AirWorks AWK-1131A Series User Manual

Version 13.4, July 2025

www.moxa.com/products

AirWorks AWK-1131A Series User Manual

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

Copyright Notice

Trademarks

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

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Introduction

The AWK-1131A industrial a/b/g/n high speed wireless access point products are ideal wireless solutions for hard-to-wire applications that use mobile equipment connected over a TCP/IP network. The AWK-1131A is rated to operate at temperatures ranging from 0 to 60°C for standard models and -40 to 75°C for wide temperature models, and is rugged enough for any harsh industrial environment.

Overview

The AWK-1131A industrial wireless AP/client meets the growing need for faster data transmission speeds by supporting IEEE 802.11n technology with a net data rate of up to 300 Mbps. The AWK-1131A is compliant with the industrial standards and approvals, covering operating temperature, power input voltage, surge, ESD and vibration. The two redundant DC power inputs increase the reliability of the power supply. The AWK-1131A can operate on either the 2.4 or 5 GHz bands and is backwards-compatible with existing 802.11a/b/g deployments to future-proof your wireless investments.

Package Checklist

Moxa's AWK-1131A is shipped with the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- AWK-1131A wireless AP/client
- 2 2.4/5 GHz antennas: ANT-WDB-ARM-02
- DIN-rail kit
- 1 plastic RJ45 protective cap
- Quick installation guide (printed)
- Warranty card

✏ **NOTE**

The above items come with the standard AWK-1131A model, but the package contents might vary for customized versions.

Product Features

- IEEE802.11a/b/g/n compliant
- Advanced wireless security
  - ➢ 64-bit and 128-bit WEP encryption, WPA /WPA2-Personal and Enterprise (IEEE 802.1X/RADIUS, TKIP, and AES)
  - ➢ SSID enable/disable
  - ➢ Packet access control & filtering
- Turbo Roaming for rapid handover (Client mode)
- ABC-01 for configuration import/export
- RS-232 console management
- DIN-rail mounting (standard) or wall mounting (optional)
- IP30-rated high-strength metal housing

Functional Design

LAN Port

The AWK-1131A comes standard with 1 Gigabit port (Ethernet RJ45). The LAN LED will light up when the LAN cable is inserted.

RJ45 Ethernet port
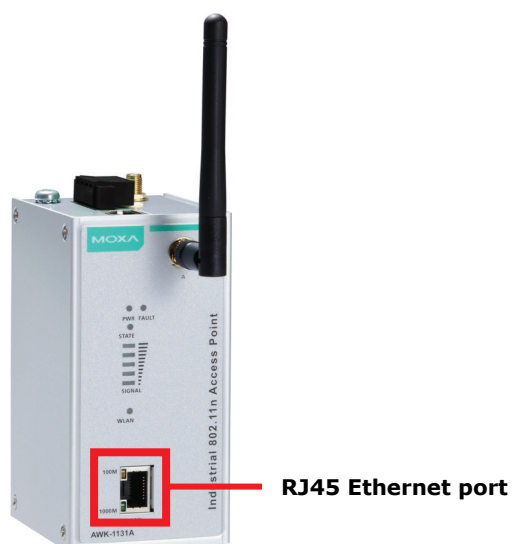
LED Indicators

The LEDs on the front panel of the AWK-1131A provide a quick and easy means of determining the current operational status and wireless settings.

The **FAULT** LED indicates system failures and user-configured events. If the AWK-1131A cannot retrieve the IP address from a DHCP server, the **FAULT** LED will blink at one second intervals. The **SIGNAL** LEDs indicate signal strength, and only operate in **Client** mode.
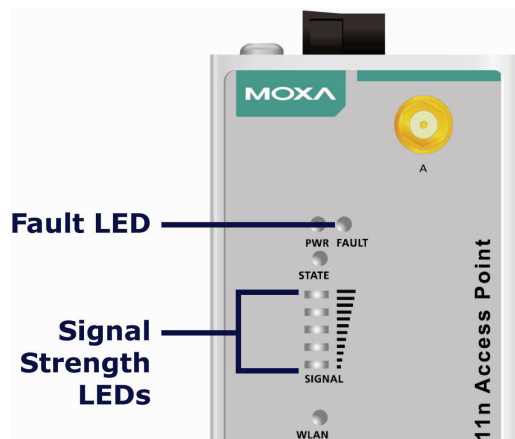
The following table summarizes how to read the device's wireless settings from the LED displays.

LED	Color	State	Description
Front Panel LED Indicators (System)			
PWR	Green	On	Power is being supplied from power input 1&2.
		Off	Power is not being supplied from power input 1&2.
FAULT	Red	Blinking (fast at 0.5-sec intervals)	Cannot get an IP address from the DHCP server
		Blinking (slow at 1-sec intervals)	IP address conflict
		Off	Error condition does not exist.
STATE	Green/ Red	Green	Software Ready
		Green/Blinking at 1-sec intervals	The AWK has been located by AWK Search Utility.
		Red	Booting error condition
SIGNAL (5 LEDs)	Green	On	Signal level(for Client mode only)
		Off	
WLAN	Green	On	WLAN function is in Client mode and AWK has established a link with an AP.
		Blinking	WLAN data communication is run in Client mode
		Off	WLAN is not in Client Mode or AWK has not established a link with an AP.
	Amber	On	WLAN function is in AP mode.
		Blinking	WLAN's data communication is run in AP mode
		Off	WLAN is not in use or not working properly
TP Port(RJ45) LED Indicators (Port Interface)			
1000M	Green	On	TP port's 1000Mbps link is active.
		Blinking	Data is being transmitted at 1000 Mbps
		Off	TP port's 1000Mbps link is inactive.
10/100M	Amber	On	TP port's 10/100Mbps link is active.
		Blinking	Data is being transmitted at 10/100 Mbps
		Off	TP port's 10/100Mbps link is inactive.

⚠ **ATTENTION**

When the system fails to boot, the LEDs for **STATE** (Green), **FAULT**, and **WLAN** will all light up simultaneously and blink at one-second intervals. This might be due to improper operation or issues such as an unexpected shutdown while updating the firmware. To instruction on recovering the firmware, refer to the "Firmware Recovery" section in Chapter 6.

Beeper

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

Reset Button

The **RESET** button is located on the rear panel of the AWK-1131A. You can reboot the AWK-1131A 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-1131A.

RESET Button

---
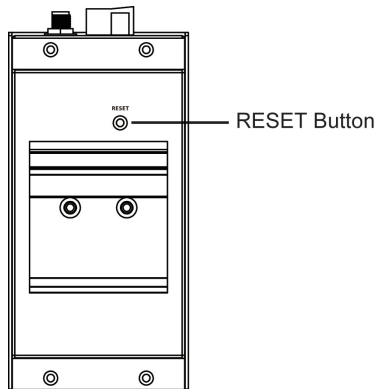
2. Getting Started

This chapter explains how to install Moxa's AirWorks AWK-1131A for the first time, and quickly set up your wireless network and test whether the connection is running well. The Function Map discussed in the third section provides a convenient means of determining which functions you need to use.

First-time Installation and Configuration

Before installing the AWK-1131A, make sure that all items in the Package Checklist are in the box. You will need access to a notebook computer or PC equipped with an Ethernet port. The AWK-1131A has a default IP address that must be used when connecting to the device for the first time.

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

The AWK-1131A can be powered by a DC power input. The AWK-1131A will use whichever power source you choose.

Step 2: **Connect the AWK-1131A to a notebook or PC.**

Since the AWK-1131A supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the AWK-1131A to a computer. The LED indicator on the AWK-1131A's LAN port will light up when a connection is established.

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

Choose an IP address on the same subnet as the AWK-1131A. Since the AWK-1131A'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-1131A will be reset to factory default settings and the IP address will be reset to **192.168.127.253**.

Step 4: **Use the web-based manager to configure the AWK-1131A**

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:
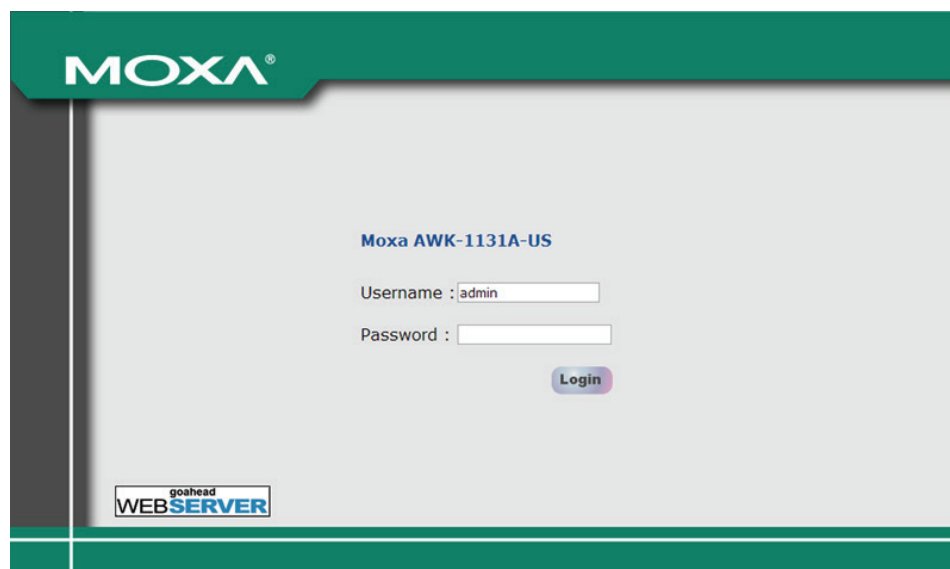
✎ NOTE

The default login credentials are:

> Username: **admin**
>
> Password: **moxa**

Once successfully logged in using the default credentials, you will be prompted to update the password. To enhance security and allow configuration changes, we strongly recommend updating the default password. You cannot change any configuration settings on the AWK when logged in with the default password.

✎ NOTE

If you logged in to the AWK via MXconfig (Java version) using the default credentials, you will be in read-only mode and cannot modify any settings. To modify the password and unlock all functions, navigate to the **Multiple Function Setting > Password Setting** page in MXconfig.
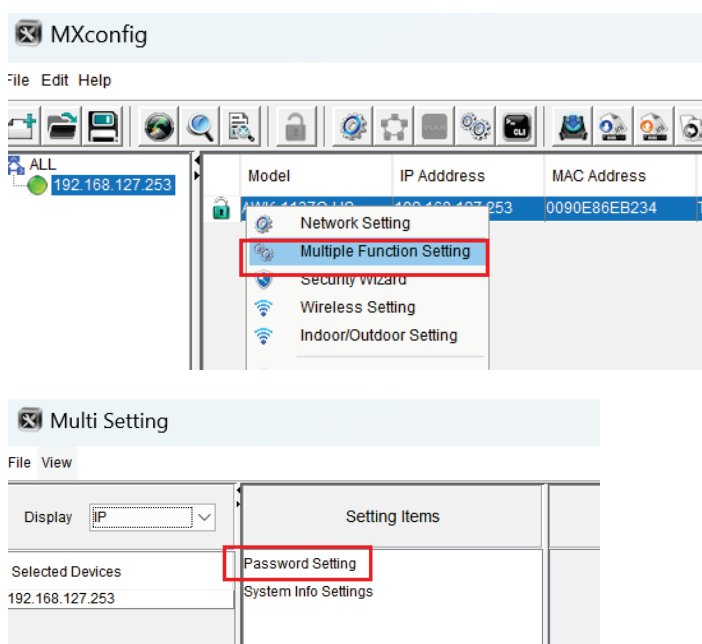
✎ NOTE

After you click **Submit** to apply changes the web page is refreshed (indicated by an "**(Updated)**" status appearing next to the title) and a blinking reminder to restart the device of the new settings to take effect, will be shown on the upper-right corner of the web page:
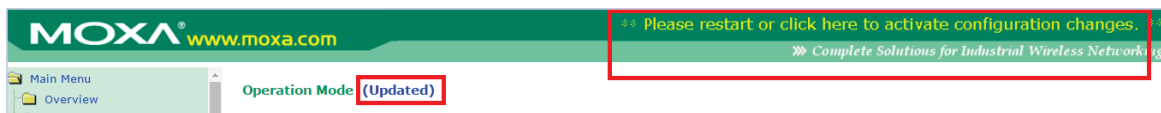
To activate the changes click **Restart** and then **Save and Restart** after you change the settings. About 30 seconds are needed for the AWK-1131A to complete the reboot procedure.

Step 5: **Select the AWK-1131A operation mode.**

By default, the AWK-1131A's operation mode is set to AP. You can change to Client mode in **Wireless LAN Setup (Operation Mode**. Detailed information about configuring the AWK-1131A's operation can be found in Chapter 3.

Step 6: **Test communications.**

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 installing the AWK-1131A you can run a sample test to make sure the AWK-1131A and wireless connection are functioning normally. Two testing methods are described below. Use the first method if you are using only one AWK-1131A device, and use the second method if you are using two or more AWK-1131A units.

How to Test One AWK-1131A

If you are only using one AWK-1131A, you will need a second notebook computer equipped with a WLAN card. Configure the WLAN card to connect to the AWK-1131A (the default SSID is **MOXA**), and change the IP address of the second notebook (Notebook B) so that it is on the same subnet as the first notebook (Notebook A), which is connected to the AWK-1131A.

After configuring the WLAN card, establish a wireless connection with the AWK-1131A and open a DOS window on Notebook B. At the prompt, type

ping *<IP address of notebook A>*

and then press **Enter** (see the figure below). A "Reply from IP address …" response means the communication was successful. A "Request timed out." response means the communication failed. In this case, recheck the configuration to make sure the connections are correct.
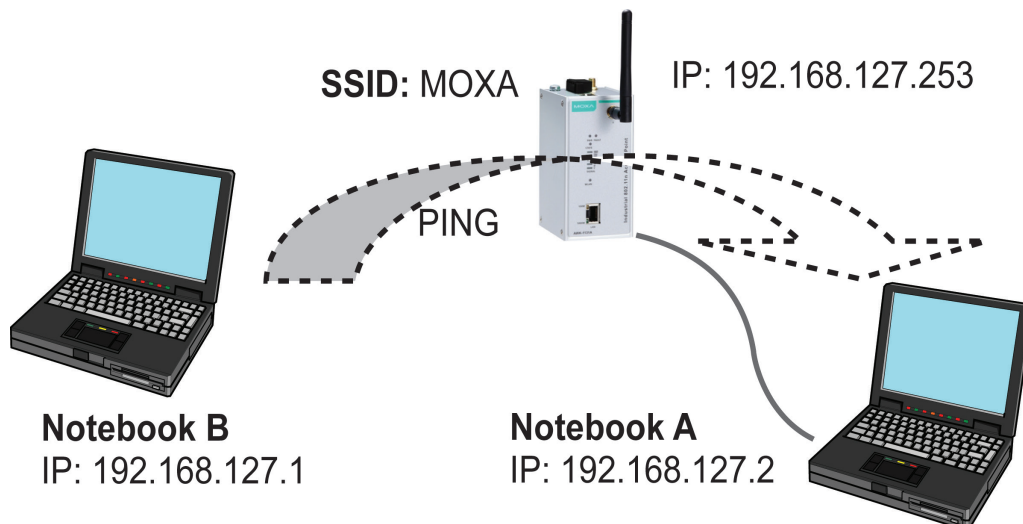
How to Test Two or More AWK-1131A Units

If you have two or more AWK-1131A units, you will need a second notebook computer (Notebook B) equipped with an Ethernet port. Use the default settings for the first AWK-1131A connected to notebook A

and change the second or third AWK-1131A connected to notebook B to Client mode, and then configure the notebooks and AWK-1131A units properly.

Client
IP: 192.168.127.252

PING

AP
IP: 192.168.127.253

SSID: MOXA

Notebook B
IP: 192.168.127.1

Notebook A
IP: 192.168.127.2

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 Map

Main Menu ——————————————— Quick overview of the AWK-1131A's status

  Overview ————————————

General Setup ——————————— Basic settings for administering the AWK-1131A

  System Information

  Network Settings

  System Time

Wireless LAN Setup

  Operation Mode

  WLAN ————————————————— Essential settings related to establishing a wireless network

    Basic WLAN Setup

    WLAN Security Settings

    Advanced WLAN Settings

    WLAN Certificate Settings

Advanced Setup

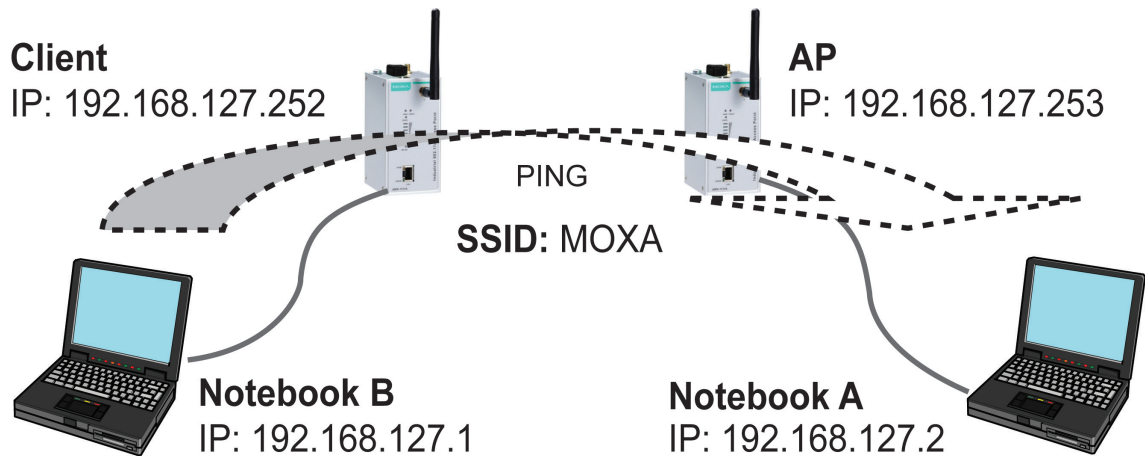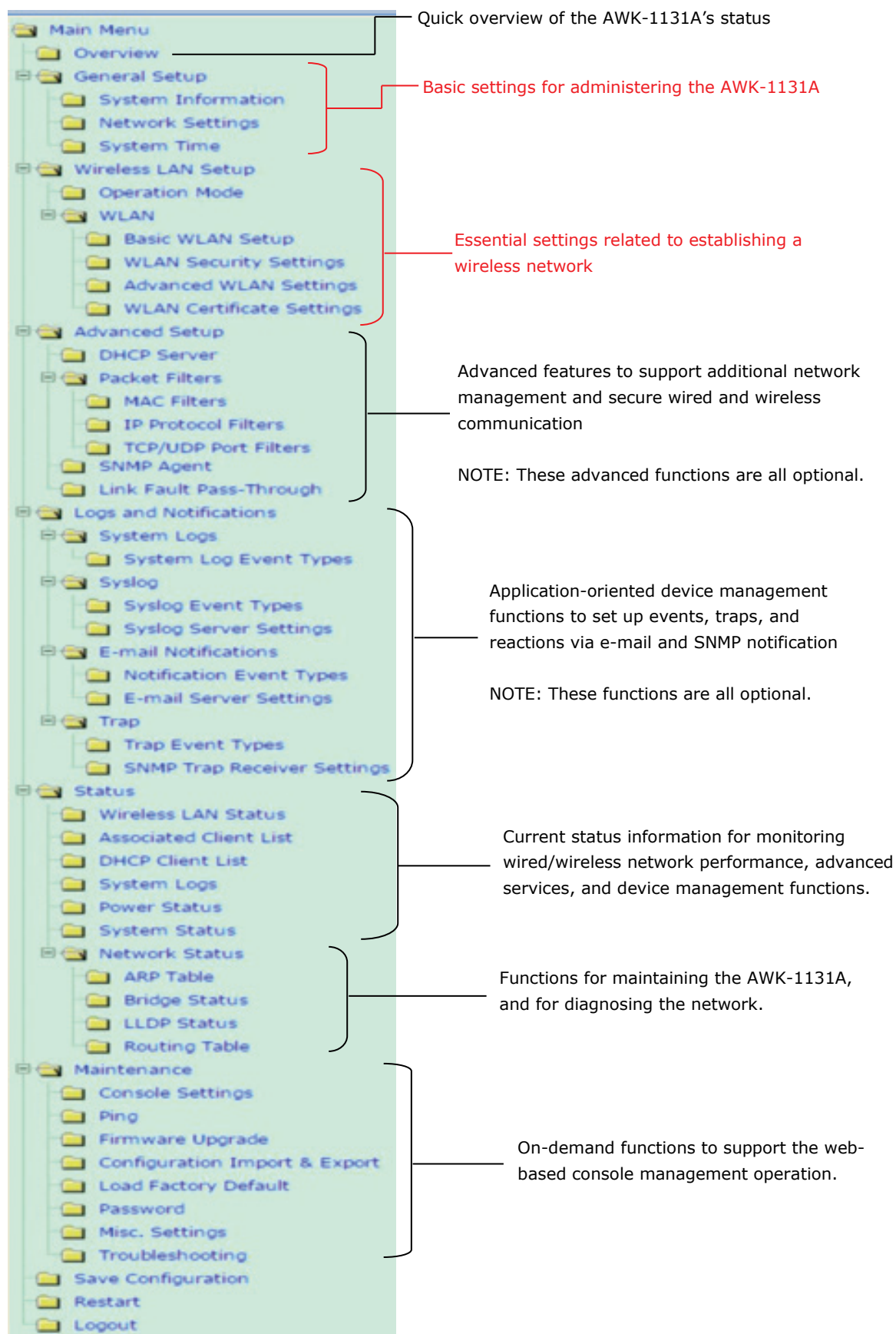 DHCP Server ————————————— Advanced features to support additional network management and secure wired and wireless communication

  Packet Filters

    MAC Filters

    IP Protocol Filters

    TCP/UDP Port Filters

  SNMP Agent ————————————— NOTE: These advanced functions are all optional.

  Link Fault Pass-Through

Logs and Notifications

  System Logs

    System Log Event Types

  Syslog ————————————————— Application-oriented device management functions to set up events, traps, and reactions via e-mail and SNMP notification

    Syslog Event Types

    Syslog Server Settings

  E-mail Notifications

    Notification Event Types

    E-mail Server Settings ————— NOTE: These functions are all optional.

  Trap

    Trap Event Types

    SNMP Trap Receiver Settings

Status

  Wireless LAN Status

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

  DHCP Client List

  System Logs

  Power Status

  System Status

  Network Status

    ARP Table ——————————————— Functions for maintaining the AWK-1131A, and for diagnosing the network.

    Bridge Status

    LLDP Status

    Routing Table

Maintenance

  Console Settings

  Ping

  Firmware Upgrade

  Configuration Import & Export —— On-demand functions to support the web-based console management operation.

  Load Factory Default

  Password

  Misc. Settings

  Troubleshooting

Save Configuration

Restart

Logout

3. Web Console Configuration

In this chapter, we explain all aspects of web-based console configuration. Moxa's easy-to-use management functions help you set up your AWK-1131A and make it easy to establish and maintain your wireless network.

Web Browser Configuration

Moxa AWK-1131A'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 Chrome version 109.0.5414.120 (Official Build, 64-bit).
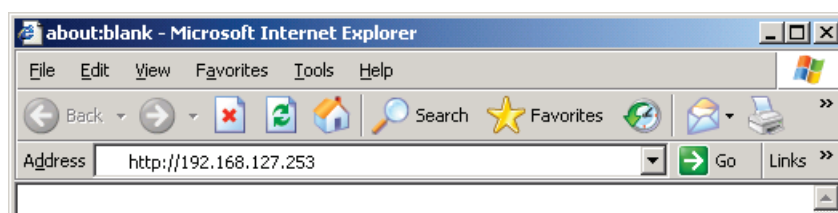

✏️ **NOTE**

To use the AWK-1131A's management and monitoring functions from a PC host connected to the same LAN as the AWK-1131A, you must make sure that the PC host and the AWK-1131A are on the same logical subnet.

The Moxa AWK-1131A's default IP is **192.168.127.253**.

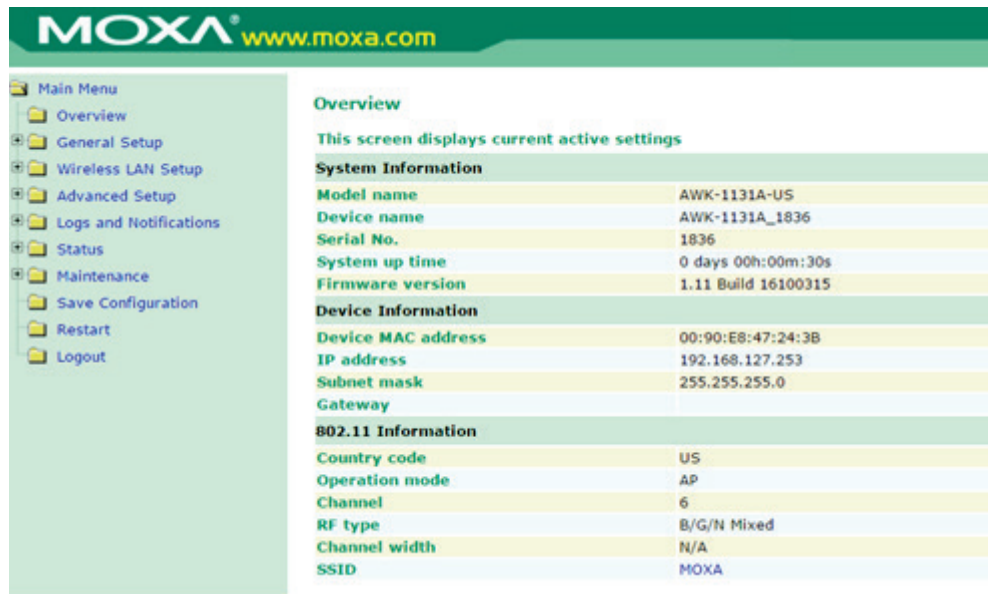Follow these steps to access the AWK-1131A's web-based console management interface.

1. Open your web browser (e.g., Internet Explorer) and type the AWK-1131A's IP address in the address field. Press **Enter** to establish the connection.

2. In the Web console Login page displayed, enter the password (default Username/password = **admin/moxa**) and then click **Login** to continue.

You might have to wait a few moments for the web page to download to your computer. Note that the Model name and IP address of your AWK-1131A are both shown in the title bar of the web page. This information can be used to help you identify multiple AWK-1131A units.

3. Use the menu tree on the left side of the window to open the function pages to access each of the AWK-1131A's functions.

In the following paragraphs, we describe each AWK-1131A 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-1131A is shown as AWK-1131A-XX, where XX indicates the country code. The country code indicates the AWK-1131A version and which frequencies it uses. We use **AWK-1131A-US** as an example in the following figures. (The country code and model name that appears on your computer screen might be different from the one shown here.)

Overview

The **Overview** page summarizes the AWK-1131A's current status. The information is categorized into several groups: **System Information, Device Information** and **802.11 Information**.

Overview

This screen displays current active settings

System Information

Model name	AWK-1131A-US
Device name	AWK-1131A_1836
Serial No.	1836
System up time	0 days 00h:00m:30s
Firmware version	1.11 Build 16100315

Device Information

Device MAC address	00:90:E8:47:24:3B
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	Client
Channel	Not connected
Channel width	N/A
RF type	B/G/N Mixed
SSID	MOXA
MAC	00:90:E8:6A:8E:4D
Security mode	OPEN
Current BSSID	N/A
AP IP address	N/A
Signal level	▫▫▫▪▪
Signal strength	-98 dBm
Noise floor	-98 dBm
SNR	N/A

Transmission Information

Rate	N/A
Power	18 dBm

Outgoing Packets

Total sent	0
Packets with errors	0
Packets dropped	240

Incoming Packets

Total received	0
Packets with errors	0
Packets dropped	0

> ✏️ **NOTE**
>
> The **802.11 Information** that is displayed might be different for different operation modes. For example, **Current BSSID**, **Signal strength**, and **SNR** are only available under Client operation modes.

Quick Setup

The AWK-1131A 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 a link at the top of the page to go to a specific step.

> ✏️ **NOTE**
>
> Move the cursor on the question mark symbol next to an entry field to view additional details regarding the field.

In the **Wi-Fi Settings** step, you can configure the basic Wi-Fi settings and 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 a channel analysis tool.

| 1. | Device Info. and IP Settings | ▶▶▶ | 2-1. | Wi-Fi Settings | ▶▶▶ | 2-2. | Security | ▶▶▶ | 2-3. | Turbo Roaming (Client Only) | ▶▶▶ | 3. | Review Settings |

Basic Settings

| Operation mode | AP ▾ |
| SSID | MOXA |

RF Settings

| RF type | B/G/N Mixed ▾ |
| Channel | 1 ▾ |

Channel Usage

| Channel Survey | Survey ❓ |

Channel Survey takes 4 seconds. The Wi-Fi communication may disconnect during Channel Survey.

Cancel   Back   Next

Channel Usage

Channel Survey   Survey ❓

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, expressed in a percentage value. Both the 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 General Setup group includes the most commonly used settings required by administrators to maintain and control the AWK-1131A.

System Information

The **System Information** items, especially *Device name* and *Device description*, are displayed and included on the **Overview** page, in SNMP information, and in alarm emails. Setting **System Information** items makes it easier to identify the different AWK-1131A units connected to your network.

Device name

Setting	Description	Factory Default
Max. 31 of characters	This option is useful for specifying the role or application of different AWK-1131A units.	Model name_<Last 3 bytes of the device MAC>

Device location

Setting	Description	Factory Default
Max. of 31 characters	Specifies the location of different AWK-1131A units.	None

Device description

Setting	Description	Factory Default
Max. of 31 characters	Use this space to record a more detailed description of the AWK-1131A	None

Device contact information

Setting	Description	Factory Default
Max. of 31 characters	Provides 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-1131A.	None

Network Settings

The Network Settings configuration panel allows you to modify the usual TCP/IP network parameters.

Network Settings for AP/Client Operation Modes

IP address assignment

Setting	Description	Factory Default
DHCP	The AWK-1131A's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the AWK-1131A's IP address manually.	

IP address

Setting	Description	Factory Default
AWK-1131A's IP address	Identifies the AWK-1131A on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
AWK-1131A's subnet mask	Identifies the type of network to which the AWK-1131A 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-1131A'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-1131A'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

MTU

Setting	Description	Factory Default
576 to 2290	MTU (Maximum Transmission Unit) refers to the maximum size of an IP packet that can be transmitted without fragmentation over a given medium.	1500

✎ **NOTE**

The MTU setting applies to all networking interfaces including Ethernet and Wi-Fi interfaces.

System Time

The AWK-1131A 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.

System Time

	Date (YYYY/MM/DD)	Time (HH:MM:SS)
Current local time	2015 / 05 / 29	08 : 11 : 54
		Set Time

Time protocol	SNTP
Time zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼
Daylight saving time	☐ Enable
Time server 1	time.nist.gov
Time server 2	
Time sync interval	600 (600~9999 seconds)

Submit

The *Current local time* shows the AWK-1131A'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 is displayed, which indicates that the change is complete. Local system time will be immediately activated in the system without running Save and Restart.

✎ **NOTE**

The AWK-1131A has a built-in real-time clock (RTC). We strongly recommend that users update the **Current local time** for the AWK-1131A 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-1131A provides the AP/client mode for point-to-multipoint communication.

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.

Sniffer: In order to provide an easier way for our customers to analyze wireless traffic, the AWK-1131A supports a "Sniffer" mode to co-work with Wireshark packet sniffer software.
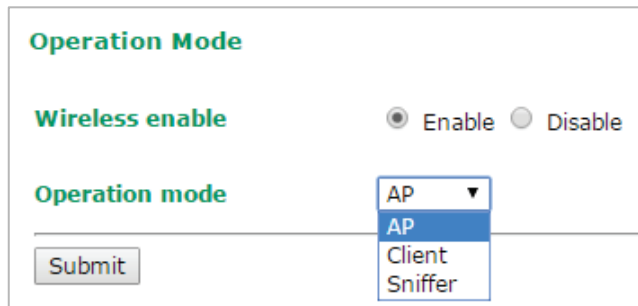
✏️ **NOTE**

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.

Operation Mode

The AWK-1131A supports three operation modes—AP, Client, and Sniffer—each of which plays a distinct role on the wireless network.

Operation Mode

Wireless enable ⦿ Enable ○ Disable

Operation mode AP ▾
                AP
                Client
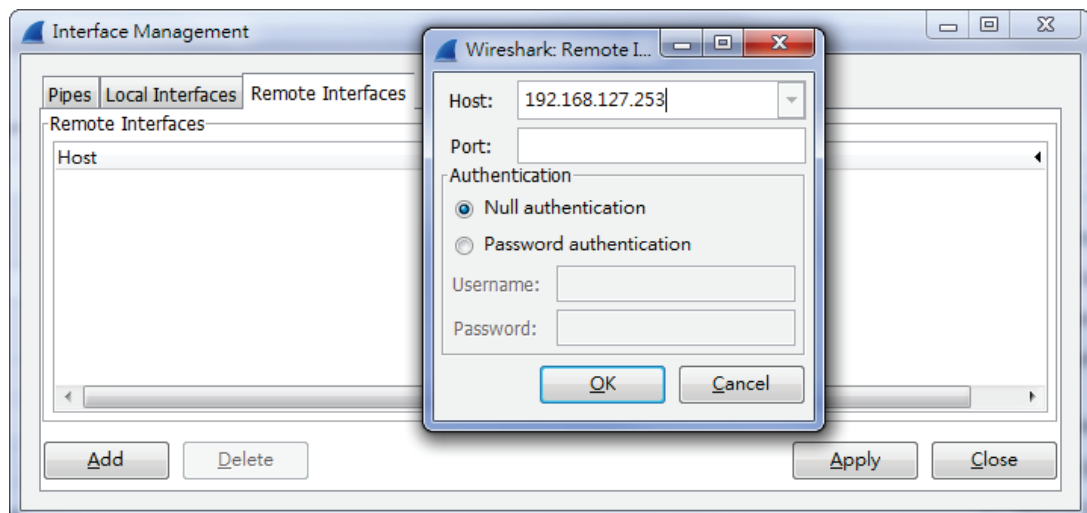   Sniffer

Submit

Wireless enable

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

Operation mode

Setting	Description	Factory Default
AP	The AWK-1131A plays the role of a wireless access point	
Client	The AWK-1131A plays the role of wireless Client	AP
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-1131A and then save/reboot the device.
2. Connect the AWK-1131A 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-1131A.

Interface Management

Pipes | Local Interfaces | Remote Interfaces
Remote Interfaces
Host

Wireshark: Remote I...
Host: 192.168.127.253
Port:
Authentication
⦿ Null authentication
○ Password authentication
Username:
Password:
OK   Cancel

Add   Delete   Apply   Close

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:

Basic WLAN Setup

Operation mode	AP
Indoor/Outdoor	Indoor ▾
RF type	B/G/N Mixed ▾
Channel width	20 MHz ▾
Channel	6 (2437MHz) ▾
SSID	MOXA
SSID broadcast	◉ Enable ○ Disable
Management frame encryption	○ Enable ◉ Disable
Management frame encryption password	••••••••

Client isolation

Client isolation	No isolation ▾

Submit

✏️ **NOTE**

When you switch to **Client** mode, a **Site Survey** button will be available on the Basic WLAN Setup panel. Click this 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 update the site-survey table.

Basic WLAN Setup

Operation mode	Client
RF type	B/G/N Mixed ▼
Channel width	20 MHz ▼
SSID	MOXA [Site Survey]

[Submit]

Site Survey

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

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 might operate at a slower speed when 802.11b clients are on the network	

Setting	Description	Factory Default
G/N Mixed	Supports IEEE 802.11g/n standards, but 802.11n might operate at a slower speed when 802.11g clients are on the network	
B/G/N Mixed	Supports IEEE 802.11b/g/n standards, but 802.11g/n might operate at a slower speed when 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 might operate at a slower speed when 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-1131A 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)

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

Channel bonding shows the channel with which the AP will bond if **Channel width** is set to 20/40 MHz.

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	SSID can be broadcast or not	Enable

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

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.

WLAN Security Settings

The AWK-1131A 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-1131A 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-1131A can support three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.

WLAN Security Settings

SSID	MOXA
Security mode	Open ▼
	Open
	WEP
	WPA
	WPA2

Submit

Security mode

Setting	Description	Factory Default
Open	No authentication	Open
WEP	Static WEP is used	
WPA	WPA is used	
WPA2	Fully supports IEEE 802.11i with "TKIP/AES + 802.1X"	

Open

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

WEP (only for legacy mode)

> **✏️ 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 in 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector.

The AWK-1131A 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.

WLAN Security Settings

SSID	MOXA
Security mode	WEP ▼
Authentication type	Open ▼
Key type	HEX ▼
Key length	64 bits ▼
Key index	1 ▼
WEP key 1	
WEP key 2	
WEP key 3	
WEP key 4	

Submit

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 hex-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 passphrase cannot contain the following special characters: ` ' " | ; & $	None

WPA/WPA2-Personal

WPA (Wi-Fi Protected Access) and WPA2 provide 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-1131A 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.

WLAN Security Settings

SSID	MOXA
Security mode	WPA2
WPA type	Personal
Encryption method	AES
EAPOL version	1
Passphrase	•••••••••• ☐ Show Password
Key renewal	3600 (60~86400 seconds)

Submit

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: ` ' " | ; & $. Check Show Password to display the password in clear text.	None

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 (6 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.

```
WLAN Security Settings

SSID                          MOXA
Security mode                 WPA ▾
WPA type                      Enterprise ▾
Encryption method             AES ▾
EAPOL version                 1 ▾
Primary RADIUS server IP      [            ]
Primary RADIUS server port    [1812       ]
Primary RADIUS shared key     [                       ]
Secondary RADIUS server IP    [            ]
Secondary RADIUS server port  [1812       ]
Secondary RADIUS shared key   [                       ]
Key renewal                   [3600 ]  (60~86400 seconds)

  [ Submit ]
```

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	None

Key renewal

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

WPA/WPA2-Enterprise (for Client)

When used as a client, the AWK-1131A can support three EAP methods (or *EAP protocols*): **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**, corresponding to WPA/WPA2-Enterprise settings on the AP side.

```
WLAN Security Settings

SSID                          MOXA
Security mode                 WPA2 ▼
WPA type                      Enterprise ▼
Encryption method             TKIP ▼
EAPOL version                 1 ▼
EAP protocol                  TLS ▼
Certificate issued to           TLS
Certificate issued by           TTLS
Certificate expiration date     PEAP

  Submit
```

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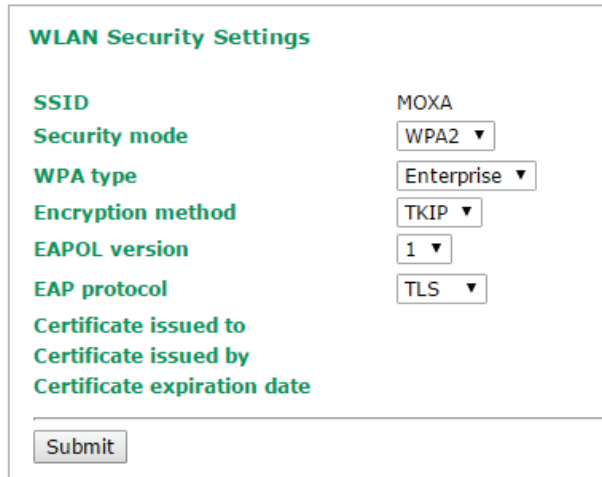
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

Before choosing the EAP protocol for your WPA/WPA2-Enterpise 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 the expiration date of the certificate

---

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-1131A 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 might 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.

```
WLAN Security Settings

SSID                        MOXA
Security mode               WPA2    ▼
WPA type                    Enterprise ▼
Encryption method           TKIP    ▼
EAPOL version               1       ▼
EAP protocol                TTLS    ▼
TTLS inner authentication   MS-CHAP-V2  ▼
                            PAP
Anonymous name              CHAP
User name                   MS-CHAP
Password                    MS-CHAP-V2

[Submit]
```

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-1131A 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.

Advanced WLAN Settings

Transmission rate	Auto ▾
Minimum transmission rate	0 (0~11Mbps, 0 to disable)
Multicast rate	11M ▾
Maximum transmission power	23 dBm ▾
Beacon interval	100 (40 to 1000 ms)
Auth/Assoc timeout	30 (30 to 200 ms)
DTIM interval	1 (1 to 15)
Inactive timeout	60 (8 to 240 second)
Fragmentation threshold	2346 (256 to 2346)
RTS threshold	2346 (32 to 2346)
Antenna	Both ▾ • Regarding Wi-Fi performance, we recommend you to use two antennas to ensure high throughput.
WMM	Enable ▾
Turbo Roaming	☐ Enable
MAC clone	Disable ▾
Remote connection check	☐ Enable

Submit

Transmission rate

Setting	Description	Factory Default
Auto	The AWK-1131A 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-1131A 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, providing the wireless clients are capable of handling the configured rate	6M

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.	10 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)

Auth/Assoc timeout (for Client mode only)

Setting	Description	Factory Default
30 to 200 ms	Specifies how long before the authentication/association management times out.	30 ms

Inactive timeout (for AP mode only)

Setting	Description	Factory Default
8 to 240 seconds	Specifies how long before the 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-1131A 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.

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

* 2T2R is 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 the 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

AP-based disconnection

Setting	Description	Factory Default
Enable/Disable	Enable or disable AP-based disconnection. This feature aims to make sure the client is always associated to the AP with the best SNR/signal strength. The associated client will be forced to connect to another AP when the SNR/Signal strength drops below the configured threshold during the specified monitoring period.	Disable

When AP-based disconnection is enabled, the following parameters will be shown:

- **Threshold:** Specify either the signal-to-noise (SNR) or signal strength threshold to determine when clients will roam to another AP once the respective value drops below the set threshold.
- **Client-signal monitor time:** Specify the duration of the signal check (in seconds). The default is 3 seconds.

Wireless link health check

Setting	Description	Factory Default
Enable/Disable	Enable or disable wireless link health check. When enabled, this feature will help detect and recover unstable connections.	Disable

---

When Wireless link health check is enabled, the following parameters will be shown:

- **Threshold:** Specify either the signal-to-noise (SNR) or signal strength threshold to determine when the AP will perform a health check on the wireless client connections.
- **Count:** Specify the number of ping packets that will be sent in a check.
- **Timeout:** Specify the duration (in ms) of receiving no response before the check times out.
- **Interval:** Specify the ping interval (in ms).

Turbo Roaming (for Client mode only)

Setting	Description	Factory Default
Enable/Disable	Moxa's Turbo Roaming can enable rapid handover when the AWK-1131A, 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.

✏️ **NOTE**

While the AWK is background scanning, the 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:** This function is used to check the usable channels for roaming. Select All to check all channels or select Partial to check up to 11 pre-defined communication and roaming channels.

✏️ **NOTE**

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 the turbo roaming function to recover the network connection faster when an AP has a sudden disconnection (such as losing power).

✏️ **NOTE**

Enabling this feature causes the AWK-1131A to send out alive check packets every 10 ms when there is no traffic; the high transmission frequency of 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 the current access point is no long available, the surrounding access points must have good enough connection qualities (SNR/Signal Strength) in order to be the qualified as AP candidates for association.

Turbo Roaming	☑ Enable
RF type	B/G/N Mixed
Roaming threshold	◉ SNR 40 dB (5 to 60)
	○ Signal Strength -55 dBm (-100 to -35)
Roaming difference	7 (5 to 20)
Scan channels	6 (2437MHz) ▼
	Not Scanning ▼
	Not Scanning ▼
	Not Scanning ▼
	Not Scanning ▼
	Not Scanning ▼
	Not Scanning ▼
	Not Scanning ▼
	Not Scanning ▼
	Not Scanning ▼
AP alive check	Disable ▼

> ✎ **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.

MAC clone (for Client mode only)

Setting	Description	Factory Default
MAC clone	Enabling this feature allows the AWK client to clone and use the MAC address of the device connected to the LAN. This overcomes the limitation of the IP-bridged behavior in a MAC-sensitive network (MAC-based communication or MAC-authenticated network).	Disable
MAC clone method	• *Auto:* The AWK client uses the MAC address of the device connected to the LAN if only one device is connected to the 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 use.	-

> ✎ **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:

Remote connection check	☑ Enable
Re-establish WLAN connection	☑ Enable
Device reboot	☐ Enable
Remote host	[_____] (ex: 192.168.127.253)
Check interval	[10] (1 to 30 seconds)
Timeout	[1000] (100 to 10000 ms)
Retry count	[3] (1 to 5)
Retry interval	[1] (1 to 30 seconds)
Reboot count	[3] (0 to 5)

- **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-3313A 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-1131A checks the connection. The range is between 1 to 30 seconds, the default is every 10 seconds.
- **Timeout:** Specify the duration the AWK-1131A 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-1131A 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 mode only)

When EAP-TLS is used, a WLAN Certificate will be required at the client end to support WPA/WPA2-Enterprise. The AWK-1131A 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.

WLAN Certificate Settings

Certificate private password	
Select certificate/key file	Browse...

Submit

Status	
Certificate issued to	
Certificate issued by	
Certificate expiration date	

Current status displays information for the current WLAN certificate, which has been imported into the AWK-1131A. 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, return to step 1 to set the password correctly and then import the certificate file again.

Step 1:

Certificate private password	

Submit

Step 2:

Select certificate/key file		Browse...

Upload Certificate File

✏️ **NOTE**

The WLAN certificate will remain after the AWK-1131A 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-1131A and wireless network system. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. And, SNMP support can make network management easier.

DHCP Server (for AP 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-1131A 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-1131A 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-1131A 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-1131A 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 expires after the lease time is completed.	14400 minutes (10 days)

Packet Filters

The AWK-1131A includes various filters for IP-based LAN-to-WAN packets, as well as WLAN-to-WLAN traffic between different SSIDs. These filters can be configured as a firewall policy to enhance network security.

✏️ **NOTE**

The Packet Filter function does not apply to WLAN-to-WLAN traffic within the same SSID.

MAC Filters

The AWK-1131A's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The AWK-1131A 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

| MAC filters function | Disable ▼ |
| Policy | Drop ▼ |

No.	☐ Active	Name	MAC Address
1	☐		
2	☐		
3	☐		
4	☐		
5	☐		
6	☐		
7	☐		
8	☐		
9	☐		
10	☐		
.			
.			
.			
50	☐		
51	☐		
52	☐		
53	☐		
54	☐		
55	☐		
56	☐		
57	☐		
58	☐		
59	☐		
60	☐		

Submit

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-1131A'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-1131A 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

IP protocol filters function	Disable ▾
Policy	Drop ▾

No.	☐ Active	Protocol	Source IP	Source Netmask	Destination IP	Destination Netmask
1	☐	All ▾				
2	☐	All ▾				
3	☐	All ▾				
4	☐	All ▾				
5	☐	All ▾				
6	☐	All ▾				
7	☐	All ▾				
8	☐	All ▾				
9	☐	All ▾				
10	☐	All ▾				
.						
.						
.						
50	☐	All ▾				
51	☐	All ▾				
52	☐	All ▾				
53	☐	All ▾				
54	☐	All ▾				
55	☐	All ▾				
56	☐	All ▾				
57	☐	All ▾				
58	☐	All ▾				
59	☐	All ▾				
60	☐	All ▾				

Submit

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-1131A'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-1131A 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

| TCP/UDP port filters function | Disable ▼ |
| Policy | Drop ▼ |

No.	☐ Active	Source Port	Destination Port	Protocol	Application Name
1	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
2	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
3	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
4	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
5	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
6	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
7	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
8	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
9	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
10	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
.					
.					
.					
50	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
51	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
52	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
53	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
54	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
55	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
56	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
57	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
58	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
59	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]
60	☐	[ ] ~ [ ]	[ ] ~ [ ]	TCP ▼	[ ]

[Submit]

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**

SNMP Agent

The AWK-1131A 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-1131A 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

Protocol Version	Setting on UI web page	Authentication Type	Data Encryption	Method
	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	
MD5	Provide authentication based on the HMAC-MD5 algorithms. 8-character passwords are the minimum requirement for authentication.	No Auth
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	
DES	DES-based data encryption	Disable
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 AWK-1131A's enterprise value, which is a fixed value.

Link Fault Pass-Through (for Client 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.

Gratuitous ARP (for Client/Client-router mode only)

Gratuitous ARP is a broadcast packet that the client (the device) sends to all nodes to share or update the latest IP/MAC mapping table to prevent nodes from dropping packets.

Gratuitous ARP enable

Setting	Description	Factory Default
Enable/Disable	Enable or disable Gratuitous ARP functionality. Enabling this function helps detect and prevent unstable connections.	Disable

When enabled, the function behaves differently depending on the operation mode of the device. Refer to the following descriptions:

- **Client** mode: You can enter the IP/MAC address of the legacy device connected to the Ethernet port of the AWK device. The AWK will send the GARP packet:
  - a. To **LAN** with the **user-defined IP/MAC address**. Sending GARP packets to LAN is configurable.
  - b. To **WLAN** with a **user-defined IP address** and **its own MAC address**.
- **Client-Router** mode: You need to enable **NAT** for GARP first to allow the server on the AP side to access the devices connected to the Ethernet ports of the AWK device. The AWK will send the GARP packet to **WLAN** as:
  - a. **N-to-1**: With **its own WAN IP** and **MAC address**.
  - b. **1-to-1**: With its own **WAN MAC address** and the **1-to-1 IP** configured by the user in the NAT configuration.

When Gratuitous ARP is enabled, the following options will be shown:

Gratuitous ARP to LAN

Setting	Description	Factory Default
Enable/Disable	Enable or disable sending Gratuitous ARP packets to LAN	Disable

Send Period

Setting	Description	Factory Default
10-1000 seconds	Specify the interval at which GARP packets are sent (in seconds).	180

IP Address/MAC Address

Setting	Description	Factory Default
IP/MAC address	The corresponding IP/MAC address of the devices under the client. You can specify up to 4 entries.	Empty

⚠️ **ATTENTION**

When specifying an IP or MAC address, you must provide the associated IP or MAC address for that entry.

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-1131A supports different approaches to warn engineers automatically, such as SNMP trap and e-mail.

System Logs

System Log Event Types

All the event group types are shown on this page. Select the event types (groups) that you want to enable by checking the **Enable logging** box next to the event types. By default, all event types are enabled (checked).

The system events log can be viewed at **Status (System Logs**.

System Log Event Types

Event Type	Enable Logging
System-related events	☑ Active
Network-related events	☑ Active
Configuration-related events	☑ Active
Power events	☑ Active

Submit

System-related events	Event is triggered when...
System warm start	The AWK-1131A is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
System cold start	The AWK-1131A is rebooted by power down.
Watchdog triggers reboot	The AWK-1131A 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-1131A is associated with an AP.
WLAN disconnected (for Client/Slave mode)	The AWK-1131A 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-1131A 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-1131A.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The AWK-1131A'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-1131A 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-1131A is powered down in PWR1/2.
PoE transition (On -> Off)	The AWK-1131A is powered down in PoE.
Power 1/2 transition (Off -> On)	The AWK-1131A is powered via PWR1/2.
PoE transition (Off -> On)	The AWK-1131A 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

The event type groups are shown on this page. Select the **Enable Logging** checkbox next to the event type to enable logging of the event. By default, all event types are enabled (checked).

Syslog Event Types

Event Type	Enable Logging
System-related events	☑ Active
Network-related events	☑ Active
Configuration-related events	☑ Active
Power events	☑ Active
RSSI report events	☐ Active

Submit

Syslog Server Settings

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

Syslog Server Settings

Syslog server 1	
Syslog port	514
Syslog server 2	
Syslog port	514
Syslog server 3	
Syslog port	514

Submit

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**

RSSI report events (Only for Client mode) event type is useful for the site survey stage. However, this function increases the traffic load because it needs to use a special utility to retrieve the RSSI values in a tabular format. So, we recommend disabling this function during normal usage.

E-mail Notifications

Notification Event Types

Check the **Active** box next to the event type to enable the event type for email notification. By default, all event types are deactivated (unchecked).

Notification Event Types

Event Type	Enable Notification
Cold start	☐ Active
Warm start	☐ Active
Power 1 transition (On-->Off)	☐ Active
Power 1 transition (Off-->On)	☐ Active
Power 2 transition (On-->Off)	☐ Active
Power 2 transition (Off-->On)	☐ Active
Configuration changed	☐ Active
Console authentication failure	☐ Active
LAN link on	☐ Active
LAN link off	☐ Active

Submit

E-mail Server Settings

You can set up to 4 e-mail addresses to receive alarm emails from the AWK-1131A. 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

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 Update** box is checked.

Certain values for **802.11 Information** might not be displayed based on the different operation modes selected. For example, the **Current BSSID, Signal strength,** and **SNR** parameters are not available in the AP mode.

It is helpful to use the continuously updated information on this page, such as **Signal Level, Noise floor,** and **SNR**, to monitor the signal strength of the AWK-1131A in Client mode.

Wireless LAN Status

☑ Auto Update

Show status of WLAN (SSID: MOXA) ▼

802.11 Information	
Operation mode	Client
Channel	Not connected
Channel width	N/A
RF type	B/G/N Mixed
SSID	MOXA
MAC	00:90:E8:6A:8E:4D
Security mode	OPEN
Current BSSID	N/A
AP IP address	N/A
Signal level	▫▫▫▫▫
Signal strength	-98 dBm
Noise floor	-98 dBm
SNR	N/A
Transmission Information	
Rate	N/A
Power	18 dBm
Outgoing Packets	
Total sent	0
Packets with errors	0
Packets dropped	240
Incoming Packets	
Total received	0
Packets with errors	0
Packets dropped	0

Associated Client List (for AP mode only)

The Associated Client List shows all the clients that are currently associated with a particular AWK-1131A. 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, the IP address will also be displayed.

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

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.

Associated Client List

Show clients for [WLAN (SSID: IW_2.4GHz) ▼]

No	MAC Address	Connection Duration	SNR	Tx (Bytes)	Tx (pkts)	Rx (Bytes)	Rx (pkts)
1	ac:81:12:59:66:2f	0 days 04h:43m:49s	45	333651441	300506	106572118	235173
2	84:3a:4b:39:b7:5c	0 days 01h:16m:05s	50	1459894	3551	957998	3553
3	18:00:2d:44:bf:5d	0 days 00h:36m:33s	22	115818	502	223030	581
4	9c:4e:36:a6:98:08	0 days 00h:20m:05s	18	236663	820	192898	739

[Refresh]

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.

DHCP Client List

	MAC	IP
1.	01:5C:96:9D:29:77:71	192.168.41.229
2.	01:30:10:B3:72:72:7F	192.168.41.142
3.	01:9C:4E:36:A6:98:08	192.168.41.216
4.	01:B4:CE:F6:4E:CB:3C	192.168.41.146
5.	01:90:B6:86:75:A5:28	192.168.41.184
6.	01:8C:70:5A:49:FF:58	192.168.41.127
7.	01:68:09:27:CD:41:43	192.168.41.143
8.	01:5C:C5:D4:75:50:7B	192.168.41.140
9.	01:84:3A:4B:39:B7:5C	192.168.41.181
10.	01:A4:C3:61:03:F0:E2	192.168.41.137
11.	*	192.168.41.226
12.	01:80:86:F2:B2:65:1F	192.168.41.222
13.	01:34:4D:F7:3A:23:FB	192.168.41.122
14.	01:30:75:12:A7:15:0E	192.168.41.139
15.	01:EC:85:2F:88:B3:6A	192.168.41.213
16.	01:30:75:12:F2:59:F9	192.168.41.125
17.	01:78:6C:1C:BF:51:0E	192.168.41.144
18.	01:AC:81:12:59:66:2F	192.168.41.156

[Select All] [Refresh]

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

	MAC	IP
1.	00:13:ce:e1:ee:ef	192.168.127.2

Cut
Copy
Paste
Select All
Print

[Select all] [Refresh]
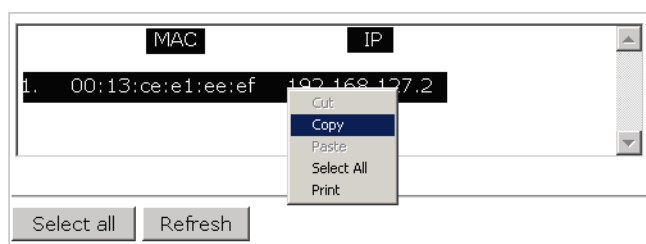
System Logs

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.

```
System Logs

( 983) 2015/05/28,04h:12m:54s System warm start, restarted by console
( 984) 2015/05/28,04h:19m:19s LAN link off
( 985) 2015/05/28,04h:19m:21s LAN link on
( 986) 2015/05/28,07h:45m:59s Configuration changed
( 987) 2015/05/28,07h:46m:23s Power 1 transition (Off -> On)
( 988) 2015/05/28,07h:46m:29s LAN link on
( 989) 2015/05/28,07h:46m:34s System warm start, restarted by console
( 990) 2015/05/28,08h:14m:07s LAN link off
( 991) 2015/05/28,08h:14m:09s LAN link on
( 992) 2015/05/28,08h:21m:55s Configuration changed
( 993) 2015/05/28,08h:22m:20s Power 1 transition (Off -> On)
( 994) 2015/05/28,08h:22m:26s WLAN disconnected, connect time(0sec), (reason 0)
( 995) 2015/05/28,08h:22m:26s LAN link on
( 996) 2015/05/28,08h:22m:29s System warm start, restarted by console
( 997) 2015/05/28,08h:24m:24s Configuration changed
( 998) 2015/05/28,08h:24m:49s Power 1 transition (Off -> On)
( 999) 2015/05/28,08h:24m:55s LAN link on
(1000) 2015/05/28,08h:24m:59s System warm start, restarted by console

[Export Log]  [Clear Log]  [Refresh]
```

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 Update** box is checked.

Power Status

☑ Auto Update

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

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.

System Status

Memory Info		
Total	(kB)	126724
Used	(kB)	48604
Free	(kB)	78120
CPU Info		
Usage	(%)	4.33

Refresh

Network Status

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

ARP Table

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

ARP Table

IP Address	MAC Address
192.168.127.18	F0:DE:F1:DD:A1:ED

Refresh

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.

Bridge Status

Interface	MAC Address
LAN	00:90:E8:22:B1:D9
ath01	00:90:E8:4E:9A:79
LAN	F0:DE:F1:DD:A1:ED

Refresh

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

Maintenance

Maintenance functions provide the administrator with tools to manage the AWK-1131A and wired/wireless networks.

Console Settings

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

Console Settings

Auto logout period   10   (1 to 60 minutes)

Accessible Interfaces

Interface	HTTP	HTTPS	Telnet	SSH	SNMP	Moxa Service
Enable services	☐	☑	☐	☑	☐	☑
Ethernet	☑	☑	☑	☑	☑	☑
WLAN	☑	☑	☑	☑	☑	☑

* If you disable all access portals, you will not be able to remotely access this device.
* If you disable HTTPS, some Moxa service features will be disabled.

Accessible Net List

Accessible Net List   ○ Enable ● Disable

Submit

SSL Certificate (For HTTPS only)

SSL certificate enable   ○ Enable ● Disable
Import SSL certificate file (PKCS12)   [ ] 瀏覽...
SSL certificate passphrase   [ ]

Submit/Import

Ping Command

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.

Ping

| Destination | 192.168.41.233 |

Ping

Otherwise, some, or even all, packets might get lost, as shown in the following figure.

Ping

| Destination | |

Ping

PING 192.168.41.233 (192.168.41.233): 56 data bytes
64 bytes from 192.168.41.233: seq=0 ttl=64 time=0.696 ms
64 bytes from 192.168.41.233: seq=1 ttl=64 time=0.548 ms
64 bytes from 192.168.41.233: seq=2 ttl=64 time=0.565 ms
64 bytes from 192.168.41.233: seq=3 ttl=64 time=0.567 ms

--- 192.168.41.233 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.548/0.594/0.696 ms

Firmware Upgrade

The AWK-1131A 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-1131A 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-1131A will reboot itself.

When upgrading firmware, the AWK-1131A's other functions will be temporarily unavailable until the upgrade is complete.

Firmware Upgrade

| Select firmware file | | Browse... |

Firmware Upgrade and Restart

✎ **NOTE**

For security reasons, a firmware signature mechanism was added to firmware v1.26. As a result, when uploading firmware in v1.26 or higher, you must upload a ZIP file that includes both the firmware file (.rom) and signature file (.sig).

When upgrading to v1.26, you only need to upload the firmware file (.rom).

NOTE

If you need to downgrade from v1.26 to an earlier version for any reason, please Moxa Technical Support.

ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup might damage your AWK-1131A.

Configuration Import and Export

You can back up and restore the AWK-1131A's configuration using the **Configuration Import & Export** function.

In the **Configuration Import** section, click **Browse** to specify the configuration file and click **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 with a general text-editing tool.

You can also back up or restore the ABC-01 configuration using **Export Configuration** or **Import Configuration**.

The SNMP MIB file is also available from SNMP MIB File EXPORT.

To download the configuration to the AWK:

1. Turn off the AWK.
2. Plug in the ABC-01 to the AWK's RS-232 console.
3. Turn on 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 and if configuration format is correct, the AWK will emit three short beeps and continue with the boot-up process.
5. Once the AWK has booted up successfully, it will emit the normal two beeps, and the ready LED will turn to solid green.

Load Factory Default

Use this function to reset the AWK-1131A and rollback all settings (except for Basic WLAN indoor/outdoor settings) to the factory default values. If you want to keep wireless enabled, select the "Enable" option for Wireless before clicking **System Reset**. You can also reset the hardware by pressing the reset button on the top panel of the AWK-1131A.

Load Factory Default

Choose the **"Wireless Enable"** setting and click **"System Reset"** to immediately restart the system to factory default values but keep the wireless enabled.

Wireless   ○ Enable ○ Disable

[System Reset]

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.

Password Policy

Minimum password length	4	(4 - 16 characters)
Password strength check	Disable ▾	
Password validity	90	(0 - 365 days, 0 is disable)
Password retry count	5	(0 - 10, 0 is disable)
Lockout time	600	(60 - 3600 seconds)

Account List

No.	Active	Account Name	User Level	HTTP/HTTPS	Telnet/SSH /Console	Moxa Services	Diagnostics	Action
1	☑	admin	Admin ▾	☑	☑	☑	☑	[Edit] [Delete]
2	☐		Admin ▾	☑	☑	☑	☑	[Edit] [Delete]
3	☐		Admin User	☑	☑	☑	☑	[Edit] [Delete]
4	☐		Admin ▾	☑	☑	☑	☑	[Edit] [Delete]
5	☐		Admin ▾	☑	☑	☑	☑	[Edit] [Delete]
6	☐		Admin ▾	☑	☑	☑	☑	[Edit] [Delete]
7	☐		Admin ▾	☑	☑	☑	☑	[Edit] [Delete]
8	☐		Admin ▾	☑	☑	☑	☑	[Edit] [Delete]

* Only characters allowed in the Account Name are alphabets, numerals, at sign (@), period (.), and underscore(_).

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.	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

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).

Locating the Device

When you click **Start to Locate** button, the AWK-1131A device uses a beeper and a blinking State LED indicator to let you know its location.

Locate Device (Beeper & LED)

Status: Ready to locate

Start to Locate

Miscellaneous Settings

Additional settings to help you manage your AWK-1131A are available on this page.

Miscellaneous Settings

Reset button	⦿ Always enable ○ Disable factory reset function after 60 seconds.
Allow special characters	○ Enable ⦿ Disable

Submit

Reset button

Setting	Description	Factory Default
Always Enable	The AWK-1131A's Reset button works normally.	Always enable
Disable the Factory Reset Function after 60 Seconds	The AWK-1131A's reset to default function will be inactive 60 seconds after the AWK-1131A 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

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.

Troubleshooting		
Export current device information	Export	☐ Wi-Fi analysis (It takes about 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.

Wi-Fi Mirror Port		
Capture Wi-Fi Frames	[ ] (1~180s)	Capture
Remote Capture	○ Enable ● Disable	

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**.
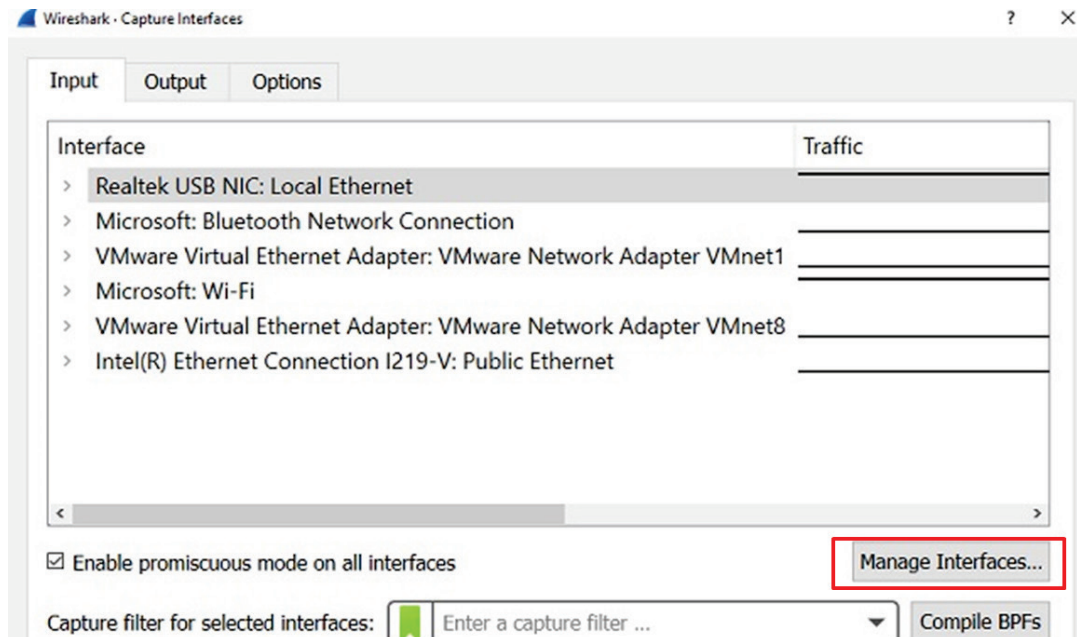
4. Click **Remote Interfaces** and add a new interface.
5. Enter the information for your AWK device.
   - ➢ **Port:** 2002
   - ➢ **Auth:** Null authentication
   - ➢ **Host:** *<AWK IP>*
6. Click **OK**.
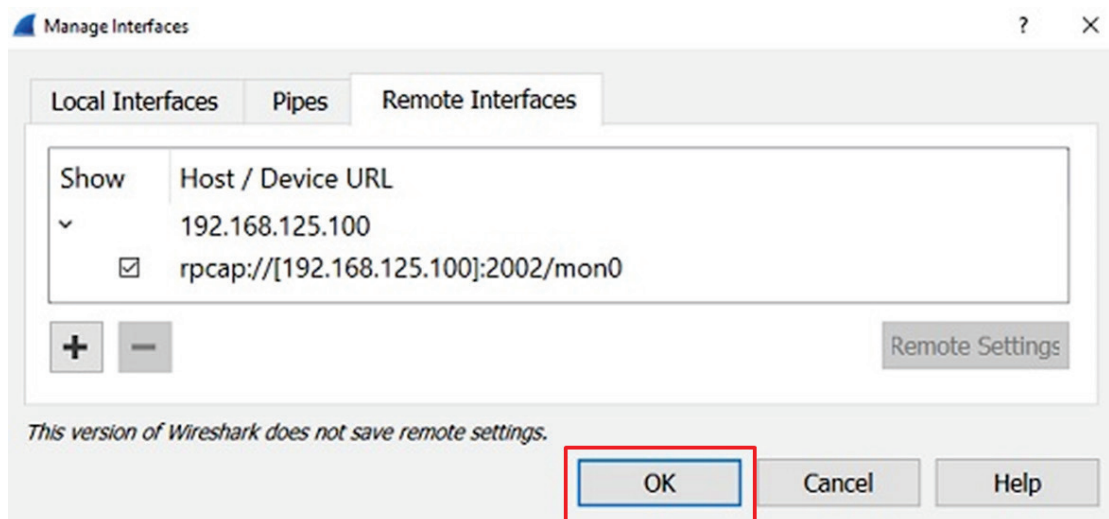
7. Select Input > Interface > rpcap://...:2002/mon0.
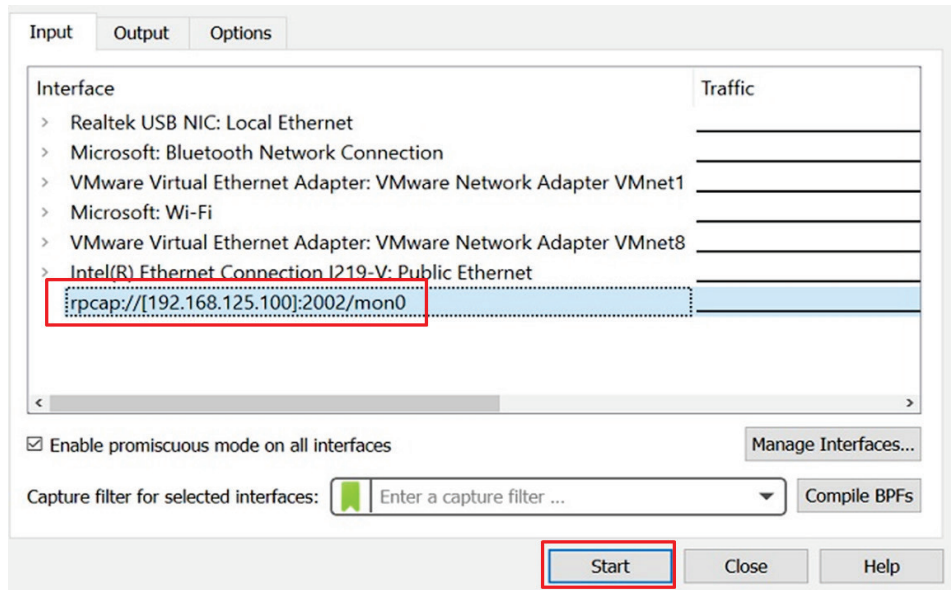
Diagnostics

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** or **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

Setting	Description
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.

Remote Diagnostics

Remote Diagnostic   ⦿ Enable ◯ Disable

Remote Diagnostics CA   [Browse...]

Warning:
Enabling this feature will generate a temporary account and password that will be used by Moxa support engineers to perform remote diagnostics of your device.
Disabling this feature will disable remote diagnostics and will erase all temporary account credentials.
Enabling this feature will temporarily disable Telnet until this feature get disabled.

[Generate Security Key]   [Export Security Key]

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-1131A stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the AWK-1131A is shutdown or rebooted unless they are **y**. Because the AWK-1131A starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the AWK-1131A.

This also means the new changes will not work unless you run either the **Save Configuration** function or the **Restart** function.
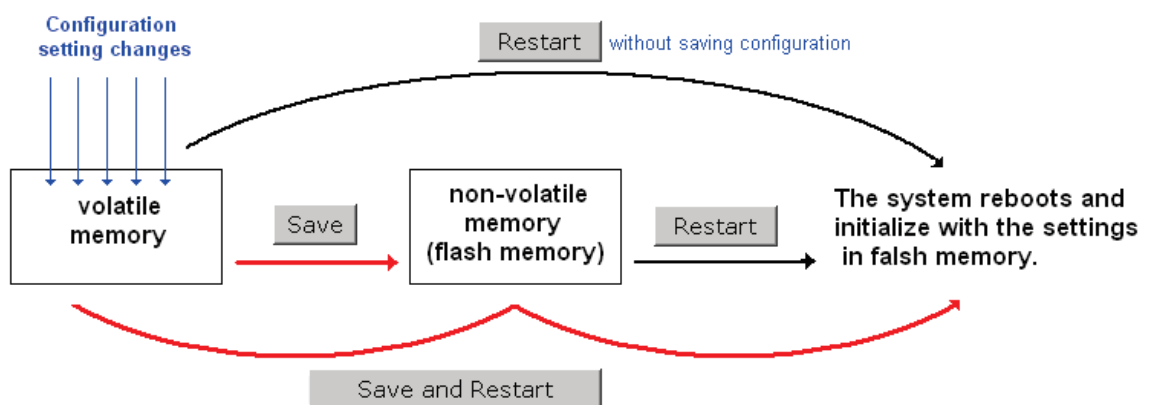
After you click on **Save Configuration** in the left menu box, the following screen is displayed. Click **Save** if you want to update the configuration settings in the flash memory at this time. Alternatively, you can choose to run other functions and put off saving the configuration until later. However, the new setting changes will remain in the non-volatile memory until you save the configurations.

Save Configuration

After you submit configuration changes, you must save the changes and restart the system to make the changes take effect. Click **Save** to save configuration changes in the system memory.

	Save

Network Settings After Reboot

Network Info	
LAN IP address	192.168.127.253
LAN subnet mask	255.255.255.0
LAN gateway	0.0.0.0

Restart

You must restart the device for any changes in the configuration setting to take effect. If you have submitted configuration changes, you will find a blinking string in the upper right corner of the configuration screen. After making all your configuration changes, click the **Restart** function in the left menu box.

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the AWK-1131A directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all changes and then reboot the AWK-1131A.

Restart

!!! Warning !!!

Click "Restart" to discard configuration changes and restart the system.

Click "Save and Restart" to save configuration changes and restart the system.

	Restart	Save and Restart

Network Settings After Reboot

Network Info	
LAN IP address	192.168.43.104
LAN subnet mask	255.255.252.0
LAN gateway	192.168.43.254

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-1131A'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 and Configuration

Overview

AWK can be managed using the MXstudio tool and Wireless Search Utility. Both the Wireless Search Utility and MXstudio can be downloaded from the Moxa website at www.moxa.com.

MXstudio

Please refer the *MXstudio User's Guide* for detailed instructions.

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.
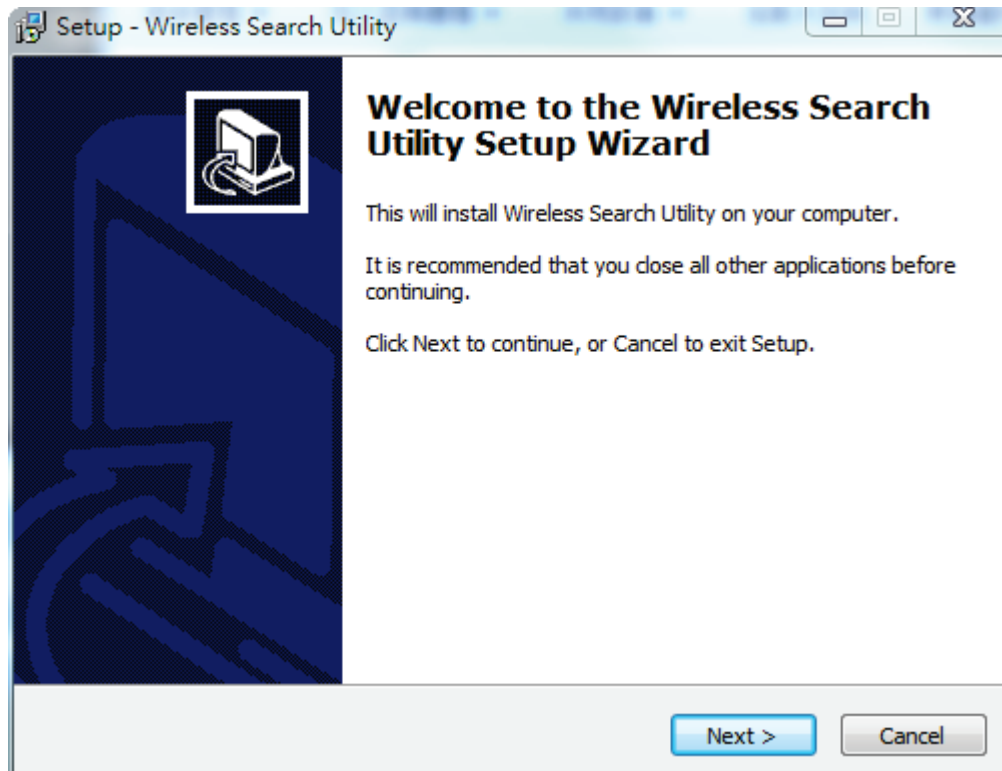
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.
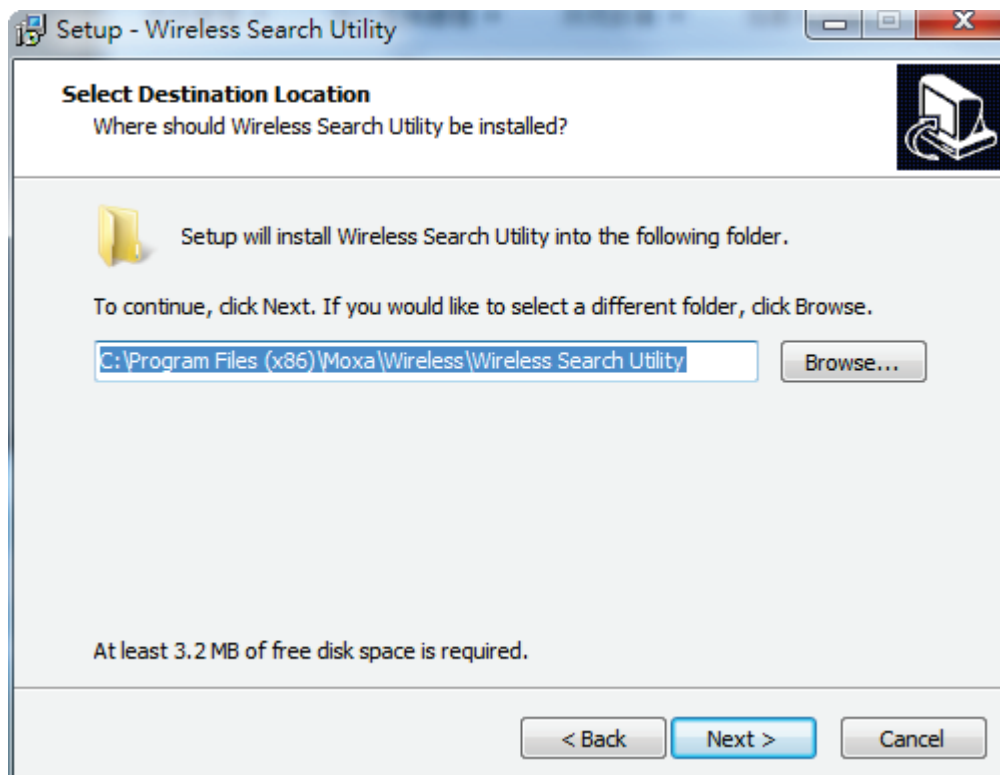
3. Click **Next** to create the program's shortcut files to the default directory, or click **Browse** to select an alternate location.
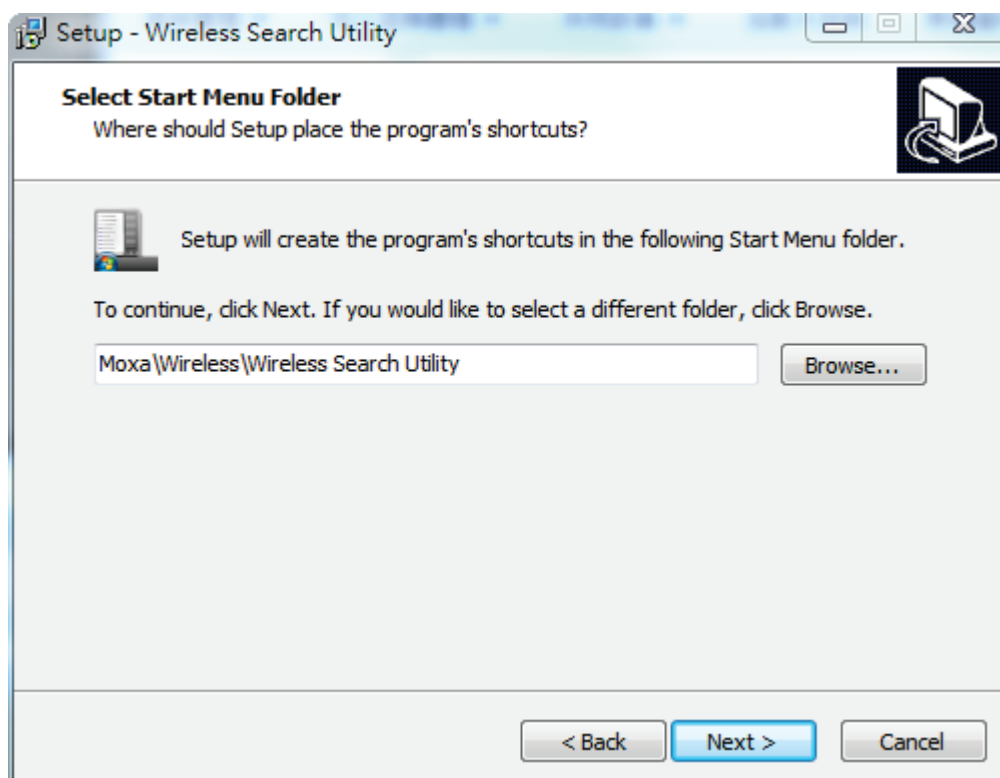
4. Click **Next** to select additional tasks.
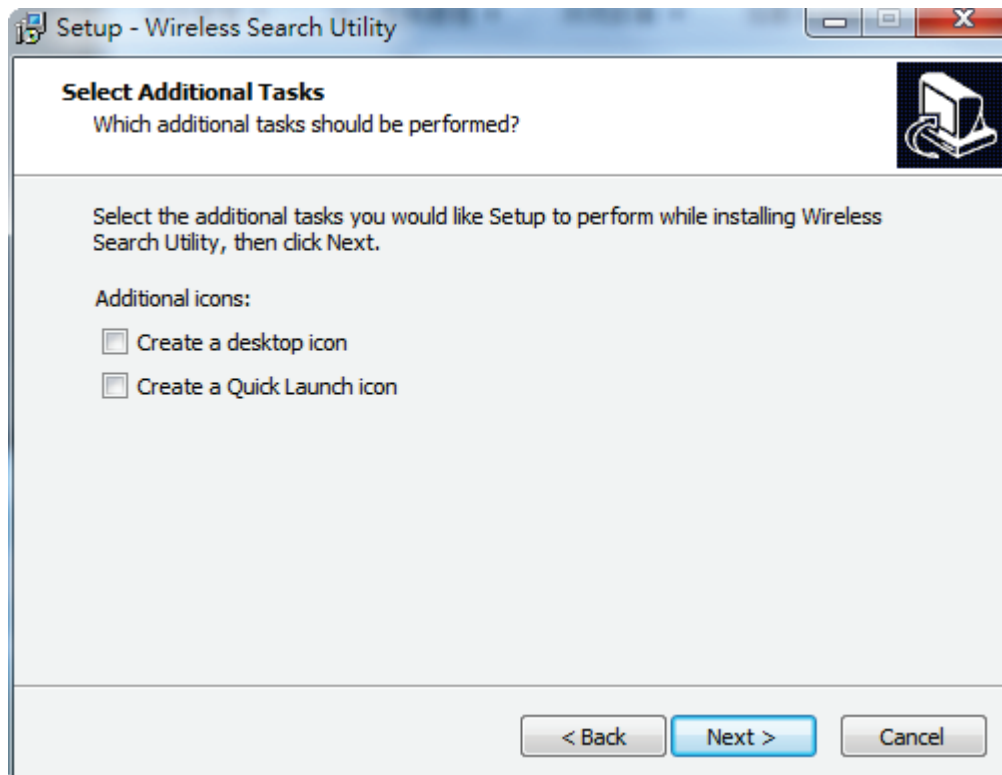
5. Click **Next** to proceed with the installation. The installer then displays a summary of the installation options.
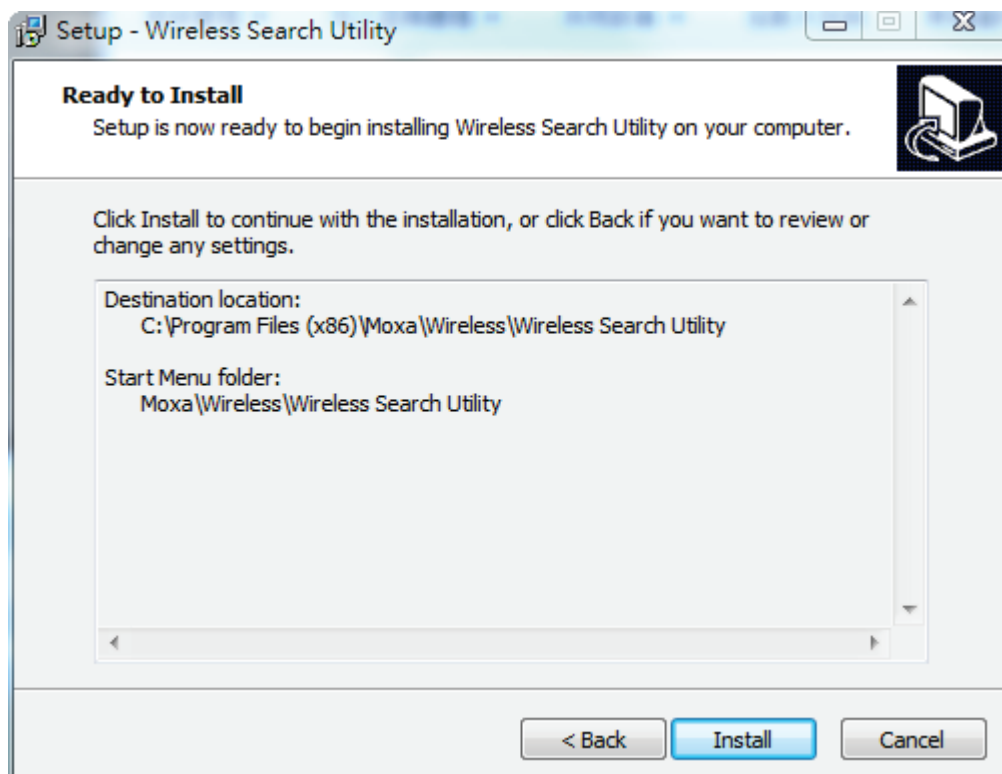
6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.

7. Click **Finish** to complete the installation of Wireless Search Utility.
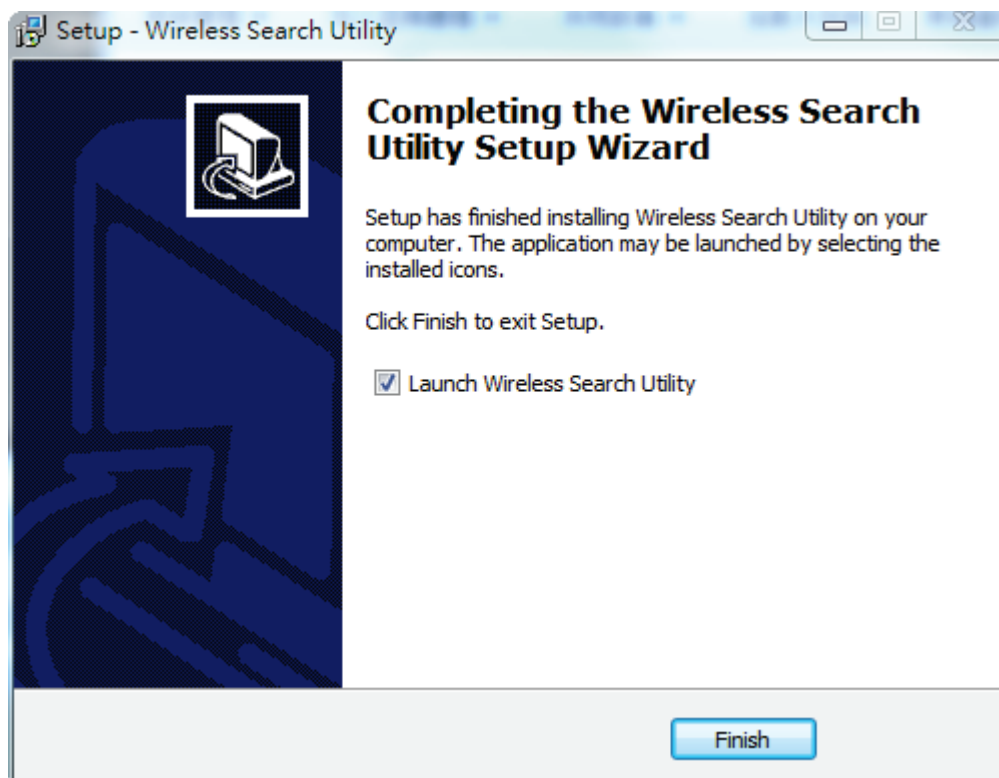
Configuring Wireless Search Utility

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.

---
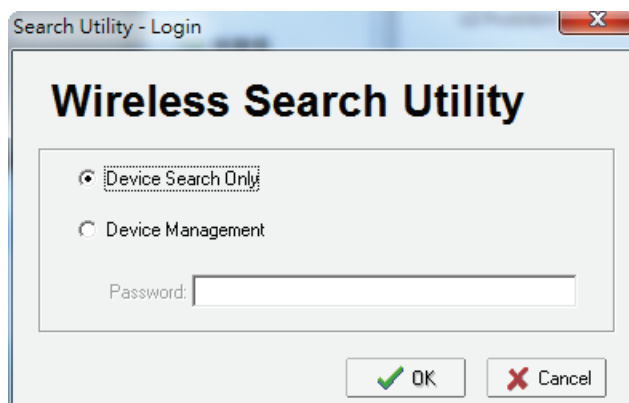
2. Open the Wireless Search Utility and then click the **Search** icon.
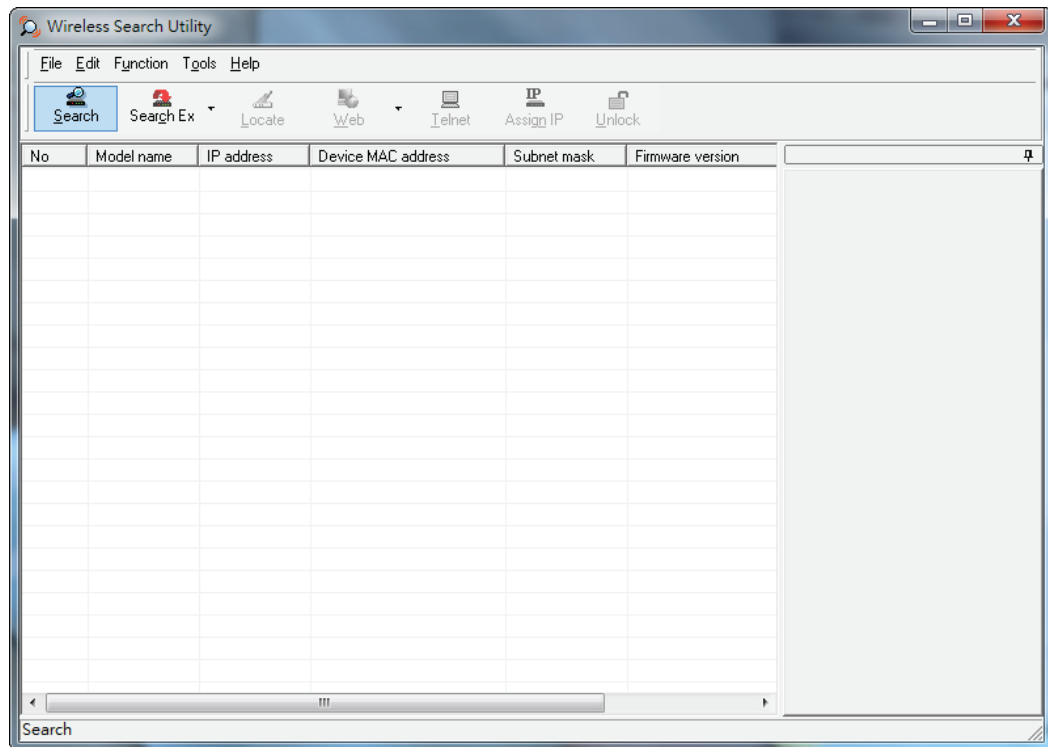
3. The "Searching" window indicates the progress of the search. When the search is complete, all AWKs that were located will be displayed in the **Wireless Search Utility** window.
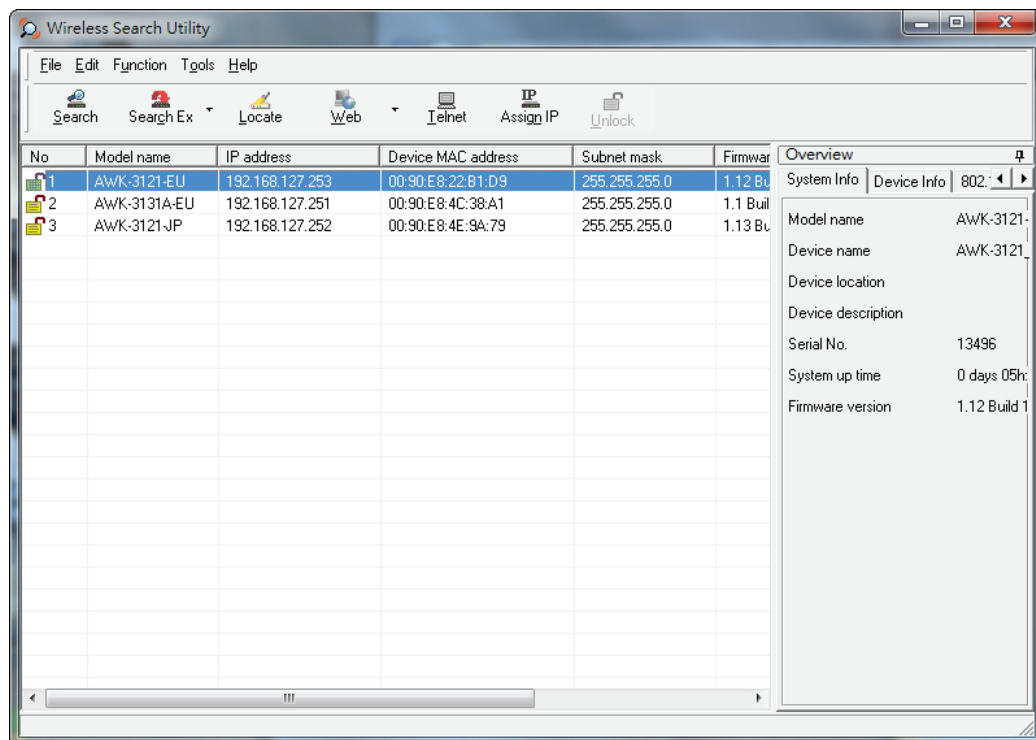
4. Click **Locate** to cause the selected device to beep.
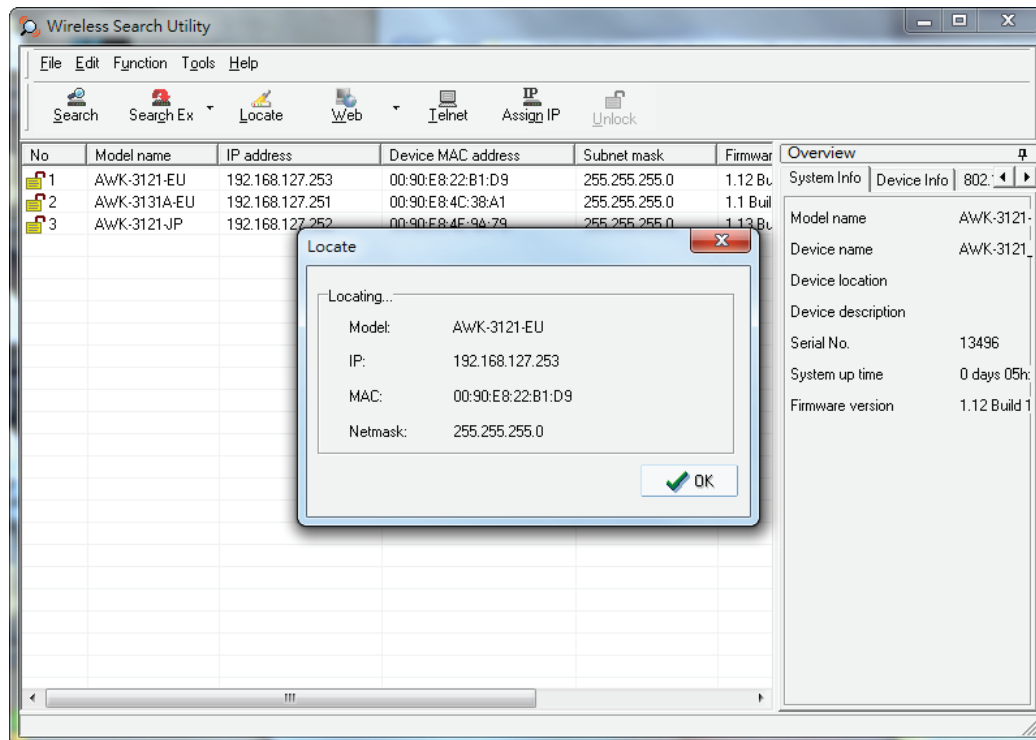
5. Make sure your AWK is **unlocked** before using the search utility's icons setting. The AWK will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.

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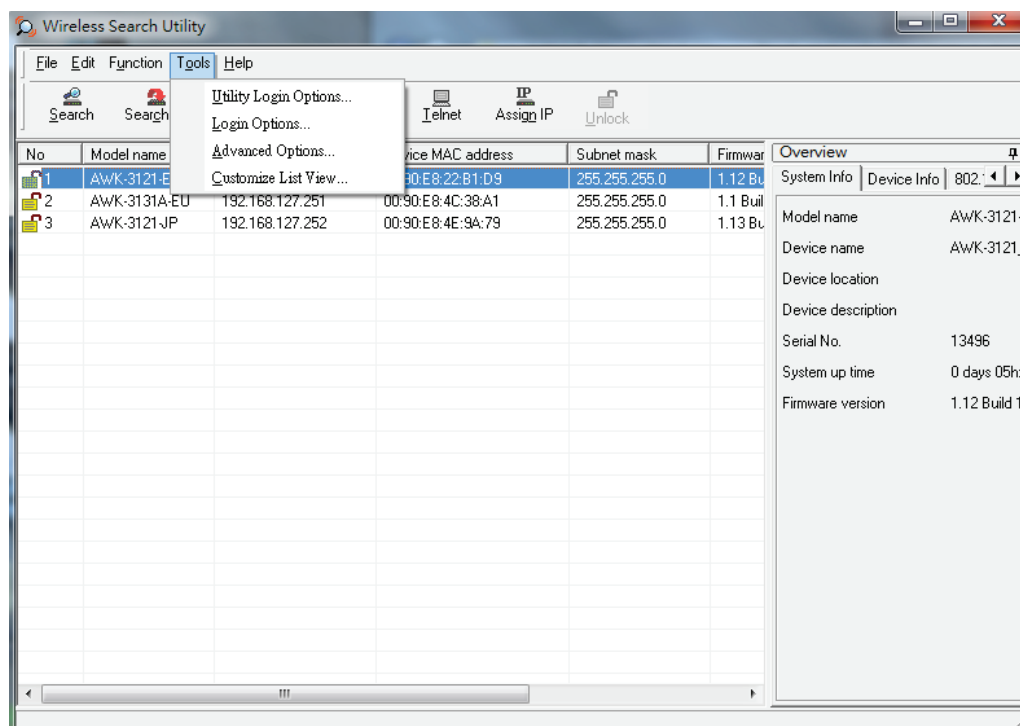
7. Use the scroll down list to select the MAC addresses of those AWKs you would like to manage, and then click **Add**. Key in the password for the AWK device and then click **OK** to save. If you return to the search page and search for the AWK again, you will find that the AWK will unlock automatically.

⚠ **ATTENTION**

Change the default password to ensure a higher level of security.

DO NOT continue to use the default password, **moxa** after the first login.

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 change the configuration of the AWK. Refer to *Chapter 3, Web Console Configuration* for information on how to use the web console.

Click on **Telnet** if you would like to use telnet to configure your AWKs.
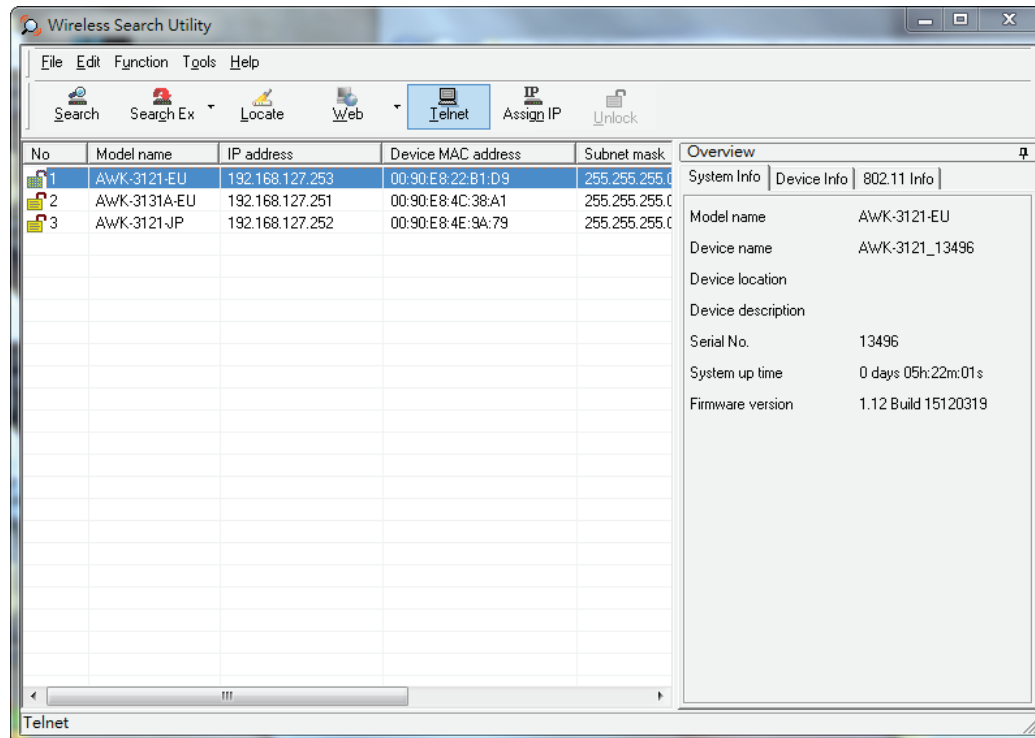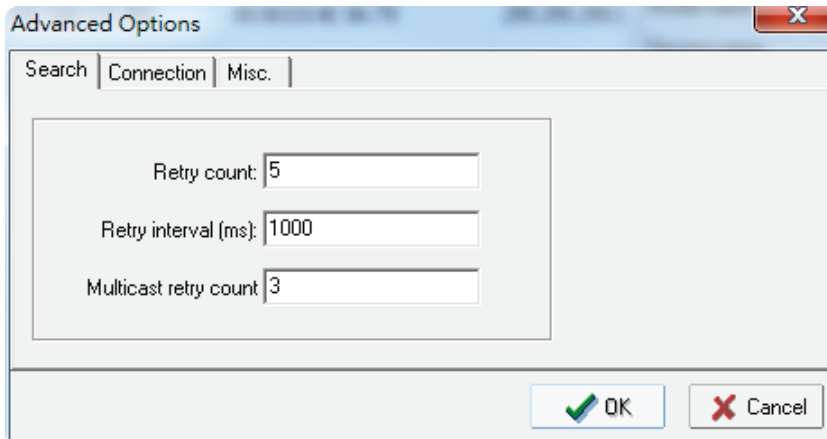
Click **Assign IP** to change the IP setting.
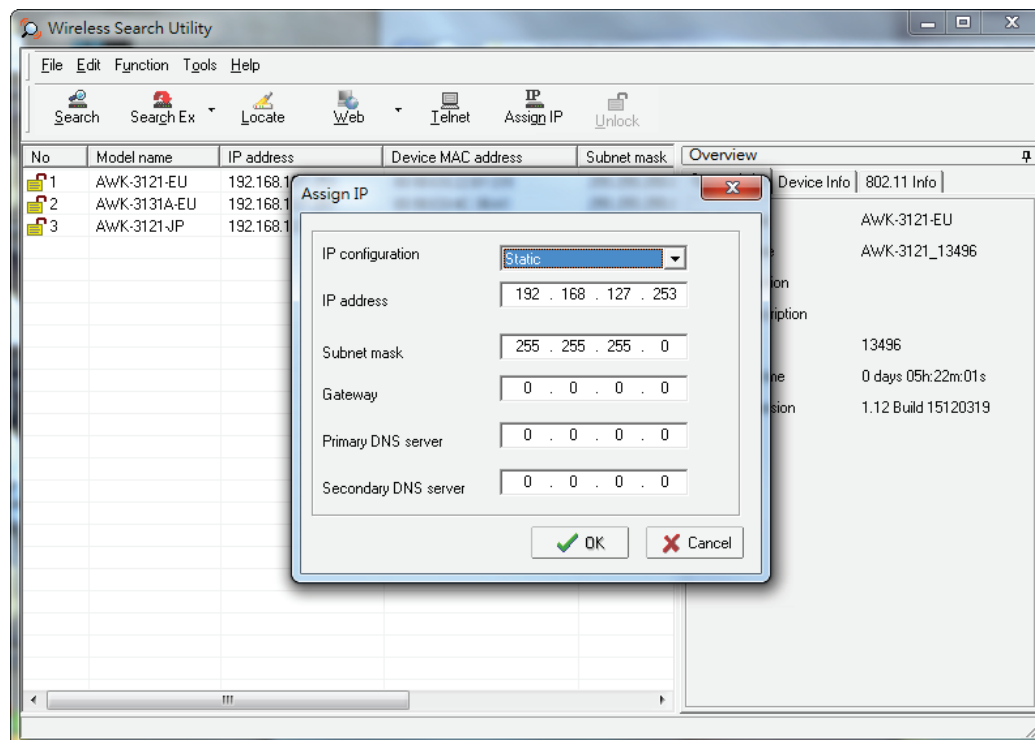
The three advanced options—**Search**, **Connection**, and **Miscellaneous**—are explained below:

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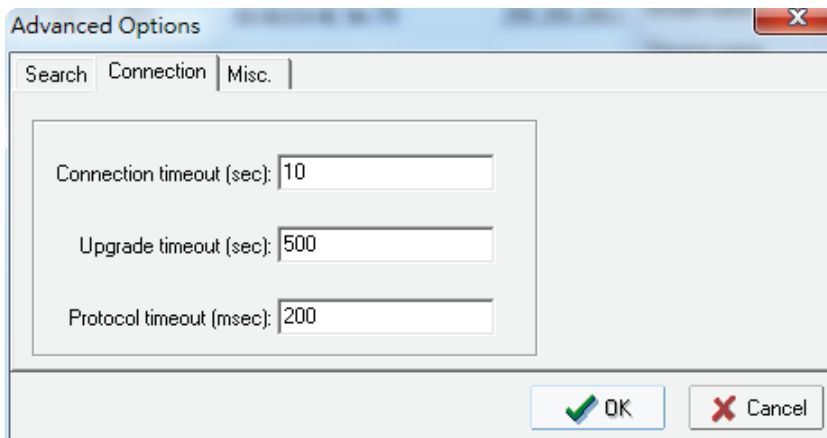
- **Retry count (default=5):** Indicates how many times the search will be retried automatically.
- **Retry interval (ms):** The time elapsed between retries.
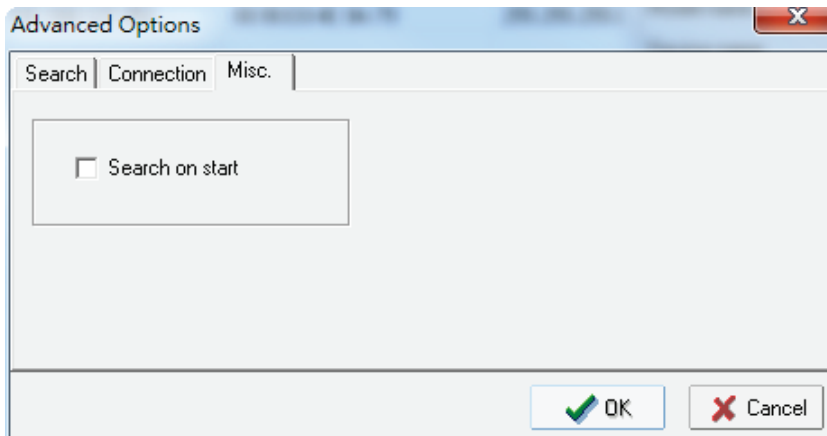
Connection

- **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. Additional Consoles

Overview

In addition to HTTP access, there are four ways to access AWK-1131A: 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-1131A to a PC's COM port, can be used if you do not know the AWK-1131A's IP address. The other consoles can be used to access the AWK-1131A over an Ethernet LAN, or over the Internet.

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-1131A to a PC's COM port, can be used if you do not know the AWK-1131A's IP address. It is also convenient to use serial console configurations when you cannot access the AWK-1131A 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-1131A is powered at reversed voltage (ex. -48VDC), even though reverse voltage protection is supported.

If you need to connect the RS-232 console at reversed 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 PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the AWK-1131A'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.
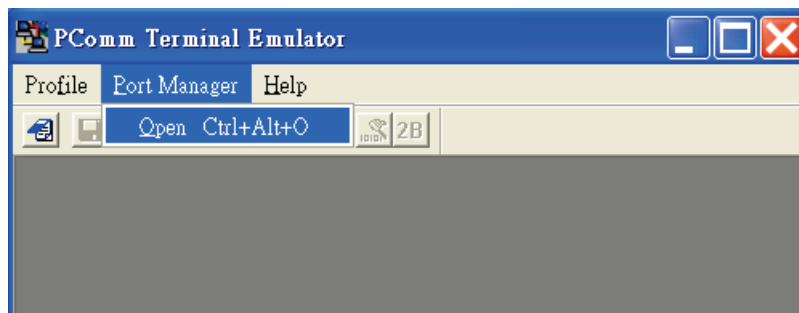
3. In the **Communication Parameter** tab of the **Property** window that opens, select the appropriate COM port for console connection using **115200** for Baud Rate, **8** for Data Bits, **None** for Parity, and **1** for Stop Bits. Click on the **Terminal** tab, and select **VT100 (or ANSI)** for Terminal Type. Click on **OK** to continue.
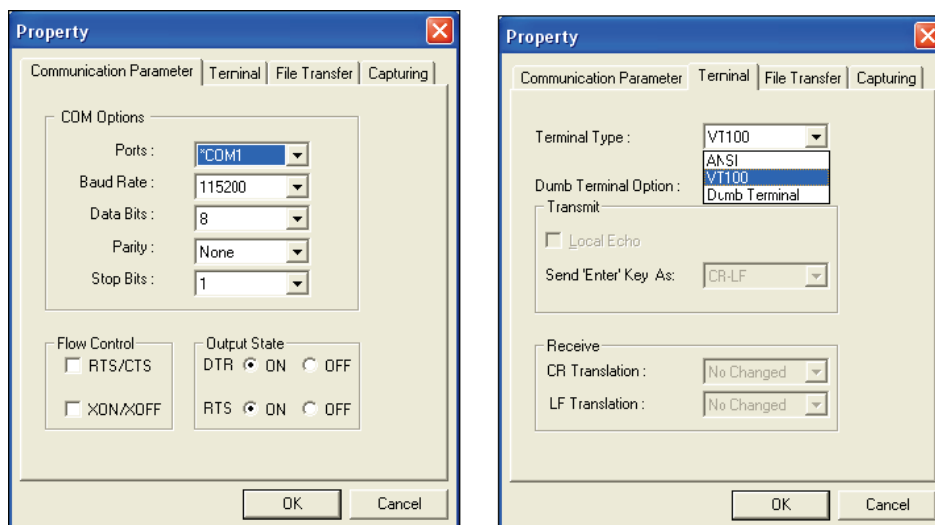
4. The console login screen is displayed. Log into the RS-232 console with the login name (default: **admin**) and password (default: **moxa**, if no new password is set).
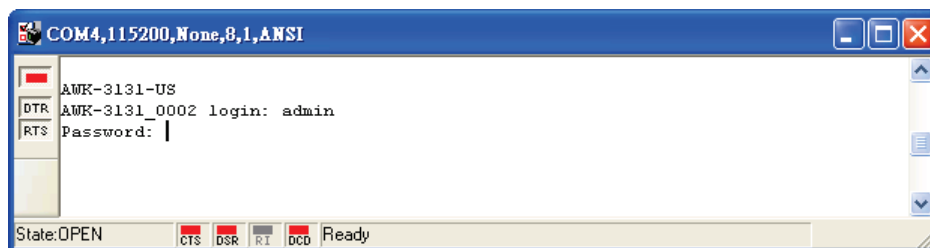
5. The AWK-1131A's device information and Main Menu will be displayed. Follow the instructions on the screen to select the administration task that you want to perform.
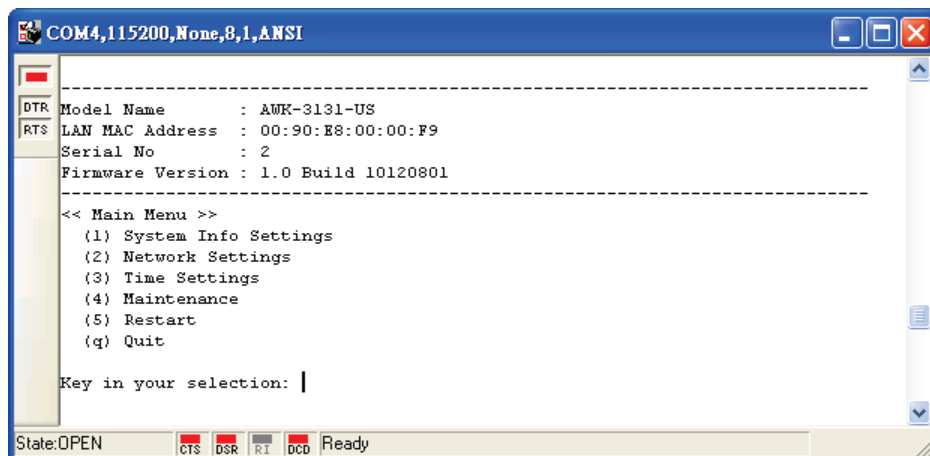
✎ **NOTE**

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**, a disconnection event will be evoked to enforce logout for network security. You will need to log in again to resume operation.

Configuration by Telnet and SSH Consoles

You can use Telnet or SSH client to access the AWK-1131A and manage the console over a network. To access the AWK-1131A's functions over the network from a PC host that is connected to the same LAN as the AWK-1131A, you need to make sure that the PC host and the AWK-1131A are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.


> ✏️ **NOTE**
>
> The AWK-1131A'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 the Telnet command or using an SSH client.

1. Start the windows **Run** command (Windows start menu, type "run" and press Enter) and use the telnet command to access the IP address of your AWK-1131A.

   Note that you can also run the telnet command from the Command Prompt.
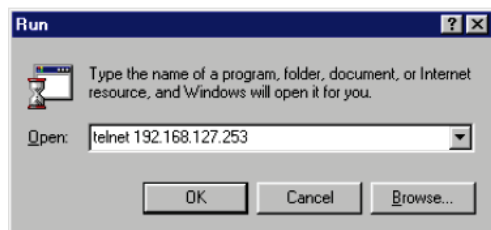
   If you are using an SSH client (ex. PuTTY), run the client program and then enter the IP address of your AWK-1131A, specifying **22** for the SSH connection port.
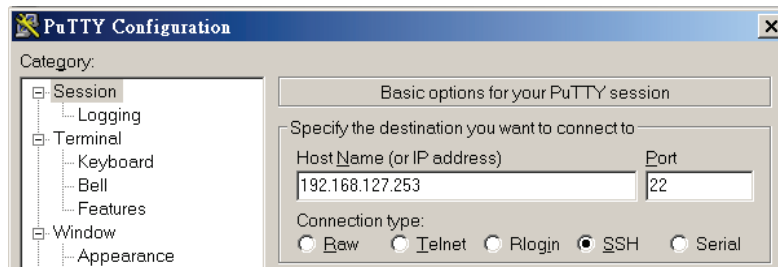

2. The console login screen is displayed. Refer to *RS-232 Console Configuration* (previous paragraph) for login and administration details.

Configuration by Web Browser with HTTPS/SSL

To secure your HTTP access, the AWK-1131A supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the AWK-1131A's web browser interface via HTTPS/SSL.

1. Open your web browser and type https://<AWK-1131A's IP address> in the address field. Press **Enter** to establish the connection.

---
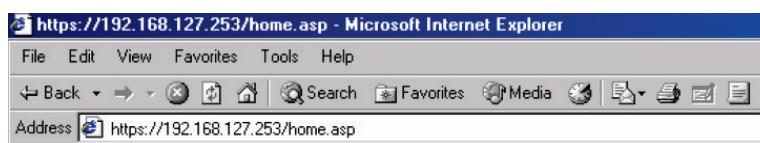
2. Warning messages will pop out to warn users that the security certificate was issued by a company they have not chosen to trust.
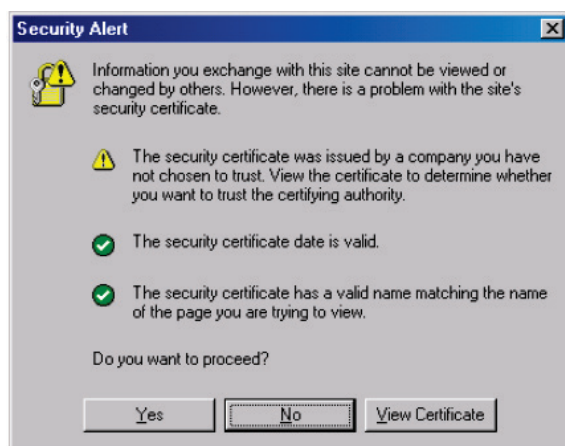
3. Select **Yes** to accept the certificate issued by Moxa IW and then enter the AWK-1131A's web browser interface secured via HTTPS/SSL. (You can see the protocol in URL is **https**.) Then you can use the menu tree on the left side of the window to open the function pages to access each of AWK-1131A's functions.
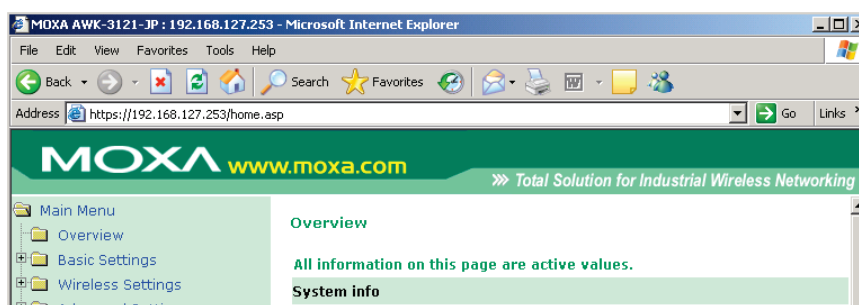
Disabling Telnet and Browser Access

If you are connecting the AWK-1131A to a public network but do not intend to use its management functions over the network, we suggest disabling the **Telnet console** and the Web consoles at **Maintenance** 〉 **Console Settings.**

A. References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your AWK-1131As and plan your industrial wireless network better.

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.

B. Supporting Information

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

Firmware Recovery

When the LEDs that indicate **FAULT**, **Signal Strength** and **WLAN** all light up simultaneously and blink at one-second intervals, it means that the system boot up process has failed. This might result from some wrong operation or issues such as an unexpected shutdown during firmware update. The AWK-1131A is designed to help administrators recover from such damage and resume system operation rapidly.

First, connect to the AWK-1131A's RS-232 console with the settings 115200 bps and N-8-1. A message is displayed on the terminal emulator at one-second intervals as shown below:

```
please set-up TFTP server 192.168.127.1 contains awk1131a.rom for firmware
recovery.

please set-up TFTP server 192.168.127.1 contains awk1131a.rom for firmware
recovery.

please set-up TFTP server 192.168.127.1 contains awk1131a.rom for firmware
recovery.

please set-up TFTP server 192.168.127.1 contains awk1131a.rom for firmware
recovery.

please set-up TFTP server 192.168.127.1 contains awk1131a.rom for firmware
recovery.

please set-up TFTP server 192.168.127.1 contains awk1131a.rom for firmware
recovery.
```

To recover the firmware, do the following:

1. Change the IP address of the laptop to 192.168.127.1.
2. Set up a TFTP server in your laptop.
3. Download AWK-1131A's firmware from Moxa Website
4. Change firmware file name to awk1131a.rom
5. Connect to the AWK-1131A's RJ45 Ethernet port

If the settings are correct, the following message is shown on the terminal emulator. The AWK-1131A will reboot when the firmware recovery process is complete.

```
Trying eth0

Using eth0 device

TFTP from server 192.168.127.1; our IP address is 192.168.127.253

Filename 'awk1131a.rom'.

Load address: 0x80060000

Loading: *#########################################################
  #########################################################
  #########################################################
```

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, might 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 will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

RED Compliance Statement

Moxa declares that the apparatus AWK-1131A complies with the essential requirements and other relevant provisions of Directive 2014/53/Eu.

The 5150 to 5350 MHz frequency range is restricted to indoor use only. Outdoor operation in this range is strictly prohibited.

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 of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Not Intended for Use

None.