

The AWK-4131A has one relay output, which consists of the 2 contacts for the 8-pin M12 connector on the bottom panel, as shown below. These relay contacts forward system failure 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 reason, the relay circuit is kept open when the AWK-4131A is not powered.

The AWK-4131A's relay status is summarized as follows:

Power Status	Event	Relay
Off	–	Open
On	Yes	Open
	No	Short



Digital Inputs and Relay-out Pin Assignment (8-pin M12 connector)

PIN	1	2	3	4	5	6	7	8
Function	DOUT_I	DOUT_O	DI0+	DI0-	DI1+	DI1-	reserved	reserved

2

Getting Started

This chapter explains how to install Moxa's AirWorks AWK-4131A for the first time, quickly set up your wireless network, and test whether the connection is running well. With the function guide, you can easily locate the functions you need.

The following topics are covered in this chapter:

- **First-time Installation and Configuration**
- **Communication Testing**
- **Function Guide**

First-time Installation and Configuration

Before installing the AWK-4131A, make sure all items in the Package Checklist are in the box. In addition, you will need access to a notebook computer or PC equipped with an Ethernet port. The AWK-4131A has a default IP address that you must use when connecting to the device for the first time.

Step 1: Select the power source.

The AWK-4131A can be powered by DC power input or PoE (Power over Ethernet). The AWK-4131A will use whichever power source you choose.

Step 2: Connect the AWK-4131A to a notebook or PC.

Since the AWK-4131A supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the AWK-4131A to a computer. If the LED indicator on AWK-4131A's LAN port lights up, it means the connection is established.

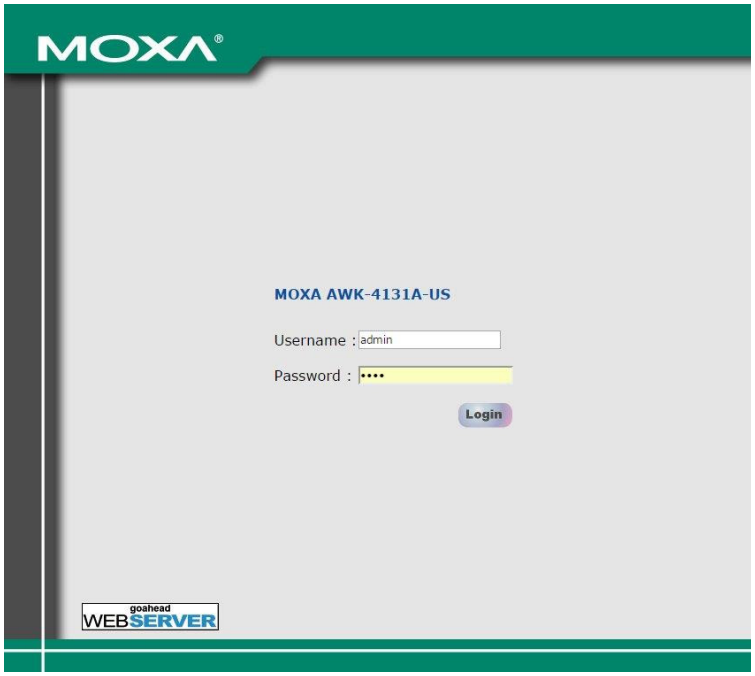
Step 3: Set up the computer's IP address.

Set an IP address on the same subnet as the AWK-4131A. Since the AWK-4131A's 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**.

NOTE After you select **Maintenance→ Load Factory Default** and click the **Submit** button, the AWK-4131A will be reset to factory default settings and the IP address will be also reset to **192.168.127.253**.

Step 4: Use the web-based manager to configure AWK-4131A

Open your computer's web browser and type http://192.168.127.253 in the address field to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the user name and password as shown in the following figure. For first-time configuration, enter the default user name and password and then click on the **Login** button:



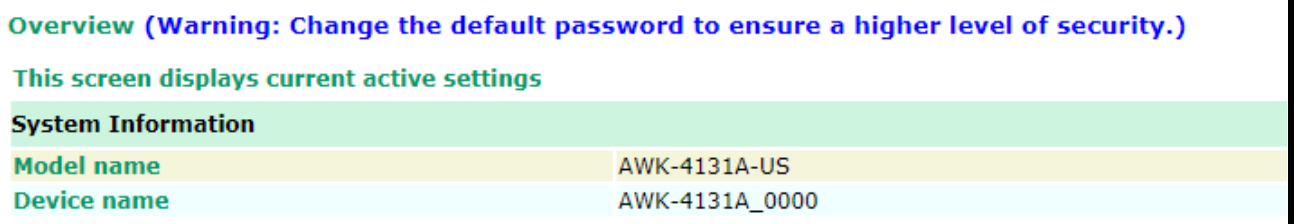
NOTE Default user name and password:

User Name: **admin**

Password: **moxa** (starting with firmware version 1.4)

root (up to firmware version 1.3)

For security reasons, we strongly recommend changing the default password. To do so, select **Maintenance** > **Password**, and then follow the on-screen instructions to change the password.



NOTE Clicking **Submit** will apply your changes and refresh the web page. The string "**(Updated)**" and a blinking reminder will appear on the upper-right corner of web page as shown below:

To make the changes effective, click **Restart** and then **Save and Restart** after you change the settings. It will take about 30 seconds for the AWK-4131A to restart.

Step 5: Select the operation mode for the AWK-4131A.

By default, the AWK-4131A's operation mode is set to AP. If you would like to use the Client mode, you can change the setting at **Wireless LAN Setup --> WLAN --> Basic WLAN Setup**. Detailed information about configuring the AWK-4131A's operation can be found in Chapter 3.

Step 6: Test the connection.

In the following sections, we describe two test methods that can be used to ensure that a network connection has been established.

Communication Testing

After installation, you can run a sample test to make sure the AWK-4131A and wireless connection are functioning normally. Two testing methods are explained in the following sections. Use the first method if you are using only one AWK-4131A device, and use the second method if you are using two or more AWK-4131A units.

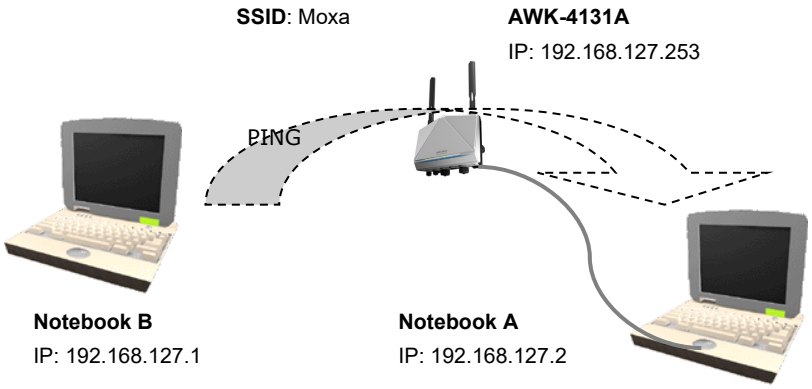
Testing Method for one AWK-4131A

If you are only using one AWK-4131A, you will need a second notebook computer equipped with a WLAN card. Configure the WLAN card to connect to the AWK-4131A (default SSID is **MOXA**), and change the IP address of the second notebook B so that it is on the same subnet as the first notebook A, which is connected to the AWK-4131A.

After configuring the WLAN card, establish a wireless connection with the AWK-4131A and open a DOS window on notebook B. At the prompt, type

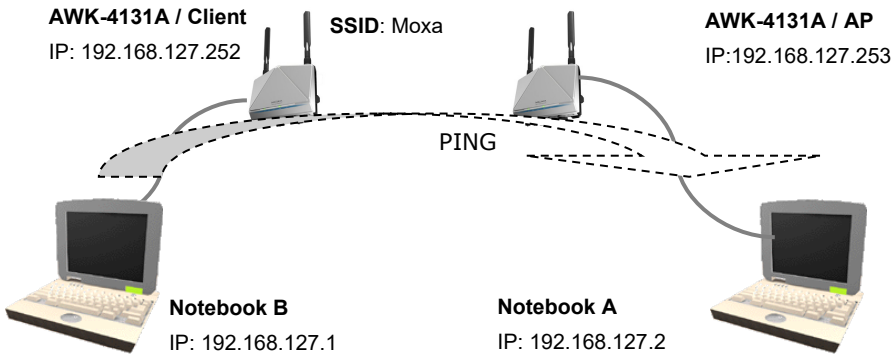
ping *<IP address of notebook A>*

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.



Testing Method for two or more AWK-4131As

If you have two or more AWK-4131As, you will need a second notebook B equipped with an Ethernet port. Use the default settings for the first AWK-4131A connected to notebook A and change the second or third AWK-4131A connected to notebook B to Client mode. Then, configure the notebooks and AWK-4131As properly.



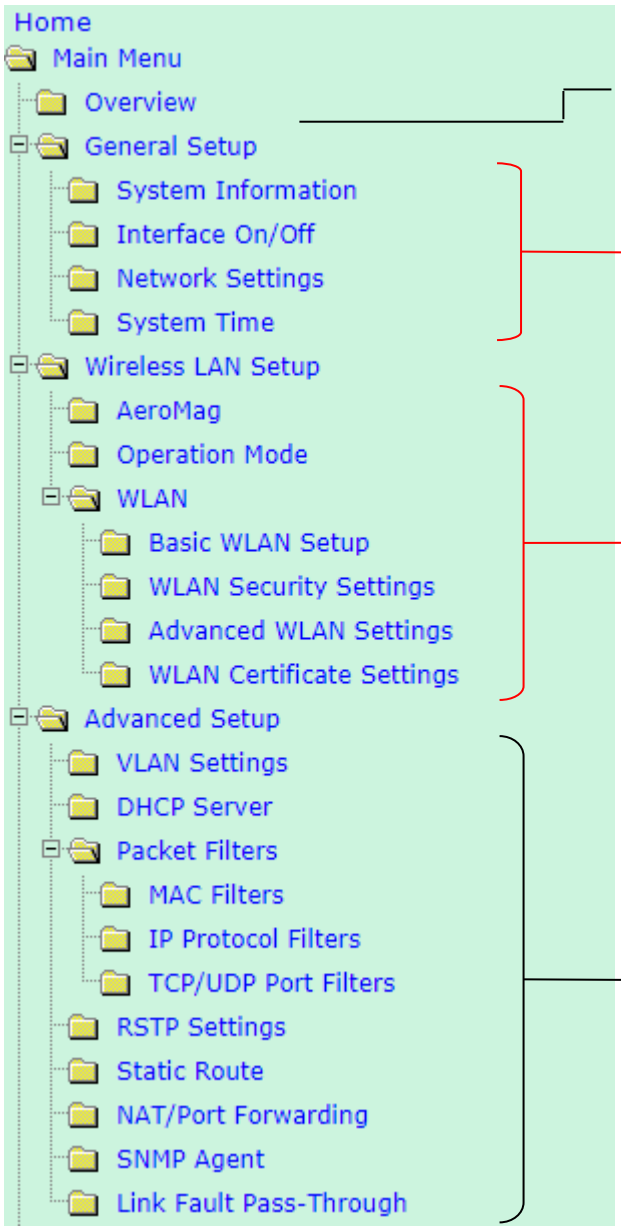
After setting up the testing environment, open a DOS window on notebook B. At the prompt, type

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.

Function Guide

The management functions are categorized in a tree and shown in the left field of the web-based management console. You can efficiently locate the function you need with the following guide.



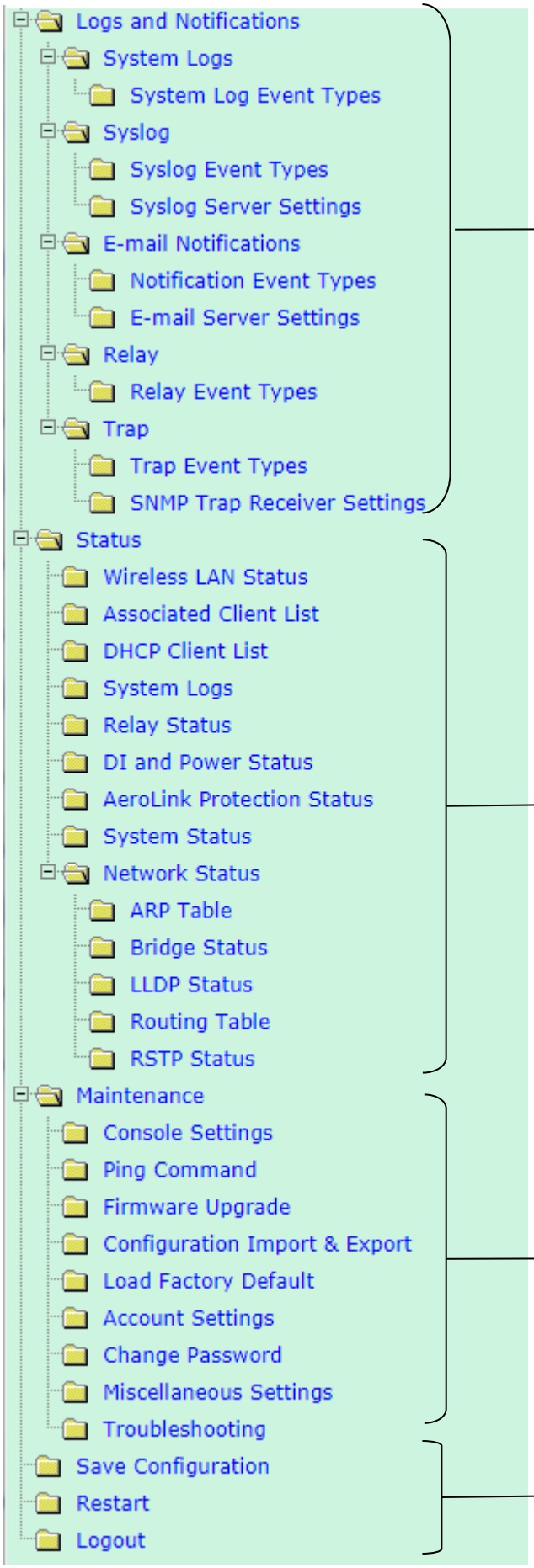
Quick overview of the AWK-4131A's status

General Setup for administering the AWK-4131A

Essential settings related to establishing a wireless network

Advanced features to support additional network management and secure wired and wireless communication

NOTE: These advanced functions are all optional.



Application-oriented device management functions to set up events, traps, and reactions via relay warning, e-mail, and SNMP notification
NOTE: These functions are all optional.

Current status information for monitoring wired/wireless network performance, advanced services, and device management functions.

Functions for maintaining the AWK-4131A, and for diagnosing the network.

On-demand functions to support the web-based console management operation.

3

Web Console Configuration

In this chapter, we will explain each web management page of the web-based console configuration. Moxa's easy-to-use management functions will help you set up your AWK-4131A, as well as establish and maintain your wireless network easily.

The following topics are covered in this chapter:

- **Configuration by Web Browser**
- **Overview**
- **General Setup**
  - System Information
  - Network Settings
  - System Time
- **Wireless LAN Setup**
  - Operation Mode
  - Basic WLAN Setup
  - WLAN Security Settings
  - Advanced WLAN Settings

Configuration by Web Browser

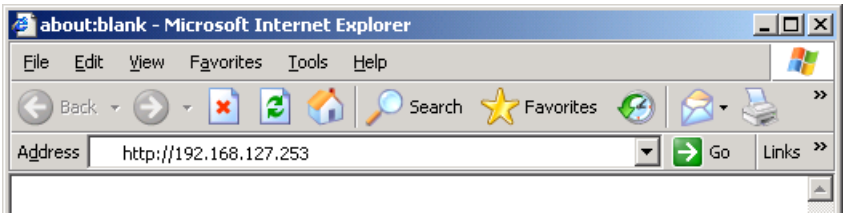
Moxa AWK-4131A's web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 or 8.0 with JVM (Java Virtual Machine) installed.

NOTE To use the AWK-4131A's management and monitoring functions from a PC host connected to the same LAN as the AWK-4131A, you must make sure that the PC host and AWK-4131A are on the same logical subnet. Similarly, if the AWK-4131A is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

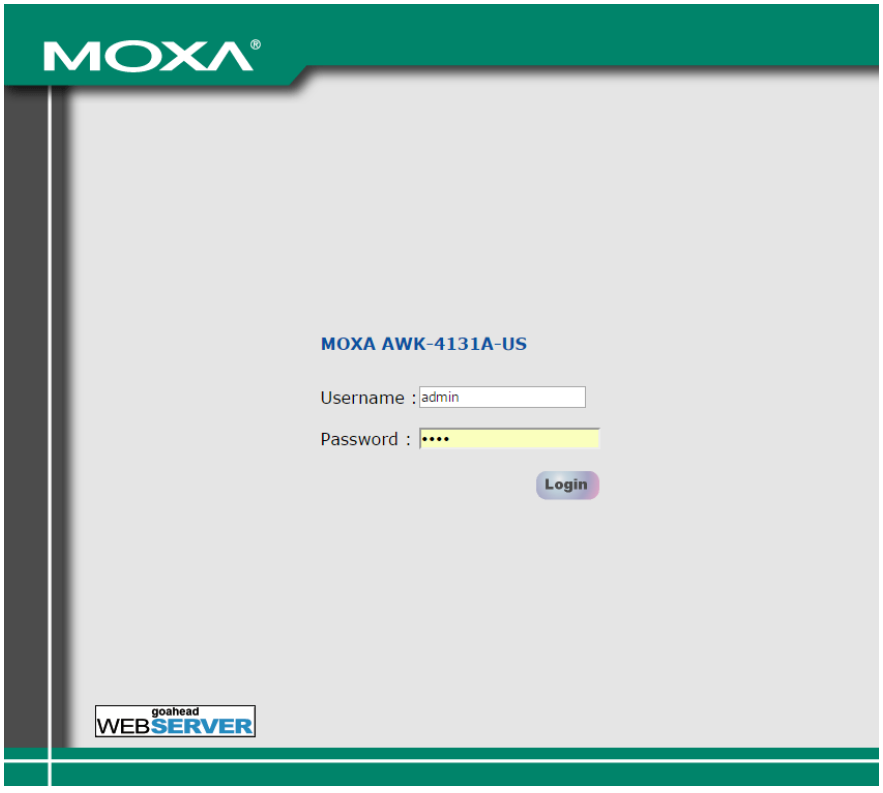
The Moxa AWK-4131A's default IP address is **192.168.127.253**.

Follow the steps below to access the AWK-4131A's web-based console management.

1. Open your web browser (ex. Internet Explorer) and type the AWK-4131A's IP address in the address field. Press **Enter** to establish the connection.



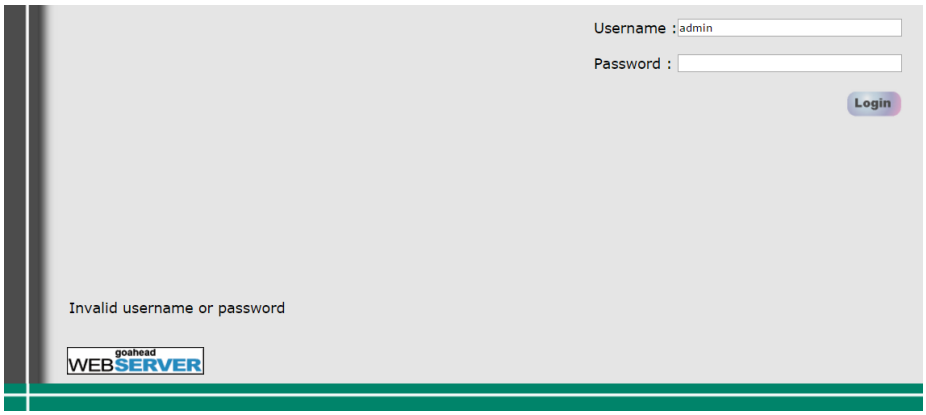
2. The Web Console Login **page** will open. Enter the password (User Name is set as **admin**; the default password is **moxa** if a new password has not been set.) and then click **Login** to continue.

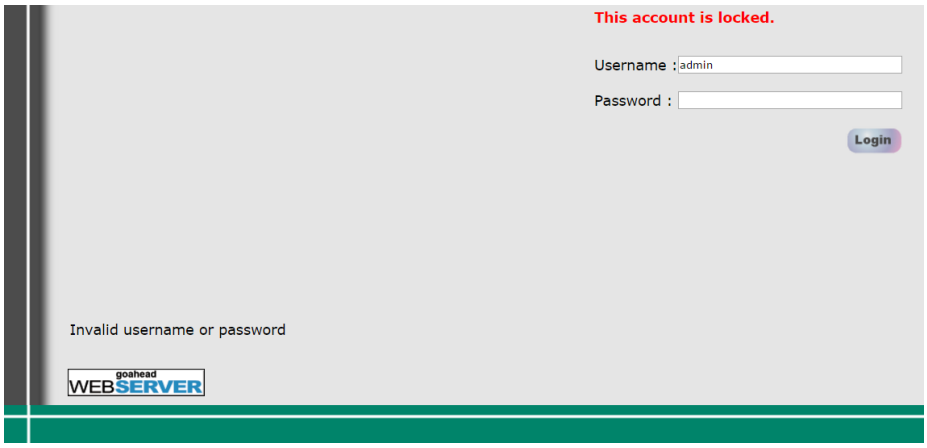


You may need to wait a few moments for the web page to download onto your computer. Please note that the model name and IP address of your AWK-4131A are both shown in the title of the web page. This information can help you identify multiple AWK-4131A units.

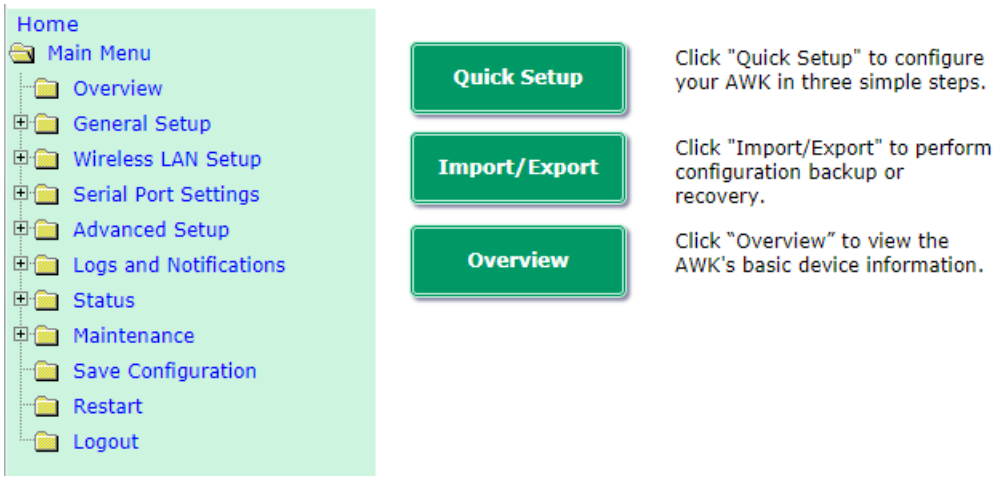
If an incorrect username or password is entered, a warning message is displayed. The system will lock the user account based on the settings configured in the **Maintenance → Account Settings** page. The default retry count is 5 times and the default lockout time is 600 seconds.

Once an account is locked, the user will have to wait out the duration of the lockout period before retrying.

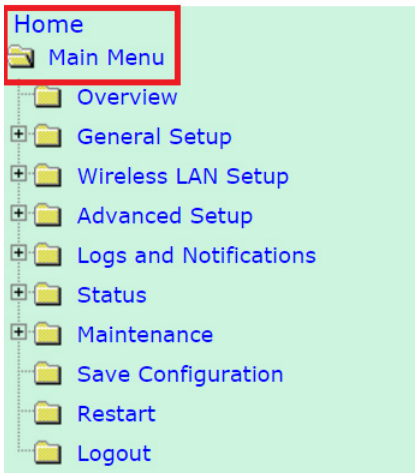




3. Use the **Quick Setup** function on the homepage to quickly set up the AWK or click on the **Overview** button to see the basic device settings. The **Import/Export** function helps you back up the system or to perform a system recovery from an existing backup.



4. Click on the **Home** link to go back to the main page.
   Use the menu tree on the left side of the browser to open the AWK-4131A functions.



In the following paragraphs, we describe each AWK-4131A management function in detail. A quick overview is available in this manual in the "Function Map" section of Chapter 3.

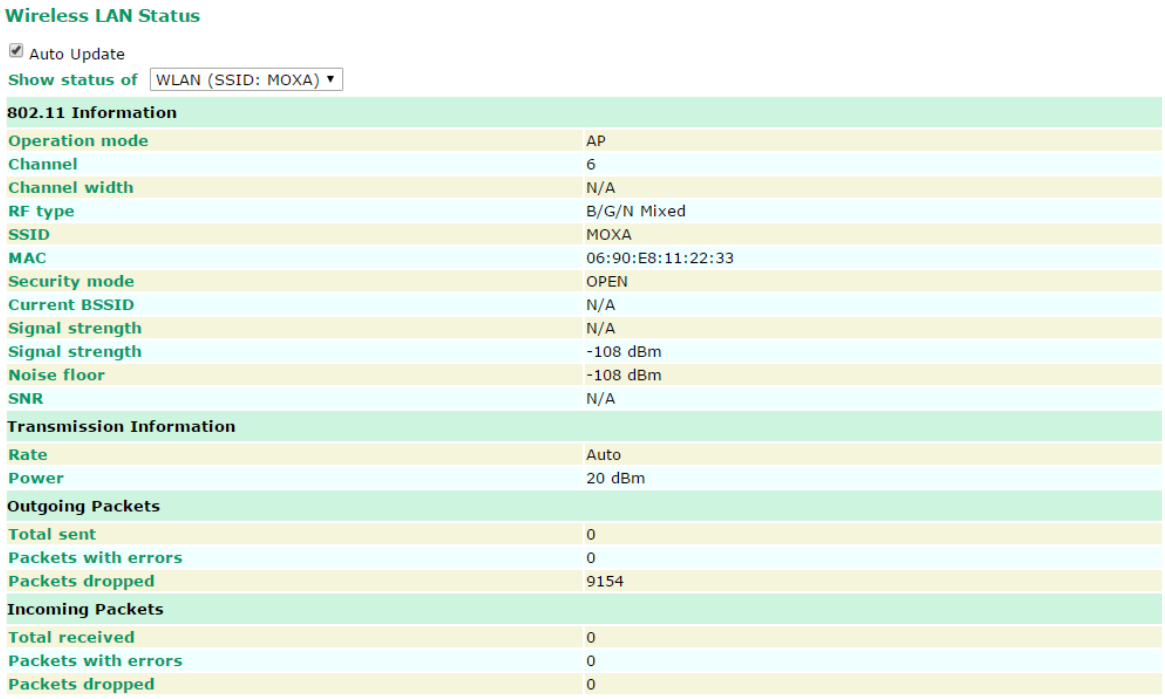
NOTE The model name of the AWK-4131A is shown as AWK-4131A-XX, where XX indicates the country code. The country code indicates the AWK-4131A version and which frequencies it uses. We use **AWK-4131A-US** as an example in the following figures. (The country code and model name that appears on your computer screen may be different than the one shown here.)

Overview

The **Overview** page summarizes the AWK-4131A's current status. The information is categorized into the groups: **System info**, **Device info,** and **802.11 info**.

System Information	
Model name	AWK-4131A-US
Device name	AWK-4131A_0000
Serial number	0
System uptime	0 days 03h:29m:48s
Firmware version	1.6 Build 17091517
Device Information	
Device MAC address	00:90:E8:11:22:33
IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	
802.11 Information	
Country code	US
Operation mode	AP
Channel	6
RF type	B/G/N Mixed
Channel width	N/A
SSID	MOXA

Click on **SSID** for more detailed 802.11 information, as shown in the following figure:



Wireless LAN Status

Auto Update

Show status of WLAN (SSID: MOXA)

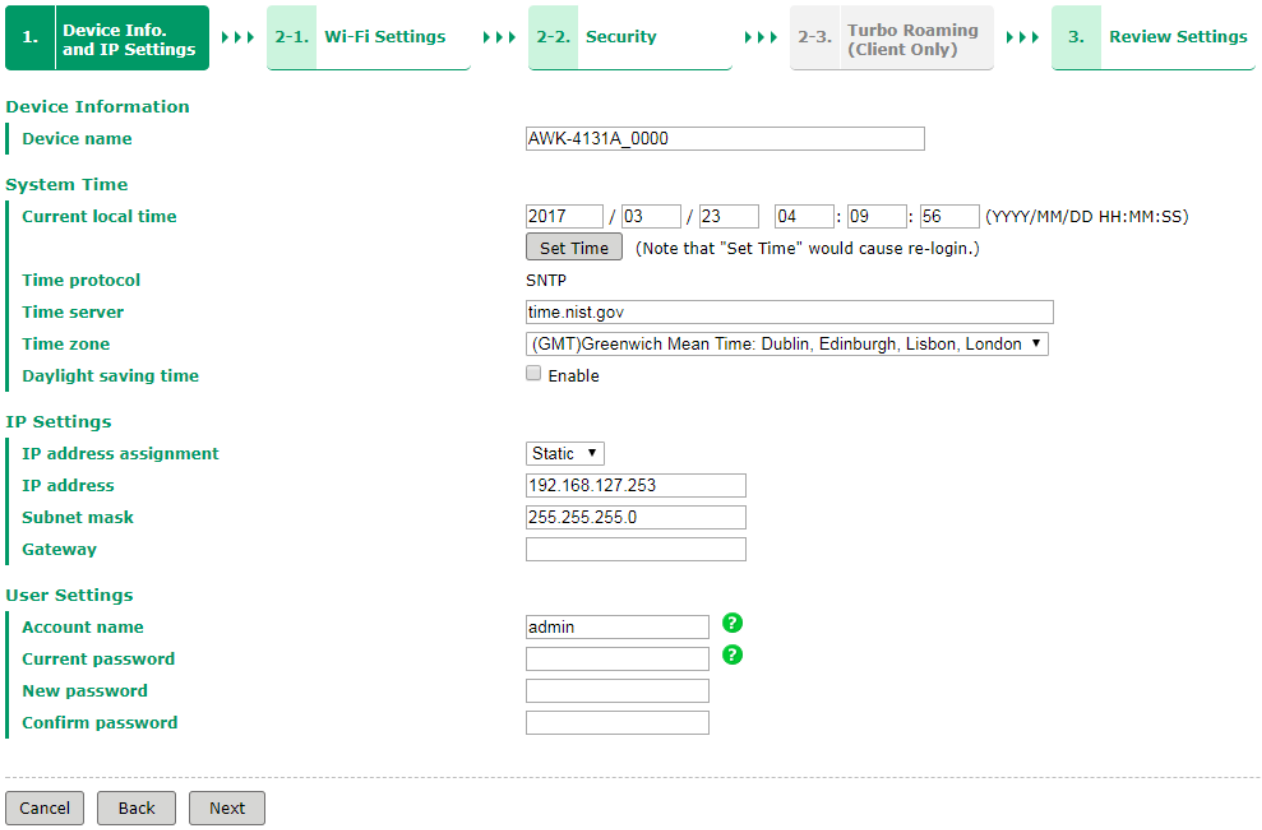
802.11 Information	
Operation mode	AP
Channel	6
Channel width	N/A
RF type	B/G/N Mixed
SSID	MOXA
MAC	06:90:E8:11:22:33
Security mode	OPEN
Current BSSID	N/A
Signal strength	N/A
Signal strength	-108 dBm
Noise floor	-108 dBm
SNR	N/A
Transmission Information	
Rate	Auto
Power	20 dBm
Outgoing Packets	
Total sent	0
Packets with errors	0
Packets dropped	9154
Incoming Packets	
Total received	0
Packets with errors	0
Packets dropped	0

NOTE The **802.11 info** that is displayed may be different for different operation modes. For example, **Current BSSID**, **Signal strength**, and **SNR** are only available under Client/Client-Router/Slave operation modes.

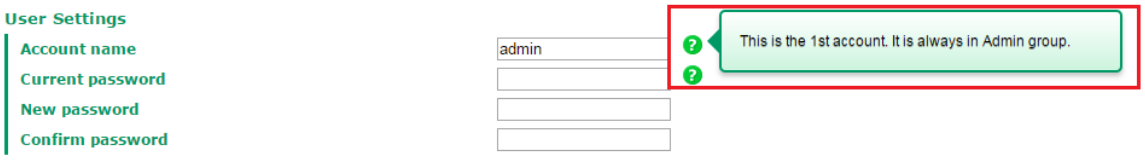
Quick Setup

The AWK-4131A provides a quick setup wizard to help you configure the basic settings including device information and wireless settings.

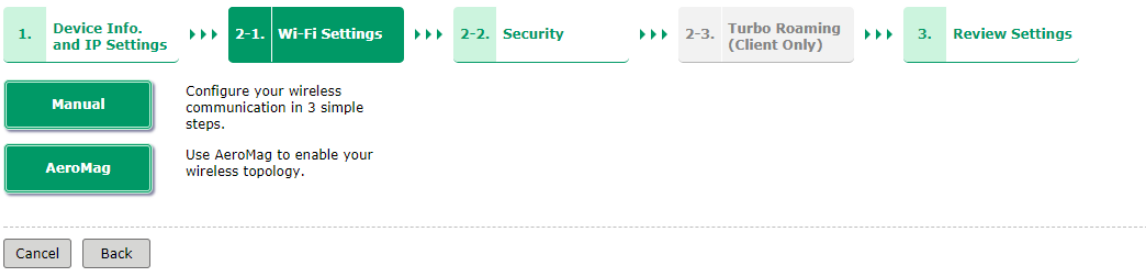
Once you enter the setup, links to each step in the process are displayed at the top of the page. You can either click **Next** to go to the next step or click directly on the links at the top of the page to go to a specific step.



NOTE You can move your cursor on the question mark symbol next to a field to view a tooltip that provides additional details regarding the corresponding field.

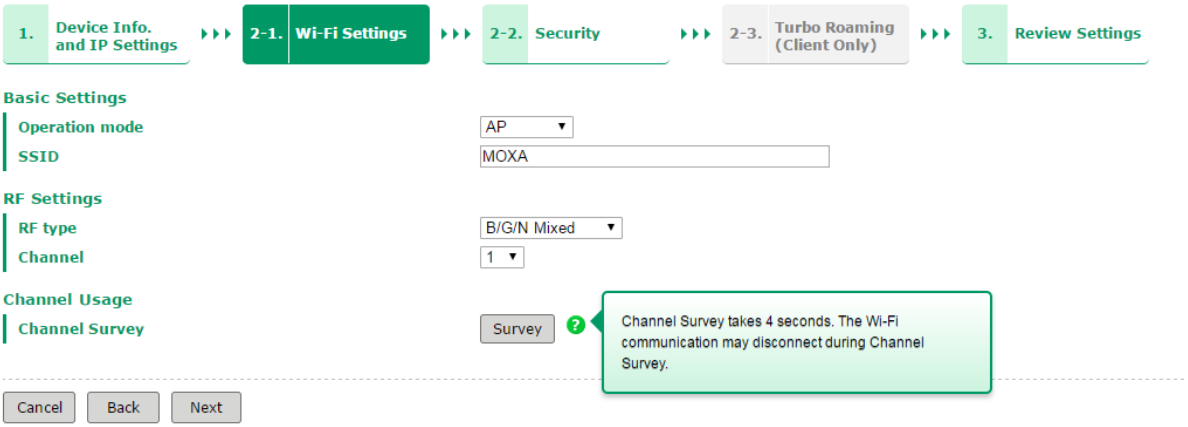


In the **Wi-Fi Settings** step, you can either use **Manual** to configure the basic Wi-Fi settings manually or click **AeroMag** to opt for AeroMag to automatically set up your Wi-Fi network.



For additional details on the AeroMag function, refer to the *Wireless LAN Setup* section. Note that Quick Setup does not support AeroMag for client-router mode.

If you use the **Manual** option to configure basic Wi-Fi settings, use the channel survey provided in the **Channel Usage** section to find out if a channel is clear or congested. This function can help you deploy a clear channel without requiring the use of an additional channel analysis tool.



Channel Usage Result - 2.4 GHz

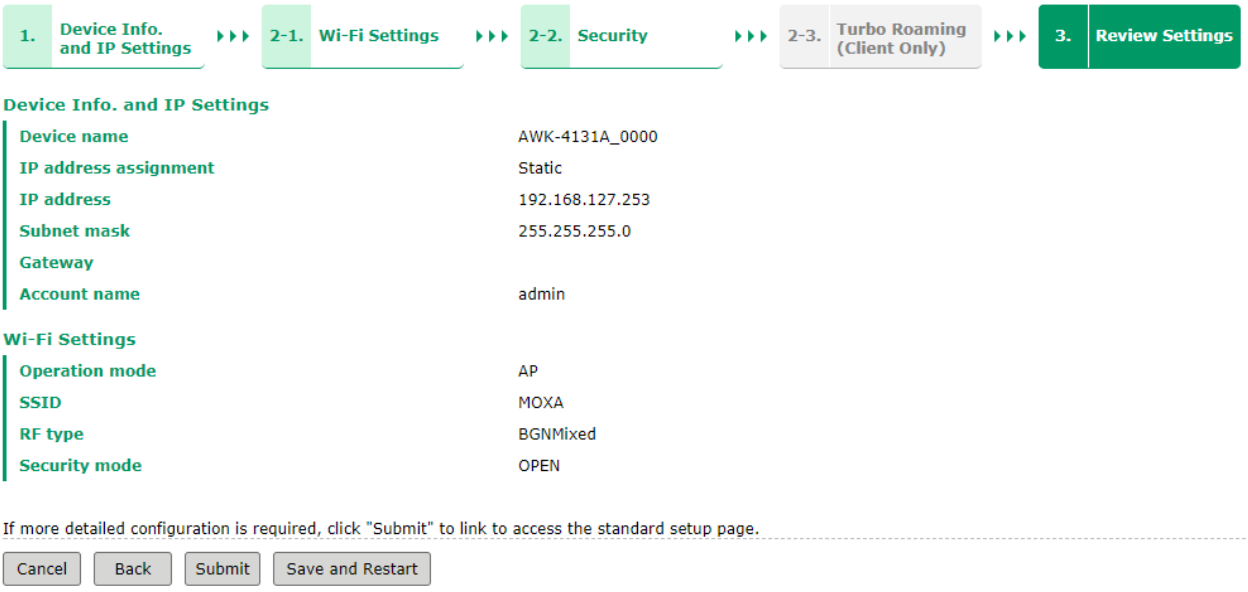
Channel	1	2	3	4	5	6	7
Number of APs	1	0	1	0	0	1	0
Load (%)	3	70	70	7	6	17	33
Noise floor (dBm)	-107	-107	-107	-107	-107	-107	-108
Channel	**8**	**9**	**10**	**11**	--	--	--
Number of APs	0	0	0	14	--	--	--
Load (%)	4	14	29	34	--	--	--
Noise floor (dBm)	-107	-109	-105	-106	--	--	--

Channel Usage Result - 5 GHz

Channel	36	40	44	48	52	56	60
Number of APs	8	2	3	1	0	0	1
Load (%)	3	1	1	1	0	0	1
Noise floor (dBm)	-113	-115	-116	-114	-115	-115	-115
Channel	**64**	**100**	**104**	**108**	**112**	**116**	**120**
Number of APs	0	0	0	0	0	0	1
Load (%)	0	0	0	0	0	0	1
Noise floor (dBm)	-114	-115	-115	-115	-116	-116	-117
Channel	**124**	**128**	**132**	**136**	**140**	**149**	**153**
Number of APs	1	1	0	0	0	3	3
Load (%)	79	57	0	0	15	6	7
Noise floor (dBm)	-115	-117	-117	-117	-112	-116	-117
Channel	**157**	**161**	**165**	--	--	--	--
Number of APs	3	12	6	--	--	--	--
Load (%)	1	17	3	--	--	--	--
Noise floor (dBm)	-117	-116	-117	--	--	--	--

Setting	Description
Number of APs	The number of APs which use this channel
Load	A measure of how congested a channel is, in percentage value. Both 802.11 and non-802.11 signals will affect the channel loading.
Noise floor	A summation of the noise level from all sources

You can see a complete preview of the Wi-Fi parameters that you configured when you click on the final step in the setup process (**Review Settings).**

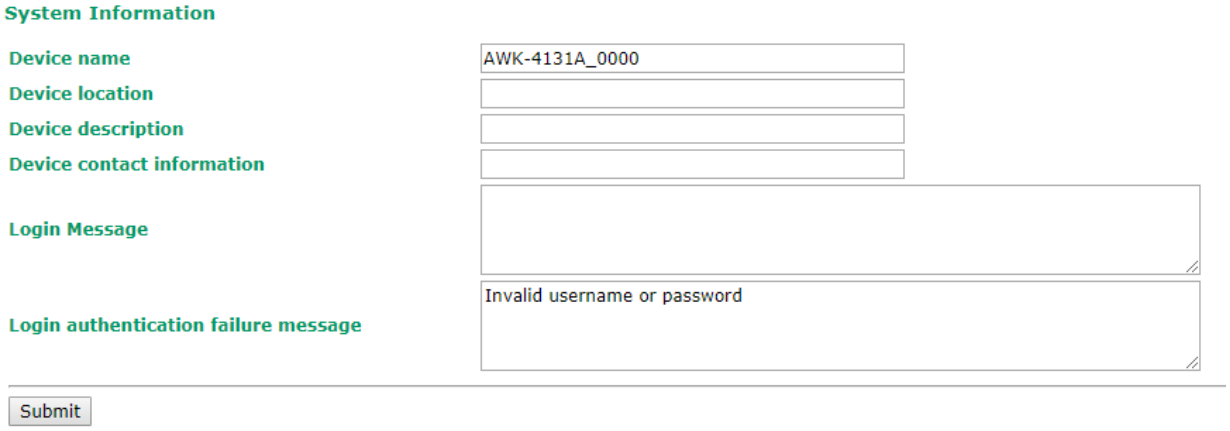


General Setup

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the AWK-4131A.

System Information

The **System Info** items, especially ***Device name*** and ***Device description***, are displayed and included on the **Overview** page, SNMP information, and alarm emails. Setting **System Info** items makes it easier to identify the different AWK-4131As connected to your network.



Device name

Format	Description	Factory Default
Max. 31 Characters	This option is useful for specifying the role or application of different AWK-4131A units.	*Model name_<Last 3 bytes of the device MAC>*

Device location

Format	Description	Factory Default
Max. 31 Characters	This specifies the location of different AWK-4131A units.	None

Device description

Format	Description	Factory Default
Max. 31 Characters	Use this space to record more detailed description of AWK-4131A.	None

Device contact information

Format	Description	Factory Default
Max. 31 Characters	To provide information about whom to contact in order to resolve problems, use this space to record contact information of the person responsible for maintaining this AWK-4131A.	None

Login Message

Setting	Description	Factory Default
Max. of 31 characters	Enter a message to display to all users when they log in	Blank

Login authentication failure message

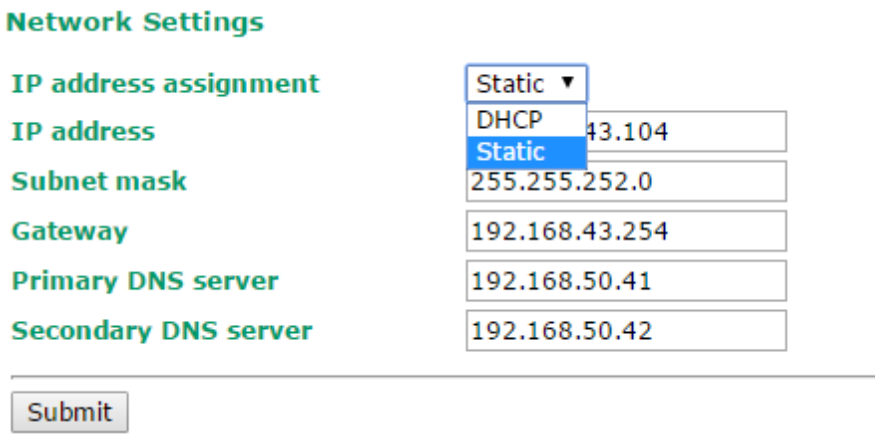
Setting	Description	Factory Default
Max. of 31 characters	Enter the login authentication failure message to display to the user who logs in with an invalid username or password	None

Interface On/Off

Network Settings

The **Network Settings** configuration panel allows you to modify the usual TCP/IP network parameters. However, due to the addition of the Client-Router operation mode, this panel provides two different sets of network parameters. Explanations for both types of configuration are given below.

Network Settings for AP/Client/Master/Slave Operation Modes



IP address assignment

Setting	Description	Factory Default
DHCP	The AWK-4131A's IP address will be assigned automatically by the network's DHCP server.	Static
Static	Set up the AWK-4131A's IP address manually.	

IP address

Setting	Description	Factory Default
AWK-4131A's IP address	Identifies the AWK-4131A on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
AWK-4131A's subnet mask	Identifies the type of network to which the AWK-4131A is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

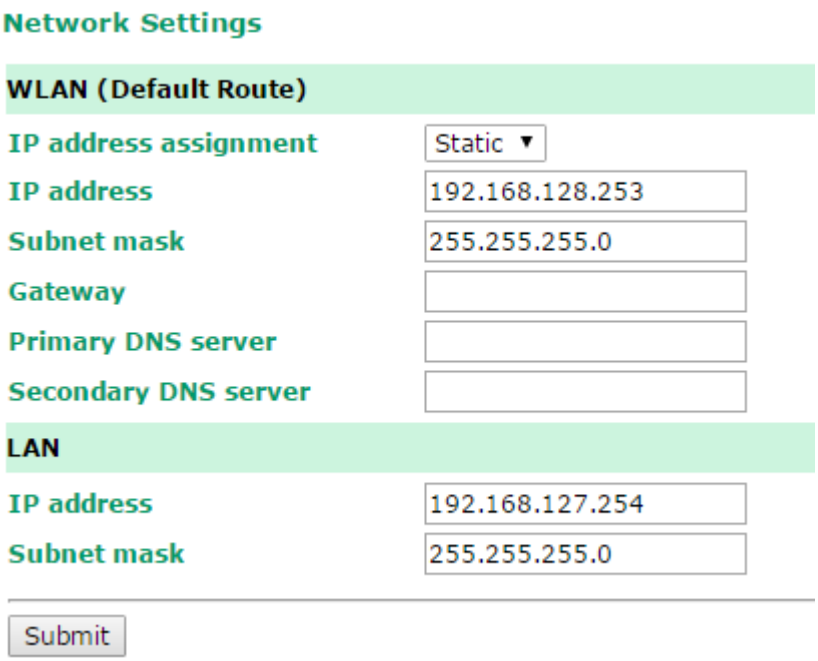
Gateway

Setting	Description	Factory Default
AWK-4131A's default gateway	The IP address of the router that connects the LAN to an outside network.	None

Primary/ Secondary DNS server

Setting	Description	Factory Default
IP address of the Primary/Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the AWK-4131A'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

Network Settings for Client-Router Operation Mode



WLAN IP address assignment

Setting	Description	Factory Default
DHCP	The AWK-4131A WLAN interface's IP address will be assigned automatically by the network's DHCP server.	Static
Static	Set up the AWK-4131A WLAN interface's IP address manually.	

WLAN IP address

Setting	Description	Factory Default
AWK-4131A WLAN interface's IP address	Identifies the AWK-4131A WLAN interface's IP address on a TCP/IP network.	192.168.128.253

WLAN subnet mask

Setting	Description	Factory Default
AWK-4131A WLAN interface's subnet mask	Identifies the type of network to which the AWK-4131A's WLAN interface is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

WLAN gateway

Setting	Description	Factory Default
AWK-4131A WLAN interface's default gateway	The IP address of the router that connects the WLAN to an outside network.	None

Primary/Secondary DNS server

Setting	Description	Factory Default
IP address of the Primary/Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the AWK-4131A'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

LAN IP address

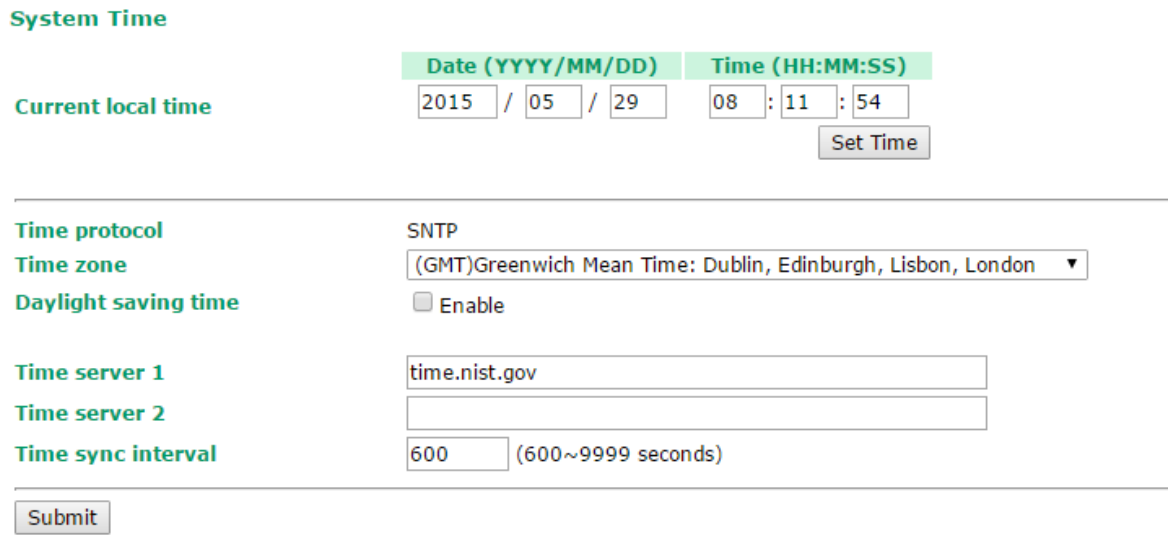
Setting	Description	Factory Default
AWK-4131A LAN interface's IP address	Identifies the AWK-4131A LAN interface's IP address on a TCP/IP network.	192.168.127.254

LAN subnet mask

Setting	Description	Factory Default
AWK-4131A LAN interface's subnet mask	Identifies the type of network to which the AWK-4131A's LAN interface is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

System Time

The AWK-4131A has a time calibration function based on information from an NTP server or user specified Date and Time information. Functions such as **Logs and Notifications** can add real-time information to the message.



The ***Current local time*** shows the AWK-4131A's system time when you open this web page. You can click on the **Set Time** button to activate the updated date and time parameters. An "(Updated)" string will appear to indicate that the change is complete. Local system time will be immediately activated in the system without running Save and Restart.

NOTE The AWK-4131A has a built-in real-time clock (RTC). We strongly recommend that users update the **Current local time** for the AWK-4131A after the initial setup or a long-term shutdown, especially when the network does not have an Internet connection for accessing the NTP server or there is no NTP server on the LAN.

Current local time

Setting	Description	Factory Default
User adjustable time	The date and time parameters allow configuration of the local time, with immediate activation. Use 24-hour format: yyyy/mm/dd hh:mm:ss	None

Time zone

Setting	Description	Factory Default
User selectable time zone	The time zone setting allows conversion from GMT (Greenwich Mean Time) to local time.	GMT (Greenwich Mean Time)

ATTENTION

Changing the time zone will automatically adjust the **Current local time**. You should configure the **Time zone** before setting the **Current local time**.

Daylight saving time

Setting	Description	Factory Default
Enable/ Disable	Daylight saving time (DST or summer time) involves advancing clocks (usually 1 hour) during the summer time to provide an extra hour of daylight in the afternoon.	Disable

When **Daylight saving time** is enabled, the following parameters will be shown:

- **Starts at:** The date that daylight saving time begins.
- **Stops at:** The date that daylight saving time ends.
- **Time offset:** Indicates how many hours forward the clock should be advanced.

Time server 1/2

Setting	Description	Factory Default
IP/Name of Time Server 1/2	IP or Domain name of the NTP time server. The 2nd NTP server will be used if the 1st NTP server fails to connect.	time.nist.gov

Time sync interval

Setting	Description	Factory Default
Time interval for NTP server synchronization (600 to 9999 seconds)	This parameter determines how often the time is synchronized from the NTP server.	600 (seconds)

Wireless LAN Setup

The AWK-4131A provides two different sets of wireless operation modes: AP/client modes for point-to-multipoint communication and master/slave modes for transparent point-to-point communication. The major differences between these two operation modes are the MAC address translation on the client/slave radio.

AP/client: The IP-Bridging mechanism is used to overcome limitations of the 802.11 standards. In this case, the MAC address of the devices connected to the client radio will be replaced with the client's MAC address. Under AP/client modes, communication problems might be encountered when you have a MAC authenticated system or MAC (Layer 2) based communication. In this case, you will need to change the network to use the master/slave operation mode.

Master/slave: A transparent point-to-point protocol that allows the devices' MAC addresses to remain unchanged when the packets get through the slave radio. If you are looking for a worry-free wireless solution to replace your wired system, use Master/Slave.

Client-router: A variation of standard client mode. WLAN behavior is identical with client mode, but a router behavior was added to separate the WLAN and LAN subnets. This allows network planners to allocate private IP addresses behind the client radio. More information on the Static Route, NAT, and Port Forwarding functions can be found in the **Advanced Setup** section.

Sniffer: In order to provide an easier way to analyze wireless traffic, the AWK-4131A supports a "Sniffer" mode to co-work with Wireshark packet sniffer software.

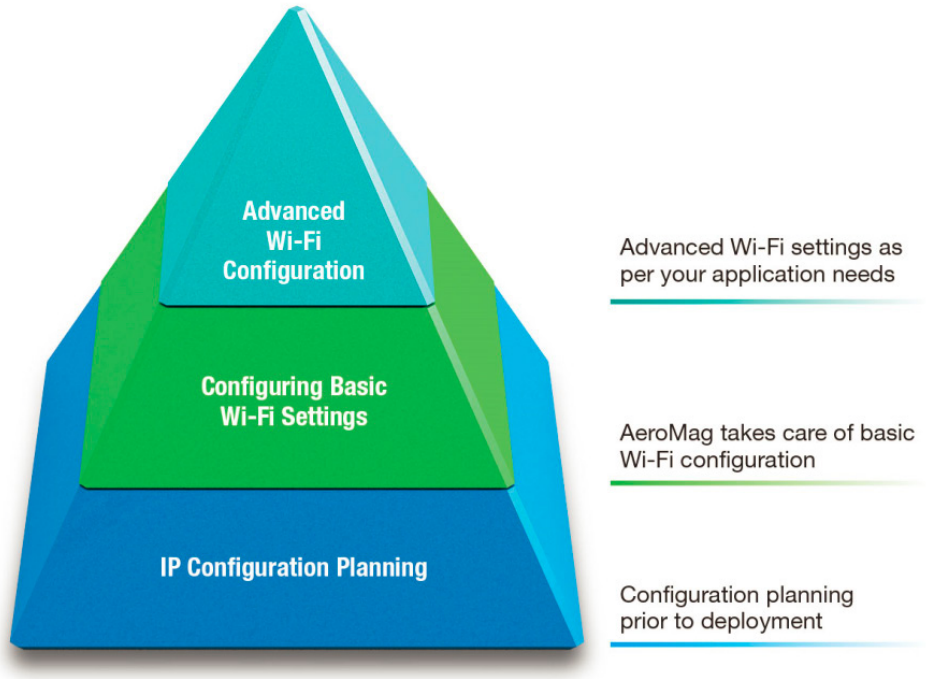
NOTE Although it is more convenient to use dynamic bridging, there is a limitation—the Client can only transmit IP-based packets between its wireless interface (WLAN) and Ethernet interface (LAN); other types of traffic (such as IPX and AppleTalk) are not forwarded.

AeroMag

Moxa's AeroMag tool enables fast, automatic, and error-free configuration of basic Wi-Fi settings based on the current wireless environment and location of the APs. The AWK-4131A can be used as an AeroMag client or client-router as well as an AeroMag AP.

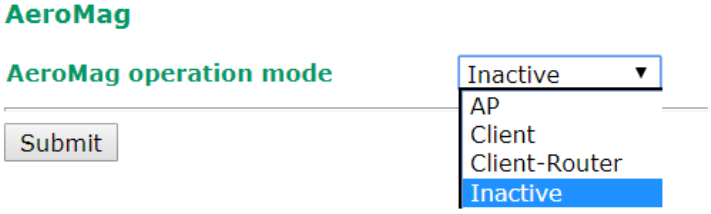
Concept

Moxa's AeroMag technology takes care of the basic Wi-Fi settings for you, saving you considerable effort when deploying your wireless networks. AeroMag is a useful tool throughout the Wi-Fi network lifecycle. When you are configuring network devices, AeroMag sets up your Wi-Fi connections correctly in a single step. During the installation phase, AeroMag streamlines network operation by analyzing the optimal channel for your current operating environment. From a maintenance perspective, new APs/clients can join the AeroMag topology without any additional configuration.



Once you have confirmed the number of APs and their location, using a site-survey tool, and have configured their device names and IP addresses, connect all the APs to the same network using Layer-2 switches. Next, activate the AeroMag function on both the APs and clients.

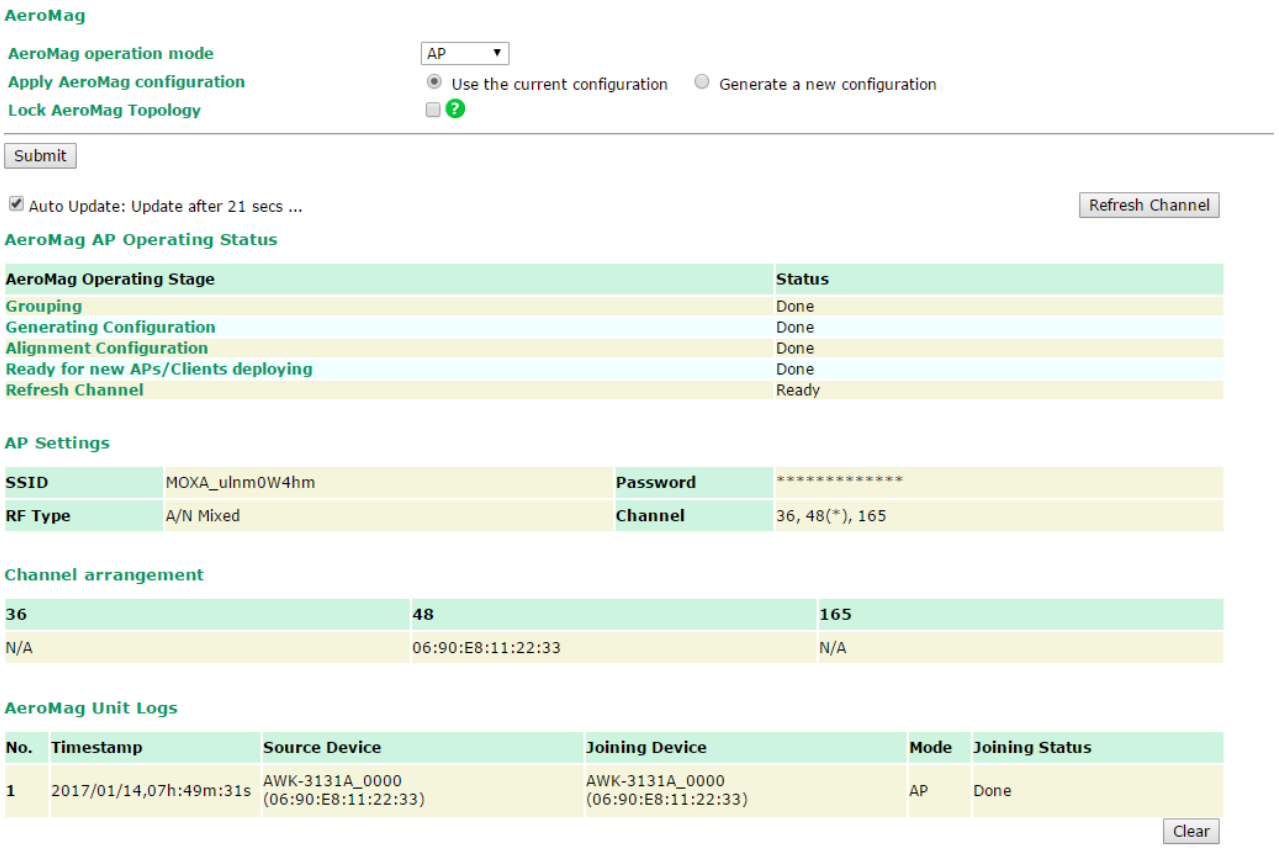
AeroMag decides the optimized RF type, channels, WPA2 password and SSID for you. AeroMag APs will generate an optimal configuration and assign it to AeroMag Clients. AeroMag Clients search AeroMag APs to achieve the optimal configuration.



Setting Up the Device as an AeroMag AP

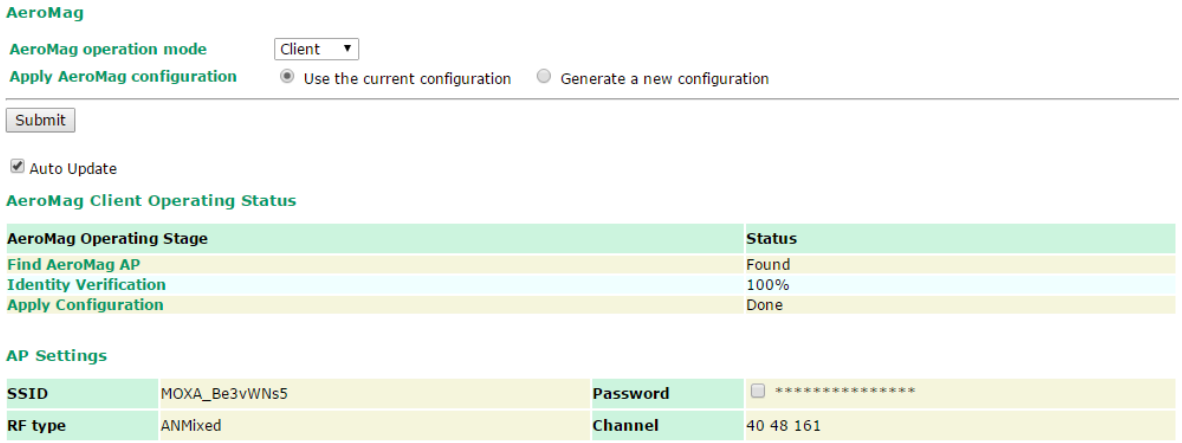
The AeroMag function is inactive by default. In the AWK-4131A, both the AP and the client modes are available under the AeroMag function. To activate AeroMag, set the **AeroMag operation mode** to **AP**.

The AeroMag function is inactive by default. Only the **AP** mode is available under the AeroMag functionality for AWK-4131A. To activate AeroMag, set the AeroMag operation mode to AP.



Setting Up the Device as an AeroMag Client/Client-router

Set the **AeroMag operation mode** to **Client** or **Client-Router.**



NOTE You can also activate AeroMag through MXconfig, SNMP, or by using the **Reset** button on the device. Press the **Reset** button on the AWK-4131A **four times** to activate the AeroMag AP. Press the **Reset** button five times to activate the AeroMag client. Press the **Reset** button three times to deactivate AeroMag (each consecutive press should be affected within 2 seconds of the previous one). You can activate either the AP first or the Client first as the order does not affect the behavior of the AeroMag tool.

You can configure the following setting when AeroMag is activated:

Setting	Description	Factory Default
Apply AeroMag configuration	• *Use the current configuration:* Use the current configuration generated by AeroMag. This option is only available if AeroMag was already active once before the current configuration change. If you are activating AeroMag for the first time, this option will not be available. • *Generate a new configuration:* - AeroMag AP: Discard the current configuration settings and generate a new set consisting of SSID, WAP2 password, RF type and search for the three best channels. - AeroMag Client/Client-Router: Discard current configuration settings and search for an AeroMag AP to get a new set of configuration settings.	*Generate a new configuration*
Lock AeroMag Topology	When this option is selected, no additional AP/Client is allowed to join this AeroMag topology and receive a new set of configuration settings. The status of all additional devices trying to join is indicated using a lock symbol. NOTE 1: Lock Down function will be active immediately. There is no need to submit the changes and reboot. NOTE 2: In the same AeroMag topology, you can access any one of AeroMag APs to trigger this function for all the topology units.	*Inactive*
Refresh Channel	All the AeroMag APs would search for the three best channels when **Refresh Channel** is triggered. If the new set of channels is different from the existing one, AeroMag APs will use the latest configuration generated and will inform the AeroMag clients to change their Turbo Roaming channels to the three channels defined by AeroMag. NOTE 1: Refresh Channel will be triggered immediately. There is no need to submit the action and reboot. NOTE 2: In the same AeroMag topology, you can access any one of AeroMag APs to trigger this function for all topology units.	

You can also view the **AeroMag AP Operating Status** listed below:

NOTE Select the **Auto Update** option for AeroMag to refresh the AeroMag Operating Status every 30 seconds. When channels are refreshed or a new configuration is generated, selecting the Auto Update option will refresh an AP's operating status every 5 seconds.

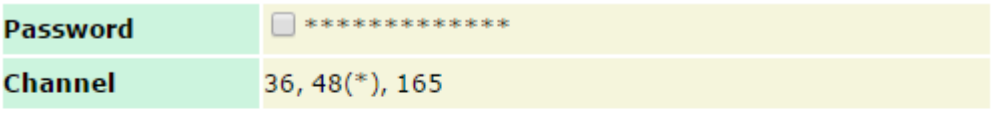
AeroMag AP Operating Status

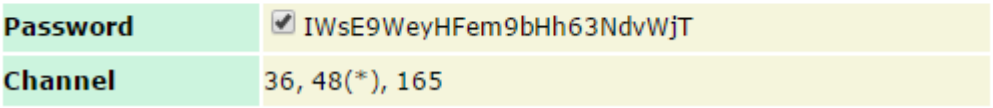
Parameter	Description
Grouping	The AeroMag APs find the units which are also connected to the same L2 subnet. They mark themselves as a group with same SSID. One AP among them would act as Master AeroMag AP.
Generating Configuration	The master AeroMag AP generates a new configuration using the spectrum report received from all AeroMag APs
Alignment Configuration	All AeroMag APs align configuration which is distributed by Master AeroMag AP
Ready for new APs/Clients deploying	Ready for offering configuration to new coming APs/Clients
Refresh Channel	Whether Refresh Channel Function is ready

AeroMag Client/Client-router Operating Status

Parameter	Description
Find AeroMag AP	AeroMag Client searches for an AeroMag AP
Identity Verification	AeroMag Client sends a connection authentication request to the AeroMag AP for the AP to verify if the client is a Moxa device.
Apply Configuration	The configuration generated by the AeroMag AP and sent to the client, after a successful authentication of the client, is applied to this client.
AP Settings	Shows the AeroMag AP that this client is connected to and the assigned configuration

AeroMag views a topology where the wireless devices with the same SSID are grouped together. If you need to assign a specific SSID to devices, you must first deactivate AeroMag and then change each AWK's SSID. The new SSID for each device will become the group index the next time you activate the AeroMag function.





For a higher level of security, the password parameter can only be viewed over HTTPS by a user with an **Admin** account. No user can read the password over HTTP, not even n **Admin** account.

The **Channel** value displays the current channels that the AeroMag APs are operating in. The channel set is updated when the current AeroMag APs change their operating channels when **Refresh Channel** is triggered.

Parameter	Description
Channel Arrangement	Indicate the channel used by every AeroMag AP in this topology along with their MAC addresses
AP Settings	Shows the configuration that the AeroMag APs are using right now. The channel marked with an asterisk is the channel used by this AeroMag AP.

AeroMag Unit Logs

Parameter	Description
Timestamp	The timestamp when the event was last triggered.
Source Device	The AeroMag unit that provides the configuration of the unit joining the topology
Joining Device	The devices that are trying to join this topology
Mode	Operation mode used by the device trying to join this topology
Joining Status	The status of joining behavior.
Clear	Use this option to clear the log contents

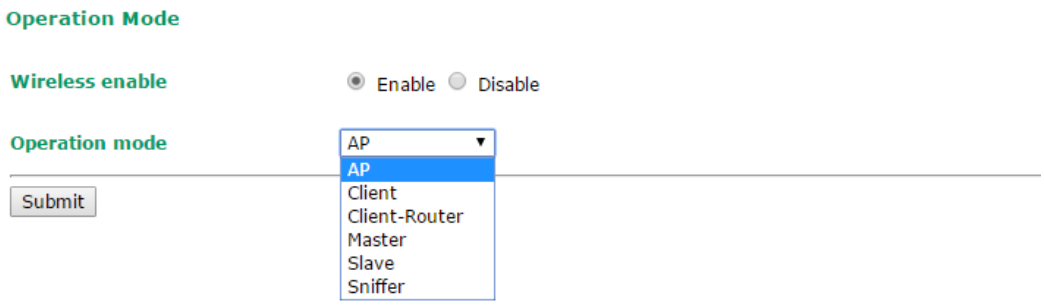
If the AeroMag APs or Clients are trying to join a topology that has been locked by AeroMag, the status will show **Block**. You should unlock the existing AeroMag topology in order to add new units. Channel-refreshing is recommended in order to optimize the channel arrangement whenever there are some new units added to the topology.

NOTE

1. An AeroMag AP allows normal Wi-Fi Clients to connect to it as long as they use the same SSID and same WAP2 settings. AeroMag will help you quickly set up the basic settings in your Wi-Fi network without changing the standard Wi-Fi behavior.
2. An AeroMag client CANNOT search and connect to a normal AP because of a null configuration during the search.
3. If two active groups of devices in an AeroMag topology connect to the same subnet network when the lock down feature is not activated, the two groups will merge and take the SSID, WAP2 password, and channels settings of one of the groups.
4. When AeroMag APs discard their configuration due to group merge, the corresponding AeroMag clients will also discard their configuration to search for new AeroMag APs.
5. We highly recommend locking down your AeroMag topology once the topology is established as planned in order to prevent unexpected AeroMag units from joining this topology.
6. We highly recommend refreshing the channels right after first installing the devices on-site the first time.
7. When AeroMag is active, you cannot change the Basic WLAN and Security Setup manually.
8. If you would like to set your own SSID yet gain benefit from AeroMag at the same time, we recommend that you activate one AeroMag AP first and then change to your own SSID. Next, connect all the other units so that the AeroMag topology can be grouped with a manually assigned SSID.
9. If an AeroMag client is informed that the Turbo Roaming channel needs to be changed due to a **Refresh Channel** action triggered by AeroMag APs, the Wi-Fi connection with the client will be disconnected for 180 seconds, until the client reconnects to an AP.
10. If an AeroMag client is disconnected from an AeroMag AP and fails to find an AeroMag AP within the Turbo Roaming channels within 150 seconds, the client starts to scan all channels for AeroMag APs to recover its AeroMag connection.
11. If an AeroMag client loses a connection for 10 minutes and fails to connect again, the AeroMag client discards the current configuration and starts searching for AeroMag APs all over again.
12. AeroMag devices in a network must operate in the same regulatory band. For example, if one AeroMag unit uses US band and the others unit use EU band, AeroMag will fail to establish a network topology.

Operation Mode

The AWK-4131A supports six operation modes—AP, Client, Client-Router, Master, Slave, and Sniffer—each of which plays a distinct role on the wireless network.



Wireless enable

Setting	Description	Factory Default
Enable/Disable	The RF (Radio Frequency) module can be manually turned on or off.	Disable

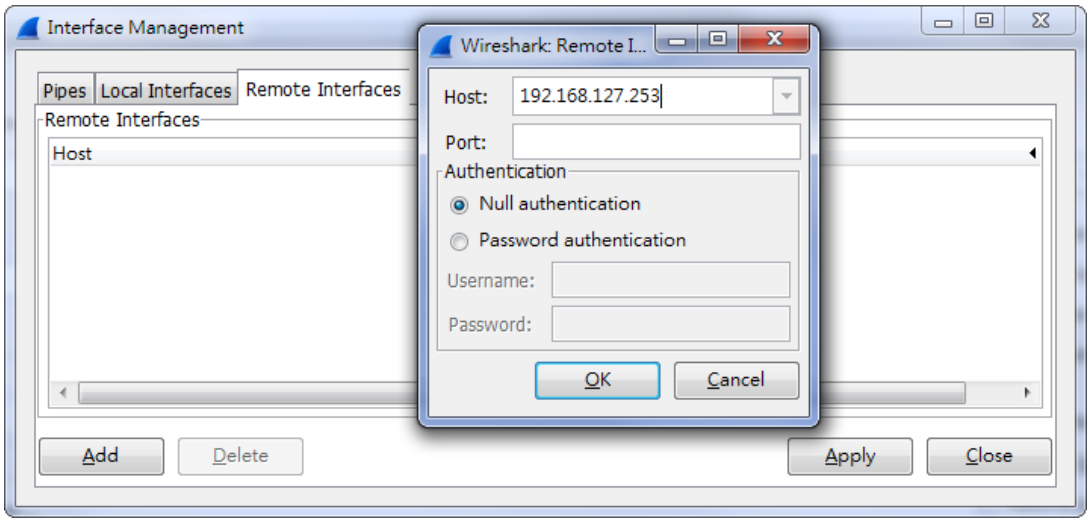
NOTE If you upgrade the firmware after performing any configuration changes, the wireless interface will remain enabled. If you reset the device back to factory default settings, the wireless interface will be disabled.

Operation mode

Setting	Description	Factory Default
AP	The AWK-4131A plays the role of wireless Access Point.	AP
Client	The AWK-4131A plays the role of wireless Client.	
Client-Router	The AWK-4131A plays the role of wireless Client, but includes the router function to divide the WLAN and LAN interfaces into two subnets.	
Master	The AWK-4131A plays the role of wireless Master.	
Slave	The AWK-4131A plays the role of wireless Slave.	
Sniffer	Turns the device into a remote Wireshark interface to capture 802.11 packets for analysis.	

Sniffer mode instructions:

1. Set operation mode to Sniffer mode on the AWK-4131A and then save/reboot the device.
2. Connect the AWK-4131A to a laptop with Wireshark installed (v1.12.0 or later release) via Ethernet.
3. Add a remote interface by entering the IP address of the AWK-4131A.



Detailed Wireshark instructions can be found at:
https://www.wireshark.org/docs/wsug_html_chunked/ChCapInterfaceRemoteSection.html

4. Start capturing 802.11 wireless packets with Wireshark.

Basic WLAN Setup

The "Basic WLAN Setup" panel is used to add and edit SSIDs. An SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. You can configure your AWK to use up to 9 SSIDs. All of the SSIDs are active at the same time; that is, client devices can use any of the SSIDs to associate with the access point.

Basic WLAN Setup (Multiple SSID)

Status	SSID	Operation Mode	Action
Active	MOXA	AP	Edit

Add SSID

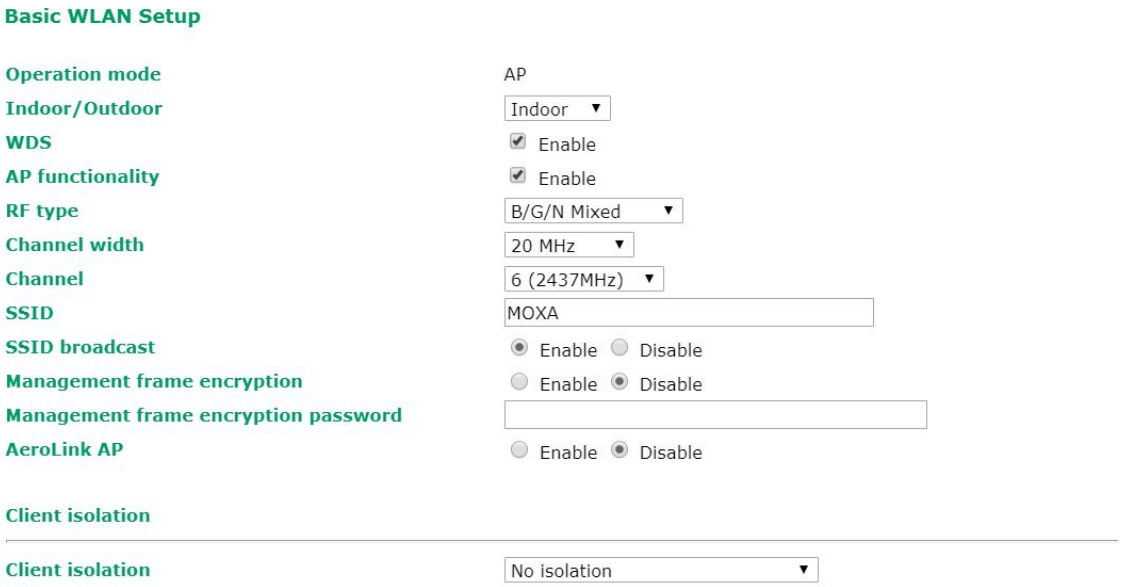
Click on **Add SSID** to create more SSIDs.

Basic WLAN Setup (Multiple SSID)

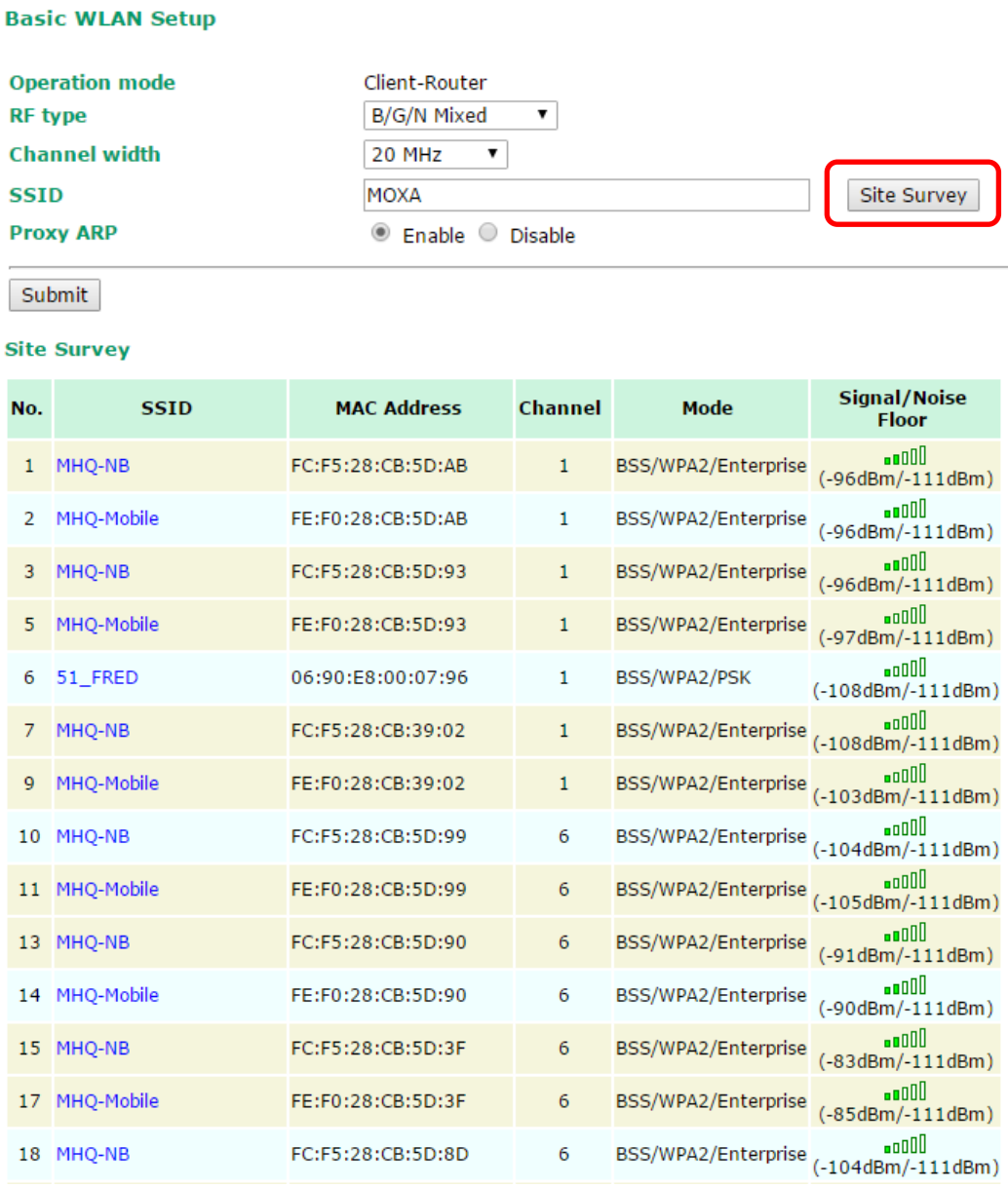
Status	SSID	Operation Mode	Action
Active	MOXA	AP	Edit
Inactive		AP	Save Cancel

Add SSID

Click on **Edit** to configure the settings. The RF type, channel, and channel width settings will apply to all SSIDs, all other settings can be configured individually for each SSID. The panel appears as follows:



NOTE When you switch to **Client, Client-Router, or Slave modes**, a **Site Survey** button will be available on the Basic WLAN Setup panel. Click the "Site Survey" button to view information about available APs, as shown in the following figure. You can click on the SSID of an entity and bring the value of its SSID onto the SSID field of the Basic WLAN Setup page. Click the **Refresh** button to re-scan and update the table.



No.	SSID	MAC Address	Channel	Mode	Signal/Noise Floor
1	MHQ-NB	FC:F5:28:CB:5D:AB	1	BSS/WPA2/Enterprise	(-96dBm/-111dBm)
2	MHQ-Mobile	FE:F0:28:CB:5D:AB	1	BSS/WPA2/Enterprise	(-96dBm/-111dBm)
3	MHQ-NB	FC:F5:28:CB:5D:93	1	BSS/WPA2/Enterprise	(-96dBm/-111dBm)
5	MHQ-Mobile	FE:F0:28:CB:5D:93	1	BSS/WPA2/Enterprise	(-97dBm/-111dBm)
6	51_FRED	06:90:E8:00:07:96	1	BSS/WPA2/PSK	(-108dBm/-111dBm)
7	MHQ-NB	FC:F5:28:CB:39:02	1	BSS/WPA2/Enterprise	(-108dBm/-111dBm)
9	MHQ-Mobile	FE:F0:28:CB:39:02	1	BSS/WPA2/Enterprise	(-103dBm/-111dBm)
10	MHQ-NB	FC:F5:28:CB:5D:99	6	BSS/WPA2/Enterprise	(-104dBm/-111dBm)
11	MHQ-Mobile	FE:F0:28:CB:5D:99	6	BSS/WPA2/Enterprise	(-105dBm/-111dBm)
13	MHQ-NB	FC:F5:28:CB:5D:90	6	BSS/WPA2/Enterprise	(-91dBm/-111dBm)
14	MHQ-Mobile	FE:F0:28:CB:5D:90	6	BSS/WPA2/Enterprise	(-90dBm/-111dBm)
15	MHQ-NB	FC:F5:28:CB:5D:3F	6	BSS/WPA2/Enterprise	(-83dBm/-111dBm)
17	MHQ-Mobile	FE:F0:28:CB:5D:3F	6	BSS/WPA2/Enterprise	(-85dBm/-111dBm)
18	MHQ-NB	FC:F5:28:CB:5D:8D	6	BSS/WPA2/Enterprise	(-104dBm/-111dBm)

Indoor/outdoor

Setting	Description	Factory Default
Indoor/Outdoor	Select the usage environment, available channels vary depending on the selection	Indoor

WDS (for AP Mode only)

In a WDS (Wireless Distribution System) configuration, a wireless link is established between two IEEE 802.11 APs. Wireless packets transmitted across the WDS link at the link layer and comply with the IEEE 802.11 WDS format. To establish a static WDS bridge link, the APs at both ends of the WDS link must be configured manually with each other's device MAC address. WDS can only be configured in a star or tree topology to prevent loops in the network that may affect performance.

Setting	Description	Factory Default
Enable/Disable	Establish a static wireless link based on the Wireless	Disable

	Distribution System (WDS).	

NOTE WPA/WPA2 encryption is **not** supported in WDS, only OPEN/WEP security is available. When WDS is enabled, you can create a strictly point-to-point WDS link by disabling AP functionality. The AWK-4131A supports up to 8 WDS links to other APs or wireless bridges. Enter the target device's MAC address to set up a WDS link. If WDS is enabled, a list of bridge connections will appear. If you are connecting the AWK to APs from different brands, please check device compatibility first.

RF type

Setting	Description	Factory Default
2.4 GHz		
B	Only supports the IEEE 802.11b standard.	B/G/N Mixed
G	Only supports the IEEE 802.11g standard.	
B/G Mixed	Supports IEEE 802.11b/g standards, but 802.11g may operate at a slower speed if when 802.11b clients are on the network.	
G/N Mixed	Supports IEEE 802.11g/n standards, but 802.11n may operate at a slower speed if 802.11g clients are on the network.	
B/G/N Mixed	Supports IEEE 802.11b/g/n standards, but 802.11g/n may operate at a slower speed if 802.11b clients are on the network.	
N Only (2.4 GHz)	Only supports the 2.4 GHz IEEE 802.11n standard.	
5 GHz		
A	Only supports the IEEE 802.11a standard.	
A/N Mixed	Supports IEEE 802.11a/n standards, but 802.11n may operate at a slower speed if 802.11a clients are on the network.	
N Only (5 GHz)	Only supports the 5 GHz IEEE 802.11n standard.	

Channel (for AP mode only)

Setting	Description	Factory Default
Available channels vary with RF type	This option is only adjustable when the AWK-4131A plays the role of wireless AP. If the device acts as a wireless client, it follows the channel of the associated access point.	6 (in B/G/N Mixed mode)

NOTE The AWK supports DFS channels in AP mode and will automatically detect interfering radar signals. The AWK will perform a 60-seconds scan to check for radar signals before starting to use the DFS channel. If a radar signal was detected, the AWK will move to another channel after 10 seconds. The channel with the interfering radar signal will be unavailable for 30 minutes.

Channel width (for any 11N RF type only)

Setting	Description	Factory Default
20 MHz	Select your channel width, If you are not sure which option to use, select 20/ 40 MHz (Auto).	20 MHz
20/40 MHz		

Channel bonding

If 20/40 MHz only is the Channel Width setting, this channel bonding will auto set the channel based on your channel setting.

SSID

Setting	Description	Factory Default
Max. of 31 characters	The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. NOTE: An SSID cannot contain the following characters:	MOXA

	` ' " | ; &	

SSID broadcast (for AP mode only)

Setting	Description	Factory Default
Enable/ Disable	Specifies if SSID can be broadcast or not.	

IMPORTANT!

If the SSID broadcast function is disabled, APs and clients cannot establish connections on DFS channels. This is because clients are only allowed to do passive scanning of DFS channels; active scanning on these channels is forbidden.

Management Frame Encryption

Setting	Description	Factory Default
Enable/Disable	Enable this function for increased security. Management Frame encryption function allows users to set a specific password for any two devices to connect with each other.	Disable

NOTE AeroMag does not support Management frame encryption.

Aerolink AP

Setting	Description	Factory Default
Enable/Disable	Enable the AeroLink APs to monitor Ethernet communication on the AP side in order to trigger AeroLink Protection on the client side under milliseconds recovery time. NOTE: AeroLink Protection should be also enabled on the client side at the same time.	Disable

Client Isolation (for AP Mode only)

Client isolation is used to isolate the wireless clients connected to one or more APs. Isolated clients cannot communicate with each other, which increases security. Depending on the type of client isolation, you can specify exceptions (for clients) within the isolation network. This function is useful for cases such as enterprise server services for example.

Setting	Description	Factory Default
No isolation	No isolation is applied.	No isolation
Isolated within the same AP	All clients associated with this AP will be isolated from one another.	
Isolated within the same subnet	All clients in the specified subnet will be isolated from one another. The subnet is defined by the gateway address and subnet mask.	

NOTE If Client Isolation is enabled, it will be impossible to ping or configure clients directly from the management PC.

AP functionality

Setting	Description	Factory Default
Enable/Disable	Enable this option to allow the AWK-4131A to perform additional AP functions such as connecting standards Wi-Fi clients in addition to acting as a bridge AP.	Disable

NOTE Both the AP and client devices must be in the same channel and use the same security settings. In addition, an identical SSID is necessary for clients that roam between APs in Bridge mode. The Client will automatically scan for any AP that is using the defined SSID and will establish a bridge link with the matching AP.

WLAN Security Settings

The AWK-4131A provides four standardized wireless security modes: **Open**, **WEP** (Wired Equivalent Privacy), **WPA** (Wi-Fi Protected Access), and **WPA2**. Several security modes are available in the AWK-4131A by selecting ***Security mode*** and ***WPA type***.

- **Open:** No authentication, no data encryption.
- **WEP:** Static WEP (Wired Equivalent Privacy) keys must be configured manually.
- **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 actually encrypt outgoing packets and decrypt incoming packets.
- **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. The AWK-4131A can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.
- **WPA-WPA2 mix:** AWK supports WPA/WPA2 at the same time. AWK is able to authenticate with both Wi-Fi clients that use WPA and WPA2.

Security mode

Setting	Description	Factory Default
Open	No authentication	Open
WEP	Static WEP is used	
WPA*	WPA is used	
WPA2*	Supports IEEE 802.11i with "TKIP/AES + 802.1X"	
WPA-WPA2 mix*	Both WPA and WPA2 clients are able to connect to AWK at the same time	

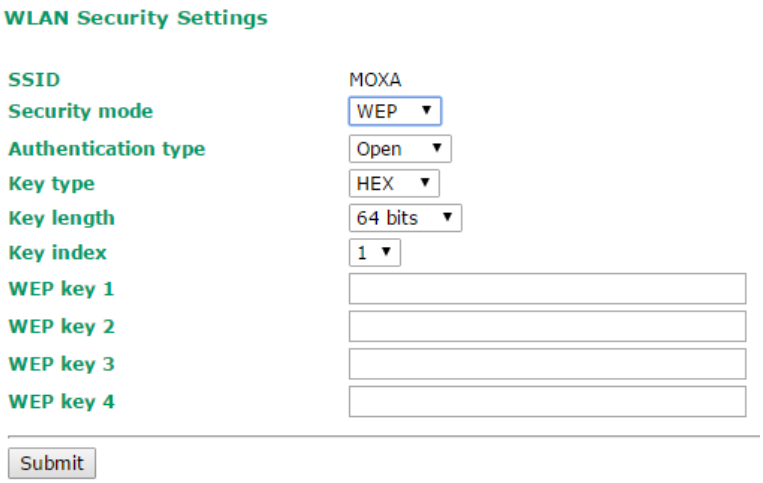
** This option is not supported when using WDS*

Open

For security reasons, you should **NOT** set security mode to Open System, since authentication and data encryption are **NOT** performed in Open System mode.

WEP (for Legacy Mode Only)

NOTE Moxa includes **WEP** security mode only for legacy purposes. **WEP** is highly insecure and is considered fully deprecated by the Wi-Fi alliance. We do not recommend the use of WEP security under any circumstances.



According to the IEEE 802.11 standard, WEP can be used for authentication and data encryption to maintain confidentiality. Shared (or Shared Key) authentication type is used if WEP authentication and data encryption are both needed. Normally, Open (or Open System) authentication type is used when WEP data encryption is run with authentication.

When WEP is enabled as a security mode, the length of a key (so-called WEP seed) can be specified as 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The AWK-4131A provides 4 entities of WEP key settings that can be selected to use with ***Key index***.

The selected key setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

The WEP key can be presented in two ***Key types***, HEX and ASCII. Each ASCII character has 8 bits, so a 40-bit (or 64-bit) WEP key contains 5 characters, and a 104-bit (or 128-bit) key has 13 characters. In hex, each character uses 4 bits, so a 40-bit key has 10 hex characters, and a 128-bit key has 26 characters.

Authentication type

Setting	Description	Factory Default
Open	Data encryption is enabled, but without authentication.	Open
Shared	Data encryption and authentication are both enabled.	

Key type

Setting	Description	Factory Default
HEX	Specifies WEP keys in hexa-decimal number form.	HEX
ASCII	Specifies WEP keys in ASCII form.	

Key length

Setting	Description	Factory Default
64 bits	Uses 40-bit secret keys with 24-bit initialization vector.	64 bits
128 bits	Uses 104-bit secret key with 24-bit initialization vector.	

Key index

Setting	Description	Factory Default
1-4	Specifies which WEP key is used.	Open

WEP key 1-4

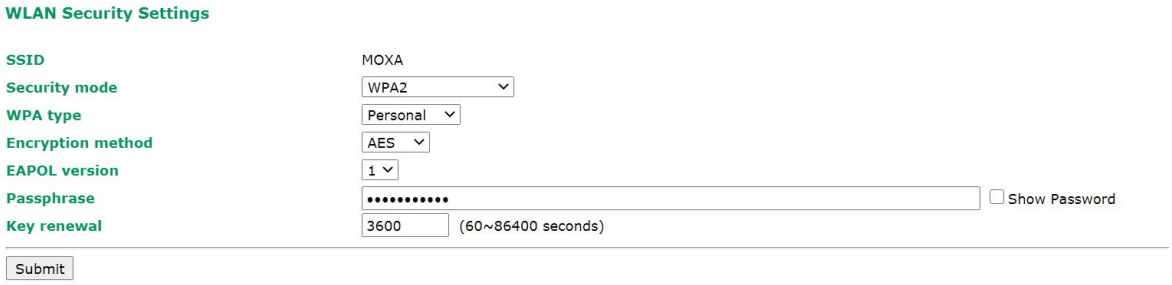
Setting	Description	Factory Default
ASCII type: 64 bits: 5 chars 128 bits: 13chars HEX type: 64 bits: 10 hex chars 128 bits: 26 hex chars	A string that can be used as a WEP seed for the RC4 encryption engine. The key cannot contain the following special characters: ` ' " | ; &	None

WPA/WPA2-Personal

WPA (Wi-Fi Protected Access) and WPA2 represent significant improvements over the WEP encryption method. WPA is a security standard based on 802.11i draft 3, while WPA2 is based on the fully ratified version of 802.11i. The initial vector is transmitted, encrypted, and enhanced with its 48 bits, twice as long as WEP. The key is regularly changed so that true session is secured.

Even though AES encryption is only included in the WPA2 standard, it is widely available in the WPA security mode of some wireless APs and clients as well. The AWK-4131A also supports AES algorithms in WPA and WPA2 for better compatibility.

Personal versions of WPA/WPA2, also known as WPA/WPA-PSK (*Pre-Shared Key*), provide a simple way of encrypting a wireless connection for high confidentiality. A ***Passphrase*** is used as a basis for encryption methods (or cipher types) in a WLAN connection. The passphrases should be complicated and as long as possible. There must be at least 8 ASCII characters in the Passphrase, and it could go up to 63. For security reasons, this passphrase should only be disclosed to users who need it, and it should be changed regularly.



WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2.	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2.	

Encryption method

Setting	Description	Factory Default
TKIP**	Temporal Key Integrity Protocol is enabled.	AES
AES	Advance Encryption System is enabled.	
Mixed*	Provides TKIP broadcast key and TKIP+AES unicast key for some legacy AP clients. This option is rarely used.	

*** This option is only available with 802.11a/b/g standard*

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

Passphrase

Setting	Description	Factory Default
8 to 63 characters	Master key to generate keys for encryption and decryption. The passphrase cannot contain the following special characters: ` ' " | ; &	None

	Check Show Password to display the password in clear text.	

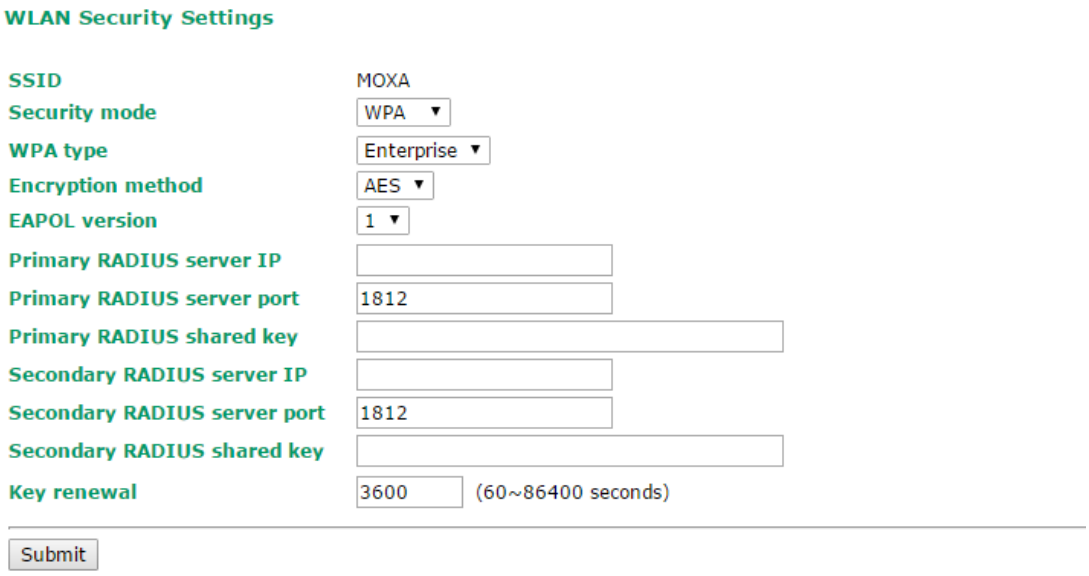
Key renewal (for AP/Master mode only)

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 day)	Specifies the time period of group key renewal.	3600 (seconds)

NOTE The ***key renewal*** value dictates how often the wireless AP encryption keys should be changed. The security level is generally higher if you set the key renewal value to a shorter number, which forces the encryption keys to be changed more frequently. The default value is 3600 seconds (60 minutes). Longer time periods can be considered if the line is not very busy.

WPA/WPA2-Enterprise (for AP/Master Mode)

By setting ***WPA type*** to **Enterprise**, you can use **EAP** (*Extensible Authentication Protocol*), a framework authentication protocol used by 802.1X to provide network authentication. In these Enterprise-level security modes, a back-end RADIUS (Remote Authentication Dial-In User Service) server is needed if IEEE 802.1X functionality is enabled in WPA /WPA2. The IEEE 802.1X protocol also offers the possibility of carrying out an efficient connection authentication on a large-scale network. It is not necessary to exchange keys or passphrases.



WPA type

Setting	Description	Factory Default
Personal	Provides Pre-Shared Key-enabled WPA and WPA2.	Personal
Enterprise	Provides enterprise-level security for WPA and WPA2.	

Encryption method

Setting	Description	Factory Default
TKIP**	Temporal Key Integrity Protocol is enabled.	AES
AES	Advance Encryption System is enabled.	
Mixed*	Provides TKIP broadcast key and TKIP+AES unicast key for some legacy AP clients. This option is rarely used.	

*** This option is only available with 802.11a/b/g standard*

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

Primary/Secondary RADIUS server IP

Setting	Description	Factory Default
The IP address of RADIUS server	Specifies the delegated RADIUS server for EAP.	None

Primary/Secondary RADIUS port

Setting	Description	Factory Default
Port number	Specifies the port number of the delegated RADIUS server.	1812

Primary/ Secondary RADIUS shared key

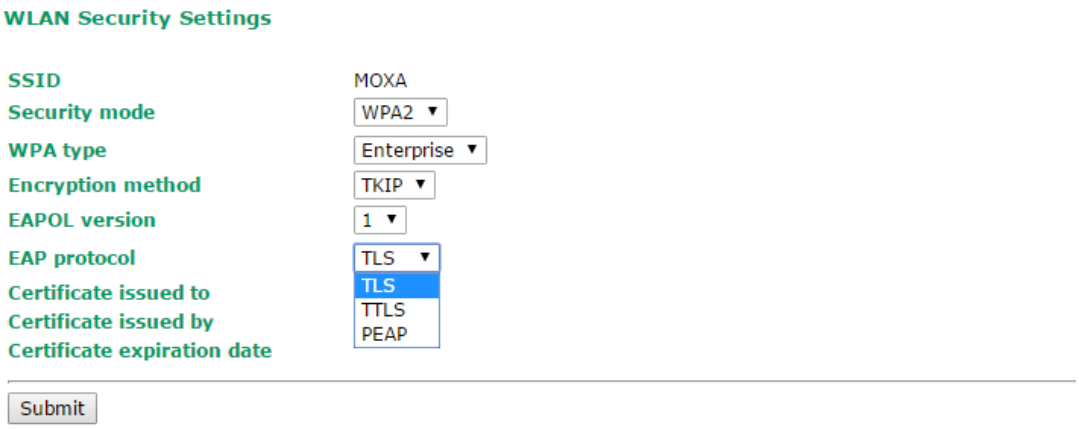
Setting	Description	Factory Default
Max. of 31 characters	The secret key shared between AP and RADIUS server. The key cannot contain the following special characters: ` ' " | ; &	None

Key renewal

Setting	Description	Factory Default
60 to 86400 seconds (1 minute to 1 day)	Specifies the time period of group key renewal.	3600 (seconds)

WPA/WPA2-Enterprise (for Client/Client-Router/Slave mode)

When used as a client, the AWK-4131A can support three EAP methods (or ***EAP protocols***): **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**, corresponding to WPA/WPA-Enterprise settings on the AP side.



Encryption method

Setting	Description	Factory Default
TKIP**	Temporal Key Integrity Protocol is enabled.	TKIP
AES	Advance Encryption System is enabled.	

***This option is only available with 802.11a/b/g standard.*

EAP protocol

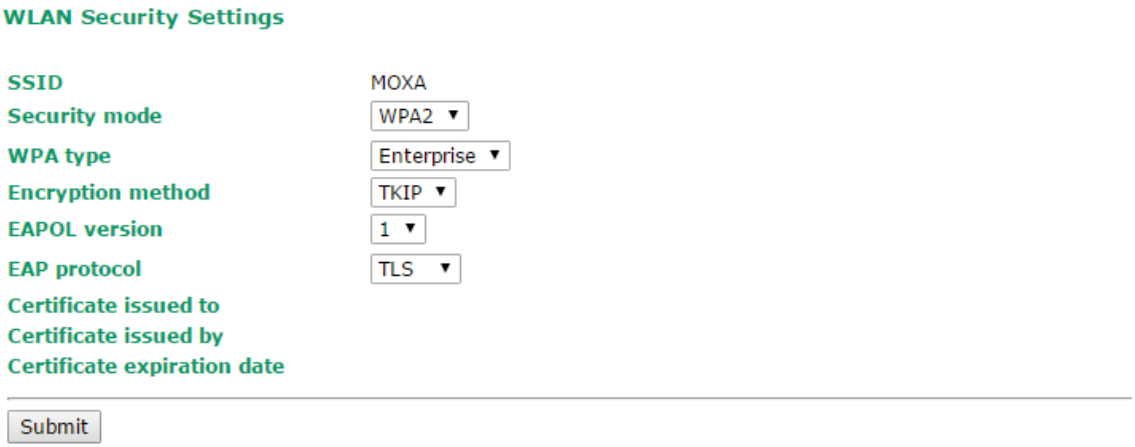
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol.	TLS
TTLS	Specifies Tunneled Transport Layer Security.	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP.	

Before choosing the EAP protocol for your WPA/WPA2-Enterprise settings on the client end, please contact the network administrator to make sure the system supports the protocol on the AP end. Detailed information on these three popular EAP protocols is presented in the following sections.

EAP-TLS

TLS is the standards-based successor to Secure Socket Layer (SSL). It can establish a trusted communication channel over a distrusted network. TLS provides mutual authentication through certificate exchange. EAP-TLS is also secure to use. You are required to submit a digital certificate to the authentication server for validation, but the authentication server must also supply a certificate.

You can use **Basic WLAN Setup** → **WLAN Certificate Settings** to import your WLAN certificate and enable EAP-TLS on the client end.



You can check the current certificate status in ***Current Status*** if it is available.

- **Certificate issued to:** Shows the certificate user
- **Certificate issued by**: Shows the certificate issuer
- **Certificate expiration date**: Indicates when the certificate has expired

EAP-TTLS

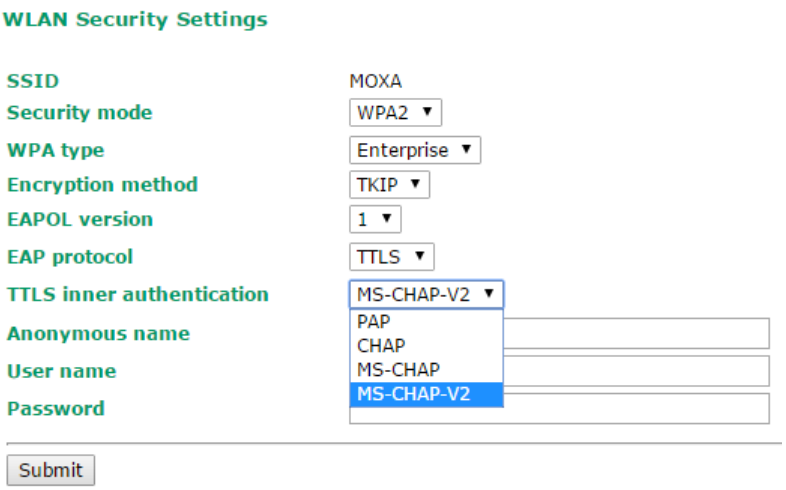
It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than creating a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called "legacy authentication methods."

TTLS and PEAP work in a similar way. First, they establish a TLS tunnel (EAP-TLS for example), and validate whether the network is trustworthy with digital certificates on the authentication server. This step establishes a tunnel that protects the next step (or "inner" authentication), and consequently is sometimes referred to as "outer" authentication. The TLS tunnel is then used to encrypt an older authentication protocol that authenticates the user for the network.

As you can see, digital certificates are still needed for outer authentication in a simplified form. Only a small number of certificates are required, which can be generated by a small certificate authority. Certificate reduction makes TTLS and PEAP much more popular than EAP-TLS.

The AWK-4131A provides some non-cryptographic EAP methods, including **PAP**, **CHAP**, **MS-CHAP**, and **MS-CHAP-V2**. These EAP methods are not recommended for direct use on wireless networks. However, they may be useful as inner authentication methods with TTLS and PEAP.

Because the inner and outer authentications can use distinct user names in TTLS and PEAP, you can use an anonymous user name for the outer authentication, with the true user name only shown through the encrypted channel. Keep in mind that not all client software supports anonymous alteration. Confirm this with the network administrator before you enable identity hiding in TTLS and PEAP.



TTL inner authentication

Setting	Description	Factory Default
PAP	Password Authentication Protocol is used.	MS-CHAP-V2
CHAP	Challenge Handshake Authentication Protocol is used.	
MS-CHAP	Microsoft CHAP is used.	
MS-CHAP-V2	Microsoft CHAP version 2 is used.	

Anonymous

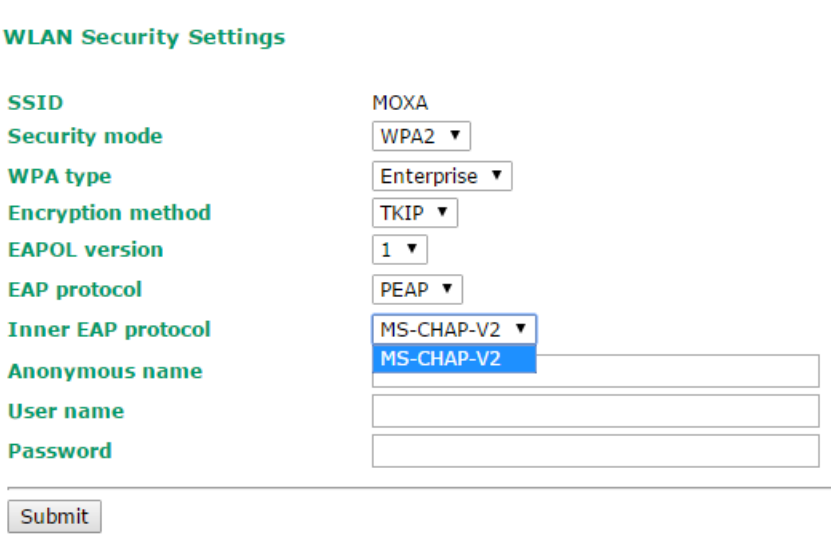
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication.	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication which cannot contain the following the special characters: ` ' " | ; &	None

PEAP

There are a few differences in the TTLS and PEAP inner authentication procedures. TTLS uses the encrypted channel to exchange attribute-value pairs (AVPs), while PEAP uses the encrypted channel to start a second EAP exchange inside of the tunnel. The AWK-4131A provides **MS-CHAP-V2** merely as an EAP method for inner authentication.



Inner EAP protocol

Setting	Description	Factory Default
MS-CHAP-V2	Microsoft CHAP version 2 is used.	MS-CHAP-V2

Anonymous

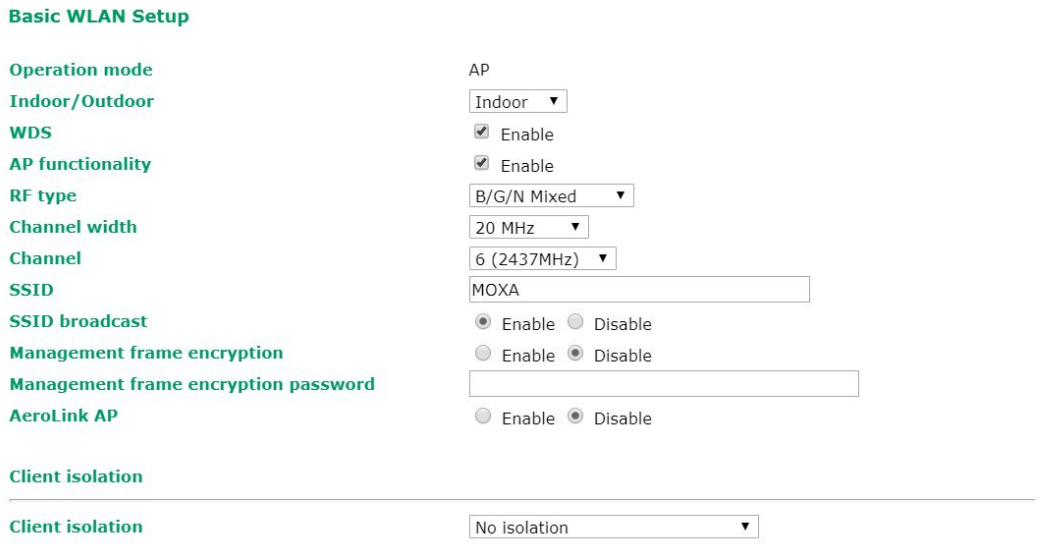
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication.	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication which cannot contain the following the special characters: ` ' " | ; &	None

Advanced WLAN Settings

Additional wireless-related parameters are presented in this section to help you set up your wireless network in detail.



Transmission rate

Setting	Description	Factory Default
Auto	The AWK-4131A senses and adjusts the data rate automatically.	Auto
Available rates	Users can manually select a target transmission data rate but does not support when RF type are G/N mixed, B/G/N mixed and A/N mixed.	

Minimum transmission rate

Setting	Description	Factory Default
0 to 64 Mbps (0 to disable)	By setting a minimum transmission rate, the AWK-4131A will avoid communicate with weak signal wireless links to maintain overall wireless performance and optimize the wireless frequency usage.	0 (Disable)

Multicast rate

Setting	Description	Factory Default
Available rates	You can set a fixed multicast rate for the transmission of broadcast and multicast packets on a per-radio basis. This parameter can be useful in an environment where multicast video streaming is occurring in the wireless medium, provided the wireless clients are capable of handling the configured rate.	6M

Maximum Transmission power

Setting	Description	Factory Default
Available power	Users can manually select a target power to mask max output power. Because different transmission rates would have their own max output power, please reference product datasheet. For 802.11b/g, the available setting is from 0 to 20	20 dBm

Beacon interval (for AP/Master mode only)

Setting	Description	Factory Default
Beacon Interval (40 to 1000 ms)	Indicates the frequency interval of the beacon.	100 (ms)

Inactive timeout (for AP mode only)

Setting	Description	Factory Default
8 to 240 seconds	Specifies how long before access point starts sending out client alive packets.	60 seconds

DTIM interval (for AP/Master mode only)

Setting	Description	Factory Default
Data Beacon Rate (1 to 15)	Indicates how often the AWK-4131A sends out a Delivery Traffic Indication Message.	1

Fragmentation threshold

Setting	Description	Factory Default
Fragment Length (256 to 2346)	Specifies the maximum size a data packet before splitting and creating another new packet.	2346

RTS threshold

Setting	Description	Factory Default
RTS/CTS Threshold (256 to 2346)	Determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication.	2346

NOTE You can refer to the related glossaries in Appendix A for detailed information about the above-mentioned settings. By setting these parameters properly, you can better tune the performance of your wireless network.

Transmission distance (5 GHz only)

Setting	Description	Factory Default
Distance or max. range for transmission (500 to 11,000 m)	Specifies the transmission distance or max. range between two AWK devices. This parameter should be set properly, especially for long-distance communication.	500

NOTE Make sure the same **Transmission distance** parameters are set in both **AP** and **Client**. When this parameter is greater than 500, an optimal algorithm will be enabled to support long-distance transmission.

Antenna

Setting	Description	Factory Default
A/B/Both	Specifies the output antenna port. Setting "Antenna" to Both allows 2x2 MIMO communication under 802.11n and 2T2R* communication in legacy 802.11a/b/g modes.	Both

**Different from 802.11n's multiple spatial data stream (2x2 MIMO), which doubles the throughput, 2T2R transmits/receives the same piece of data on both antenna ports.*

WMM

Setting	Description	Factory Default
Enable/Disable	WMM is a QoS standard for WLAN traffic. Voice and video data will be given priority bandwidth when enabled with WMM supported wireless clients. NOTE: WMM will always be enabled under 802.11n mode.	Enable

Turbo Roaming (for Client/Client-Router/Slave Mode only)

Setting	Description	Factory Default
Enable/ Disable	Moxa's Turbo Roaming can enable rapid handover when the AWK-4131A, as a client, roams among a group of APs.	Disable

When Turbo Roaming is enabled, the following parameters will be shown:

- **Roaming threshold:** Determines when to start looking for new AP candidates. If the current connection quality (SNR or Signal Strength) is lower than the specified threshold, the AWK will start background scanning and look for next-hop candidates.
  The following table lists the default threshold values for different RF types:

RF Type	RSSI	Signal Strength
Legacy 2.4G	30	-65
Legacy 5G	30	-65
N-mode 2.4G	40	-55
N-mode 5G	40	-50

NOTE While the AWK is scanning the background, its wireless performance will be reduced by 1/3 of its normal performance.

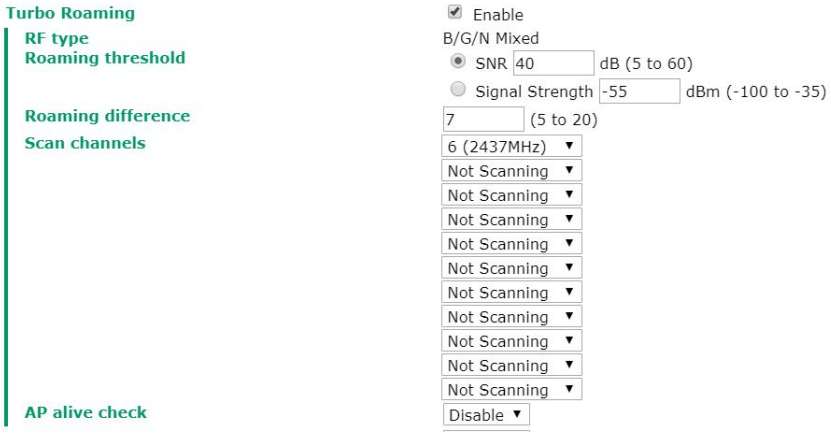
- **Roaming difference:** Determines if roaming should be executed. After background scan has been triggered, the roaming will only occur if the AP candidate(s) provide a better (Roaming difference) connection quality than the current connection. If multiple access points fulfill the criteria, the AWK will pick the best one to roam to.
- **Scan channels:** Pre-define up to 11 communication and roaming channels.

NOTE If AeroMag client is enabled, there will only be three scan channels which are assigned by AeroMag automatically.
The more channels are configured, the longer the scan will take to complete. This may increase the risk of disconnection if applied to fast moving clients. In high-density client environments, it may also cause performance drops.

- **AP alive check:** Allows roaming to react faster to WLAN disconnections.

NOTE Enabling this feature causes the AWK-4131A to send out alive-check packets every 10 ms when there is no traffic; the high transmission frequency of these small alive-check packets could potentially affect your other wireless communications that use the same channel, so only enable this feature when you have full control of the designated radio channel.

- **AP candidate threshold:** After the "AP alive check" declares that the current access point is no longer available, the surrounding access points must have good enough connection qualities (SNR/Signal Strength) in order to qualify as AP candidates for client association.



NOTE The Turbo Roaming recovery time (<150 ms) listed in the product documentation is an average of test results documented, in optimized conditions, across APs configured with interference-free 20-MHz RF channels, WPA2-PSK security, and default Turbo Roaming parameters. The clients are configured with 3-channel roaming at 100 Kbps traffic load. However, a combination of factors affect the AP handover recovery time of a roaming client, including but not limited to the following:

- On-site RF interference
- Velocity of the moving client devices
- Application traffic throughput
- Turbo Roaming parameters configured. i.e., Roaming threshold, Roaming difference, and AP candidate threshold.

Therefore, a site survey prior to device deployment is recommended to evaluate the ideal parameter settings on both clients and APs so that you can come up with an optimal deployment plan for your applications.

AeroLink Protection (for Client/Slave mode only)

Setting	Description	Factory Default
Enable/Disable	Enable AeroLink Protection to allow wireless clients on the same LAN network to automatically negotiate with each other and form a redundant wireless communication, for more details, see Status → AeroLink Protection Status.	Disable

When **AeroLink Protection** is enabled, the following parameter will be shown:
AP alive check: Enable to allow AeroLink Protection to react faster to WLAN disconnections.

NOTE Enabling this feature causes the AWK-4131A to send out alive-check packets every 10 ms when there is no traffic; the high transmission frequency of these small alive-check packets could potentially affect your other wireless communications that use the same channel, so only enable this feature when you have full control of the designated radio channel.

MAC clone (Client mode only)

Setting	Description	Factory Default
MAC clone	Enabling this feature allows the AWK client to copy the MAC address of the equipment connected to the LAN. This	Disable

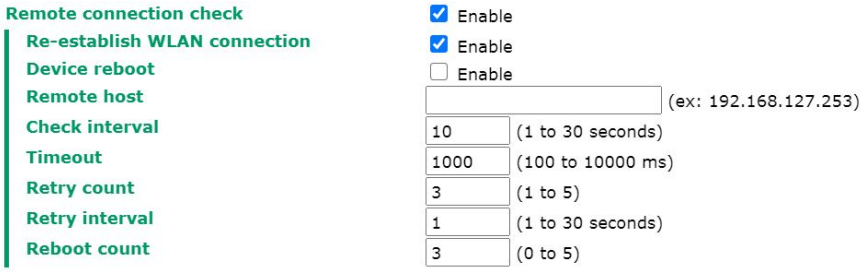
	overcomes the limitation of the IP-Bridged behavior in a MAC-sensitive network (MAC-based communication or MAC-authenticated network).	
MAC clone method	• Auto: The AWK client copies the MAC address of the device connected to the LAN if only one device connects to AWK. • Static: The AWK client shares the assigned MAC address with multiple devices connected to the LAN. This allows for multiple devices to connect to the AWK via the LAN and only one of them needs to be assigned a MAC address.	Auto
MAC clone static address	Specifies the static MAC address that the connected AWK devices should copy.	-

NOTE Auto MAC Cloning cannot be used together with Link Fault Pass Through.

Remote connection check (for Client/Client-router/Slave mode only)

Setting	Description	Factory Default
Enable/Disable	Enable remote connection check to automatically check the status of the connection and re-establish the connection when a connection failure occurs	Disable

When Remote connection check is enabled, the following parameters will be shown:



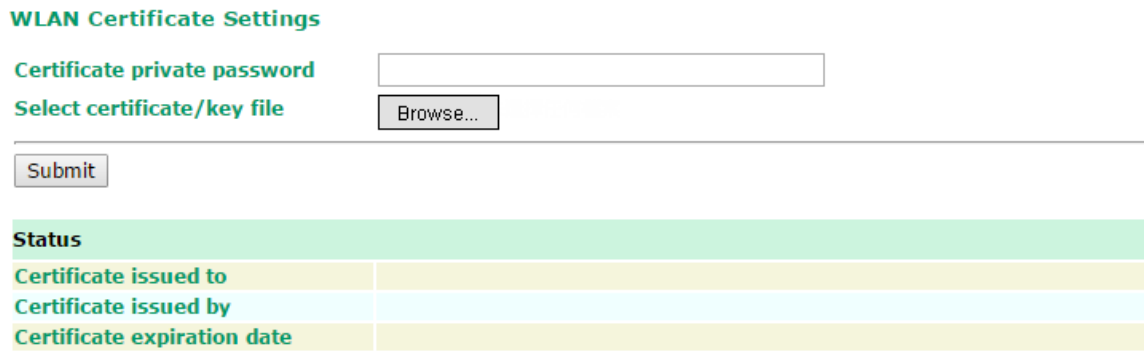
- **Re-establish WLAN connection:** Re-establish the WLAN connection in the event a connection failure.
- **Device reboot:** Reboot the device in the event of a connection failure.

NOTE If **Re-establish WLAN connection** and **Device reboot** are both enabled, the AWK-4131A will attempt to restore the WLAN connection first. If re-establishing the WLAN connection fails, the device will reboot.

- **Remote host:** Enter the IP address of a remote host to ping. This is used for the WLAN connection alive and packet-level connection checks.
- **Check interval:** Specify the time interval when the AWK-4131A checks the connection. The range is between 1 to 30 seconds, the default is every 10 seconds.
- **Timeout:** Specify the duration the AWK-4131A must wait before terminating the connection. The range is between 100 to 10,000 ms, the default is 1000 ms.
- **Retry count:** Specify the number of times the AWK-4131A the will check the connection status. If the connection fails more than the specified number of tries, the device will attempt to recover the WLAN connection. The range is between 1 to 5, the default is 3 retries.
- **Retry Interval:** Specify the time interval in between each retry. The range is between 1 to 30 seconds, the default is 1 second.
- **Reboot count:** If **Device reboot** is enabled, specify the number of times the device will reboot after failing to re-establish the connection.

WLAN Certificate Settings (for EAP-TLS in Client/Client-router/Slave mode only)

When EAP-TLS is used, a WLAN Certificate will be required at the client end to support WPA/WPA2-Enterprise. The AWK-4131A can support the **PKCS #12**, also known as *Personal Information Exchange Syntax Standard*, certificate formats that define file formats commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.



Current status displays information for the current WLAN certificate, which has been imported into the AWK-4131A. Nothing will be shown if a certificate is not available.

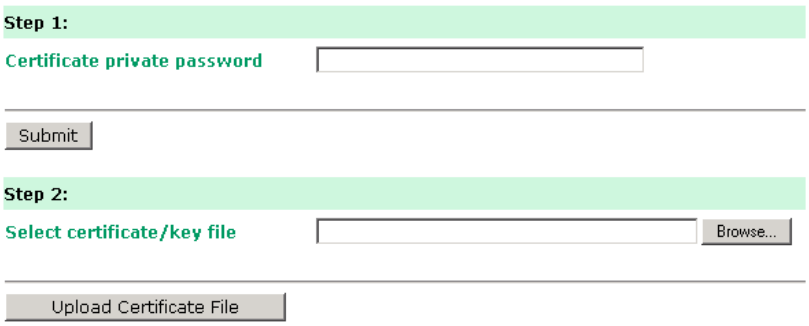
Certificate issued to: Shows the certificate user

Certificate issued by: Shows the certificate issuer

Certificate expiration date: Indicates when the certificate has expired

You can import a new WLAN certificate in ***Import WLAN Certificate*** by following these steps, in order:

1. Input the corresponding password (or key) in the **Certificate private password** field and then click **Submit** to set the password.
2. The password will be displayed in the Certificate private password field. Click on the **Browse** button in ***Select certificate/key file*** and select the certificate file.
3. Click **Upload Certificate File** to import the certificate file. If the import succeeds, you can see the information uploaded in ***Current Certificate***.
   If it fails, you may need to return to step 1 to set the password correctly and then import the certificate file again.



NOTE The WLAN certificate will remain after the AWK-4131A reboots. Even though it is expired, it can still be seen on the ***Current Certificate***.

Advanced Setup

Several advanced functions are available to increase the functionality of your AWK-4131A and wireless network system. A VLAN is a collection of clients and hosts grouped together as if they were connected to the broadcast domains in a layer-2 network. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, the AWK-4131A can support STP/RSTP protocol to increase reliability across the entire network, and SNMP support can make network management easier.

Using Virtual LAN

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

The 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 attached 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 adds, moves, 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

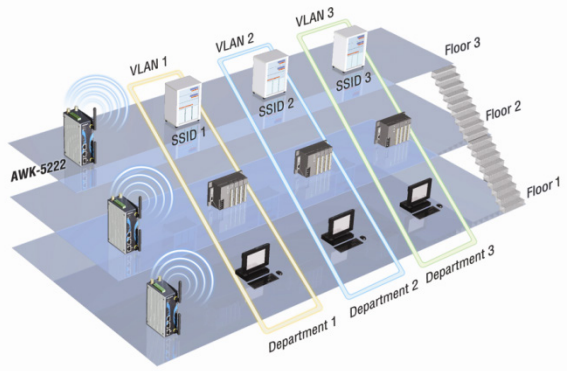
The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 9 SSIDs per radio interface, with a unique VLAN configurable per SSID.

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.

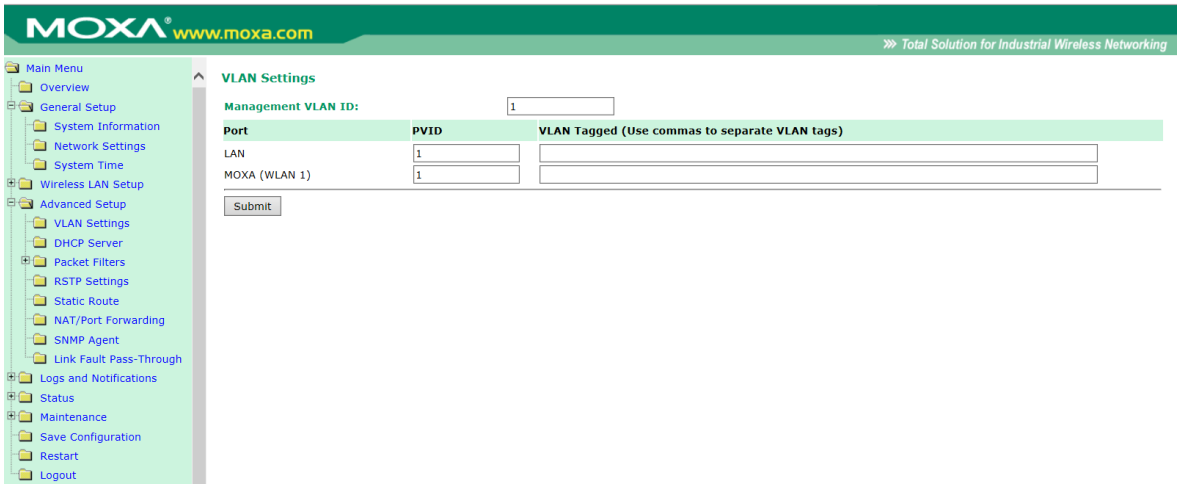
Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resource department could be restricted to a gateway that allowed access to only the Internet. A member of the human resource 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.



Configuring Virtual LAN

VLAN Settings

To configure the AWK's VLAN, use the VLAN Setting page to configure the ports.



Management VLAN ID

Setting	Description	Factory Default
VLAN ID ranges from 1 to 4094	Set the management VLAN of this AWK.	1

Port

Type	Description	Trunk Port
LAN	This port is the LAN port on the AWK.	Yes
WLAN	This is a wireless port for the specific SSID. This field will refer to the SSID that you have created. If more SSIDs have been created, new rows will be added.	

Port PVID

Setting	Description	Factory Default
VLAN ID ranging from 1 to 4094	Set the port's VLAN ID for devices that connect to the port. The port can be a LAN port or WLAN ports.	1

VLAN Tagged

Setting	Description	Factory Default
A comma-separated list of VLAN IDs. Each of the VLAN IDs range from 1 to 4094.	Specify which VLANs can communicate with this specific VLAN.	(Empty)

NOTE The VLAN feature can allow wireless clients to manage the AP. If the VLAN Management ID matches a VLAN ID, then those wireless clients who are members of that VLAN will have AP management access.

CAUTION: Once a VLAN Management ID is configured and is equivalent to one of the VLAN IDs on the AP, all members of that User VLAN will have management access to the AP. Be careful to restrict VLAN membership to those with legitimate access to the AP.

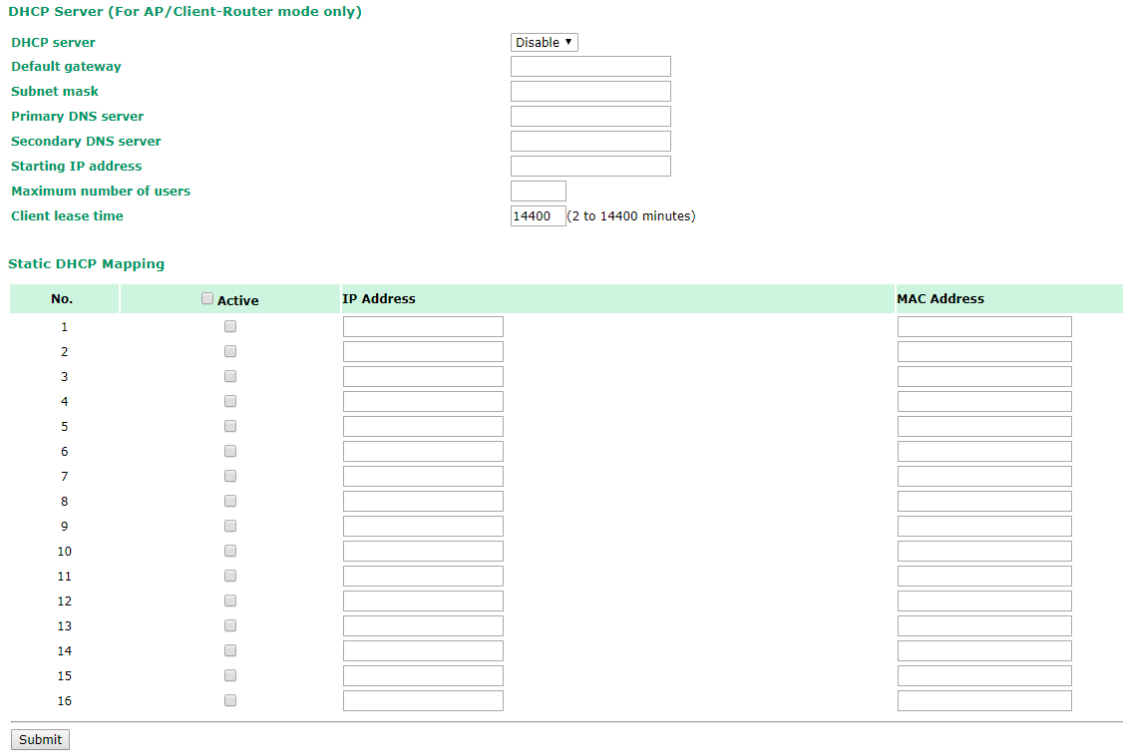
DHCP Server (for AP/Client-router mode only)

DHCP (Dynamic Host Configuration Protocol) is a networking protocol that allows administrators to assign temporary IP addresses to network computers by "leasing" an IP address to a user for a limited amount of time, instead of assigning permanent IP addresses.

The AWK-4131A can act as a simplified DHCP server and easily assign IP addresses to your DHCP clients by responding to the DHCP requests from the client ends. The IP-related parameters you set on this page will also be sent to the client.

You can also assign a static IP address to a specific client by entering its MAC address. The AWK-4131A provides a **Static DHCP mapping** list with up to 16 entities. Be reminded to check the **Active** check box for each entity to activate the setting.

You can check the IP assignment status under **Status → DHCP Client List**.



DHCP server

Setting	Description	Factory Default
Enable	Enables AWK-4131A as a DHCP server.	Disable
Disable	Disable DHCP server function.	

Default gateway

Setting	Description	Factory Default
IP address of a default gateway	The IP address of the router that connects to an outside network.	None

Subnet mask

Setting	Description	Factory Default
subnet mask	Identifies the type of sub-network (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	None

Primary/ Secondary DNS server

Setting	Description	Factory Default
IP address of Primary/ Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can use URL as well. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Start IP address

Setting	Description	Factory Default
IP address	Indicates the IP address which AWK-4131A can start assigning.	None

Maximum number of users

Setting	Description	Factory Default
1 to 128	Specifies how many IP address can be assigned continuously.	None

Client lease time

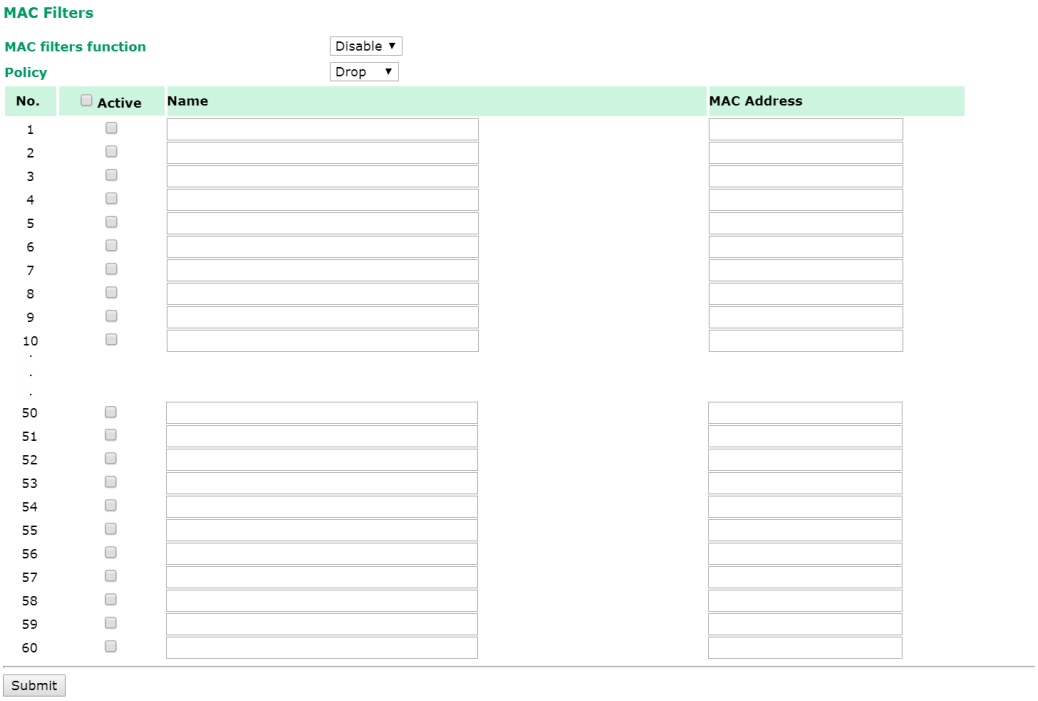
Setting	Description	Factory Default
2 to 14400 minutes	The lease time for which an IP address is assigned. The IP address may go expired after the lease time is reached.	14400 minutes (10 days)

Packet Filters

The AWK-4131A includes various filters for **IP-based** packets going through LAN and WLAN interfaces. You can set these filters as a firewall to help enhance network security.

MAC Filters

The AWK-4131A's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The AWK-4131A provides 60 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the setting.



MAC filters

Setting	Description	Factory Default
Enable	Enables MAC filters.	Disable
Disable	Disables MAC filters.	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Accept
Drop	Any packet fitting the entities on list will be denied.	

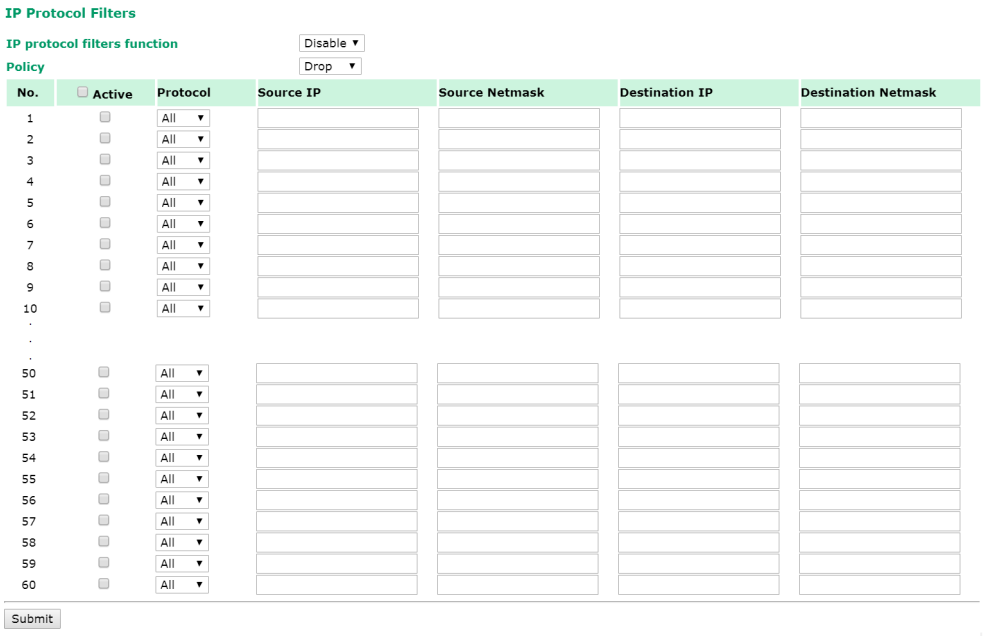
ATTENTION

Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed**
Accept + "no entity on list is activated" = all packets are **denied**

IP Protocol Filters

The AWK-4131A'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-4131A provides 60 entities for setting IP protocol and source/destination IP addresses in your filtering policy. Four IP protocols are available: **All**, **ICMP**, **TCP**, and **UDP**. You must specify either the Source IP or the Destination IP. By combining IP addresses and netmasks, you can specify a single IP address or a range of IP addresses to accept or drop. For example, "IP address 192.168.1.1 and netmask 255.255.255.255" refers to the sole IP address 192.168.1.1. "IP address 192.168.1.1 and netmask 255.255.255.0" refers to the range of IP addresses from 192.168.1.1 to 192.168.255. Remember to check the **Active** check box for each entity to activate the setting.



IP protocol filters

Setting	Description	Factory Default
Enable	Enables IP protocol filters.	Disable
Disable	Disables IP protocol filters.	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on the list can be allowed.	Accept
Drop	Any packet fitting the entities on the list will be denied.	

ATTENTION

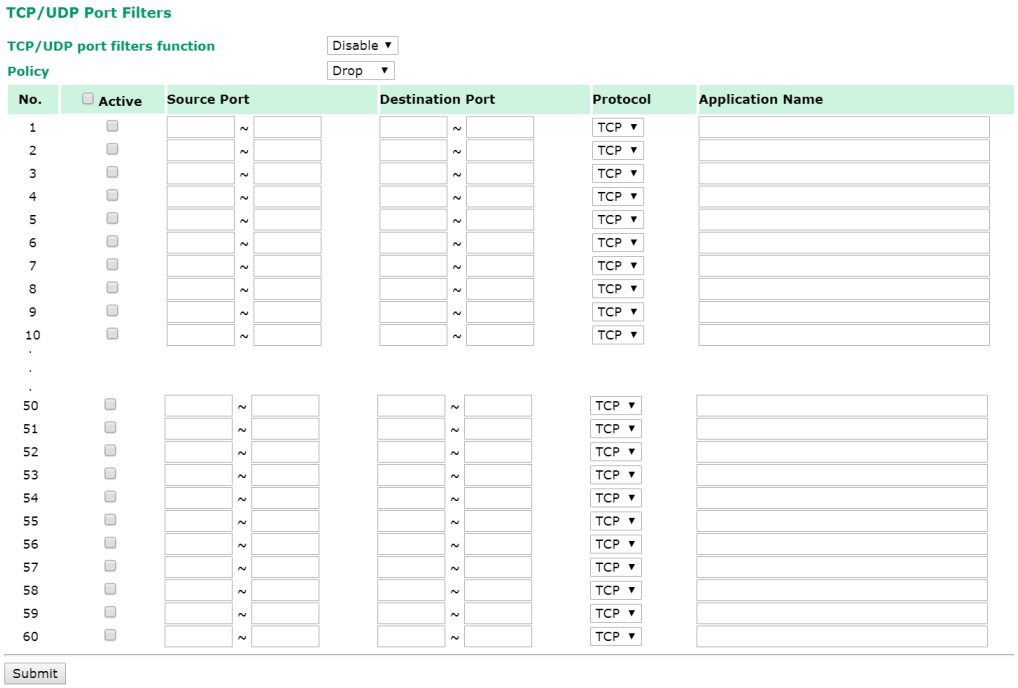
Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed.**
Accept + "no entity on list is activated" = all packets are **denied.**

TCP/UDP Port Filters

The AWK-4131A's TCP/UDP port filter is a policy-based filter that can allow or filter out TCP/UDP-based packets with a specified source or destination port.

The AWK-4131A provides 60 entities for setting the range of source/destination ports of a specific protocol. In addition to selecting TCP or UDP protocol, you can set either the source port, destination port, or both. The end port can be left empty if only a single port is specified. Of course, the end port cannot be larger than the start port.

The **Application name** is a text string that describes the corresponding entity with up to 31 characters. Remember to check the **Active** check box for each entity to activate the setting.



TCP/UDP port filters

Setting	Description	Factory Default
Enable	Enables TCP/UDP port filters.	Disable
Disable	Disables TCP/UDP port filters.	

Policy

Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Accept
Drop	Any packet fitting the entities on list will be denied.	

ATTENTION

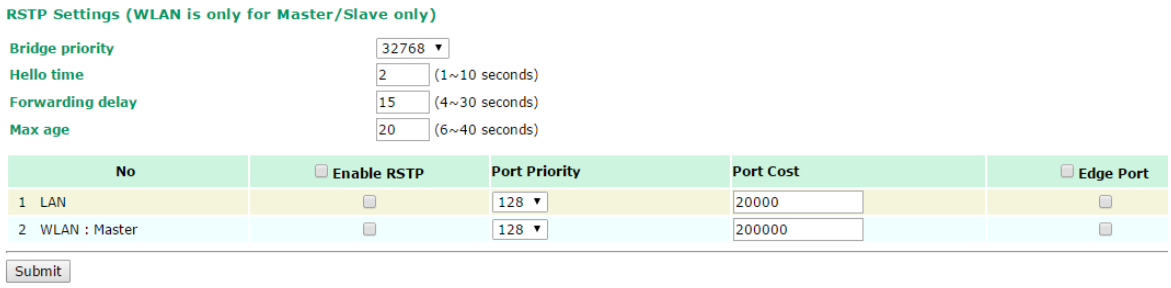
Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed**
Accept + "no entity on list is activated" = all packets are **denied**

RSTP Settings (Master/Slave mode only)

AWK-4131A supports IEEE 802.1D for Spanning Tree Protocol (STP) and IEEE 802.1w for Rapid STP standards. In addition to eliminating unexpected path looping, STP/RSTP can provide a backup path recovery if a wired/ wireless path fails accidentally. The reliability and availability can increase because this fail-over function.

AWK-4131A's STP/RSTP feature is disabled by default. To be completely effective, you must enable RSTP/STP on every AWK-4131A connected to your network. If AWK-4131A plays a **Slave** role, which is connected to a device (PLC, RTU, etc.) as opposed to network switch equipment, it is not necessary to enable STP/RSTP. The reason is that it will cause unnecessary negotiation. AWK-4131As support STP/RSTP in **Master/Slave mode** only.

The following figures indicate which Spanning Tree Protocol parameters can be configured. A more detailed explanation of each parameter is given below the figure.



RSTP status

This field will appear only when selected to operate STP/RSTP. It indicates whether this AWK-4131A is the Root of the Spanning Tree (the root is determined automatically) or not.

Bridge priority

Setting	Description	Factory Default
Numerical value selected by user	You can increase the bridge priority by selecting a lower number. A higher bridge priority brings a greater chance of being established as the root of the Spanning Tree topology.	32768

Hello time

Setting	Description	Factory Default
Numerical value input by user (1 – 10 seconds)	The root of the Spanning Tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is healthy. Hello time indicates how often the root sends hello messages.	2 (seconds)

Forwarding delay

Setting	Description	Factory Default
Numerical value input by user (4 to 30 seconds)	The amount of time this device waits before checking to see if it should change to a different topology.	15 (seconds)

Max. age

Setting	Description	Factory Default
Numerical value input by user (6 to 40 seconds)	When it is in a non-root role, if the device has not received a hello message from the root for a time longer than Max. age, it will reconfigure itself as a root. Once two or more devices on the network are recognized as a root, the devices will renegotiate to set up a new Spanning Tree topology.	20 (seconds)

Enable RSTP

Setting	Description	Factory Default
Enable/Disable	Enables or disables the port as a node on the Spanning Tree topology.	Disable (unchecked)

Port priority

Setting	Description	Factory Default
Numerical value selected by user	Increase this port's priority as a node on the Spanning Tree topology by inputting a lower number.	128

Port cost

Setting	Description	Factory Default
Enable/Disable	Input a higher cost to indicate that this port is less suitable as a node for the Spanning Tree topology.	20000(LAN)

Edge port

Setting	Description	Factory Default
Checked/Unchecked	Sets a port, which no BPDU expectedly goes through, as an edge port.	Unchecked, except AP port

NOTE We recommend you set an edge port for the port, which is connected to a non-STP/RSTP sub-network or an end device (PLC, RTU, etc.) as opposed to network equipment. This can prevent unnecessary waiting and negotiation of STP/RSTP protocol, and accelerate system initialization. When an edge port receives BPDUs, it can still function as an STP/RSTP port and start negotiation.

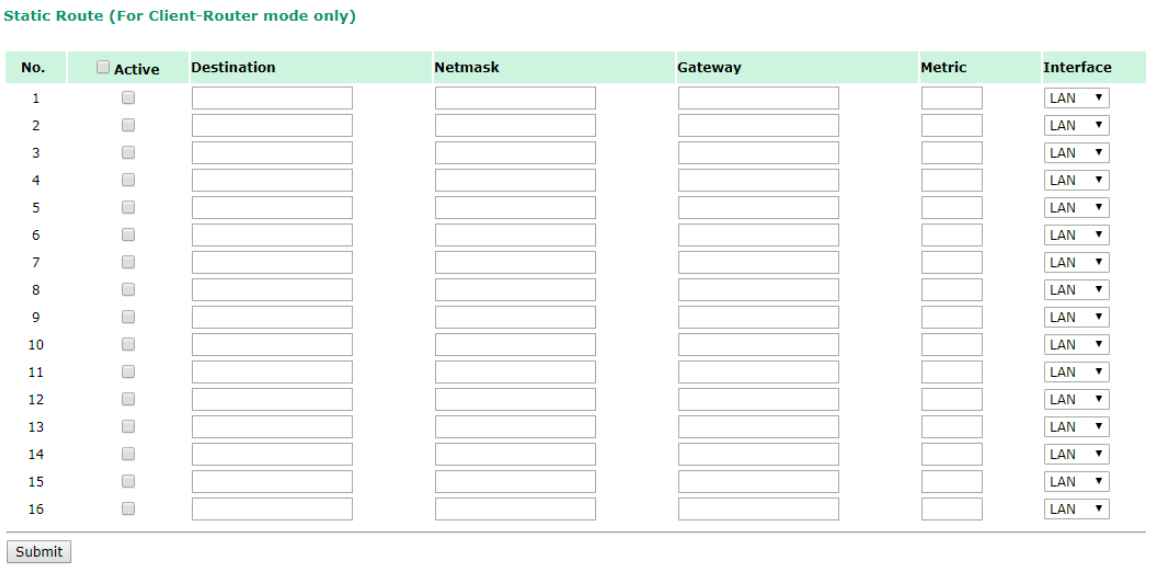
Setting an edge port is different from disabling STP/RSTP on a port. If you disable STP/RSTP, a port will not deal with STP/RSTP BPDUs at all.

Port Status

Port Status indicates the current Spanning Tree status of this port. Use **Forwarding** for normal transmission, or **Blocking** to block transmission.

Static Route (Client-Router mode only)

The Static Route page is used to configure the AWK-4131A's static routing table.



Active

Click the checkbox to enable Static Routing.

Destination

Specifies the destination IP address.

Netmask

Specifies the subnet mask for this IP address.

Gateway

Specifies the IP address of the router that connects the LAN to an outside network.

Metric

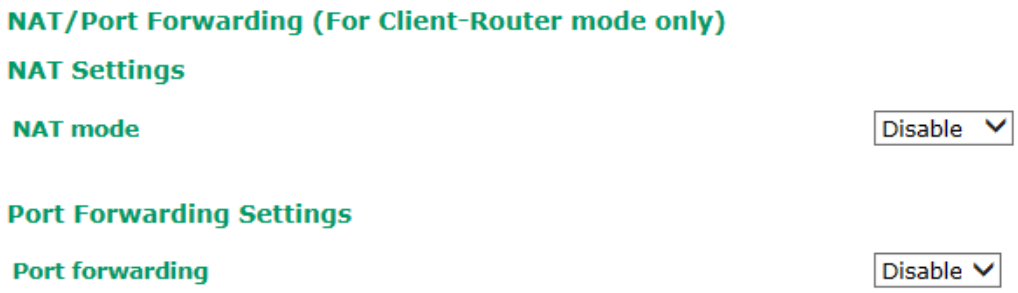
Specifies a "cost" for accessing the neighboring network.

Interface

Specifies the designated network interface for this routing rule.

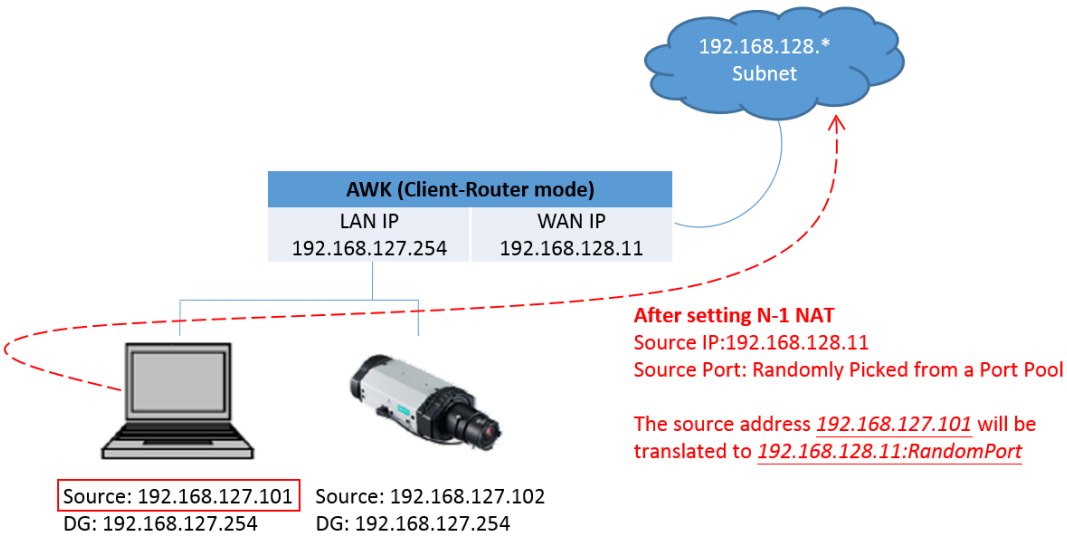
NAT Settings/Port Forwarding (for Client-router mode only)

Network Address Translation (NAT) and Port Forwarding is supported in the AWK-4131A to facilitate the Client-Router operation mode. This feature translates the outgoing communication from private IPs to external IPs (WAN IP).

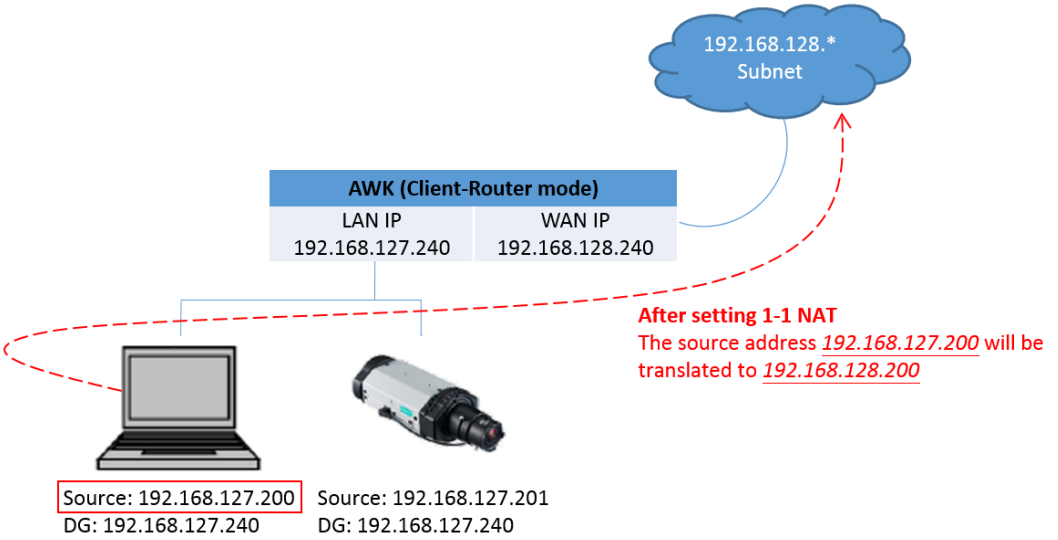


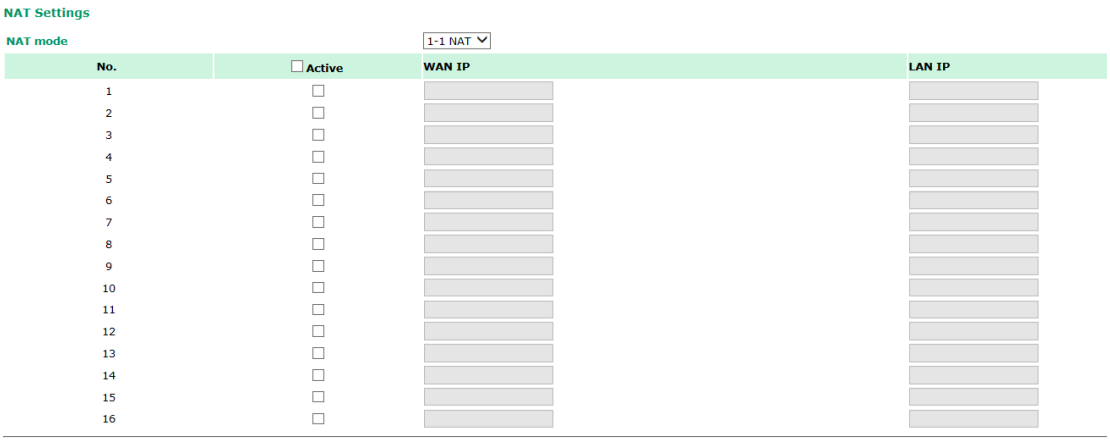
Setting	Description	Factory Default
NAT mode	Enable (N-1 NAT or 1-1 NAT) or disable the NAT mode.	Disable
Port Forwarding	Enable or disable the port forwarding function	Disable

N-1 NAT



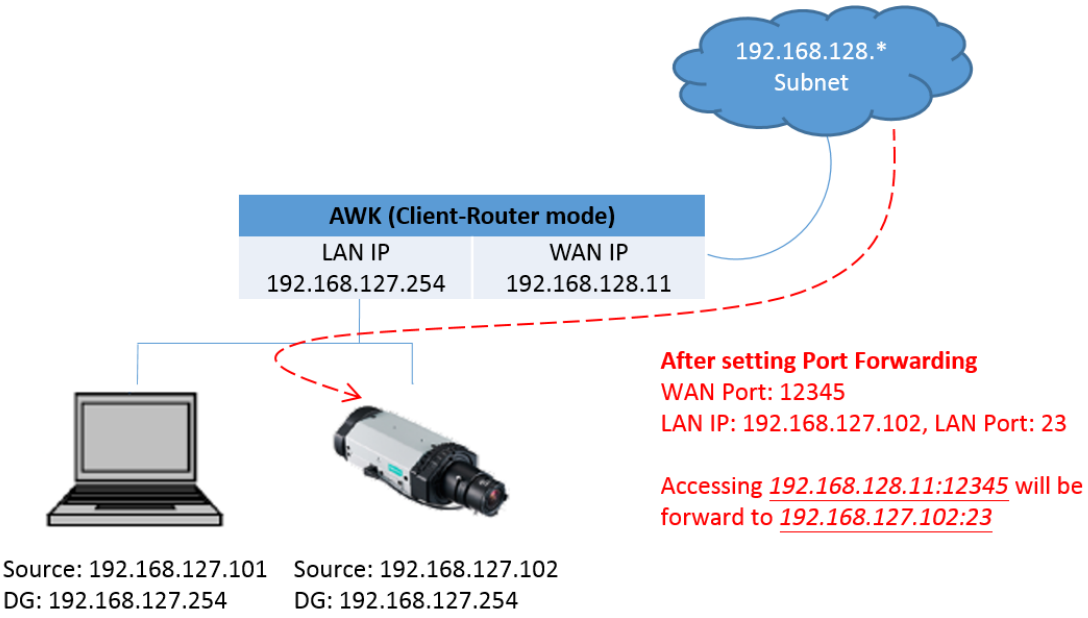
1-1 NAT

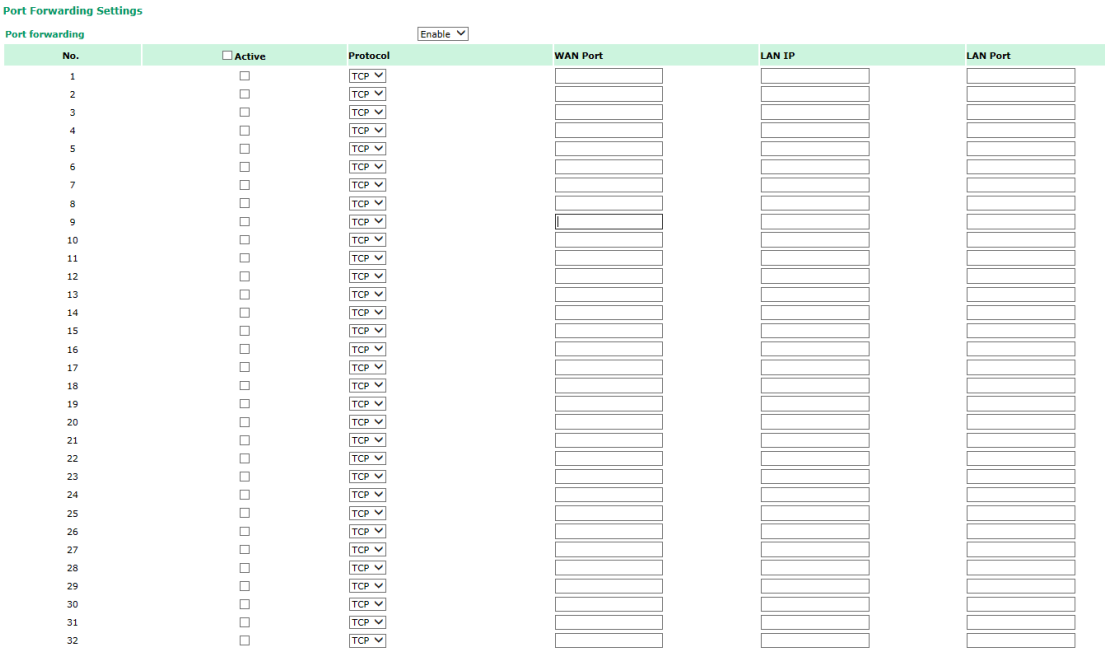




Setting	Description
Active	Click the checkbox to enable 1-1 NAT
WAN IP	Specifies the "forward to" WAN IP
LAN IP	Specifies the "forward to" LAN IP

Port Forwarding





Setting	Description
Active	Click the checkbox to enable Port Forwarding rule(s).
Protocol:	Specifies the communication protocol.
WAN Port	Specifies the external port to be forwarded to
LAN IP	Specifies the "forward to" LAN IP
LAN Port	Specifies the "forward to" LAN Port

In order to allow external devices to initiate the communication, Port Forwarding is used to specify a static map between external ports (WAN Port) and internal IP/port combos (LAN IP/LAN Port), so as to allow external devices to initiate connection with this device.

SNMP Agent

The AWK-4131A supports SNMP V1/V2c/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 community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

SNMP security modes and security levels supported by the AWK-4131A are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
SNMP V1, V2c	V1, V2c Read Community	Community string	No	Use a community string match for authentication.
	V1, V2c Write/Read Community	Community string	No	Use a community string match for authentication.
SNMP V3	No-Auth	No	No	Use account with admin or user to access objects.
	MD5 or SHA	Authentication based on MD5 or SHA	No	Provides 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	Provides authentication based on HMAC-MD5 or HMAC-SHA algorithms, and data encryption key. 8-character passwords and a data encryption key are the minimum requirements for authentication and encryption.

The following parameters can be configured on the **SNMP Agent** page. A more detailed explanation of each parameter is given below the following figure.

SNMP agent

Setting	Description	Factory Default
Enable	Enables SNMP agent.	Disable
Disable	Disables SNMP agent.	

Remote management

Setting	Description	Factory Default
Enable	Allow remote management via SNMP agent.	Disable
Disable	Disallow remote management via SNMP agent.	

Read community (for V1, V2c)

Setting	Description	Factory Default
V1, V2c Read Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can access all objects with read-only permissions using this community string.	public

Write community (for V1, V2c)

Setting	Description	Factory Default
V1, V2c Read /Write Community	Use a community string match with a maximum of 31 characters for authentication. This means that the SNMP agent can accesses all objects with read/write permissions using this community string.	private

SNMP agent version

Setting	Description	Factory Default
V1, V2c, V3, or V1, V2c, or V3 only	Select the SNMP protocol version used to manage the switch.	V1, V2c

Admin auth type (for V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
No Auth	Use admin account to access objects. No authentication.	No Auth
MD5	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	
SHA	Provides authentication based on HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	

Admin private key (for V1, V2c, V3, and V3 only)

Setting	Description	Factory Default
Disable	No data encryption.	Disable
DES	DES-based data encryption.	
AES	AES-based data encryption.	

Private key

A data encryption key is the minimum requirement for data encryption (maximum of 63 characters)

Private MIB Information Device Object ID

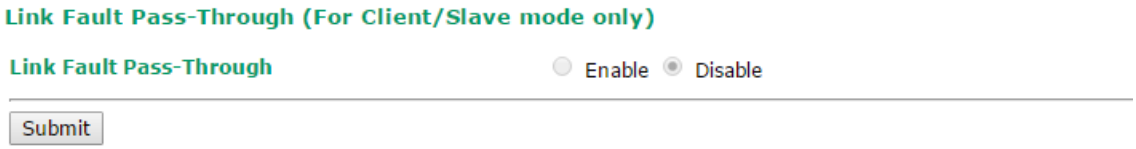
Also known as ***OID***. This is the AWK-4131A's enterprise value. It is fixed.

Link Fault Pass-through (Client/Slave mode only)

This function means if Ethernet port is link down, wireless connection will be forced to disconnect. Once Ethernet link is recovered, AWK will try to connect to AP.

If wireless is disconnected, AWK restarts auto-negotiation on Ethernet port but always stays in the link failure state. Once the wireless connection is recovered, AWK will try to recover the Ethernet link.

System log will indicate the link fault pass through events in addition to the original link up/down events.



Link Fault Pass-Through

Setting	Description	Factory Default
Enable	Enables Link Fault Pass-Through.	Disable
Disable	Disables Link Fault Pass-Through.	

NOTE Auto MAC Cloning cannot be used together with Link Fault Pass Through.

Logs and Notifications

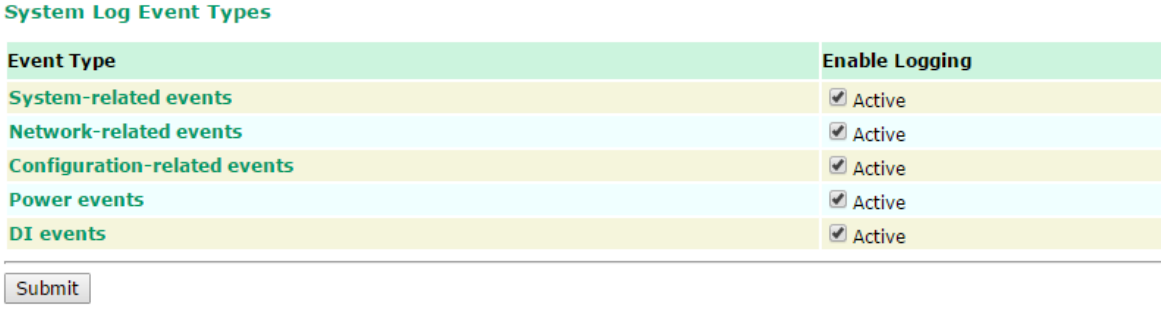
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system administrators are out of the control room for an extended period, they can still be informed of the status of devices almost instantaneously when exceptions occur.

In addition to logging these events, the AWK-4131A supports different approaches to warn engineers automatically, such as SNMP trap, e-mail, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Logs

System Log Event Types

Detailed information for grouped events is shown in the following table. Check the box for **Enable logging** to enable the grouped events. All default values are enabled (checked). The log for system events can be seen in **Status → System Logs**.



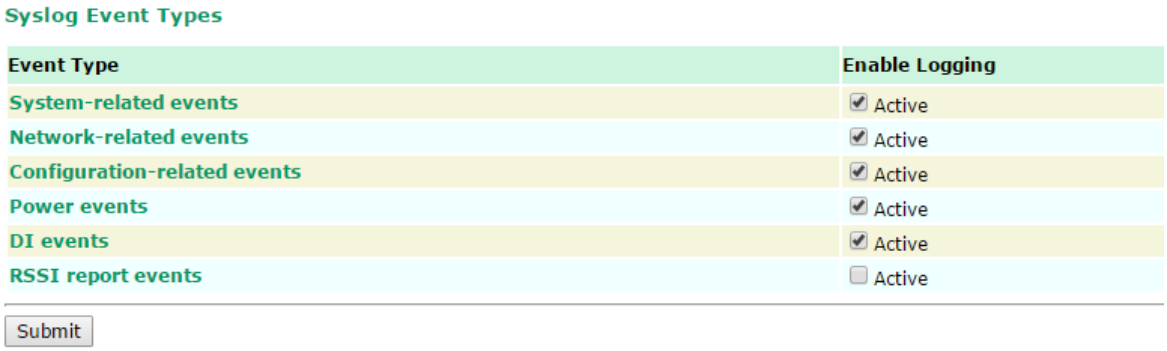
System-related events	Event is triggered when…
System warm start	The AWK-4131A is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
System cold start	The AWK-4131A is rebooted by power down.
Watchdog triggers reboot	The AWK-4131A is rebooted by watchdog.
Network-related events	**Event is triggered when…**
LAN link on	The LAN port is connected to a device or network.
LAN link off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).
Client joined/ left (for AP/Master mode)	A wireless client is associated or disassociated.
WLAN connected to AP (for Client/Slave mode)	The AWK-4131A is associated with an AP.
WLAN disconnected (for Client/Slave mode)	The AWK-4131A is disassociated from an AP.
RSTP changed	The RSTP topology has changed
RSTP new root bridge ID	The RSTP changes its root bridge ID
Client Roaming from previous AP to current AP (for Client/Slave mode)	A client roams from a previous AP to the current AP if the signal strength of the current AP is greater than the previous AP by a certain value.
IP address conflict	The AWK-4131A has the same IP address as another device connected to the same subnet.
Link fault pass-through LAN/WLAN connected because of WLAN/LAN up	The WLAN/LAN link is up and the Link fault pass-through (LFPT) enables the LAN/WLAN functionality.
Link fault pass-through LAN/WLAN disconnected because of WLAN/LAN down	The WLAN/LAN link is down and the Link fault pass-through (LFPT) disables the LAN/WLAN functionality.
Channel availability check over DFS frequency (for AP/Master mode)	The channel availability check (CAC) is started on channel [channel] at [frequency] GHz for 60 sec./ The channel availability check (CAC) task has been completed on channel [channel] at [frequency] GHz./ A radar signal is detected on channel [channel] at [frequency] GHz.
AeroLink protection state	The AeroLink protection state changes. AeroLink states: Initialize (init)/ Discovery/ Idle/ Negotiation (nego)/ Back up/ Active/ Changed/ Undefined (undef)
Configuration-related events	**Event is triggered when…**
Configuration Changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the AWK-4131A.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The AWK-4131A's firmware is updated.
Loaded the configuration from ABC-01	The configuration is successfully loaded/there is an error loading the configuration from ABC-01.
Saving configuration to ABC-01	The configuration is successfully saved/there is an error saving the configuration to ABC-01.
ABC-01 failure	AWK-4131A cannot detect an ABC-01 at the console port.
Configuration reset to default	The configuration is reset to factory default.
Power events	**Event is triggered when…**
Power 1/2 transition (On -> Off)	The AWK-4131A is powered down in PWR1/2.
PoE transition (On -> Off)	The AWK-4131A is powered down in PoE.
Power 1/2 transition (Off -> On)	The AWK-4131A is powered via PWR1/2.
PoE transition (Off -> On)	The AWK-4131A is powered via PoE.

Syslog

This function provides the event logs for the Syslog server. The function supports up to three configurable Syslog servers and Syslog server UDP port numbers. When an event occurs, the event will be sent as a Syslog UDP packet to the specified Syslog servers.

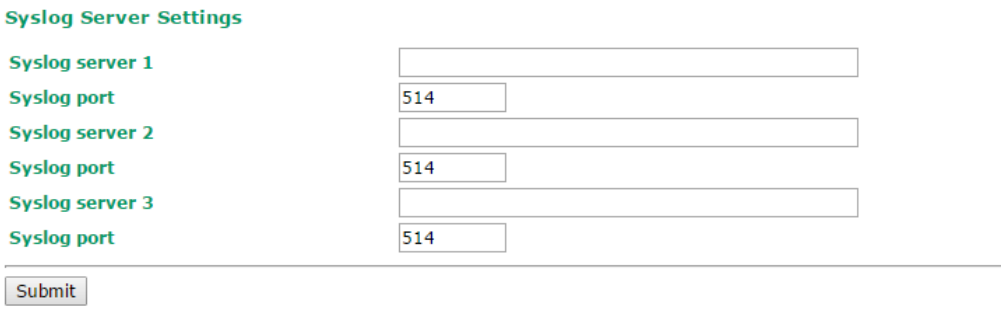
Syslog Event Types

Detailed information for the grouped events is shown in the following table. Check the box for **Enable logging** to enable the grouped events. All default values are enabled (checked). Detail for each event group is available in the **System Log Event Types** section.



Syslog Server Settings

You can configure the parameters for your Syslog servers in this page.



Syslog server 1/ 2/ 3

Setting	Description	Factory Default
IP address	Enter the IP address of the 1st/ 2nd/ 3rd Syslog Server.	None

Syslog port

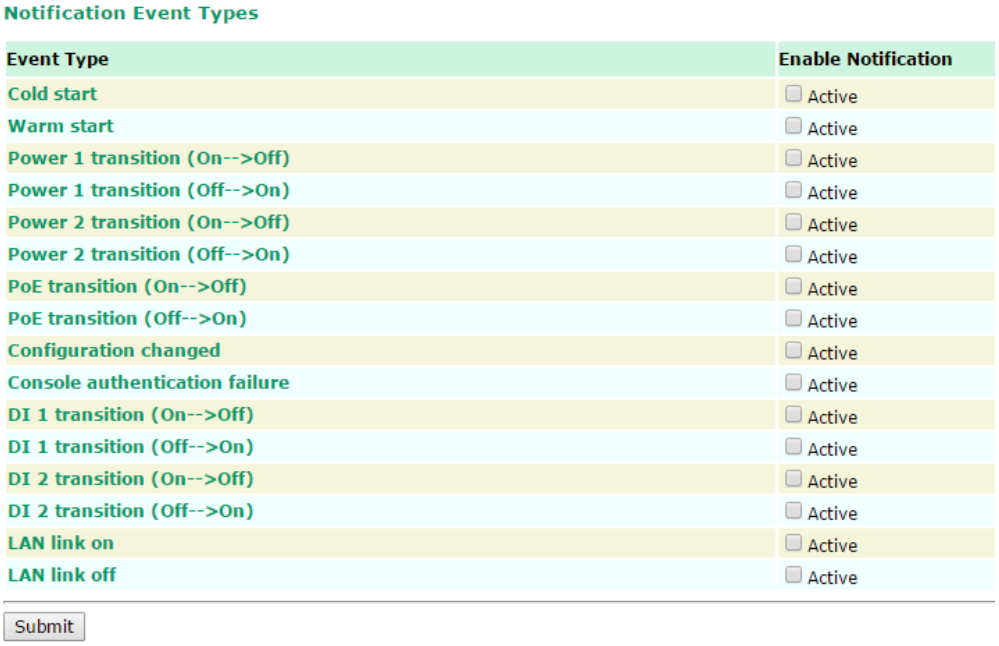
Setting	Description	Factory Default
Port destination (1 to 65535)	Enter the UDP port of the corresponding Syslog server.	514

NOTE The **RSSI report events (Only for Client mode)** function is useful during the site survey stage and needs to use a special Utility to retrieve the RSSI values as a table. However, this function increases the traffic load, so we recommend setting this function to **disable** during normal usage.

E-mail Notifications

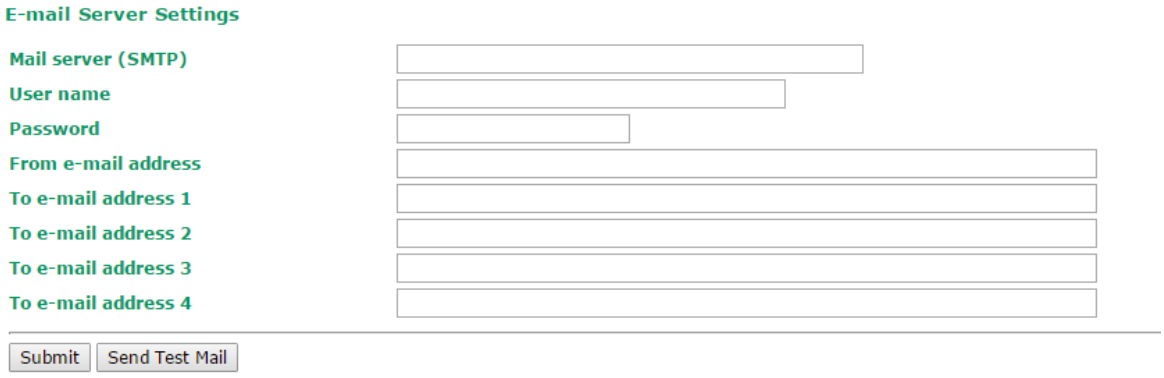
Notification Event Types

Check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Detail for each event group is available in the **System Log Event Types** section.



E-mail Server Settings

You can set up to 4 e-mail addresses to receive alarm emails from the AWK-4131A. The following parameters can be configured on the **E-mail Server Settings** page. In addition, a **Send Test Mail** button can be used to test whether the Mail server and e-mail addresses work well. More detailed explanations about these parameters are given after the following figure.



Mail server (SMTP)

Setting	Description	Factory Default
IP address	The IP Address of your email server.	None

User name & Password

Setting	Description	Factory Default
	User name and password used in the SMTP server.	None

From e-mail address

Setting	Description	Factory Default
Max. 63 characters	Enter the administrator's e-mail address which will be shown in the "From" field of a warning e-mail.	None

To E-mail address 1/ 2/ 3/ 4

Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' e-mail addresses.	None

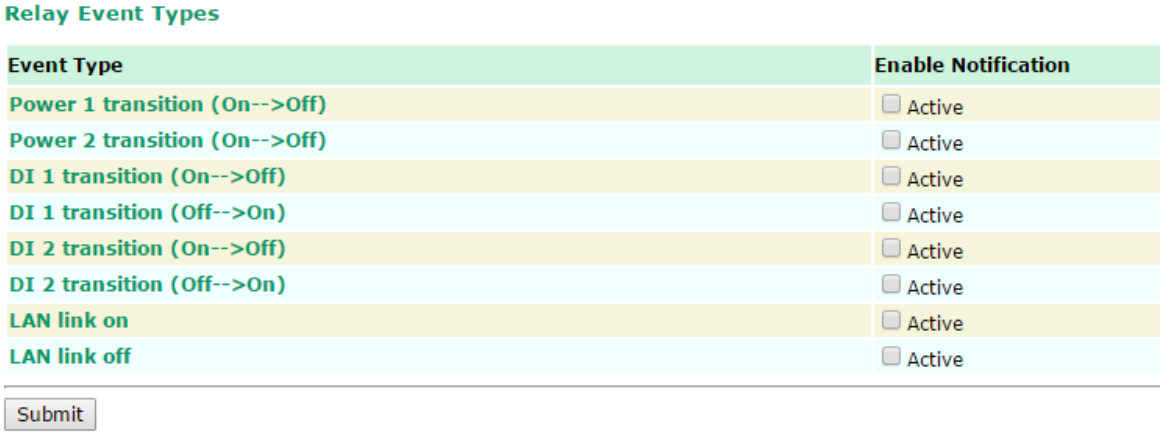
Relay

The AWK-4131A has one relay output, which consists of 2 terminal block contacts on the AWK-4131A's top panel. These relay contacts are used to indicate user-configured events and system failure.

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 AWK-4131A is not powered.

Relay Event Types

You can check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Detail for each event group is available in the **System Log Event Types** section.

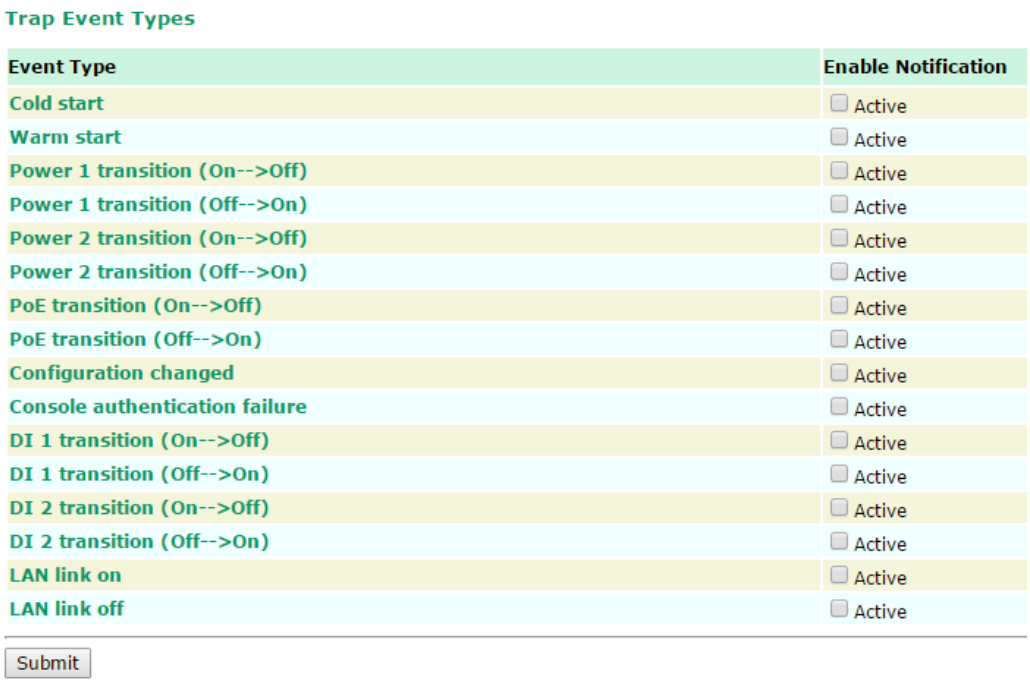


Trap

Traps can be used to signal abnormal conditions (notifications) to a management station. This trap-driven notification can make your network more efficient.

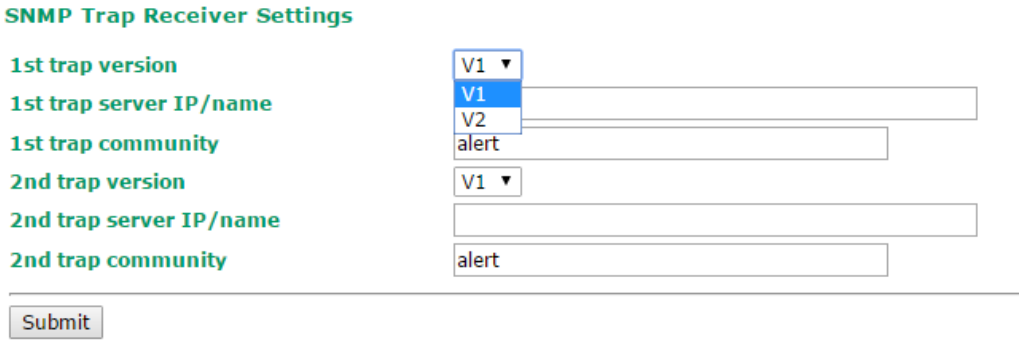
Because a management station usually takes care of a large number of devices that have a large number of objects, it will be overloading for the management station to poll or send requests to query every object on every device. It would be better if the managed device agent could notify the management station by sending a message known as a trap for the event.

Trap Event Types



SNMP Trap Receiver Settings

SNMP traps are defined in SMIv1 MIBs (SNMPv1) and SMIv2 MIBs (SNMPv2c). The two styles are basically equivalent, and it is possible to convert between the two. You can set the parameters for SNMP trap receivers through the web page.



1st / 2nd trap version

Setting	Description	Factory Default
V1	SNMP trap defined in SNMPv1	V1
V2	SNMP trap defined in SNMPv2	

1st / 2nd trap server IP/name

Setting	Description	Factory Default
IP address or host name	Enter the IP address or name of the trap server used by your network.	None

1st / 2nd trap community

Setting	Description	Factory Default
Max. of 31 characters	Use a community string match with a maximum of 31 characters for authentication.	Alert

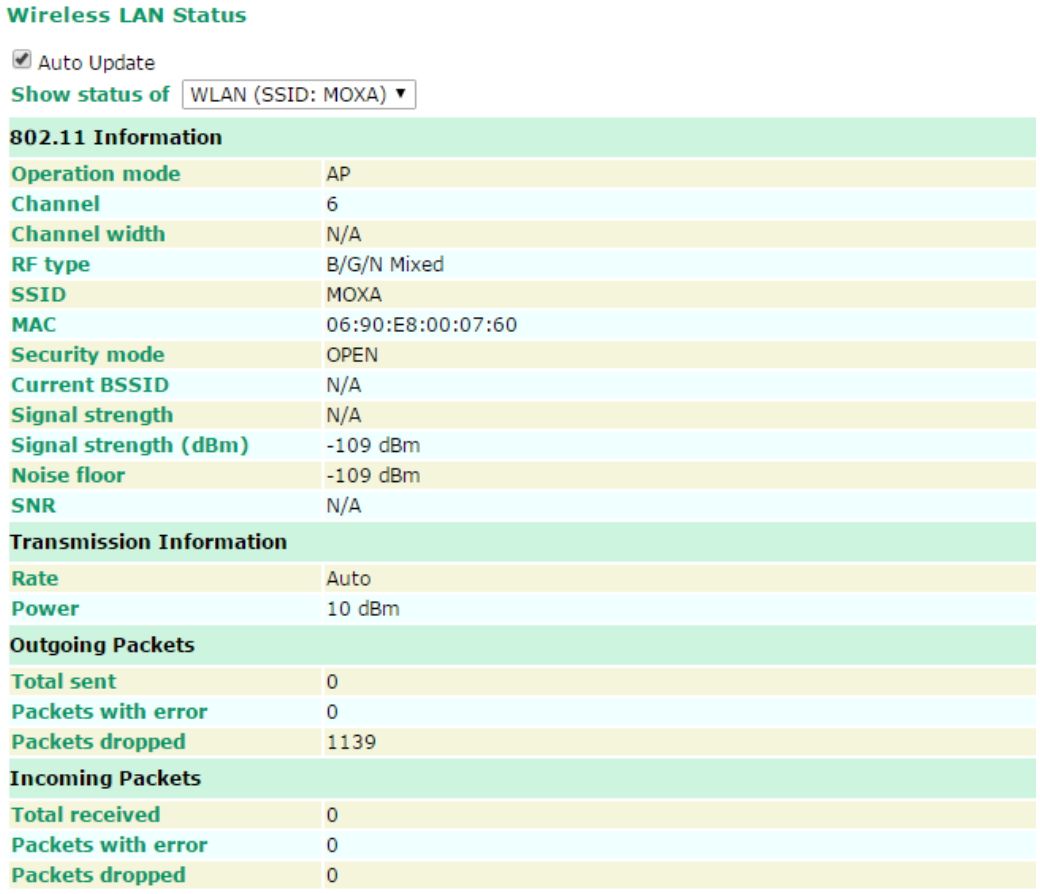
Status

Wireless LAN Status

The status for **802.11 Information** parameters, such as Operation mode and Channel, are shown on the **Wireless Status** page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

Certain values for **802.11 Information** may not show up due to different operation modes. As a result, **Current BSSID, Signal strength,** and **SNR** are not available in AP mode.

It is helpful to use the continuously updated information on this page, such as **Signal strength, Noise floor,** and **SNR**, to monitor the signal strength of the AWK-4131A in Client mode.



Wireless LAN Status

Auto Update

Show status of WLAN (SSID: MOXA)

802.11 Information	
Operation mode	AP
Channel	6
Channel width	N/A
RF type	B/G/N Mixed
SSID	MOXA
MAC	06:90:E8:00:07:60
Security mode	OPEN
Current BSSID	N/A
Signal strength	N/A
Signal strength (dBm)	-109 dBm
Noise floor	-109 dBm
SNR	N/A
Transmission Information	
Rate	Auto
Power	10 dBm
Outgoing Packets	
Total sent	0
Packets with error	0
Packets dropped	1139
Incoming Packets	
Total received	0
Packets with error	0
Packets dropped	0

Associated Client List (for AP/Master mode only)

The Associated Client List shows all the clients that are currently associated with a particular AWK-4131A. This page provides useful information for easier network diagnosis:

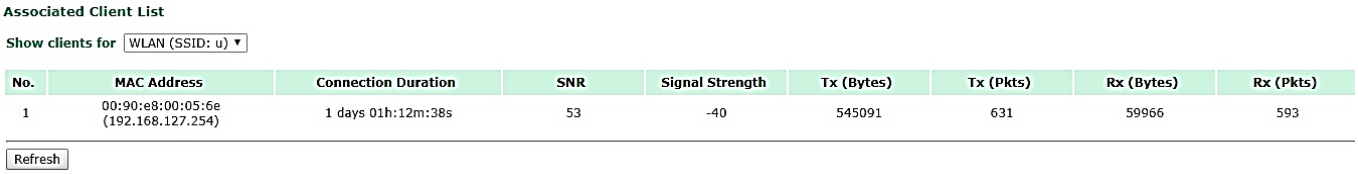
MAC Address: Displays the associated client MAC address. If DHCP server is enabled on this AP/Master, the IP address will also be displayed.

Connection Duration: States how long the client has been connecting to this AP/Master.

SNR: States the Signal-Noise Ratio of the associated client. This is especially useful for identifying a weak signal client that is potentially reducing the overall wireless performance.

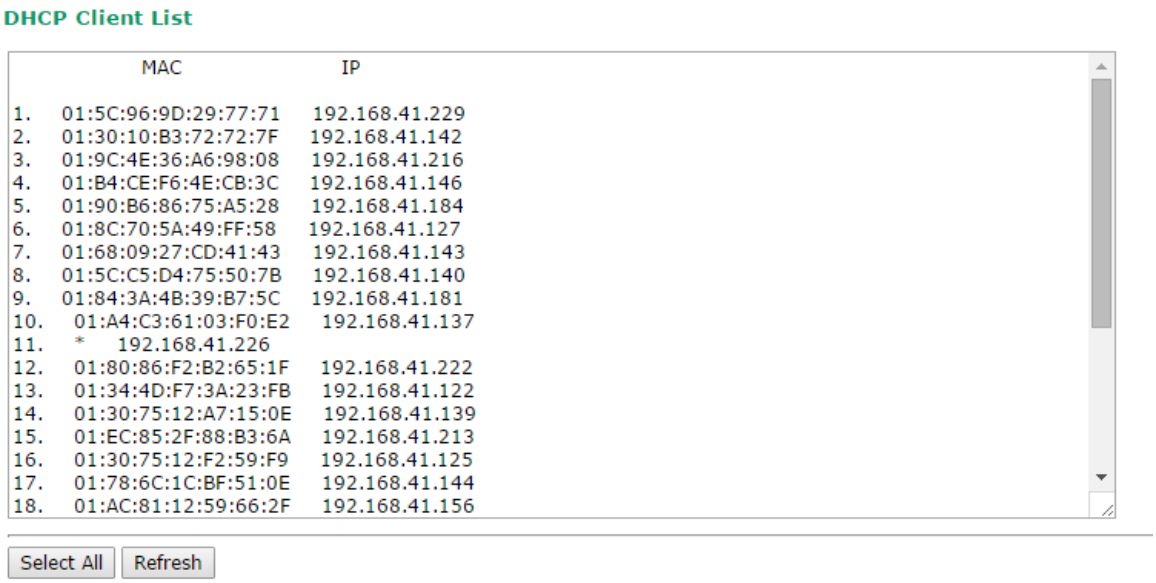
Tx (Bytes/Pkts): Records the AP-to-client traffic after a client is associated.

Rx (Bytes/Pkts): Records the client-to-AP traffic after a client is associated.

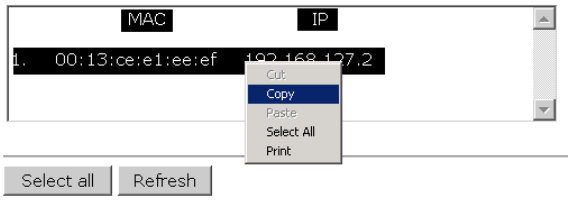


DHCP Client List (for AP mode only)

The DHCP Client List shows all the clients that require and have successfully received IP assignments. You can click the **Refresh** button to refresh the list.

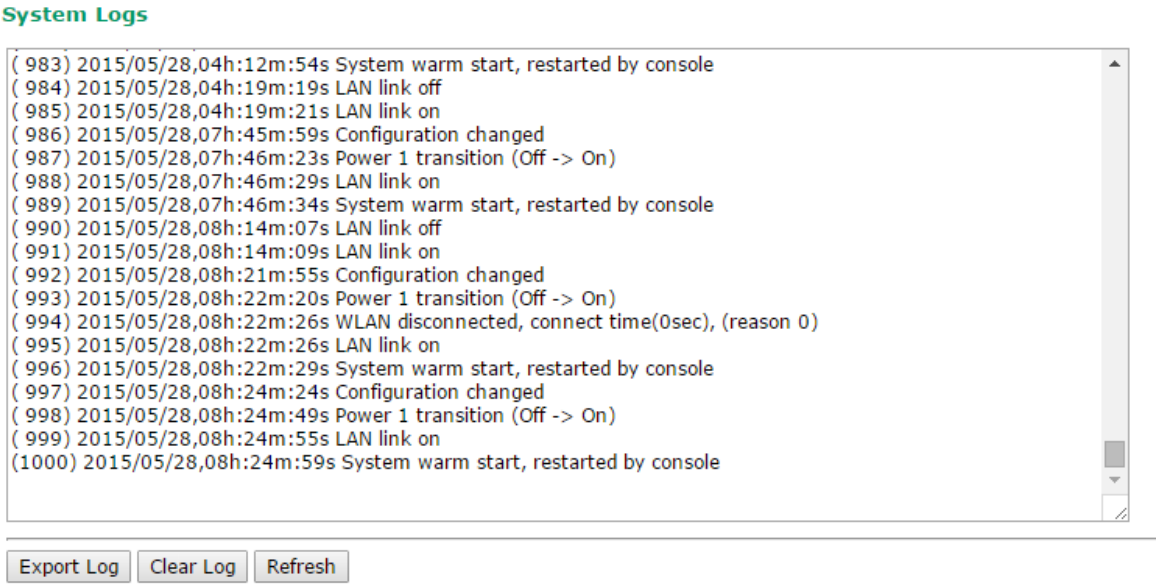


You can press **Select all** button to select all content in the list for further editing.



System Logs

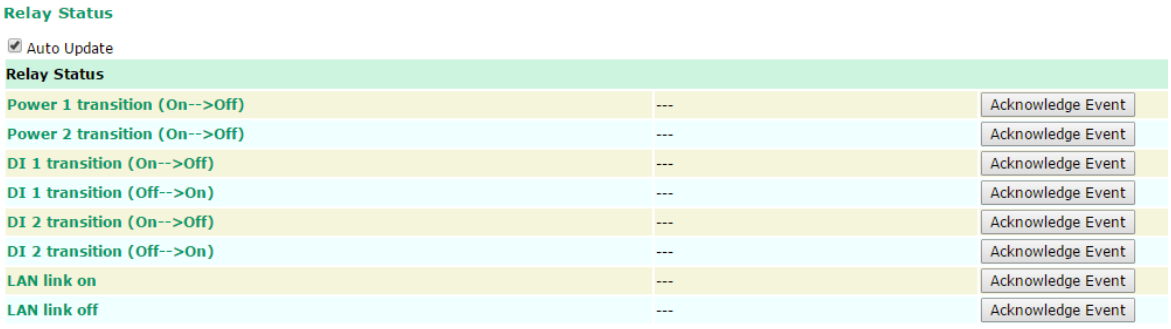
Triggered events are recorded in System Log. You can export the log contents to an available viewer by clicking **Export Log**. You can use the **Clear Log** button to clear the log contents and the **Refresh** button to refresh the log.



Relay Status

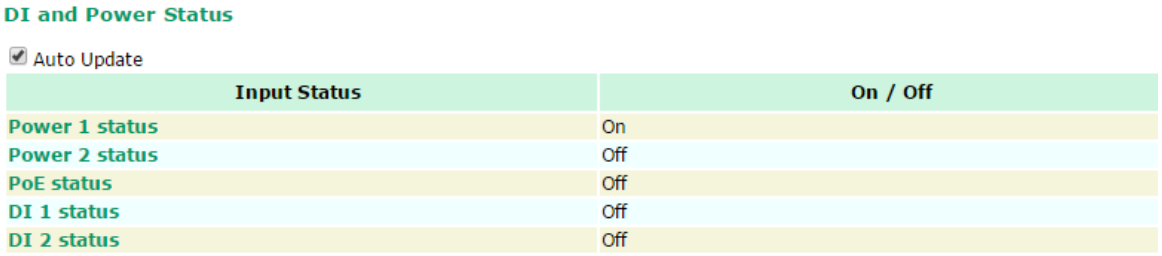
The status of user-configurable events can be found under **Relay Status**. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

If an event is triggered, it will be noted on this list. System administrators can click **Acknowledge Event** when he has acknowledged the event and addressed it.



DI and Power Status

The status of power inputs and digital inputs is shown on this web page. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

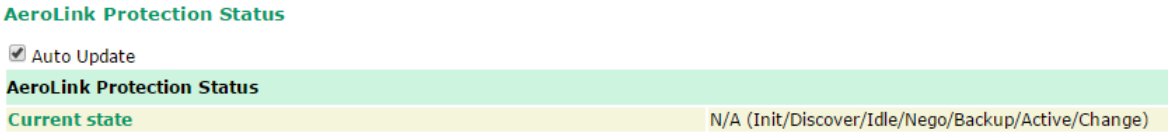

DI and Power Status

Auto Update

Input Status	On / Off
Power 1 status	On
Power 2 status	Off
PoE status	Off
DI 1 status	Off
DI 2 status	Off

AeroLink Protection Status (Client/Slave mode only)

After you have enabled AeroLink Protection in the **Advanced WLAN Setup** panel, the current state of the AeroLink Protection is displayed here for easy diagnosis.


AeroLink Protection Status

Auto Update

AeroLink Protection Status	
Current state	N/A (Init/Discover/Idle/Nego/Backup/Active/Change)

A member of the AeroLink Protection group can take one of the following seven states:

- **Initiation State (Init)**: Initiates the AeroLink Protection Protocol
- **Discovering State (Discover)**: Discovers other AeroLink Protection members for further negotiation
- **Idle State (Idle)**: Internal protocol checkpoint
- **Negotiation State (Nego)**: Negotiates with other AeroLink Protection members and elects an Active node.
- **Backup State (Backup)**: After negotiation, this node is assigned as a Backup node. All traffic will go through the Active node instead.

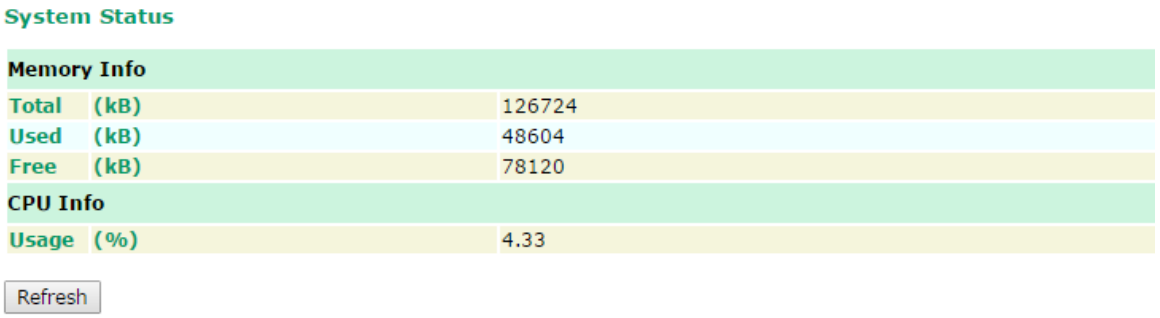
NOTE When a node is in Backup state, the STATE LED will be blinking.

- **Active State (Active)**: After negotiation, this node is assigned as Active node, which means that all traffic will go through this node.
- **Role Change State (Change)**: If the Active node is no longer capable of data transmission via the WLAN, it will turn into Change State to trigger the re-negotiation of the Active node from the Backup nodes.

System Status

The system status section indicates the status of the device memory and CPU usage in the current device.

NOTE A CPU overload can result in a watchdog-triggered reboot of the system. Factors such as a high number of firewall rules (IP/MAC/Protocol filters) and traffic PPS (packet per second) contribute to the rise in CPU usage.

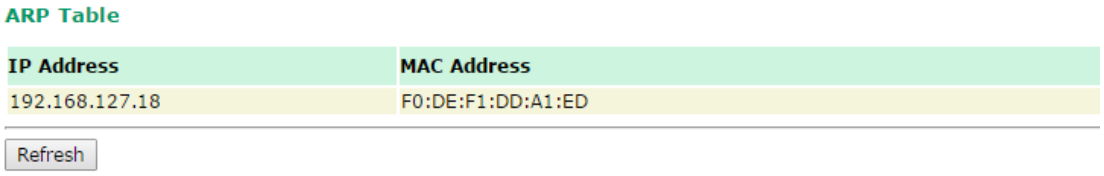


Network Status

The network status section indicates the network status of the device with respect to ARP, bridge status, LLDP, RSTP, and the routing table.

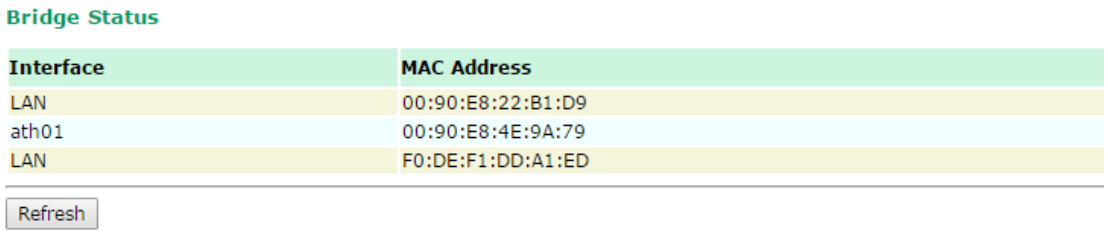
ARP Table

Address Resolution Protocol (ARP) Table - indicates the current IP to MAC address mapping for the device.



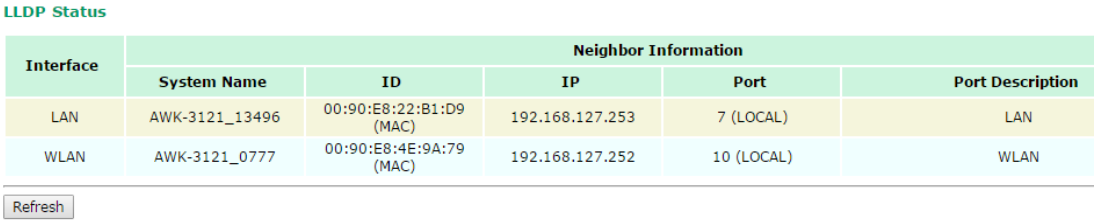
Bridge Status

Indicates the current status of the network bridge on the device. The interfaces and the corresponding MAC addresses in this section are the entry points for ingress traffic.



LLDP Status

Displays information on neighboring devices collected via LLDP (Link Layer Discovery Protocol).

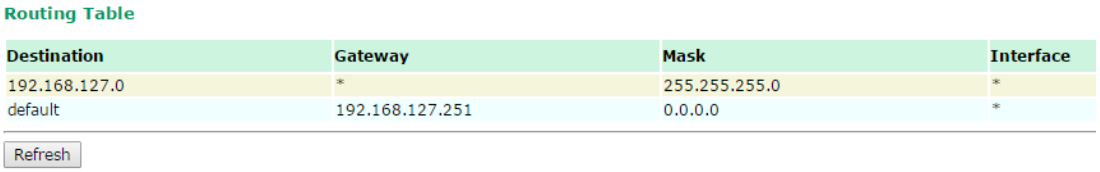

LLDP Status

Interface	Neighbor Information				
	System Name	ID	IP	Port	Port Description
LAN	AWK-3121_13496	00:90:E8:22:B1:D9 (MAC)	192.168.127.253	7 (LOCAL)	LAN
WLAN	AWK-3121_0777	00:90:E8:4E:9A:79 (MAC)	192.168.127.252	10 (LOCAL)	WLAN

Refresh

Routing Table

Displays the routing information for the current device.


Routing Table

Destination	Gateway	Mask	Interface
192.168.127.0	*	255.255.255.0	*
default	192.168.127.251	0.0.0.0	*

Refresh

RSTP Status

Displays the Spanning Tree Protocol parameters configured.

RSTP Status

RSTP status --------
Bridge priority 32768
Hello time 2 seconds
Forwarding delay 15 seconds
Max age 20 seconds

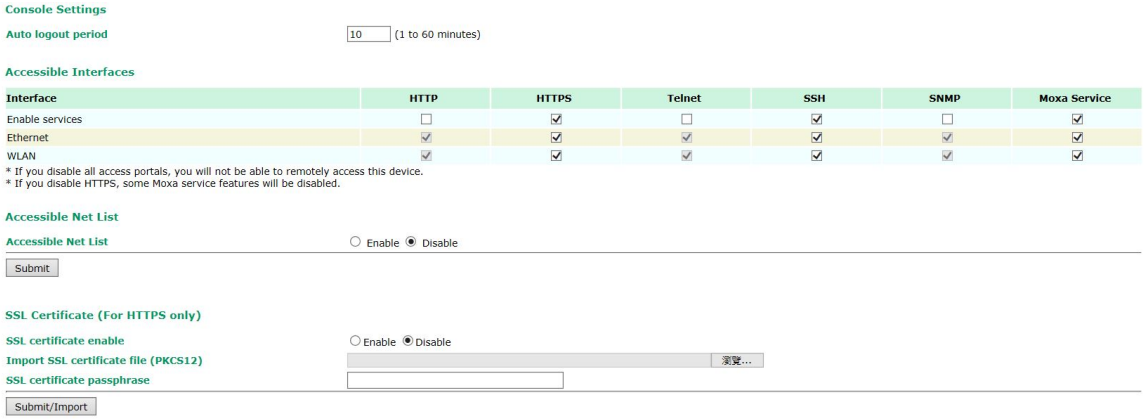
No	Enable RSTP	Port Priority	Port Cost	Edge Port	Status

Maintenance

Maintenance functions provide the administrator with tools to manage the AWK-4131A and wired/wireless networks.

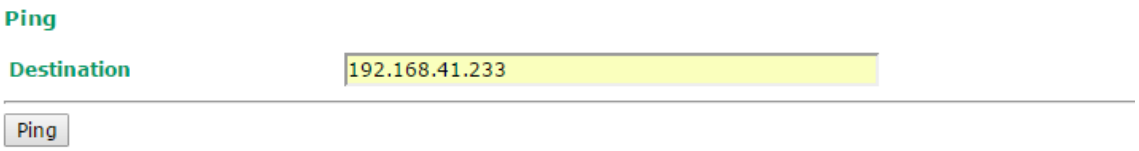
Console Settings

You can enable or disable access permission for the following consoles: HTTP, HTTPS, Telnet, and SSH. For higher security, we recommend that you only allow access to the two secured consoles, HTTPS and SSH.

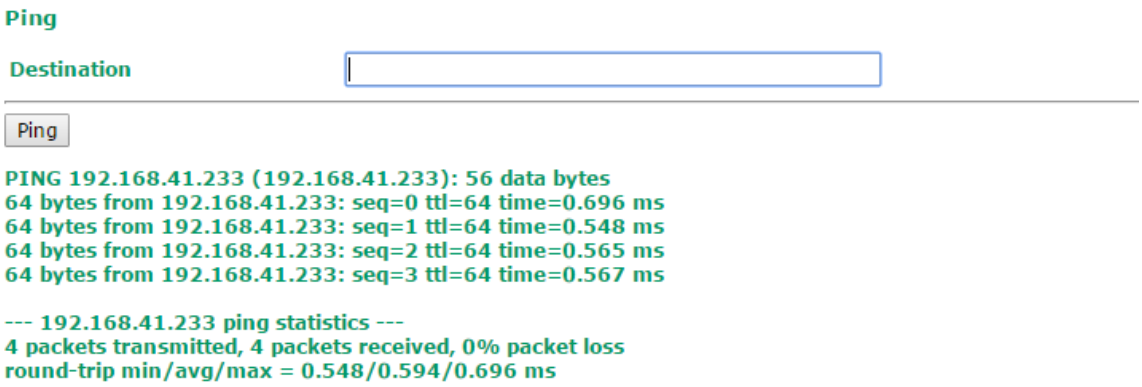


Ping

Ping helps to diagnose the integrity of wired or wireless networks. By inputting a node's IP address in the **Destination** field, you can use the **ping** command to make sure it exists and whether or not the access path is available.



If the node and access path are available, you will see that all packets were successfully transmitted with no loss. Otherwise, some, or even all, packets may get lost, as shown in the following figure.

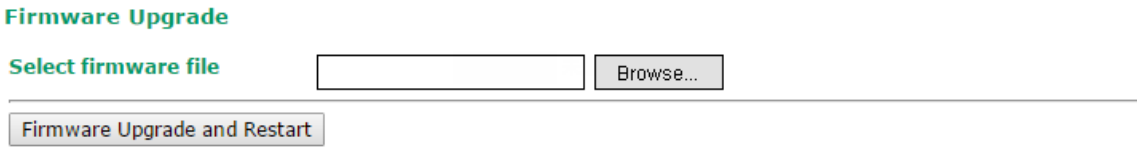


Firmware Upgrade

The AWK-4131A can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available at Moxa's download center.

Before running a firmware upgrade, make sure the AWK-4131A is off-line. Click the **Browse** button to specify the firmware image file and click **Firmware Upgrade and Restart** to start the firmware upgrade. After the progress bar reaches 100%, the AWK-4131A will reboot itself.

When upgrading your firmware, the AWK-4131A's other functions are forbidden.



ATTENTION

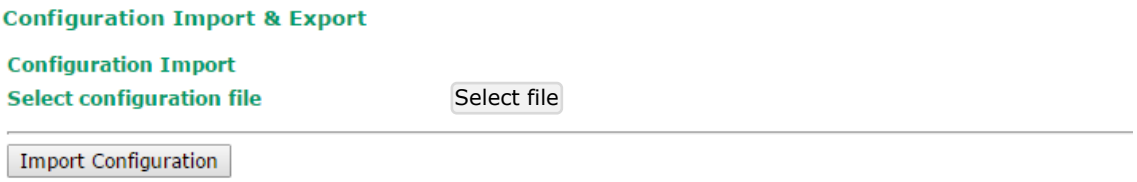
Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your AWK-4131A.

Firmware upgrade may change the current roaming configuration. Please check the roaming configuration of the device after it reboots.

Configuration Import and Export

You can back up or restore the AWK-4131A's configuration using the functions available in the **Configuration Import & Export** section.

In the **Configuration Import** section, click **Browse** to specify the configuration file and click on the **Import Configuration** button to begin importing the configuration.



In the **Configuration Export** section, click the **Export Configuration** button and save the configuration file onto your local storage media. The configuration file is a text file and you can view and edit it with a general text-editing tool.

You can also back up or restore the configuration from an ABC-01 device.

You can use the SNMP MIB File Export section to export your network MIB file.

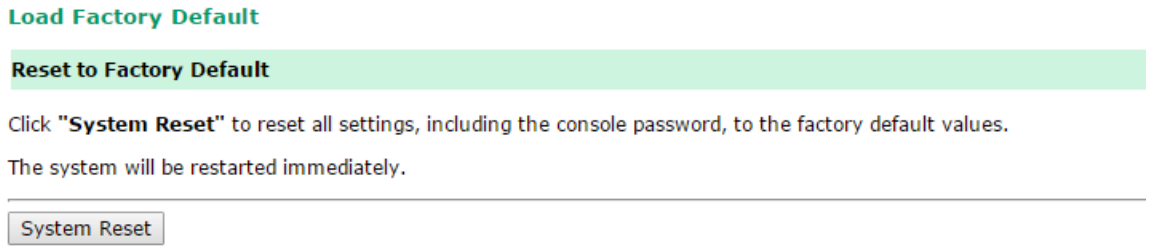
To download the configuration to the AWK device:

1. Power off the AWK.

2. Plug in the ABC-01 to the AWK's RS-232 console.
3. Power on the AWK.
4. AWK will detect the ABC-01 during the boot up process, and download the configuration from the ABC-01 to the AWK automatically. Once the configuration downloads, the AWK will emit three short beeps if the configuration format is correct and will then continue with the boot-up process.
5. Once the AWK has booted up successfully, it will beep two times, and the ready LED will turn a steady green.

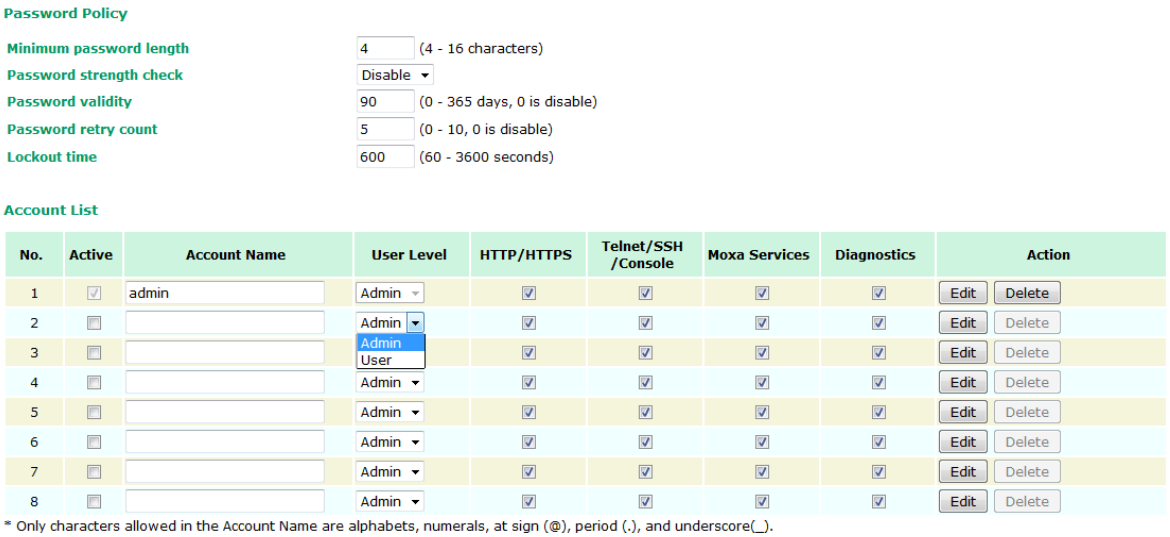
Load Factory Default

Use this function to reset the AWK-4131A and roll back all settings to the factory default values. You can also reset the hardware by pressing the reset button on the top panel of the AWK-4131A.



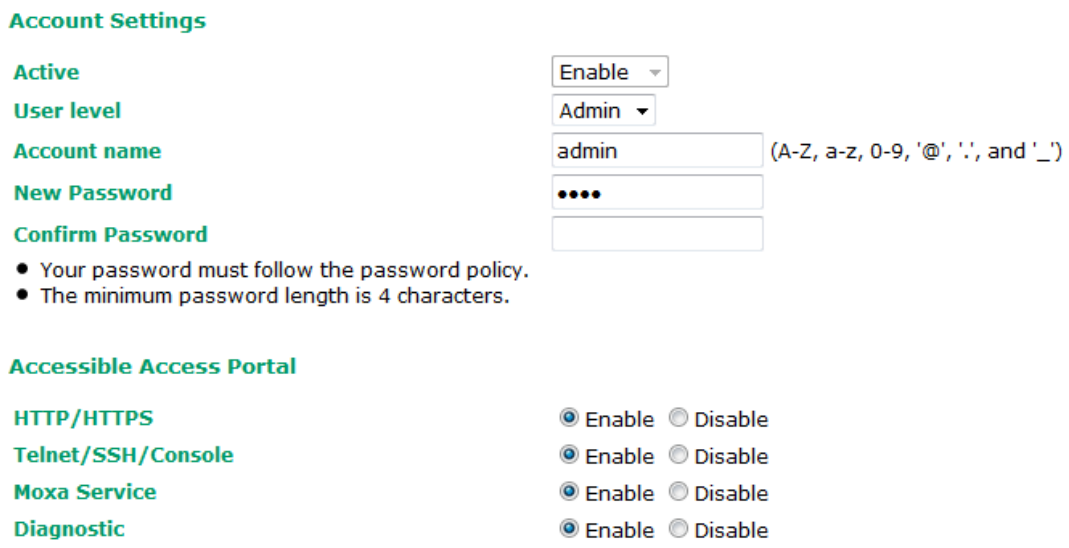
Account Settings

To ensure that devices located at remote sites are secure from hackers, we recommend setting up a high-strength password the first time you configure the device.



Field	Description	Default setting
Minimum password length	By default, passwords can be between 4 and 16 characters. For improved security, we recommend changing the minimum password length to at least 8 characters the first time you configure the device.	4
Password strength check	Enable the password strength check option to ensure that users are required to select high-strength passwords. NOTE: See the **Change Password** section below for details.	Disable
Password validity	The number of days after which the password must be changed. Passwords should be updated regularly to protect against hackers.	90 days
Password retry count	The number of consecutive times a user can enter an incorrect password while logging in before the device's login function is locked.	5
Lockout time	The number of seconds the device's login function will be locked after n consecutive unsuccessful login attempts, where n = the password retry count.	600 seconds

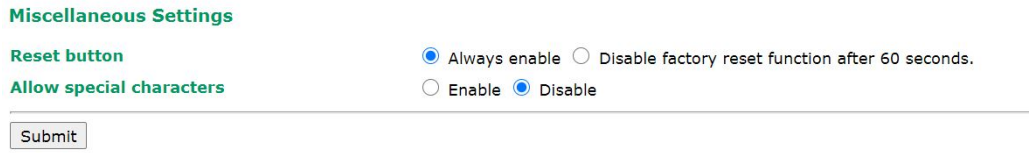
Click **Edit** to create a new, or edit an existing, user account. The items shown below can be configured.



Field	Description	Default Setting
Active	Select Enable to enable the user account.	Disable
User level	Administrator: Allows the user to access the Web UI, change the device's configuration, and use the device's import/export capability. User: Allows the user to access the Web UI, but the user will not be able to change the device's configuration or use the device's import/export capability.	Admin
Account name	The username of the account.	Admin
New Password	The password used to log in to the device.	moxa
Confirm Password	Retype the password. If the Confirm Password and New Password fields do not match, you will be asked to reenter the password.	N/A

Misc. Settings

Additional settings to help you manage your AWK-4131A are available on this page.



Reset button

Setting	Description	Factory Default
Always Enable	The AWK-4131A's Reset button works normally.	Always enable
Disable the Factory Reset Function after 60 Seconds	The AWK-4131A's reset to default function will be inactive 60 seconds after the AWK-4131A finishes booting up.	

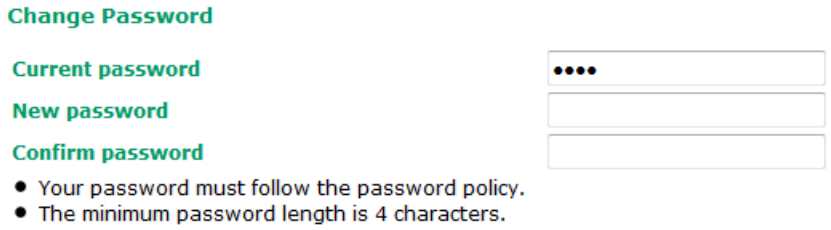
Allow special characters

Setting	Description	Factory Default
Enable/disable	Allow or prohibit the use of special characters (` ' " | ; &). For security reasons, we recommend disabling special characters.	Disable

Changing the Password

Use the **Change Password** function to change the password of existing user accounts. First input the current password, and then type the new password in the **New password** and **Confirm password** input boxes.

NOTE To maintain a higher level of network security, do not use the default password (moxa), and be sure to change all user account passwords regularly.



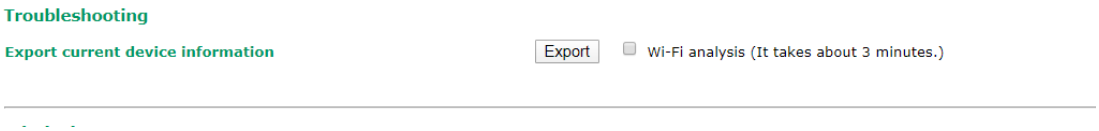
NOTE If the Password-strength test option is enabled, you will be prompted to use passwords that adhere to the following password policy:

- The password must contain at least one digit: 0, 1, 2, …, 9.
- The password must contain both upper and lower case letters:
- A, B, …, Z, a, b, …, z.
- The password must contain at least one of the following special characters:
  ~!@#$%^-_:,.<>[]{}
- The password cannot contain the following special characters:
  `' " | ; &
- The password must have more characters than the minimum password length (default = 4).

Troubleshooting

This feature allows you to quickly obtain the current system status and provide diagnostics information to Moxa engineers.

To export the current device information, click **Export**. If more detailed Wi-Fi information is required, enable **Wi-Fi Analysis** and then click **Export**. Retrieving the additional information may take up to 3 minutes.



Wi-Fi Mirror Port

A Wi-Fi mirror port can help you obtain the current Wi-Fi communication behavior of your network over the current channel when it is not convenient to set up a Wi-Fi sniffer in the system operating environment.

To setup a Wi-Fi mirror port, you will need a computer with the Wireshark tool installed, which will be used to connect to the AWK device via the Ethernet.

NOTE A Wi-Fi mirror port is useful for gathering information. However, the DFS function may not work properly when you enable the Wi-Fi Mirror Port function. Hence, we recommend disabling the Wi-Fi Mirror Port function during normal usage.

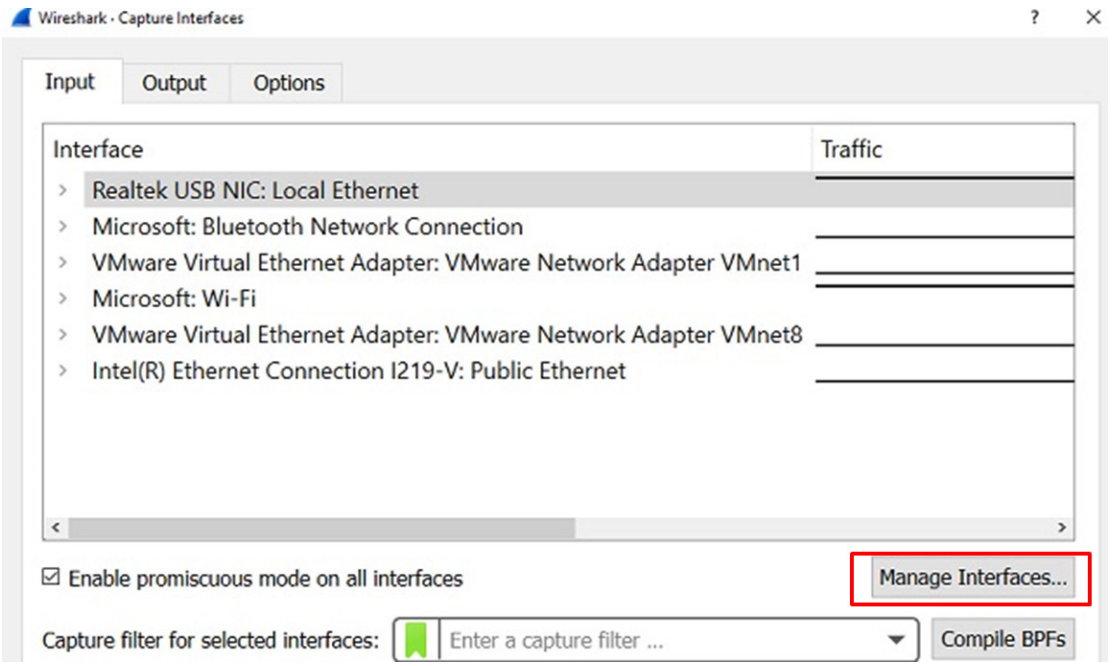
To set up a Wi-Fi mirror port for short-term monitoring, do the following:

1. Enter the duration in the **Capture Wi-Fi Frames** box.
   You can enter a value between 1 to 180 seconds.
2. Click **Capture**
3. Wait for a timeout on the web console

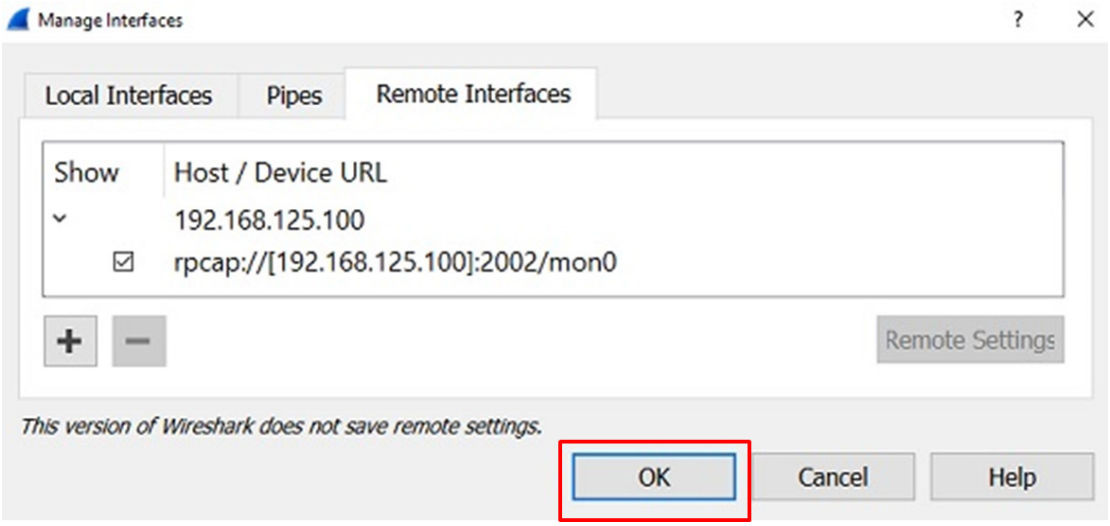
You will be able to download a report from the web browser.

To set up a Wi-Fi mirror port for long-term monitoring, do the following:

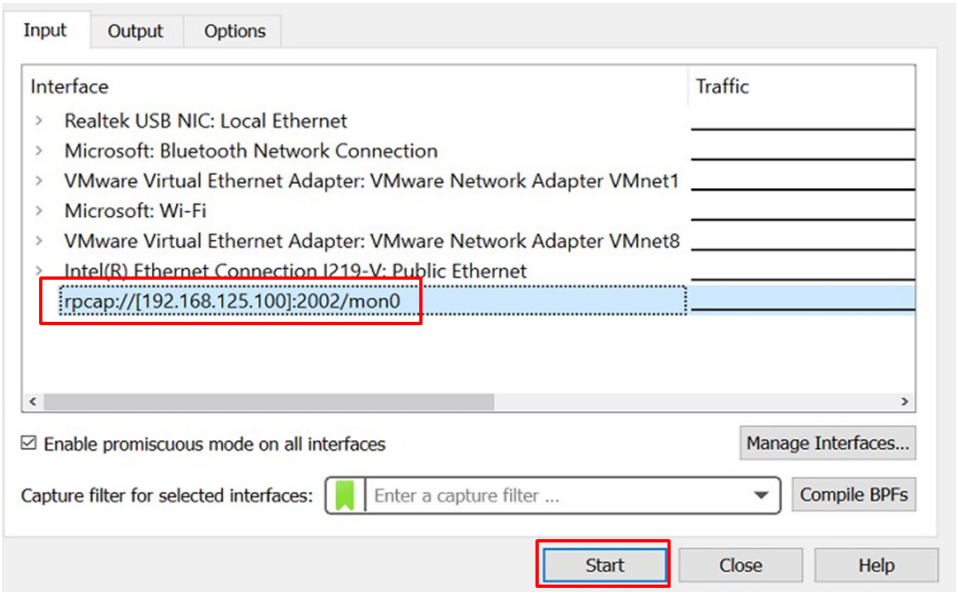
1. On the **Wi-Fi Mirror Port** page, set the **Remote Capture** option to **Enable.**
2. Run the Wireshark tool on your computer, click **Capture** and then click **Options**.
3. In the **Input** tab of the Wireshark tool, click **Manage Interfaces**



4. Click **Remote Interfaces** and add a new interface
5. Enter the information for your AWK device
   - Port: 2002
   - Auth: Null authentication
   - Host: *<AWK IP>*
6. Click **OK**



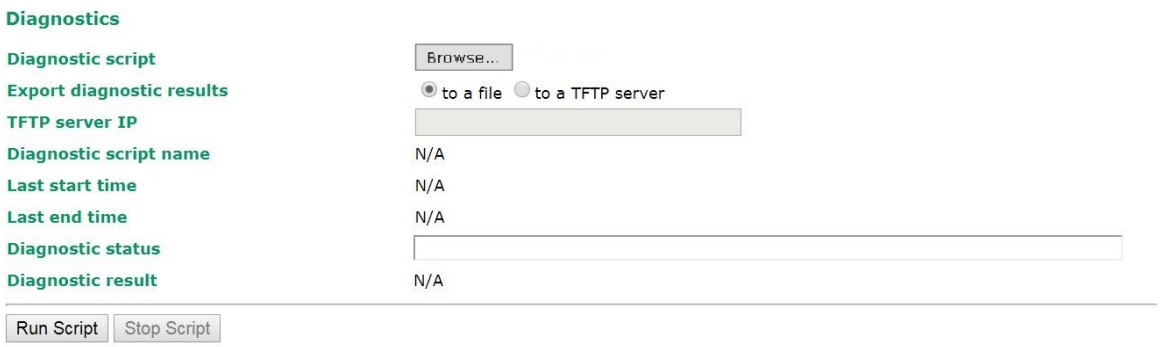
7. Select Input --> Interface --> rpcap://...:2002/mon0



Diagnostics

For cases where advanced troubleshooting is required, Moxa Service Center will send you an encrypted script file. The script file can capture additional details on the system.

To run the script, browse to and select the script file using **Browse** and click **Run Script** after you have filled in the following details:

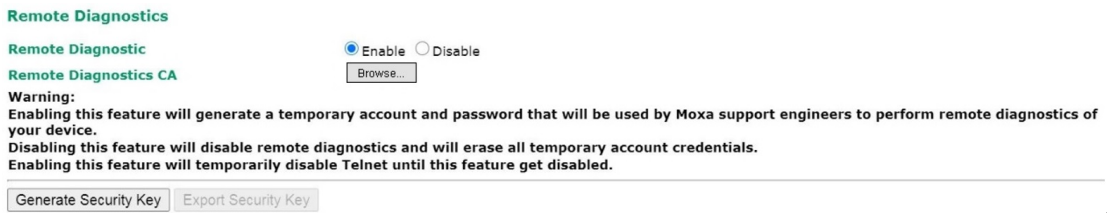


Setting	Description
Diagnostic script	Use the **Browse** button to select the Moxa diagnosis script file.
Export diagnostic results	Select if you want to export: • **to a file** • **to a TFTP server**
TFTP server IP	If you have selected the TFTP option, specify the IP address of the TFTP server.
Diagnostic script name	Displays the name of the script file
Last start time	Displays the start time of the last script execution
Last end time	Displays the end time of the last script execution
Diagnostic status	Displays the progress of the system diagnostics
Diagnostic result	Displays the result of the system diagnostics. If you have selected the export **to a file** option, the system log is encrypted and packed into a file. The limit on the log file size is 1 MB. When the size of the log file reaches 1MB another file is created. A maximum of 5 files (5MB) will be kept for downloading. When the number of files exceeds five, the oldest file is deleted.

Remote Diagnostics

If technical support from a Moxa engineer is needed, admin level users can enable remote diagnostics through HTTPS. This feature will generate a temporary account and password that will be used by Moxa support engineers to perform remote diagnostics on your device. When completed, we recommend disabling this feature again, which will remove all the temporary account information.

NOTE Remote diagnostics is only available for administrator-level users.

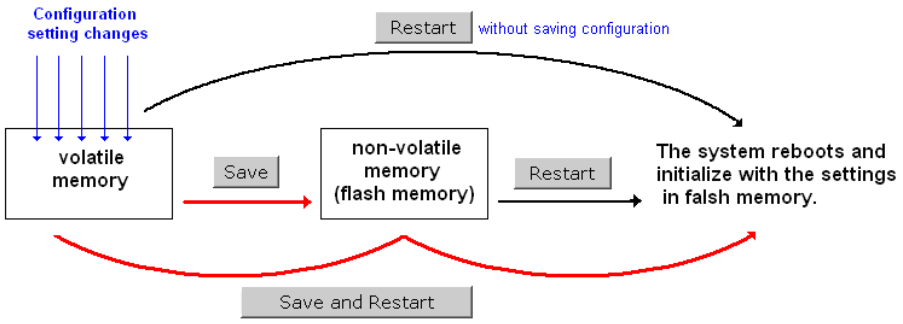


Setting	Description
Remote Diagnostics	Enable this option to allow remote technical support from Moxa engineers.
Remote Diagnostics CA	When enabled, the Moxa engineer will request the admin to provide the AWK's serial number and MAC address to generate a certificate file. Click **Browse** and upload the certificate file and then click **Generate Security Key**. When completed, click **Export Security Key** to generate a file named *remoteSecurityKey* and send this key to the support engineer.

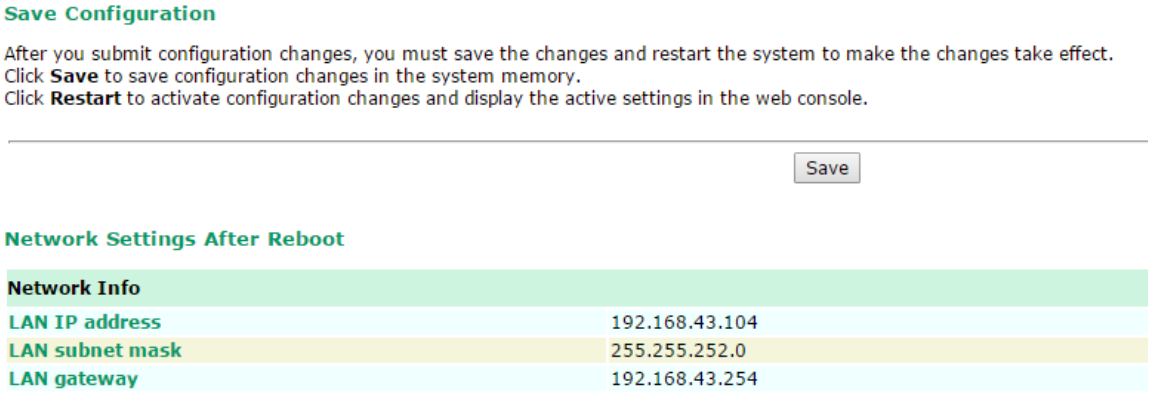
Save Configuration

The following figure shows how the AWK-4131A stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the AWK-4131A is shutdown or rebooted. Because the AWK-4131A starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the AWK-4131A.

This also means the new changes will not work unless you run either the **Save Configuration** function or the **Restart** function.



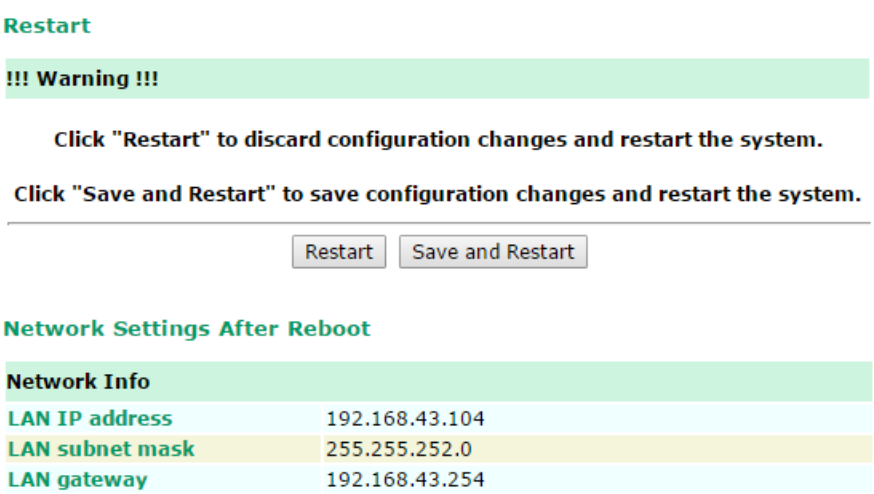
After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However, the new setting changes will remain in the non-volatile memory until you save the configurations.



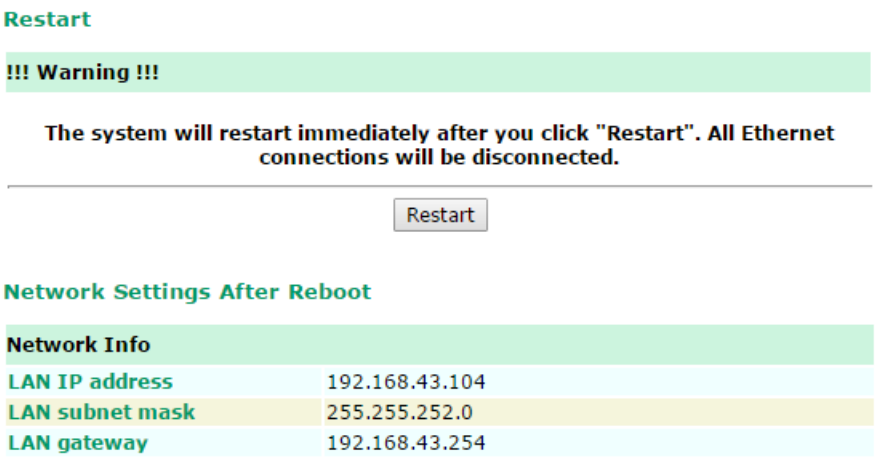
Restart

If you submitted configuration changes, you will find a blinking string in the upper right corner of the screen. After making all your changes, click the **Restart** function in the left menu box. One of two different screens will appear.

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the AWK-4131A directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the AWK-4131A.



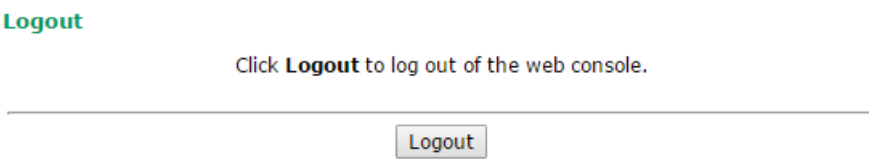
If you run the **Restart** function without changing any configurations or saving all your changes, you will see just one **Restart** button on your screen.



You will not be able to run any of the AWK-4131A's functions while the system is rebooting.

Logout

Logout helps users disconnect the current HTTP or HTTPS session and go to the Login page. For security reasons, we recommend you logout before quitting the console manager.



4

Software Installation/Configuration

The following topics are covered in this chapter:

- **Overview**
- **Wireless Search Utility**
  - Installing Wireless Search Utility
  - Configuring Wireless Search Utility

Overview

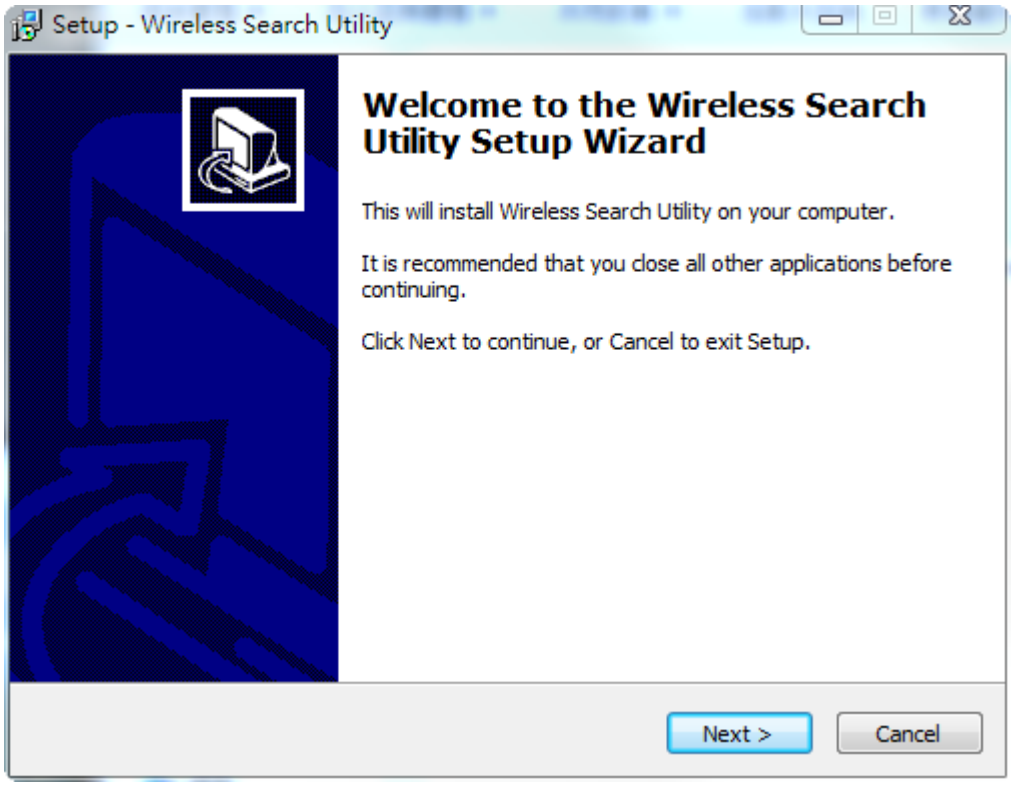
The Wireless Search Utility can be downloaded from the Moxa website at www.moxa.com.

Wireless Search Utility

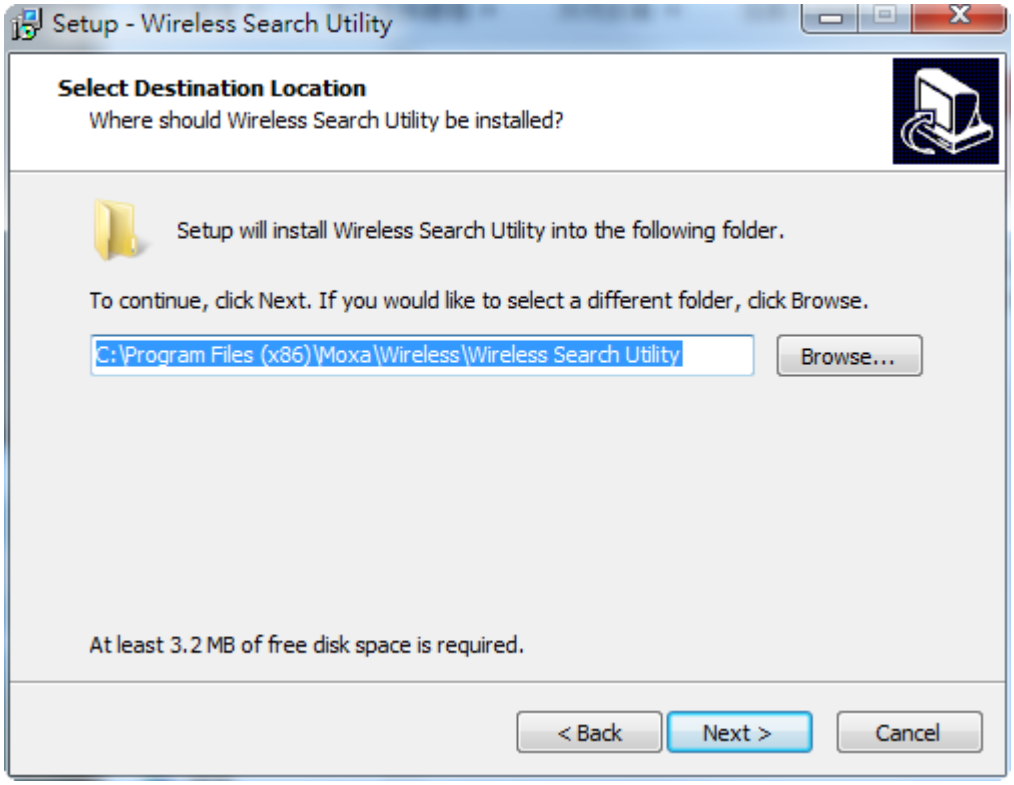
Installing Wireless Search Utility

Once the Wireless Search Utility is downloaded, run the setup executable to start the installation.

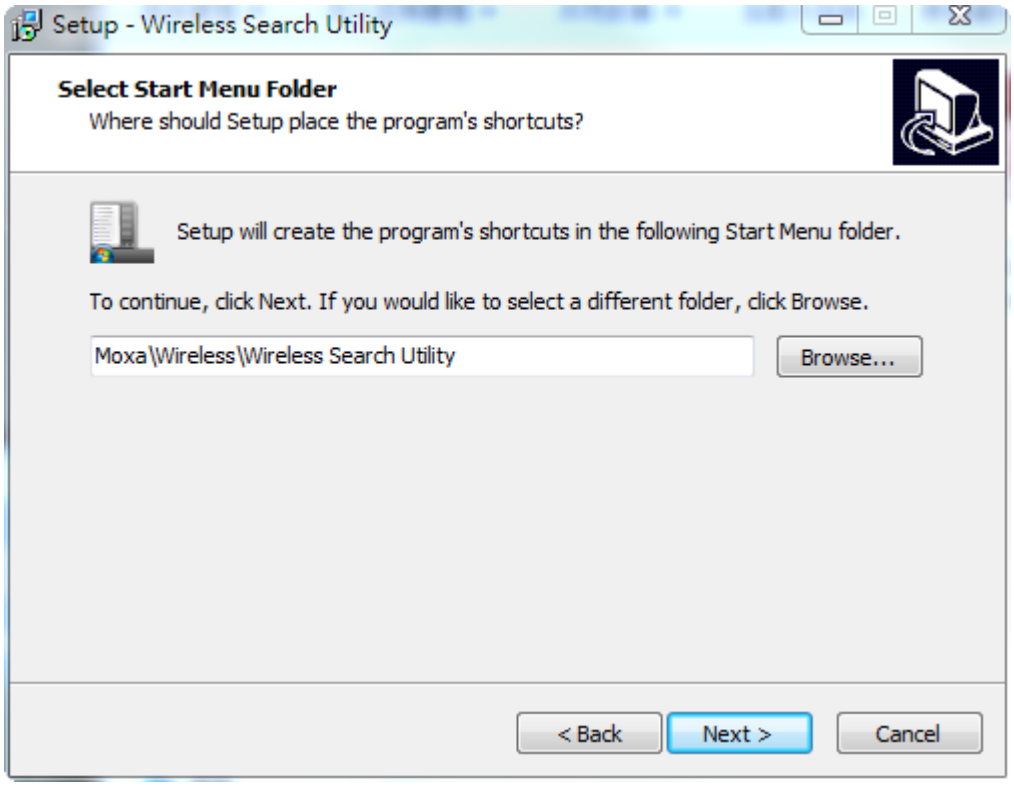
1. Click **Next** when the **Welcome** screen opens to proceed with the installation.



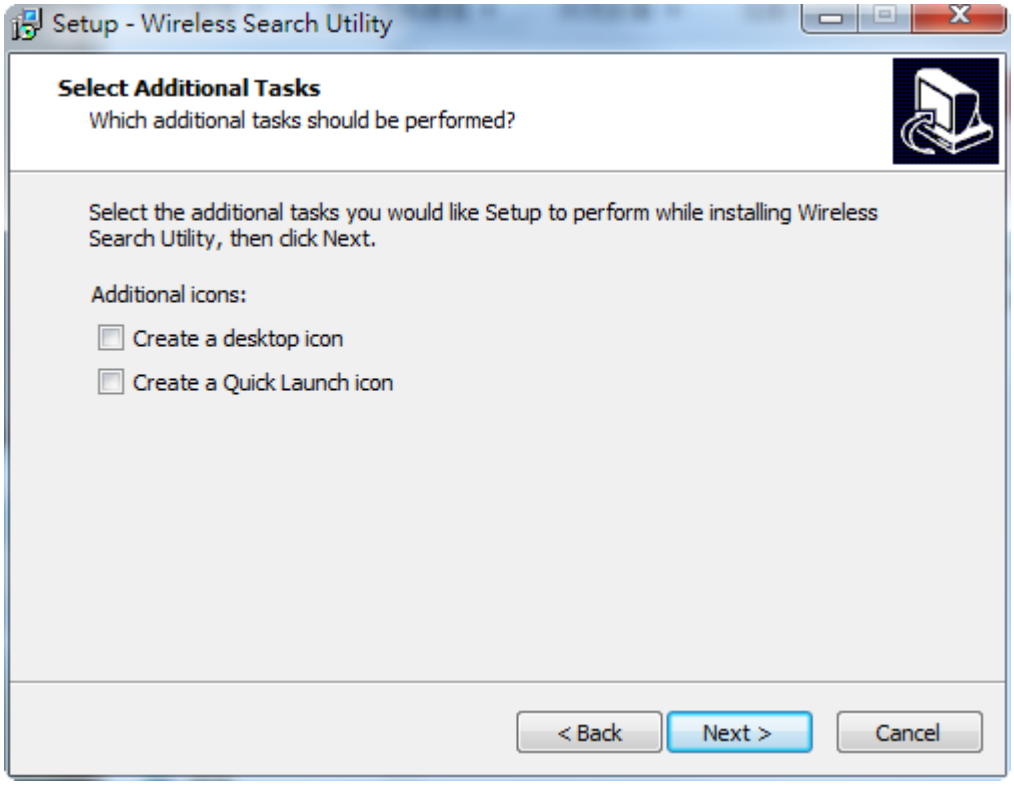
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



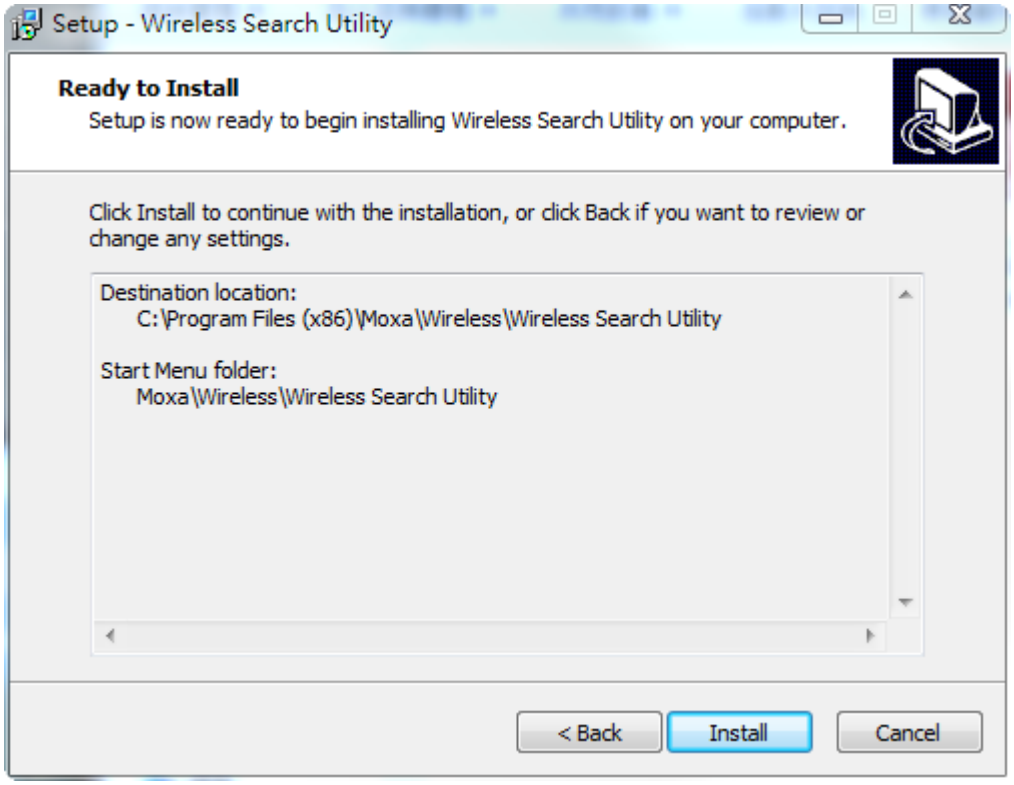
3. Click **Next** to create the program's shortcut files to the default directory, or click **Browse** to select an alternate location.



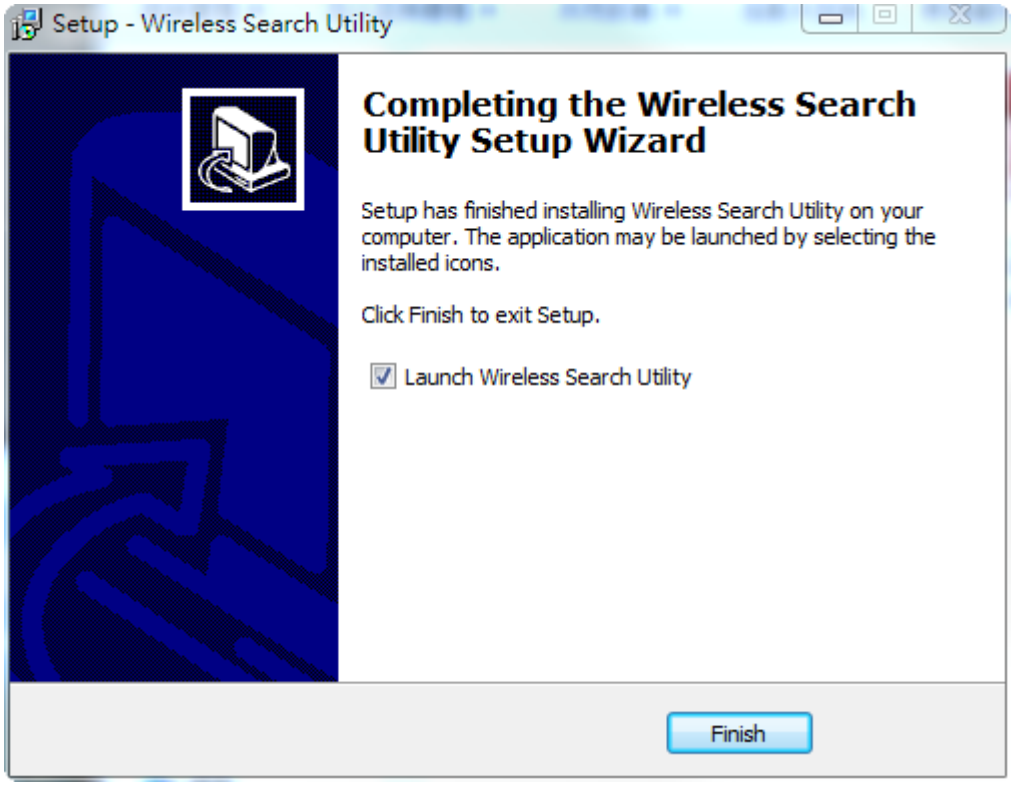
4. Click **Next** to select additional tasks.



5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.



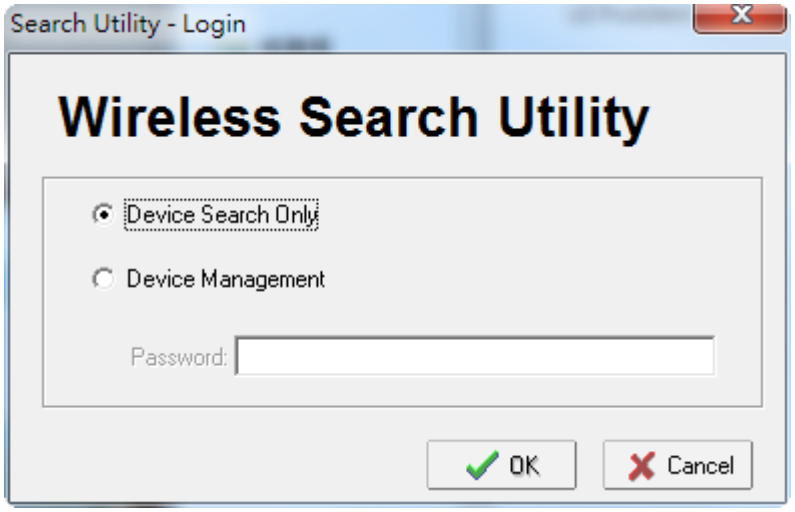
6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.
7. Click **Finish** to complete the installation of Wireless Search Utility.



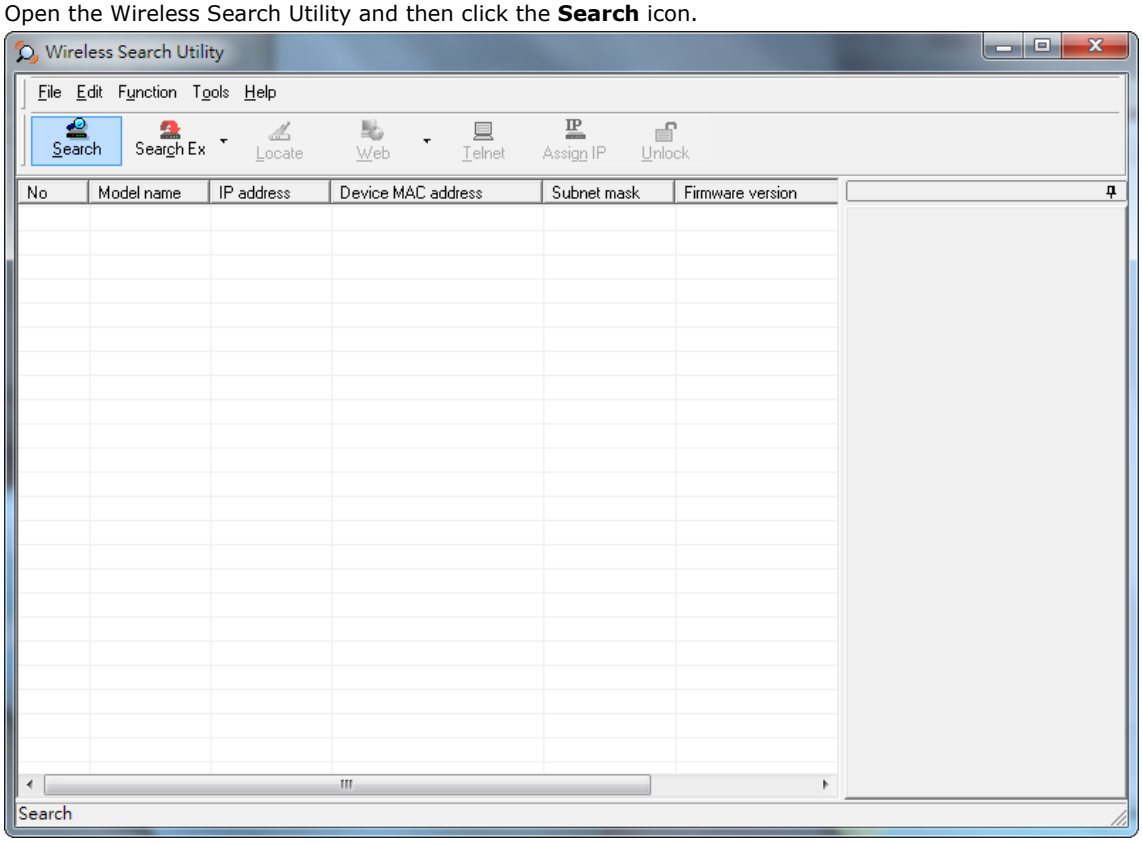
Configuring Wireless Search Utility

The Broadcast Search function is used to locate all AWK-4131A APs that are connected to the same LAN as your computer. After locating an AWK-4131A, you will be able to change its IP address. Since the Broadcast Search function searches by TCP packet and not IP address, it doesn't matter if the AWK-4131A is configured as an AP or Client. In either case, APs and Clients connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

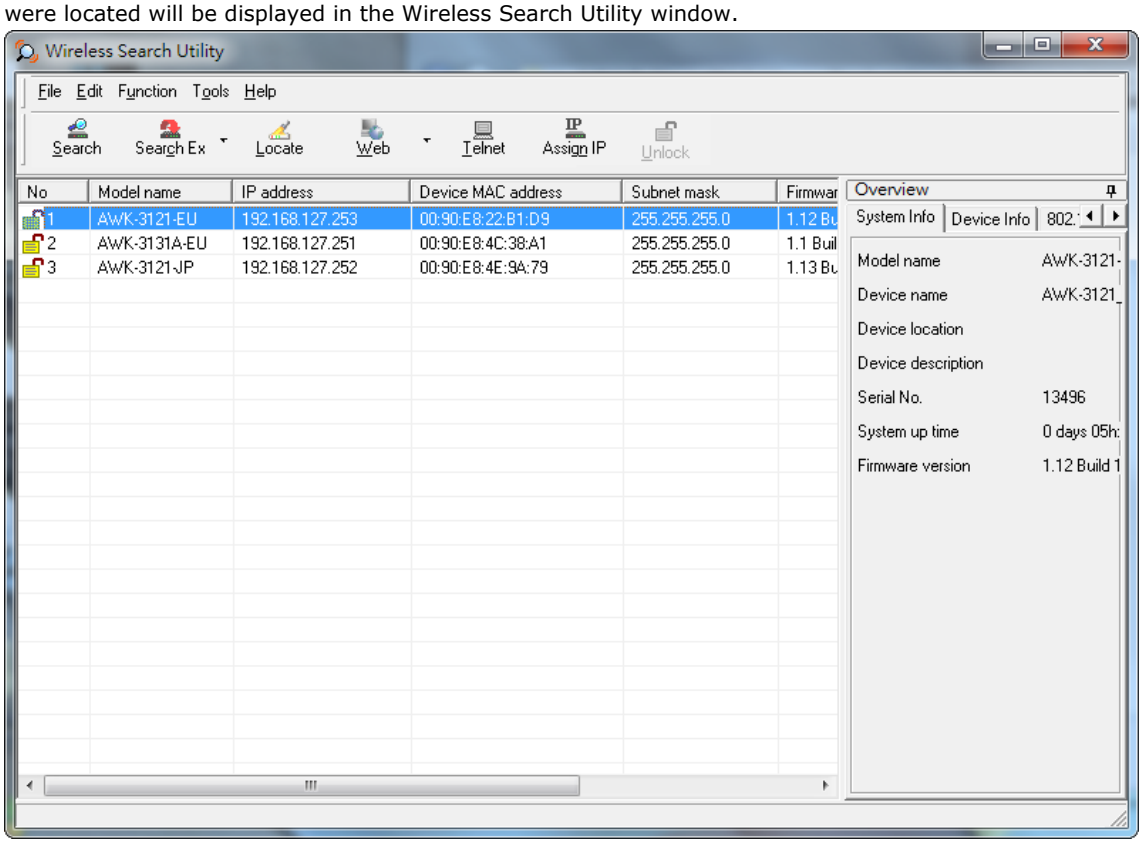
1. Start the **Wireless Search Utility** program. When the Login page appears, select the "Device Search only" option to search for devices and to view the configuration of each device. Select the "Device management" option to assign IPs, upgrade firmware, and locate devices.



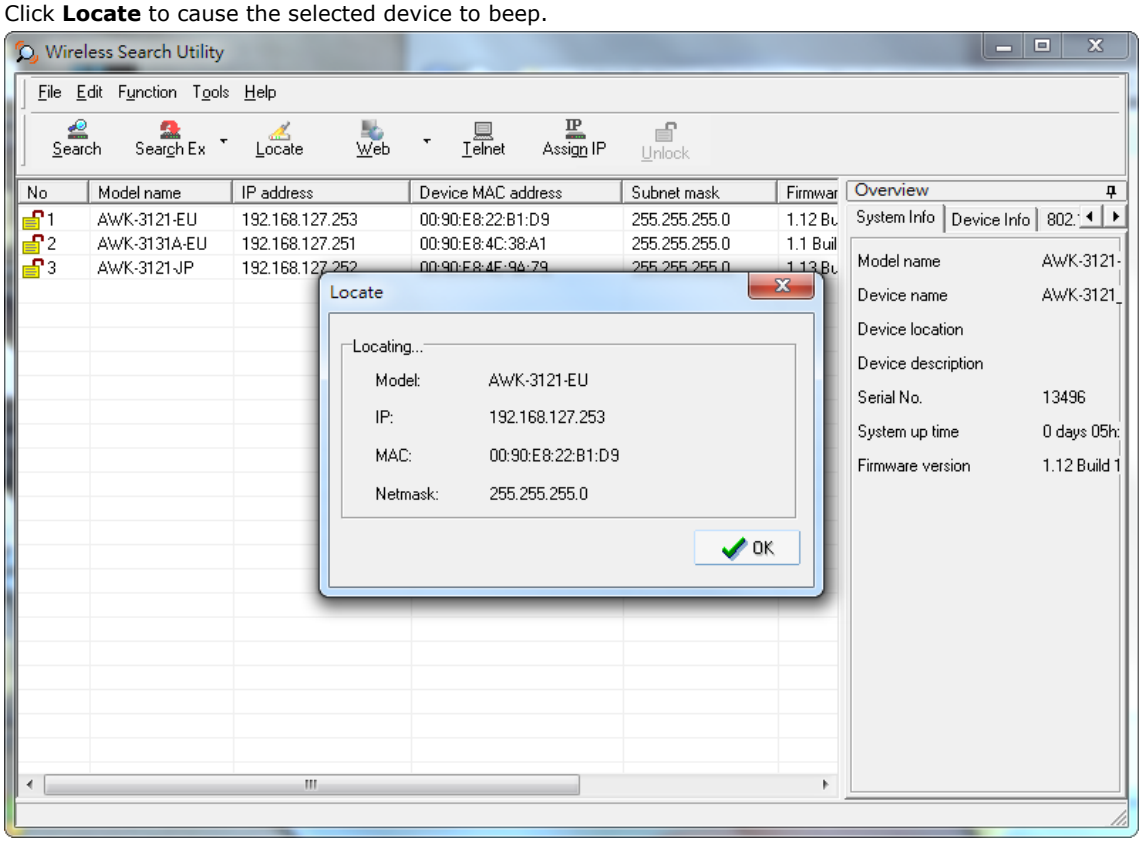
2. Open the Wireless Search Utility and then click the **Search** icon.



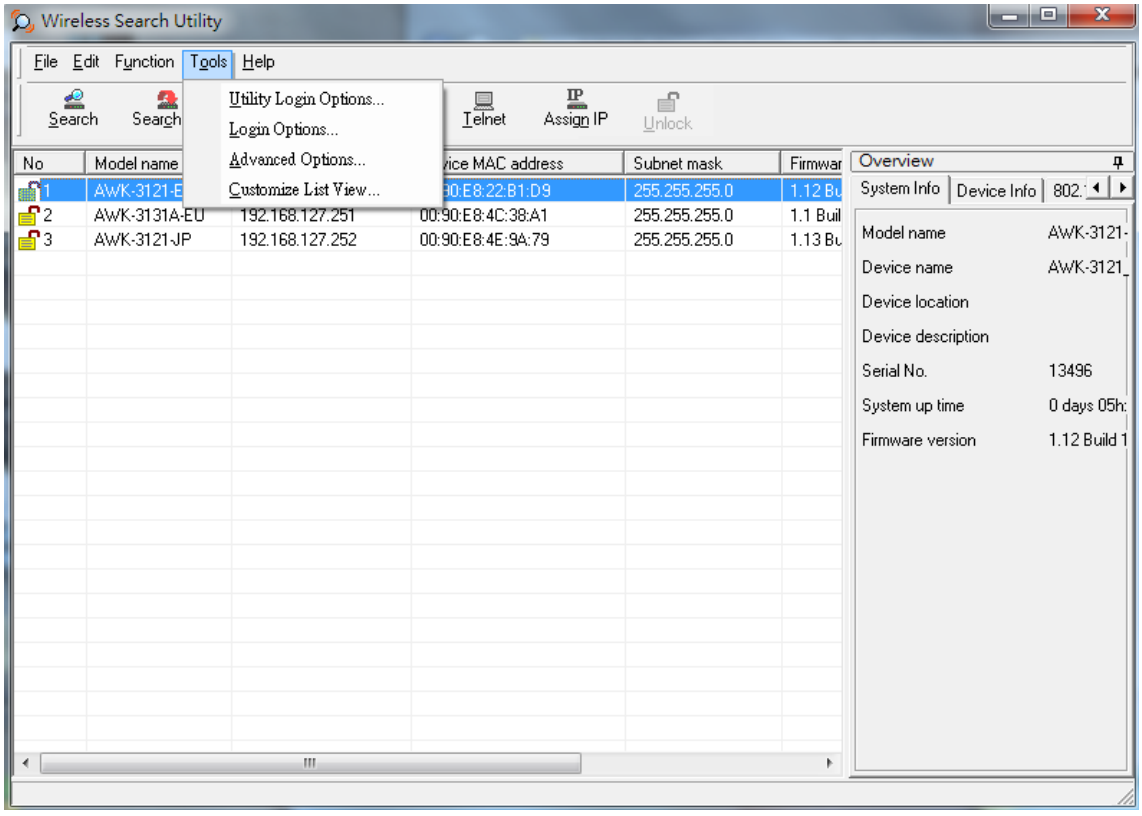
3. The "Searching" window indicates the progress of the search. When the search is complete, all AWKs that were located will be displayed in the Wireless Search Utility window.



4. Click **Locate** to cause the selected device to beep.



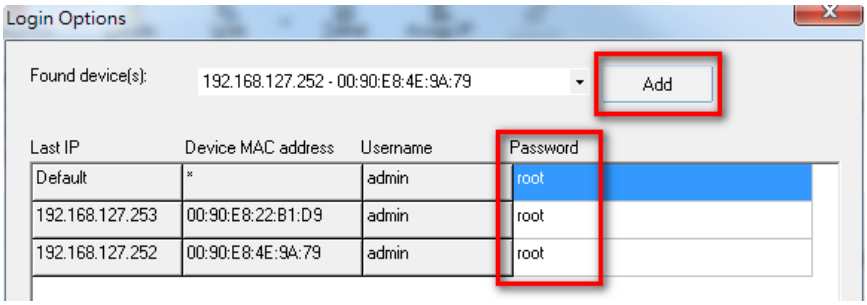
5. Make sure your AWK is **unlocked** before using the search utility's icons setting. The AWK will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.
6. Go to **Tools → Login Options** to manage and unlock additional AWKs.



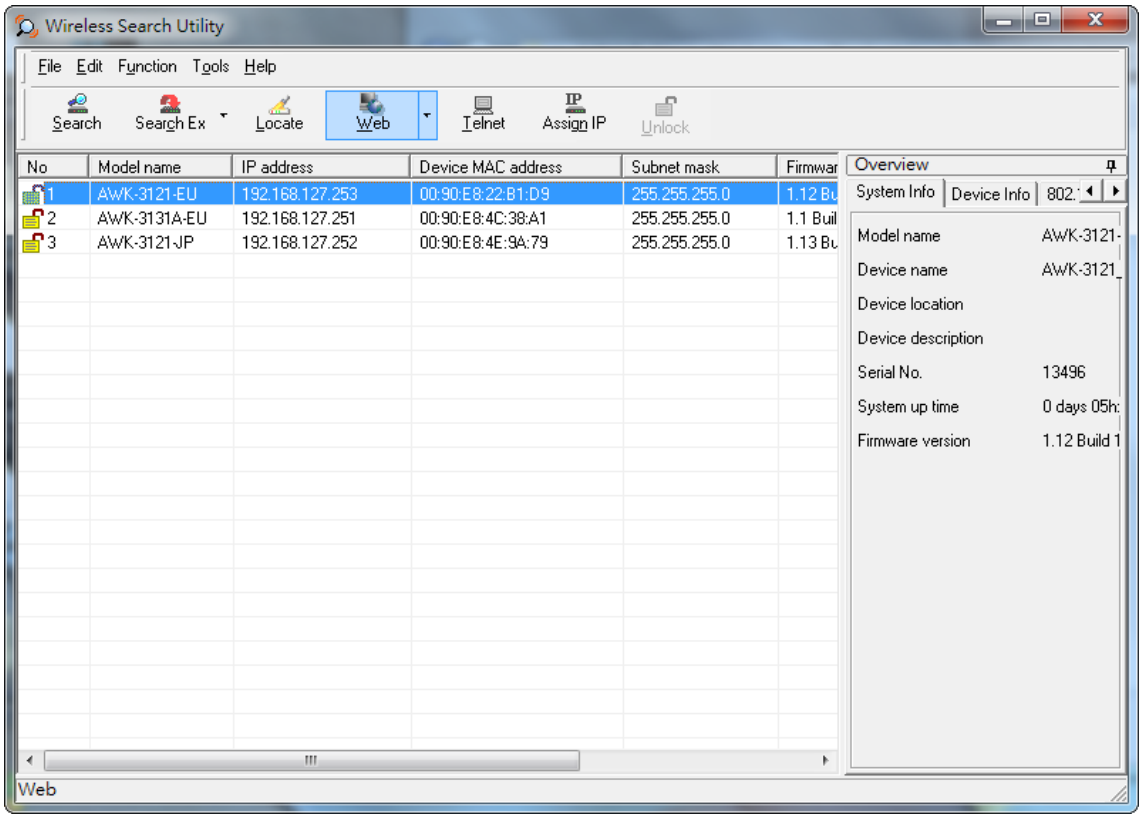
7. Use the scroll down list to select the MAC addresses of those AWKs you would like to manage, and then click **Add**. Key in the password for the AWK device and then click **OK** to save. If you return to the search page and search for the AWK again, you will find that the AWK will unlock automatically.

ATTENTION

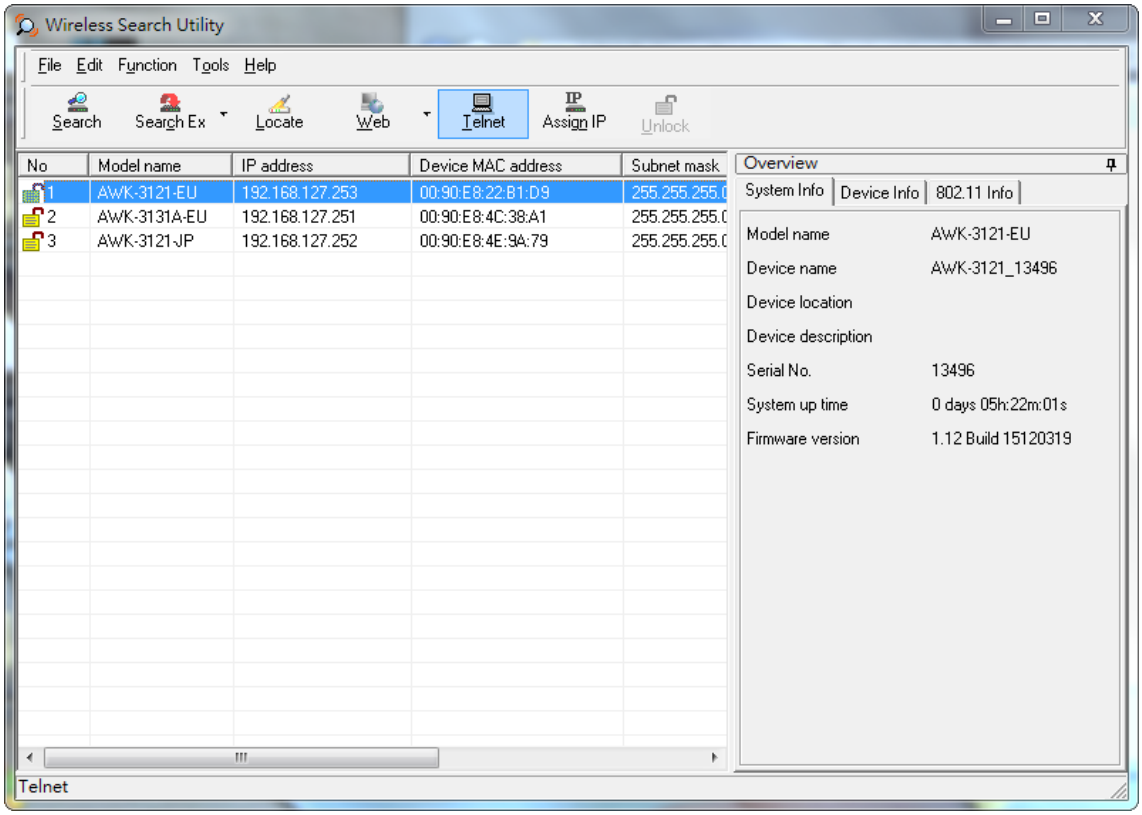
For security purposes, we suggest you can change the Wireless Search Utility login password instead of using the default.



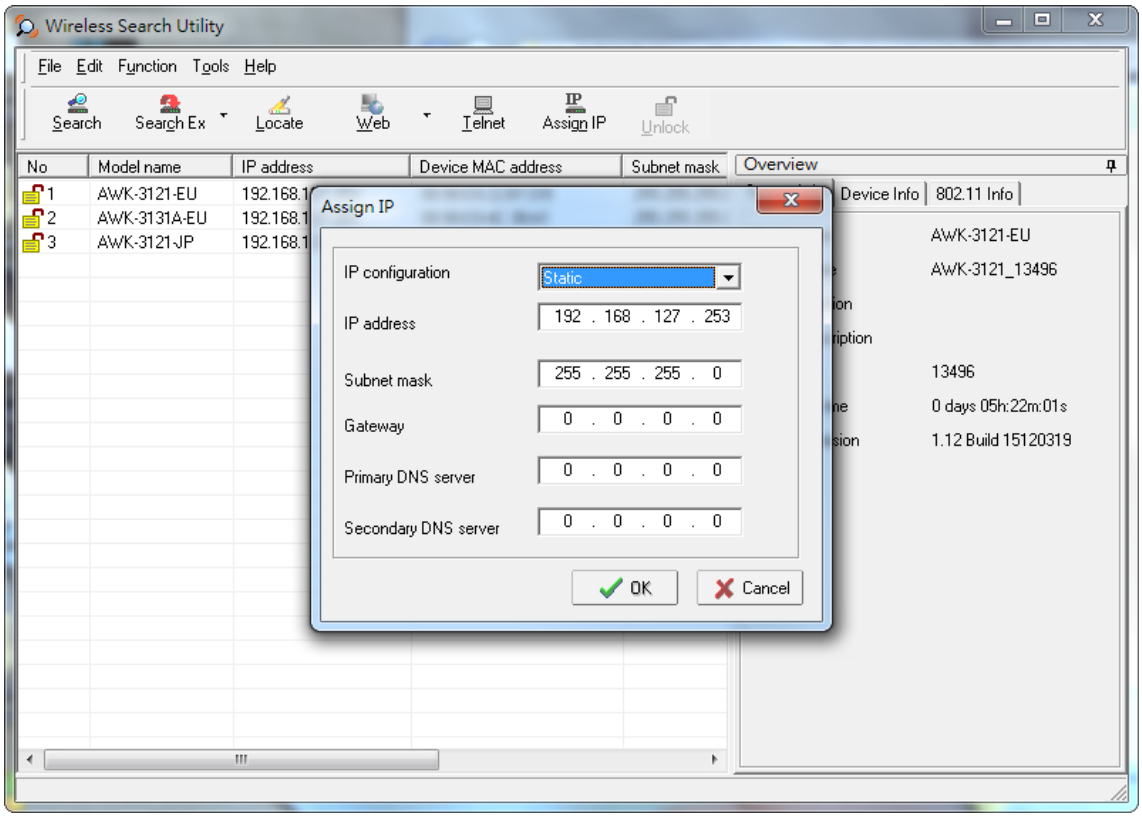
To modify the configuration of the highlighted AWK, click on the Web icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, "Using the Web Console," for information on how to use the web console.



Click on **Telnet** if you would like to use telnet to configure your AWKs.



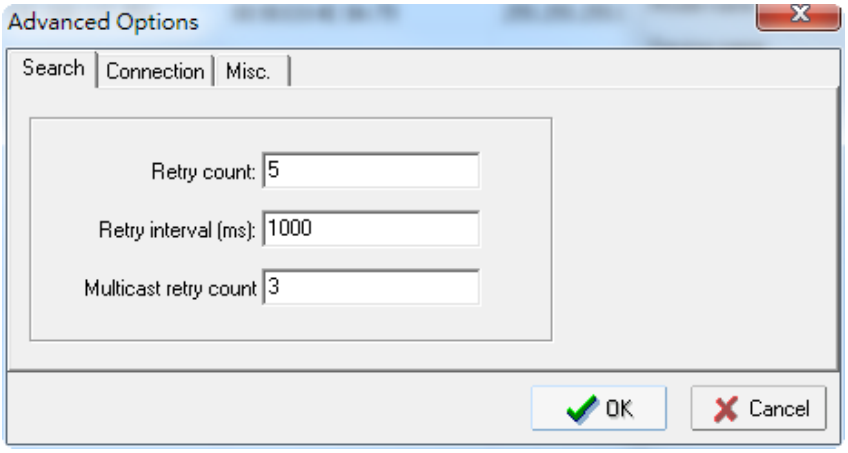
Click **Assign IP** to change the IP setting.



The three advanced options—**Search**, **Connection**, and **Miscellaneous**—are explained below:

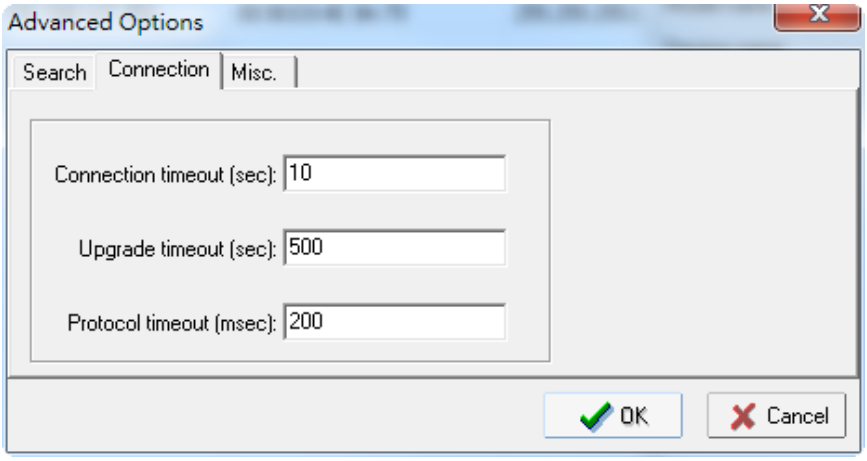
Search

- **Retry count (default=5):** Indicates how many times the search will be retried automatically.
- **Retry interval (ms):** The time elapsed between retries.



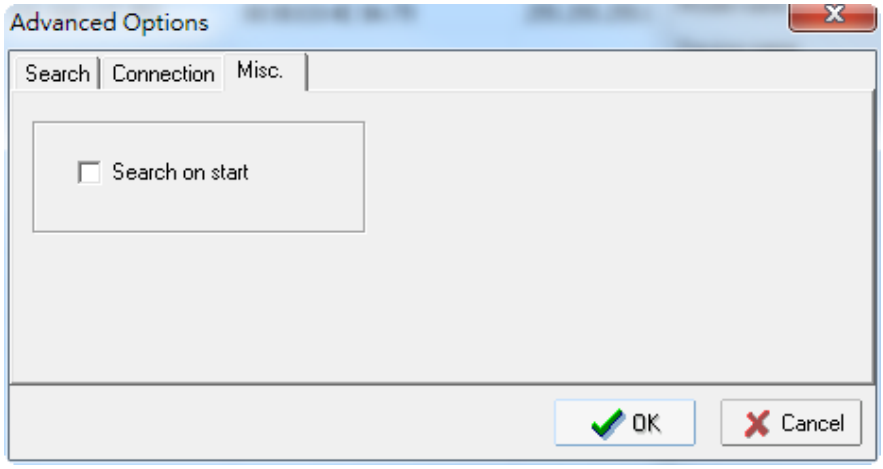
Connection

- **Connection timeout (secs):** Use this option to set the waiting time for the **Default Login**, **Locate**, **Assign IP**, **Upload Firmware**, and **Unlock** to complete.
- **Upgrade timeout (secs):** Use this option to set the waiting time for the connection to disconnect while the firmware is upgrading. Use this option to set the waiting time for the Firmware to write to flash.



Misc.

Search on start: Checkmark this box if you would like the search function to start searching for devices after you log in to the Wireless Search Utility.



5

Other Console Configurations

This chapter explains how to access the AWK-4131A for the first time. In addition to HTTP access, there are four ways to access AWK-4131A: serial console, Telnet console, SSH console, and HTTPS console. The serial console connection method, which requires using a short serial cable to connect the AWK-4131A to a PC's COM port, can be used if you do not know the AWK-4131A's IP address. The other consoles can be used to access the AWK-4131A over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

- **RS-232 Console Configuration (115200, None, 8, 1, VT100)**
- **Configuration by Telnet and SSH Consoles**
- **Configuration by Web Browser with HTTPS/SSL**
- **Disabling Telnet and Browser Access**

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

The serial console connection method, which requires using a short serial cable to connect the AWK-4131A to a PC's COM port, can be used if you do not know the AWK-4131A's IP address. It is also convenient to use serial console configurations when you cannot access the AWK-4131A over Ethernet LAN, such as in the case of LAN cable disconnections or broadcast storming over the LAN.

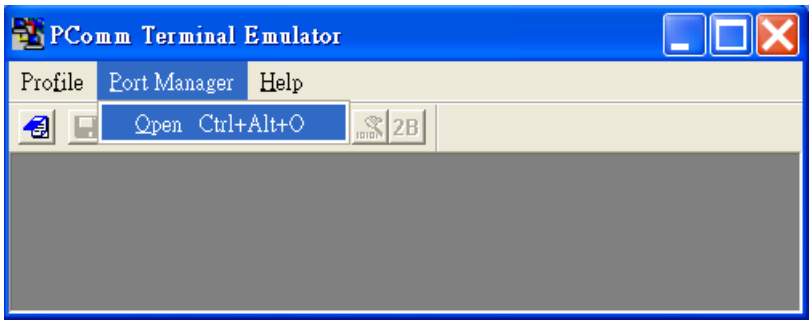
ATTENTION

Do not use the RS-232 console manager when the AWK-4131A is powered at reversed voltage (ex. -48VDC), even though reverse voltage protection is supported. If you need to connect the RS-232 console at reverse voltage, Moxa's TCC-82 isolator is your best solution.

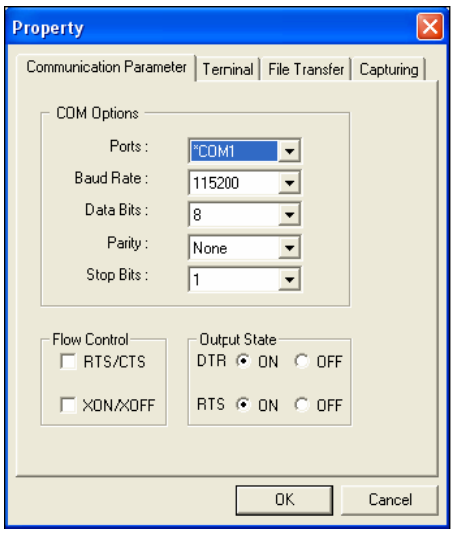
NOTE We recommend using **Moxa PComm (Lite)** Terminal Emulator, which can be downloaded free of charge from Moxa's website.

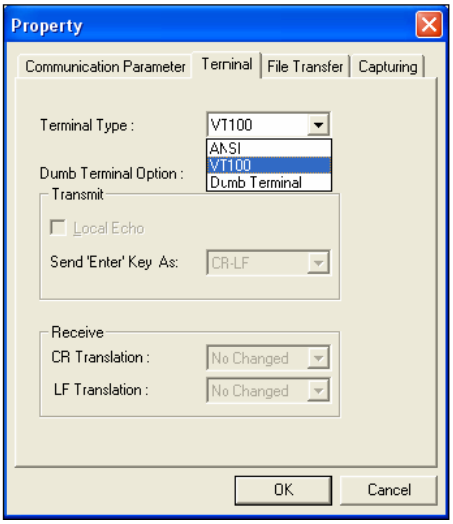
Before running the PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the AWK-4131A's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, take the following steps to access the RS-232 console utility.

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

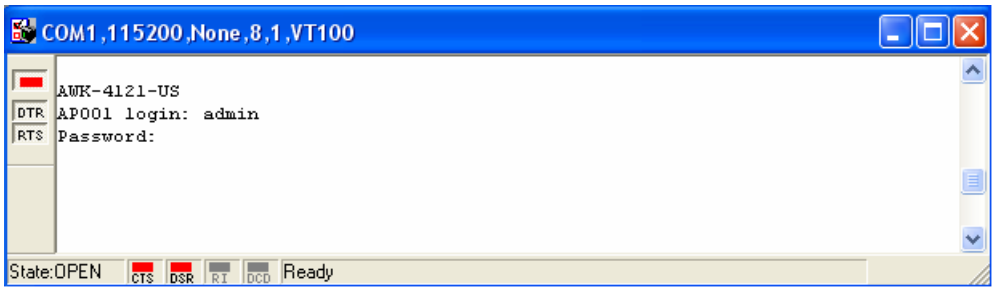


3. The **Communication Parameter** page of the Property window opens. Select the appropriate COM port for Console Connection, **115200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits.

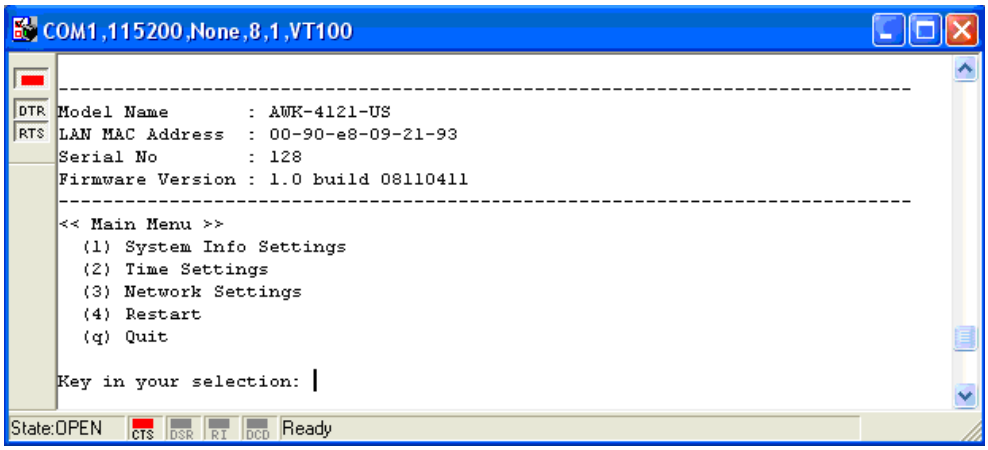




4. Click on the **Terminal** tab, and select **VT100 (or ANSI)** for Terminal Type. Click on **OK** to continue.
5. The Console login screen will appear. Log into the RS-232 console with the login name (default: **admin**) and password (default: **moxa**, if no new password is set).



6. The AWK-4131A's device information and Main Menu will be displayed. Please follow the description on screen and select the administration option you wish to perform.



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 automatically be logged out for network security. You will need to log in again to resume operation.

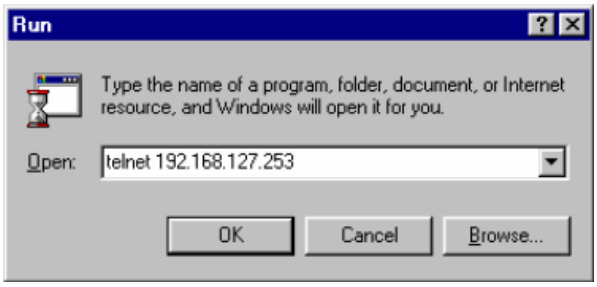
Configuration by Telnet and SSH Consoles

You may use Telnet or SSH client to access the AWK-4131A and manage the console over a network. To access the AWK-4131A's functions over the network from a PC host that is connected to the same LAN as the AWK-4131A, you need to make sure that the PC host and the AWK-4131A are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

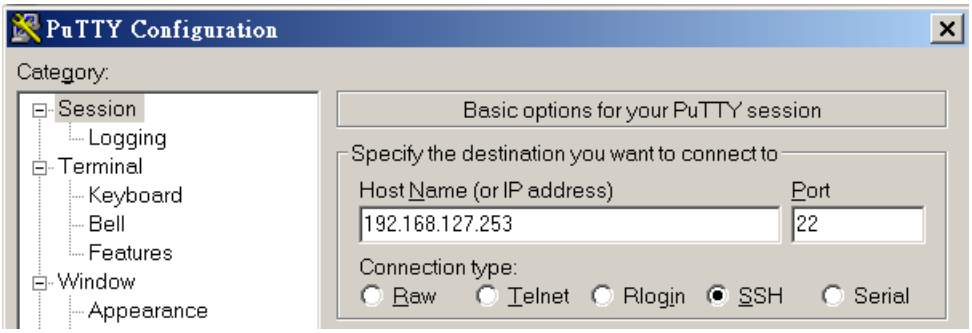
NOTE The AWK-4131A's default IP address is **192.168.127.253** and the default subnet mask is 255.255.255.0 (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

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

1. From Windows Desktop, run **Start → Run**, and then use Telnet to access the AWK-4131A's IP address from the Windows Run window. (You may also issue the telnet command from the MS-DOS prompt.)



When using SSH client (ex. PuTTY), please run the client program (ex. putty.exe) and then input the AWK-4131A's IP address, specifying **22** for the SSH connection port.

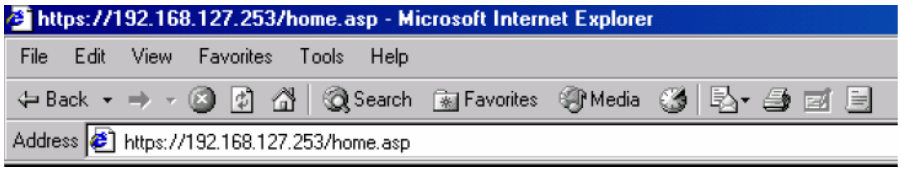


2. The Console login screen will appear. Please refer to the previous paragraph "RS-232 Console Configuration" and for login and administration.

Configuration by Web Browser with HTTPS/SSL

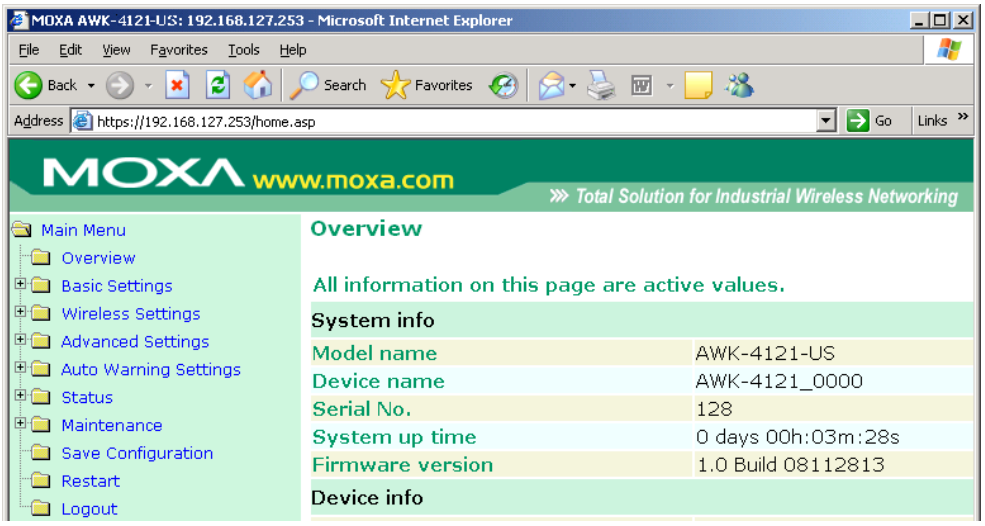
To secure your HTTP access, the AWK-4131A supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the AWK-4131A's web browser interface via HTTPS/SSL.

1. Open your web browser and type https://*<AWK-4131A's IP address>* in the address field. Press **Enter** to establish the connection.



2. Warning messages are displayed to warn users that the security certificate was issued by a company they have not chosen to trust.

Select **Yes** to accept the certificate issued by Moxa IW and then enter the AWK-4131A's web browser interface secured via HTTPS/SSL. (You can see the protocol in URL is **https**.) Then you can use the menu tree on the left side of the window to open the function pages to access each of the AWK-4131A's functions.



Disabling Telnet and Browser Access

If you are connecting the AWK-4131A to a public network but do not intend to use its management functions over the network, then we suggest disabling both Telnet Console and Web Configuration. Please run **Maintenance → Console Settings** to disable them, as shown in the following figure.

A

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your AWK-4131As and plan your industrial wireless network better.

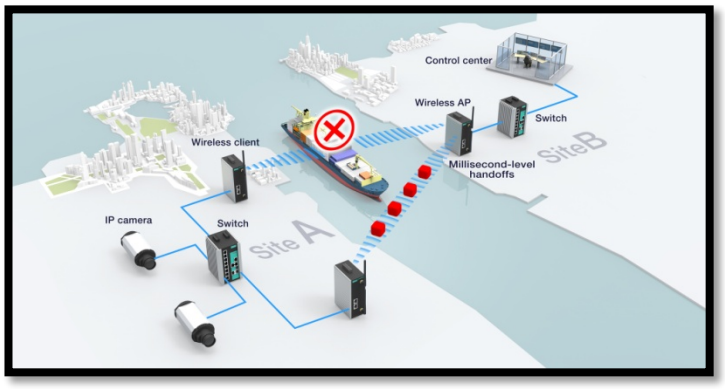
The following topics are covered in this appendix:

- **AeroLink Protection**
- **Wireless Distribution System (WDS)**
- **Beacon**
- **DTIM**
- **Fragment**
- **RTS Threshold**
- **STP and RSTP**
  - The STP/RSTP Concept
  - Differences between RSTP and STP

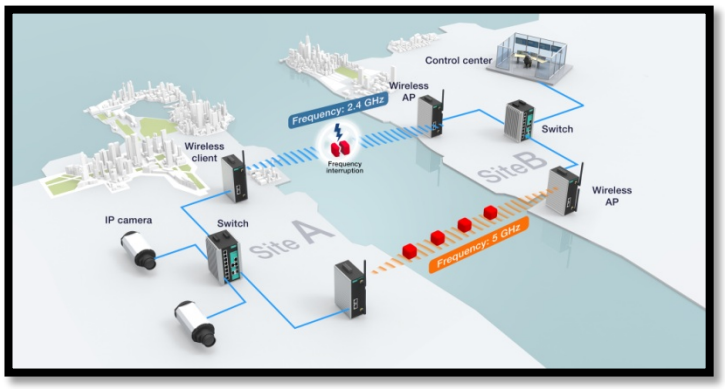
AeroLink Protection

In industrial applications, such as communication between off-shore oil platforms, or train-to-ground communications, a reliable wireless bridge is essential to minimize system downtime and maximize system availability. Moxa's AeroLink Protection provides a reliable wireless bridge between two networks to form network-level redundancy.

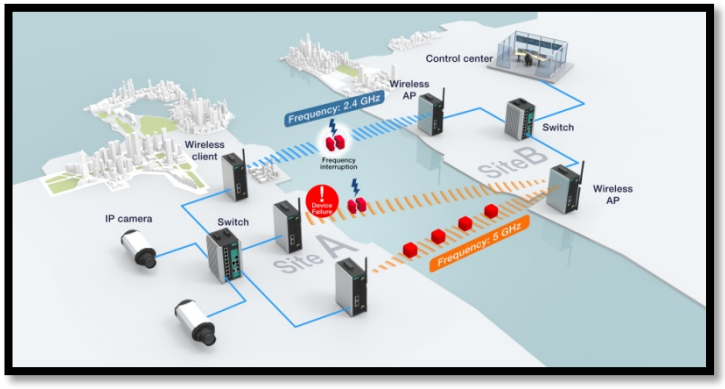
1. **Communication Failover:** AeroLink Protection members can negotiate with each other to automatically elect an Active node for data communication. If the Active node is no long capable of sending data to its access point, it will inform other Backup nodes to resume the communication via another path.



2. **Frequency-Interference Failover:** This concept is similar to the previous model. If the communication frequency experiences interference and data can no longer be transmitted over the Active frequency, it will resume the connection via another Backup frequency.



3. **Device Failover:** After covering the communication and frequency failures, in order to provide a single-point-of-failure free wireless network, AeroLink Protection also checks the device status. If the Active node has a power failure, the Backup nodes will automatically resume the wireless communication.



4. **Scalable:** AeroLink Protection is designed to allow scalable backup paths so that users can realize complete wireless redundancy from all of the above failure types by increasing the number of backup nodes.

5. **Fast Recovery:** In addition to maintaining a redundant wireless network, another key is providing uninterrupted communication even when a failure occurs. AeroLink protection is designed to restore commutation from all failures with 300 ms.
   A member of the AeroLink Protection group can take one of the following seven states:

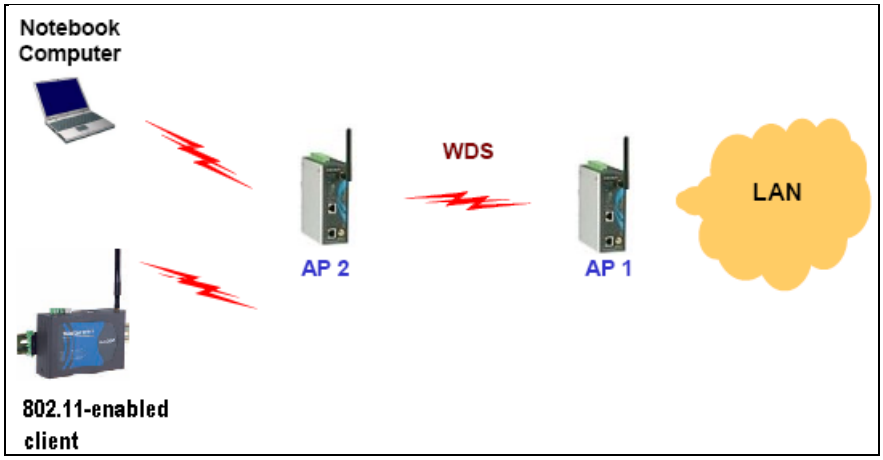
   - **Initiation State (Init):** Initiates the AeroLink Protection Protocol
   - **Discovering State (Discover):** Discovers other AeroLink Protection members for further negotiation
   - **Idle State (Idle):** Internal protocol checkpoint
   - **Negotiation State (Nego):** Negotiates with other AeroLink Protection members and elects an Active node.
   - **Backup State (Backup):** After negotiation, this node is assigned as a Backup node. All traffic will go through the Active node instead.

NOTE When a node is in Backup state, the STATE LED will be blinking.

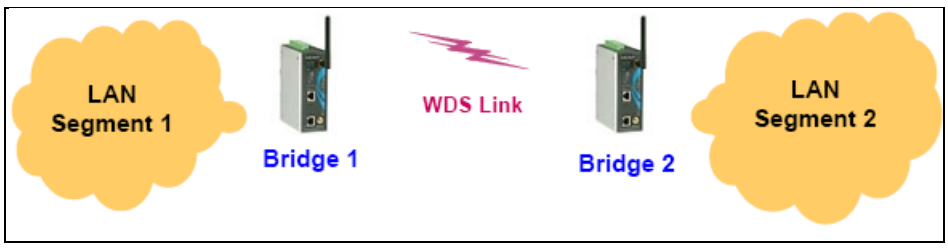
- **Active State (Active)**: After negotiation, this node is assigned as Active node, which means that all traffic will go through this node.
- **Role Change State (Change)**: If the Active node is no longer capable of data transmission via the WLAN, it will turn into Change State to trigger the re-negotiation of the Active node from the Backup nodes.

Wireless Distribution System (WDS)

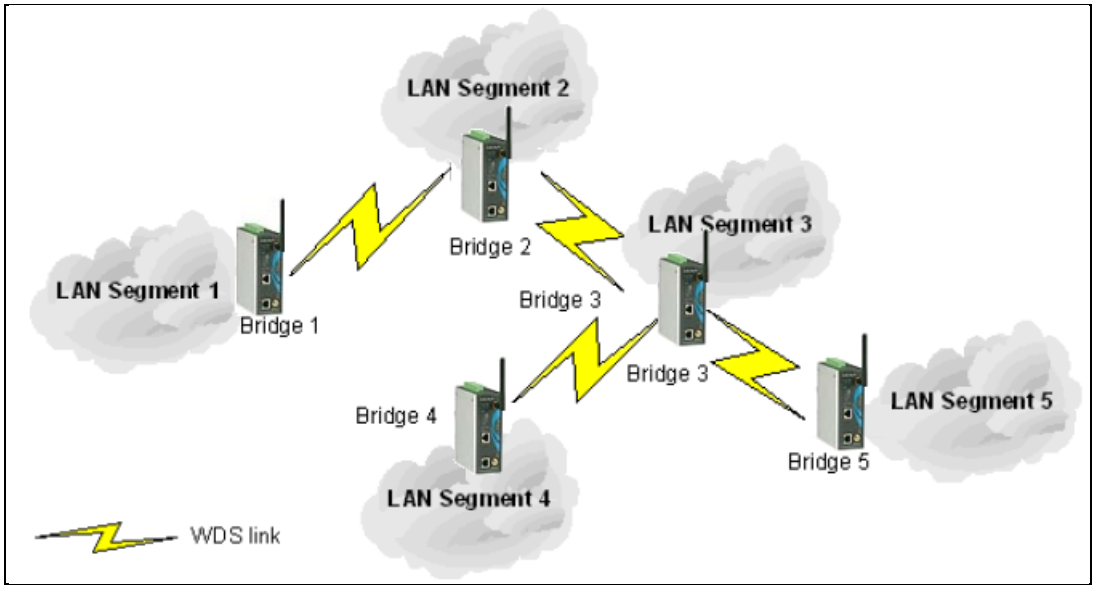
Traditionally, APs are connected via Ethernet LAN ports. By using a Wireless Distribution System (WDS), APs can communicate with one another wirelessly. For example, AP 2 acts as an access point for the notebook computers or other IEEE 802.11-enabled clients, and forwards packets sent from the notebook computers to AP 1 through WDS. Then, AP 1 forwards the packets to the Ethernet LAN. Packets destined for the notebook computers follow a reverse path from the Ethernet LAN through the APs to the notebook computers. In this way, AP 2 acts as an "AP repeater."



By using WDS, two or more LAN segments can be connected wirelessly. As illustrated in the figure below, a pair of wireless LAN-to-LAN bridges is used to connect two LAN segments. Since the AP is WDS-enabled, it can be used as a wireless bridge.

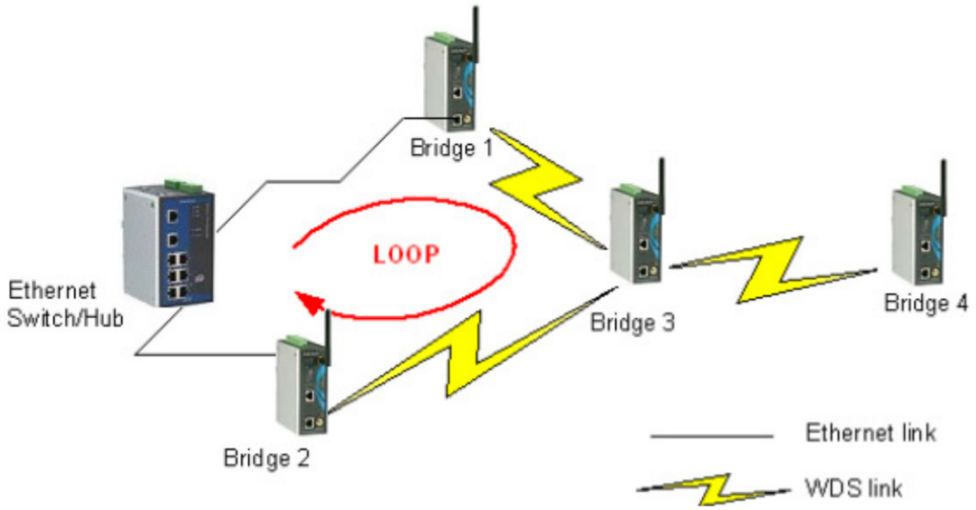


It is a good idea to plan your wireless network by drawing a diagram so that you know how each AWK-4131A is connected to other peer APs or wireless bridges by WDS, and how bridges are connected to other peer bridges by WDS. See the following figure for an example of a network-planning diagram.



ATTENTION

Be sure to eliminate loops from networks that consist of wireless bridges, Ethernet switches, Ethernet links, and WDS links. If any loops exist, packets will circle around the loops and network performance will be seriously degraded. The following figure shows a network topology containing a loop.



Beacon

A beacon is a packet broadcast by the AP to keep the network synchronized. A beacon includes the wireless LAN service area, the AP address, the Broadcast destination address, a time stamp, Delivery Traffic Indicator Maps (DTIM), and the Traffic Indicator Message (TIM). Beacon Interval indicates the frequency interval of AP.

DTIM

Delivery Traffic Indication Map (DTIM) is contained in beacon frames. It is used to indicate that broadcast and multicast frames buffered by the AP will be delivered shortly. Lower settings result in more efficient networking, while preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power.

Fragment

A lower setting means smaller packets, which will create more packets for each transmission. If you have decreased this value and experience high packet error rates, you can increase it again, but it will likely decrease overall network performance. Only minor modifications of this value are recommended.

RTS Threshold

RTS Threshold (256-2346) – This setting determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication. This value should remain at its default setting of 2,346. When you encounter inconsistent data flow, only minor modifications are recommended.

STP and RSTP

The STP/RSTP Concept

Spanning Tree Protocol (STP) was designed to help reduce link failures in a network, and provide protection from loops. Networks that have a complicated architecture are prone to broadcast storms caused by unintended loops in the network. The STP protocol is part of the IEEE 802.1D standard, 1998 Edition bridge specification.

Rapid Spanning Tree Protocol (RSTP) implements the Spanning Tree Algorithm and Protocol defined by IEEE 802.1w-2001 standard. RSTP provides the following benefits:

- The topology of a bridged network will be determined much more quickly compared to STP.
- RSTP is backward compatible with STP, making it relatively easy to deploy. For example:
  - Defaults to sending 802.1D-style BPDUs if packets with this format are received.
  - STP (802.1D) and RSTP (802.1w) can operate on the LAN ports and WLAN ports (Master and Slave mode) of the same AWK-4131A.

This feature is particularly helpful when the AWK-4131A connects to older equipment, such as legacy switches.

Differences between RSTP and STP

RSTP is similar to STP, but includes additional information in the BPDUs that allow each bridge to confirm that it has taken action to prevent loops from forming when it decides to enable a link to a neighboring bridge. Adjacent bridges connected via point-to-point links will be able to enable a link without waiting to ensure that all other bridges in the network have had time to react to the change. The main benefit of RSTP is that the configuration decision is made locally rather than network-wide, allowing RSTP to carry out automatic configuration and restore a link faster than STP.

B

Supporting Information

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

The following topics are covered in this appendix:

- **About This User's Manual**
- **Firmware Recovery**
- **DoC (Declaration of Conformity)**
  - Federal Communication Commission Interference Statement
- **RED Compliance Statement**

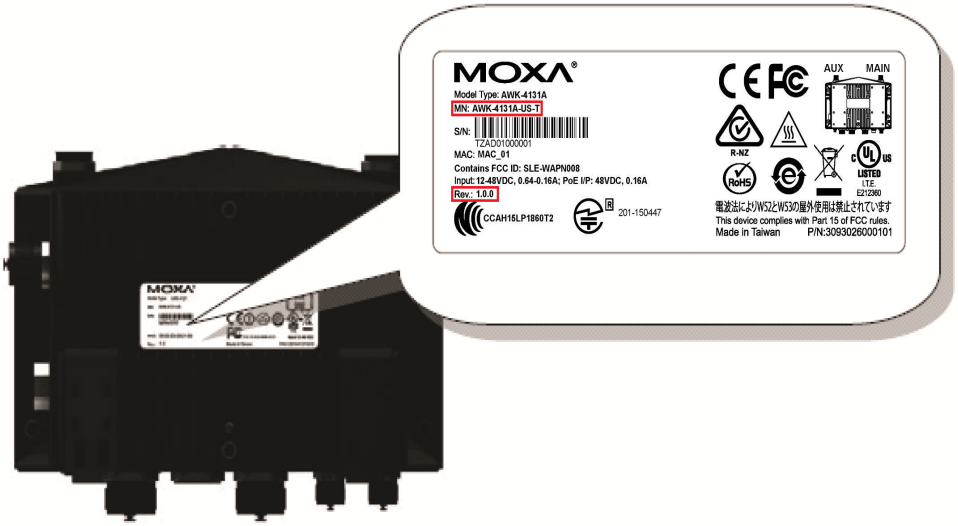
About This User's Manual

This manual is mainly designed for, but no limited to, the following hardware and firmware for the AWK-4131A:

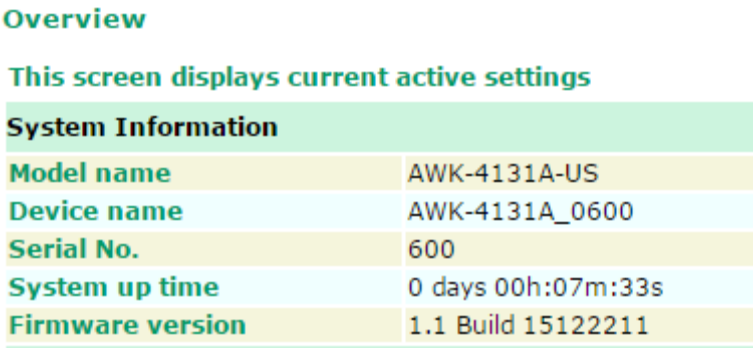
- Hardware Revision: **1.0.0**
- Firmware Version: **1.1**

You are strongly recommended to visit Moxa's website (http://www.moxa.com) and find the latest product datasheet, firmware, QIG (Quick Installation Guide), UM (User's Manual) and related information.

NOTE You can find out the hardware revision number of AWK-4131A on the side label.



The firmware version number can be seen on the Overview page, as follows:



Firmware Recovery

When the LEDs of **FAULT**, **Signal Strength**, **CLIENT**, **BRIDGE** and **WLAN** all light up simultaneously and blink at one-second interval, it means the system booting has failed. It may result from some wrong operation or issues such as an unexpected shutdown during firmware update. The AWK-4131A is designed to help administrators recover such damage and resume system operation rapidly. You can refer to the following instructions to recover the firmware:

Connect to the AWK-4131A's RS-232 console with **115200bps and N-8-1**. You will see the following message shown on the terminal emulator every one second.

```
Section userdisk Cksum error = 0xa5feadde --> 0x658c5051
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
Press Ctrl-C to enter Firmware Recovering Process.....
```

Press **Ctrl - C** and the following message will appear.

```
Press Ctrl-C to enter Firmware Recovering Process.....
==============================================================================
IP address of AWK-4121 : 0.0.0.0
IP address of TFTP server : 0.0.0.0
==============================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 
```

Enter **2** to change the network setting. Specify the location of the AWK-4131A's firmware file on the TFTP server and press **y** to write the settings into flash memory.

```
==============================================================================
IP address of AWK-4121 : 0.0.0.0
IP address of TFTP server : 0.0.0.0
==============================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 2

IP address of AWK-4121 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
Update RedBoot non-volatile configuration - continue (y/n)? y
```

AWK-4131A restarts and the "Press Ctrl-C to enter Firmware Recovery Process…" message will reappear. Press **Ctrl-C** to enter the menu and select **1** to start the firmware upgrade process.

```
Press Ctrl-C to enter Firmware Recovering Process.....
==============================================================================
IP address of AWK-4121 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
==============================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 1
```

Select **0** in the sub-menu to load the firmware image via LAN, and then enter the file name of the firmware to start the firmware recovery.

```
==============================================================================
Load method select :
0. Load from LAN
1. Load from serial with Xmodem
q. Abort select.
==============================================================================
Please select item : 0
Please input load image name..
Default file name : AWK-4121.rom
User Input file name : AWK-4121_1.0.rom
```

DoC (Declaration of Conformity)

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, (example – use only shielded interface cables when connecting to computer or peripheral devices). Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. This transmitter must not be co-located or operated in conjunction with any other antenna or transmitter.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 cm between the radiator & your body.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC 15.407(e): Within the 5.15-5.25 GHz band, U-NII devices are restricted to indoor operations to reduce any potentially harmful interference to co-channel MSS operations.

NOTE The availability of some specific channels and / or operational frequency bands are country dependent and are firmware programmed at the factory to match the intended destination. The firmware setting is not accessible by the end user.

RED Compliance Statement

Moxa declares that the apparatus AWK-4131A complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

The essential requirements laid down in Directive 1999/5/EC, which are relevant to fixed-line terminal equipment, i.e. to ensure the protection of health and safety of persons and of domestic animals and the protection of property and an adequate level of electromagnetic compatibility, are appropriately covered by Directive 2014/35/EU of the European Parliament and of the Council and Directive 2014/30/EU of the European Parliament and of the Council. This Directive should therefore not apply to fixed-line terminal equipment.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines for the manufacturer of this device and that of the computer manufacturer must therefore be followed at all times to ensure the safe use of equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France (with Frequency channel restrictions), Germany, Greece, Ireland, Italy, Luxembourg, Portugal, Spain, Sweden, The Netherlands, and United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states Norway and Switzerland.

EU Countries Not Intended for Use

None.

Potential Restrictive Use

France: Only channels 10, 11, 12, and 13.