AirWorks AWK-1137C User's Manual

Version 5.0, July 2020

www.moxa.com/product

AirWorks AWK-1137C 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

The AWK-1137C industrial a/b/g/n high-speed Wi-Fi clients are ideal wireless solutions for hard-to-wire applications that use mobile equipment connected over a TCP/IP network. The AWK-1137C's standard models can operate at temperatures ranging from 0 to 60°C and wide temperature models can operate in the range-40 to 75°C. The AWK-1137C is rugged enough to operate in harsh industrial environments.

The following topics are covered in this chapter:

- **Overview**
- **Package Checklist**
- **Product Features**
- **Functional Design**
  - LED Indicators
  - Beeper
  - Reset Button

Overview

The AWK-1137C is 802.11n compliant to deliver speed, range, and reliability to support even the most bandwidth-intensive applications. The 802.11n standard incorporates multiple technologies, including Spatial Multiplexing MIMO (Multi-In, Multi-Out), 20 and 40 MHz channels, and dual bands (2.4 GHz and 5 GHz) to provide high speed wireless communication, while still being able to communicate with legacy 802.11a/b/g devices.

AWK-1137C is used to connect RS-232/422/485 serial devices or Ethernet devices to a wireless LAN. The AWK-1137C is a best fit in industrial applications, such as machine built-in design and moving equipment or parts, because of its compact size, 9-30 VDC power input, and dual isolation design.

The AWK's operating temperature ranges from 0 to 60°C for standard models and -40 to 75°C for wide temperature models, and is rugged enough for all types of harsh industrial environments. Installation of the AWK is easy using DIN-rail mounting, wall mounting, or distribution boxes, and with its wide operating temperature range, IP30-rated housing with LED indicators, and DIN-rail/wall mounting, it is a convenient yet reliable solution for all types of industrial wireless applications.

Package Checklist

Before you install the AWK-1137C, verify that the package contains the following items. If any of these items is missing or damaged, please contact your customer service representative for assistance.

- 1 AWK-1137C wireless client
- 2 2.4/5 GHz antennas:ANT-WDB-ARM-0202
- DIN-rail kit
- Quick installation guide (printed)
- Warranty card

NOTE The above items come with the standard AWK-1137C model, but the package contents may vary for customized versions.

Product Features

- IEEE 802.11a/b/g/n compliant
- Advanced wireless security
  - 64-bit and 128-bit WEP/WPA/WPA2
  - SSID Hiding/IEEE 802.1X/RADIUS
  - Packet access control & filtering
- Turbo Roaming enables rapid handover
- Wide -40 to 75°C operating temperature range (-T model)
- DIN-rail or wall mounting
- IP30 protected high-strength metal housing

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

ATTENTION

- The AWK-1137C is NOT a portable mobile device and should be located at least 20 cm away from the human body.
- The AWK-1137C is NOT designed for the general public. A well-trained technician should be enlisted to ensure safe deployment of AWK-1137C units, and to establish a wireless network.

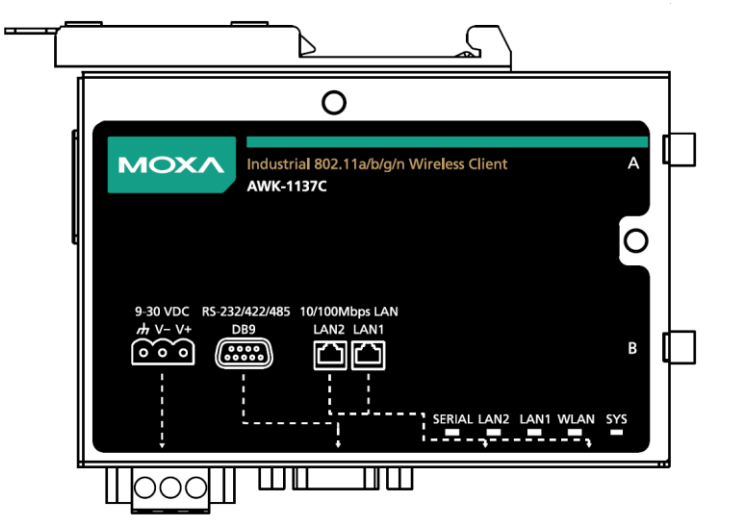
Patent http://www.moxa.com/doc/operations/Moxa_Patent_Marking.pdf

Functional Design

LED Indicators

The LEDs located both on the front and side panel of the AWK-1137C provide a quick and easy means of determining the current operational status and wireless settings.

The **SYS** LED indicates system failures and user-configured events. If the AWK-1137C cannot retrieve the IP address from a DHCP server, the **SYS** LED will blink at one-second intervals.



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 WLAN Setup" section.

LED	Color	State	Description
SYS	Green	On	System start up complete and the system is in operation
		Blinking + Beeps (at 1-sec intervals)	Device has been located by the Wireless Search Utility
	Red	On	System is booting or a system booting error has occurred
		Blinking (at 0.5-sec intervals)	IP address conflict
		Blinking (at 1-sec intervals)	Cannot obtain an IP address from DHCP server
WLAN	Green	On (RSSI > 35)	WLAN interface has connected
		Blinking	Data communication via WLAN
	Amber	On	WLAN interface has connected
		Blinking	Data communication via WLAN

LAN 1	Green	On	Ethernet LAN 1 interface has connected
		Off	Data communication via Ethernet LAN 1
LAN 2	Green	On	Ethernet LAN 2 interface has connected
		Off	Data communication via Ethernet LAN 2
Serial	Amber	Blinking	Data Transmission via serial data port

ATTENTION

- When firmware upgrade fails, the LEDs for **SYS** (Red), **WLAN (**Amber**), LAN1 (**Amber**) and LAN2 (**Amber**)** will light up simultaneously.
- When the system fails to boot, the LEDs for **SYS** (Red) will light up along with the **LAN 1** and **LAN 2** (if there is data traffic passing through the Ethernet interfaces). This may be due to improper operation or issues, such as an unexpected shutdown while updating the firmware. To recover the firmware, refer to the "Firmware Recovery" section in Appendix B.

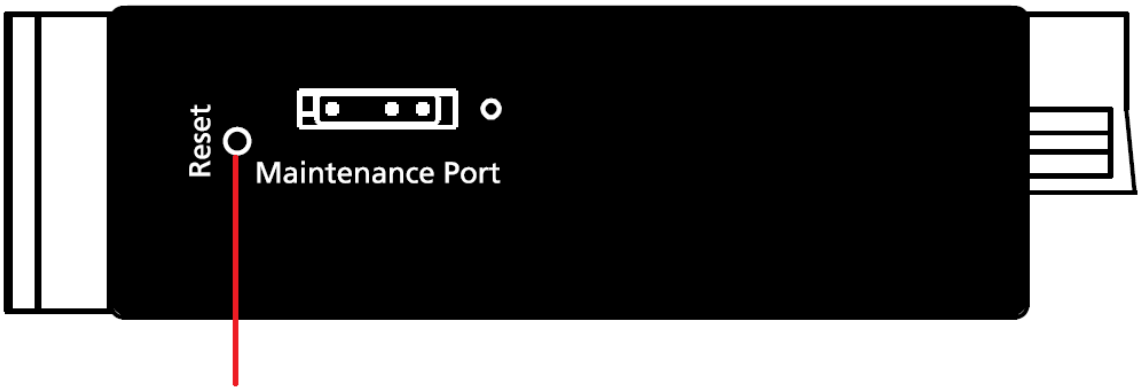
Beeper

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

Reset Button

The **RESET** button is located on the side panel of the AWK-1137C. You can reboot the AWK-1137C 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-1137C.



RESET button

2

Getting Started

This chapter explains how to install Moxa's AirWorks AWK-1137C for the first time, and quickly set up your wireless network and test whether the connection is running well. The Function Map discussed in the third section provides a convenient means of determining which functions you need to use.

The following topics are covered in this chapter:

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

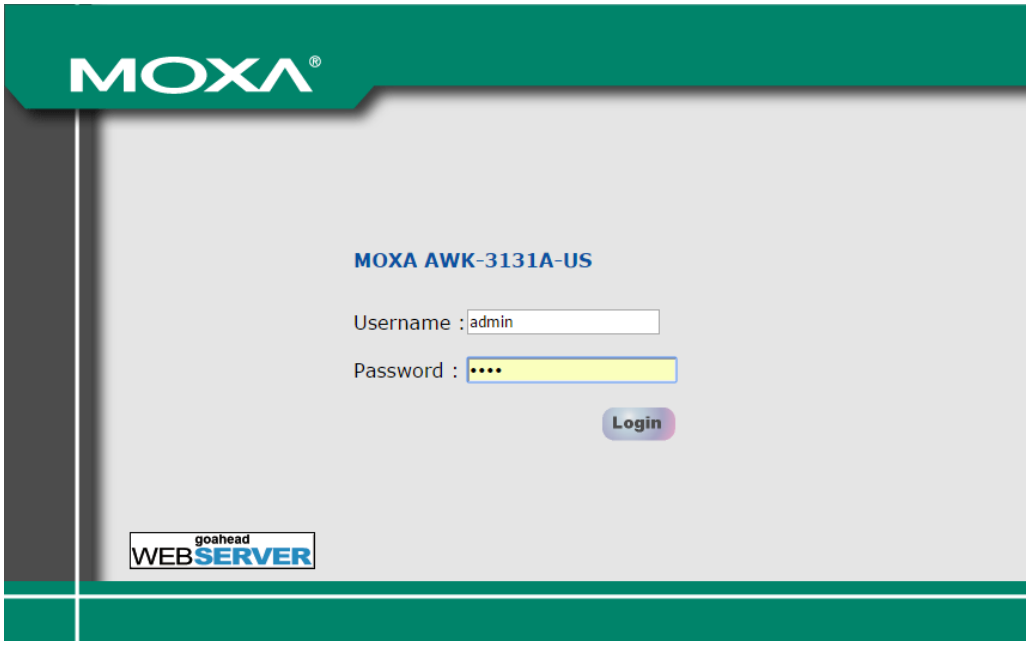
First-time Installation and Configuration

Before installing the AWK-1137C, 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-1137C has a default IP address that must be used when connecting to the device for the first time.

- **Step 1: Connect a power source.**
  The AWK-1137C can be powered by a DC power input.
- **Step 2: Connect the AWK-1137C to a notebook or PC.**
  Since the AWK-1137C supports MDI/MDI-X auto-sensing, you can use either a straight-through cable or crossover cable to connect the AWK-1137C to a computer. The LED indicator on the AWK-1137C'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-1137C. Since the AWK-1137C'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-1137C will be reset to factory default settings and the IP address will be reset to **192.168.127.253**.

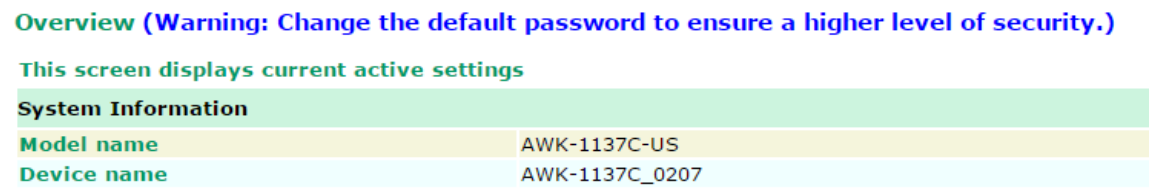
- **Step 4: Use the web-based manager to configure the AWK-1137C**
  Open your computer's web browser and type **http://192.168.127.253** in the address field to access the homepage of the web-based Network Manager. Before the homepage opens, you will need to enter the **Username** and **Password** as shown in the following figure. For first-time configuration, enter the default username and password and then click on the **Login** button.



NOTE Default user name and password:

User Name: **admin**

Password: **moxa**



We strongly recommend changing the default password to ensure higher level of security. To do so, select **Maintenance** → **Password**, and then follow the on-screen instructions to change the password.

NOTE After you click **Submit** to apply changes, the web page will refresh and a **(Updated)** status with a blinking reminder on the upper-right corner of the web page is displayed.

To activate the changes click **Restart** and then **Save and Restart** after you change the settings. About 30 seconds are needed for the AWK-1137C to complete the reboot procedure.

- **Step 5: Select the AWK-1137C operation mode.**
  By default, the AWK-1137C's operation mode is set to client. Detailed information about configuring the AWK-1137C'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.

Testing the Communication

After setting up the AWK-1137C for the first time, you can perform a simple test to make sure that the AWK can establish a wireless connection with an AP and is functioning properly.

In this example, an AWK-1137C is configured as a client on the wireless network.

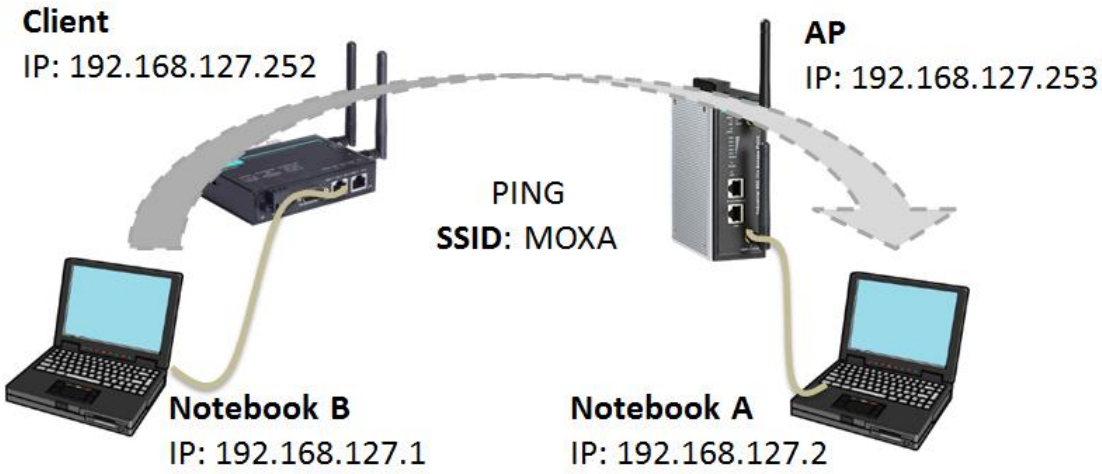
Testing Network Connectivity on AWK-1137C

Connect an AWK-3131A (or another access point) in AP mode to Notebook A. Connect an AWK-1137C to Notebook B. Configure the AWK-1137C and AWK-1137C with the same SSID and set their IP addresses as shown in the following figure:

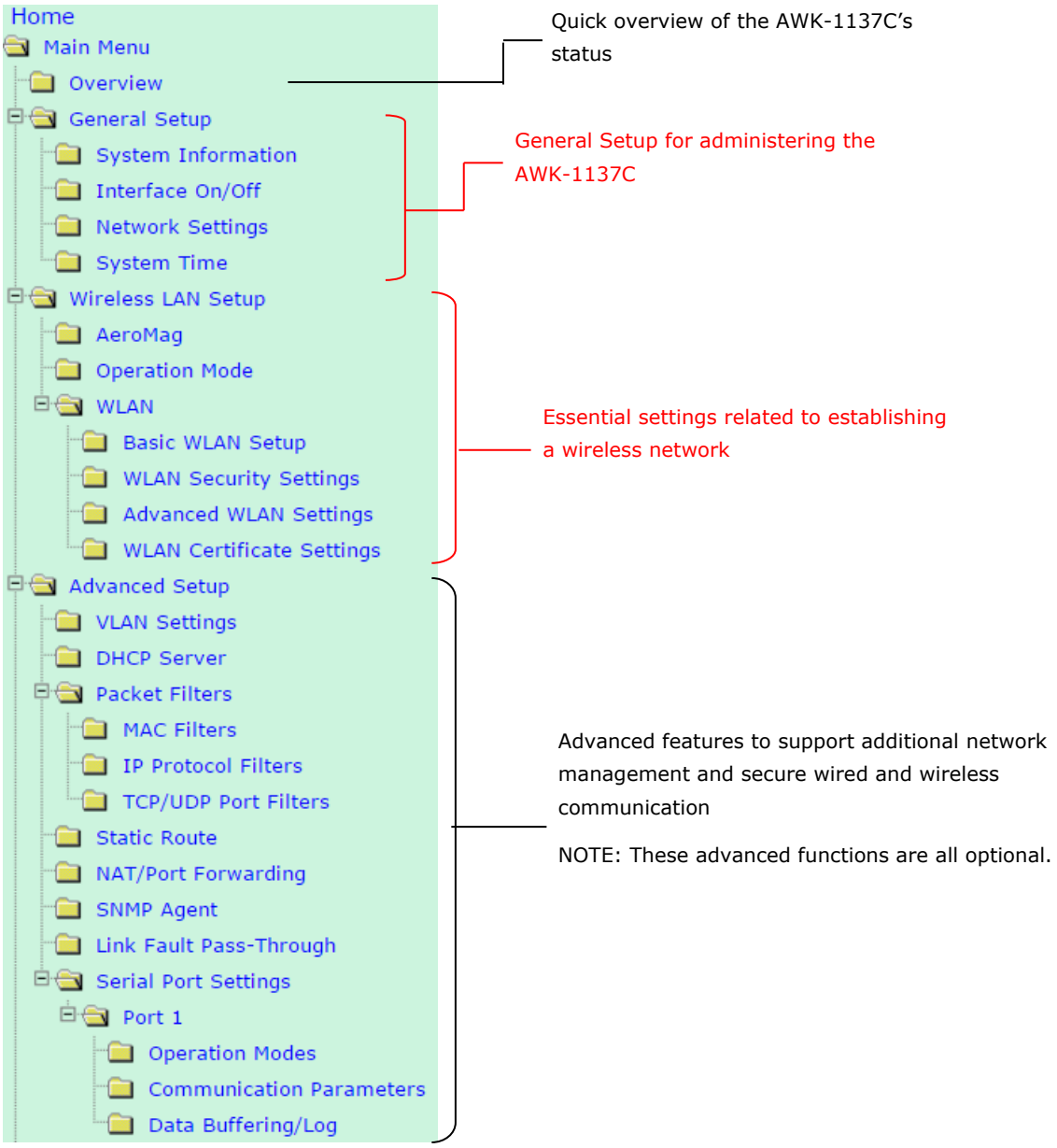
After configuring the WLAN card, establish a wireless connection with the AWK-1137C and open a DOS window on Notebook B. At the prompt, type

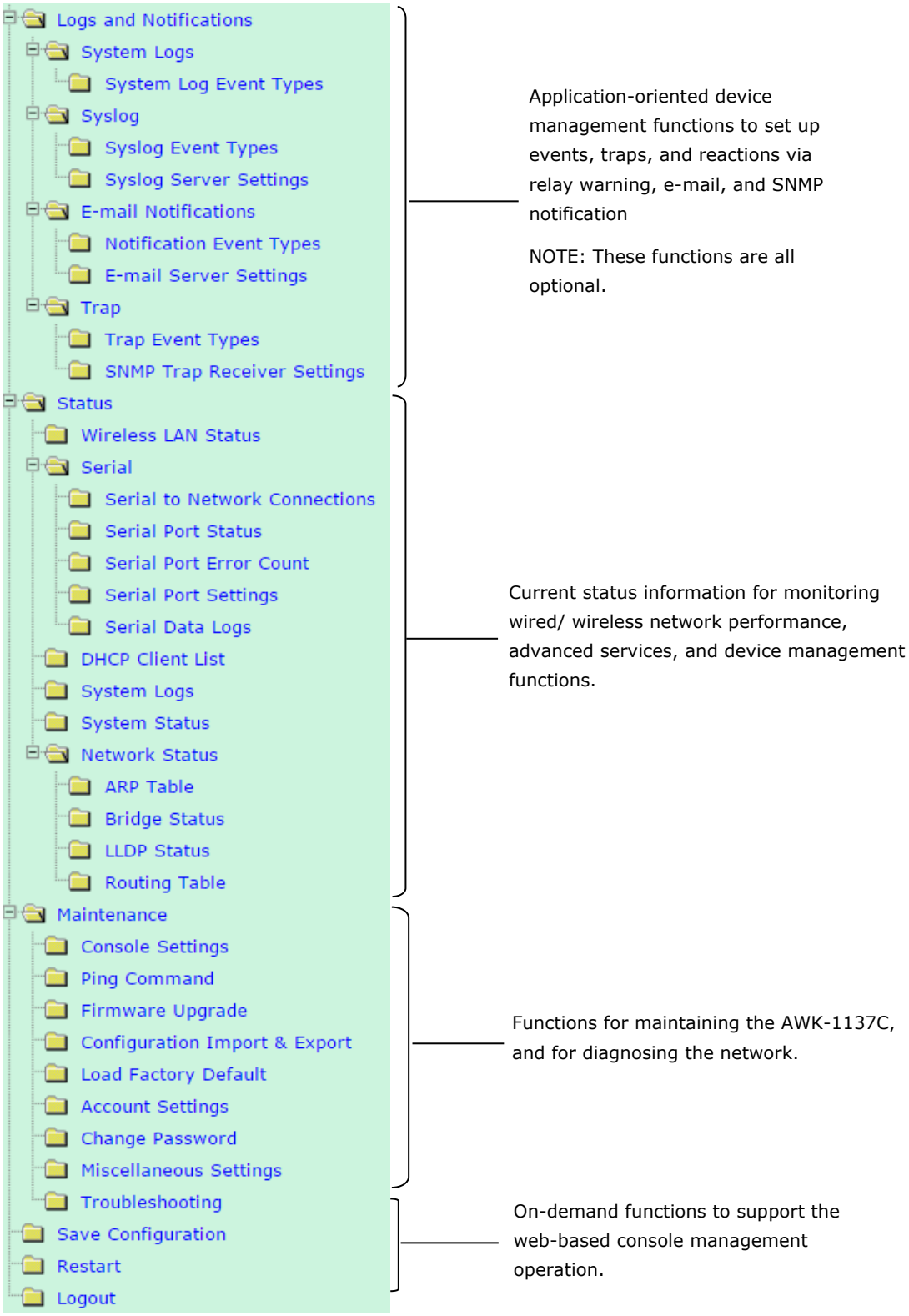
ping *<IP address of notebook A>*

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



Function Map




Logs and Notifications
System Logs
System Log Event Types
Syslog
Syslog Event Types
Syslog Server Settings
E-mail Notifications
Notification Event Types
E-mail Server Settings
Trap
Trap Event Types
SNMP Trap Receiver Settings
Status
Wireless LAN Status
Serial
Serial to Network Connections
Serial Port Status
Serial Port Error Count
Serial Port Settings
Serial Data Logs
DHCP Client List
System Logs
System Status
Network Status
ARP Table
Bridge Status
LLDP Status
Routing Table
Maintenance
Console Settings
Ping Command
Firmware Upgrade
Configuration Import & Export
Load Factory Default
Account Settings
Change Password
Miscellaneous Settings
Troubleshooting
Save Configuration
Restart
Logout
Application-oriented device management functions to set up events, traps, and reactions via relay warning, e-mail, and SNMP notification
NOTE: These functions are all optional.
Current status information for monitoring wired/ wireless network performance, advanced services, and device management functions.
Functions for maintaining the AWK-1137C, 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-1137C and make it easy to establish and maintain your wireless network.

The following topics are covered in this chapter:

- **Web Browser Configuration**
- **Overview**
- **Quick Setup**
- **General Setup**
  - System Information
  - Interface On/Off
  - Network Settings
  - System Time
- **Wireless LAN Setup**
  - AeroMag
  - Operation Mode
  - Basic WLAN Setup
  - Proxy ARP (for Client-Router mode only)
  - WLAN Security Settings
  - Advanced WLAN Settings
  - WLAN Certificate Settings (for EAP-TLS in Client/Client-router/Slave mode only)
- **Serial Port Settings**
  - Communication Parameters
  - Data Buffering/Log
- **Advanced Setup**
  - Using Virtual LAN
  - Configuring Virtual LAN
  - DHCP Server (for Client-Router mode only)
  - Packet Filters
  - Static Route (for Client-router mode only)
  - NAT Settings/Port Forwarding (for Client-router mode only)

Web Browser Configuration

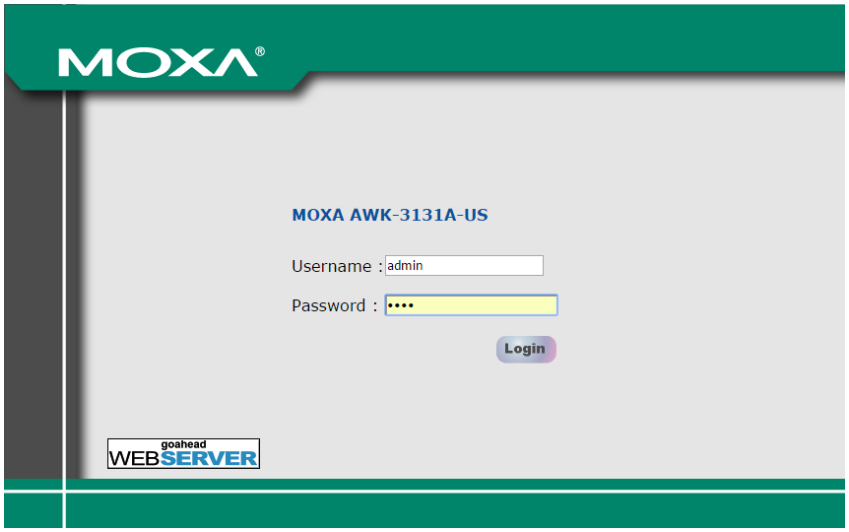
Moxa AWK-1137C's web browser interface provides a convenient way to modify its configuration and access the built-in monitoring and network administration functions. The recommended web browser is Microsoft® Internet Explorer 7.0 or 8.0 with JVM (Java Virtual Machine) installed.

NOTE To use the AWK-1137C's management and monitoring functions from a PC host connected to the same LAN as the AWK-1137C, you must make sure that the PC host and the AWK-1137C are on the same logical subnet. Similarly, if the AWK-1137C is configured for other VLAN settings, you must make sure your PC host is on the management VLAN.

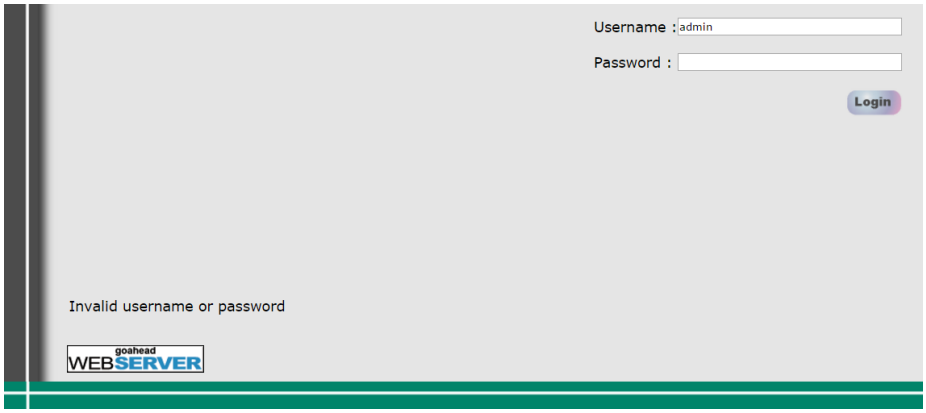
The Moxa AWK-1137C's default IP is **192.168.127.253**.

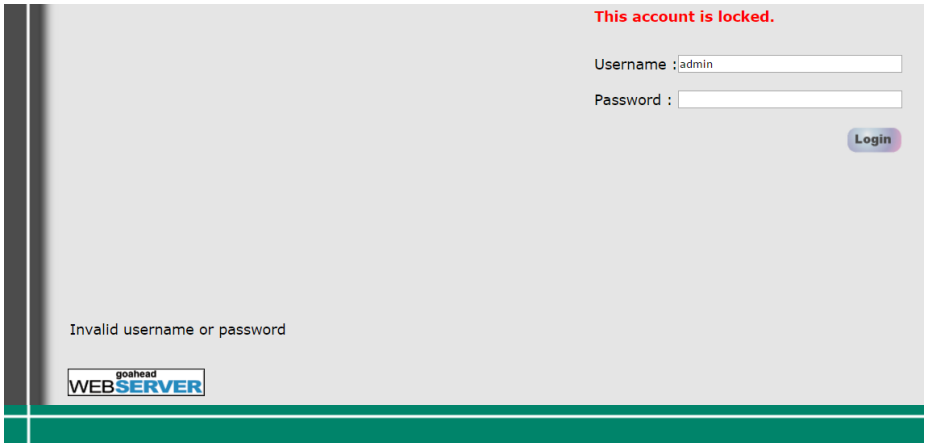
Follow these steps to access the AWK-1137C's web-based console management interface.

1. Open your web browser and type AWK-1137C's IP address in the address field and press **Enter**.
2. The Web Console Login page will open. Enter the password (default Username = **admin**; Password = **moxa**) 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-1137C are both shown in the title bar of the web page. This information can be used to help you identify multiple AWK-1137C units.
   If an incorrect username or password is entered, a warning message is displayed. The system will lock the user account based on the settings configured in the **Maintenance**->**Account Settings** page. The default retry count is 5 times and the default lockout time is 600 seconds. Once an account is locked, the user will have to wait out the duration of the lockout period before retrying.

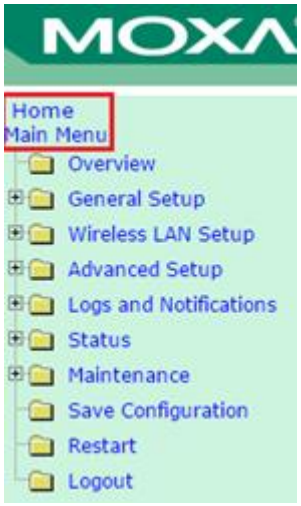




For additional details, see *Account Settings* under *Maintenance.*

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

5. Use the menu tree on the left side of the window to open the function pages to access the AWK-1137C's functions.



To go back to the main page, click on the **Home** link.

An overview of the menu is available at *Chapter 2, Function Map*. The AWK-1137C management functions are described in detail in the following sections.

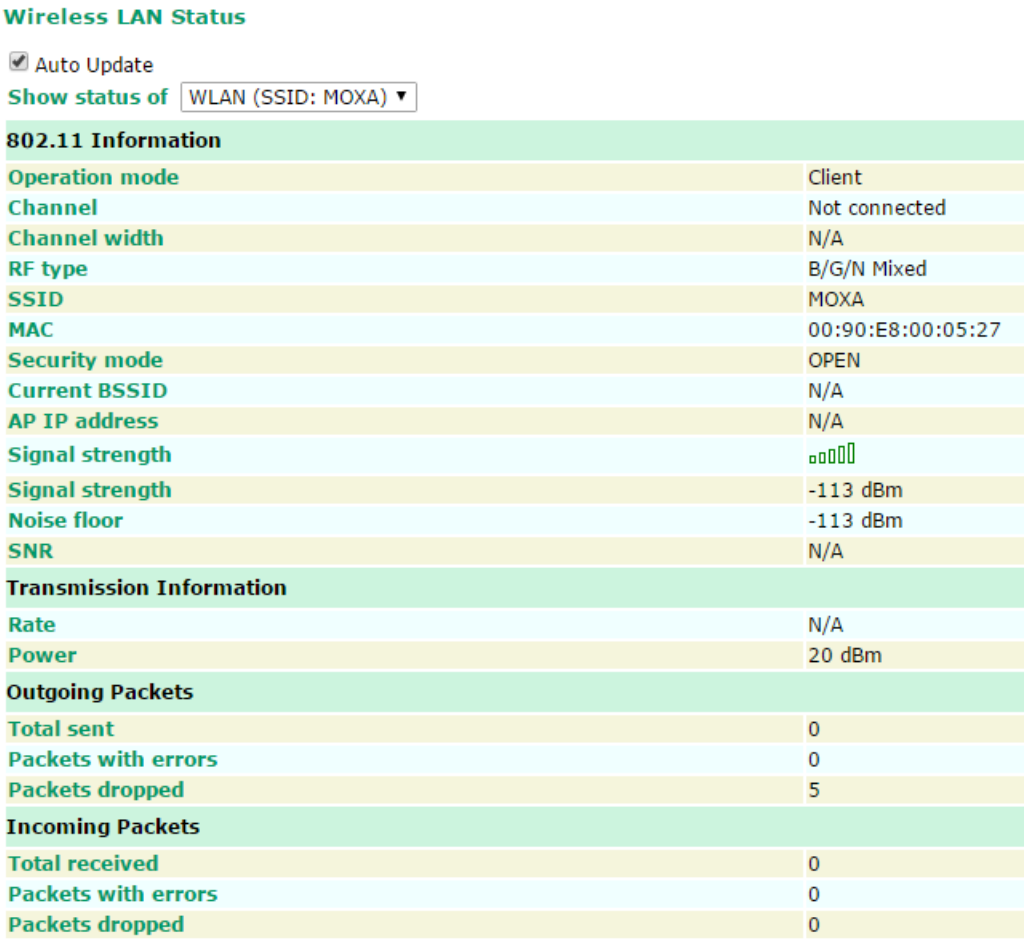
NOTE The model name of the AWK-1137C is shown as AWK-1137C-XX, where XX indicates the country code. The country code indicates the AWK-1137C version and which frequencies it uses. We use **AWK-1137C-US** as an example in the following figures. The country code and model name that appears on your computer screen may be different than the one shown here.

Overview

The **Overview** page summarizes the AWK-1137C's current status. The information is categorized into several groups: **System Information, Device Information** and **802.11 Information**.

System Information	
Model name	AWK-1137C-US
Device name	AWK-1137C_0207
Serial number	207
System uptime	0 days 00h:13m:57s
Firmware version	1.0 Build 17021617
Device Information	
Device MAC address	00:90:E8:00:05:27
IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	
802.11 Information	
Country code	US
Operation mode	Client
Channel	Not connected
RF type	B/G/N Mixed
Channel width	N/A
SSID	MOXA

Click on the **SSID** link for detailed 802.11 Information as shown in the following figure:



Wireless LAN Status

Auto Update

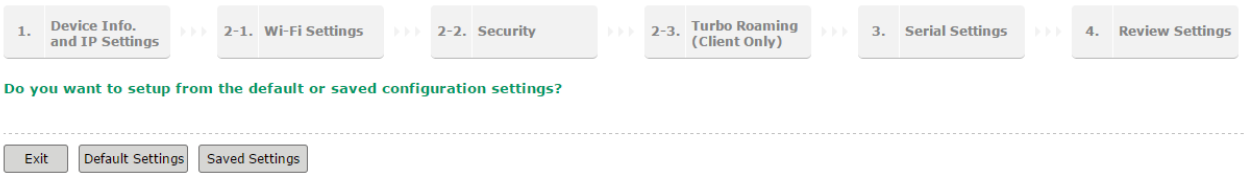
Show status of WLAN (SSID: MOXA)

802.11 Information	
Operation mode	Client
Channel	Not connected
Channel width	N/A
RF type	B/G/N Mixed
SSID	MOXA
MAC	00:90:E8:00:05:27
Security mode	OPEN
Current BSSID	N/A
AP IP address	N/A
Signal strength	
Signal strength	-113 dBm
Noise floor	-113 dBm
SNR	N/A
Transmission Information	
Rate	N/A
Power	20 dBm
Outgoing Packets	
Total sent	0
Packets with errors	0
Packets dropped	5
Incoming Packets	
Total received	0
Packets with errors	0
Packets dropped	0

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

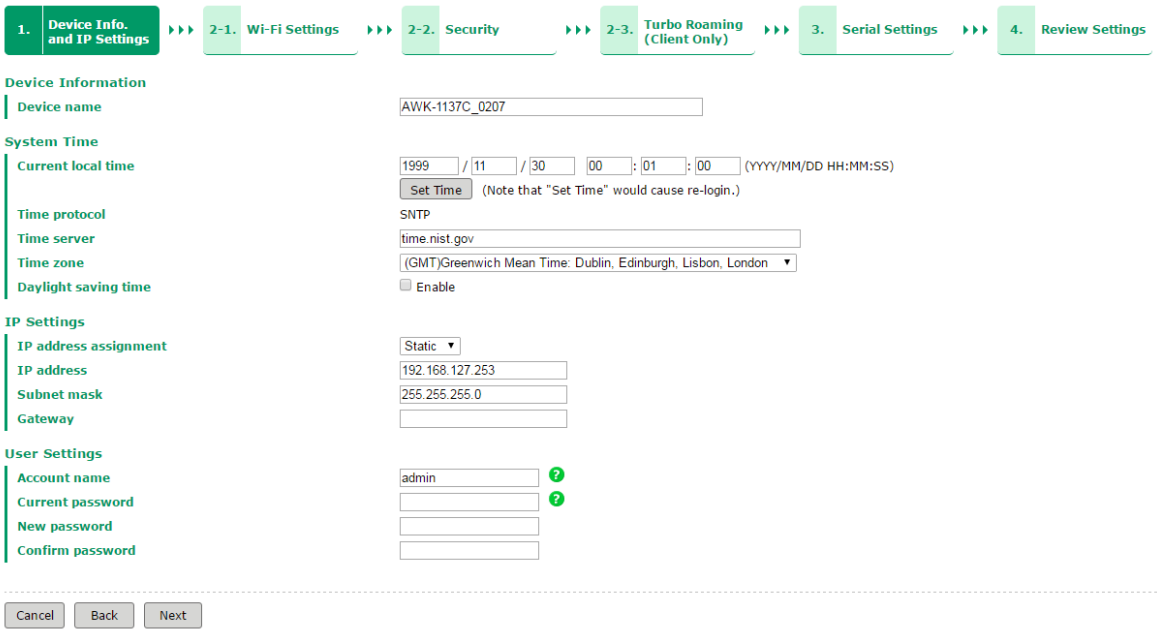
Quick Setup

The AWK-1137C provides a quick setup wizard to help you configure the basic settings, including wireless and serial (for devices that support a serial console) settings. Before you enter the setup wizard, you will see a list of the tasks as shown below:

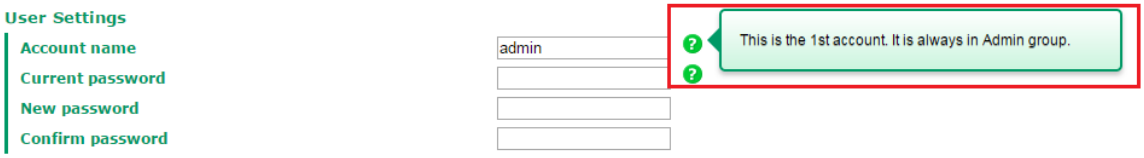


Choose **Default Settings** to see the default parameters or the **Saved Settings** to view the current parameters.

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



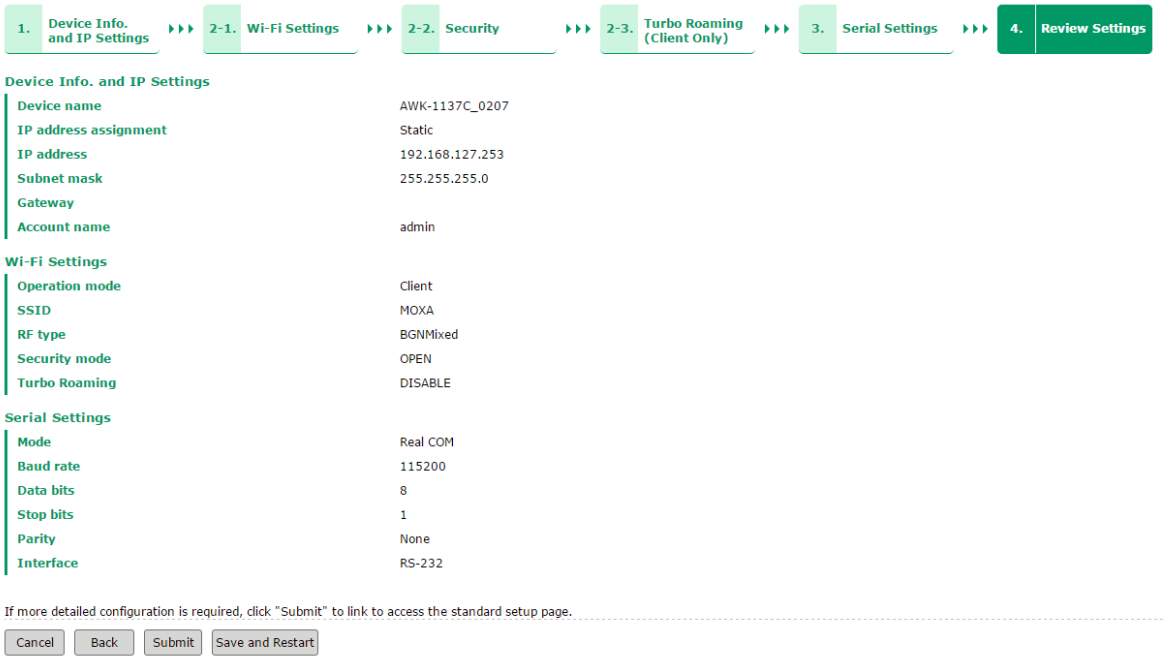
NOTE You can move your cursor on the question mark symbol to view a tooltip for additional details regarding the corresponding field.



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

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

In the last step of the setup process, "**4. Review Settings"**, you will be able to view the basic Wi-Fi parameters that you configured in the previous steps.

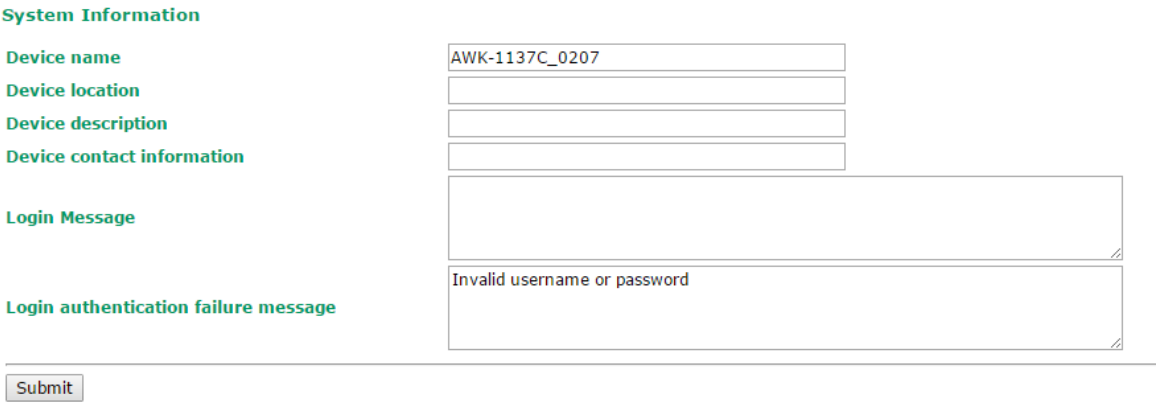


General Setup

The General Setup group includes the most commonly used settings required by administrators to maintain and control the AWK-1137C.

System Information

The **System Information** items, especially ***Device name*** and ***Device description***, are displayed and included on the **Overview** page, in SNMP information, and in alarm emails. Setting **System Information** items makes it easier to identify the different AWK-1137C units connected to your network.



Device name

Setting	Description	Factory Default
Max. 31 of characters	This option is useful for specifying the role or application of different AWK-1137C units.	AWK-1137C_<Serial No. of this AWK-1137C>

Device location

Setting	Description	Factory Default
Max. of 31 characters	Specifies the location of different AWK-1137C units.	None

Device description

Setting	Description	Factory Default
Max. of 31 characters	Use this space to record a more detailed description of the AWK-1137C.	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-1137C.	None

Login Message

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

Login authentication failure message

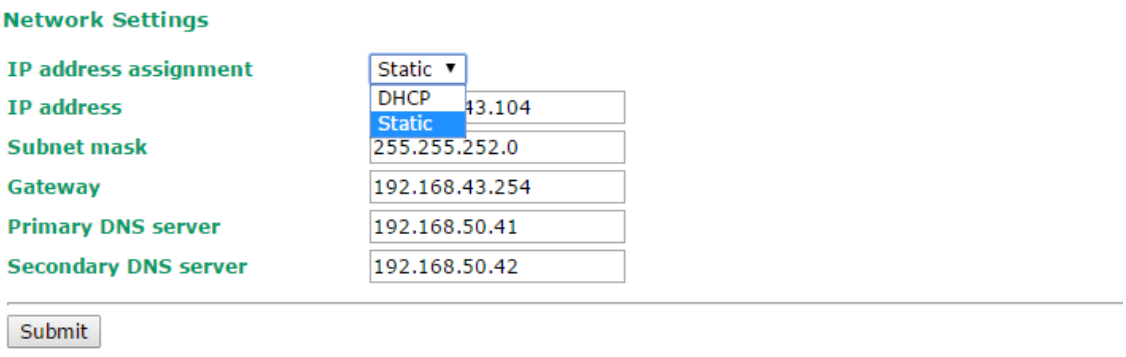
Setting	Description	Factory Default
Max. of 31 characters	Enter the login authentication failure message to display to the user who logs in with an invalid username or password	None

Interface On/Off

Network Settings

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

Network Settings for Client /Slave Operation Modes



IP address assignment

Setting	Description	Factory Default
DHCP	The AWK-1137C's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the AWK-1137C's IP address manually.	

IP address

Setting	Description	Factory Default
AWK-1137C's IP address	Identifies the AWK-1137C on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
AWK-1137C's subnet mask	Identifies the type of network to which the AWK-1137C 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

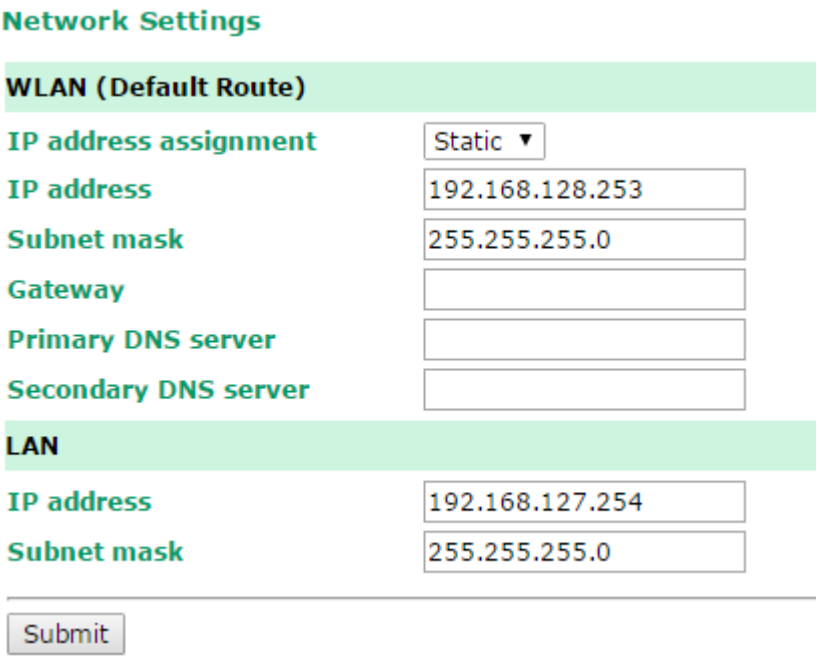
Gateway

Setting	Description	Factory Default
AWK-1137C'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-1137C's URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Network Settings for Client-Router Operation Mode



WLAN IP address assignment

Setting	Description	Factory Default
DHCP	The AWK-1137C WLAN interface's IP address will be assigned automatically by the network's DHCP server	Static
Static	Set up the AWK-1137C WLAN interface's IP address manually.	

WLAN IP address

Setting	Description	Factory Default
AWK-1137C WLAN interface's IP address	Identifies the AWK-1137C WLAN interface's IP address on a TCP/IP network.	192.168.128.253

WLAN subnet mask

Setting	Description	Factory Default
AWK-1137C WLAN interface's subnet mask	Identifies the type of network to which the AWK-1137C's WLAN interface is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

WLAN gateway

Setting	Description	Factory Default
AWK-1137C WLAN interface's default gateway	The IP address of the router that connects the WLAN to an outside network.	None

Primary/Secondary DNS server

Setting	Description	Factory Default
IP address of the Primary/Secondary DNS server	The IP address of the DNS Server used by your network. After entering the DNS Server's IP address, you can input the AWK-1137C's URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

LAN IP address

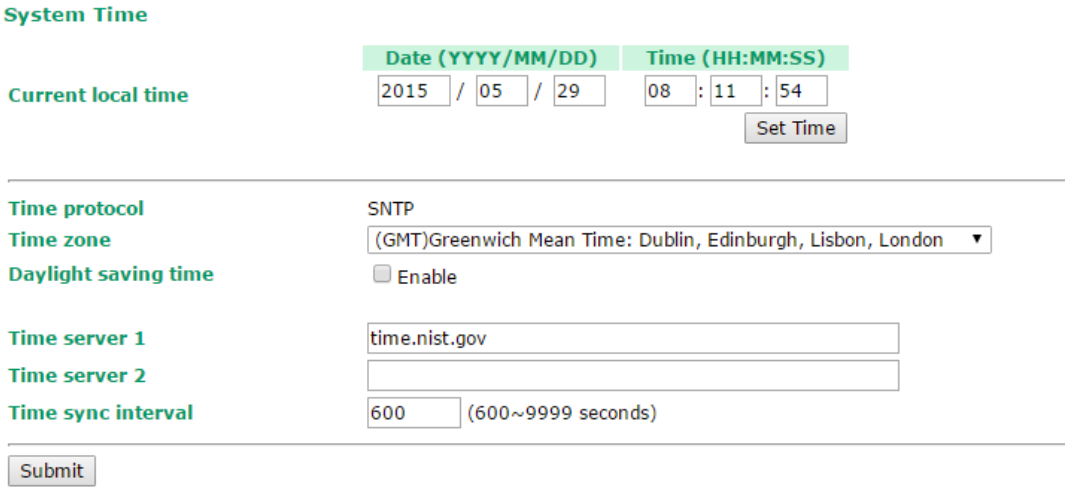
Setting	Description	Factory Default
AWK-1137C LAN interface's IP address	Identifies the AWK-1137C LAN interface's IP address on a TCP/IP network.	192.168.127.254

LAN subnet mask

Setting	Description	Factory Default
AWK-1137C LAN interface's subnet mask	Identifies the type of network to which the AWK-1137C's LAN interface is connected (e.g., 255.255.0.0 for a Class B network, or 255.255.255.0 for a Class C network).	255.255.255.0

System Time

The AWK-1137C has a time calibration function based on information from an NTP server or user specified Date and Time information. Functions such as **Logs and Notifications** can add real-time information to the message.



The ***Current local time*** shows the AWK-1137C's system time when you open this web page. You can click on the **Set Time** button to activate the updated date and time parameters. An "(Updated)" string will appear to indicate that the change is complete. Local system time will be immediately activated in the system without running Save and Restart.

NOTE The AWK-1137C has a built-in real time clock (RTC). We strongly recommend that users update the **Current local time** for the AWK-1137C after the initial setup or a long-term shutdown, especially when the network does not have an Internet connection for accessing the NTP server or there is no NTP server on the LAN.

Current local time

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

Time zone

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

ATTENTION

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

Daylight saving time

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

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

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

Time server 1/2

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

Time sync interval

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

Wireless LAN Setup

The AWK-1137C deployed as a Wi-Fi client can be used as an Ethernet-to-wireless and serial-to-wireless network adapter. AWK-1137C provides point-to-multipoint communication as a client device or MAC-transparent point-to-point communication as a slave device.

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.

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

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

Sniffer: In order to provide an easier way for our customers to analyze wireless traffic, the AWK-1137C supports a "Sniffer" mode to co-work with Wireshark packet sniffer software.

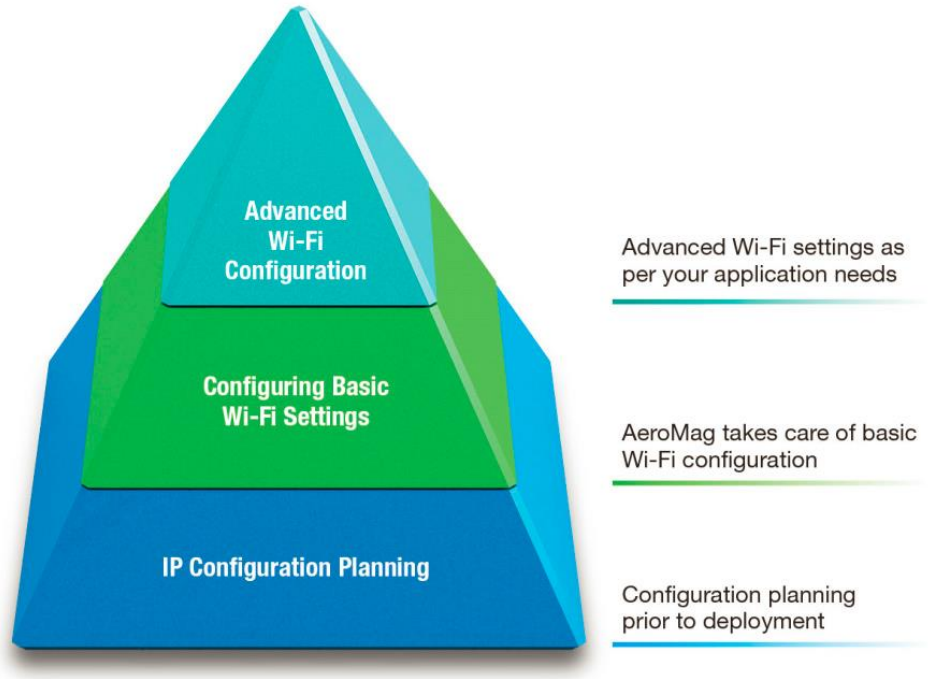
NOTE Although it is more convenient to use dynamic bridging, there is a limitation—the Client can only transmit IP-based packets between its wireless interface (WLAN) and Ethernet interface (LAN); other types of traffic (such as IPX and AppleTalk) are not forwarded.

AeroMag

Moxa's AeroMag tool enables fast, automatic, and error-free configuration of basic Wi-Fi settings based on the current wireless environment and location of the APs. In an AeroMag topology, the AWK-1137C is used as the AeroMag client or client-router with the AWK-3131A or AWK-4131A as the AeroMag AP.

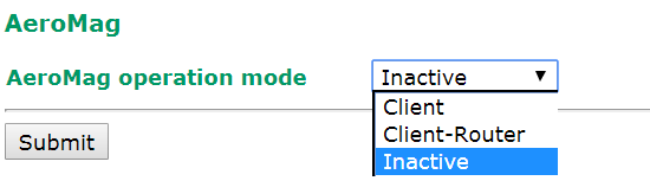
Concept

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

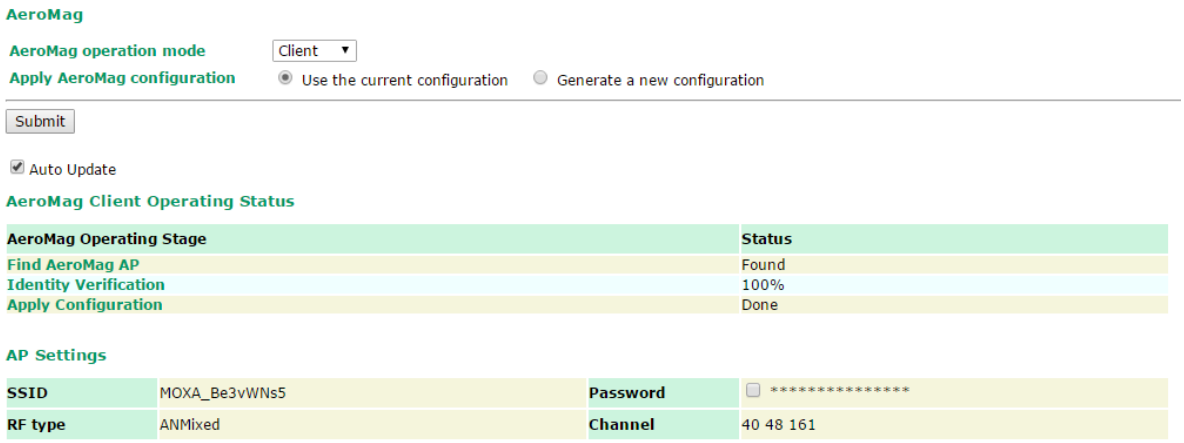


Once you have confirmed the number of APs and their location using a site-survey tool and have configured their device names and IP addresses, connect all the APs to the same network using Layer-2 switches. Next, activate the AeroMag function on both the APs and clients.

AeroMag decides on the optimum RF type, channels, WPA2 password, and SSID, based on which, AeroMag APs will generate an optimal configuration and assign it to the AeroMag Clients. AeroMag Clients search for AeroMag APs to acquire an optimal configuration.



The AeroMag function is inactive by default. The AWK-1137C supports **Client** and **Client-Router** mode AeroMag functionality. To activate AeroMag, set the **AeroMag operation mode** to **Client** or **Client-Router**.



NOTE You can also activate AeroMag through MXconfig, SNMP, or by using the Reset button.
Press the Reset button on the AWK-1137C **five times** to activate AeroMag client.
Press the Reset button **three times** to deactivate AeroMag (each consecutive press should be affected within 2 seconds.)
You can activate either the AP first or the Client first as the sequence of activation does not affect the behavior of the AeroMag tool.

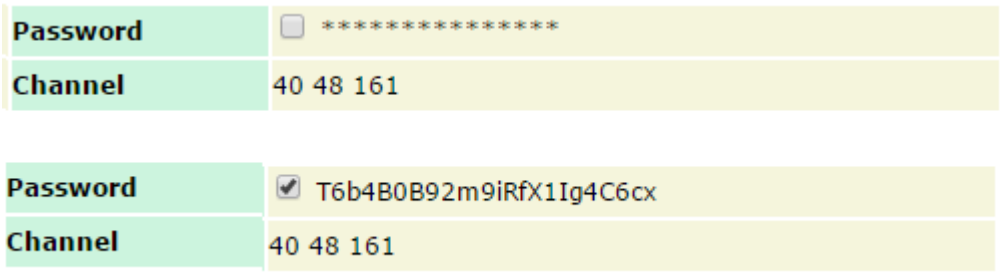
You can configure the following setting when AeroMag is active:

Setting	Description	Factory Default
Apply AeroMag configuration	• *Use the current configuration:* Use the current configuration generated by AeroMag. This option is only available if AeroMag was already active at least once before the current configuration change. If you are activating AeroMag for the first time, this option will not be available. • *Generate a new configuration:* Discard current configuration settings and search for an AeroMag AP to get a new set of configuration settings.	*Generate a new configuration*

You can also view the **AeroMag Client/Client-Router Operating Status** listed below:

NOTE Select the **Auto Update** option for AeroMag to refresh the client operating status every 30 seconds. When the AeroMag Client receives information on a change in the configuration, the **Auto Update** function refreshes the Client's operating status every 5 seconds.

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



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

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

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

If AeroMag clients are trying to join a topology that has been locked by AeroMag, they will see the **Block** status. To add new units to an existing AeroMag topology, you must first unlock the topology.

NOTE

1. AeroMag client CANNOT search and connect to a normal AP because of a null configuration during the search.
2. When AeroMag APs discard their configuration due to a group merge, the corresponding AeroMag clients will also discard their configuration and reboot to search for new AeroMag APs.
3. If an AeroMag client is disconnected from an AeroMag AP and fails to find an AeroMag AP in the Turbo Roaming channel within 150 seconds, the client starts to scan all channels for AeroMag APs to recover its AeroMag connection.
4. If an AeroMag client loses a connection for 10 minutes and fails to connect again, the AeroMag client discards the current configuration, reboots, and starts searching for AeroMag APs all over again.
5. If an AeroMag client is informed that the Turbo Roaming channel needs to be changed due to the **Refresh Channel** being triggered by AeroMag APs, the Wi-Fi connection with the clients will be disconnected for 180 seconds until it is reconnected to the APs.
6. If an AeroMag client is blocked outside an existing AeroMag group for 5 minutes, the AeroMag client will reboot and search for another AeroMag AP.
7. AeroMag devices in a network must operate in the same regulatory band. For example, if one AeroMag unit uses US band and the other units use EU band, AeroMag will fail to establish a network topology.

Operation Mode

The AWK-1137C supports four operation modes—Client, Client-Router, Slave, and Sniffer—each of which plays a distinct role in a wireless network.

Wireless enable

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

Operation mode

Setting	Description	Factory Default
Client	The AWK-1137C plays the role of wireless Client.	Client
Client-Router	The AWK-1137C plays the role of wireless Client, but includes the router function to divide the WLAN and LAN interfaces into two subnets.	
Slave	The AWK-1137C plays the role of wireless Slave.	
Sniffer	Turns the device into a remote Wireshark interface to capture 802.11 packets for analysis.	

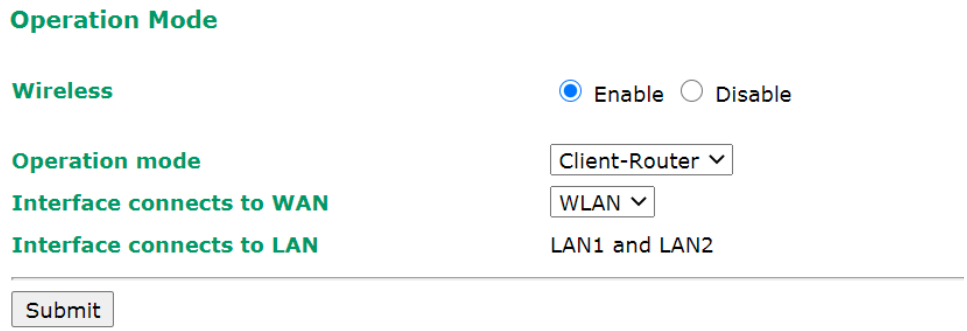
08 NAT box

Client-Router Mode Instructions:

Set the operation mode to Client-Router mode on the AWK-1137C and then define the WAN and LAN subnets. There are two scenarios:

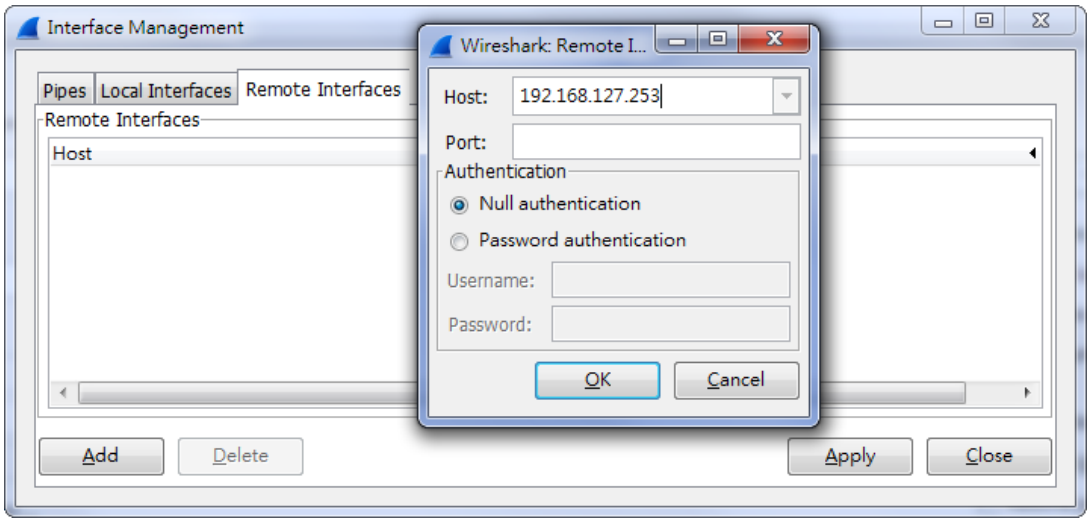
1. General case: The WLAN interface connects to the WAN, LAN1 and LAN2 connect to the allocated private network.
2. NAT box: LAN 1 connects to the WAN, WLAN and LAN 2 connect to the allocated private network.

Setting	Description	Factory Default
interface connects to WAN	Use a wireless (WLAN) or wired (LAN1) method to connect to the WAN.	WLAN
interface connects to LAN	Depending on the interface connected to the WAN, the LAN connection will change accordingly.	LAN1 and LAN2



Sniffer Mode Instructions:

3. Set operation mode to Sniffer mode on the AWK-1137C and then save/reboot the device.
4. Connect the AWK-1137C to a laptop with Wireshark installed (v1.12.0 or later release) via Ethernet.
5. Add a remote interface by entering the IP address of the AWK-1137C.



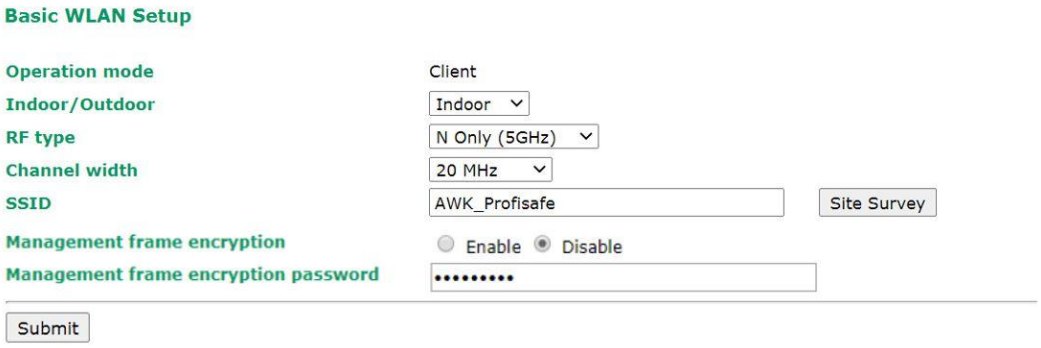
Detailed Wireshark instructions can be found at:
https://www.wireshark.org/docs/wsug_html_chunked/ChCapInterfaceRemoteSection.html

6. Start capturing 802.11 wireless packets with Wireshark.

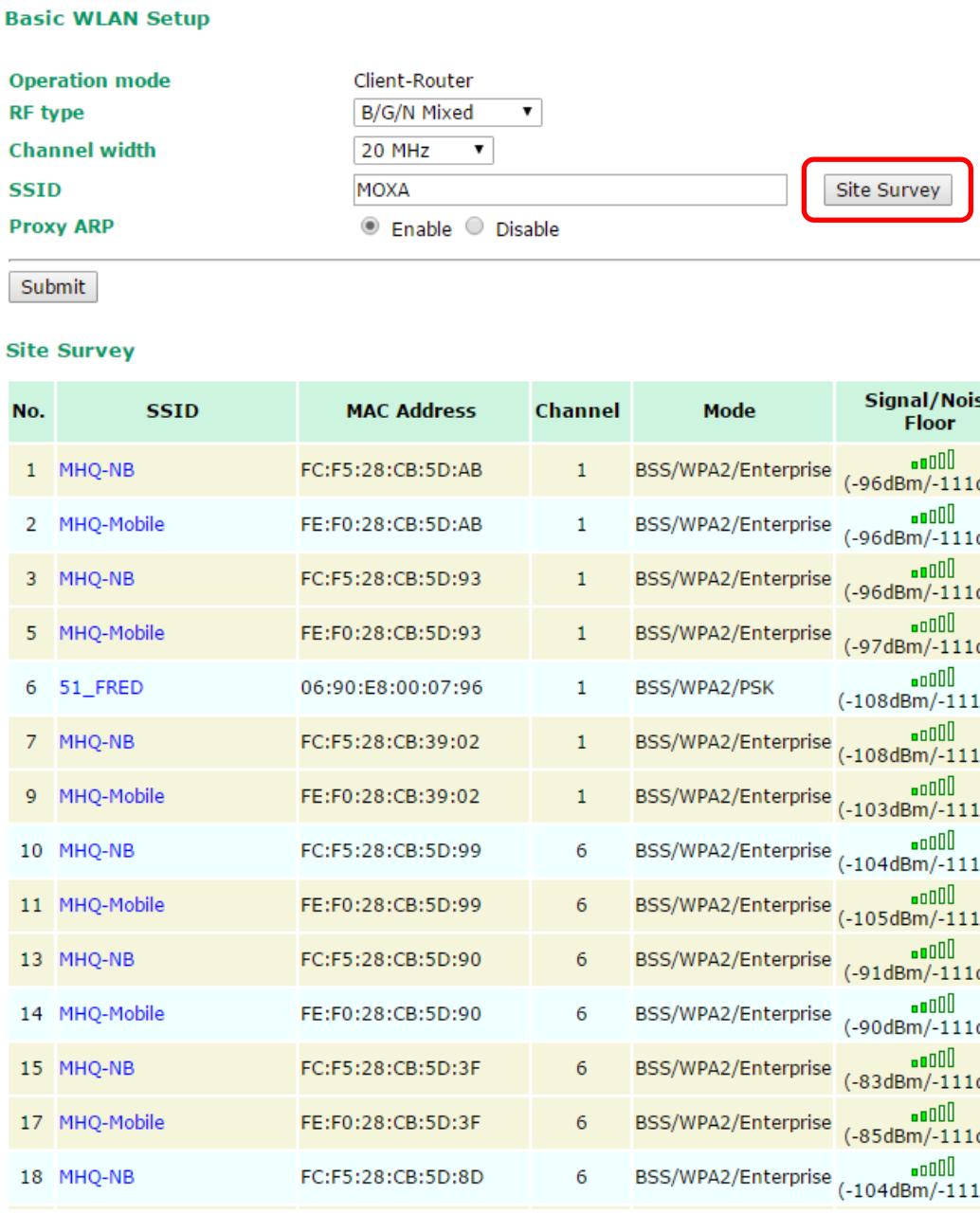
Basic WLAN Setup

The **WLAN Basic Setting Selection** panel is used to edit the SSIDs and set the RF type for the AWK device. You can use the RF type selection to configure the AWK-1137C to operate either on the 2.4 GHz or 5 GHz frequency band. An SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. Set the SSID of the AWK-1137C to match with the SSID of the AP that you want it to connect to so that the AWK-1137C will associate with the network defined by the SSID.

Click on **Edit** to configure settings. The configuration panel appears as follows:



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



Indoor/outdoor

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

RF type

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

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

Channel width (for any 11N RF type only)

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

Channel bonding

Channel bonding shows the channel used by the AP if **Channel width** is set to 20/40 MHz.

SSID

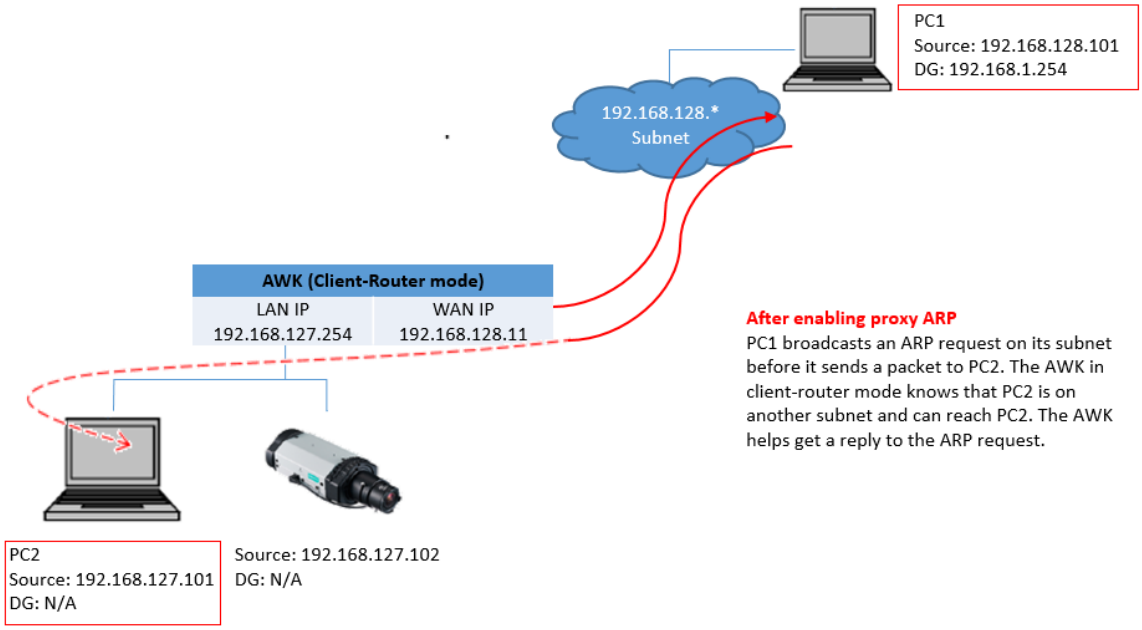
Setting	Description	Factory Default
Max. of 31 characters	The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. NOTE: An SSID cannot contain the following characters: ` ' " | ; &	MOXA

Management Frame Encryption

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

Proxy ARP (for Client-Router mode only)

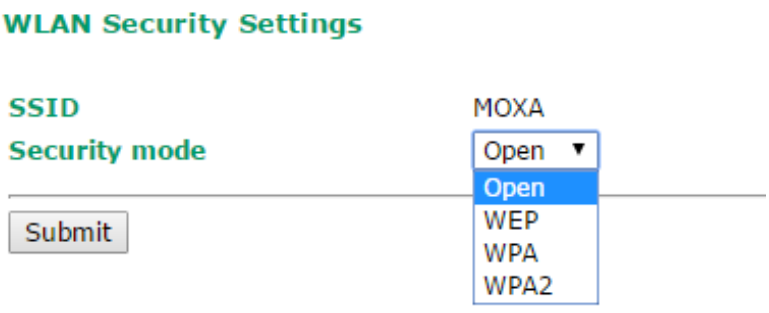
Proxy Address Resolution Protocol (ARP) is supported in the AWK to facilitate the Client-Router operation mode. Enabling Proxy ARP helps devices on remote subnets reach the local subnet. The AWK devices respond to the ARP requests intended for the devices are connected to them, but this will increase the ARP traffic in the network.



WLAN Security Settings

The AWK-1137C 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-1137C 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-1137C can support 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"	

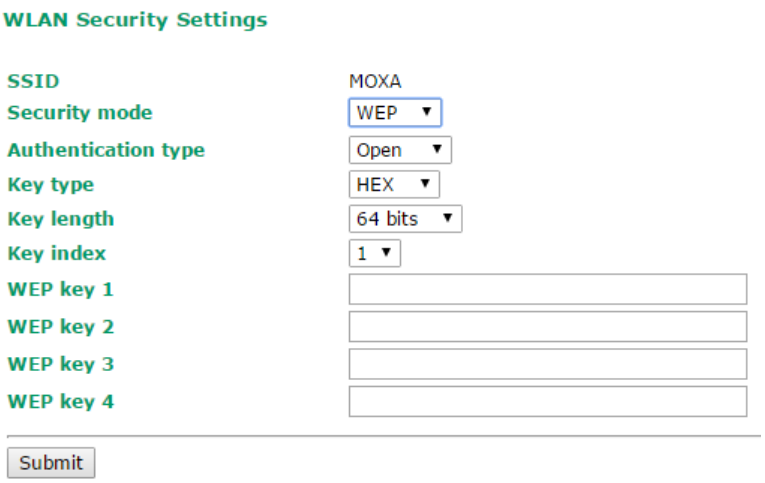
Open

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 (only for legacy mode)

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

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



When WEP is enabled as a security mode, the length of a key (so-called WEP seed) can be 64/128 bits, which is actually a 40/104-bit secret key with a 24-bit initialization vector. The AWK-1137C 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 hex-decimal number form	HEX
ASCII	Specifies WEP keys in ASCII form	

Key length

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

Key index

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

WEP key 1-4

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

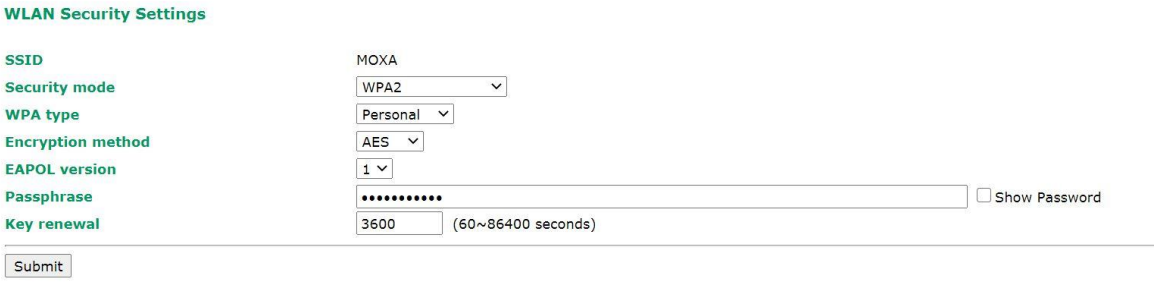
HEX type: 64 bits: 10 hex chars 128 bits: 26 hex chars		

WPA/WPA2-Personal

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

Even though AES encryption is only included in the WPA2 standard, it is widely available in the WPA security mode of some wireless APs and clients as well. The AWK-1137C also supports AES algorithms in WPA and WPA2 for better compatibility.

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



WPA type

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

Encryption method

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

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

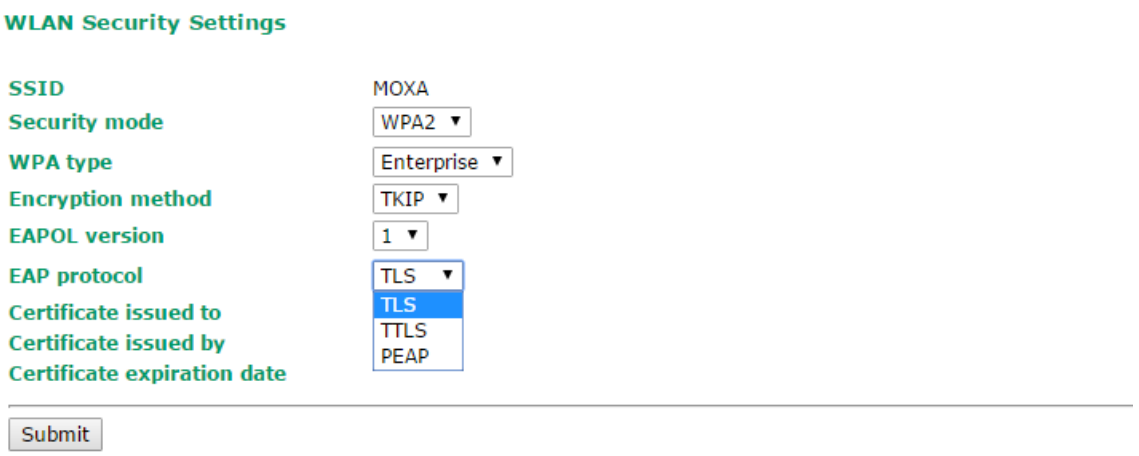
** This option is available for legacy mode in AP/Master only, and does not support AES-enabled clients.*

Passphrase

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

WPA/WPA2-Enterprise

When used as a client, the AWK-1137C can support three EAP methods (or ***EAP protocols***): **EAP-TLS**, **EAP-TTLS**, and **EAP-PEAP**, corresponding to WPA/WPA-Enterprise settings on the AP side.



Encryption method

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

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

EAP protocol

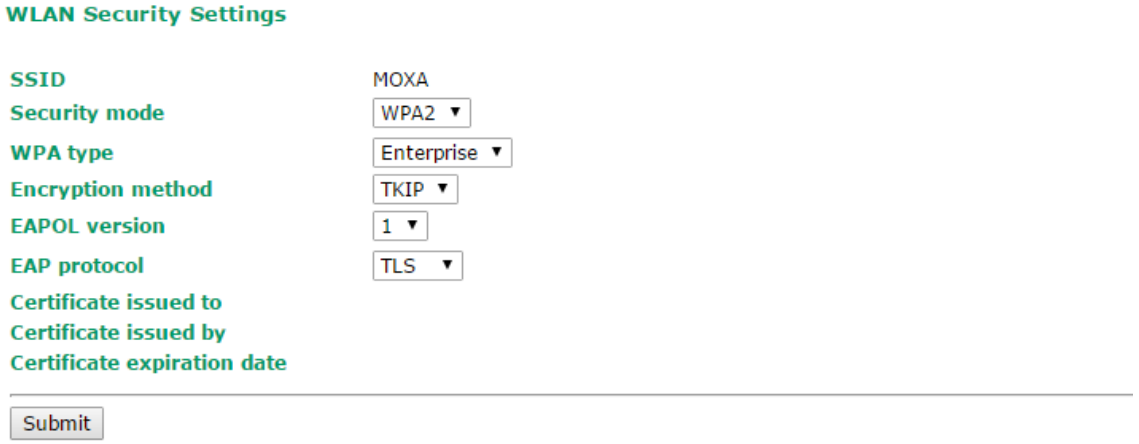
Setting	Description	Factory Default
TLS	Specifies Transport Layer Security protocol	TLS
TTLS	Specifies Tunneled Transport Layer Security	
PEAP	Specifies Protected Extensible Authentication Protocol, or Protected EAP	

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

EAP-TLS

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

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



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

- **Certificate issued to:** Shows the certificate user

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

EAP-TTLS

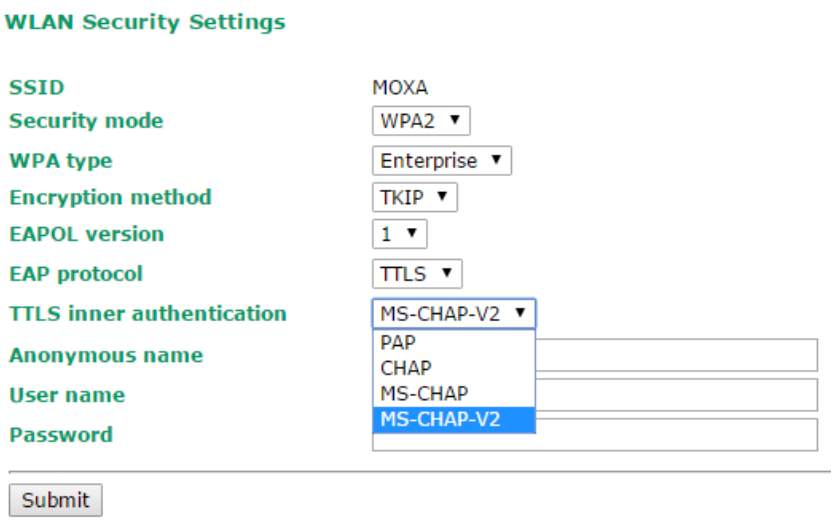
It is usually much easier to re-use existing authentication systems, such as a Windows domain or Active Directory, LDAP directory, or Kerberos realm, rather than creating a parallel authentication system. As a result, TTLS (Tunneled TLS) and PEAP (Protected EAP) are used to support the use of so-called "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-1137C 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

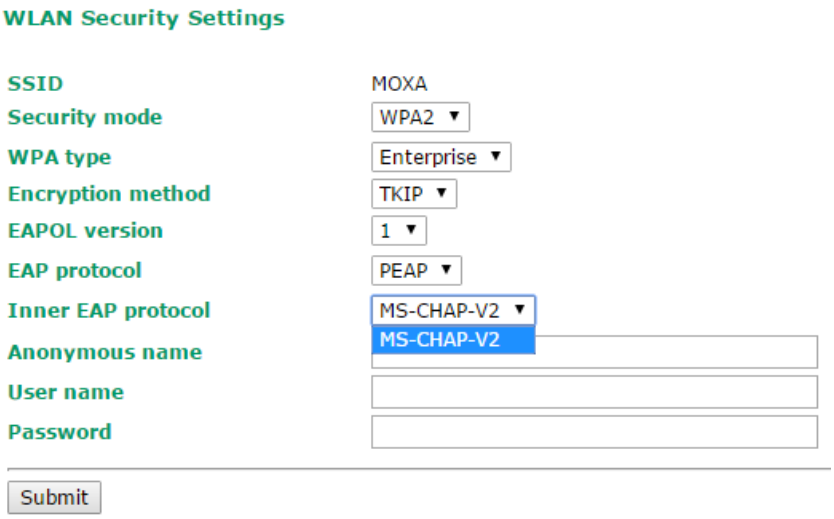
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

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

PEAP

There are a few differences in the TTLS and PEAP inner authentication procedures. TTLS uses the encrypted channel to exchange attribute-value pairs (AVPs), while PEAP uses the encrypted channel to start a second EAP exchange inside of the tunnel. The AWK-1137C 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

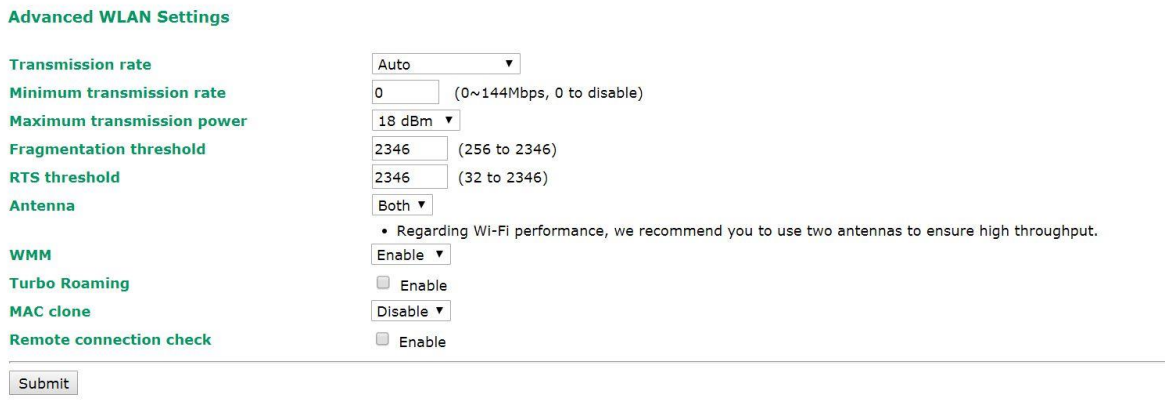
Setting	Description	Factory Default
Max. of 31 characters	A distinct name used for outer authentication	None

User name & Password

Setting	Description	Factory Default
-	User name and password used for internal authentication	None

Advanced WLAN Settings

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



Transmission rate

Setting	Description	Factory Default
Auto	The AWK-1137C senses and adjusts the data rate automatically	Auto
Available rates	Users can manually select a target transmission data rate but does not support when RF type are G/N mixed, B/G/N mixed and A/N mixed.	

Minimum transmission rate

Setting	Description	Factory Default
0 to 64 Mbps (0 to disable)	By setting a minimum transmission rate, the AWK-1137C will avoid communicate with weak signal wireless links to maintain overall wireless performance and optimize the wireless frequency usage.	0 (Disable)

Transmission power

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

Fragmentation threshold

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

RTS threshold

Setting	Description	Factory Default
RTS/CTS Threshold (32 to 2346)	Determines how large a packet can be before the Access Point coordinates transmission and reception to ensure efficient communication.	2346

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

Antenna

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

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

WMM

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

Turbo Roaming

Setting	Description	Factory Default
Enable/ Disable	Moxa's Turbo Roaming can enable rapid handover when the AWK-1137C, as a client, roams among a group of APs.	Disable

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

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

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

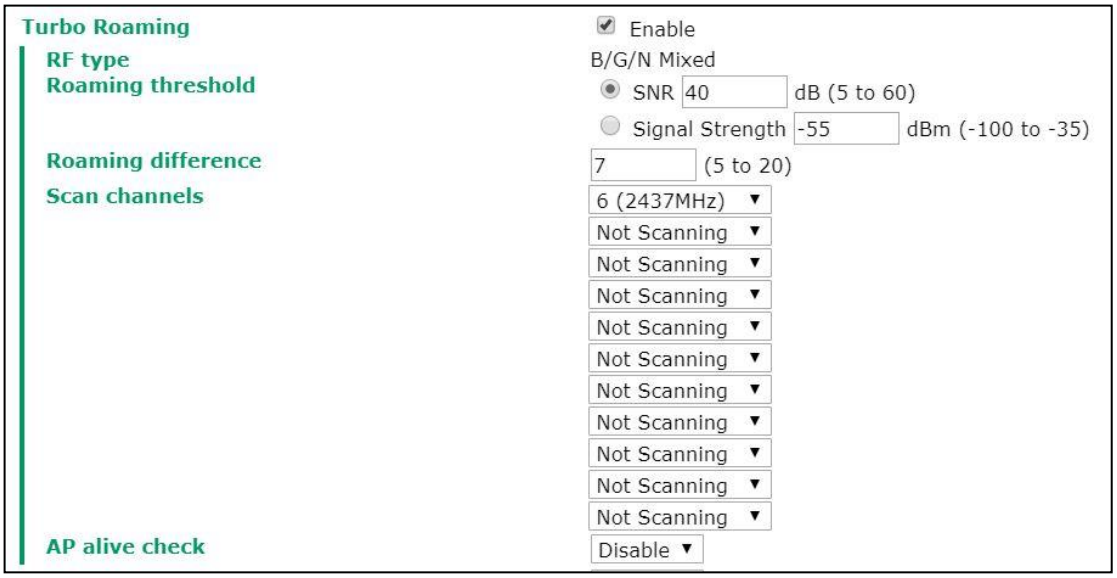
- **Roaming difference:** Determines if roaming should be executed. After background scan has been triggered, the roaming will only occur if the AP candidate(s) provide a better connection quality (based on the roaming difference value) than the current connection. If multiple access points fulfill the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

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

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

NOTE Enabling this feature causes the AWK-1137C to send out packets every 10 ms when there is no traffic to check if the connection is alive. The high transmission frequency of small alive check packets could potentially affect your other wireless communications that use the same channel, so only enable this feature when you have full control of the designated radio channel.

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



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

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

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

MAC clone

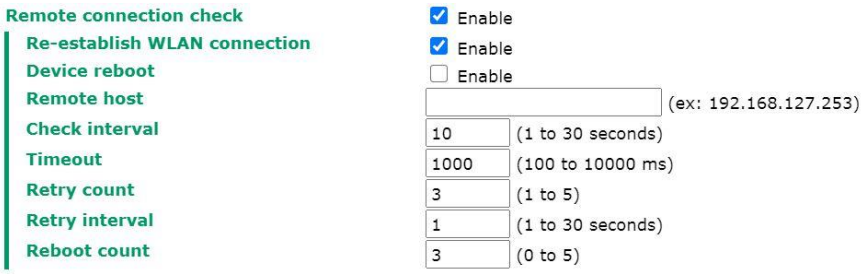
Setting	Description	Factory Default
Enable/Disable	Enabling this feature allows the AWK client to copy the MAC address of LAN connected equipment as its own. This overcomes the limitation of the IP-Bridged behavior in a MAC-sensitive network (MAC-based communication or MAC-authenticated network). Limitation: Only ONE device is allowed to connect to the AWK client while this feature is enabled.	Disable
MAC clone method	Auto: The AWK client uses the MAC address of the device connected to the LAN if only one device is connected to the AWK. Static: The AWK client shares the assigned MAC address with multiple devices connected to the LAN. This allows for multiple devices to connect to the AWK via the LAN and only one of them needs to be assigned a MAC address.	Auto
MAC clone static address	Specifies the static MAC address that the connected AWK devices should use.	
MAC clone interface	Specify the LAN interface to clone the MAC address from. The AWK-1137C will copy the MAC address of the device connected to the specified interface.	LAN 1

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

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

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

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



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

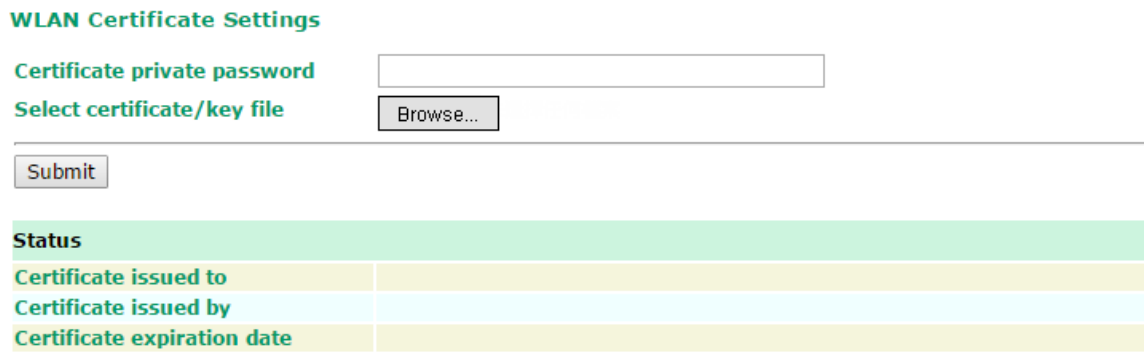
NOTE If **Re-establish WLAN connection** and **Device reboot** are both enabled, the AWK-3313A will attempt to restore the WLAN connection first. If re-establishing the WLAN connection fails, the device will reboot.

- **Remote host:** Enter the IP address of a remote host to ping. This is used for the WLAN connection alive and packet-level connection checks.

- **Check interval:** Specify the time interval when the AWK-1131A checks the connection. The range is between 1 to 30 seconds, the default is every 10 seconds.
- **Timeout:** Specify the duration the AWK-1131A must wait before terminating the connection. The range is between 100 to 10,000 ms, the default is 1000 ms.
- **Retry count:** Specify the number of times the AWK-1131A the will check the connection status. If the connection fails more than the specified number of tries, the device will attempt to recover the WLAN connection. The range is between 1 to 5, the default is 3 retries.
- **Retry Interval:** Specify the time interval in between each retry. The range is between 1 to 30 seconds, the default is 1 second.
- **Reboot count:** If **Device reboot** is enabled, specify the number of times the device will reboot after failing to re-establish the connection.

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

When EAP-TLS is used, a WLAN Certificate will be required at the client end to support WPA/WPA2-Enterprise. The AWK-1137C can support the **PKCS #12**, also known as *Personal Information Exchange Syntax Standard*, certificate formats that define file formats commonly used to store private keys with accompanying public key certificates, protected with a password-based symmetric key.



Current status displays information for the current WLAN certificate, which has been imported into the AWK-1137C. Nothing will be shown if a certificate is not available.

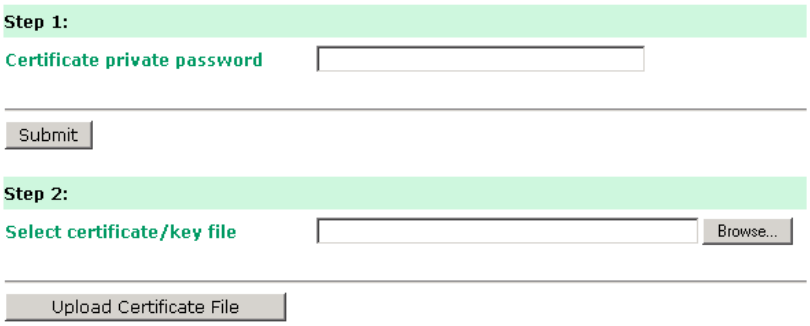
Certificate issued to: Shows the certificate user

Certificate issued by: Shows the certificate issuer

Certificate expiration date: Indicates when the certificate has expired

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

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



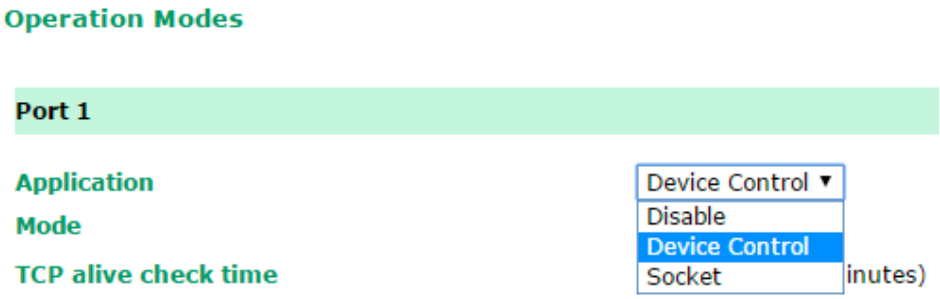
NOTE The WLAN certificate will remain after the AWK-1137C reboots. Even though it is expired, it can still be seen on the ***Current Certificate***.

Serial Port Settings

The AWK-1137C is provided with a serial port for connecting serial devices to the WLAN network. The AWK support various useful serial operation modes to make connecting to your serial devices much simpler.

Operation Modes

The Operation Modes page for the serial port is where you can configure the serial port operation mode and related settings.



Application

This field specifies the application of this serial port. Depending on the application, the different operation modes and their settings will be displayed.

Setting	Description	Factory Default
Disable	This serial port will be disabled.	Device Control
Device Control	This serial port will be used to control a device using legacy software installed on a Windows, Linux, or UNIX system. Drivers will need to be installed that will allow your software to communicate with the device as if it were physically attached to a local COM or TTY port. You may select between Real COM and RFC2217 operation modes.	
Socket	This serial port will be used for a TCP or UDP socket-based application. You may select between TCP Client, TCP Server, and UDP operation modes.	

NOTE We recommend disabling the port if no serial devices are connected to the AWK.

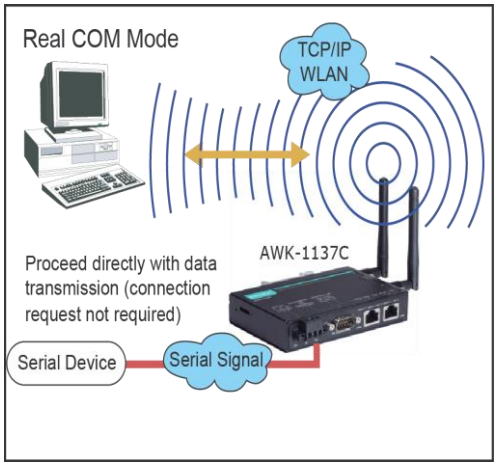
Mode

Along with the **Application** field, this field specifies the serial port's operation mode, or how it will interact with network devices. Depending on how the **Application** field is configured, different options are available for each **Mode**. And, depending on the mode that you configure, additional configuration settings will be displayed.

Setting	Description	Factory Default
Real COM	This serial port will operate in Real COM mode.	Real COM
RFC2217	This serial port will operate in RFC2217 mode.	
TCP Server	This serial port will operate in TCP Server mode.	
TCP Client	This serial port will operate in TCP Client mode.	
UDP	This serial port will operate in UDP mode.	

Real COM Mode

Real COM mode is designed to work with AWK drivers that are installed on a network host. COM drivers are provided for Windows systems, and TTY drivers are provided for Linux and UNIX systems. The driver establishes a transparent connection to the attached serial device by mapping a local serial port to the AWK-1137C serial port. Real COM mode supports up to four simultaneous connections, so multiple hosts can collect data from the attached device at the same time.



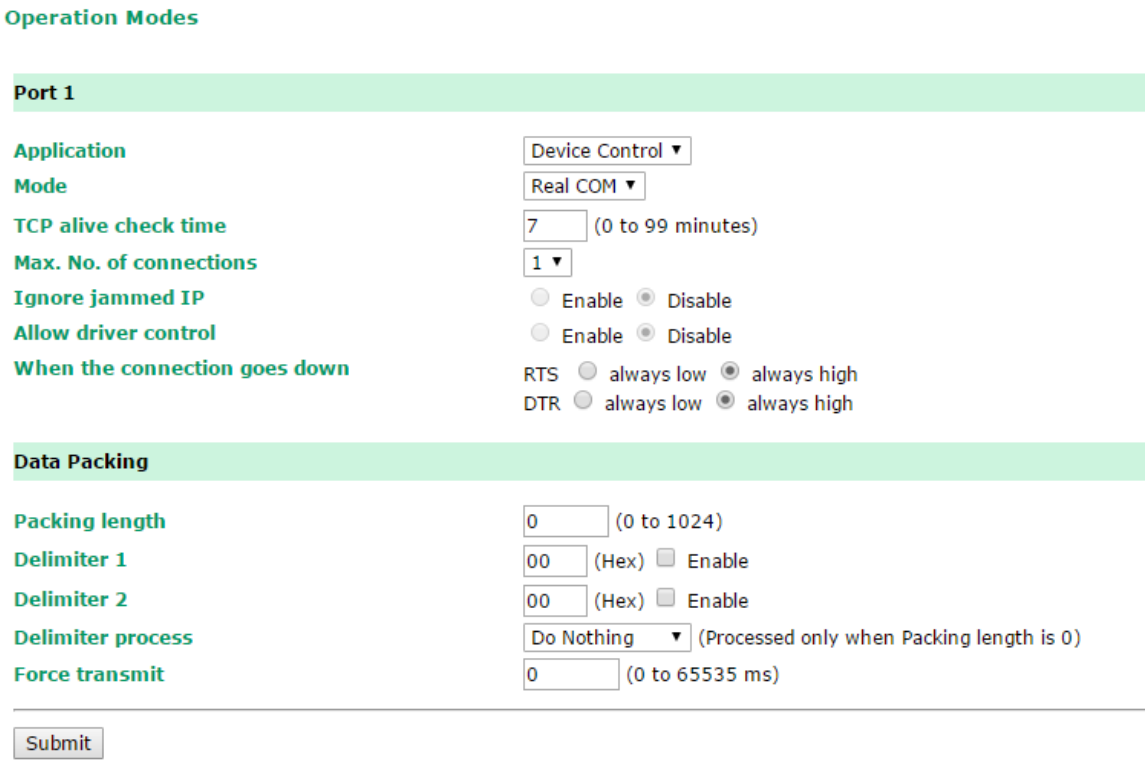
ATTENTION

Real COM drivers are installed and configured through NPort/OnCell Windows Driver Manager.

Real COM mode allows you to continue using your serial communications software to access devices that are now attached to your AWK-1137C. On the host, the AWK Real COM driver automatically intercepts data sent to the COM port, packs it into a TCP/IP packet, and redirects it to the network. At the other end of the connection, the AWK-1137C accepts the Ethernet frame, unpacks the TCP/IP packet, and sends the serial data to the appropriate device.

ATTENTION

In Real COM mode, two hosts can have simultaneous access control over the AWK-1137C serial port.



When **Mode** is set to Real COM on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Max. no. of connections**, and **Ignore jammed IP**.

TCP Alive Check Time

Setting	Description	Factory Default
0 to 99 min.	This field specifies how long the AWK-1137C will wait for a response to "keep alive" packets before closing the TCP connection. The AWK-1137C checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the AWK-1137C will force the existing TCP connection to close.	7 min.

Max no. of connections

This field specifies the maximum number of connections that will be accepted by the serial port.

Setting	Description	Factory Default
1 or 2	1: Only one specific host can access this serial port, and the Real COM driver on that host will have full control over the port. 2: This serial port will allow the two connections to be opened simultaneously. With simultaneous connections, the Real COM driver will only provide a pure data tunnel with no control ability. The serial communication will be determined by the AWK-1137C rather than by your application program. Application software that is based on the Real COM driver will receive a driver response of "success" when using any of the Win32 API functions. The AWK-1137C will send data only to the Real COM driver on the host. Data received from hosts will be sent to the attached serial device on a first-in- first-out basis.	1

ATTENTION

When **Max no. of connections** is 2, the serial port's communication settings (i.e., baudrate, parity, data bits, etc.) will be determined by the AWK-1137C. Any host that opens the COM port connection must use identical serial communication settings.

Ignore Jammed IP

This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port.

Setting	Description	Factory Default
Disable	All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded.	Disable
Enable	Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.	

Allow Driver Control

This field specifies how the port will proceed if driver control commands are received from multiple hosts that are connected to the port.

Setting	Description	Factory Default
Disable	Driver control commands will be ignored.	Disable
Enable	Control commands will be accepted, with the most recent command received taking precedence.	

When the Connection Goes Down

This field specifies what happens to the RTS signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS signals sent through the serial port.

Setting	Description	Factory Default
always low	The selected signal will change to low when the Ethernet connection goes down.	always high
always high	The selected signal will remain high when the Ethernet connection goes down.	

Packet Length

This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending.

Setting	Description	Factory Default
0 to 1024	0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.	0

Delimiter 1 and 2

These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence.

Setting	Description	Factory Default
Enable	When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter characters are received. For example, the	Unchecked

	carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level. The Delimiter value can be set ranging from 00 to FF.	

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

Delimiter Process

This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.

Setting	Description	Factory Default
Do Nothing	Data accumulated in the serial port's buffer will be packed, including delimiters.	Do Nothing
Delimiter + 1	One additional character must be received before the data in the serial port's buffer is packed.	
Delimiter + 2	Two additional characters must be received before the data in the serial port's buffer is packed.	
Strip Delimiter	Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.	

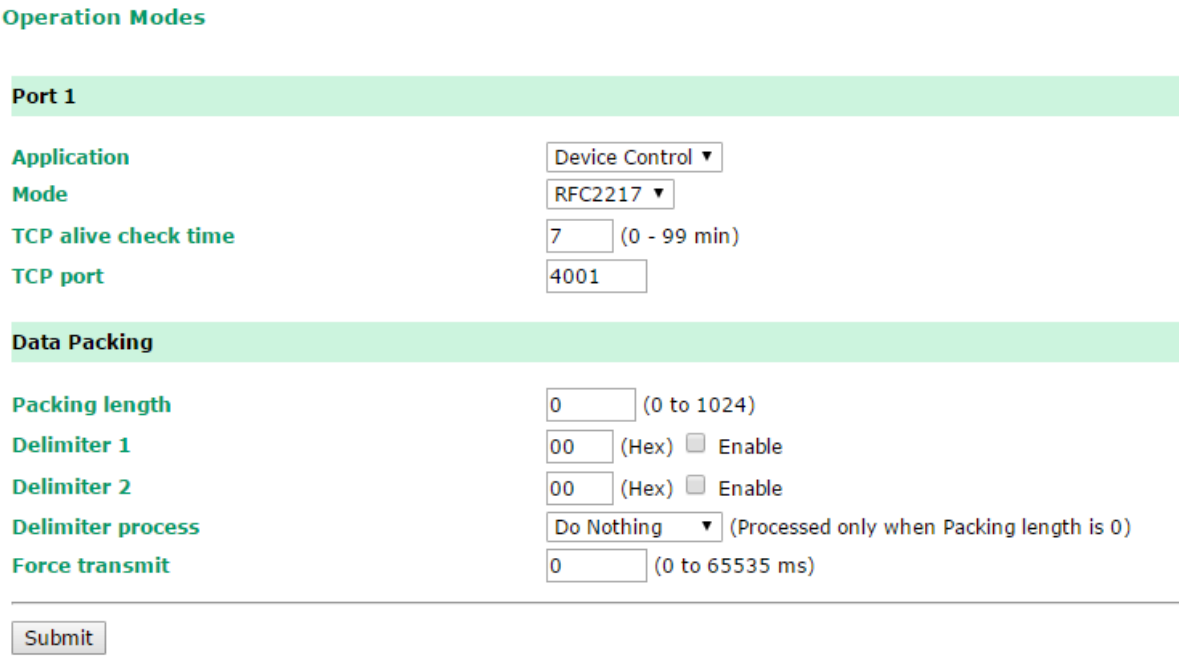
Force Transmit

This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted.

Setting	Description	Factory Default
0 to 65535	0: If serial data is received, setting this value to 0 means no data will be buffered and all data will be transmitted immediately as received. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time should be greater than 8.3 ms.	0 ms

RFC2217 Mode

RFC2217 mode is similar to Real COM mode, since it relies on a driver to transparently map a virtual COM port on a host computer to a serial port on the AWK-1137C. The RFC2217 standard defines general COM port control options based on the Telnet protocol and supports one connection at a time. Third party drivers supporting RFC2217 are widely available on the Internet and can be used to implement virtual COM mapping.



When **Mode** is set to RFC2217 on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **TCP port**, and **Packet length**.

TCP Alive Check Time

Setting	Description	Factory Default
0 to 99 min.	This field specifies how long the AWK will wait for a response to "keep alive" packets before closing the TCP connection. The AWK-1137C checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the AWK-1137C will force the existing TCP connection to close.	7 min.

TCP Port

Setting	Description	Factory Default
0 to 9999	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.	4001

Packet Length

Setting	Description	Factory Default
0 to 1024	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.	0

Delimiter 1 and 2

Setting	Description	Factory Default
Enable	When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the	Unchecked

	carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level. The Delimiter value can be set ranging from 00 to FF.	

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

Delimiter Process

This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.

Setting	Description	Factory Default
Do Nothing	Data accumulated in the serial port's buffer will be packed, including delimiters.	Do Nothing
Delimiter + 1	One additional character must be received before the data in the serial port's buffer is packed.	
Delimiter + 2	Two additional characters must be received before the data in the serial port's buffer is packed.	
Strip Delimiter	Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.	

Force Transmit

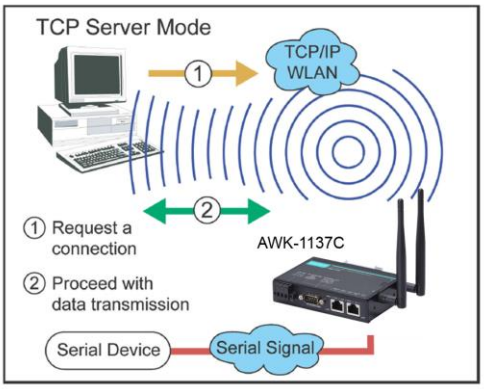
Setting	Description	Factory Default
0 to 65535	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is received, setting this value to 0 means no data will be buffered and all data will be transmitted immediately as received. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.	0 ms

TCP Server Mode

In TCP Server mode, the AWK-1137C serial port is assigned an IP port address that is unique on your TCP/IP network. It waits for the host computer to establish a connection to the attached serial device. This operation mode also supports up to four simultaneous connections, so multiple hosts can collect data from the attached device at the same time.

Data transmission proceeds as follows:

1. A host requests a connection to the AWK-1137C serial port.
2. Once the connection is established, data can be transmitted in both directions—from the host to the device, and from the device to the host.



Operation Modes

Port 1

Application	Socket
Mode	TCP Server
TCP alive check time	7 (0 to 99 minutes)
Max. No. of connections	1
Ignore jammed IP	Enable Disable
Allow driver control	Enable Disable
Inactivity time	0 (0 - 65535 ms)
TCP port	4001
Cmd port	966
When the connection goes down	RTS always low always high DTR always low always high

Data Packing

Packing length	0 (0 to 1024)
Delimiter 1	00 (Hex) Enable
Delimiter 2	00 (Hex) Enable
Delimiter process	Do Nothing (Processed only when Packing length is 0)
Force transmit	0 (0 to 65535 ms)

Submit

When **Mode** is set to **TCP Server** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, and **Max connection**.

TCP Alive Check Time

Setting	Description	Factory Default
0 to 99 min.	This field specifies how long the AWK-1137C will wait for a response to "keep alive" packets before closing the TCP connection. The AWK-1137C checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no	7 min.

	response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the AWK will force the existing TCP connection to close.	

Inactivity Time

Setting	Description	Factory Default
0 to 65535 ms	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, make sure that it is greater than the Force transmit time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted.	0 ms

Max No. of connection

Setting	Description	Factory Default
1 to 2	This field specifies the maximum number of connections that will be accepted by the serial port. 1: Only a single host may open the TCP connection to the serial port. 2: This serial port will allow the specified number of connections to be opened simultaneously. When multiple connections are established, serial data will be duplicated and sent to all connected hosts. Data from hosts will be sent to the attached serial device on a first-in-first-out basis.	1

Ignore Jammed IP

This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port.

Setting	Description	Factory Default
Disable	All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded.	Disable
Enable	Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.	

Allow Driver Control

This field specifies how the port will proceed if driver control commands are received from multiple hosts that are connected to the port.

Setting	Description	Factory Default
Disable	Driver control commands will be ignored.	Disable
Enable	Control commands will be accepted, with the most recent command received taking precedence.	

TCP Port

Setting	Description	Factory Default
0 to 9999	This field specifies the TCP port number that the serial port will use to listen to connections, and that other devices must use to contact the serial port.	4001

Cmd Port

Setting	Description	Factory Default
0 to 9999	This field specifies the TCP port number for listening to SSDK commands from the host.	966

When the connection goes down

This field specifies what happens to the RTS signals when the Ethernet connection goes down. For some applications, serial devices need to know the Ethernet link status through RTS signals sent through the serial port.

Setting	Description	Factory Default
always low	The selected signal will change to low when the Ethernet connection goes down.	always high
always high	The selected signal will remain high when the Ethernet connection goes down.	

Packet Length

Setting	Description	Factory Default
0 to 1024	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.	0

Delimiter 1 and 2

Setting	Description	Factory Default
Enable	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.	Unchecked

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

Delimiter Process

This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.

Setting	Description	Factory Default
Do Nothing	Data accumulated in the serial port's buffer will be packed, including delimiters.	Do Nothing
Delimiter + 1	One additional character must be received before the data in the serial port's buffer is packed.	
Delimiter + 2	Two additional characters must be received before the data in	

	the serial port's buffer is packed.	
Strip Delimiter	Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.	

Force Transmit

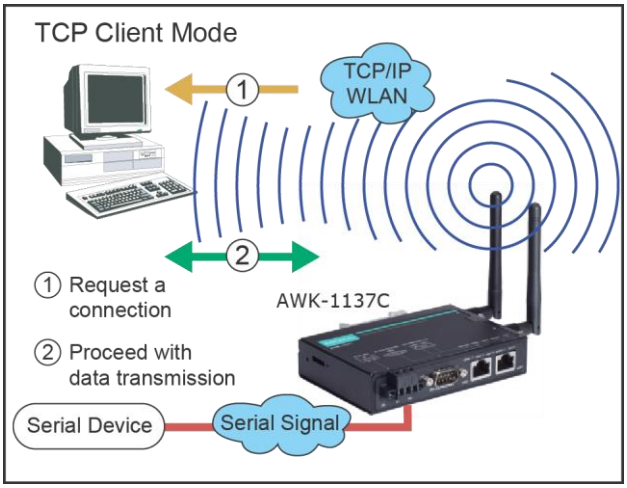
Setting	Description	Factory Default
0 to 65535	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is received, setting this value to 0 means no data will be buffered and all data will be transmitted immediately as received. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.	0 ms

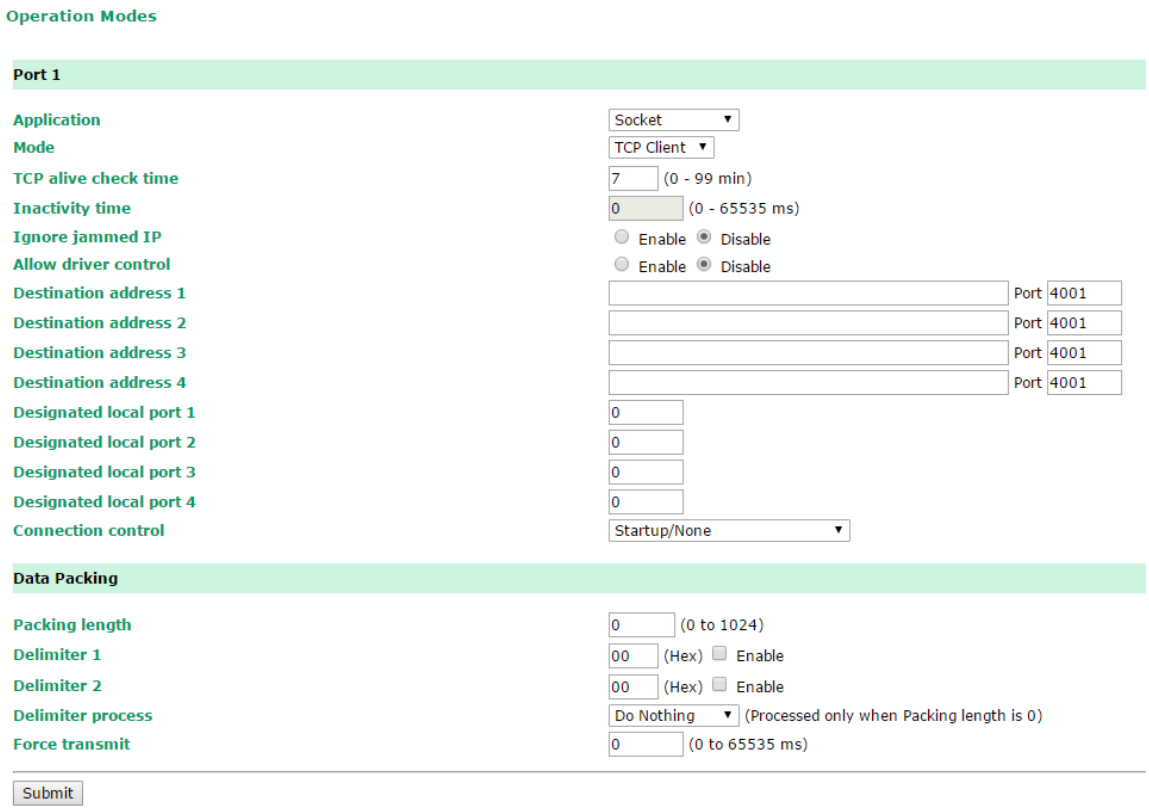
TCP Client Mode

In TCP Client mode, the AWK-1137C actively establishes a TCP connection to a specific network host when data is received from the attached serial device. After the data has been transferred, the AWK-1137C can automatically disconnect from the host computer through the **Inactivity time** settings.

Data transmission proceeds as follows:

1. The AWK-1137C requests a connection from the host.
2. The connection is established and data can be transmitted in both directions between the host and device.





When **Mode** is set to **TCP Client** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **TCP alive check time**, **Inactivity time**, and **Ignore jammed IP**.

TCP Alive Check Time

Setting	Description	Factory Default
0 to 99 min.	This field specifies how long the AWK-1137C will wait for a response to "keep alive" packets before closing the TCP connection. The AWK-1137C checks connection status by sending periodic "keep alive" packets. 0: The TCP connection will remain open even if there is no response to the "keep alive" packets. 1 to 99: If the remote host does not respond to the packet within the specified time, the AWK-1137C will force the existing TCP connection to close.	7 min.

Inactivity Time

Setting	Description	Factory Default
0 to 65535 ms	This field specifies the time limit for keeping the connection open if no data flows to or from the serial device. 0: The connection will remain open even if data is never received. For many applications, the serial device may be idle for long periods of time, so 0 is an appropriate setting. 1 to 65535: If there is no activity for the specified time, the connection will be closed. When adjusting this field, make sure that it is greater than the Force transmit time. Otherwise, the TCP connection may be closed before data in the buffer can be transmitted. **Connection Control** must be set to "Any character/Inactivity time" for this setting to have effect.	0 ms

Ignore Jammed IP

Setting	Description	Factory Default
Disable	All transmission will be suspended if one IP address becomes unresponsive. Transmission will only resume when all hosts have responded.	Disable
Enable	Data transmission to the other hosts will not be suspended if one IP address becomes unresponsive.	

This field specifies how an unresponsive IP address is handled when there are simultaneous connections to the serial port.

Destination Address 1 to 4

Setting	Description	Factory Default
IP address and port (e.g., "192.168.1.1" and "4001")	This field specifies the remote host(s) that will access the attached device. At least one destination must be provided. This field supports the use of domain names and names defined in the host table.	IP Address: Empty Port: 4001

ATTENTION

In TCP Client mode, up to 4 connections can be established between the serial port and TCP hosts. The connection speed or throughput may be low if any one of the four connections is slow, since the one slow connection will slow down the other 3 connections.

Designated Local Port 1 to 4

Setting	Description	Factory Default
1 to 65535	This field specifies the TCP port number that will be used for data transmission with the serial port.	0

Connection Control

This field specifies how connections to the device are established and closed.

Setting	Description	Factory Default
Startup/None	The connection will be opened as the AWK-1137C starts up. The connection will only be closed manually.	Startup/None
Any Character/None	The connection will be opened as soon as a character is received from the attached device. The connection will only be closed manually.	
Any Character/ Inactivity Time	The connection will be opened as soon as a character is received from the attached device. The connection will be closed if no data is received for the time specified in Inactivity time.	
DSR on/DSR off	The TCP connection is opened when the DSR signal is on, and closed when the DSR signal is off.	
DSR on/None	The TCP connection is opened when the DSR signal is on. The connection will only be closed manually.	
DCD On/DCD Off	The TCP connection is opened when the DCD (data carrier detect) signal is on, and closed when the DCD signal is off.	
DCD On/None	The TCP connection is opened when the DCD signal is on. The connection will only be closed manually.	

Packet Length

Setting	Description	Factory Default
0 to 1024	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be	0

	sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.	

Delimiter 1 and 2

Setting	Description	Factory Default
Enable	These fields are used to define special delimiter character(s) for data packing. Enable Delimiter 1 to control data packing with a single character; enable both Delimiter 1 and 2 to control data packing with two characters received in sequence. When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level.	Unchecked

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

Delimiter Process

This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.

Setting	Description	Factory Default
Do Nothing	Data accumulated in the serial port's buffer will be packed, including delimiters.	Do Nothing
Delimiter + 1	One additional character must be received before the data in the serial port's buffer is packed.	
Delimiter + 2	Two additional characters must be received before the data in the serial port's buffer is packed.	
Strip Delimiter	Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.	

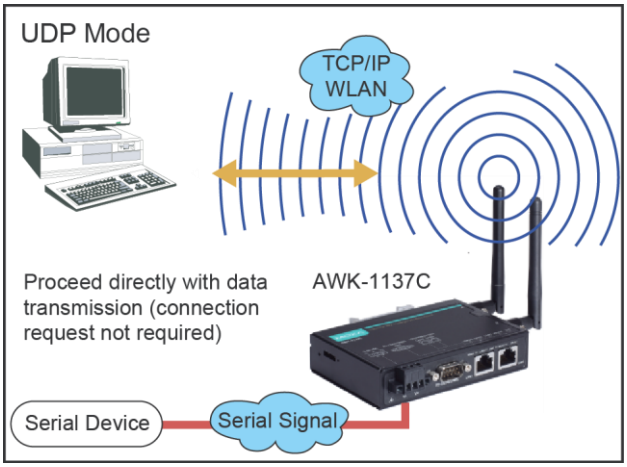
Force Transmit

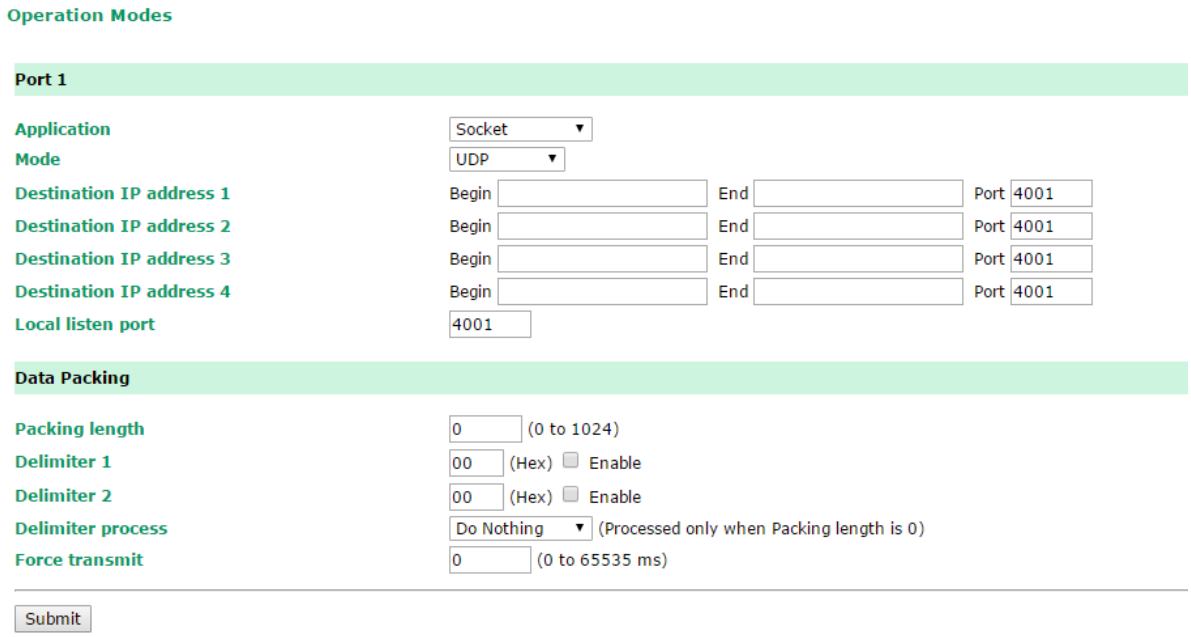
Setting	Description	Factory Default
0 to 65535	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is received, setting this value to 0 means no data will be buffered and all data will be transmitted immediately as received. 1 to 65535: If serial data is not received for the specified amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of	0 ms

	bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.	

UDP Mode

UDP is similar to TCP but is faster and more efficient. Data can be broadcast to or received from multiple network hosts. However, UDP does not support verification of data and would not be suitable for applications where data integrity is critical. It is ideal for message display applications.





When **Mode** is set to **UDP** on a serial port's **Operation Modes** page, you will be able to configure additional settings such as **Destination address 1** through **4**, **Local listen port**, and **Packet length**.

Destination Address 1 to 4

Setting	Description	Factory Default
IP address range and port (e.g., "192.168.1.1" to "192.168.1.64" and "4001")	In UDP mode, you may specify up to 4 ranges of IP addresses for the serial port to connect to. At least one destination range must be provided. The maximum selectable IP address range is 64 addresses. However, you can enter multicast addresses in the Begin field, in the form xxx.xxx.xxx.255. For example, enter "192.127.168.255" to allow the AWK-1137C to broadcast UDP packets.	Begin: Empty End: Empty Port: 4001

Local Listen Port

Setting	Description	Factory Default

0 to 9999	This field specifies the UDP port that the AWK-1137C listens to and that other devices must use to contact the attached serial device.	4001

Packet Length

Setting	Description	Factory Default
0 to 1024	This field specifies the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0: Packet length is disregarded and data in the buffer will be sent as specified by the delimiter settings or when the buffer is full. 1 to 1024: Data in the buffer will be sent as soon it reaches the specified length.	0

Delimiter 1 and 2

Setting	Description	Factory Default
Enable	When these fields are enabled, serial data will accumulate in the serial port's buffer until the buffer is full or until the specified delimiter character(s) are received. For example, the carriage return character could be used as a delimiter in order to transmit each sentence or paragraph in a separate packet. Data will be packed according to Delimiter process. Delimiters must be incorporated into the data stream at the software or device level. The Delimiter value can be set ranging from 00 to FF.	Unchecked

ATTENTION

When **Delimiter 1** is enabled, **Packet length** must be set to 0.

Delimiter Process

This field specifies how data is packed when delimiter characters are received. This field has no effect if Delimiter 1 is not enabled.

Setting	Description	Factory Default
Do Nothing	Data accumulated in the serial port's buffer will be packed, including delimiters.	Do Nothing
Delimiter + 1	One additional character must be received before the data in the serial port's buffer is packed.	
Delimiter + 2	Two additional characters must be received before the data in the serial port's buffer is packed.	
Strip Delimiter	Data accumulated in the serial port's buffer will be packed, but the delimiter character(s) will be stripped from the data.	

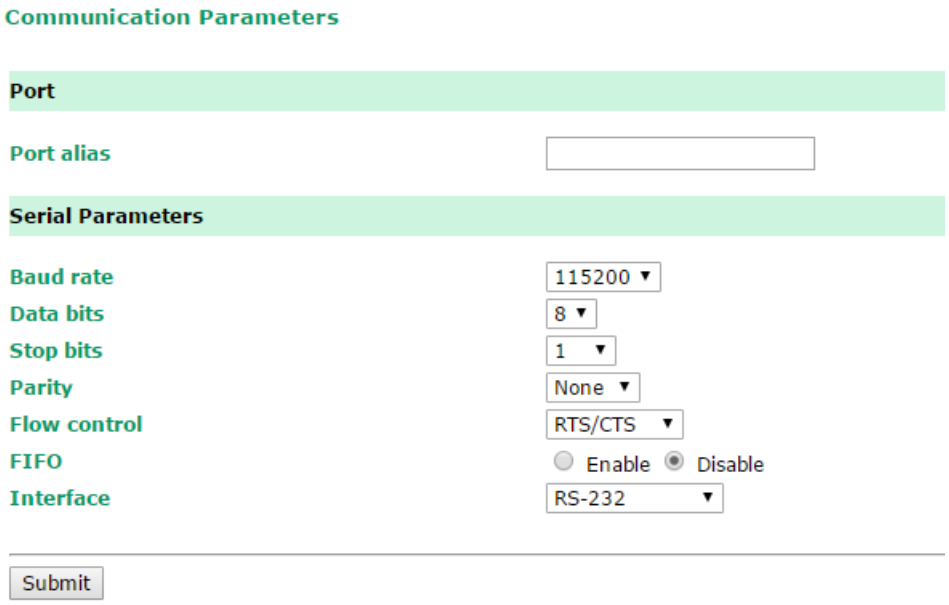
Force Transmit

Setting	Description	Factory Default
0 to 65535	This field controls data packing by the amount of time that elapses between bits of data. When using this field, make sure that Inactivity time is disabled or set to a larger value. Otherwise the connection may be closed before the data in the buffer can be transmitted. 0: If serial data is received, setting this value to 0 means no data will be buffered and all data will be transmitted immediately as received. 1 to 65535: If serial data is not received for the specified	0 ms

Setting	Description	Factory Default
	amount of time, the data that is currently in the buffer will be packed for network transmission. The optimal force transmit time depends on your application, but it must be at least larger than one character interval within the specified baudrate. For example, assume that the serial port is set to 1200 bps, 8 data bits, 1 stop bit, and no parity. In this case, the total number of bits needed to send a character is 10 bits, and the time required to transfer one character is 8.3 ms, so the force transmit time to be larger than 8.3 ms.	

Communication Parameters

The **Communication Parameters** page for the serial port is where serial communication settings are specified, such as **Baud rate**, **Data bits**, and **Stop bits**.



The **Communication Parameters** page for the serial port is where serial communication settings are specified, such as **Baud rate**, **Data bits**, and **Stop bits**.

Port Alias

Setting	Description	Factory Default
free text (e.g., "Secondary console connection")	This is an optional free text field to help you differentiate one serial port from another. It does not affect operation of the AWK-1137C.	

ATTENTION

Serial communication settings should match the attached serial device. Check the communication settings in the user's manual for your serial device.

Baud Rate

Setting	Description	Factory Default
75, 110, 134, 150, 300, 600, 1200, 1800, 2400, 4800, 7200, 9600, 19200, 38400, 57600,	This field specifies the baudrate for the serial port. 75 to 921600: The serial port will operate at the specified baudrate.	115200

115200, 230400, 460800, 921600		

Data Bits

Setting	Description	Factory Default
5, 6, 7, 8	This field specifies the number of data bits used to encode each character of data.	8

Stop Bits

Setting	Description	Factory Default
1, 1.5, 2	This field specifies the number of stop bits used for each character frame.	1

Parity

Setting	Description	Factory Default
None, Odd, Even, Space, Mark	This field specifies the type of parity bit used for each character frame.	None

Flow Control

Setting	Description	Factory Default
None, RTS/CTS, XON/XOFF	This field specifies the type of flow control used by the serial port.	RTS/CTS

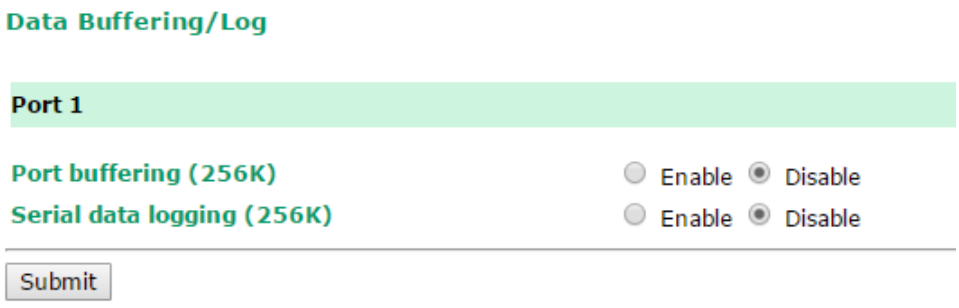
FIFO

Setting	Description	Factory Default
Enable, Disable	This field specifies whether the serial port will use the built-in FIFO. A 128-byte FIFO is provided to each serial port for both Tx and Rx directions. To prevent data loss during serial communication, this should be set to Disable if the attached serial device does not have a FIFO.	Disable

Interface

Setting	Description	Factory Default
RS-232, RS-422, RS-485 2-wire, RS-485 4-wire	This field specifies the type of interface the serial port will use.	RS-232

Data Buffering/Log



On the serial port's **Data Buffering/Log** page, you can enable or disable **Port buffering** and **Serial data logging**.

Port Buffering

Setting	Description	Factory Default
Enable, Disable	This field specifies whether the serial port will use port buffering. Port buffering can be used in Real COM mode, TCP Server mode, and TCP Client mode. For other modes, the port buffering settings will have no effect.	Disable

Serial Data Logging

Setting	Description	Factory Default
Enable, Disable	This field specifies whether data logs for the serial port will be stored on system RAM. Each serial port is allotted 256 KB for data logging. The data log is not saved when the AWK-1137C is powered off.	Disable

Advanced Setup

Several advanced functions are available to increase the functionality of your AWK-1137C 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, AWK-1137C's SNMP support can make network management easier.

Using Virtual LAN

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

The Virtual LAN (VLAN) Concept

What is a VLAN?

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

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

Benefits of VLANs

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

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

VLAN Workgroups and Traffic Management

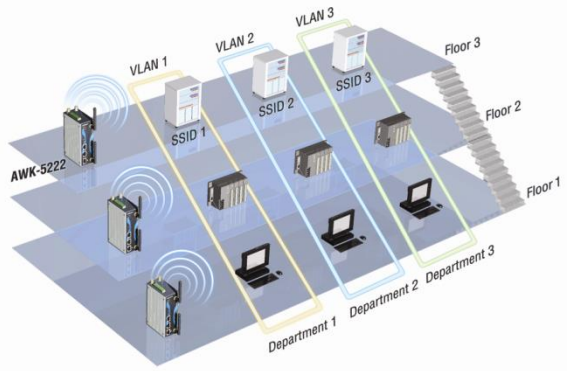
The AP assigns clients to a VLAN based on a Network Name (SSID). The AP can support up to 9 SSIDs per radio interface, with a unique VLAN configurable per SSID.

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

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

In this scenario, the AP would assign every packet it accepted to a VLAN. Each packet would then be identified as marketing or human resource, depending on which wireless client received it. The AP would insert VLAN headers or "tags" with identifiers into the packets transmitted on the wired backbone to a network switch.

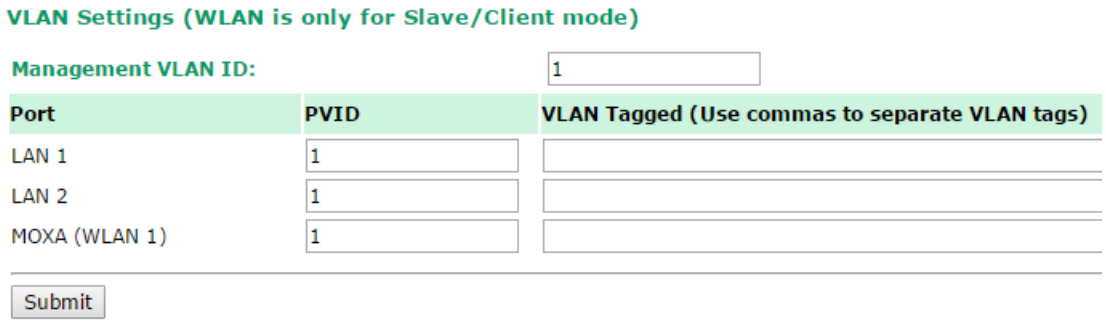
Finally, the switch would be configured to route packets from the marketing department to the appropriate corporate resources such as printers and servers. Packets from the human resource department could be restricted to a gateway that allowed access to only the Internet. A member of the human resource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



Configuring Virtual LAN

VLAN Settings

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



Management VLAN ID

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

Port

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

Port PVID

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

VLAN Tagged

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

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

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.

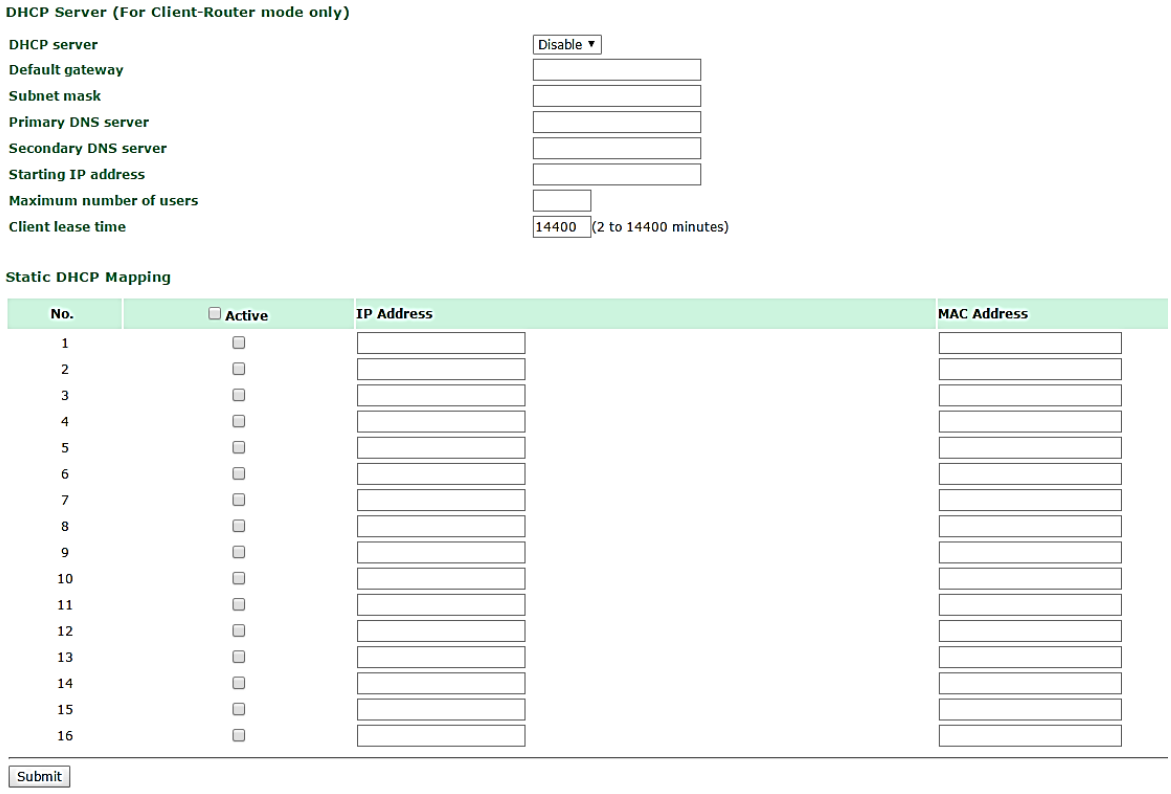
DHCP Server (for Client-Router mode only)

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

The AWK-1137C 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-1137C provides a **Static DHCP mapping** list with up to 16 entities. Be reminded to check the **Active** check box for each entity to activate the setting.

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



DHCP server

Setting	Description	Factory Default

Enable	Enables AWK-1137C as a DHCP server	Disable
Disable	Disable DHCP server function	

Default gateway

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

Subnet mask

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

Primary/ Secondary DNS server

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

Start IP address

Setting	Description	Factory Default
IP address	Indicates the IP address which AWK-1137C can start assigning	None

Maximum number of users

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

Client lease time

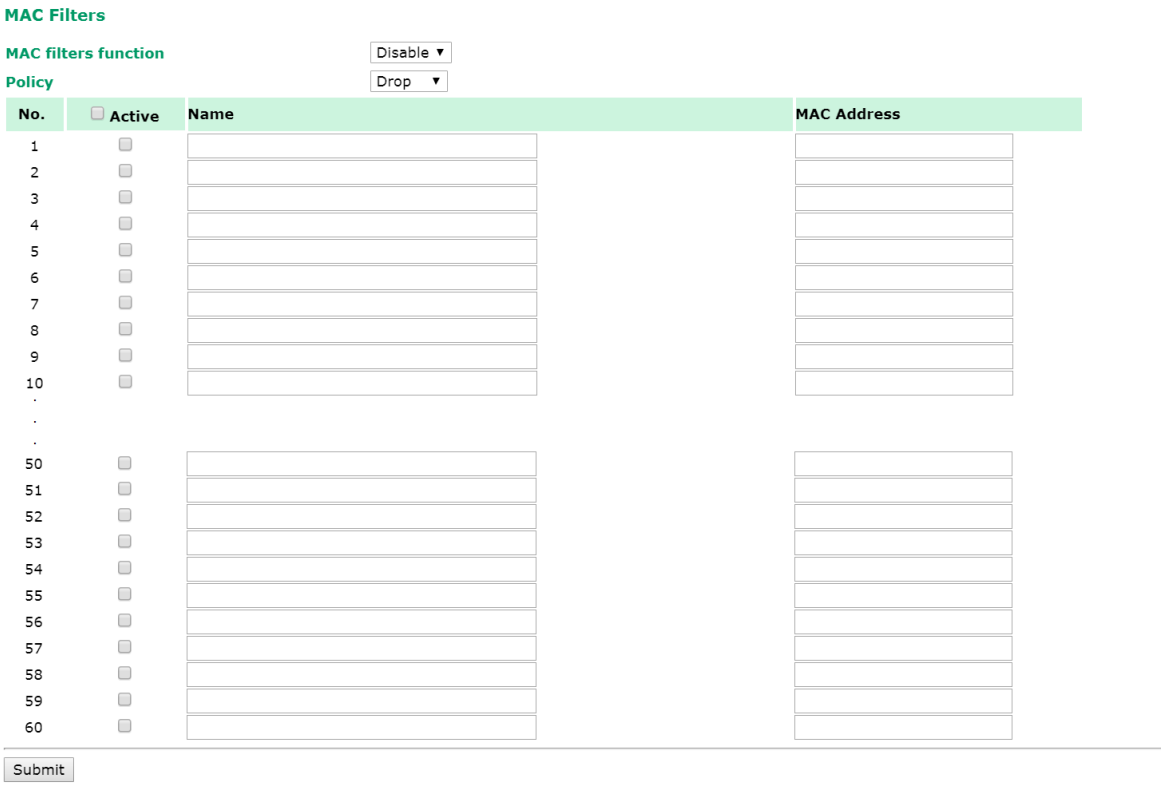
Setting	Description	Factory Default
2 to 14400 minutes	The lease time for which an IP address is assigned. The IP address may go expired after the lease time is reached.	14400 minutes (10 days)

Packet Filters

The AWK-1137C includes various filters for **IP-based** packets going through LAN and WLAN interfaces. You can set these filters as a firewall to help enhance network security.

MAC Filters

The AWK-1137C's MAC filter is a policy-based filter that can allow or filter out IP-based packets with specified MAC addresses. The AWK-1137C provides 60 entities for setting MAC addresses in your filtering policy. Remember to check the **Active** check box for each entity to activate the setting.



MAC filters

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

Policy

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

ATTENTION

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

IP Protocol Filters

The AWK-1137C's IP protocol filter is a policy-based filter that can allow or filter out IP-based packets with specified IP protocol and source/destination IP addresses.

The AWK-1137C provides 60 entities for setting IP protocol and source/destination IP addresses in your filtering policy. Four IP protocols are available: **All**, **ICMP**, **TCP**, and **UDP**. You must specify either the Source IP or the Destination IP. By combining IP addresses and netmasks, you can specify a single IP address or a range of IP addresses to accept or drop. For example, "IP address 192.168.1.1 and netmask 255.255.255.255" refers to the sole IP address 192.168.1.1. "IP address 192.168.1.1 and netmask 255.255.255.0" refers to the range of IP addresses from 192.168.1.1 to 192.168.255. Remember to check the **Active** check box for each entity to activate the setting.

IP protocol filters

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

Policy

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

ATTENTION

Be careful when you enable the filter function:

Drop + "no entity on list is activated" = all packets are **allowed.**

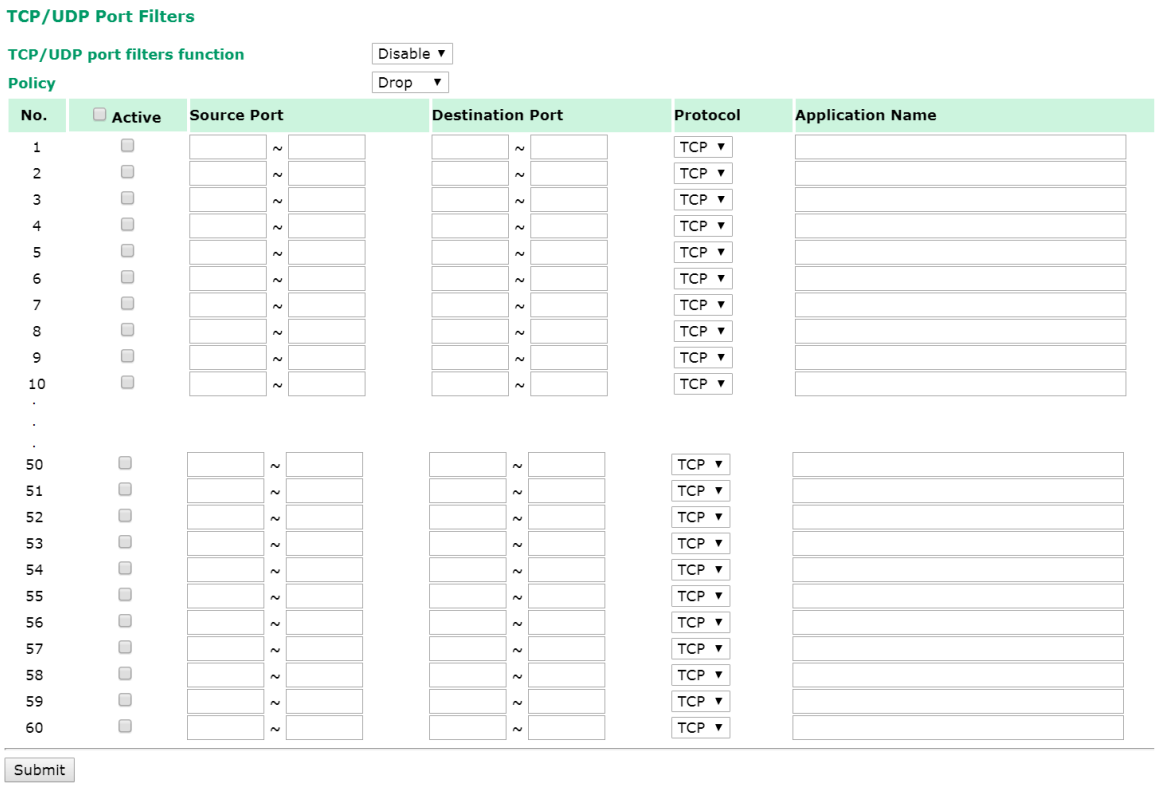
Accept + "no entity on list is activated" = all packets are **denied.**

TCP/UDP Port Filters

The AWK-1137C'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-1137C provides 60 entities for setting the range of source/destination ports of a specific protocol. In addition to selecting TCP or UDP protocol, you can set either the source port, destination port, or both. The end port can be left empty if only a single port is specified. Of course, the end port cannot be larger than the start port.

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



TCP/UDP port filters

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

Policy

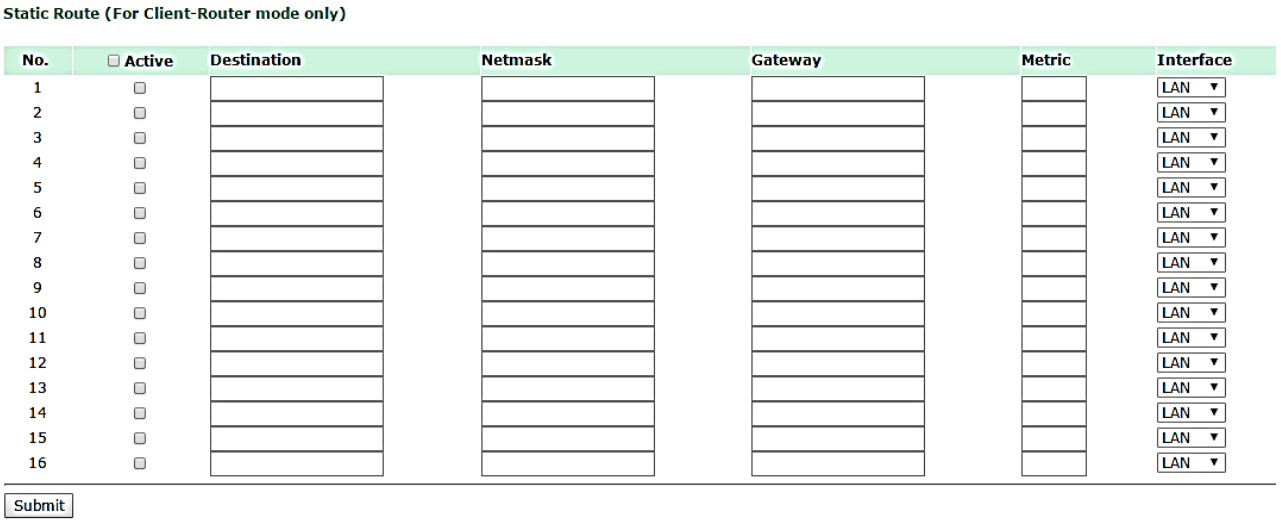
Setting	Description	Factory Default
Accept	Only the packets fitting the entities on list can be allowed.	Accept
Drop	Any packet fitting the entities on list will be denied.	

ATTENTION

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

Static Route (for Client-router mode only)

The Static Route page is used to configure the AWK-1137C's static routing table.



Active

Click the checkbox to enable Static Routing.

Destination

Specifies the destination IP address.

Netmask

Specifies the subnet mask for this IP address.

Gateway

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

Metric

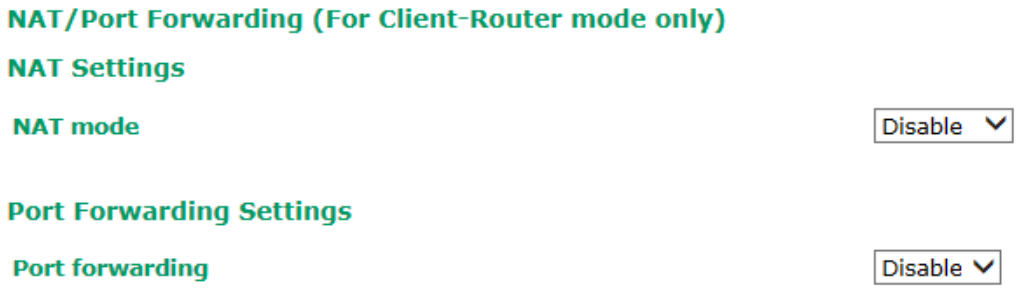
Specifies a "cost" for accessing the neighboring network.

Interface

Specifies the designated network interface for this routing rule.

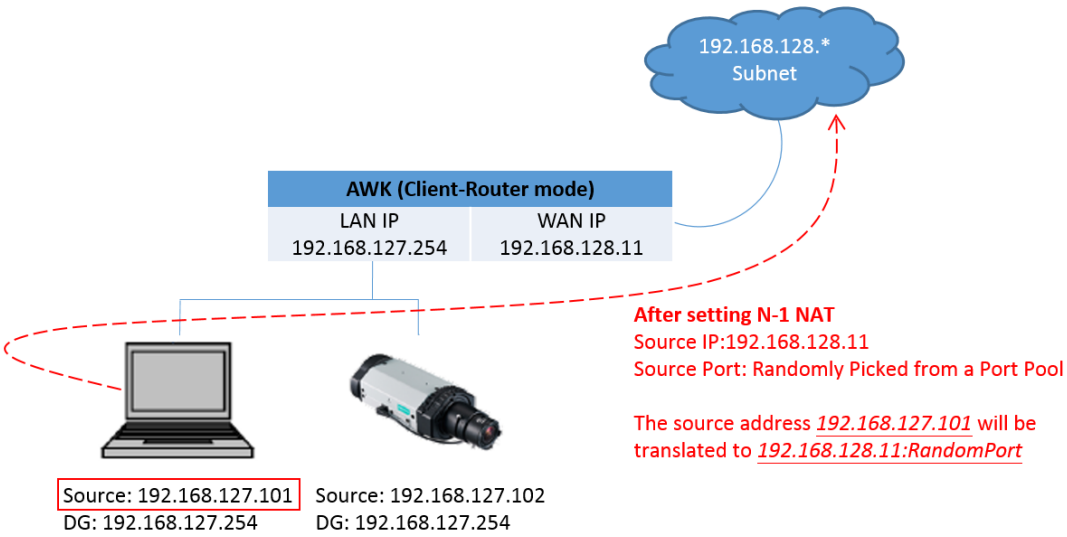
NAT Settings/Port Forwarding (for Client-router mode only)

Network Address Translation (NAT) and Port Forwarding are supported by the AWK-1137C to facilitate the Client-Router operation mode. This feature translates the outgoing communication from private IPs to external IPs (WAN IP).

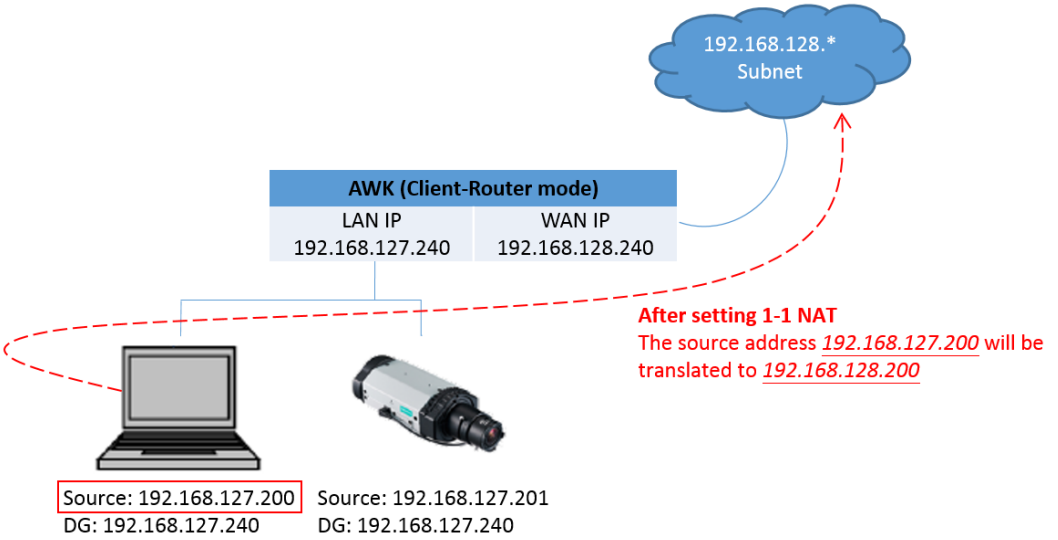


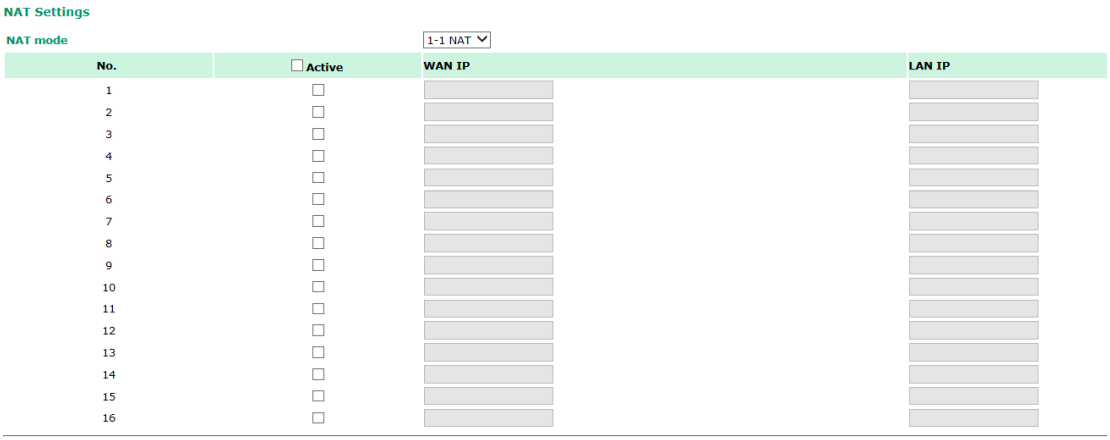
Setting	Description	Factory Default
NAT mode	Enable (N-1 NAT or 1-1 NAT) or disable the NAT mode.	Disable
Port Forwarding	Enable or disable the port forwarding function	Disable

N-1 NAT



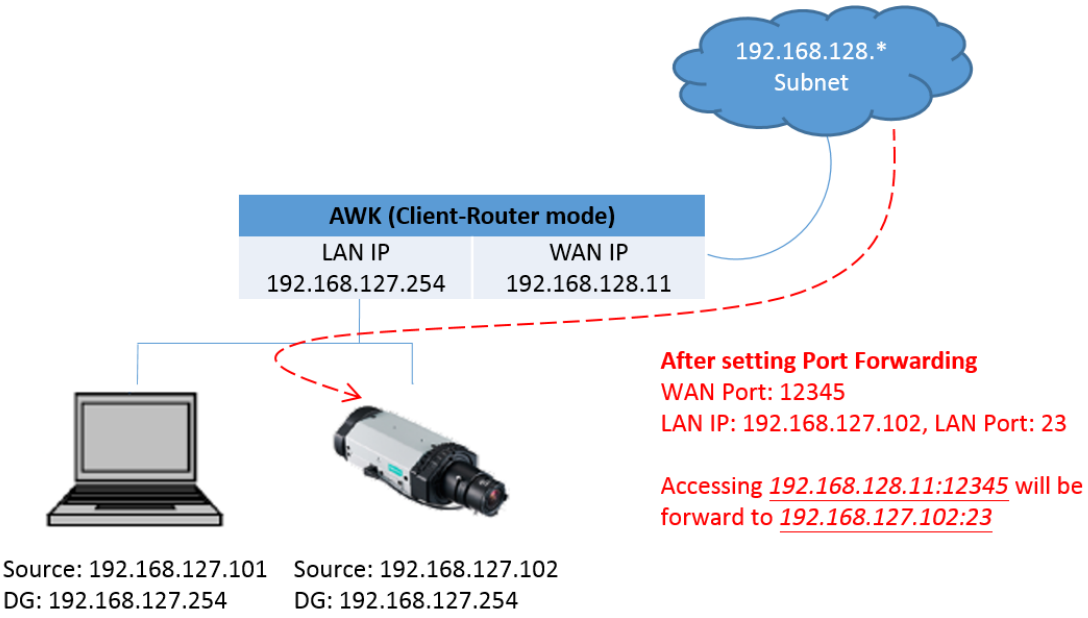
1-1 NAT

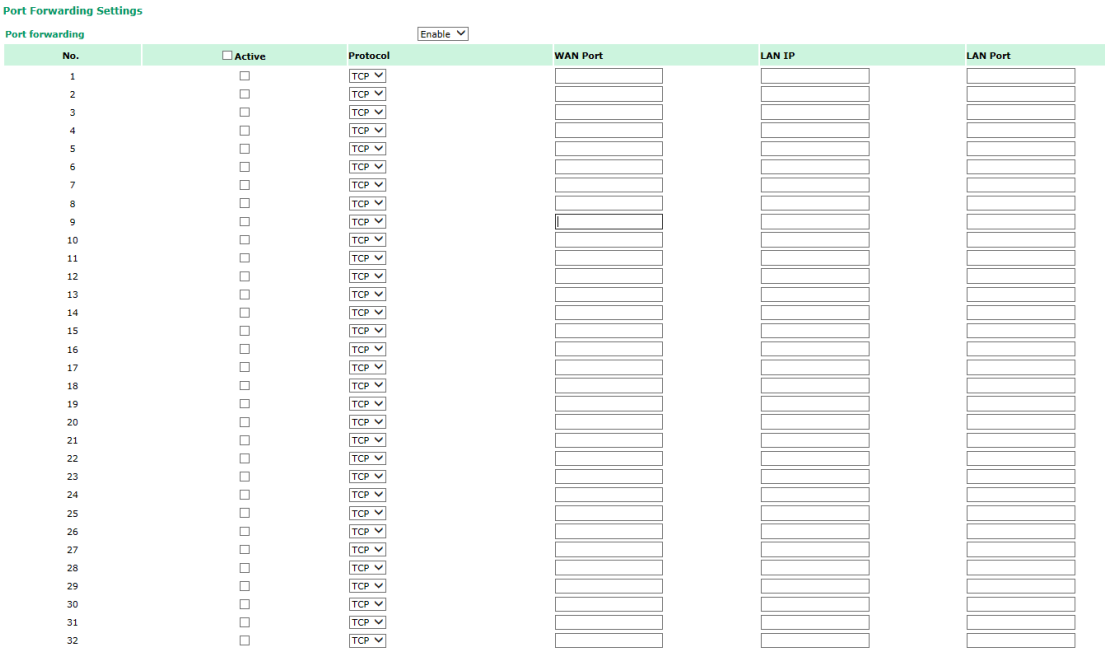




Setting	Description
Active	Click the checkbox to enable 1-1 NAT
WAN IP	Specifies the "forward to" WAN IP
LAN IP	Specifies the "forward to" LAN IP

Port Forwarding





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

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

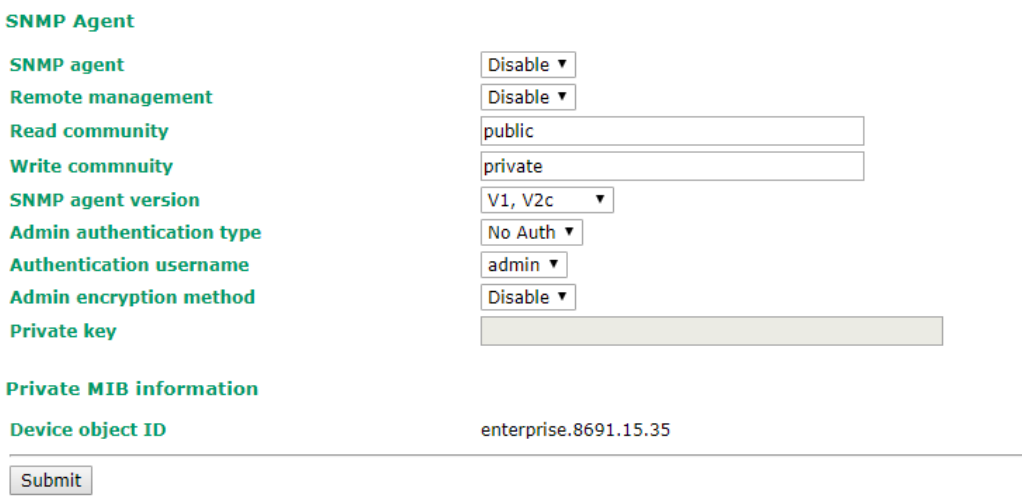
SNMP Agent

The AWK-1137C supports SNMP V1/V2c/V3. SNMP V1 and SNMP V2c use a community string match for authentication, which means that SNMP servers access all objects with read-only or read/write permissions using the community string *public*/*private* (default value). SNMP V3, which requires you to select an authentication level of MD5 or SHA, is the most secure protocol. You can also enable data encryption to enhance data security.

SNMP security modes and security levels supported by the AWK-1137C are shown in the following table. Select the security mode and level that will be used to communicate between the SNMP agent and manager.

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

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



SNMP agent

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

Remote management

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

Read community (for V1, V2c)

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

Write community (for V1, V2c)

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

SNMP agent version

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

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

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

Authentication username: Determines one account setting among eight possible accounts as SNMP authentication account setting when authentication type is MD5/SHA.

Admin private key (for V1, V2, 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

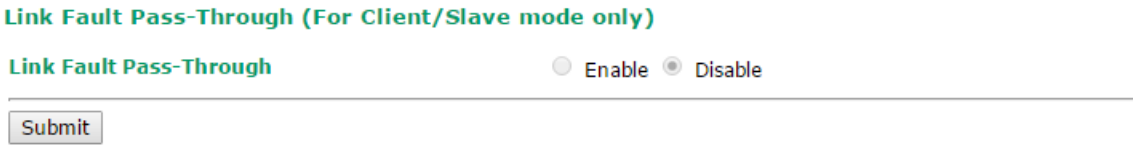
Also known as ***OID,*** this is the AWK-1137C's enterprise value. It is fixed.

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

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

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

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



Link Fault Pass-Through

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

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

Logs and Notifications

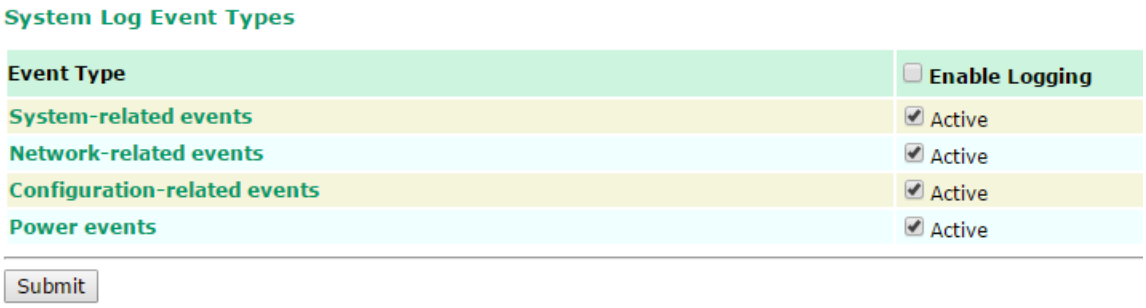
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system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

In addition to logging these events, the AWK-1137C supports different approaches to warn engineers automatically, such as SNMP trap, e-mail, and relay output. It also supports two digital inputs to integrate sensors into your system to automate alarms by email and relay output.

System Logs

System Log Event Types

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



System-related events	Event is triggered when…
System warm start	The AWK-1137C is rebooted, such as when its settings are changed (IP address, subnet mask, etc.).
System cold start	The AWK-1137C is rebooted by power down.
Watchdog triggers reboot	The AWK-1137C is rebooted by watchdog .
Network-related events	**Event is triggered when…**
LAN link on	The LAN port is connected to a device or network.
LAN link off	The port is disconnected (e.g., the cable is pulled out, or the opposing device shuts down).

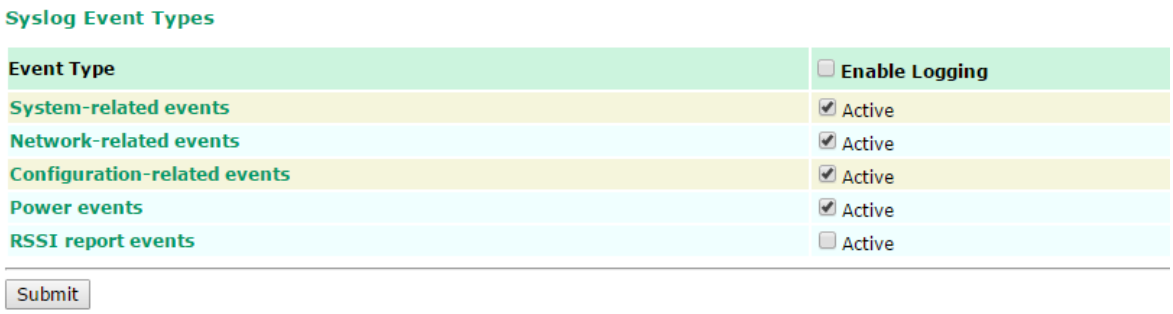
WLAN connected to AP (for Client/Slave mode)	The AWK-1137C is associated with an AP.
WLAN disconnected (for Client/Slave mode)	The AWK-1137C is disassociated from an AP.
Client Roaming from previous AP to current AP (for Client/Slave mode)	A client roams from a previous AP to the current AP if the signal strength of the current AP is greater than the previous AP by a certain value.
IP address conflict	The AWK-1137C has the same IP address as another device connected to the same subnet.
Link fault pass-through LAN/WLAN connected because of WLAN/LAN up	The WLAN/LAN link is up and the Link fault pass-through (LFPT) enables the LAN/WLAN functionality.
Link fault pass-through LAN/WLAN disconnected because of WLAN/LAN down	The WLAN/LAN link is down and the Link fault pass-through (LFPT) disables the LAN/WLAN functionality.
Configuration-related events	**Event is triggered when…**
Configuration Changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the AWK-1137C.
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The AWK-1137C's firmware is updated.
Configuration reset to default	The configuration is reset to factory default.
Power events	**Event is triggered when…**
Power transition (On -> Off)	The AWK-1137C is powered down
Power transition (Off -> On)	The AWK-1137C is powered.

Syslog

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

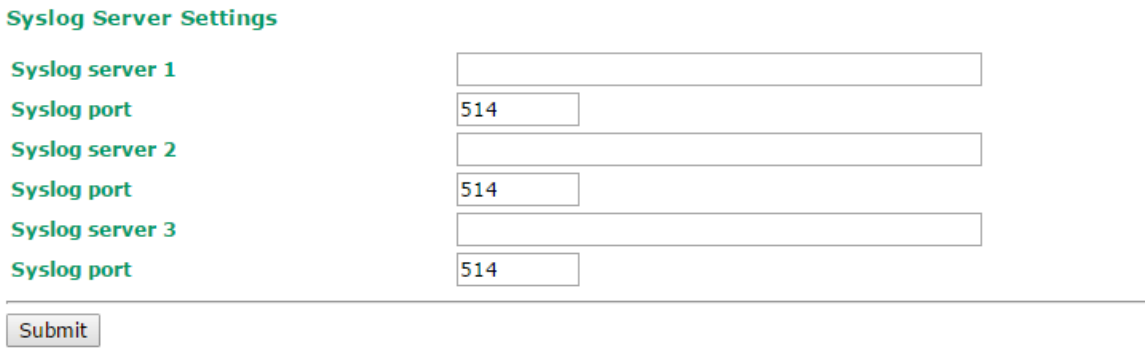
Syslog Event Types

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



Syslog Server Settings

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



Syslog server 1/ 2/ 3

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

Syslog port

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

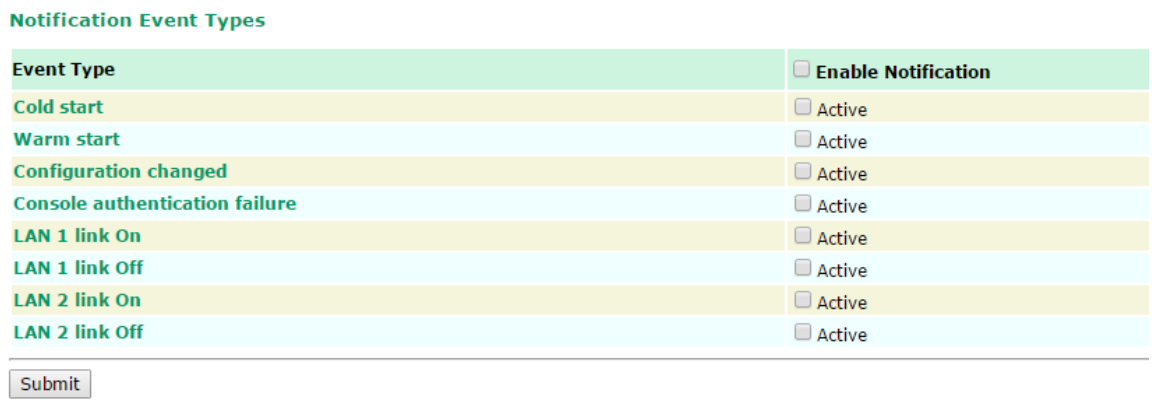
NOTE

- The event type, **RSSI report events** is useful during the site survey stage and uses a special utility to draw values from the device RSSI tables. However, this function increases the network traffic load. Hence, we recommend setting this function to **disable** during normal operations.
- You will have to stop the communication traffic in order to generate a report that is suitable for use with the Turbo Roaming Analyzer if you have activated the **RSSI report events** event type.

E-mail Notifications

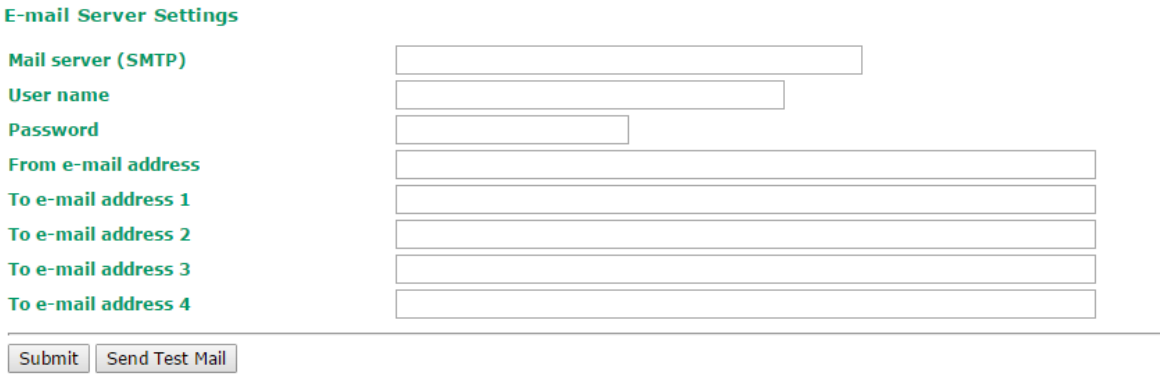
Notification Event Types

Check the box for **Active** to enable the event items. All default values are deactivated (unchecked). Details for each event item can be found in the "System log Event Types" section.



E-mail Server Settings

You can set up to 4 e-mail addresses to receive alarm emails from the AWK-1137C. The following parameters can be configured on the **E-mail Server Settings** page. In addition, a **Send Test Mail** button can be used to test whether the Mail server and e-mail addresses work well. More detailed explanations about these parameters are given after the following figure.



Mail server (SMTP)

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

User name & Password

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

From e-mail address

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

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

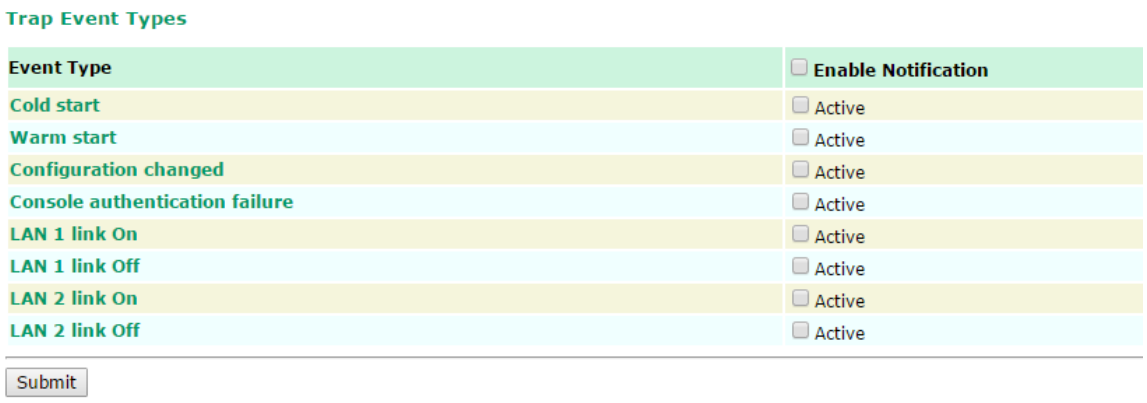
Setting	Description	Factory Default
Max. 63 characters	Enter the receivers' e-mail addresses.	None

Trap

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

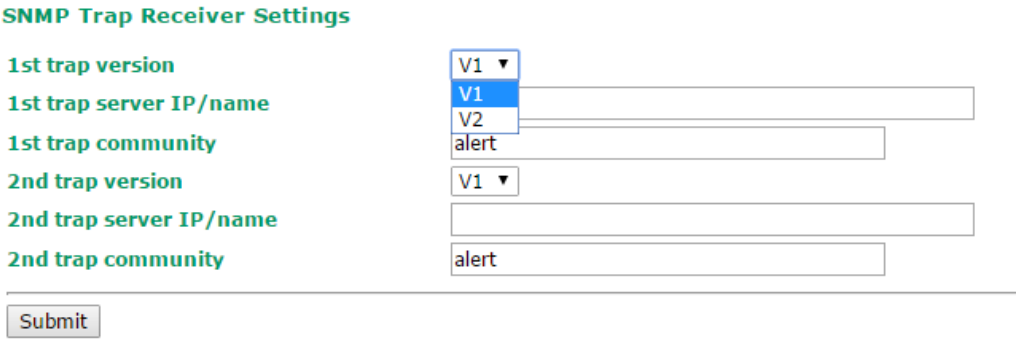
Because a management station usually takes care of a large number of devices that have a large number of objects, it will be overloading for the management station to poll or send requests to query every object on every device. It would be better if the managed device agent could notify the management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

Trap Event Types



SNMP Trap Receiver Settings

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



1st / 2nd trap version

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

1st / 2nd trap server IP/name

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

1st / 2nd trap community

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

Status

Wireless LAN Status

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

It is helpful to use the continuously updated information on this page, such as **Signal strength, Noise floor,** and **SNR**, to monitor the signal strength of the AWK-1137C in Client mode.

Wireless LAN Status

Auto Update

Show status of WLAN (SSID: MOXA)

802.11 Information	
Operation mode	Client
Channel	6
Channel width	20M
RF type	B/G/N Mixed
SSID	MOXA
MAC	00:90:E8:00:05:27
Security mode	OPEN
Current BSSID	06:90:E8:00:05:7E
AP IP address	192.168.127.222
Signal strength	
Signal strength	-69 dBm
Noise floor	-114 dBm
SNR	45
Transmission Information	
Rate	78 Mb/s
Power	20 dBm
Outgoing Packets	
Total sent	511
Packets with errors	0
Packets dropped	835
Incoming Packets	
Total received	206
Packets with errors	0
Packets dropped	0

Serial Status

Serial to Network Connections

Go to **Serial to Network Connections** under **Serial Status** to view the operation mode and status of each connection for each serial port. All monitor functions will refresh automatically every 15 seconds.

The Real COM mode, Reverse Real COM mode and TCP server mode support up to 2 devices connection, TCP Client mode support up to 4 devices connection.

Serial to Network Connections

Auto refresh

Port	OP Mode	Connections
1	Device Control/RealCOM	[192.168.127.55]

Serial Port Status

Go to **Serial Port Status** under **Serial Status** to view the current status of each serial port. **Serial Port Status Buffering** monitors port buffering usage (bytes) of the serial port. Go to **Serial Port Settings** > **Port 1** > **Data Buffering/Log** to enable Port buffering function.

A green dot indicates active, and a gray dot indicates inactive

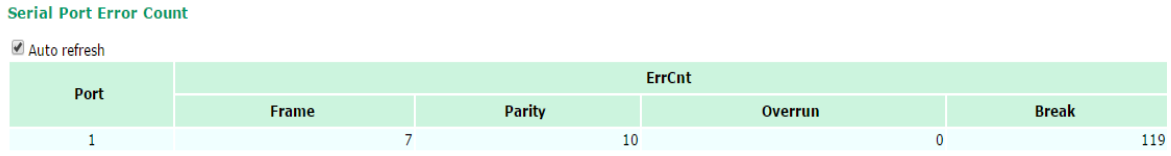
Serial Port Status

Auto refresh

Port	TxCnt	RxCnt	TxTotalCnt	RxTotalCnt	DSR	DTR	RTS	CTS	DCD	Buffering
1	64	68	64	68						0

Serial Port Error Count

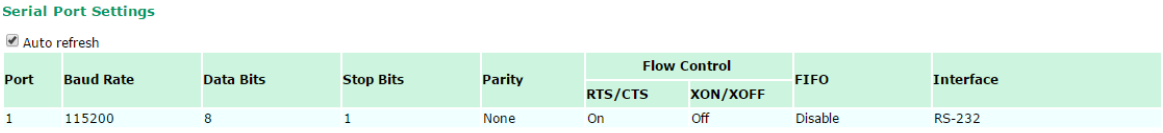
Go to **Serial Port Error Count** under **Serial Status** to view the error count for each serial port.



	Description
Frame	Frame error due to incorrect settings of Baudrate, Parity (even/odd) and Stop bits
Parity	Error resulting from the parity on / off setting between both sites
Overrun	AWK serial interface is overloaded due to mass data transmission from users' serial device.
Break	Transmission breaks resulting from serial devices connected behind the AWK.

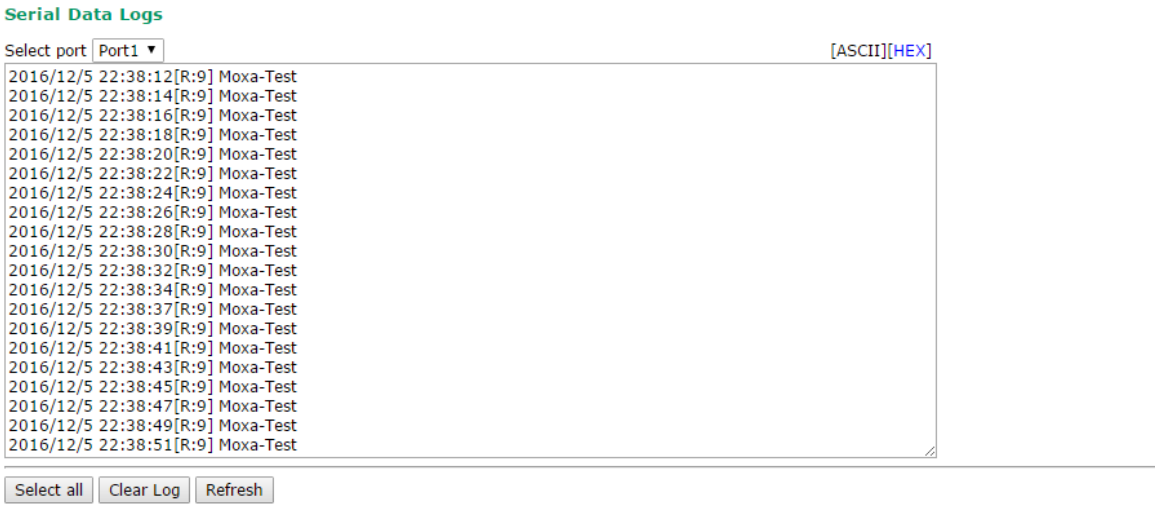
Serial Port Settings

Go to **Serial Port Settings** under **Serial Status** to view a summary of the settings for each serial port.



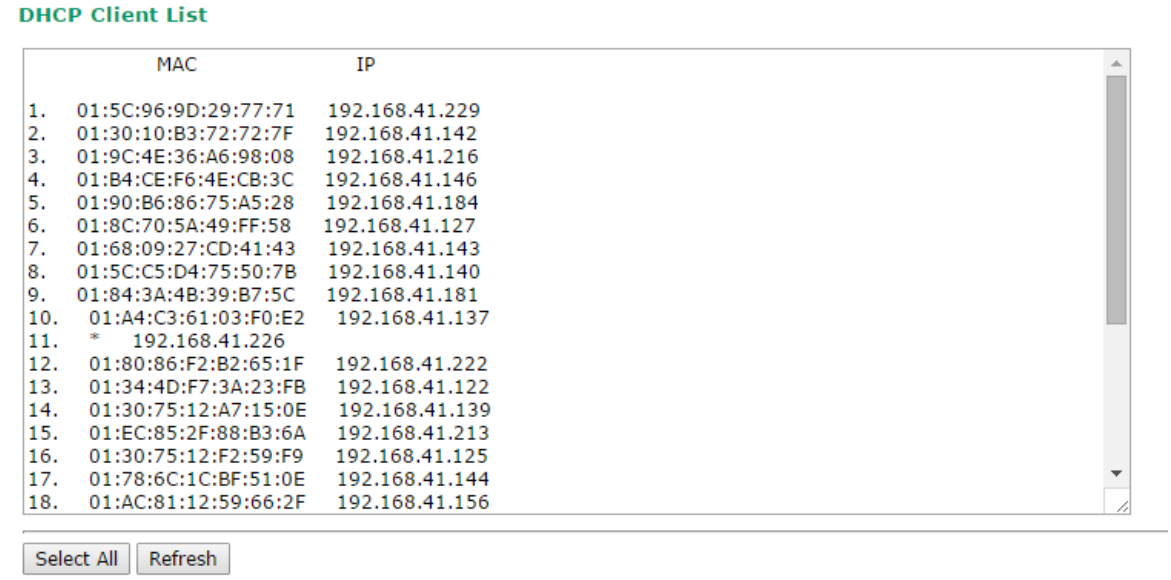
Serial Data Log

Data logs for the serial port can be viewed in ASCII or HEX format. After selecting the serial port and format, you may click **Select all** to select the entire log if you wish to copy and paste the contents into a text file. R - Receiver / T - Transmission to the serial device.

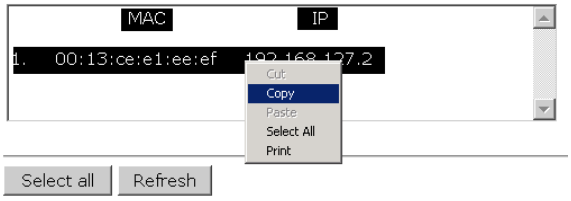


DHCP Client List (for Client-router mode only)

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

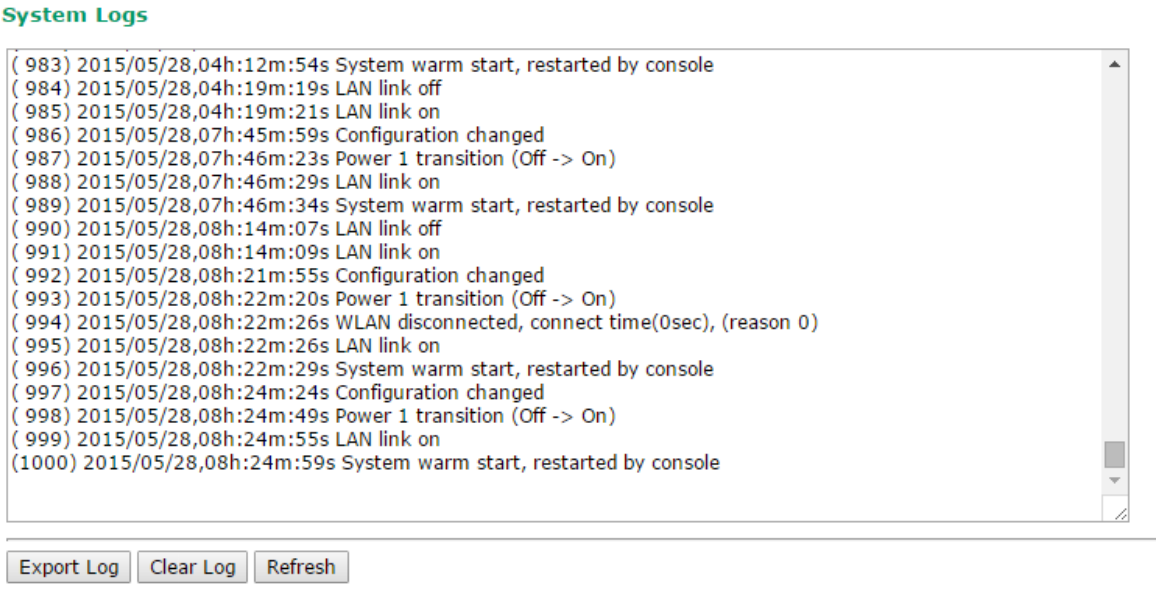


You can press **Select all** button to select all content in the list for further editing.



System Logs

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



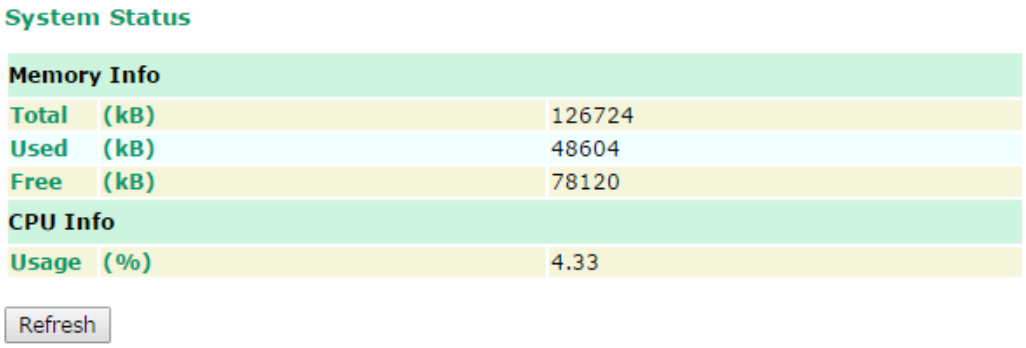
Reason Code	Name	Description
0	MOXA_NORMAL_JOIN	The station joined normally, no extra information.
3	MOXA_DEAUTH_LEFT	Received a de-authentication frame.

4	MOXA_DISASSOC_LEFT	Received a disassociation frame.
6	MOXA_INACTIVE_LEFT	The AP has sent a de-authentication frame to drop the station due to station inactivity.

System Status

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

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

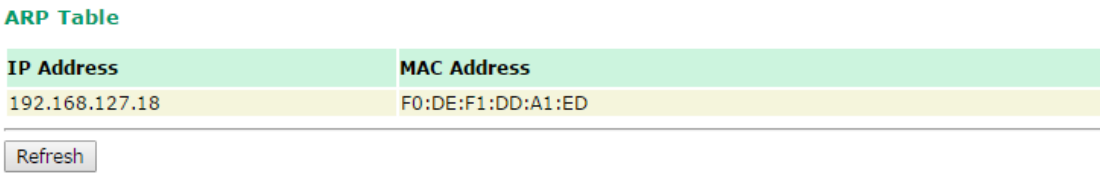


Network Status

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

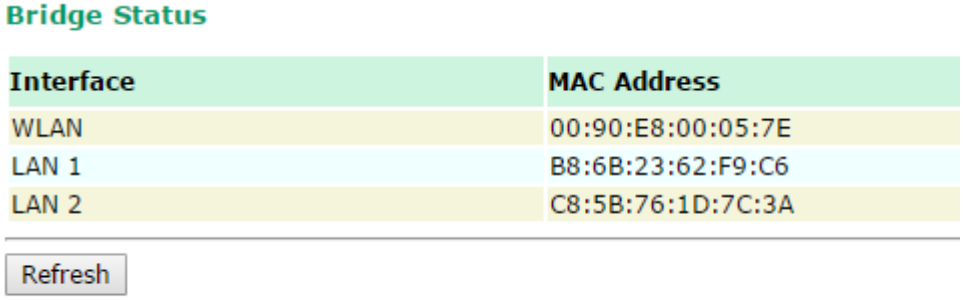
ARP Table

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



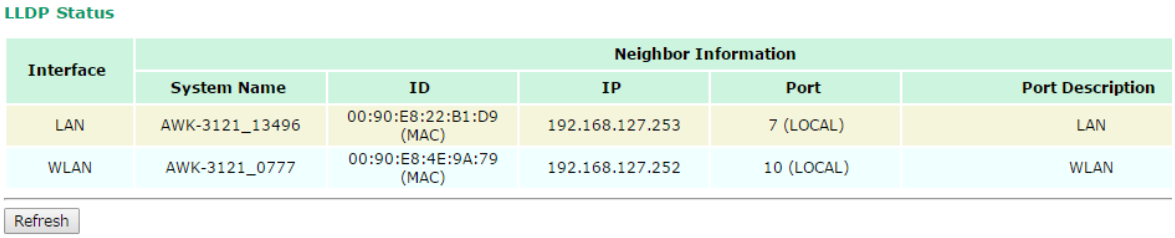
Bridge Status

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



LLDP Status

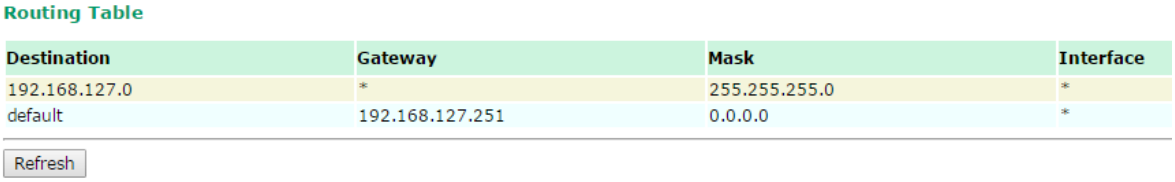
Displays information on neighboring devices collected via LLDP (Link Layer Discovery Protocol).



NOTE The AWK-1137C's LLDP function does not support IEEE 802.3.

Routing Table

Displays the routing information for the current device.

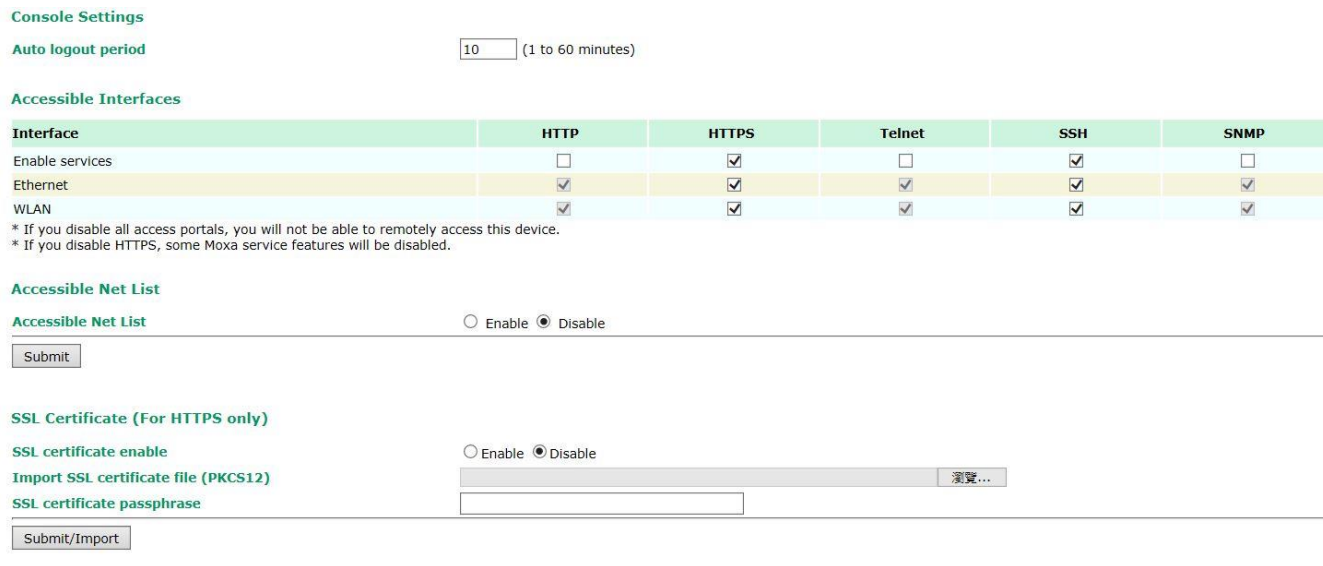


Maintenance

Maintenance functions provide the administrator with tools to manage the AWK-1137C and wired/wireless networks.

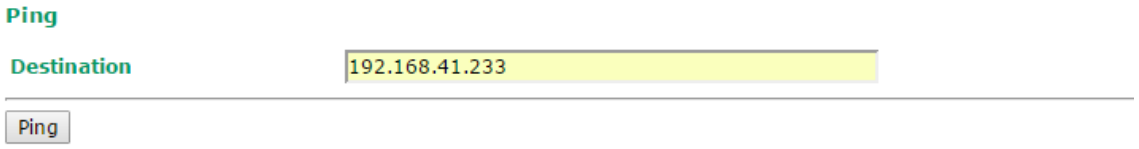
Console Settings

You can enable or disable access permissions to the device and Moxa Service such as MXstudio and Wireless Search Utility. For greater security, we recommend only allowing access to the two secure consoles, HTTPS and SSH.

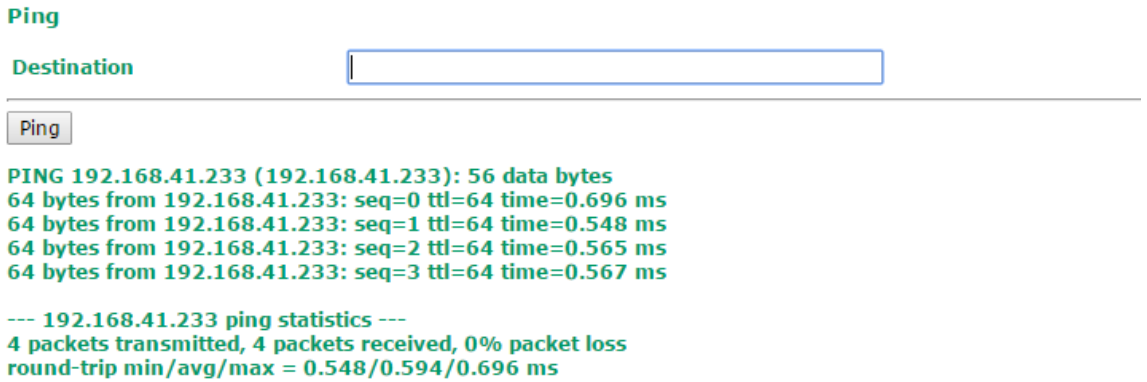


Ping

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 the access path is available.



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

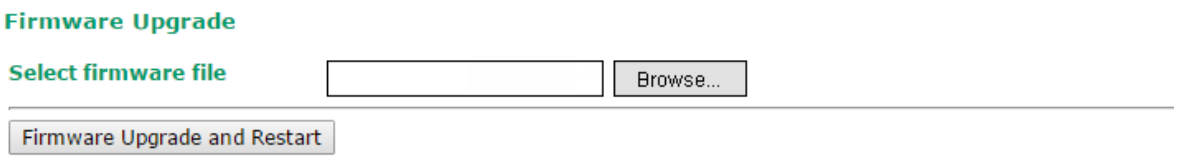


Firmware Upgrade

The AWK-1137C can be enhanced with more value-added functions by installing firmware upgrades. The latest firmware is available at Moxa's download center.

Before running a firmware upgrade, make sure the AWK-1137C is off-line. Click the **Browse** button to specify the firmware image file and click **Firmware Upgrade and Restart** to start the firmware upgrade. After the progress bar reaches 100%, the AWK-1137C will reboot itself.

When upgrading your firmware, the AWK-1137C's other functions are forbidden.



ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your AWK-1137C.

Configuration Import and Export

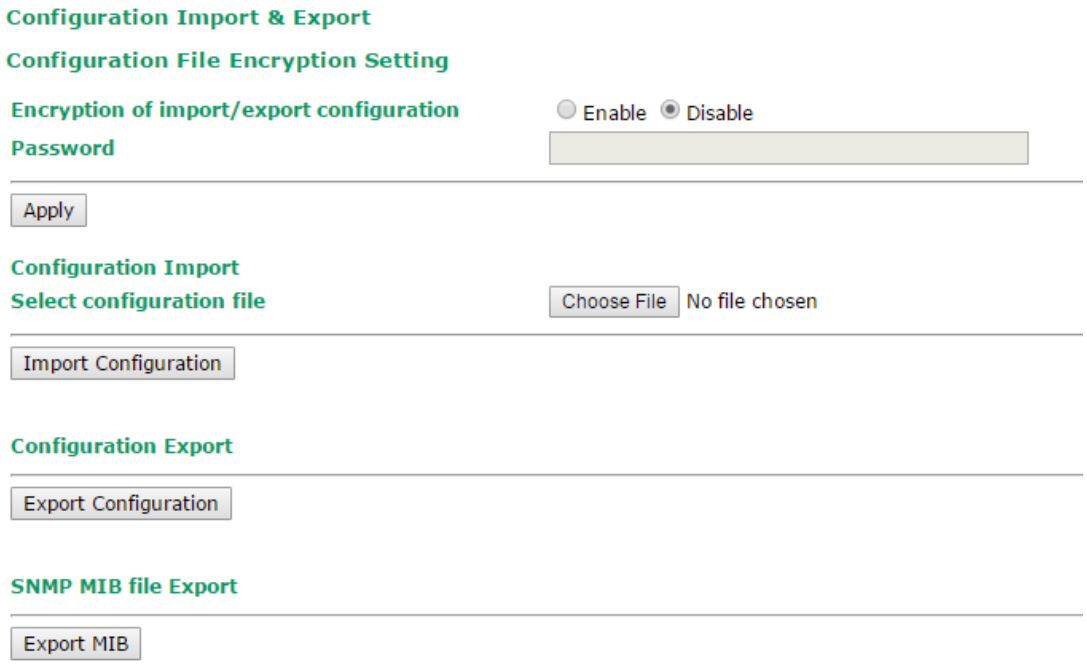
You can use the **Configuration Import & Export** page to back up or restore the following:

- Configuration settings on the AWK-1137C
- MIB

In the **Configuration Import** section, click **Choose File** to select a configuration file and click **Import Configuration** button to begin importing configuration settings. The password is up to 31 characters.

To save the configuration file to a storage media, click **Export Configuration**. The configuration file is a text file and you can view and edit it with a general text-editing tool.

Click **Export MIB** to save the MIB file to a storage media. The configuration file is a ***.my** file that you can import using a general SNMP tool and use to remotely control or configure the AWK-1137C.

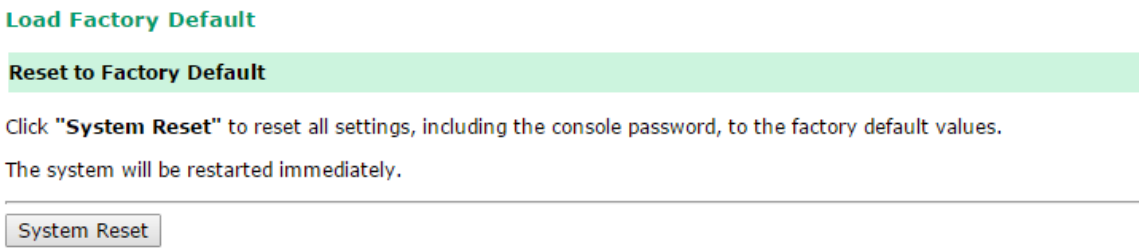


In the **Configuration Export** section, click the **Export Configuration** button and save the configuration file onto your local storage media. The configuration file is a text file and you can view and edit it with a general text-editing tool.

The SNMP MIB file is also available for download from the SNMP MIB File Export section.

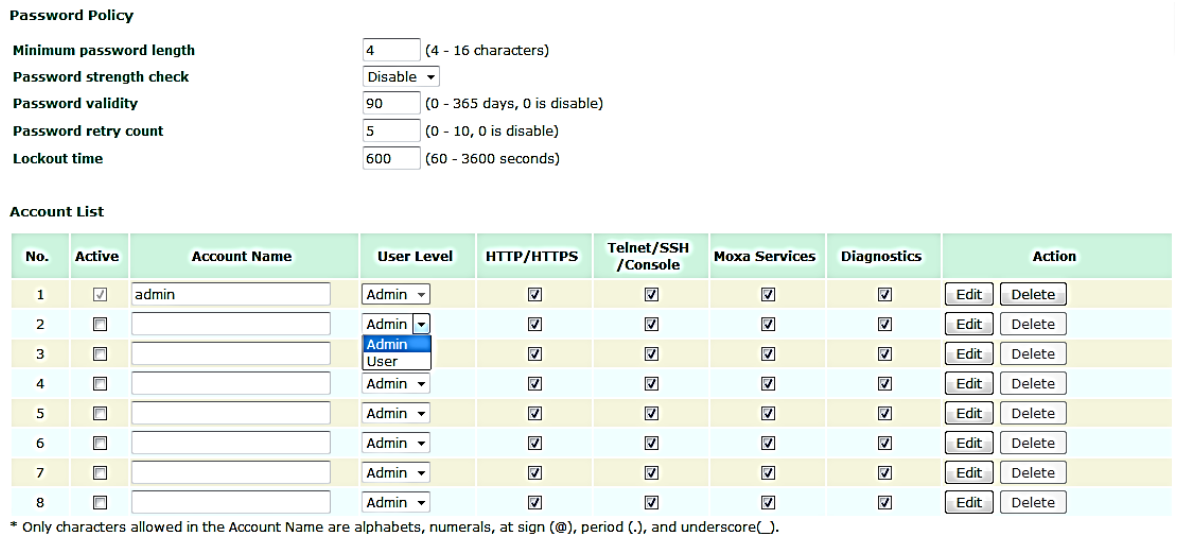
Load Factory Default

Use this function to reset the AWK-1137C 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-1137C.



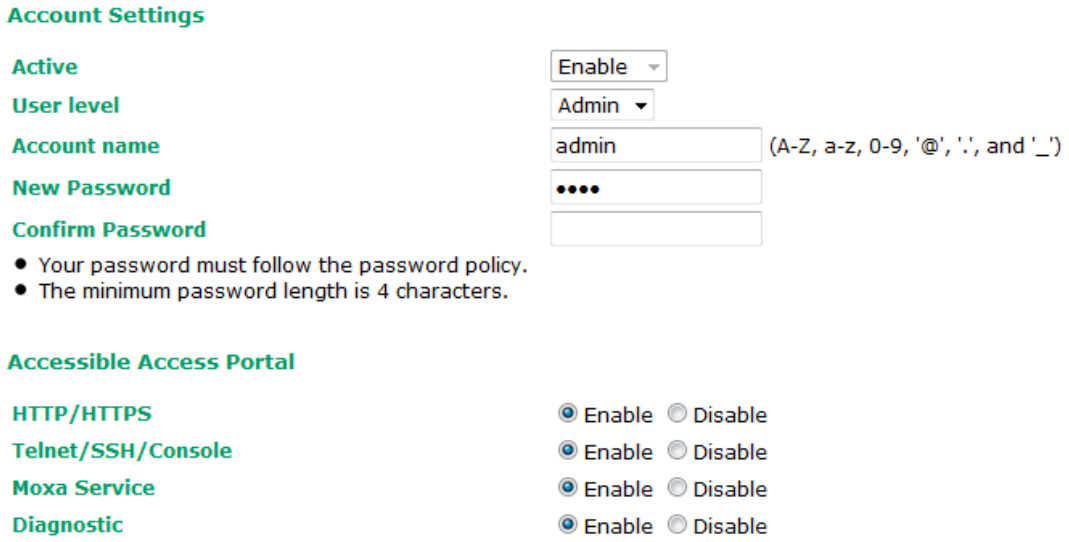
Account Settings

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



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

Click **Edit** to create a new user account or edit an existing one. You can configure the items shown below:

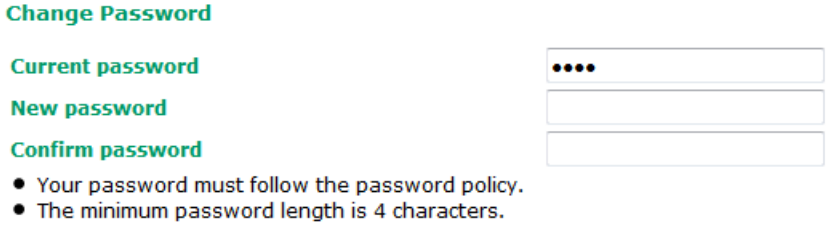


Field	Description	Default Setting
Active	Select Enable to enable the user account.	Disable
User level	Administrator: Allows the user to access the Web UI, change the device's configuration, and use the device's import/export capability. User: Allows the user to access the Web UI, but the user will not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

Change Password

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

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



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

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

Miscellaneous Settings

Additional settings that help you manage your AWK-1137C are available on this page.

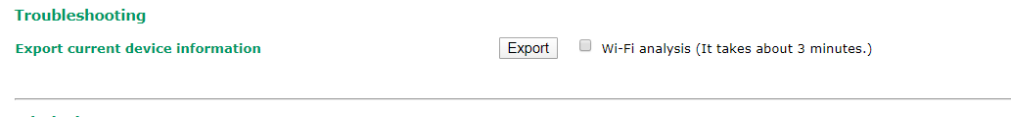
Select one of the following **Reset button** options:

- **Always enable**–Set the reset button to perform a factory restore on the AWK-1137C. This is the default option.
- **Disable factory reset function after 60 seconds**–Deactivate the factory reset function of the reset button 60 seconds after the AWK-1137C restarts.

Troubleshooting

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

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



Wi-Fi Mirror Port

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

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

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

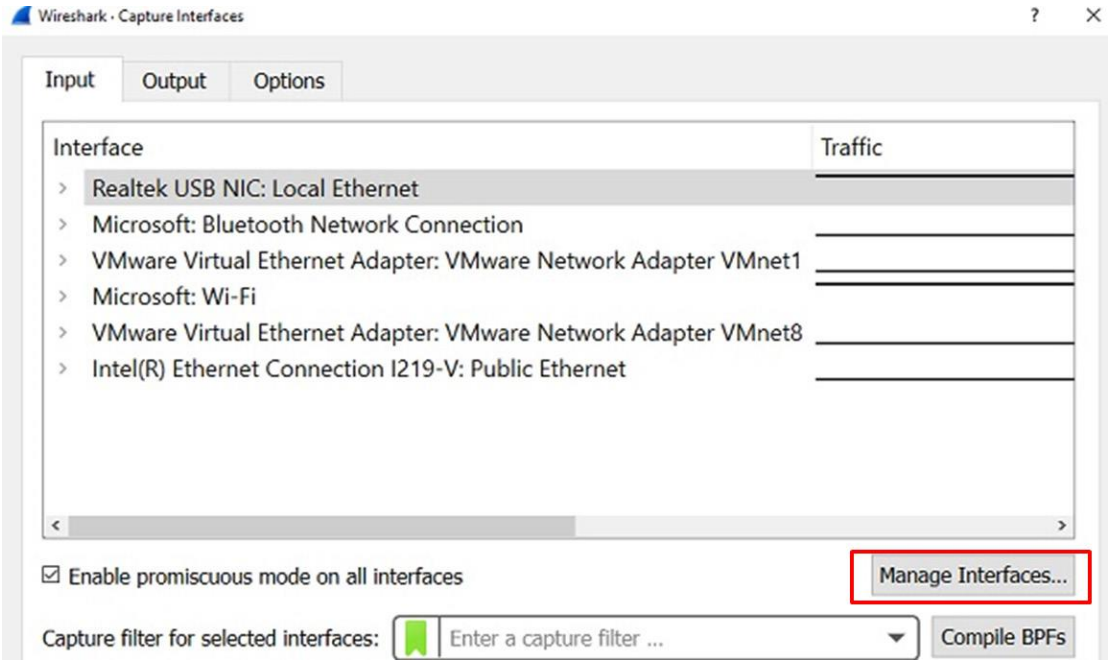
To set up a Wi-Fi mirror port for short-term monitoring, do the following:

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

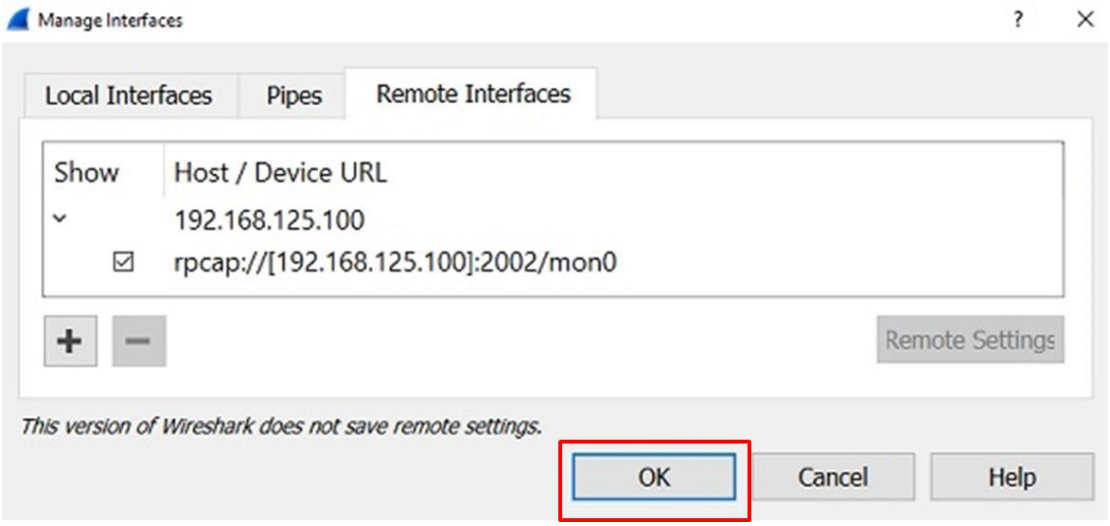
You will be able to download a report from the web browser.

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

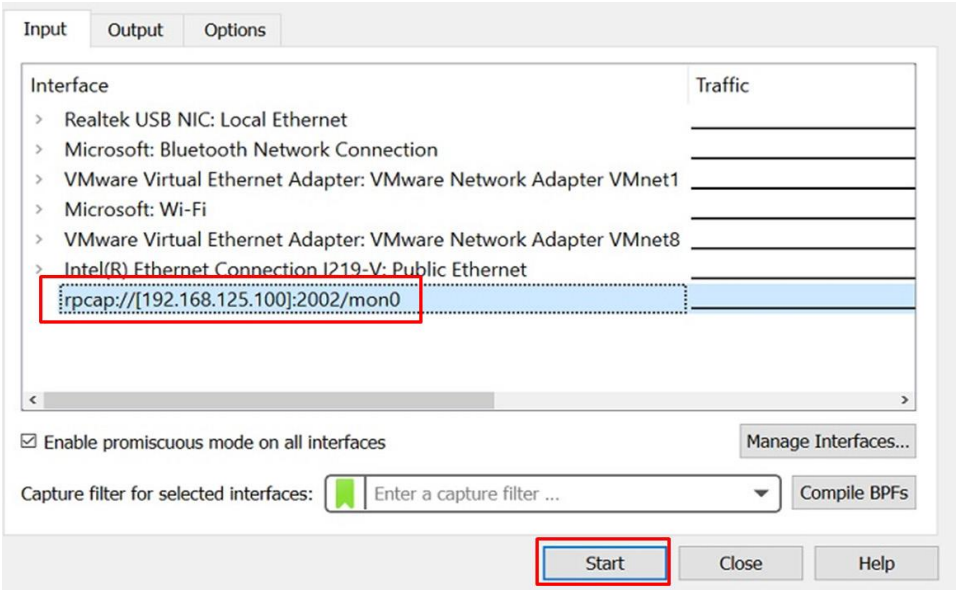
1. On the **Wi-Fi Mirror Port** page, set the **Remote Capture** option to **Enable.**
2. Run the Wireshark tool on your computer, click **Capture** and then click **Options**.
3. In the **Input** tab of the Wireshark tool, click **Manage Interfaces**



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



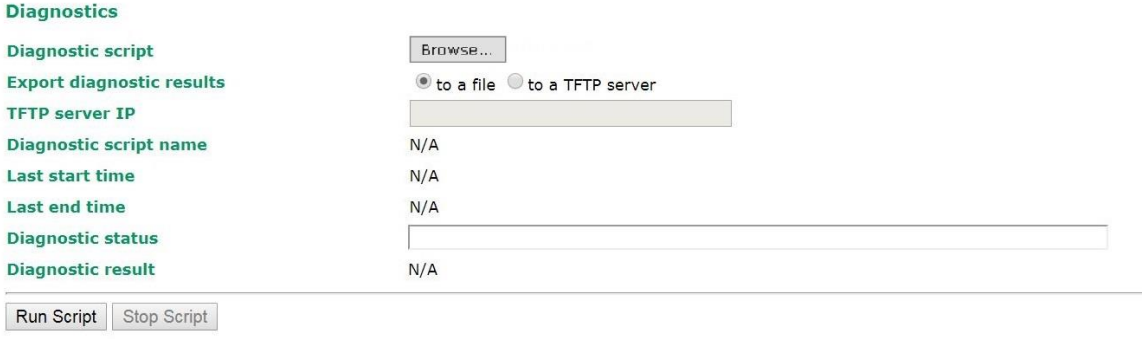
7. Select Input --> Interface --> rpcap://...:2002/mon0



Diagnostics

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

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

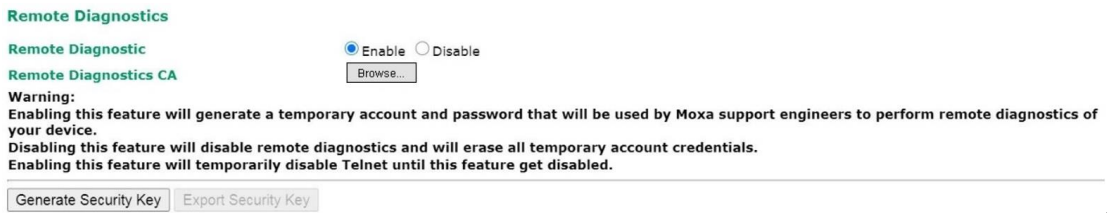


Setting	Description
Diagnostic script	Use the Browse button to select the Moxa diagnosis script file.
Export diagnostic results	Select if you want to export: • **to a file** • **to a TFTP server**
TFTP server IP	If you have selected the TFTP option, specify the IP address of the TFTP server.
Diagnostic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

Remote Diagnostics

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

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

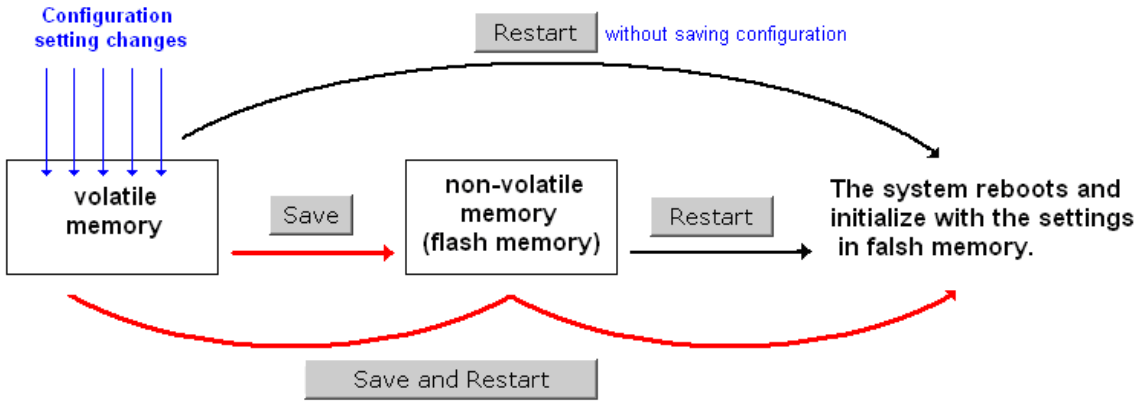


Setting	Description
Remote Diagnostics	Enable this option to allow remote technical support from Moxa engineers.
Remote Diagnostics CA	When enabled, the Moxa engineer will request the admin to provide the AWK's serial number and MAC address to generate a certificate file. Click **Browse** and upload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

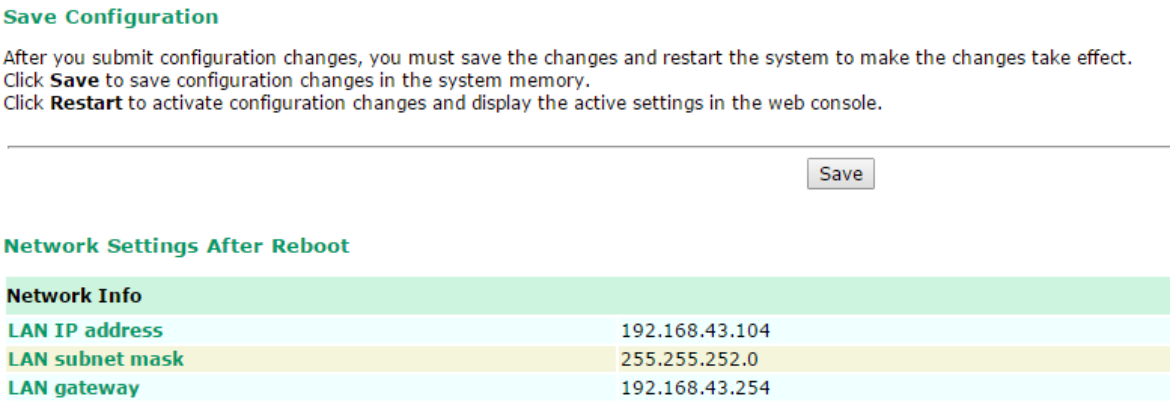
Save Configuration

The following figure shows how the AWK-1137C stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the AWK-1137C is shutdown or rebooted. Because the AWK-1137C starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the AWK-1137C.

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



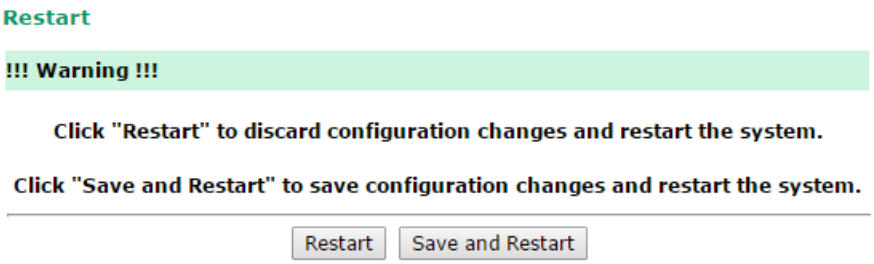
After you click on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** if you wish to update the configuration settings in the flash memory at this time. Alternatively, you may choose to run other functions and put off saving the configuration until later. However,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



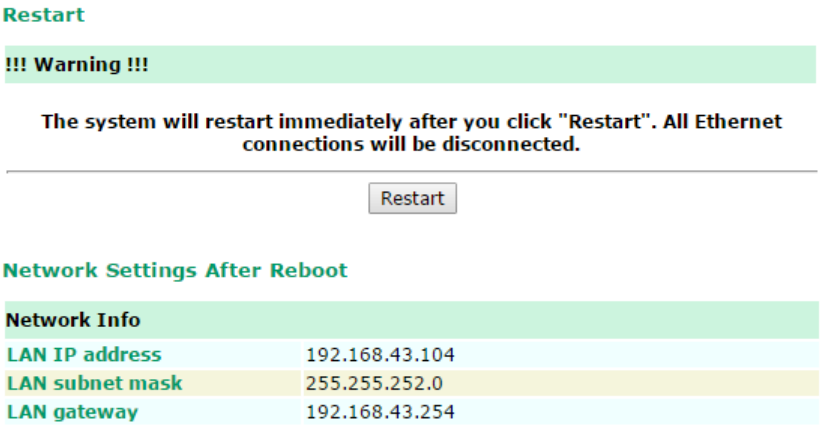
Restart

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

If you made changes recently but did not save, you will be given two options. Clicking the **Restart** button here will reboot the AWK-1137C directly, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the AWK-1137C.



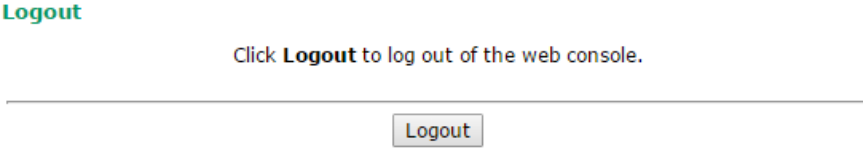
If you run the **Restart** function without changing any configurations or saving all your changes, you will see just one **Restart** button on your screen.



You will not be able to run any of the AWK-1137C's functions while the system is rebooting.

Logout

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



4

Software Installation and Configuration

The following topics are covered in this chapter:

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

Overview

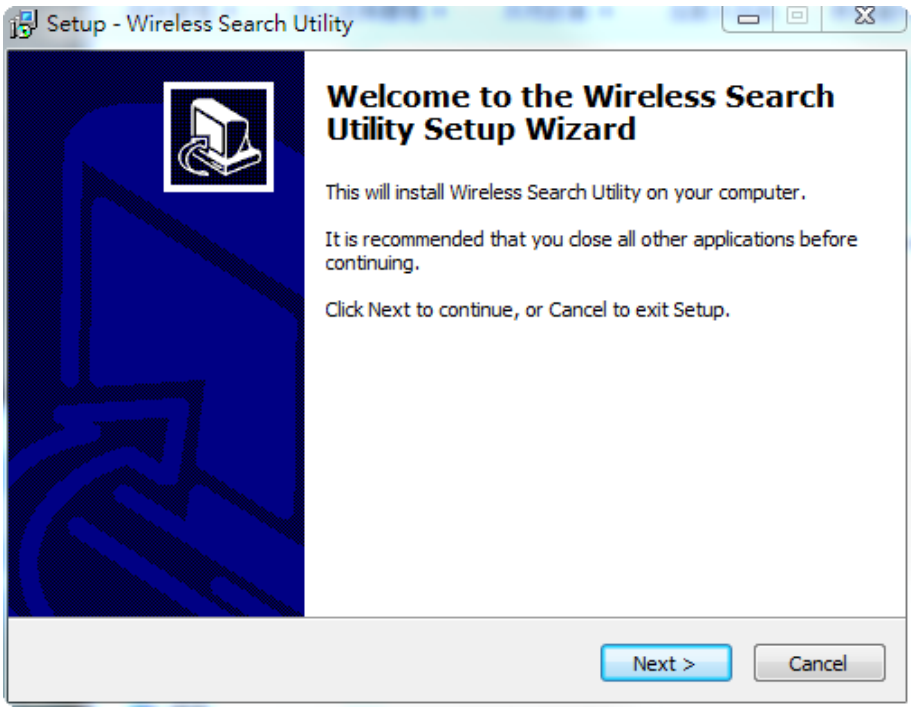
The Wireless Search Utility can be downloaded from the Moxa website at www.moxa.com.

Wireless Search Utility

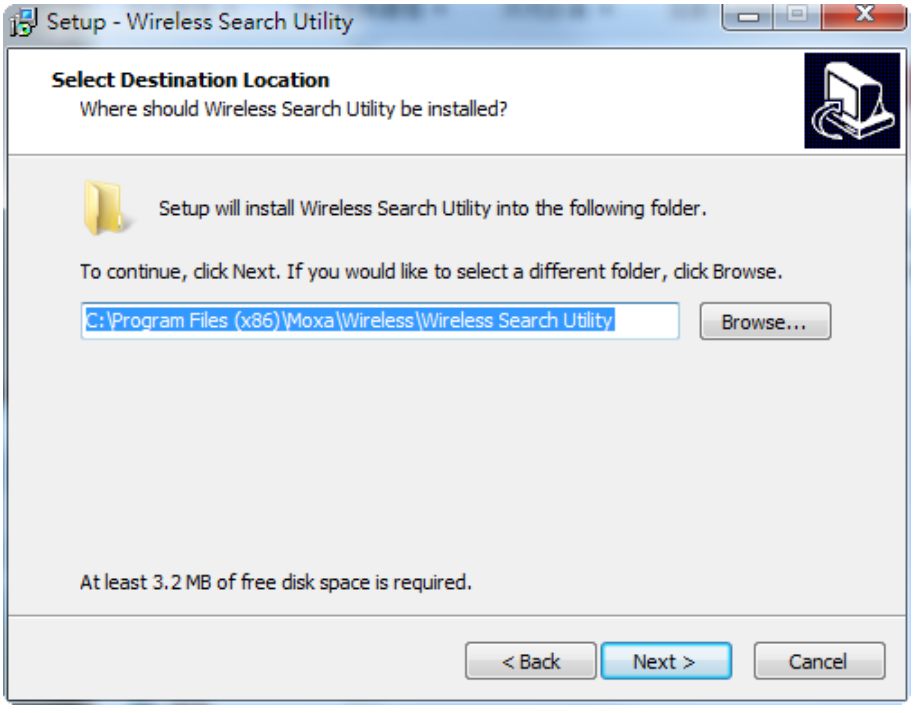
Installing Wireless Search Utility

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

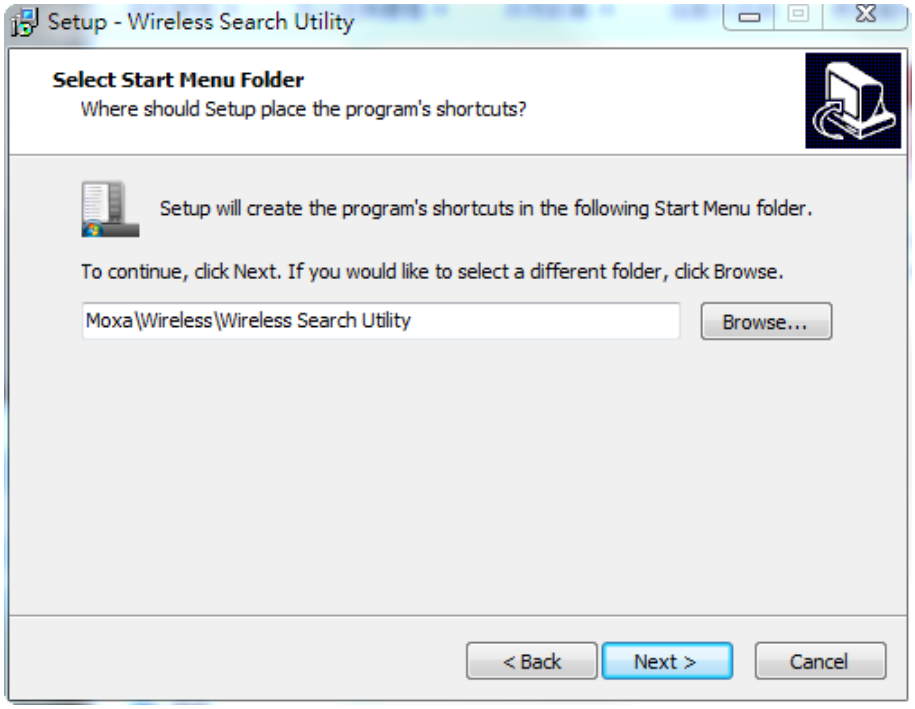
1. Click **Next** when the **Welcome** screen opens to proceed with the installation.



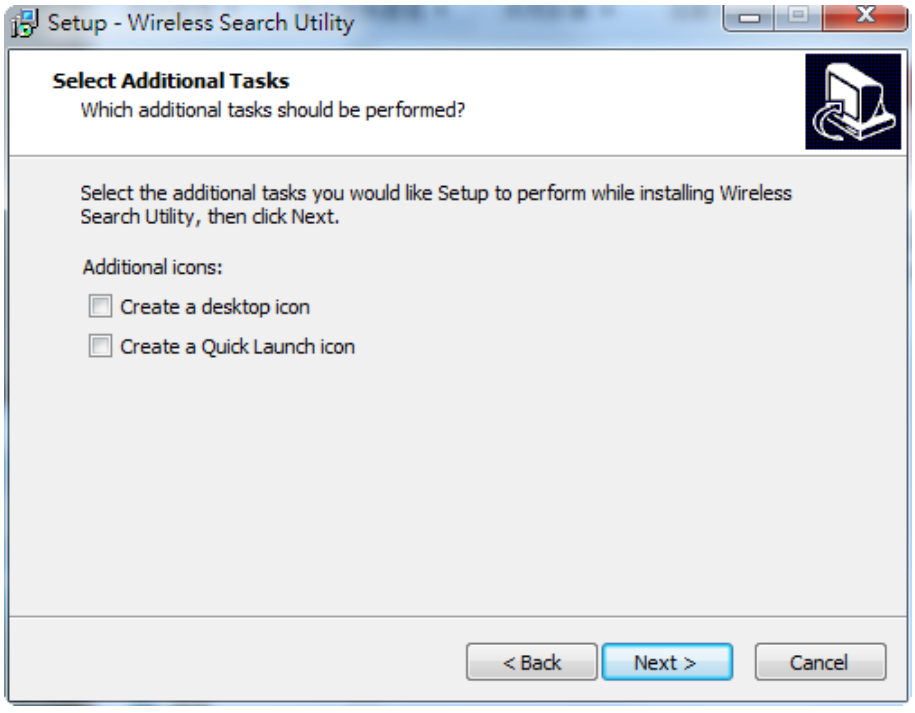
2. Click **Next** to install program files to the default directory, or click **Browse** to select an alternate location.



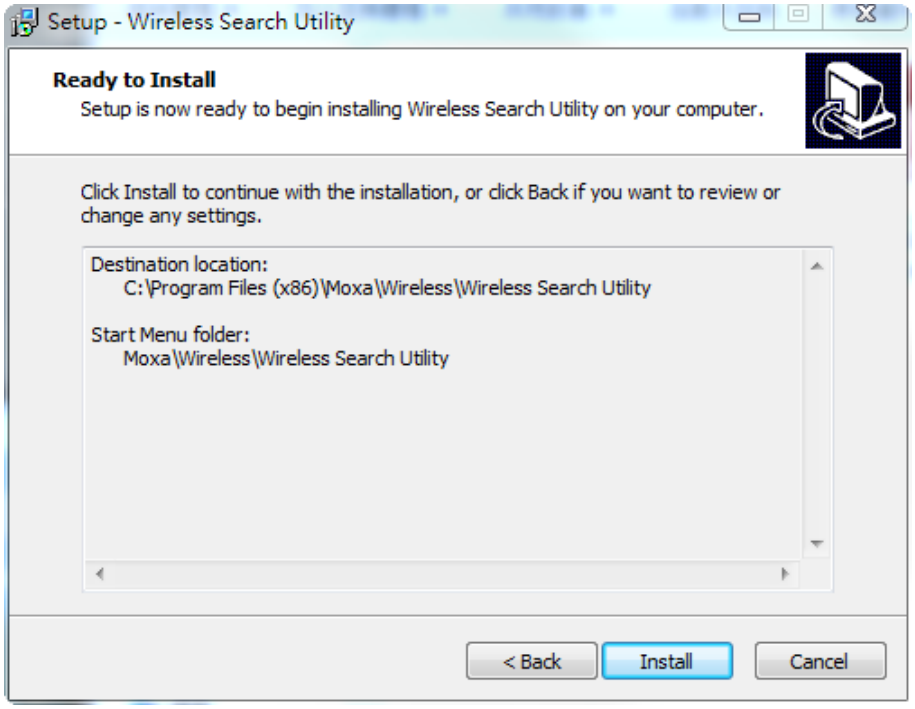
3. Click **Next** to create the program's shortcut files to the default directory, or click **Browse** to select an alternate location.



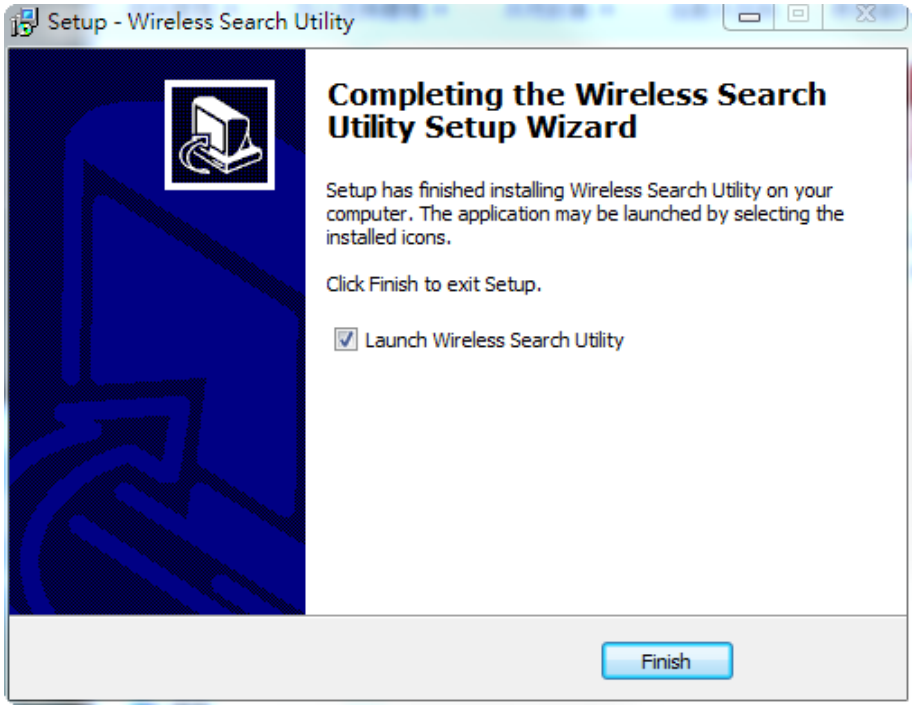
4. Click **Next** to select additional tasks.



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



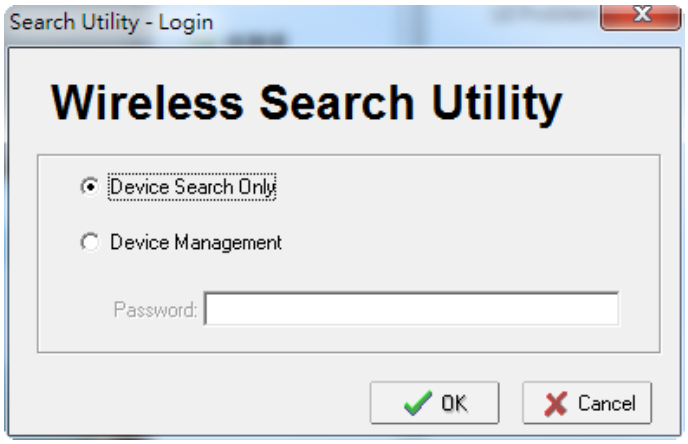
6. Click **Install** to begin the installation. The setup window will report the progress of the installation. To change the installation settings, click **Back** and navigate to the previous screen.
7. Click **Finish** to complete the installation of Wireless Search Utility.



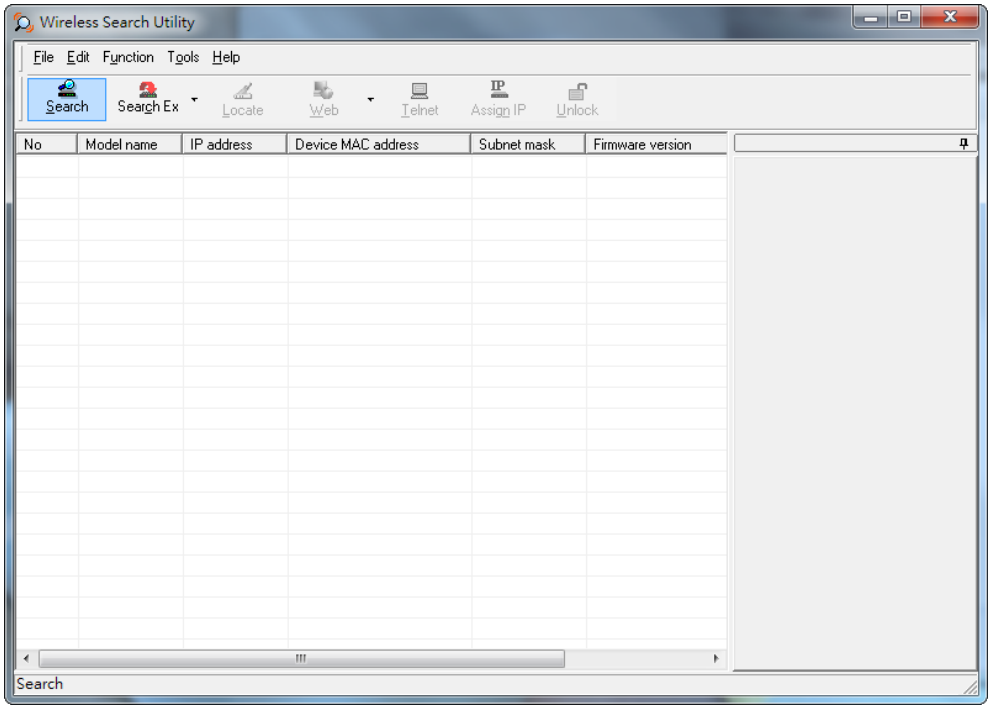
Configuring Wireless Search Utility

The Broadcast Search function is used to locate all AWK-1137C APs that are connected to the same LAN as your computer. After locating an AWK-1137C, 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-1137C is configured as an AP or Client. In either case, APs and Clients connected to the LAN will be located, regardless of whether or not they are part of the same subnet as the host.

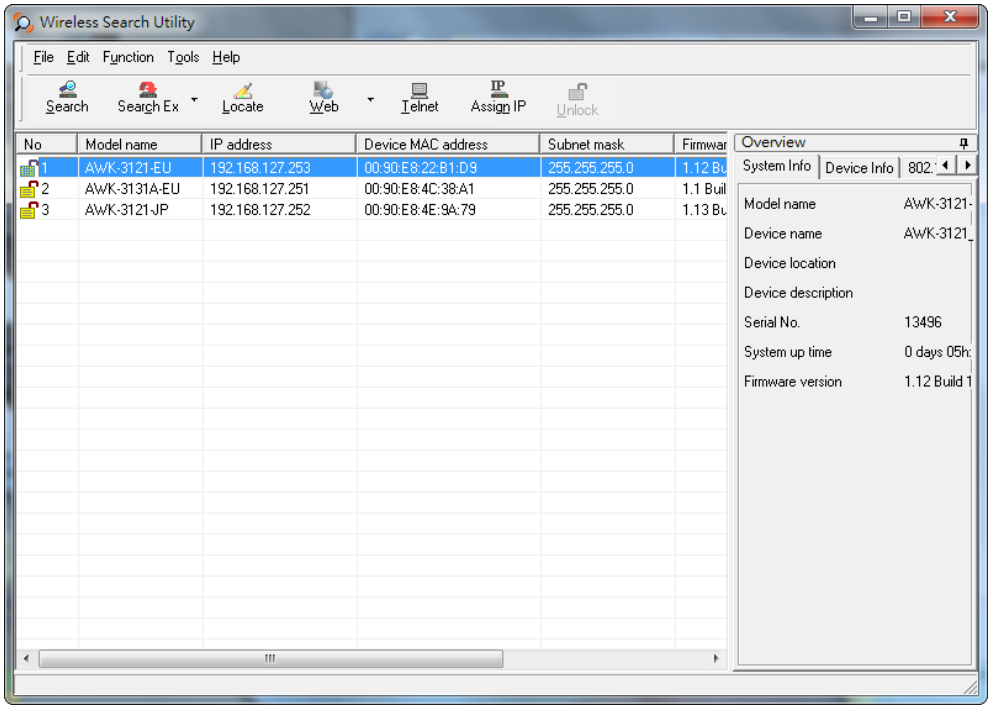
1. Start the **Wireless Search Utility** program. When the Login page appears, select the "Device Search only" option to search for devices and to view the configuration of each device. Select the "Device management" option to assign IPs, upgrade firmware, and locate devices.



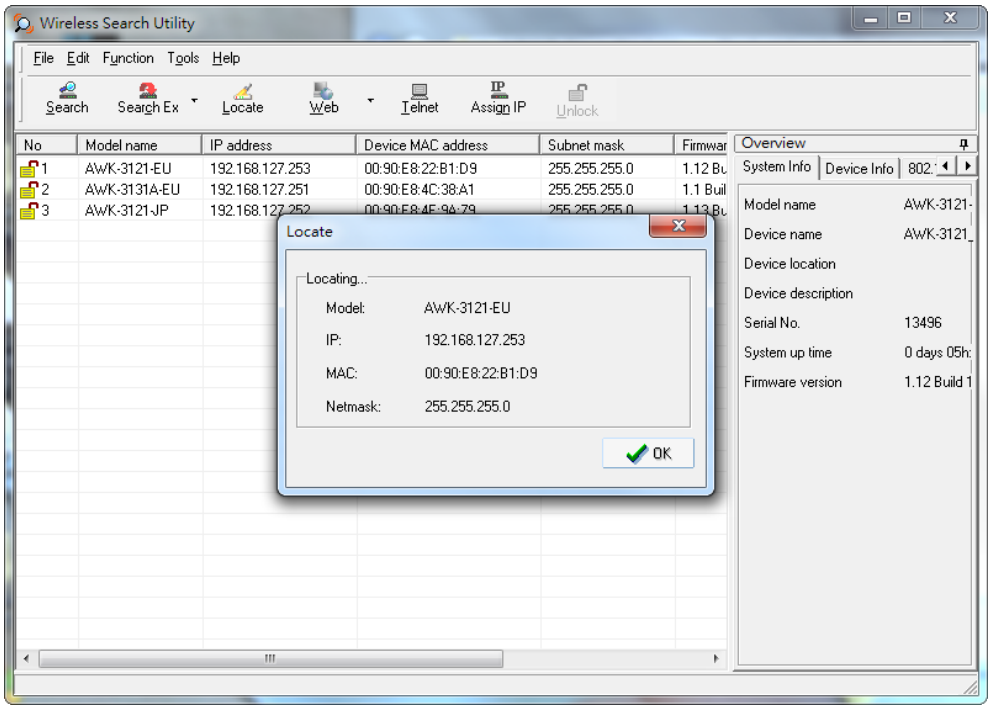
2. Open the Wireless Search Utility and then click the **Search** icon.



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

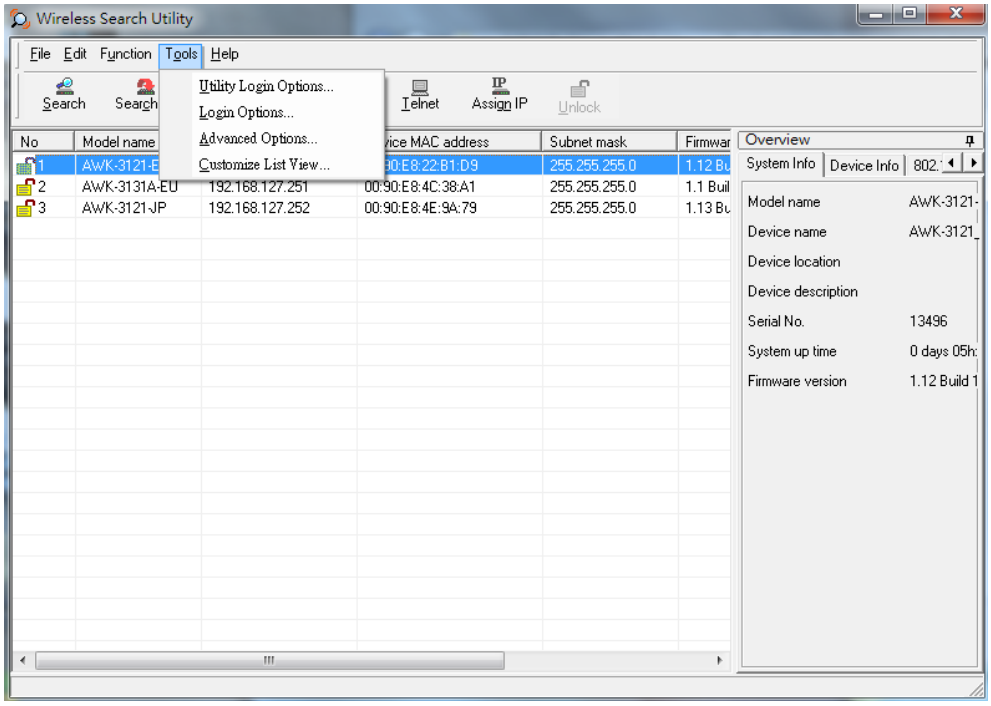


4. Click **Locate** to cause the selected device to beep.



5. Make sure your AWK is **unlocked** before using the search utility's icons setting. The AWK will unlock automatically if the password is set to the default. Otherwise you must enter the new password manually.

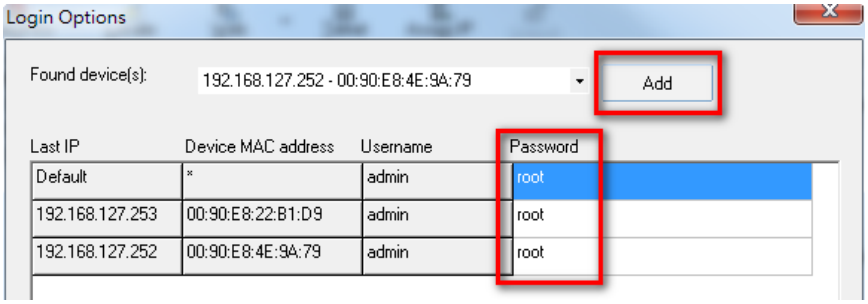
6. Go to **Tools → Login Options** to manage and unlock additional AWKs.



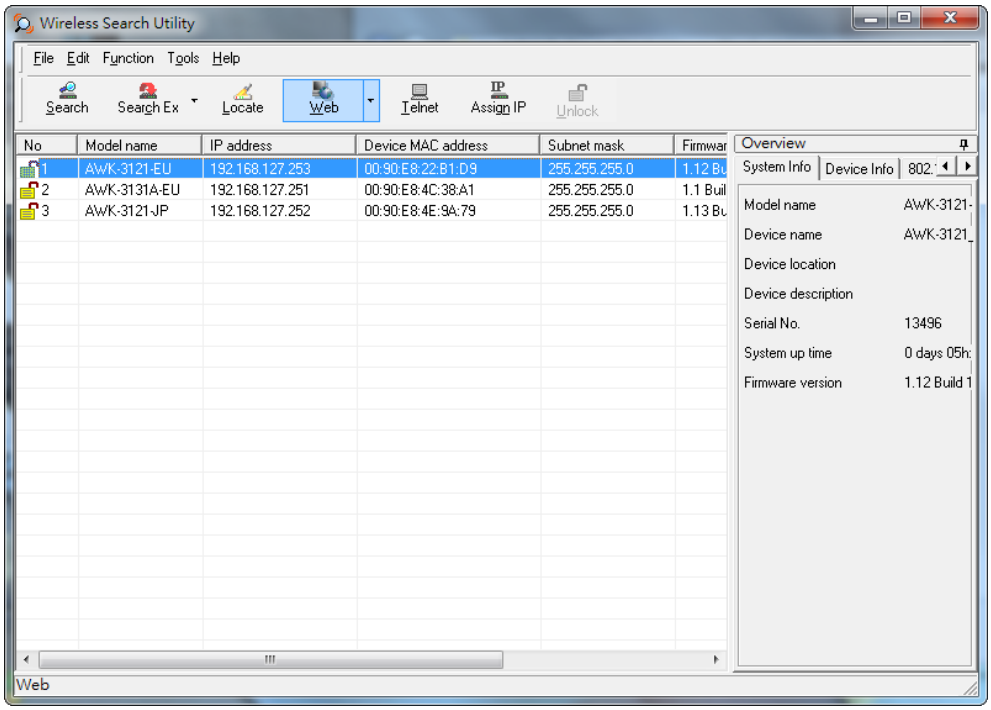
7. Use the scroll down list to select the MAC addresses of those AWKs you would like to manage, and then click **Add**. Key in the password for the AWK device and then click **OK** to save. If you return to the search page and search for the AWK again, you will find that the AWK will unlock automatically.

ATTENTION

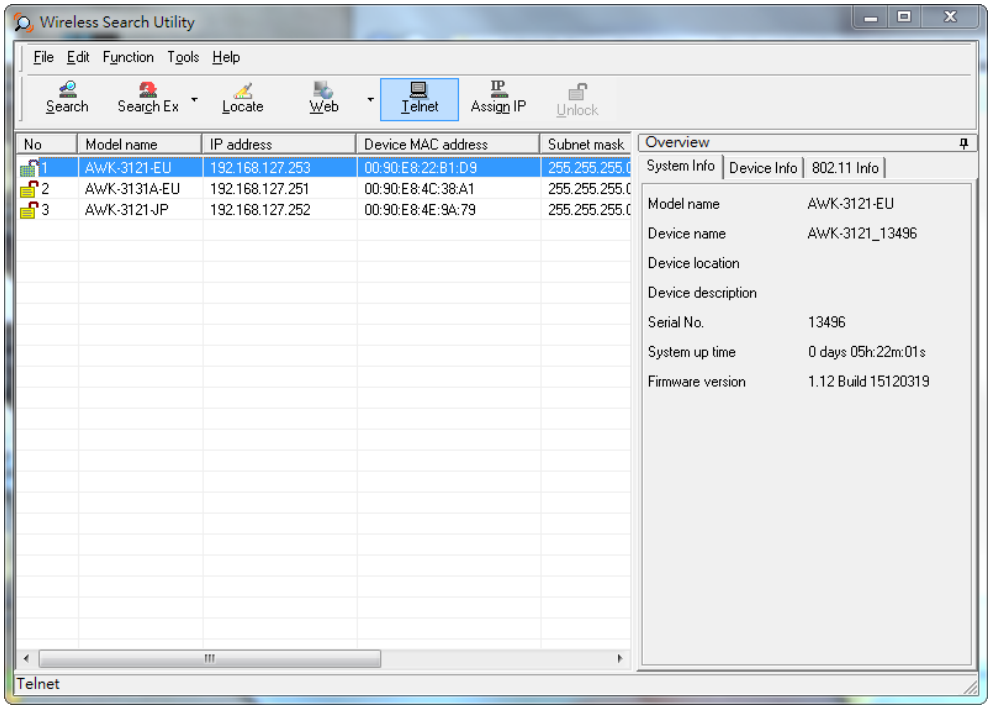
For security purposes, we suggest you can change the Wireless Search Utility login password instead of using the default.



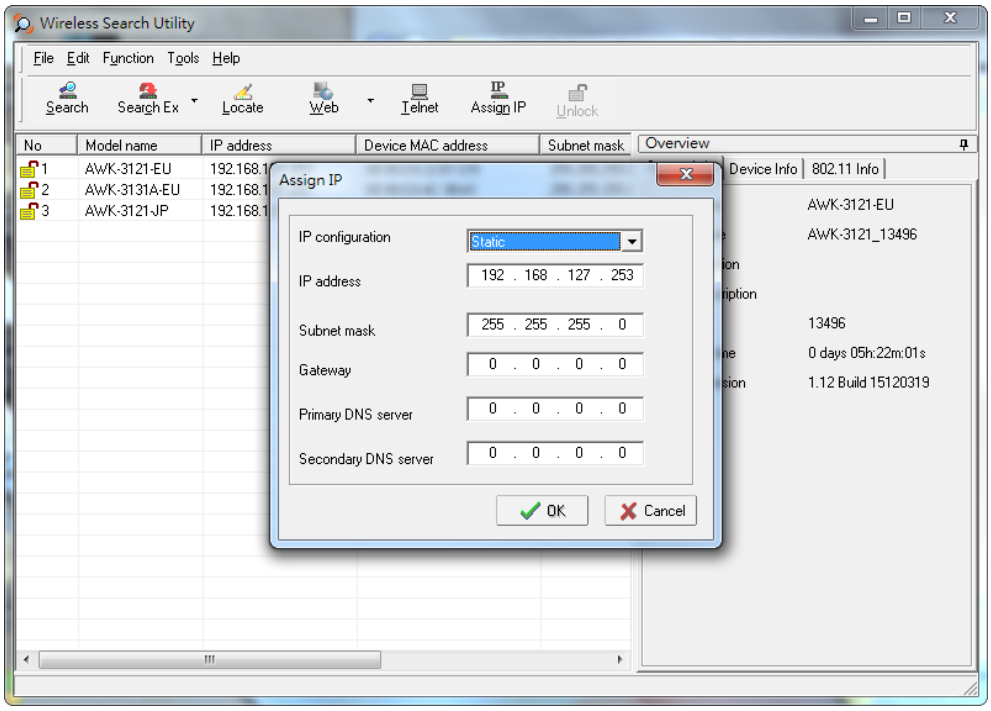
To modify the configuration of the highlighted AWK, click on the Web icon to open the web console. This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, "Using the Web Console," for information on how to use the web console.



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



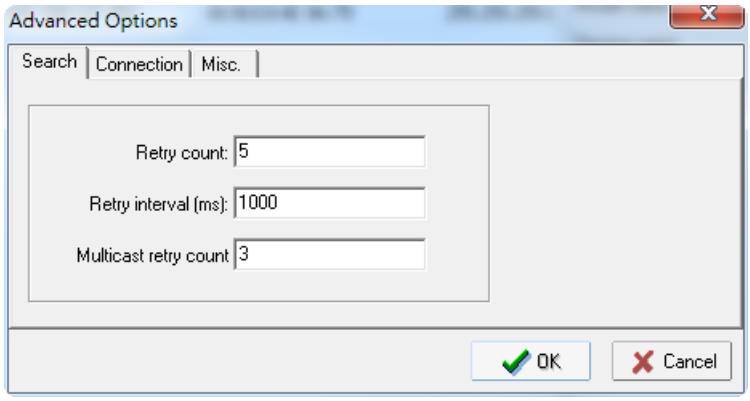
Click **Assign IP** to change the IP setting.



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

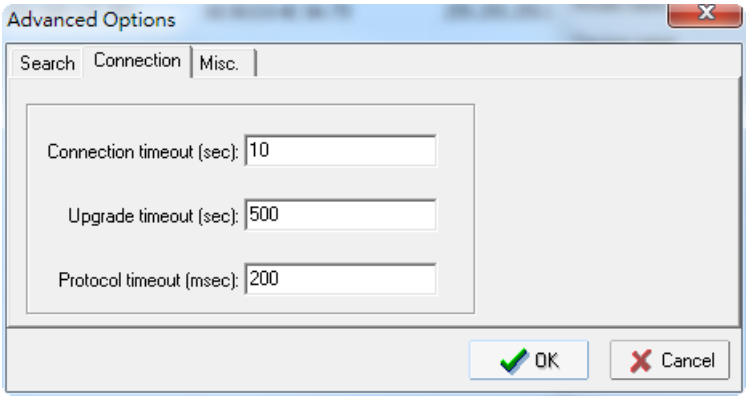
Search

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



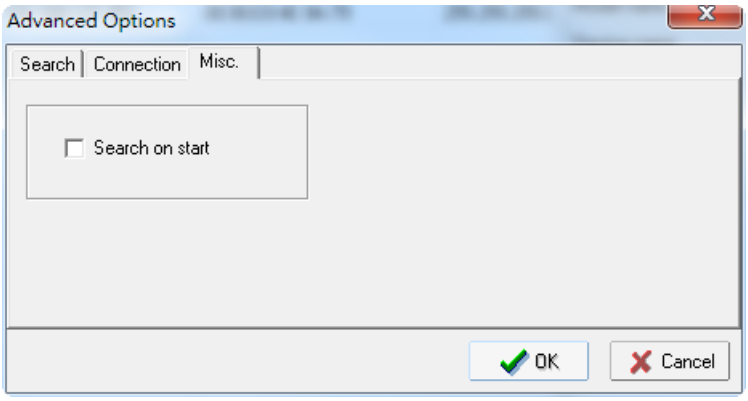
Connection

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



Misc.

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



5

Using Other Consoles

This chapter explains how to access the AWK-1137C for the first time. In addition to HTTP access, there are four ways to access AWK-1137C: Telnet console, SSH console, HTTPS console, and serial console. Telnet console, SSH console and HTTPS console can be used to access the AWK-1137C over an Ethernet LAN, or over the Internet. The serial console is for use by a Moxa service representative for troubleshooting product issues.

The following topics are covered in this chapter:

- **Configuration by Telnet and SSH Consoles**
- **Configuration by Web Browser with HTTPS/SSL**
- **Disabling Telnet and Browser Access**
- **Configuration by the RS-232 Console**

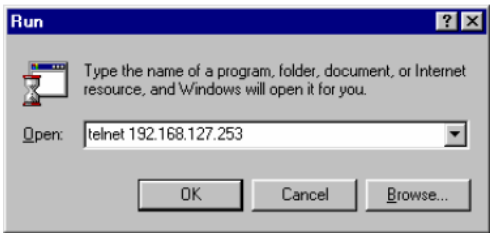
Configuration by Telnet and SSH Consoles

You may use Telnet or SSH client to access the AWK-1137C and manage the console over a network. To access the AWK-1137C's functions over the network from a PC host that is connected to the same LAN as the AWK-1137C, you need to make sure that the PC host and the AWK-1137C are on the same logical subnet. To do this, check your PC host's IP address and subnet mask.

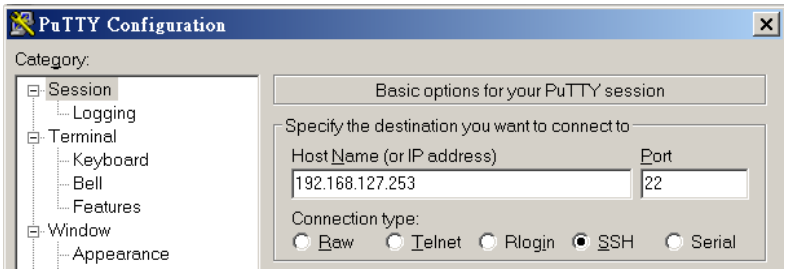
NOTE The AWK-1137C's default IP address is **192.168.127.253** and the default subnet mask is **255.255.255.0** (for a Class C network). If you do not set these values properly, please check the network settings of your PC host and then change the IP address to 192.168.127.xxx and subnet mask to 255.255.255.0.

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

1. From Windows Desktop, run **Start → Run**, and then use Telnet to access the AWK-1137C'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), please run the client program (e.g., putty.exe) and then input the AWK-1137C's IP address, specifying **22** for the SSH connection port.

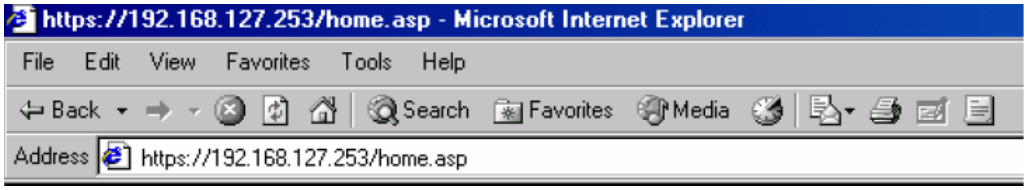


3. The Console login screen will appear. Please refer to the previous paragraph "RS-232 Console Configuration" and for login and administration.

Configuration by Web Browser with HTTPS/SSL

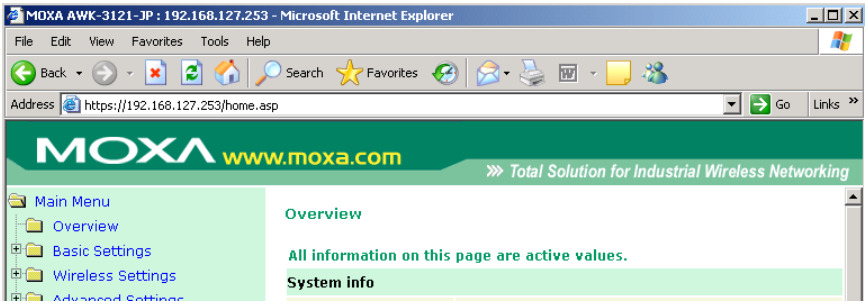
To secure your HTTP access, the AWK-1137C supports HTTPS/SSL encryption for all HTTP traffic. Perform the following steps to access the AWK-1137C's web browser interface via HTTPS/SSL.

1. Open your web browser and type https://<AWK-1137C's IP address> in the address field. Press **Enter** to establish the connection.



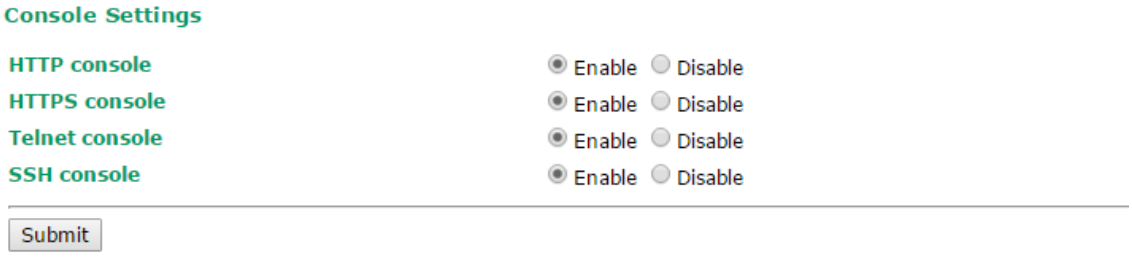
2. Warning messages will pop out to warn users that the security certificate was issued by a company they have not chosen to trust.

Select **Yes** to accept the certificate issued by Moxa and then enter the AWK-1137C's web browser interface secured via HTTPS/SSL. (You can see the protocol in URL is **https**.) Then you can use the menu tree on the left side of the window to open the function pages to access each of AWK-1137C's functions.



Disabling Telnet and Browser Access

If you are connecting the AWK-1137C to a public network but do not intend to use its management functions over the network, then we suggest disabling both Telnet Console and Web Configuration. Please run **Maintenance** → **Console Settings** to disable them, as shown in the following figure.



Configuration by the RS-232 Console

The RS-232 console configuration method is for use only by Moxa service engineer in case of trouble shooting

A

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your AWK-1137Cs 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, the time stamp, Delivery Traffic Indicator Maps (DTIM), and the Traffic Indicator Message (TIM). Beacon Interval indicates the frequency interval of an 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. A lower DTIM setting results in more efficient networking by preventing your PC from dropping into power-saving sleep mode. Higher settings allow your PC to enter sleep mode, thus saving power.

Fragment

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

RTS Threshold

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

B

Supporting Information

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

The following topics are covered in this appendix:

- **Firmware Recovery**
- **Declaration of Conformity**
  - Federal Communication Commission Interference Statement
  - RED Compliance Statement

Firmware Recovery

When the LEDs of **FAULT**, **Signal Strength** and **WLAN** all light up simultaneously and blink at one-second interval, it means the system booting has failed. It may result from some wrong operation or uncontrollable issues, such as an unexpected shutdown during firmware update. The AWK-1137C is designed to help administrators recover such damage and resume system operation rapidly. You can refer to the following instructions to recover the firmware:

Connect to the AWK-1137C's ES-232 console with **115200bps and N-8-1**. You will see the following message shown on the terminal emulator every one second.

```
please set-up TFTP server 192.168.127.1 contains awk1137c.rom for firmware recovery.
please set-up TFTP server 192.168.127.1 contains awk1137c.rom for firmware recovery.
please set-up TFTP server 192.168.127.1 contains awk1137c.rom for firmware recovery.
please set-up TFTP server 192.168.127.1 contains awk1137c.rom for firmware recovery.
please set-up TFTP server 192.168.127.1 contains awk1137c.rom for firmware recovery.
please set-up TFTP server 192.168.127.1 contains awk1137c.rom for firmware recovery.
```

Take the following steps for the firmware recovery:

1. Change the IP address of the laptop to 192.168.127.1.
2. Set up a TFTP sever on your laptop.
3. Download the AWK-1137C's firmware from Moxa's Website
4. Change the firmware file name to *awk1137c*.rom
5. Connect to the AWK-1137C's RJ45 Ethernet port

If the setting is correct, you will see the following message shown on the terminal emulator, and the AWK-1137C will reboot when the firmware recovery process has finished.

```
Trying eth0
Using eth0 device
TFTP from server 192.168.127.1; our IP address is 192.168.127.253
Filename 'awk1137c.rom'.
Load address: 0x80060000
Loading:
*#################################################################
#################################################################
#################################################################
```

Declaration of Conformity

Federal Communication Commission Interference Statement

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

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

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

FCC Radiation Exposure Statement

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

Within the 5.15-5.25 GHz band, U-NII devices will be restricted to indoor operations to reduce any potential for harmful interference to co-channel MSS operations.

RED Compliance Statement

Hereby, MOXA declares that this AWK-1137C is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

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

Moxa declares that the apparatus AWK-1137C 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 guidelines of this and of the computer manufacturer must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries 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.