AirWorks AWK-3191 User's Manual

Edition 3.0, January 2017

www.moxa.com/product

AirWorks AWK-3191 User's Manual

Copyright Notice

Trademarks

Disclaimer

Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.

Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.

Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

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

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

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

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

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

Table of Contents

1

Introduction

This chapter provides an overview of the AWK-3191. See the Product Checklist and Optional Parts sections to double check what was already shipped and what needs to be purchased additionally. See the Product Features and Product Specifications sections to get a quick overview of this product's functionality and its detailed specs. And see the Functional Design section to learn about the hardware interfaces.

For detailed hardware installation information, see the quick installation guide for this product, which can found on Moxa's official website at www.moxa.com.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Ordering Information**
  - Available Models
  - Optional Accessories (can be purchased separately)
- **Product Features**
- **Product Specifications**
- **Functional Design**
  - LED Indicators
  - Beeper
  - Reset Button

Overview

The AWK-3191 900 MHz wireless AP/bridge/client is Moxa's answer to long distance wireless communication for industrial applications. By combining the characteristics of the 33-centimeter band and the proven 802.11 standards, Moxa is able to provide a reliable long distance wireless solution. Unlike traditional point-to-point 900 MHz radios, the AWK-3191 supports both master/slave and AP/client operation modes to enable both point-to-point and point-to-multi-point communication for higher flexibility and lower total cost of ownership.

Furthermore, the AWK-3191 is designed to be deployed easily, but in case of external interference, Moxa also provides the ability to allow engineers to adjust their 900 MHz central frequency and bandwidth (5/10 MHz and 20 MHz) to optimize their wireless performance.

The AWK-3191 is rated to operate at temperatures ranging from -25 to 60°C for standard models and -40 to 75°C for wide temperature models, and with an industrial-oriented design, it is compliant with various standards and approvals, making it rugged enough for any harsh industrial environment.

Package Checklist

Moxa's AWK-3191 is shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative for assistance.

- AWK-3191
- Cable holder with one screw
- 2 plastic RJ45 protective caps
- Documentation and software CD
- Quick installation guide (printed)
- Warranty card

NOTE The above items come with the standard AWK-3191 model, but the package contents may vary for customized versions.

Ordering Information

Available Models

AWK-3191-US: Industrial 900 MHz access point, US band (902 to 928 MHz)
AWK-3191-US-T: Industrial 900 MHz access point, US band (902 to 928 MHz), and -40 to 75°C operating temperature
Note: Moxa's AWK-3191 does NOT include default antennas; refer to the following information to choose a suitable antenna system

Optional Accessories (can be purchased separately)

A-CRF-RMNM-L1-X00: N-type (male) to RP SMA (male), LMR-195 Lite RF cable, available in lengths of 3 m, 6 m, and 9 m
ANT-WSB0.9-YNF-12: 900 MHz, Yagi antenna for point-to-point applications, 12 dBi, N-type (female)
ANT-WSB0.9-ANF-09: 900 MHz, omni-directional antenna for point-to-multi-point applications, 9 dBi, N-type (female)

Note: Please visit Moxa's website for a complete list of optional wireless accessories and antennas available for Moxa's wireless products.

Product Features

- 900 MHz transmission for long distance wireless communication
- AP/client and master/slave modes supported for point-to-point and point-to-multi-point connections
- QoS (WMM) and VLAN for efficient network traffic
- Maximum security with WEP/WPA/WPA2/802.11X and powerful filters
- -40 to 75°C operating temperature range (T models)
- Power and antenna isolation design for higher operation stability

Product Specifications

WLAN Interface

Standards:

IEEE 802.11i for Wireless Security

IEEE 802.1Q for VLAN

IEEE 802.3af for Power-over-Ethernet*

IEEE 802.1X for Security and Authentication

*Hardware Rev. 3.0.0 supports PoE; hardware Rev. 2.0.0 does not support PoE.

Spread Spectrum and Modulation (typical):

• OFDM with BPSK, QPSK, 16QAM, 64QAM

• 64QAM @ 54/48 Mbps, 16QAM @ 36/24 Mbps,
QPSK @ 18/12 Mbps, BPSK @ 9/6 Mbps

Channel Band Width:

US: 5 MHz, 10 MHz, 20 MHz

Operating Channels (central frequency):

US: 902 to 928 MHz (ISM band)

• 915 MHz (BW = 20 MHz)

• 908.5, 915, 921.5 MHz (BW = 10 MHz)

• 905.25, 908.5, 911.75, 915, 918.25, 921.5, 924.75 MHz (BW = 5 MHz)

Security:

• SSID broadcast enable/disable

• Firewall for MAC/IP/protocol/port-based filtering

• 64-bit and 128-bit WEP encryption, WPA /WPA2-Personal and Enterprise (IEEE 802.1X/RADIUS, TKIP and AES)

Transmission Rates:

6, 9, 12, 18, 24, 36, 48, 54 Mbps

TX Transmit Power:

• Typ. 24±1.5 dBm @ 6 to 24 Mbps

• Typ. 23±1.5 dBm @ 36 Mbps

• Typ. 22±1.5 dBm @ 48 Mbps

• Typ. 21±1.5 dBm @ 54 Mbps

RX Sensitivity:

• -90 dBm @ 6 Mbps

• -88 dBm @ 9 Mbps

• -87 dBm @ 12 Mbps

• -85 dBm @ 18 Mbps

• -81 dBm @ 24 Mbps

• -77 dBm @ 36 Mbps

• -73 dBm @ 48 Mbps

• -71 dBm @ 54 Mbps

Protocol Support

General Protocols: DNS, HTTP, HTTPS, IP, ICMP, SNTP, TCP, UDP, RADIUS, SNMP, DHCP

Interface

Connector for External Antennas: RP-SMA (female)

RJ45 Ports: 1, 10/100BaseT(X) auto negotiation speed, F/H duplex mode, and auto MDI/MDI-X connection

Console Port: RS-232 (RJ45-type)

Reset: Present

LED Indicators: PWR1, PWR2, PoE (Hardware Rev. 3.0.0 supports PoE; hardware Rev. 2.0.0 does not support PoE.), FAULT, STATE, signal strength, CLIENT MODE, BRIDGE MODE, WLAN, 10M, 100M

Alarm Contact: 1 relay output with current carrying capacity of 1 A @ 24 VDC

Digital Inputs: 2 electrically isolated inputs

- +13 to +30 V for state “1”
- +3 to -30 V for state “0”
- Max. input current: 8 mA

Physical Characteristics

Housing: Metal, providing IP30 protection

Weight: 930 g

Dimensions: 53 x 135 x 105 mm (2.08 x 5.3 x 4.13 in)

Installation: DIN-rail mounting, wall mounting (with optional kit)

Environmental Limits

Operating Temperature:

Standard Models: -25 to 60°C (-13 to 140°F)

Wide Temp. Models: -40 to 75°C (-40 to 167°F)

Storage Temperature: -40 to 85°C (-40 to 185°F)

Ambient Relative Humidity: 5% to 95% (non-condensing)

Power Requirements

Input Voltage: 12 to 48 VDC, redundant dual DC power inputs or 48 VDC Power-over-Ethernet* (IEEE 802.3af compliant)

*Hardware Rev. 3.0.0 supports PoE; hardware Rev. 2.0.0 does not support PoE.

Connector: 10-pin removable terminal block

Power Consumption: 5.928 W (12 V / 0.494 A to 48 V / 0.121 A)

Reverse Polarity Protection: Present

Standards and Certifications

Safety: UL 60950-1

EMC: FCC Part 15, Subpart B

Radio: FCC ID SLE-WFS001

Note: Please check Moxa’s website for the most up-to-date certification status.

Reliability

MTBF (mean time between failures): 484,469 hrs

Warranty

Warranty Period: 5 years

Details: See www.moxa.com/support/warranty.aspx

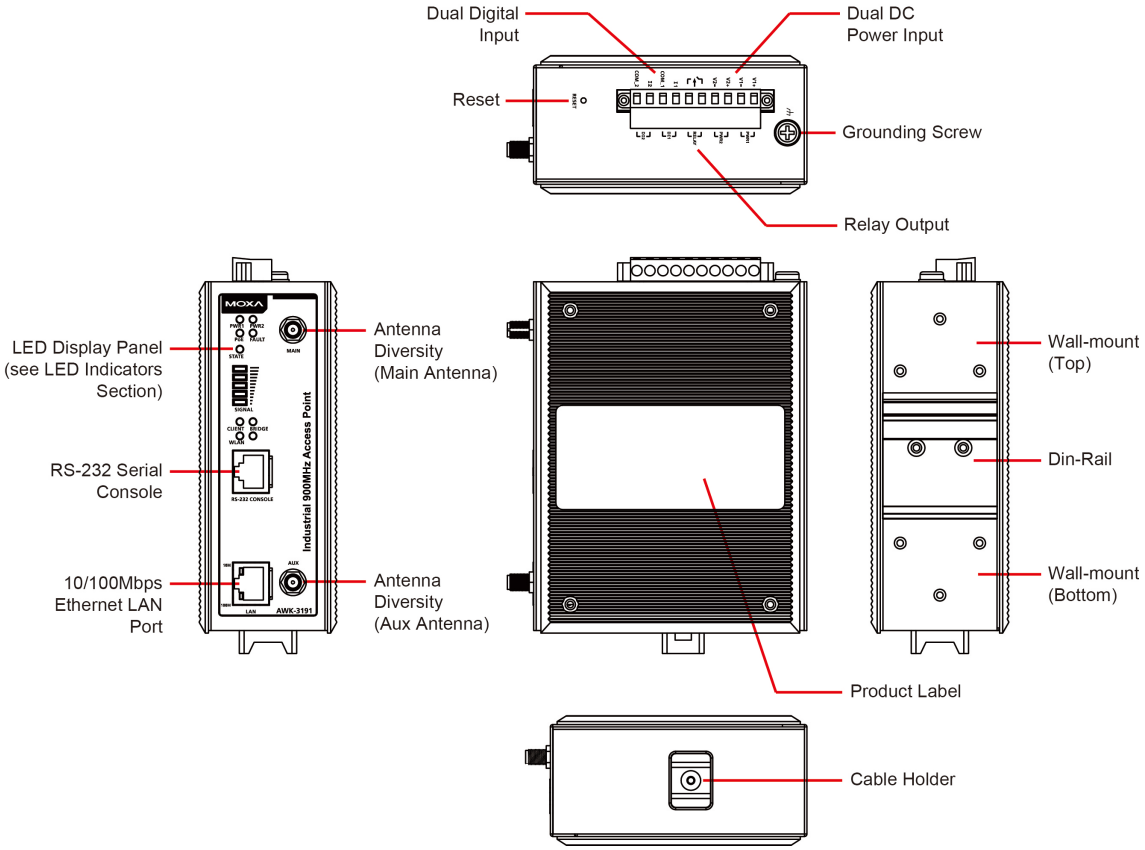
ATTENTION

The AWK-3191 is NOT a portable mobile device and should be located at least 20 cm away from the human body.

The AWK-3191 is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of AWK-3191 units, and to establish a wireless network.

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

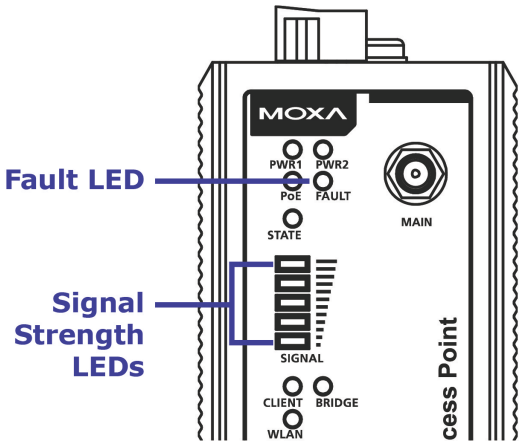
Functional Design



LED Indicators

The LEDs on the front panel of the AWK-3191 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-3191 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/Slave** mode.



The following table summarizes how to read the device's wireless settings from the LED displays. More information is available in Chapter 3 in the "Basic Wireless Settings" section.

LED	Color	State	Description
Front Panel LED Indicators (System)			
PWR1	Green	On	Power is being supplied from power input 1.
		Off	Power is **not** being supplied from power input 1.
PWR2	Green	On	Power is being supplied from power input 2.
		Off	Power is **not** being supplied from power input 2.
PoE (Hardware Rev. 3.0.0 supports PoE; hardware Rev. 2.0.0 does not support PoE.)	Amber	On	Power is being supplied via PoE.
		Off	Power is **not** being supplied via PoE.
FAULT	Red	Blinking (slow at 1-second intervals)	Cannot get an IP address from the DHCP server
		Blinking (fast at 0.5-second intervals)	IP address conflict
		Off	Error condition does not exist.
STATE	Green/ Red	Green	Software Ready
		Green (blinking at 1-second intervals)	The AWK has been located by Wireless Search Utility
		Red	Booting error condition
SIGNAL (5 LEDs)	Green	On	Signal level (for **Client/Slave** mode only)
		Off	
BRIDGE	Green	On	WLAN function is in Wireless Bridge (Master/Slave) Mode.
		Off	WLAN is not in Wireless Bridge (Master/Slave) Mode.
CLIENT	Green	On	WLAN function is in Client/Slave mode.
		Off	WLAN function is in AP/Master mode.
WLAN	Amber	On	WLAN radio is activated.
		Blink	Data is being transmitted over WLAN interface.
		Off	WLAN radio has been disabled.
TP Port LED Indicators (Port Interface)			
100M	Green	On	TP port's 100 Mbps link is **active**.
		Blink	Data is being transmitted at 100 Mbps
		Off	TP port's 100 Mbps link is **inactive**.
10M	Amber	On	TP port's 10 Mbps link is **active**.
		Blink	Data is being transmitted at 10 Mbps
		Off	TP port's 100 Mbps link is **inactive**.

ATTENTION

The **FAULT**, **SIGNAL**, **CLIENT**, **BRIDGE**, and **WLAN** LEDs lighting up simultaneously and blinking at one-second intervals indicates that the system has failed to boot. This may be due to improper operation or an uncontrollable factor, such as an unexpected shutdown during firmware update. Instructions on how to recover the firmware can be found in Chapter 6 in the "Firmware Recovery" section.

Beeper

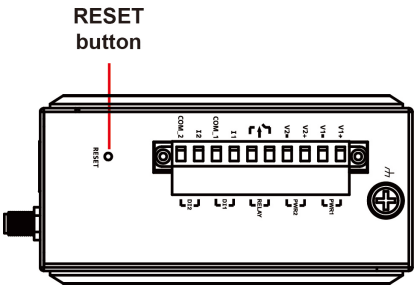
The beeper emits beeps in one of two ways:

- **Two short beeps** when the system is ready.
- **Continuous short beeps** with one-second intervals when the device is "located" by Moxa's Search Utility

Reset Button

The **RESET** button is located on the top panel of the AWK-3191. You can reboot the AWK-3191 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-3191.



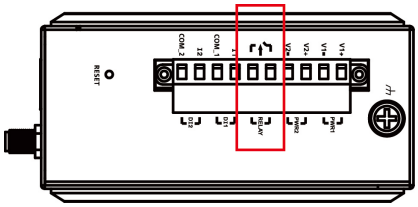
Relay (Digital Output)

The AWK-3191 has one relay output consisting of the 2 terminal block contacts on the top panel, as shown below. These relay contacts are used to forward system failures and user-configured events.

The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the AWK-3191 is not powered up.

Summary of the AWK-3191's Relay Status

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



2

Getting Started

This chapter explains how to install Moxa's AirWorks AWK-3191 for the first time, and quickly set up your wireless network and test whether the connection is running well. The function guide provides a convenient means of determining which functions you need to use.

The following topics are covered in this chapter:

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

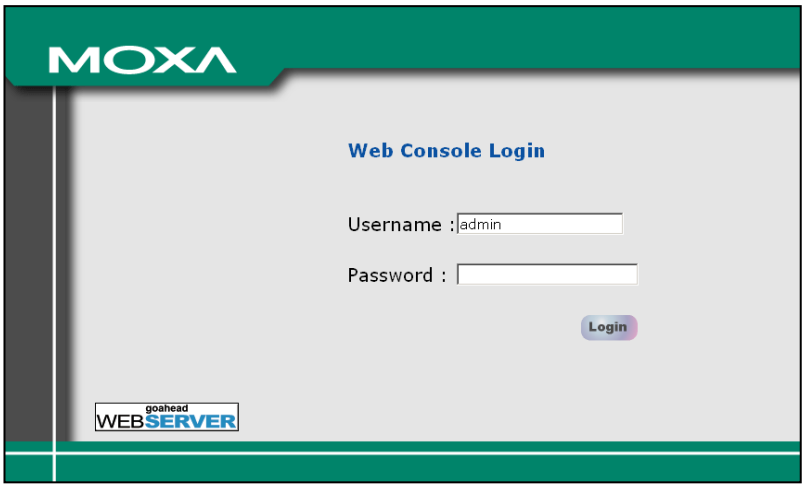
First-time Installation and Configuration

Before installing the AWK-3191, 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-3191 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-3191 can be powered by a DC power input or PoE (Hardware Rev. 3.0.0 supports PoE; hardware Rev. 2.0.0 does not support PoE.). The AWK-3191 will use whichever power source you choose.
- **Step 2: Connect the AWK-3191 to a notebook or PC.**
  Since the AWK-3191 supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the AWK-3191 to a computer. The LED indicator on the AWK-3191'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-3191. Since the AWK-3191'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-3191 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-3191**
  Open your computer's web browser and type **http://192.168.127.253** in the address field to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the user name and password as shown in the following figure. For first-time configuration, enter the default user name and password and then click on the **Login** button:



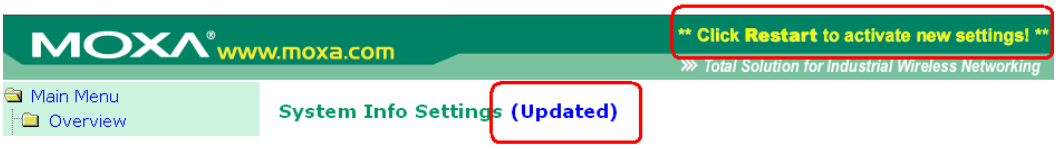
NOTE Default user name and password:

User Name: **admin**

Password: **root**

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

NOTE After you click Submit to apply changes to the web page **(Updated)** will appear on the page and a blinking reminder will be shown in 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-3191 to complete the reboot procedure.

- **Step 5: Select the AWK-3191 operation mode.**
  By default, the AWK-3191's operation mode is set to AP. You can change to Client mode in **Wireless Settings → Basic Wireless Settings**. Detailed information about configuring the AWK-3191'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

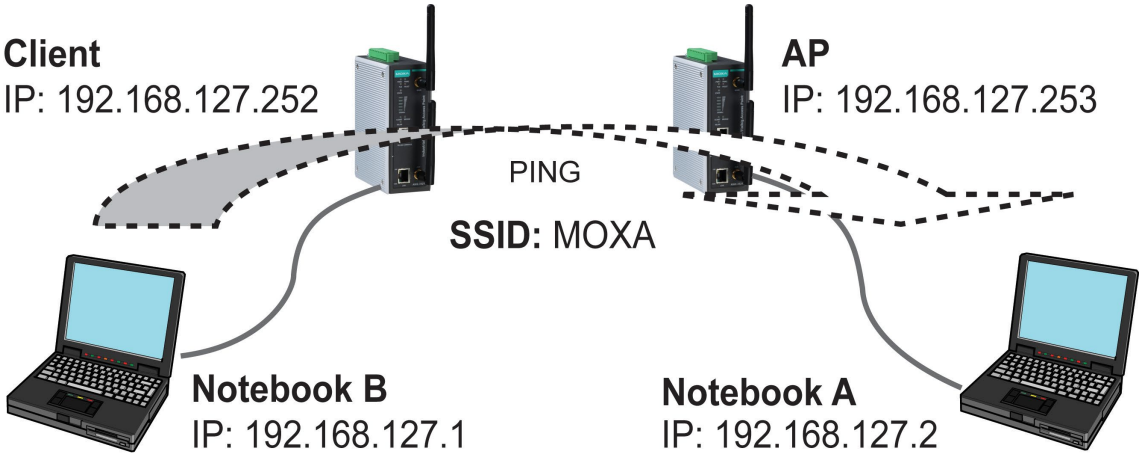
After installing the AWK-3191 you can run a simple test to make sure the AWK-3191 and wireless connection are functioning normally. The AWK-3191 is a 900 MHz Access Point. Laptops are generally NOT equipped with 900 MHz radio, so you must use a pair of AWK-3191 units to complete the communication test. (NOTE: By default, the AWK-3191 is not shipped with an antenna; be sure to purchase an antenna and attach the antenna before you do your test.)

Required Equipment: AWK-3191 x 2 (one as AP, another as Client), 900 MHz Antenna Set x 2, Power Supply x 2, Laptop x 2, Ethernet Cable x 2

Setup AP Side: Configure Notebook A to be on the same subnet as the AWK-3191; for example, 192.168.127.2/24. After the network configuration, connect Notebook A to the AP AWK-3191 via Ethernet. (NOTE: The default AWK IP is 192.168.127.253) Double confirm that the AWK-3191 is configured to AP mode. (NOTE: The default AP SSID is MOXA)

Setup Client Side: Configure Notebook B to be on the same subnet as the AWK-3191; for example, 192.168.127.1/24. After the network configuration, connect Notebook B to the Client AWK-3191 via Ethernet. (NOTE: The default AWK IP is 192.168.127.253) Once the connection is made, change the Client AWK-3191's IP address to avoid an IP conflict with the AP AWK-3191; for example, 192.168.127.252/24, and set the wireless operation mode to Client.

Setting Confirmation: The RF bandwidth, Central Frequency, and SSID of the AP and Client must match in order to establish a connection.

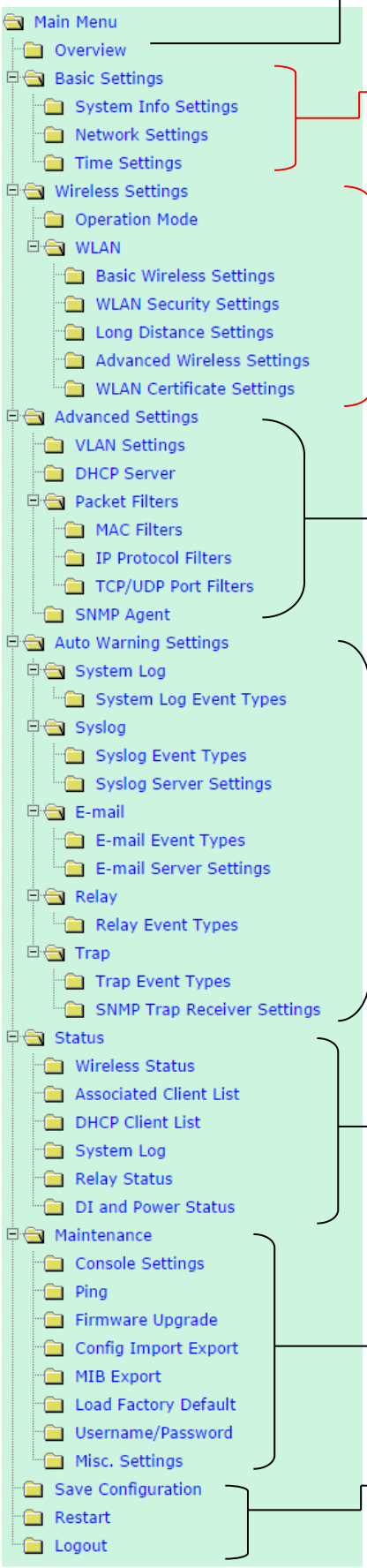


Verification: Once the connection is established, the Client side's SIGNAL LED will show its connection strength. Test the IP level communication by opening a DOS window command prompt on Notebook B and type:

ping <IP address of Notebook A, for example 192.168.127.2>

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

Function Map



Quick overview of the AWK-3191's status

Basic settings for administering the AWK-3191

Essential settings related to establishing a wireless network

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

Note: These advanced functions are all optional.

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

Note: These functions are all optional.

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

Functions for maintaining the AWK-3191, and for diagnosing the network.

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

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-3191 and make it easy to establish and maintain your wireless network.

The following topics are covered in this chapter:

- **Web Browser Configuration**
- **Overview**
- **Basic Settings**
  - System Info Settings
  - Network Settings
  - Time Settings
- **Wireless Settings**
- **Operation Mode**
- **Basic Wireless Settings**
  - WLAN Security Settings
  - Long Distance Setting
  - Advanced Wireless Settings
  - WLAN Certification Settings (for EAP-TLS in Client mode only)
- **Advanced Settings**
  - Using Virtual LAN
  - Configuring a Virtual LAN
  - DHCP Server (for AP mode only)
  - Packet Filters
  - SNMP Agent
- **Auto Warning Settings**
  - System Log
  - Syslog
  - E-mail
  - Relay
  - Trap
- **Status**
  - Wireless Status
  - Associated Client List (for AP mode only)
  - DHCP Client List (for AP mode only)
  - System Log
  - Relay Status
  - DI and Power Status
- **Maintenance**
  - Console Settings
  - Ping
  - Firmware Upgrade
  - Config Import/Export
  - MIB Export
  - Load Factory Default
  - Username/Password
  - Misc. Settings
- **Save Configuration**
- **Restart**
- **Logout**

Web Browser Configuration

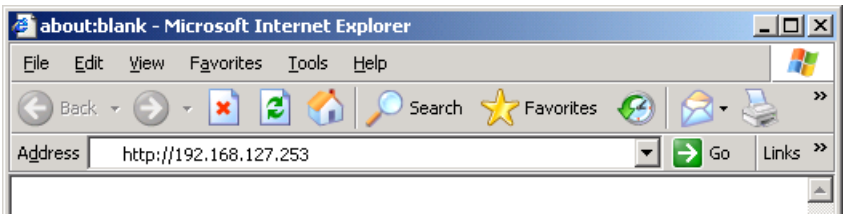
The AWK-3191's web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 or 8.0 with JVM (Java Virtual Machine) installed.

NOTE To use the AWK-3191's management and monitoring functions from a PC host connected to the same LAN as the AWK-3191, you must make sure that the PC host and the AWK-3191 are on the same logical subnet. Similarly, if the AWK-3191 is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

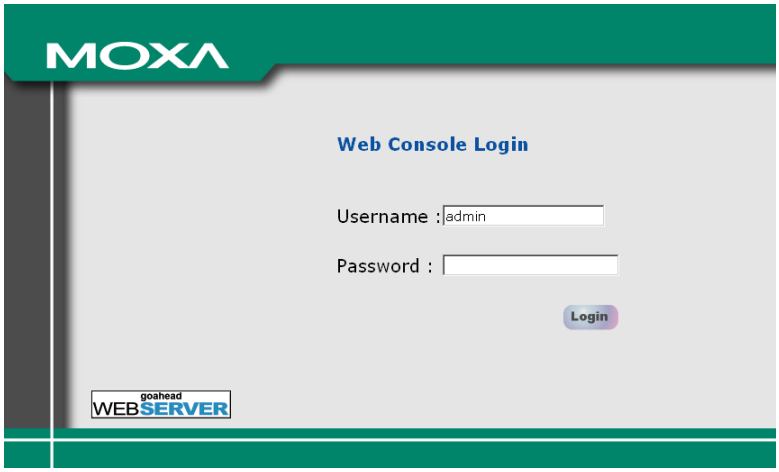
The Moxa AWK-3191's default IP is **192.168.127.253**.

Follow these steps to access the AWK-3191's web-based console management interface.

1. Open your web browser (e.g., Internet Explorer) and type the AWK-3191's IP address in the address field. Press **Enter** to establish the connection.

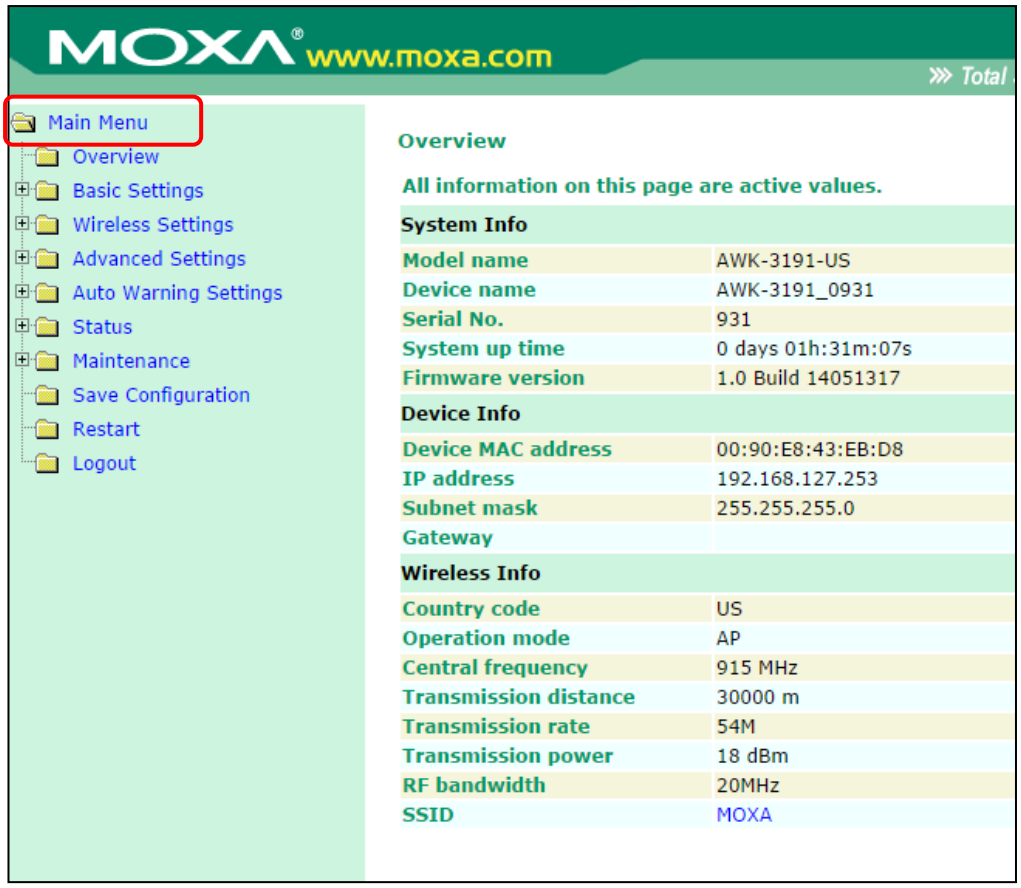


2. The Web Console Login page will open. Enter the password (default Username = **admin**; default Password = **root**) and then click **Login** to continue.



3. You may need 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-3191 are both shown in the title bar of the web page. This information can be used to help you identify multiple AWK-3191 units.

4. Use the menu tree on the left side of the window to open the function pages to access each of the AWK-3191's functions.



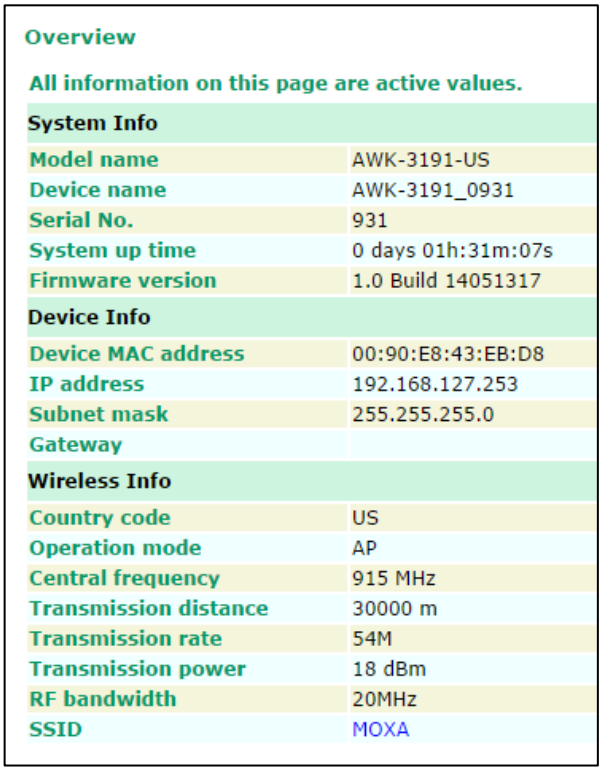
In the following paragraphs, we describe each AWK-3191 management function in detail. A quick overview is available in this manual in the "Function Map" section of Chapter 2.

NOTE The model name of the AWK-3191 is shown as AWK-3191-XX, where XX indicates the country code. The country code indicates the AWK-3191 version and which bandwidth it uses. We use **AWK-3191-US** as an example in the following figures. (The country code and model name that appears on your computer screen may be different than the one shown here.)

NOTE For security reasons, you will need to log back into the AWK-3191 after a 5-minute time-out.

Overview

The **Overview** page summarizes the AWK-3191's current status. The information is categorized into several groups: **System Info**, **Device Info**, and **Wireless Info**.

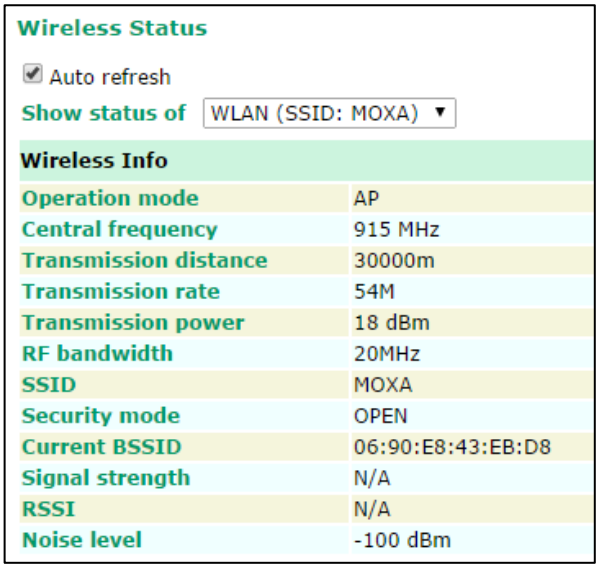


Overview

All information on this page are active values.

System Info	
Model name	AWK-3191-US
Device name	AWK-3191_0931
Serial No.	931
System up time	0 days 01h:31m:07s
Firmware version	1.0 Build 14051317
Device Info	
Device MAC address	00:90:E8:43:EB:D8
IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	
Wireless Info	
Country code	US
Operation mode	AP
Central frequency	915 MHz
Transmission distance	30000 m
Transmission rate	54M
Transmission power	18 dBm
RF bandwidth	20MHz
SSID	MOXA

Click on **SSID** for more detailed Wireless Information, as shown in the following figure.



Wireless Status

Auto refresh

Show status of WLAN (SSID: MOXA)

Wireless Info	
Operation mode	AP
Central frequency	915 MHz
Transmission distance	30000m
Transmission rate	54M
Transmission power	18 dBm
RF bandwidth	20MHz
SSID	MOXA
Security mode	OPEN
Current BSSID	06:90:E8:43:EB:D8
Signal strength	N/A
RSSI	N/A
Noise level	-100 dBm

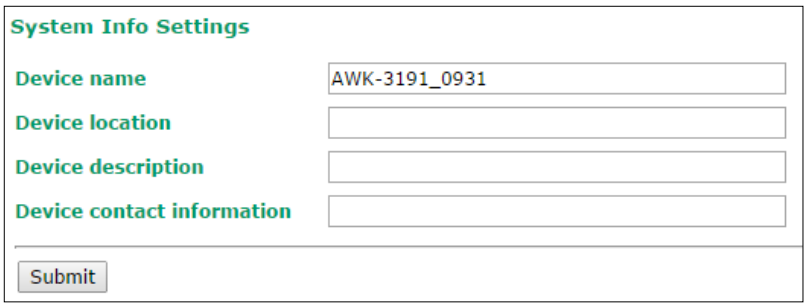
NOTE The wireless info that is displayed may be different for different operation modes. For example, "Current BSSID" is not available in Client mode, and "Signal strength" is not available in AP mode.

Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the AWK-3191.

System Info Settings

The **System Info** items, especially ***Device name*** and ***Device description***, are displayed and included on the **Overview** page, in SNMP information, and in alarm emails. Setting **System Info** items makes it easier to identify the different AWK-3191 units connected to your network.



Device name

Setting	Description	Factory Default
Max. of 31 characters	This option is useful for specifying the role or application of different AWK-3191 units.	AWK-3191_<Serial No. of this AWK-3191>

Device location

Setting	Description	Factory Default
Max. of 31 characters	Specifies the location of different AWK-3191 units.	None

Device description

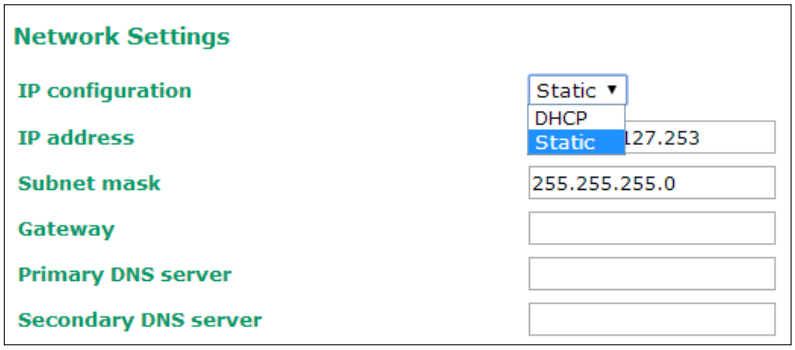
Setting	Description	Factory Default
Max. of 31 characters	Use this space to record a more detailed description of the AWK-3191.	None

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-3191.	None

Network Settings

The Network Settings configuration panel allows you to modify the usual TCP/IP network parameters. An explanation of each configuration item is given below.



IP configuration

Setting	Description	Factory Default
DHCP	The AWK-3191's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the AWK-3191's IP address manually.	

IP address

Setting	Description	Factory Default
AWK-3191's IP address	Identifies the AWK-3191 on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
AWK-3191's subnet mask	Identifies the type of network to which the AWK-3191 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

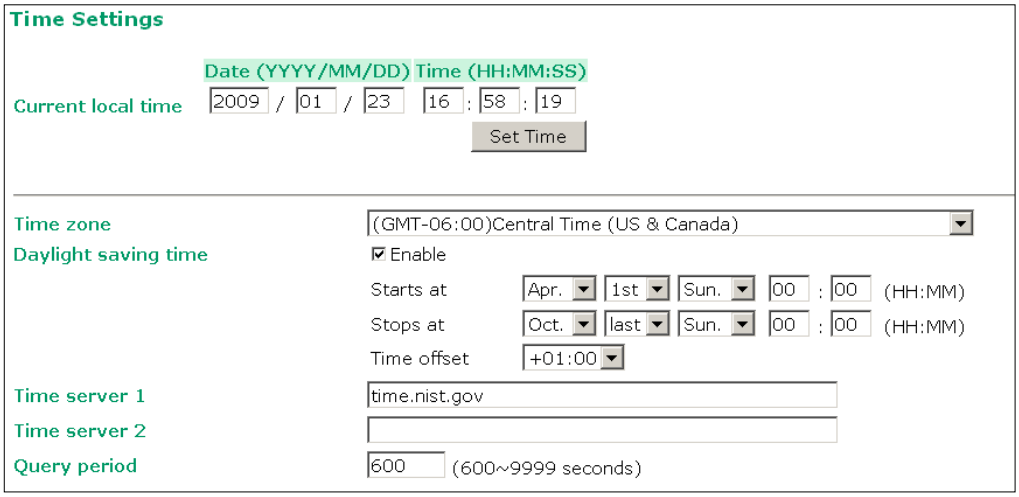
Setting	Description	Factory Default
AWK-3191's default gateway	The IP address of the router that connects the LAN to an outside network.	None

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-3191'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

Time Settings

The AWK-3191 has a time calibration function based on information from an NTP server or user specified Date and Time information. Functions such as Auto warning can add real-time information to the message.



The ***Current local time*** shows the AWK-3191's system time when you open this web page. You can click on the **Set Time** button to activate the updated date and time parameters. An "(Updated)" string will appear to indicate that the change is complete. Local time settings will be immediately activated in the system without running Save and Restart.

NOTE The AWK-3191 has a built-in real time clock (RTC). We strongly recommend that users update the Local time for the AWK-3191 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 (also known as 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

Query period

Setting	Description	Factory Default
Query period time (1 to 9999 seconds)	This parameter determines how often the time is updated from the NTP server.	600 (seconds)

Wireless Settings

The AWK-3191 provides two different sets of wireless operation modes: **AP/client** mode for point-to-multipoint communication and **master/slave** mode for transparent point-to-point communication. The major differences between these two operation modes are the MAC address translation on the client/slave radio.

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

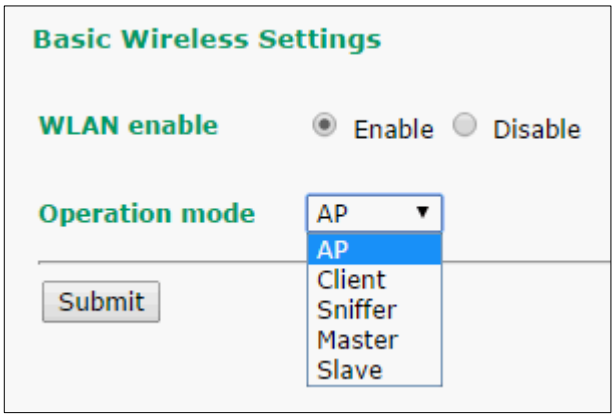
Master/slave: A transparent point-to-point protocol that allows the devices' MAC addresses to remain unchanged when the packets get through the slave radio. If you are looking for a worry-free wireless solution to replace your wired system, use Master/Slave.

Sniffer: Since the 900 MHz band is not a standard 802.11 frequency, no currently available laptop or sniffer can diagnose this frequency. In order to provide an easier way for our customers to analyze wireless traffic, the AWK-3191 provides 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-3191 supports five operation modes—AP, Client, Master, Slave, and Sniffer—each of which plays a distinct role on the wireless network.



Wireless Enable

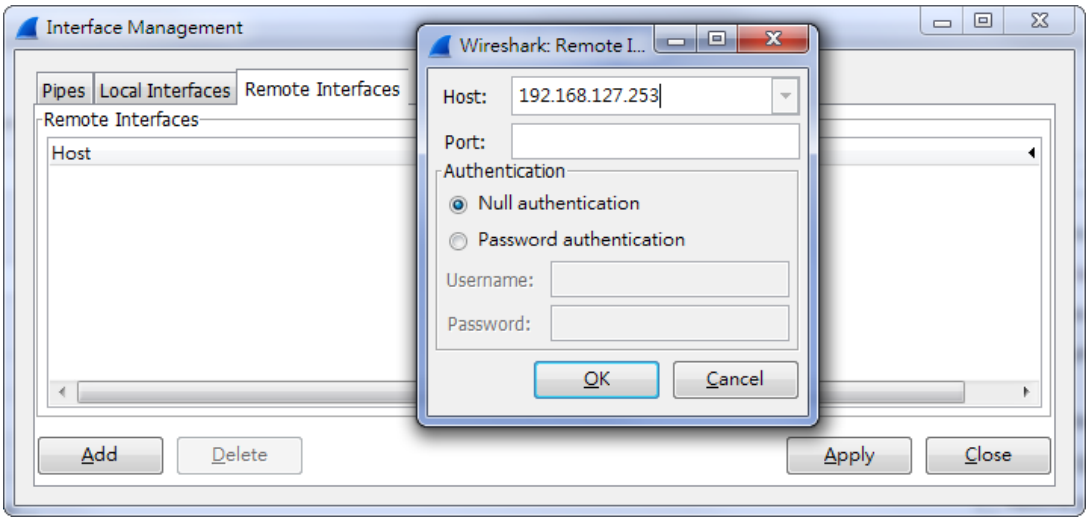
Setting	Description	Factory Default
Enable/Disable	The RF (Radio Frequency) module can be manually turned on or off.	Enable

Operation Mode

Setting	Description	Factory Default
AP	The AWK-3191 plays the role of wireless AP to allow multiple AWK-3191 wireless Client connections.	AP
Client	The AWK-3191 plays the role of wireless Client to allow connection to a AWK-3191 wireless AP.	
Master	The AWK-3191 plays the role of wireless Master to pair with wireless Slave to allow transparent point-to-point communication.	
Slave	The AWK-3191 plays the role of wireless Slave to pair with wireless Master to allow transparent point-to-point communication.	
Sniffer	Turns the device into a remote Wireshark interface to capture 900 MHz packets for analysis.	

Sniffer mode instructions:

1. Set operation mode to Sniffer mode on the AWK-3191 and then save/reboot the device.
2. Connect the AWK-3191 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-3191.

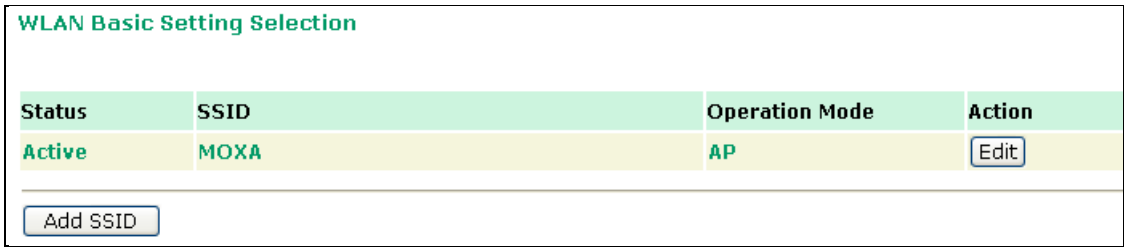


Detailed Wireshark instructions can be found at the following link:
https://www.wireshark.org/docs/wsug_html_chunked/ChCapInterfaceRemoteSection.html

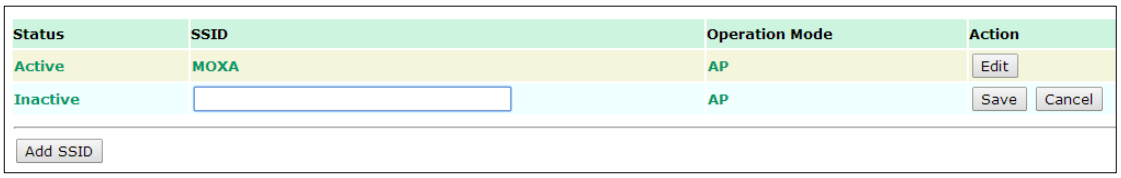
4. Start capturing 900 MHz wireless packets with Wireshark.

Basic Wireless Settings

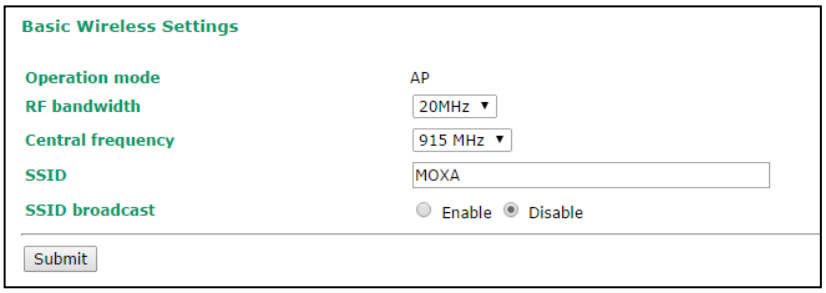
The "WLAN Basic Setting Selection" panel is used to add and edit SSIDs. An SSID (Service Set IDentifier) is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSIDs. You can configure your AWK to use up to 9 SSIDs, and configure each SSID differently. 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.



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



Click on **Edit** to assign different configuration settings to each SSID. The configuration panel appears as follows:



NOTE In the Basic Wireless Settings page, all settings need to be matching between AP/Client and Master/Slave devices in order to establish connections.

RF bandwidth

Setting	Description	Factory Default
20MHz	Set channel bandwidth to 20 MHz	20MHz
10MHz	Set channel bandwidth to 10 MHz	
5MHz	Set channel bandwidth to 5 MHz	

Central frequency

Setting	Description	Factory Default
Available channels vary with RF bandwidth	Based on different channel bandwidths, users can select their central frequency freely to optimize their 900 MHz connection.	915MHz

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.	MOXA

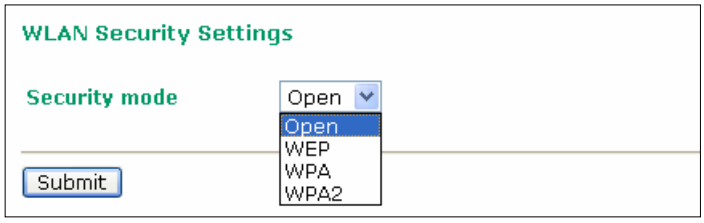
SSID broadcast (for AP/Master mode only)

Setting	Description	Factory Default
Enable/ Disable	Determines whether or not the SSID can be broadcast	Enable

WLAN Security Settings

The AWK-3191 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-3191 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-3191 supports three EAP methods: EAP-TLS, EAP-TTLS, and EAP-PEAP.



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

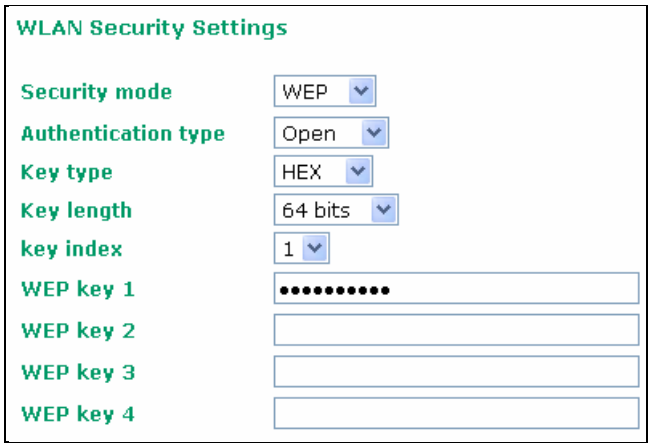
For security reasons, you should **NOT** set security mode to Open System, since authentication and data encryption are **NOT** performed in Open System mode.

WEP

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

When WEP is enabled as a security mode, the length of a key (so-called WEP seed) can be specified as 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The AWK-3191 provides 4 entities of WEP key settings that can be selected to use with ***Key index***. The selected key setting specifies the key to be used as a *send-key* for encrypting traffic from the AP side to the wireless client side. All 4 WEP keys are used as *receive-keys* to decrypt traffic from the wireless client side to the AP side.

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



Authentication type

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

Key type

Setting	Description	Factory Default
HEX	Specifies WEP keys in hexadecimal format	HEX
ASCII	Specifies WEP keys in ASCII format	

Key length

Setting	Description	Factory Default
64 bits	Uses 40-bit secret key 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

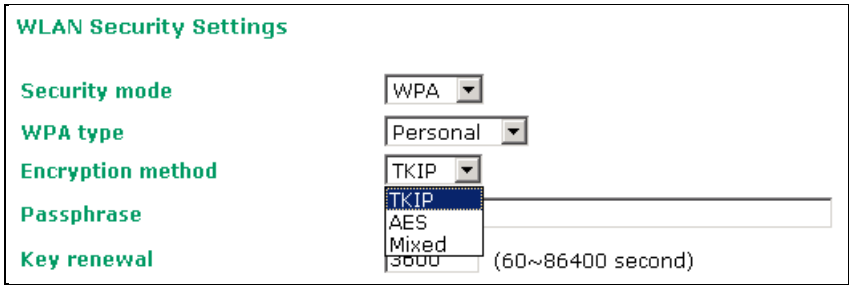
Setting	Description	Factory Default
ASCII type: 64 bits: 5 chars 128 bits: 13chars HEX type: 64 bits: 10 hex chars 128 bits: 26 hex chars	A string that can be used as a WEP seed for the RC4 encryption engine	None

WPA / WPA2-Personal

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

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-3191 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. The Passphrase must contact at least 8 ASCII characters, and could be as long as 63 ASCII characters. For security reasons, this passphrase should only be disclosed to users who need it, and it should be changed regularly.



WPA type

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

Encryption method

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

**This option is available in AP/Master mode 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	None

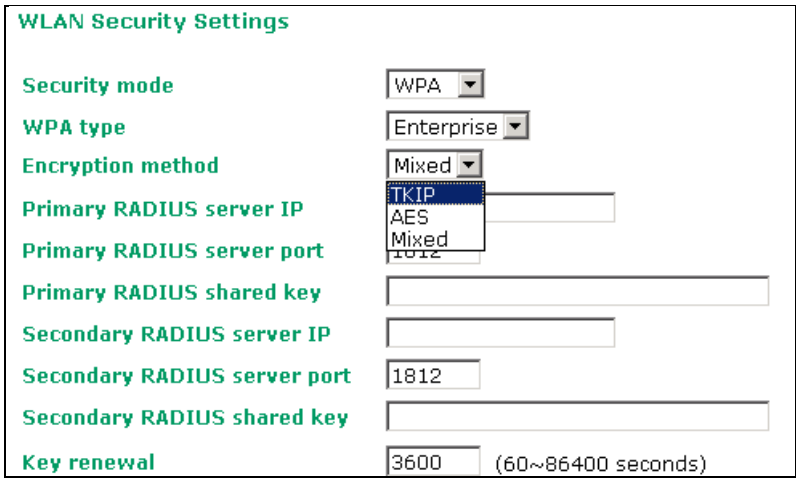
Key renewal (for AP/Master mode only)

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.



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	TKIP
AES	Advanced Encryption System is enabled	
Mixed*	Provides TKIP broadcast key and TKIP+AES unicast key for some legacy Clients. This option is rarely used.	

**This option is available in AP/Master mode only, and cannot support AES-enabled clients.*

Primary/Secondary RADIUS server IP

Setting	Description	Factory Default
The IP address of the 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

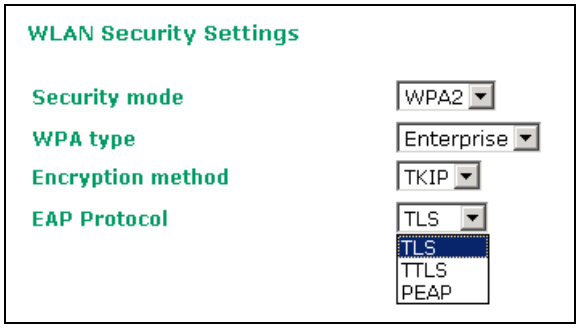
Setting	Description	Factory Default
Max. of 31 characters	The secret key shared between the AP and RADIUS server	None

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/Slave mode)

When used as a client, the AWK-3191 can support three EAP methods (or ***EAP protocols***): **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**, corresponding to WPA/WPA-Enterprise settings on the AP side.



Encryption method

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

EAP Protocol

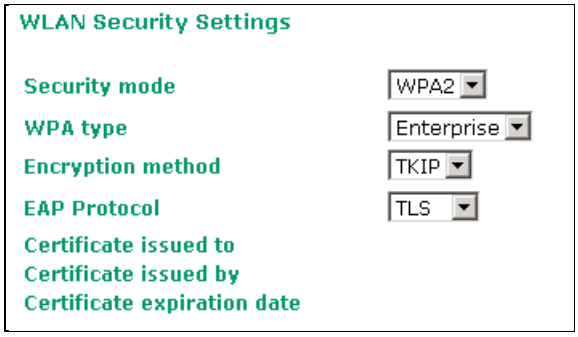
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

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

EAP-TLS

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

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



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

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

EAP-TTLS

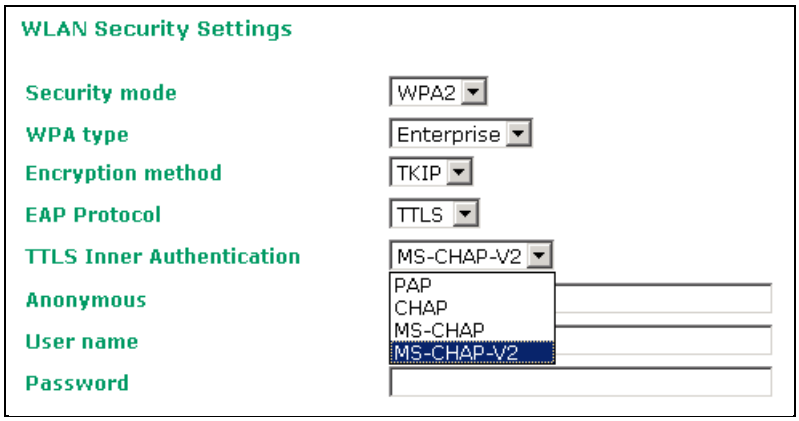
It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than creating a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called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

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

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

The AWK-3191 provides some non-cryptographic EAP methods, including **PAP**, **CHAP**, **MS-CHAP**, and **MS-CHAP-V2**. These EAP methods are not recommended for direct use on wireless networks. However, they may be useful as inner authentication methods with TTLS and PEAP.

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



TTL Inner Authentication

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

Anonymous

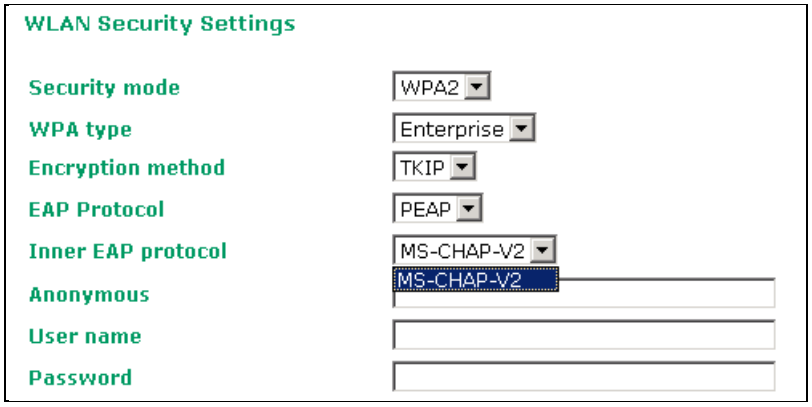
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	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 the tunnel. The AWK-3191 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

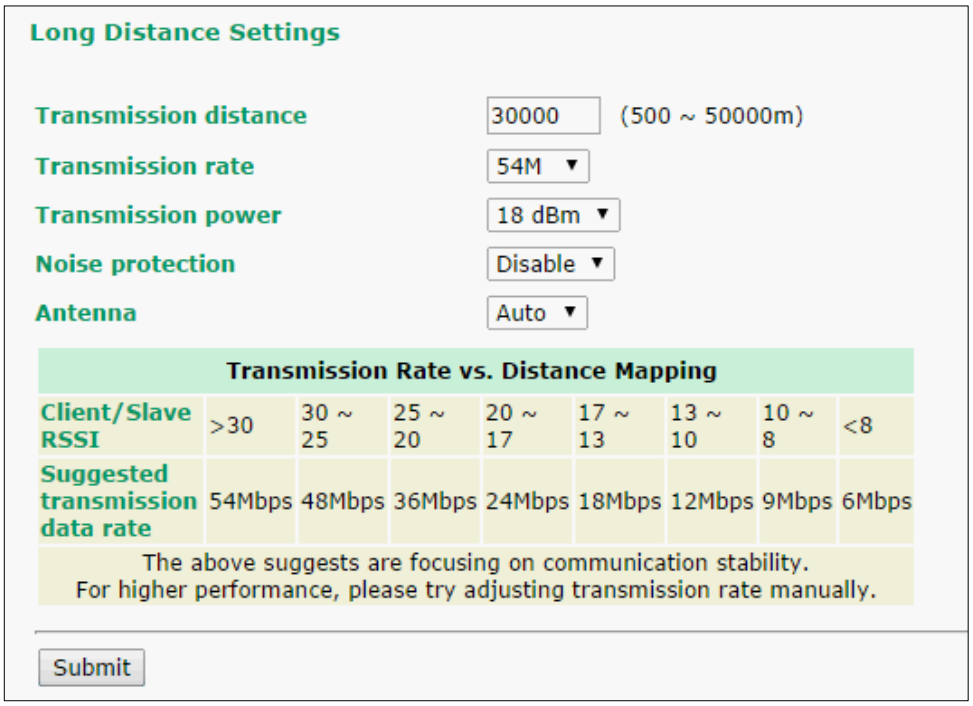
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
	User name and password used in inner authentication	None

Long Distance Setting

This menu contains all the essential settings to establish a successful long distance communication. The default values in this section aim to provide a stable connection rather than an optimized connection. To have an optimized performance, you must fine tune the parameter based on your application and onsite installation.



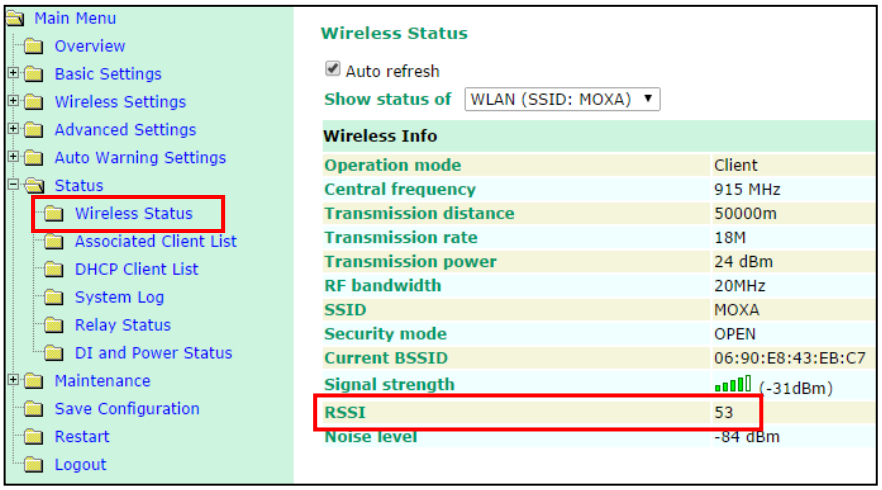
Transmission distance

Setting	Description	Factory Default
500 to 50000 meters	Specify the maximum transmission distance. IMPORTANT: The specified distance must be longer than the actual transmission distance. AP mode: Specify the longest transmission distance among all Client devices. Master/Client/Slave: Specify the transmission distance to the target device.	50,000m

Transmission rate

Setting	Description	Factory Default
6, 9, 12, 18, 24, 36, 48, 54Mbps	Specify the target transmission rate. Refer to the RSSI vs. TX Rate table below.	18M

After installing the device, fine tune the transmission rate based on the onsite RSSI value. For Client/Slave radios, the RSSI value can be seen on the Client device's Wireless Status page. For AP/Master radios, follow the lowest rate among all Client radios.



RSSI vs. Transmission Rate Mapping								
Client/Slave RSSI	> 30	30-25	25-20	20-17	17-13	13-10	10-8	< 8
Suggested Transmission Data Rate	54 Mbps	48 Mbps	36 Mbps	24 Mbps	18 Mbps	12 Mbps	9 Mbps	6 Mbps
The above suggestions focus on communication stability. For higher performance, try adjusting the transmission rate manually.								

Transmission power

Setting	Description	Factory Default
0 to 24 dBm	Adjust the transmission power	18M

NOTE The term **over saturated** refers to when the power of the radio signal is too strong for the signal to be received correctly at the receiving end. This problem can usually be observed when using high gain antennas over short distances. The radio signal tends to reach the saturation point when the RSSI is over 80 or Signal Strength is over -20 dBm. When saturation occurs, you should detect a very strong radio signal and communication will be disrupted. When this happens, you can reduce the transmission power, reduce the antenna gain, or increase the communication distance.

Noise protection

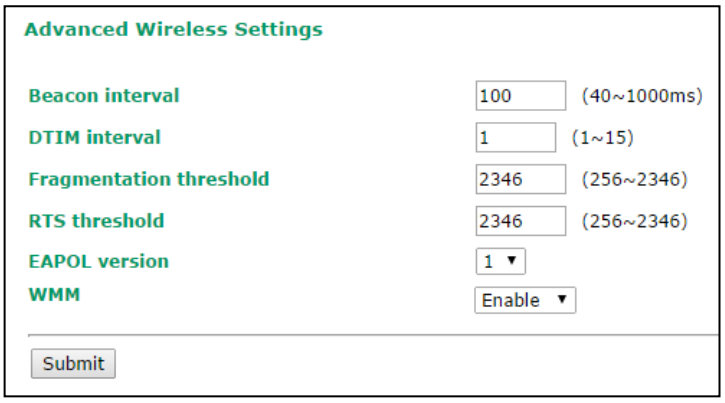
Setting	Description	Factory Default
Enable/Disable	Adjusts the capability of the wireless signal to cope with interference. This option should be enabled for communication distances less than 500 meters, and should be disabled for communication distances over 500 meters.	Disable

Antenna

Setting	Description	Factory Default
Auto	The AWK-3191 uses two antennas (MAIN and AUX) to reduce multipath effects.	Main
Main	Diversity function is disabled. Only MAIN antenna is in use.	
Aux	Diversity function is disabled. Only AUX antenna is in use.	

Advanced Wireless Settings

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



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)

DTIM Interval (for AP/Master mode only)

Setting	Description	Factory Default
Data Beacon Rate (1 to 15)	Indicates how often the AWK-3191 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 should be before splitting it 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 Refer to the relevant glossaries in Chapter 5 for detailed information about the above-mentioned settings. By setting these parameters properly, you can better tune the performance of your wireless network.

EAPOL Version

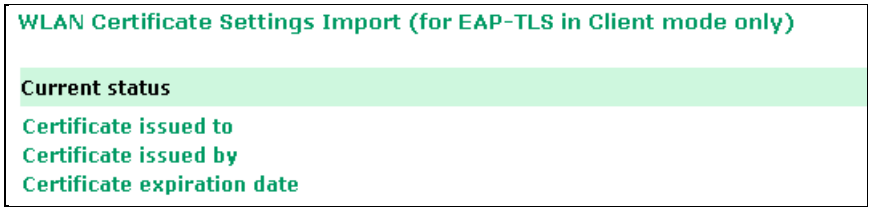
Setting	Description	Factory Default
1	EAPOL version 1 was standardized in the 2001 version of 802.1X, which is much more commonly implemented.	1
2	EAPOL version 2 was specified in 802.1X-2004.	

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.	Disable

WLAN Certification 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 mode. The AWK-3191 supports **PKCS #12**, also known as *Personal Information Exchange Syntax Standard*, certificate formats that define file formats commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.

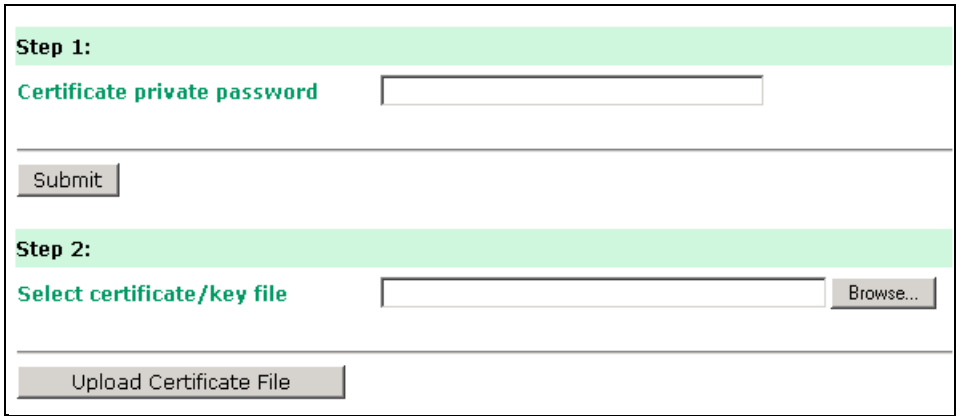


Current Status displays information for the current WLAN certificate, which has been imported into the AWK-3191. Nothing will be shown if a certificate is not available.

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, the information will be uploaded to ***Current Certificate***. If it fails, you may need to return to step 1 to set the password correctly and then import the certificate file again.



NOTE The WLAN certificate will remain after the AWK-3191 reboots. Even though it has expired, it can still be seen on the **Current Certificate**.

Advanced Settings

Several advanced functions are available to increase the functionality of your AWK-3191 and wireless network system. A VLAN is a collection of clients and hosts grouped together as if they were connected to the broadcast domains in a layer 2 network. The DHCP server helps you deploy wireless clients efficiently. Packet filters provide security mechanisms, such as firewalls, in different network layers. Moreover, the AWK-3191 can support STP/RSTP protocol to increase reliability across the entire network, and SNMP support can make network management easier.

Using Virtual LAN

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

The Virtual LAN (VLAN) Concept

What is a VLAN?

A virtual LAN, commonly known as a VLAN, is a group of hosts with a common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of their physical location. A VLAN has the same attributes as a physical LAN, but it allows end stations to be grouped together even if they are not located on the same network switch. Network reconfiguration can be done through software instead of physically relocating devices.

VLANs now extend as far as the reach of the access point signal. Clients can be segmented into wireless sub-networks via SSID and VLAN assignments. A Client can access the network by connecting to an AP configured to support its assigned SSID/VLAN.

Benefits of VLANs

VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage adds, moves, and changes from a single point of contact
- Define and monitor groups
- Reduce broadcast and multicast traffic to unnecessary destinations
- Improve network performance and reduce latency
- Increase security
- Create a secure network that restricts members to resources on their own VLAN
- Clients can roam without compromising security

VLAN Workgroups and Traffic Management

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

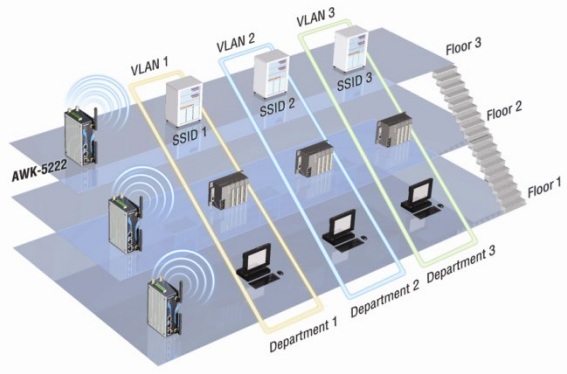
The AP matches packets transmitted or received to a network name with the associated VLAN. Traffic received by a VLAN is only sent on the wireless interface associated with that same VLAN. This eliminates unnecessary traffic on the wireless LAN, conserving bandwidth and maximizing throughput.

In addition to enhancing wireless traffic management, the VLAN-capable AP supports easy assignment of wireless users to workgroups. In a typical scenario, each user VLAN represents a department workgroup; for example, one VLAN could be used for a marketing department and the other for a human resource department.

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as, for example, marketing or human resources, depending on which wireless client received it. The AP would

insert VLAN headers or “tags” with identifiers into the packets transmitted on the wired backbone to a network switch.

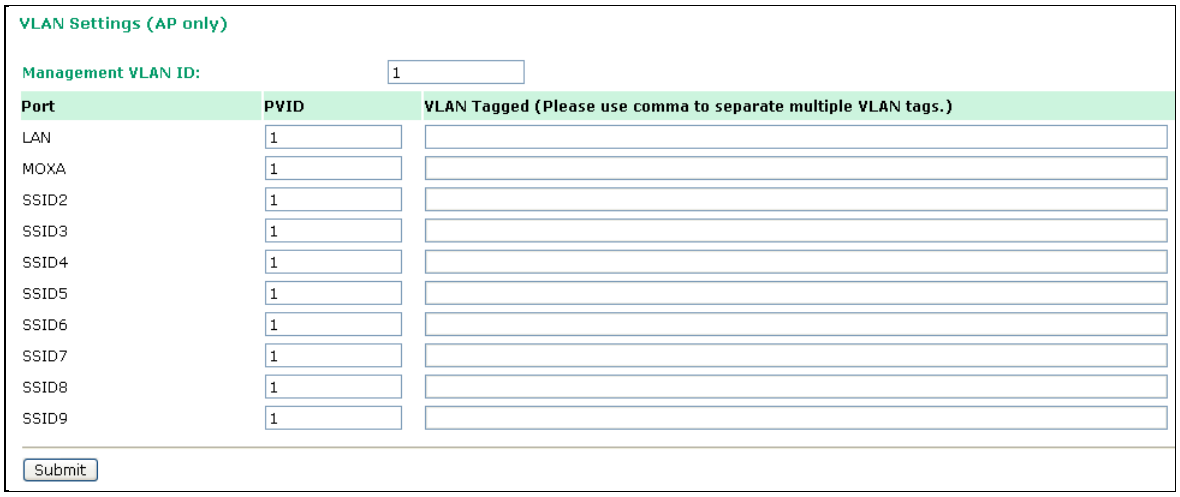
Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resources department, for example, could be restricted to a gateway that allowed access to only the Internet. A member of the human resources department could send and receive e-mail and access the Internet, but would be prevented from accessing servers or hosts on the local corporate network.



Configuring a Virtual LAN

VLAN Settings

To configure the AWK’s VLAN, use the VLAN Settings page to configure the ports.



Management VLAN ID

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

Port

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

Port PVID

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

VLAN Tagged

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

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

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

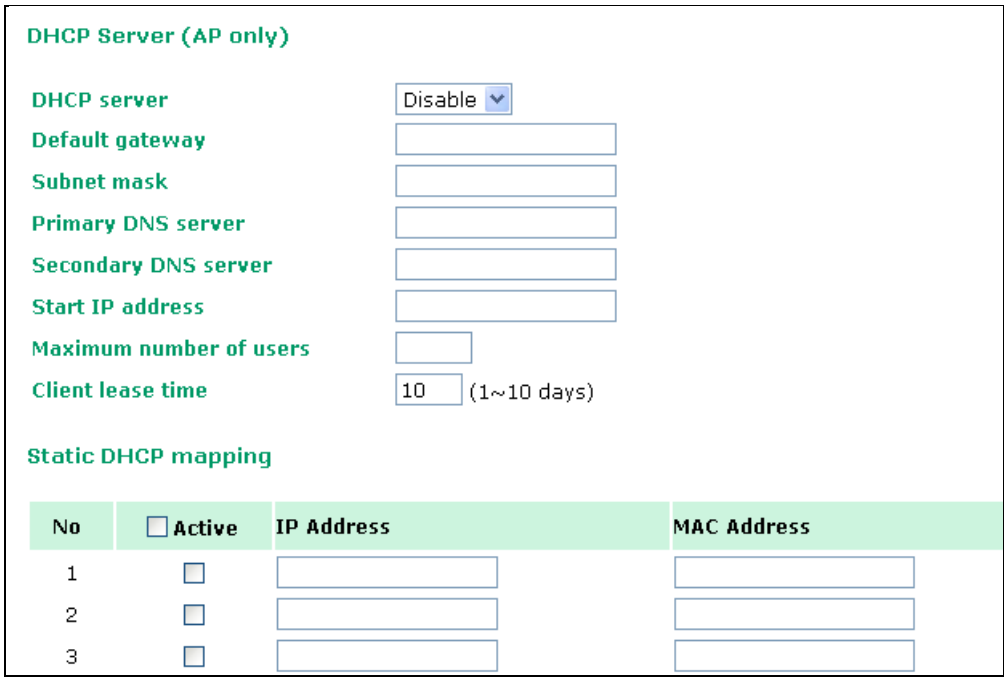
DHCP Server (for AP mode only)

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-3191 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-3191 provides a **Static DHCP mapping** list with up to 16 entities. Don't forget 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 the AWK-3191 as a DHCP server	Disable
Disable	Disables the 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 the 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	The first IP address the AWK-3191 will assign	None

Maximum number of users

Setting	Description	Factory Default
1 to 999	Specifies how many IP addresses can be assigned continuously	None

Client lease time

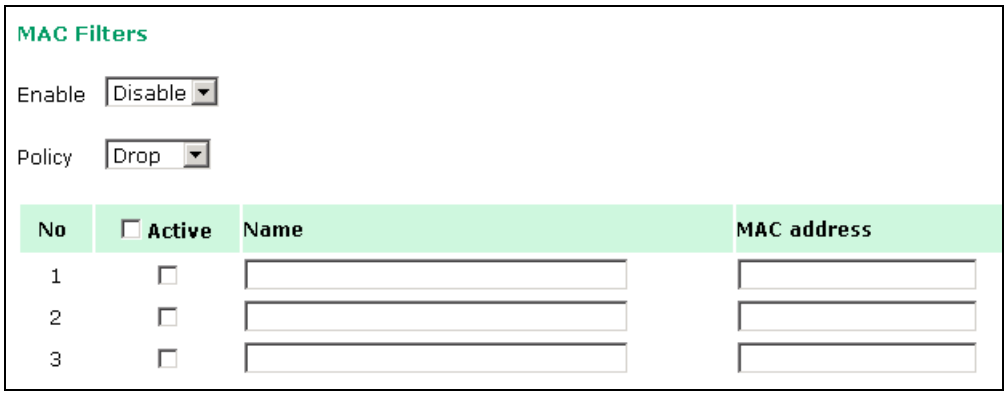
Setting	Description	Factory Default
1 to 10 days	The lease time for which an IP address is assigned. The IP address will expire after the lease time is reached.	10 (days)

Packet Filters

The AWK-3191 includes various filters for **IP-based** packets going through LAN and WLAN interfaces. You can set these filters as a firewall to help enhance network security.

MAC Filter

The AWK-3191's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The AWK-3191 provides 8 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the setting.



Enable

Setting	Description	Factory Default
Enable	Enables MAC filter	Disable
Disable	Disables MAC filter	

Policy

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

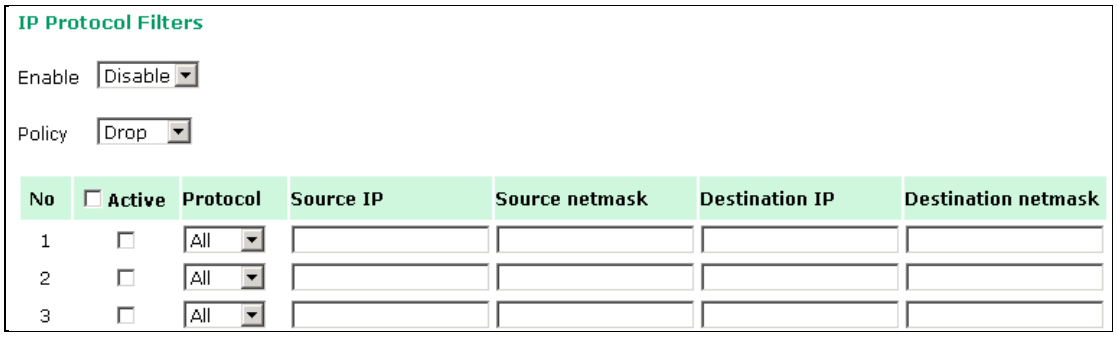
ATTENTION

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 Filter

The AWK-3191's IP protocol filter is a policy-based filter that can allow or filter out IP-based packets with specified IP protocols and source/destination IP addresses.

The AWK-3191 provides 8 entities for setting IP protocols 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.



Enable

Setting	Description	Factory Default
Enable	Enables IP protocol filter	Disable
Disable	Disables IP protocol filter	

Policy

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

ATTENTION

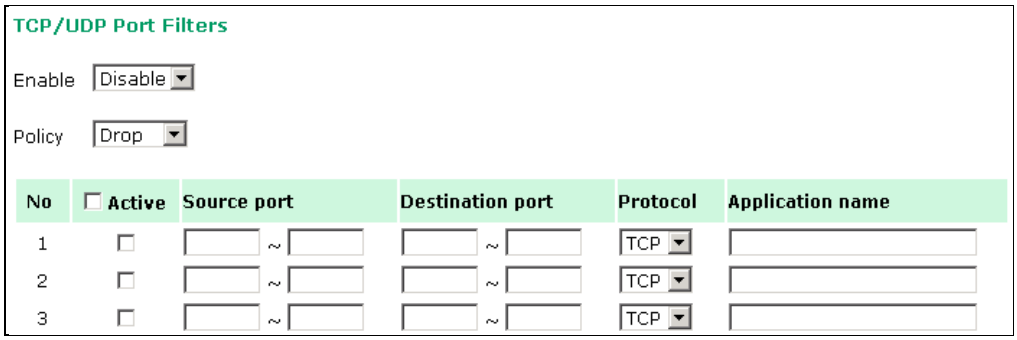
Be careful when you enable the filter function:
Drop + "no entity on list is activated" = all packets are **allowed**
Accept + "no entity on list is activated" = all packets are **denied**

TCP/UDP Port Filter

The AWK-3191'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-3191 provides 8 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.



Enable

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

Policy

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

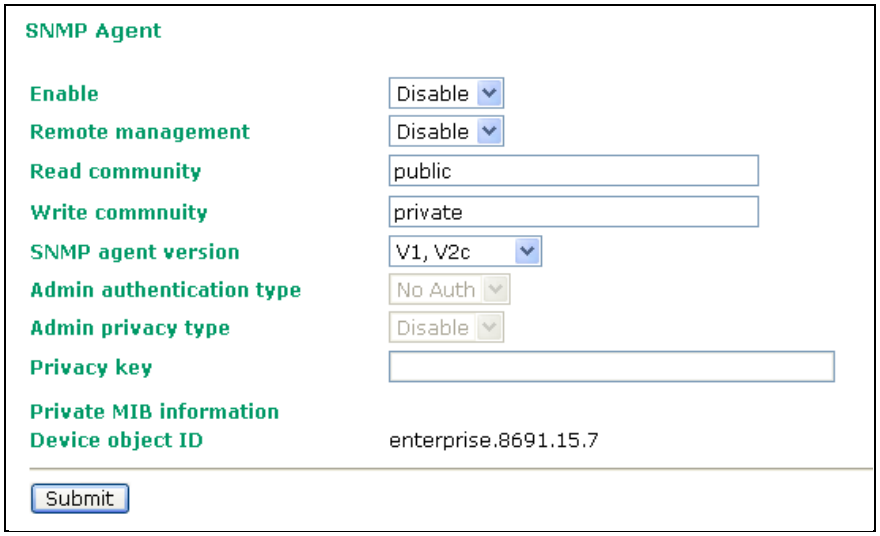
The AWK-3191 supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

The AWK-3191's MIB (management information base), which can be downloaded from the Moxa website, supports reading the attributes via SNMP. Currently only the HTTP ***get*** method is supported.

SNMP security modes and security levels supported by the AWK-3191 are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

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

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



Enable

Setting	Description	Factory Default
Enable	Enables SNMP Agent	Disable
Disable	Disables SNMP Agent	

Remote Management

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

Read community (for V1, V2c)

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

Write community (for V1, V2c)

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

SNMP agent version

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

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

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

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

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

Private key

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

Private MIB Information Device Object ID

Also known as ***OID,*** this is the AWK-3191's enterprise value and is a fixed value.

Auto Warning Settings

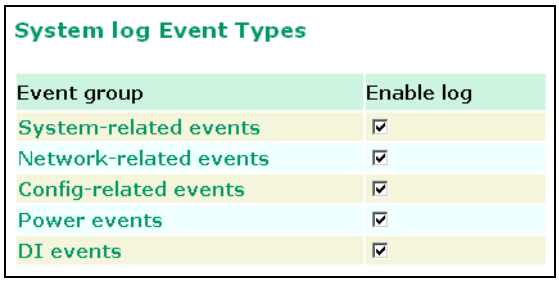
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system 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-3191 supports different approaches to warn engineers automatically, such as SNMP trap, e-mail, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Log

System Log Event Types

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



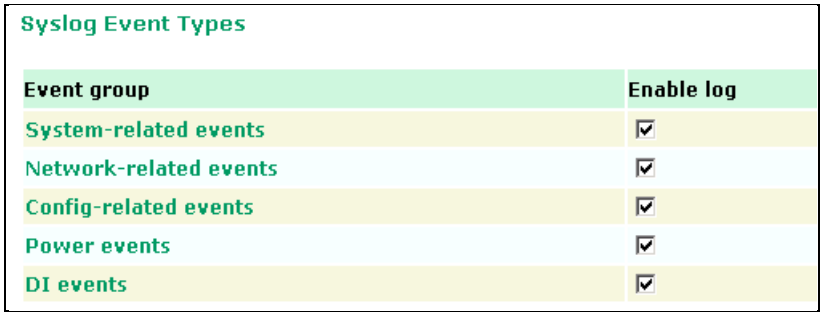
System-related events	**Event is triggered when…**
System restarts (warm start)	The AWK-3191 is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
LAN link on	The LAN port is connected to a device or network.
LAN link off	The port is disconnected (e.g., the cable is pulled 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-3191 is associated with an AP.
WLAN disconnected (for Client/Slave mode)	The AWK-3191 is disassociated from an AP.
Config-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-3191.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The AWK-3191's firmware is updated.
Power events	**Event is triggered when…**
Power 1/2 transition (On -> Off)	The AWK-3191's PWR1/2 is powered down.
PoE transition (On -> Off)	The AWK-3191's PoE (Hardware Rev. 3.0.0 supports PoE; hardware Rev. 2.0.0 does not support PoE.) is powered down.
Power 1/2 transition (Off -> On)	The AWK-3191 is powered with PWR1/2.
PoE transition (Off -> On)	The AWK-3191 is powered with PoE (Hardware Rev. 3.0.0 supports PoE; hardware Rev. 2.0.0 does not support PoE.).
DI events	**Event is triggered when…**
DI1/2 transition (On -> Off)	Digital Input 1/2 is triggered by on to off transition
DI1/2 transition (Off -> On)	Digital Input 1/2 is triggered by off to on transition

Syslog

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

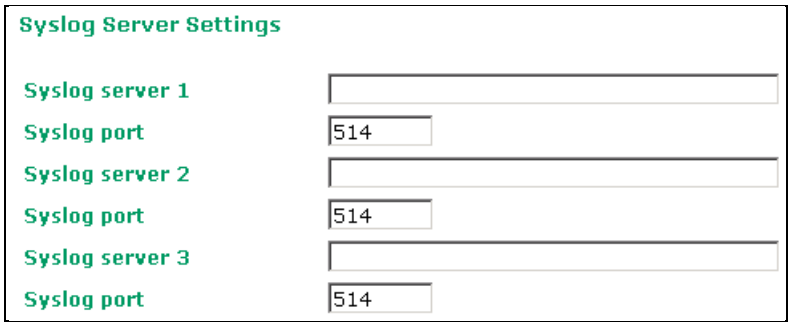
Syslog Event Types

Detailed information for the grouped events is shown in the following table. You can check the box for **Enable log** to enable the grouped events. All default values are enabled (checked). Details for each event group can be found on the "System log Event Types" table on page 3-31.



Syslog Server Settings

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



Syslog server 1 / 2 / 3

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

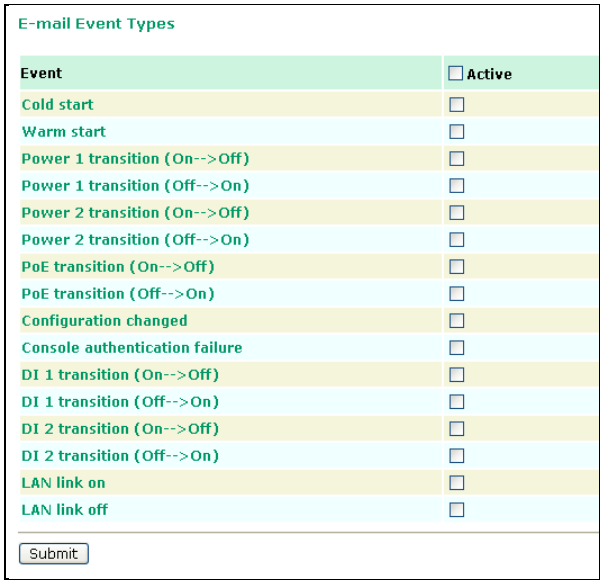
Syslog port

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

E-mail

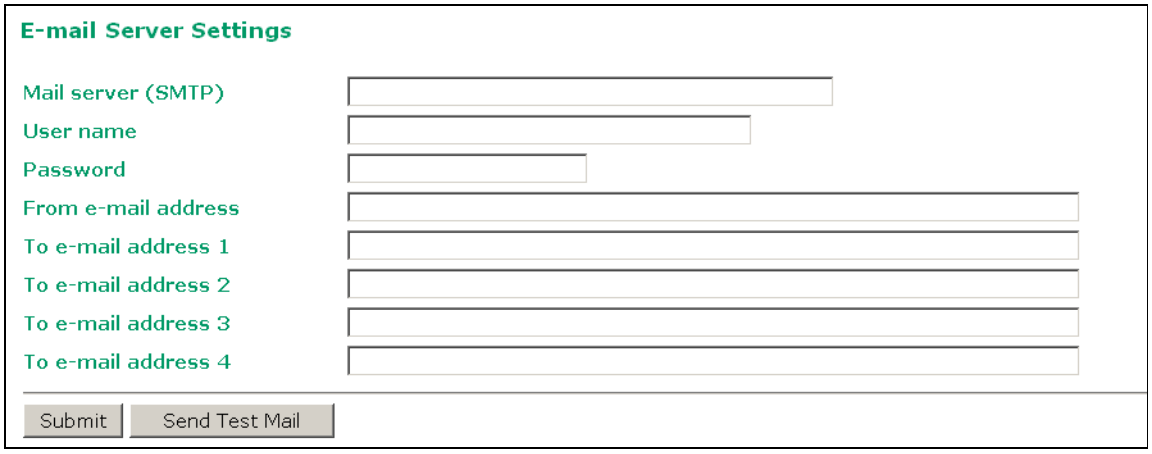
E-mail Event Types

Check the box for **Active** to enable the event items. The default values for all items is deactivated (unchecked). Details for each event item can be found on the "System log Event Types" table on page 3-31.



E-mail Server Settings

You can set up to 4 email addresses to receive alarm emails from the AWK-3191. 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 email 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 email address, which will be shown in the "From" field of a warning email.	None

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

Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' email addresses.	None

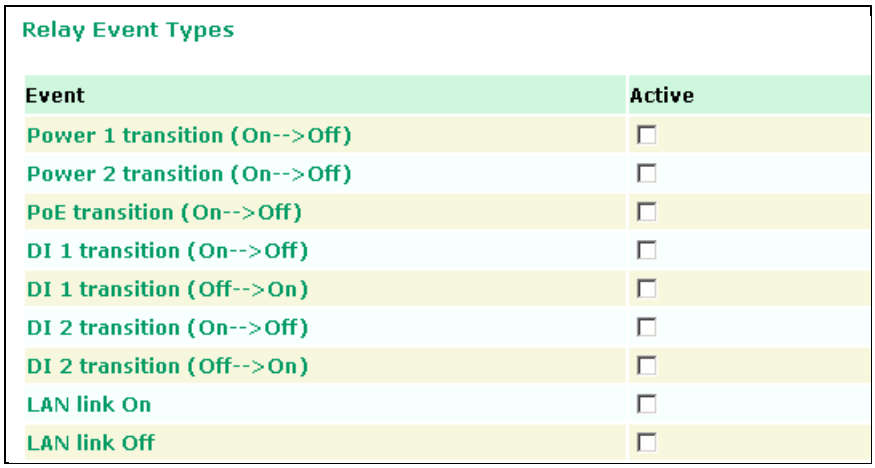
Relay

The AWK-3191 has one relay output, which consists of 2 terminal block contacts on the AWK-3191's top panel. These relay contacts are used to indicate user-configured events and system failure.

The two wires attached to the relay contacts form an open circuit when a user-configured event is triggered. If a user-configured event does not occur, the relay circuit will remain closed. For safety reasons, the relay circuit is kept open when the AWK-3191 is not powered on.

Relay Event Types

Checkmark the **Active** checkbox to enable an event item. The default values for all items is deactivated (unchecked). Details for each event item can be found in the "System log Event Types" table on page 3-31.

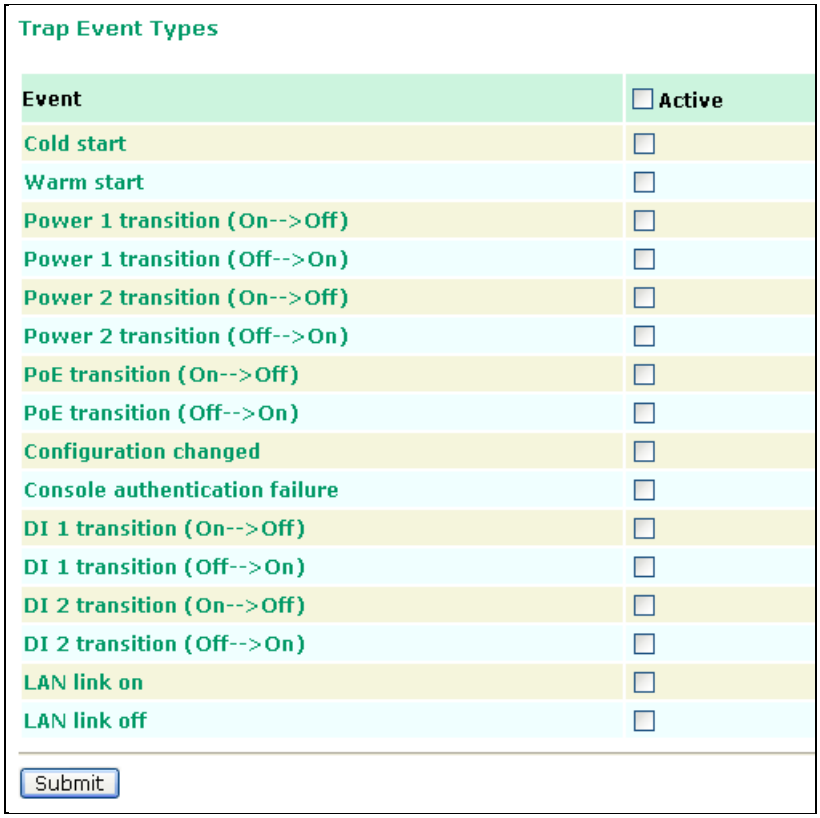


Trap

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

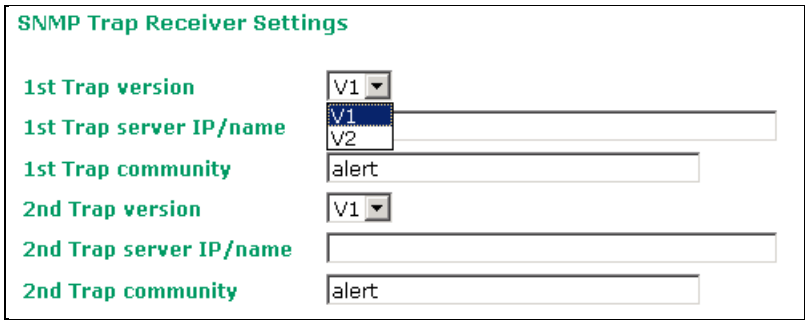
Because a management station usually takes care of a large number of devices that have a large number of objects, the management station will be overloaded if it needs to poll or send requests to query every object on every device. It would be better if the managed device agent could notify the management 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

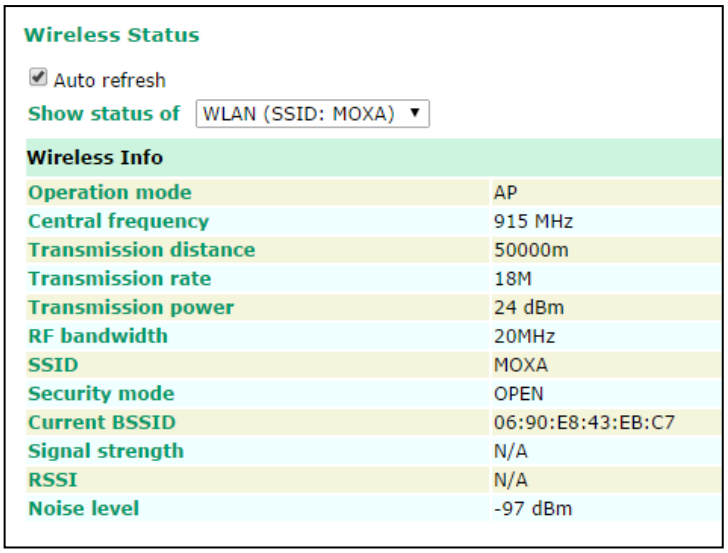
Status

Wireless Status

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

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

It is helpful to use the continuously updated information on this page, such as **Signal strength**, to monitor the signal strength of the AWK-3191 in Client mode.

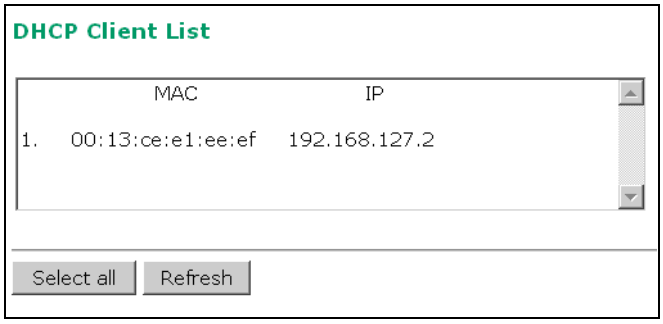


Associated Client List (for AP mode only)

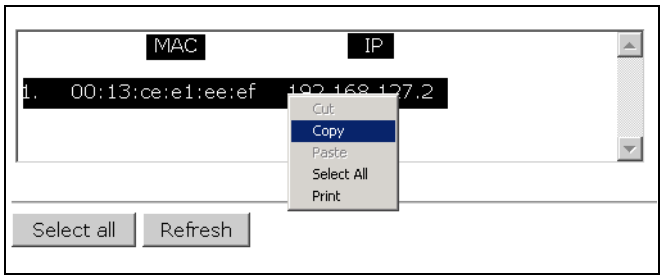
The Associated Client List shows all the clients that are currently associated to a particular AWK-3191. You can click **Select all** to select all the content in the list for further editing. You can click **Refresh** to refresh the list.

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.

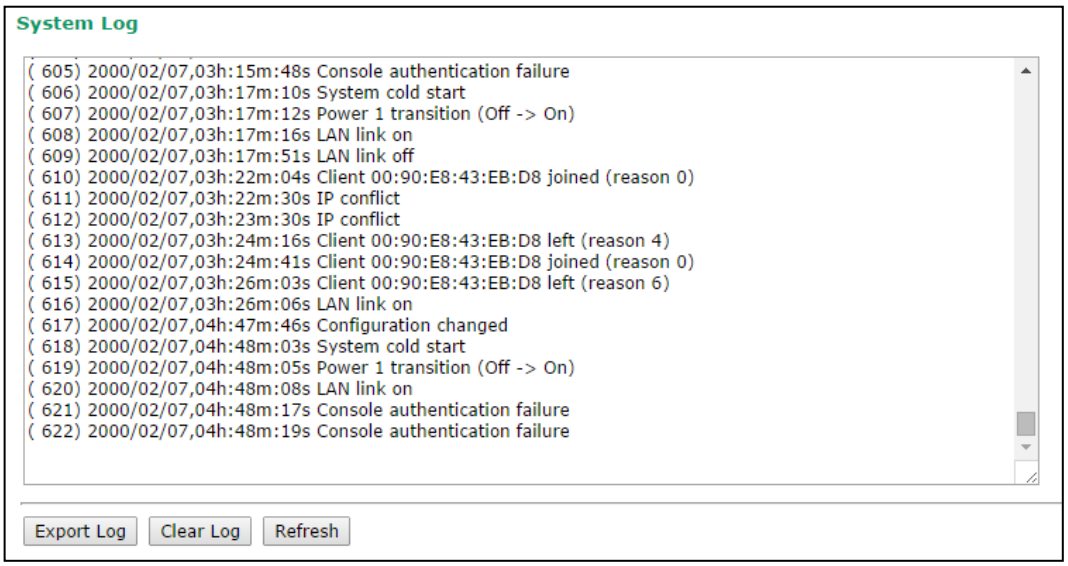


Click the **Select all** button to select all of the content in the list for further editing.



System Log

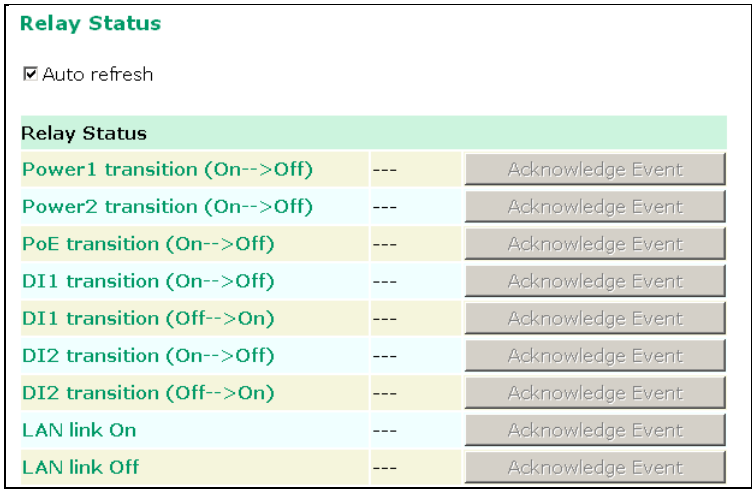
Triggered events are recorded in the System Log. You can export the log contents to an available viewer by clicking **Export Log**. You can use the **Clear Log** button to clear the log contents and the **Refresh** button to refresh the log. **NOTE: The System Log only stores the latest 1000 entries.**



Relay Status

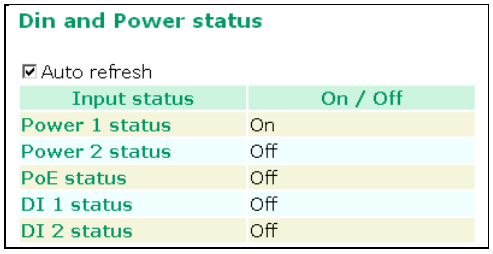
The status of user-configurable events can be found under **Relay Status**. The status will refresh every 5 seconds if the **Auto refresh** box is checked.

If an event is triggered, it will be noted on this list. The system administrator can click **Acknowledge Event** after the event has been acknowledged and addressed.



DI and Power Status

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

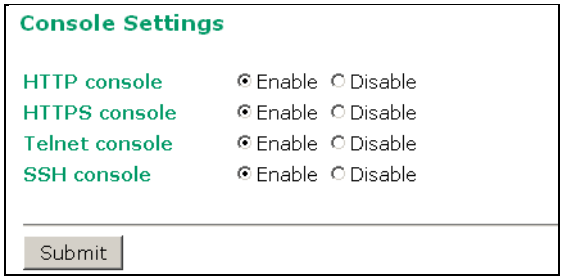


Maintenance

Maintenance functions provide the administrator with tools to manage the AWK-3191 and wired/wireless networks.

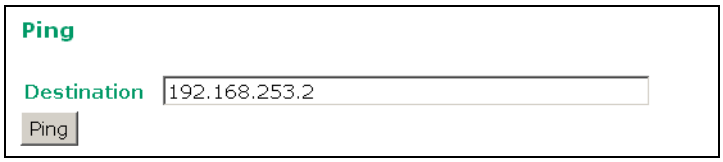
Console Settings

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

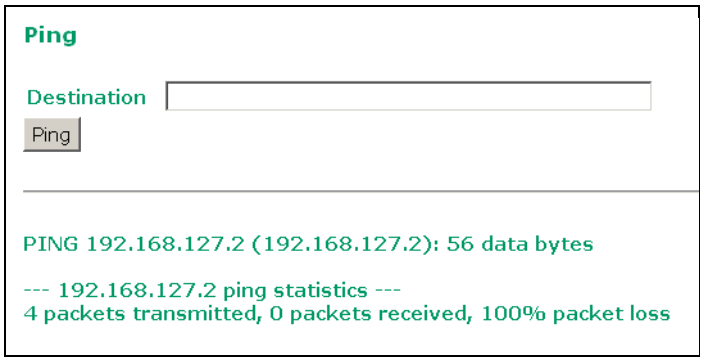


Ping

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



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

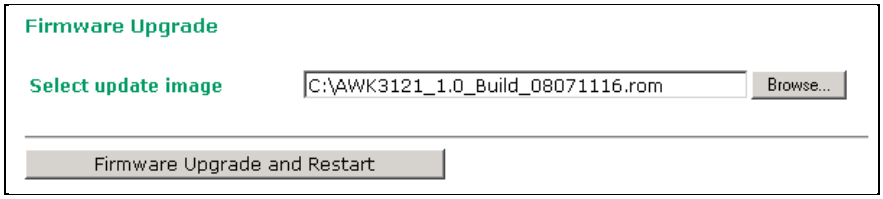


Firmware Upgrade

The AWK-3191 can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available from Moxa's download center.

Before running a firmware upgrade, make sure the AWK-3191 is offline. 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-3191 will reboot itself.

When upgrading your firmware, the AWK-3191's other functions are deactivated.



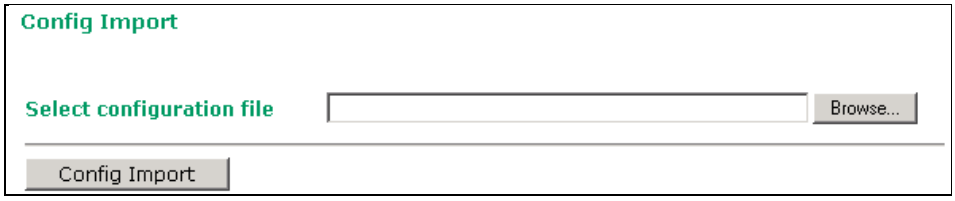
ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your AWK-3191.

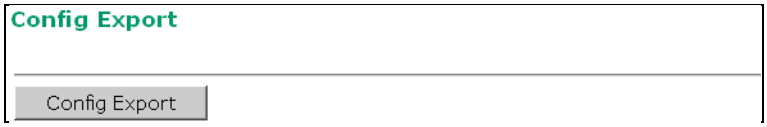
Config Import/Export

You can back up or restore the AWK-3191's configuration with **Config Import/Export**.

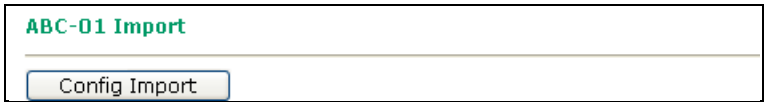
In the **Config Import** section, click **Browse** to specify the configuration file and click the **Config Import** button to begin importing the configuration.

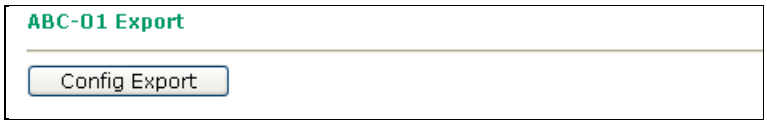


In the **Config Export** section, click the **Config Export** button and save the configuration file to your local storage media. The configuration file is a text file and you can view and edit it with a general text-editing tool.



You can also back up or restore the ABC-01 (HW Rev. 1.1 support only) configuration with **Config Import/Export**.



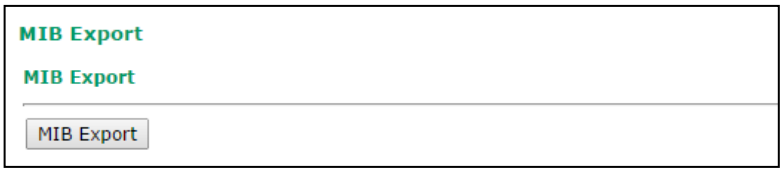


To download the configuration to the AWK:

1. Turn off the AWK.
2. Plug the ABC-01 into the AWK's RS-232 console port.
3. Turn on the AWK.
4. The 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 has been downloaded, and if the configuration format is correct, the AWK will emit three short beeps, and then continue the boot up process.
5. Once the AWK has booted up successfully, it will emit the usual two beeps, and the ready LED will turn to a solid green color.

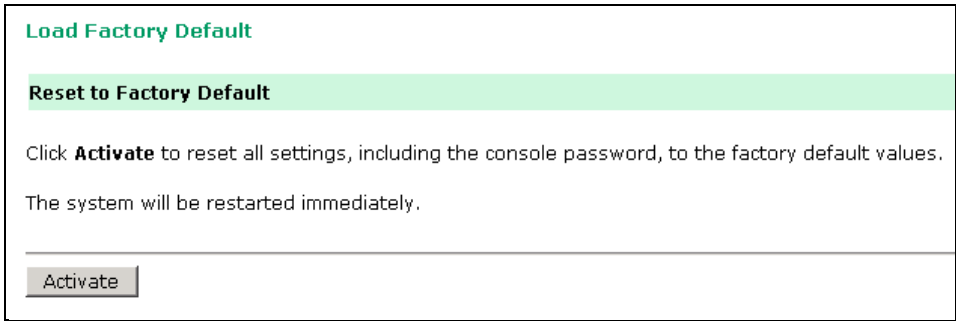
MIB Export

Use this function to export the MIB library for SNMP communication. After enabling the SNMP agent, you can use SNMP to communicate with the device. For details of the node corresponding to each function, refer to the exported MIB library.



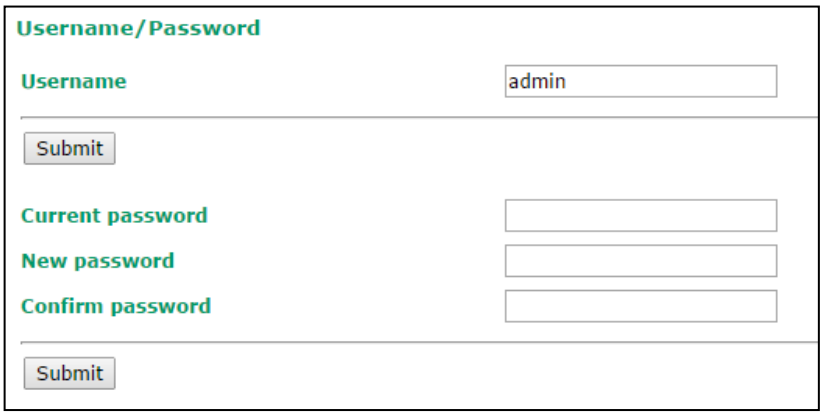
Load Factory Default

Use this function to reset the AWK-3191 and roll all settings back to the factory default values. You can also reset the hardware by pressing the reset button on the top panel of the AWK-3191.



Username/Password

You can change the administration username and password for each of the AWK-3191's console managers by using the **Username/Password** function. Before you set up a new password, you must input the current password and reenter the new password for confirmation. For security reasons, do not use the default password ***root***, and remember to change the administration password regularly.



Misc. Settings

Additional settings to help you manage your AWK-3191 are available on this page.

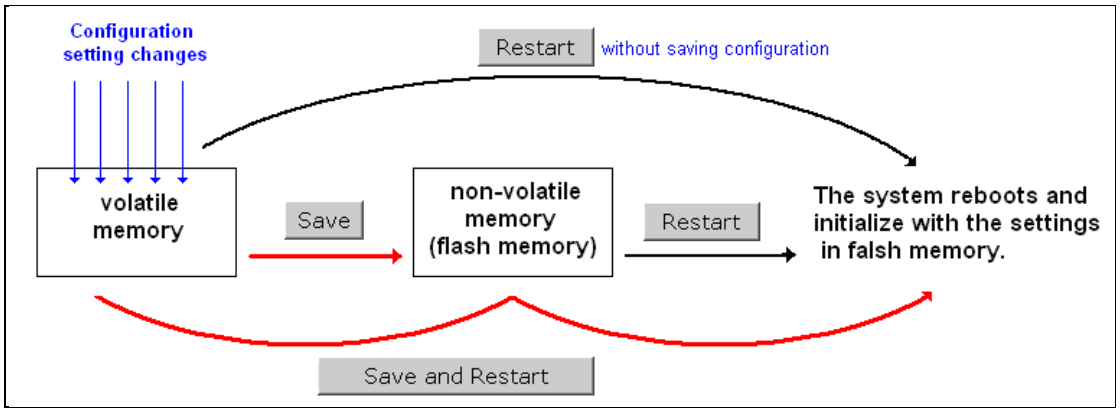
Reset button

Setting	Description	Factory Default
Always enable	The AWK-3191's Reset button works normally.	Always enable
Disable after 60 sec	The AWK-3191's reset to default function will be inactive 60 seconds after the AWK-3191 finishes booting up.	

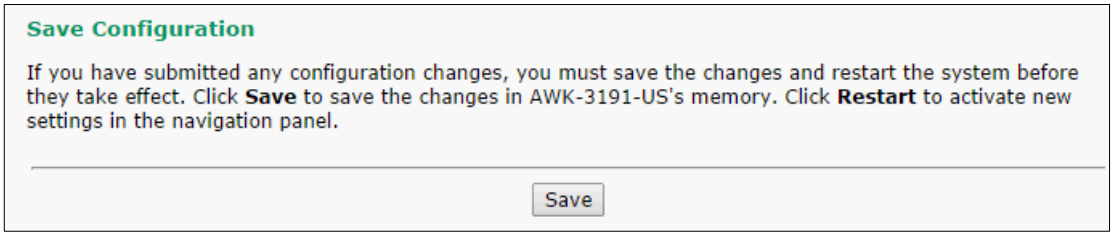
Save Configuration

The following figure shows how the AWK-3191 stores configuration changes to volatile and non-volatile memory. All data stored in volatile memory will disappear when the AWK-3191 is shut down or rebooted, unless the data is first saved to non-volatile memory. Because the AWK-3191 starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the AWK-3191.

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



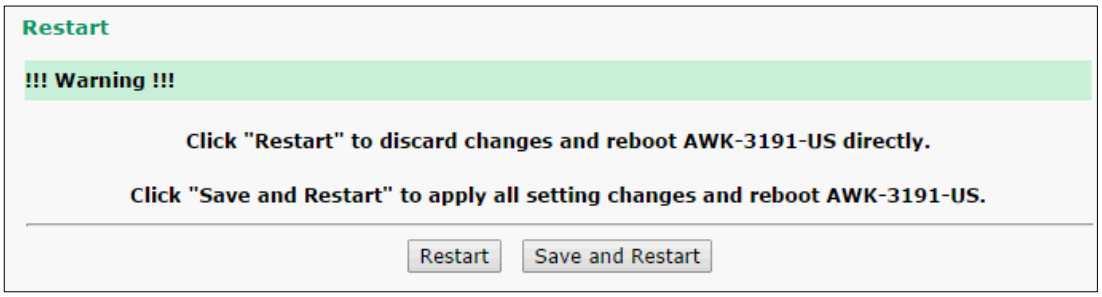
After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However,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



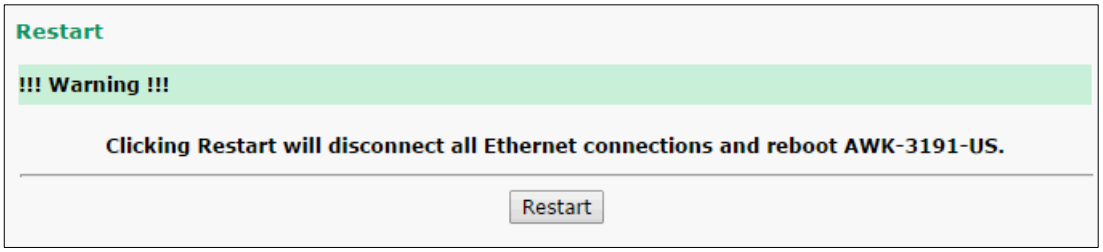
Restart

After you submit configuration changes, you should see a blinking message in the upper right corner of the screen. After making all your changes, click the **Restart** function in the left menu box. One of two different screens will appear.

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the AWK-3191 directly, and all configuration changes will be ignored. Clicking the **Save and Restart** button will apply all configuration changes and then reboot the AWK-3191.



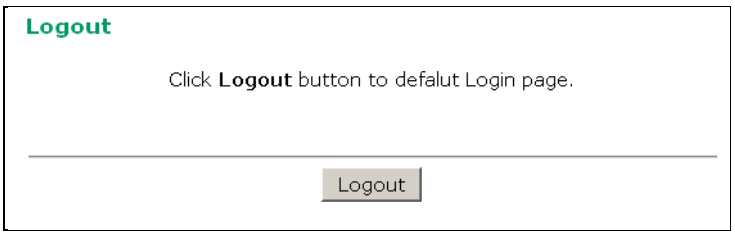
If you run the **Restart** function without changing any configurations or saving all your changes, you will see just one **Restart** button on your screen.



You will not be able to run any of the AWK-3191'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 that you log out before quitting the console manager.



4

Software Installation and Configuration

The following topics are covered in this chapter:

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

Overview

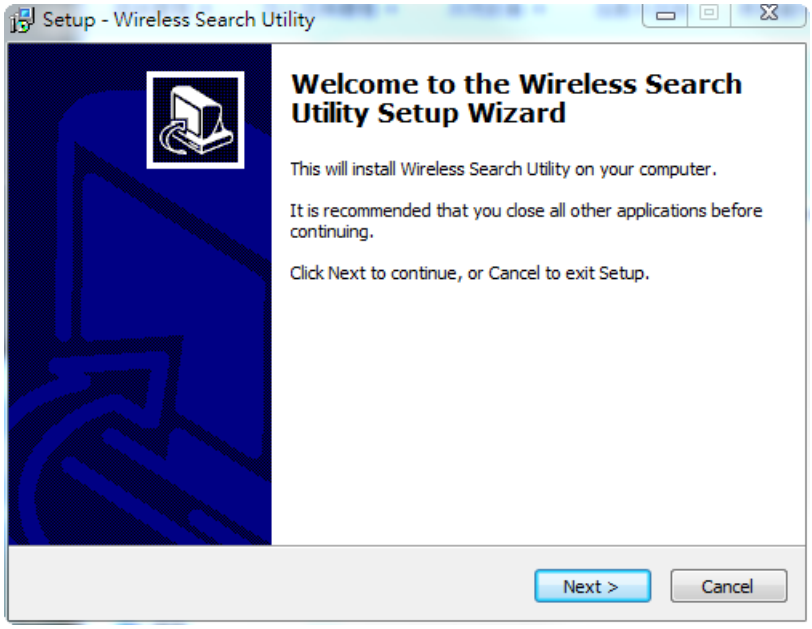
The Wireless Search Utility can be downloaded from the Moxa website at www.moxa.com.

Wireless Search Utility

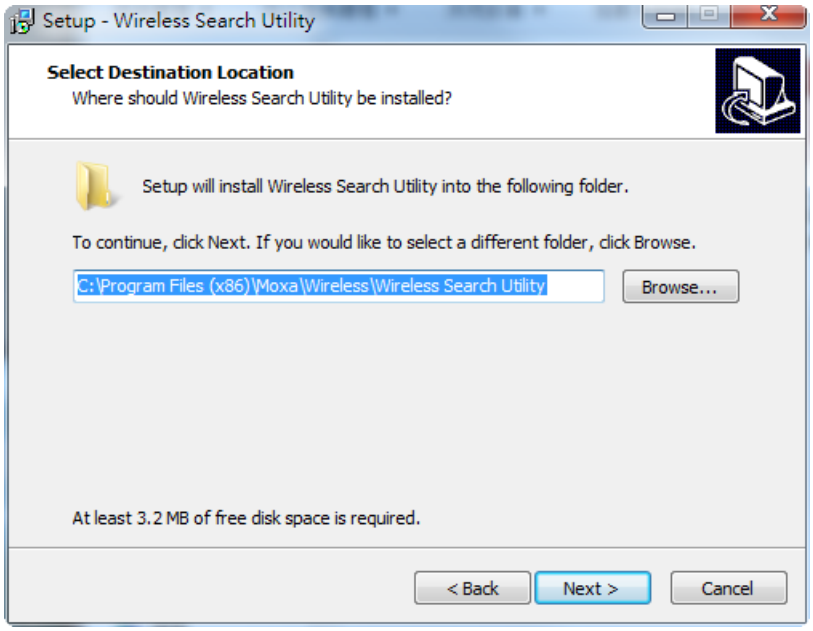
Installing Wireless Search Utility

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

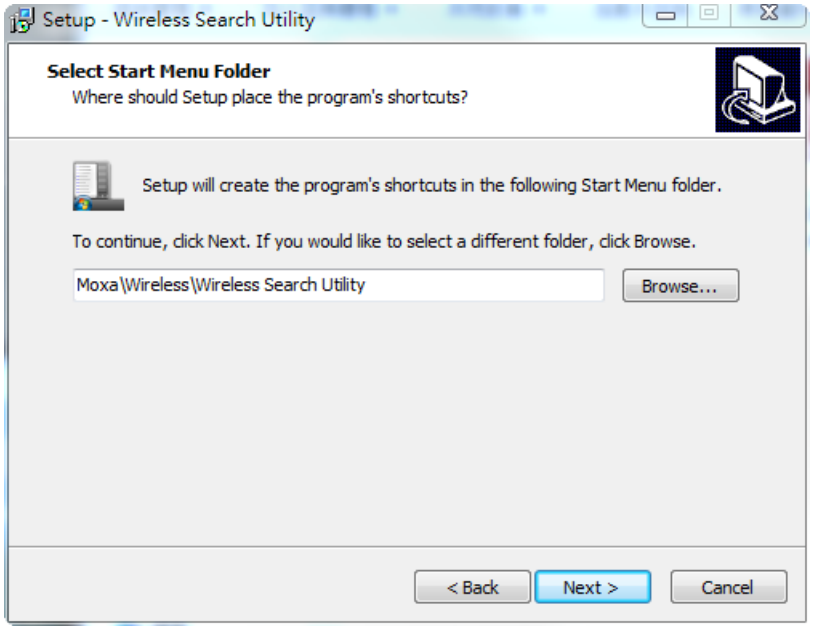
1. Click **Next** on the **Welcome** screen that opens to proceed with the installation.



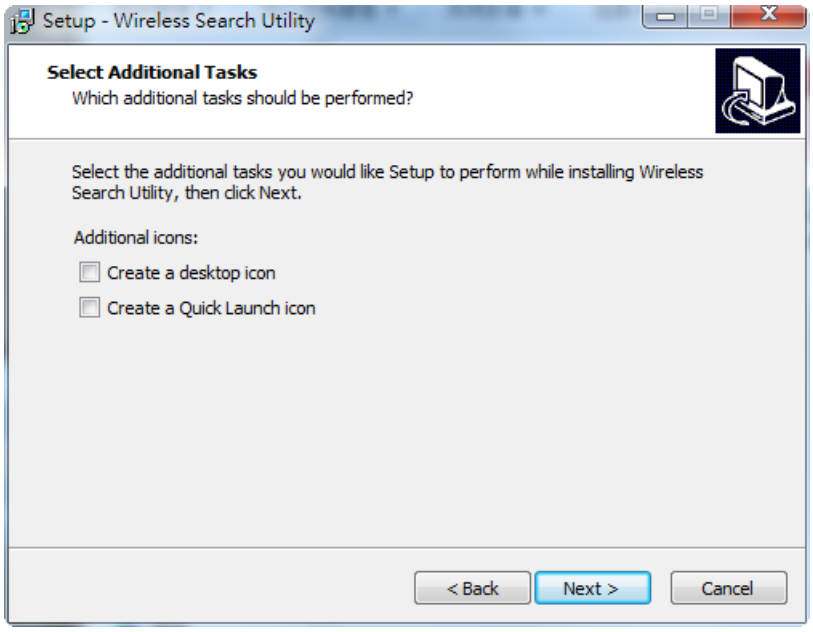
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



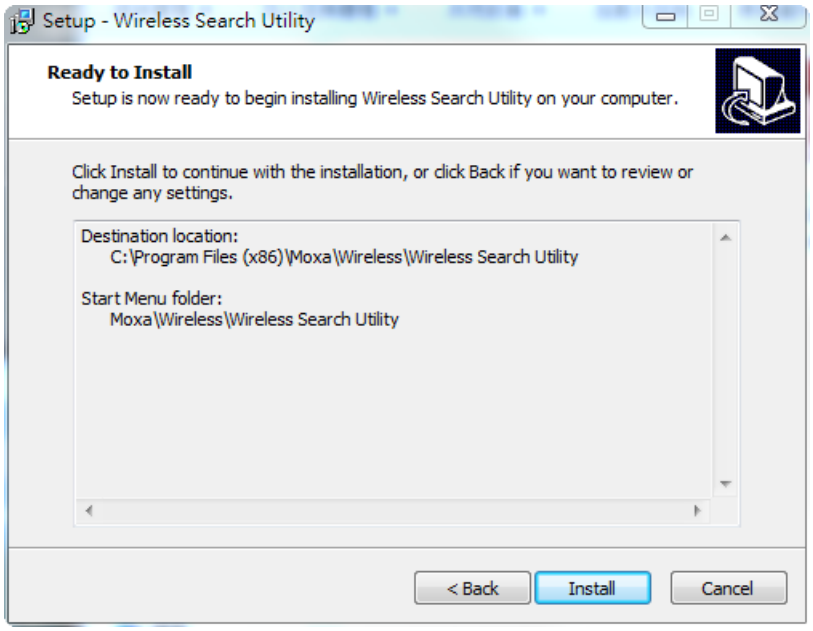
3. Click **Next** to create the program's shortcut files in the default directory, or click **Browse** to select an alternate location.



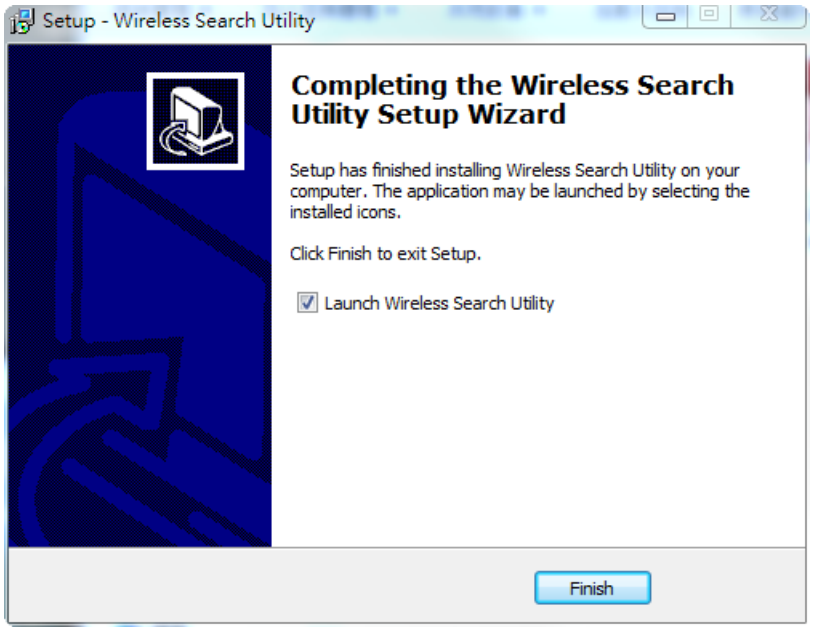
4. Click **Next** to select additional tasks.



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



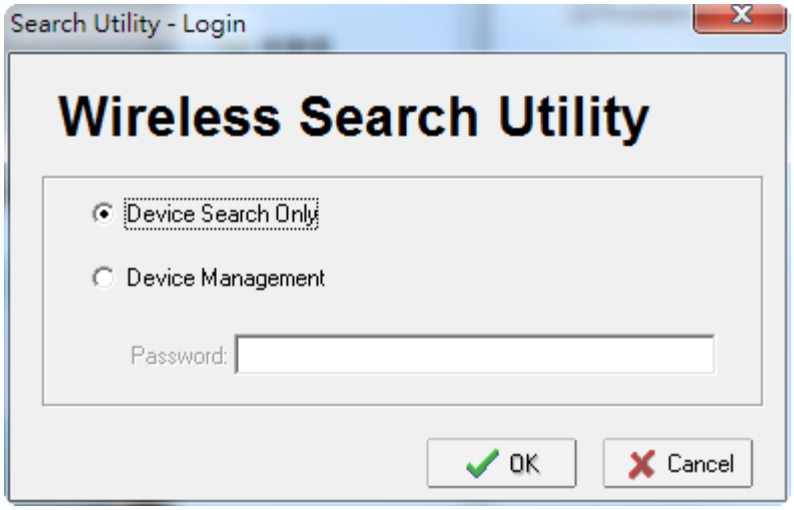
6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.
7. Click **Finish** to complete the installation of the Wireless Search Utility.



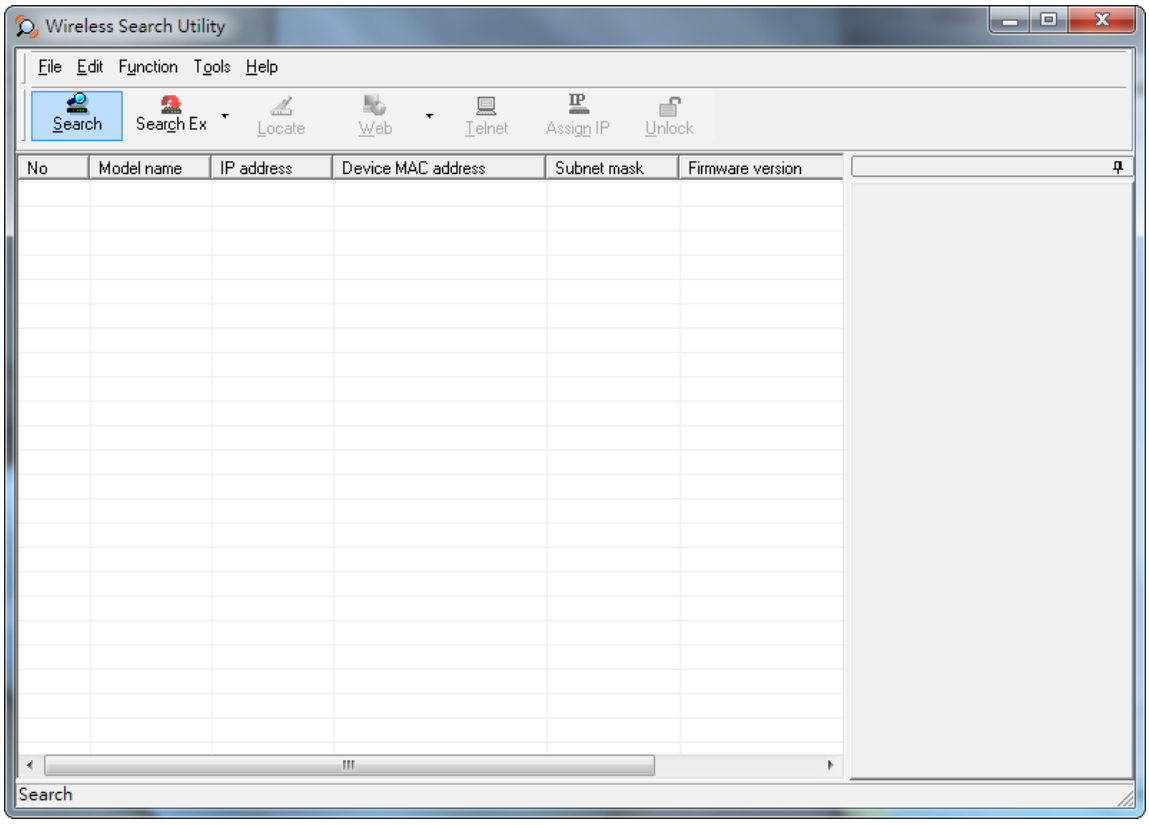
Configuring the Wireless Search Utility

The Broadcast Search function is used to locate all AWK-3191 APs that are connected to the same LAN as your computer. After locating an AWK-3191, 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-3191 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 is displayed, select the **Device Search Only** option to search for AWKs and to view each AWK's configuration. Select the **Device Management** option to assign IPs, upgrade firmware, and locate devices.

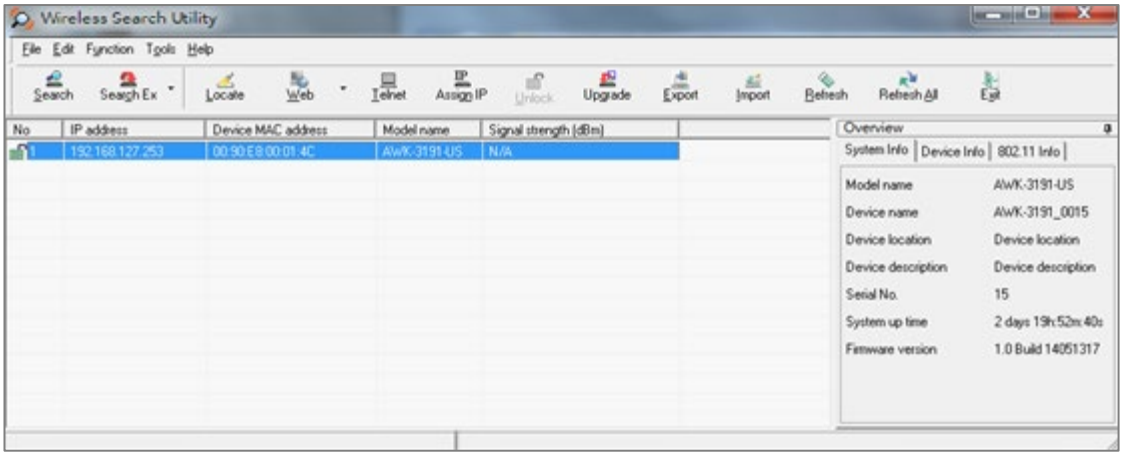


2. Open the Wireless Search Utility and then click the **Search** icon.

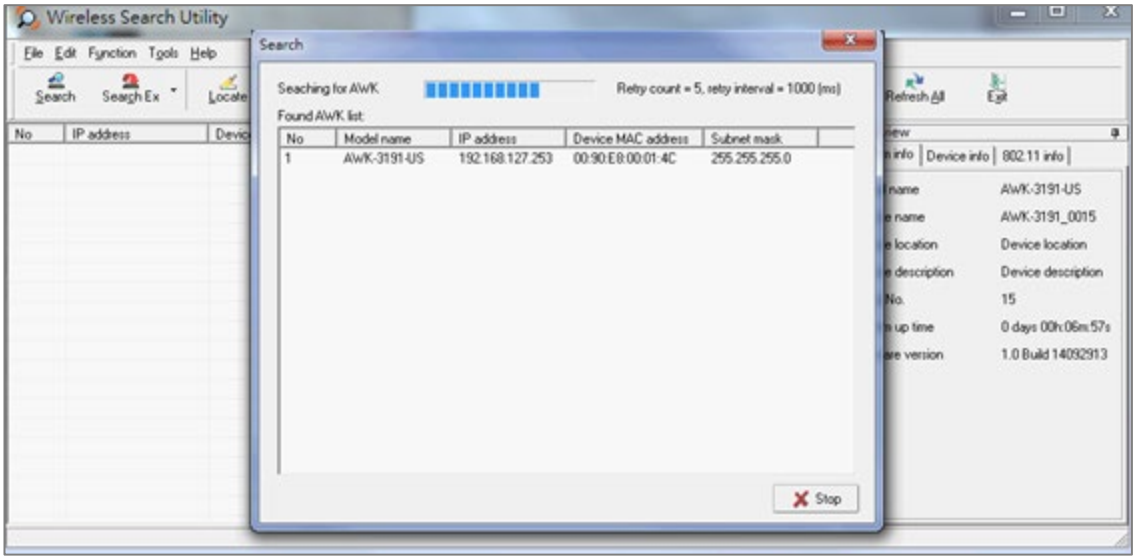


The **Searching** window indicates the progress of the search.

3. When the search is complete, all AWKs that were located will be displayed in the **Wireless Search Utility** window.

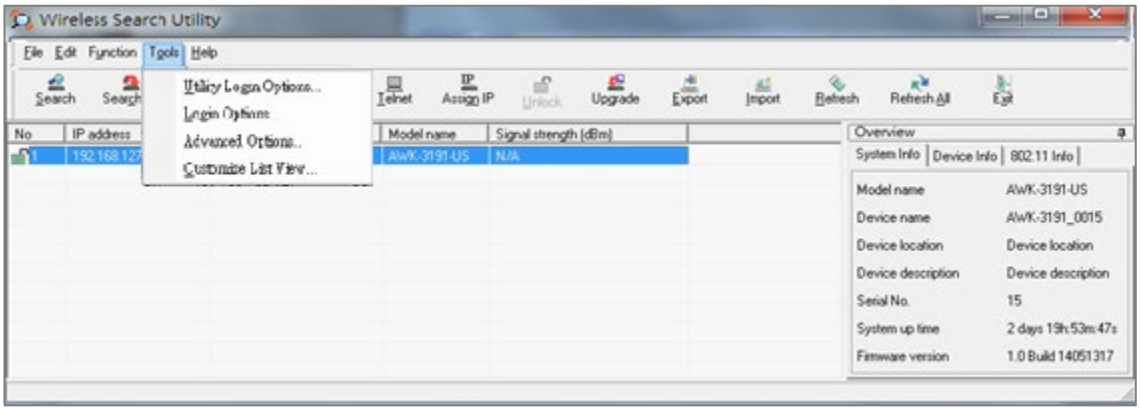


4. Click **Locate** to cause the selected device to beep.



Make sure your AWK is **unlocked** before using the search utility function buttons (Locate, Assign IP, etc.). The AWK will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.

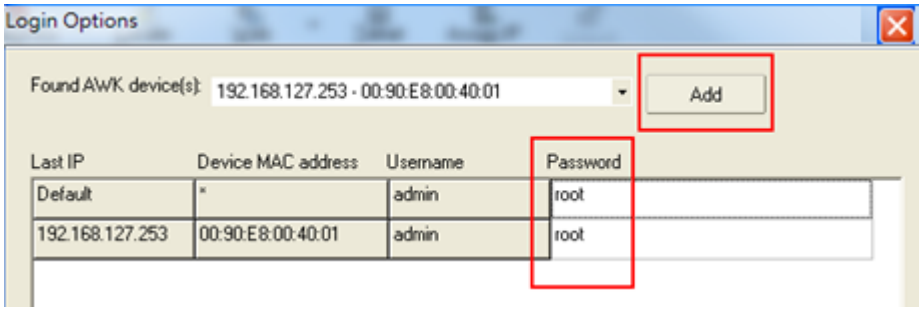
Go to **Tools → Login Options** to manage and unlock additional AWKs.



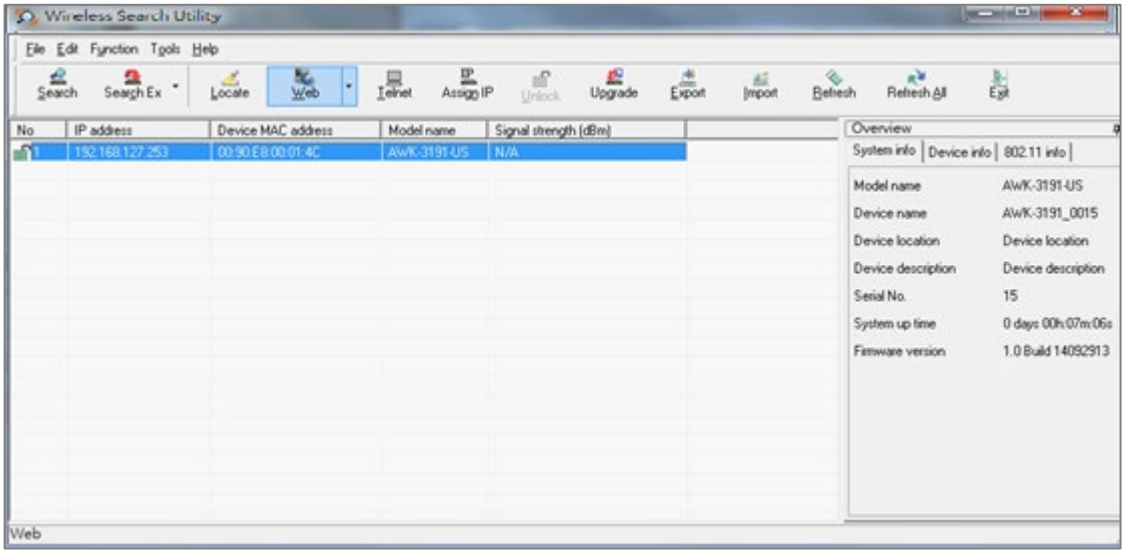
Use the scroll down list to select the MAC addresses of those AWKs you would like to manage, and then click **Add**. Key in the password for the AWK device and then click **OK** to save. If you return to the search page and search for the AWK again, you will find that the AWK is automatically unlocked.

ATTENTION

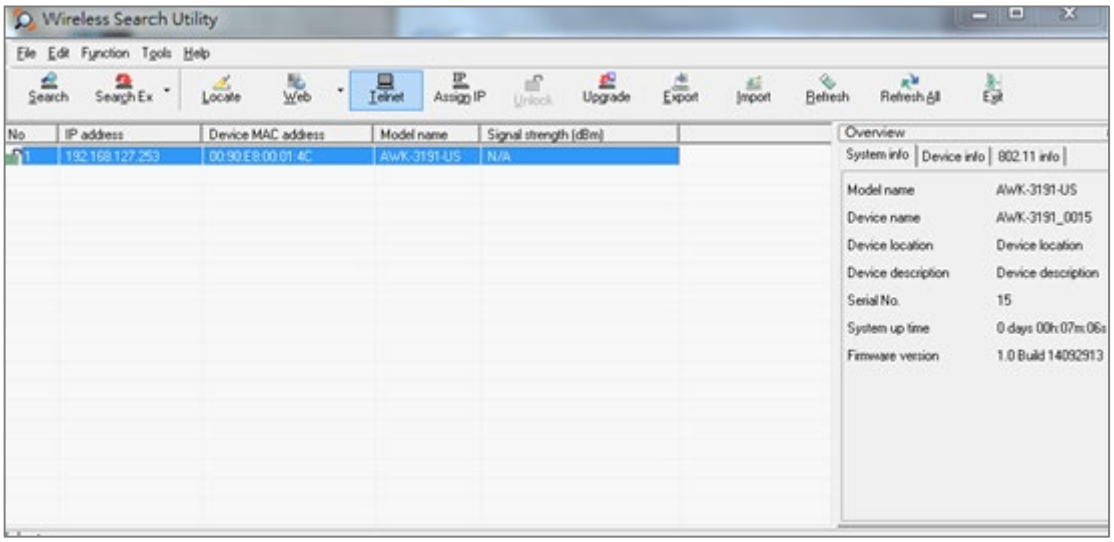
For security reasons, be sure to change the Wireless Search Utility login password instead of using the default.



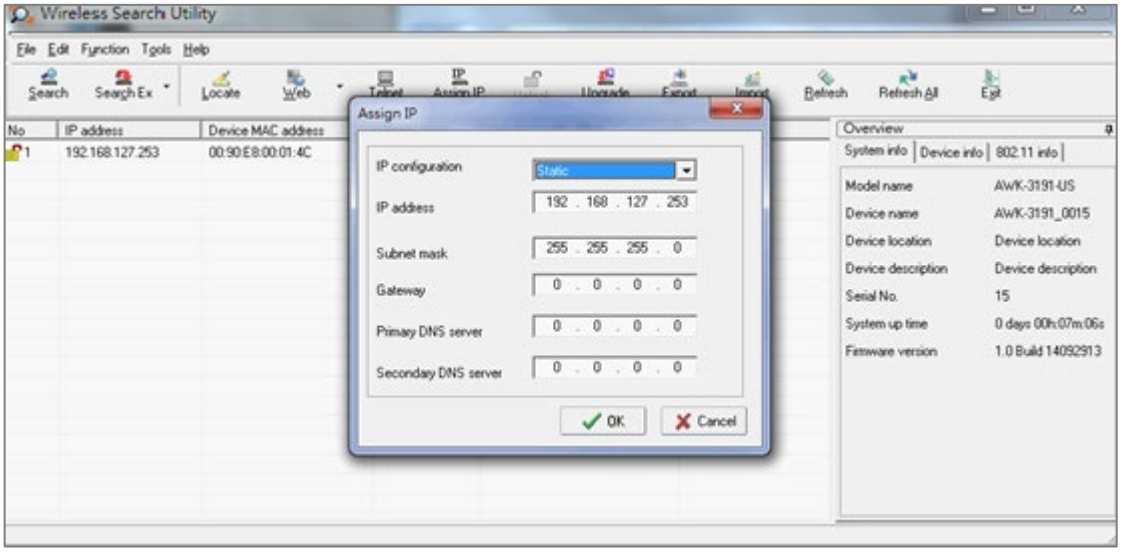
To modify the configuration of the highlighted AWK, click on the Web icon to open the web console. Refer to Chapter 3, "Using the Web Console," for information on how to use the web console.



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



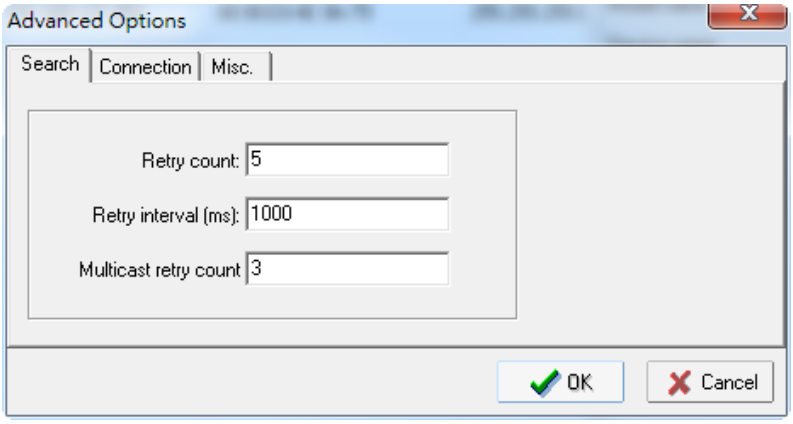
Click **Assign IP** to change the IP setting.



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

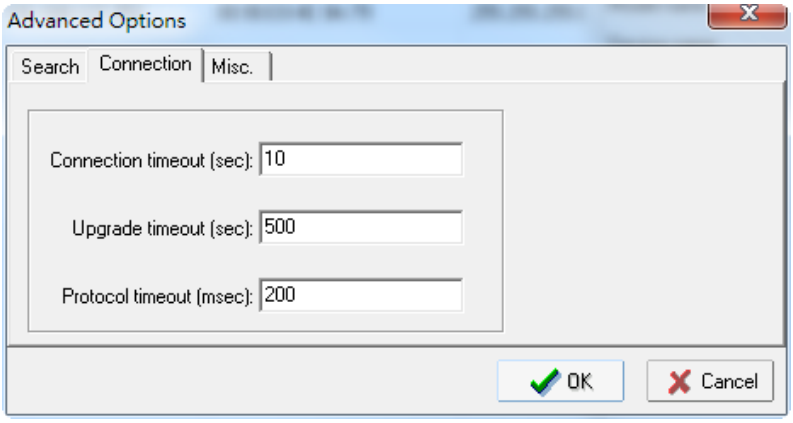
Search

- **Retry count (default=5):** Indicates the number of times the search will be automatically retried.
- **Retry interval (ms):** Specifies the interval between retries.



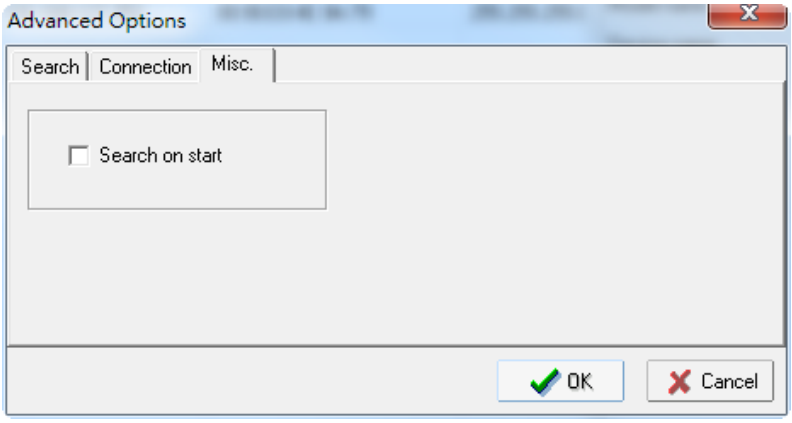
Connection

- **Connection timeout (secs):** Sets the waiting time for the **Default Login**, **Locate**, **Assign IP**, **Upload Firmware**, and **Unlock** actions to complete.
- **Upgrade timeout (secs):** Sets the waiting time for a firmware upgrade before a connection is disconnected, which is the waiting time for the firmware to be written to flash.



Misc.

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



5

Other Console Considerations

This chapter explains how to access the AWK-3191 for the first time. In addition to HTTP access, there are four ways to access AWK-3191: 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-3191 to a PC's COM port, can be used if you do not know the AWK-3191's IP address. The other consoles can be used to access the AWK-3191 over an Ethernet LAN, or over the Internet.

The following topics are covered in this chapter:

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

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

The serial console connection method, which requires using a short serial cable to connect the AWK-3191 to a PC's COM port, can be used if you do not know the AWK-3191's IP address. It is also convenient to use serial console configurations when you cannot access the AWK-3191 over an Ethernet LAN, such as when the LAN cable is disconnected or the LAN is hit by a broadcast storm.

ATTENTION

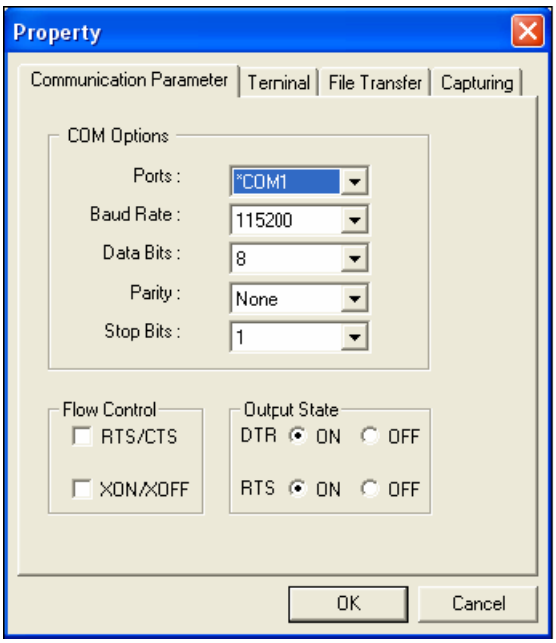
Do not use the RS-232 console manager when the AWK-3191 is powered using reverse voltage (e.g., -48 VDC), even though reverse voltage protection is supported. If you need to connect the RS-232 console using reverse voltage, we suggest using Moxa's TCC-82 isolator.

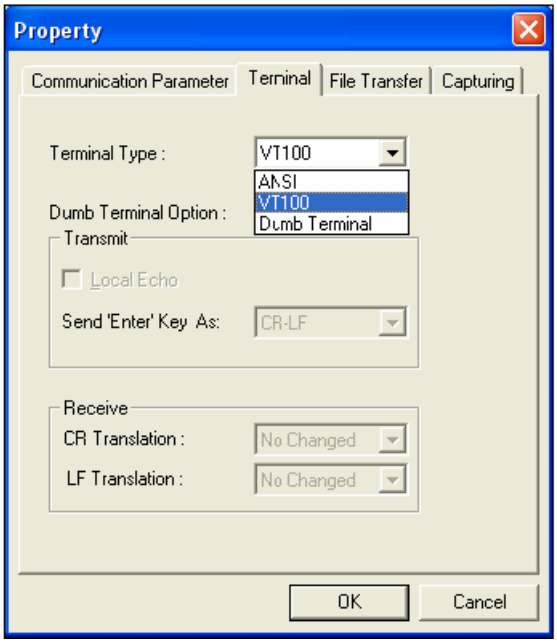
NOTE We recommend using **Moxa PComm (Lite)** Terminal Emulator, which can be downloaded free of charge from Moxa's website.

Before running PComm Terminal Emulator, use an RJ45 to DB9-F (or RJ45 to DB25-F) cable to connect the AWK-3191's RS-232 console port to your PC's COM port (generally COM1 or COM2, depending on how your system is set up). After installing PComm Terminal Emulator, take the following steps to access the RS-232 console utility.

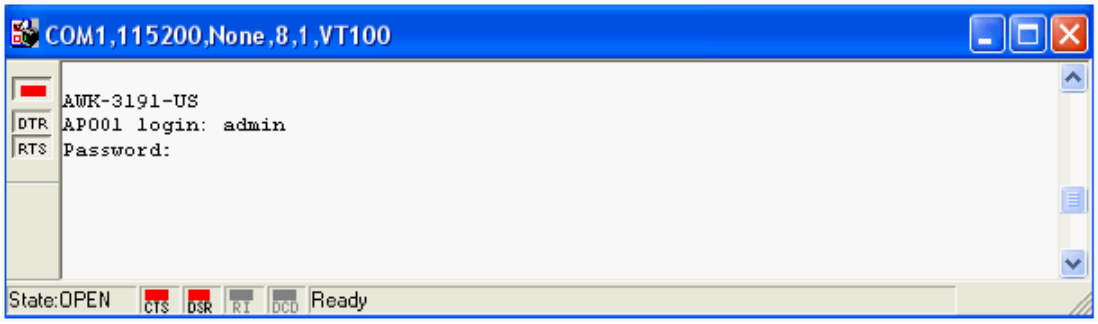
1. From the Windows desktop, open the Start menu and start **PComm Terminal Emulator** in the PComm (Lite) group.
2. Select Open under Port Manager to open a new connection.

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

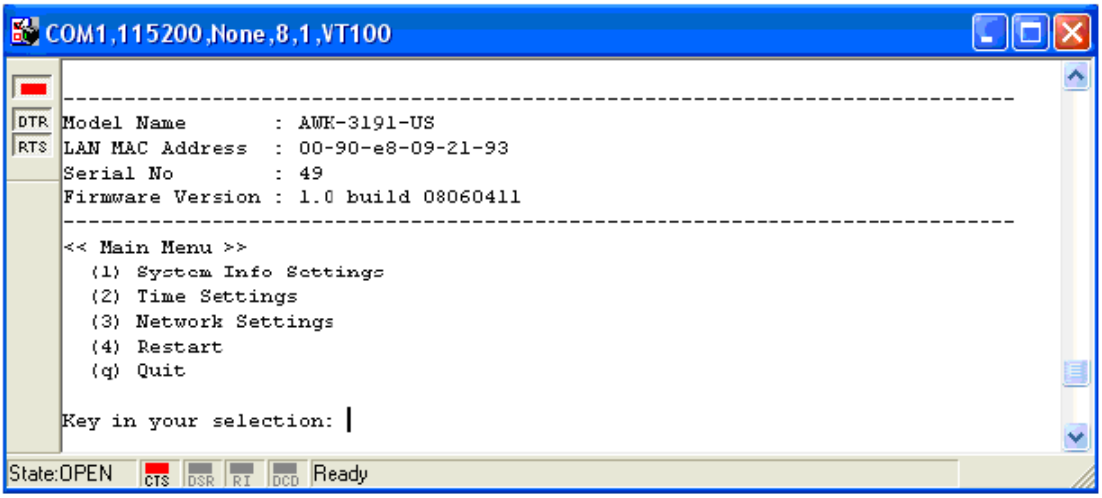




4. The Console login screen will appear. Log in to the RS-232 console with the login name (default: **admin**) and password (default: **root**, if a new password has not been set).



5. The AWK-3191's device information and Main Menu will be displayed. Follow the description displayed on the screen and select the administration option you wish to perform.



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

ATTENTION

If you unplug the RS-232 cable or trigger **DTR**, a disconnection event will be evoked to enforce logout for network security. You will need to log in again to resume operation.

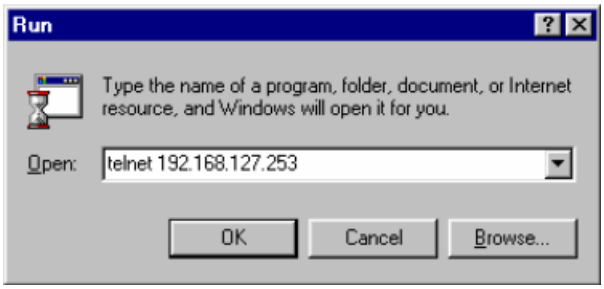
Configuration by Telnet and SSH Consoles

You may use Telnet or SSH client to access the AWK-3191 and manage the console over a network. To access the AWK-3191's functions over the network from a PC host that is connected to the same LAN as the AWK-3191, you need to make sure that the PC host and the AWK-3191 are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

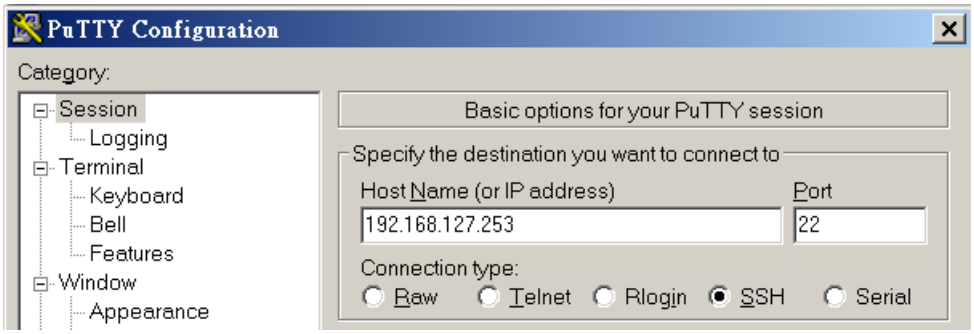
NOTE The AWK-3191's default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

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

1. From Windows Desktop, click **Start → Run**, and then use Telnet to access the AWK-3191's IP address from the Windows Run window (you may also issue the Telnet command from the MS-DOS prompt).



2. When using SSH client (e.g., PuTTY), run the client program (e.g., putty.exe) and then input the AWK-3191's IP address, specifying **22** for the SSH connection port.

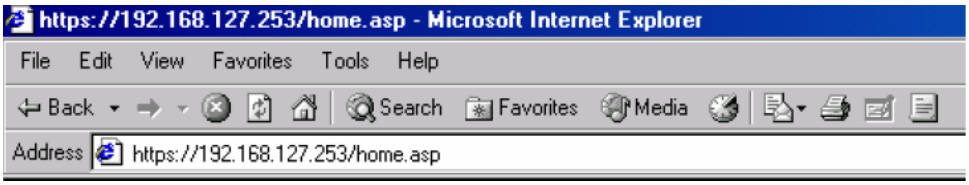


3. The Console login screen will appear. Refer to the previous section, "RS-232 Console Configuration," for login and administration information.

Configuration by Web Browser with HTTPS/SSL

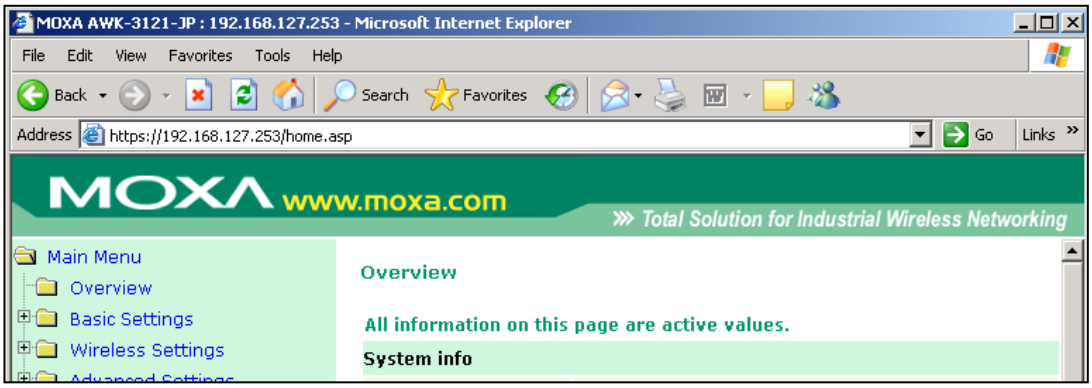
To secure your HTTP access, the AWK-3191 supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the AWK-3191's web browser interface via HTTPS/SSL.

1. Open your web browser and type https://<AWK-3191's IP address> in the address field. Press **Enter** to establish the connection.



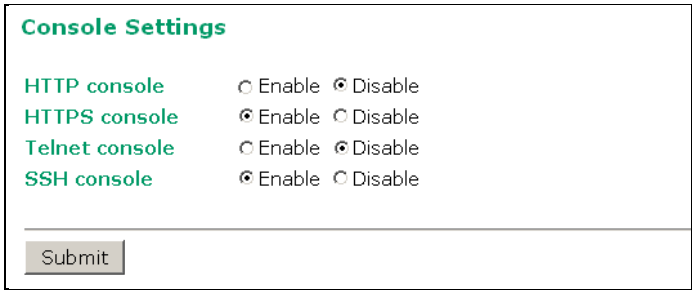
2. Warning messages will pop out to warn users that the security certificate was issued by a company they have not chosen to trust.

3. Select **Yes** to accept the certificate issued by Moxa IW and then enter the AWK-3191's web browser interface, secured via HTTPS/SSL. The secure **https** protocol should be visible in the URL. Next, use the tree menu on the left side of the window to open the function pages for accessing each of the AWK-3191's functions.



Disabling Telnet and Browser Access

If you are connecting the AWK-3191 to a public network, but do not intend to use its management functions over the network, then we suggest disabling both the Telnet Console and Web Configuration. Click **Maintenance → Console Settings** to disable them, as shown in the following screenshot.



A

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your AWK-3191s and plan your industrial wireless network better.

The following topics are covered in this appendix:

- **Beacon**
- **DTIM**
- **Fragment**
- **RTS Threshold**

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 the 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

The RTS Threshold (256-2346) defines the size a packet must be before it triggers the RTS/CTS mechanism. RTS/CTS (Request to Send / Clear to Send) is an optional mechanism used by the 802.11 wireless networking protocol to reduce frame collisions introduced by the hidden node problem.

B

Supporting Information

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

The following topics are covered in this appendix:

- **About this User's Manual**
- **DoC (Declaration of Conformity)**
  - Federal Communications Commission Interference Statement
  - R&TTE Compliance Statement
- **Firmware Recovery**

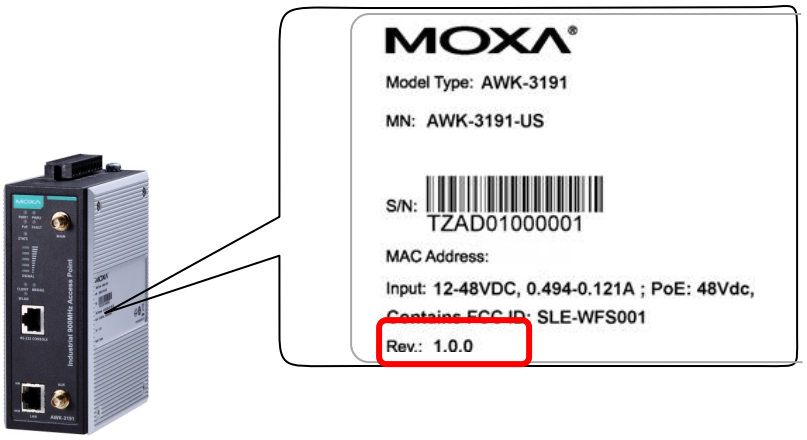
About this User's Manual

This manual is mainly designed for, but not limited to, the following hardware and firmware for the AWK-3191:

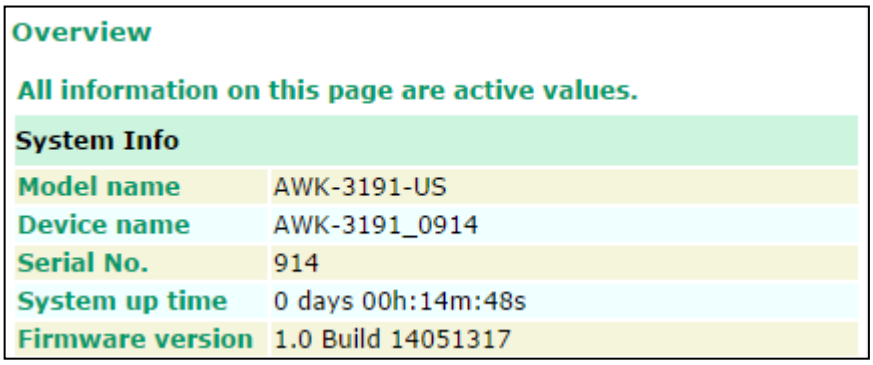
- Hardware Revision: **1.0.0**
- Firmware Version: **1.0**

We strongly recommend visiting Moxa's website (http://www.moxa.com) to download the latest product datasheet, firmware, QIG (Quick Installation Guide), UM (User's Manual), and related information.

NOTE The AWK-3191's hardware revision number is located on the side label.



The firmware version number can be found on the Overview page, as shown below:



DoC (Declaration of Conformity)

Federal Communications Commission Interference Statement

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

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: To assure continued compliance, use only shielded interface cables when connecting to a 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 and 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.

NOTE The availability of some specific channels and/or operational frequency bands are country dependent and are programmed into the firmware at the factory to comply with the regulations for the intended destination. These firmware settings cannot be accessed or changed by the end-user.

R&TTE Compliance Statement

Moxa declares that the apparatus AWK-3191 complies with the essential requirements and other relevant provisions of Directive 1999/5/EC.

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE).

The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

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 safety guidelines of the computer manufacturer must therefore be followed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

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

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

EU Countries Not Intended for Use

None.

Potential Restrictive Use

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

Firmware Recovery

When the **FAULT**, **Signal Strength**, **CLIENT**, **BRIDGE**, and **WLAN** LEDs all light up simultaneously and blink at one-second intervals, system boot up has failed. The failure may be due to improper usage of the AWK-3191, or to factors beyond the control of the user, such as an unexpected shutdown during a firmware update. The AWK-3191 is designed to help administrators recover from such situations and resume system operation rapidly. Refer to the following instructions to recover the firmware:

Connect to the AWK-3191's ES-232 console with **115200bps and N-8-1**. The following message will be shown on the terminal emulator every second:

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

Press **Ctrl-C**. The following message will appear:

```
Press Ctrl-C to enter Firmware Recovering Process........
==============================================================================
IP address of AWK-3121 : 0.0.0.0
IP address of TFTP server : 0.0.0.0
==============================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 
```

Enter **2** to change the network setting. Specify where the AWK-3191's firmware file is located on the TFTP server and press **y** to write the settings to flash memory.

```
==============================================================================
IP address of AWK-3121 : 0.0.0.0
IP address of TFTP server : 0.0.0.0
==============================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 2

IP address of AWK-3121 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
Update RedBoot non-volatile configuration - continue (y/n)? y
```

When the AWK-3191 restarts, the message "Press Ctrl-C to enter Firmware Recovery Process…" will reappear. Press **Ctrl-C** to display the menu, and select **1** to start the firmware upgrade process.

```
Press Ctrl-C to enter Firmware Recovering Process........
==============================================================================
IP address of AWK-3121 : 192.168.1.2
IP address of TFTP server : 192.168.1.1
==============================================================================
1. Start to firmware upgrade using the above network setting immediately.
2. Change the network settings.
Enter your selection :  (1-2,enter for abort): 1
```

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

```
==============================================================================
Load method select :
0. Load from LAN
1. Load from serial with Xmodem
q. Abort select.
==============================================================================
Please select item : 0
Please input load image name..
Default file name : AWK-3121.rom
User Input file name : AWK-3121_1.0.rom
```