WAC-2004A User’s Manual

Version 1.0, October 2021

www.moxa.com/product

WAC-2004A User’s Manual

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

Copyright Notice

Trademarks

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

Disclaimer

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

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

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

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

Technical Support Contact Information

www.moxa.com/support

Moxa Americas

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

Moxa Europe

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

Moxa India

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

Moxa China (Shanghai office)

Toll-free:	800-820-5036
Tel:	+86-21-5258-9955
Fax:	+86-21-5258-5505

Moxa Asia-Pacific

Tel:	+886-2-8919-1230
Fax:	+886-2-8919-1231

Table of Contents

1

Introduction

The WAC-2004A is Moxa’s high-end Wireless Access Controller that incorporates with the **TAP-213 Series**, **TAP-323 Series**, and **AWK 3131A-RTG (Rail Train to Ground) Series** and is designed **specifically for Railway applications**. The WAC-2004A supports not only single-subnet roaming (Layer 2), but also allows roaming between multiple subnets (Layer 3) with Mobile IP technology.

The following topics are covered in this chapter:

Overview

The goal of zero-latency roaming is to allow clients to seamlessly maintain their communications as they move from one access point to another. The advanced Moxa Wireless Access Controller, WAC-2004A, together with controller-based Turbo Roaming technology, enables **millisecond-level roaming over multiple IP subnets.** The advanced roaming algorithm, along with Mobile IP technology, allows wireless clients to roam between APs in different IP subnets within milliseconds while upholding stringent security in extremely demanding environments. The WAC-2004A is rated to operate at temperatures of 0 to 50°C and is rugged enough for on-site installation in any harsh industrial environment.

Package Checklist

The WAC-2004A Series wireless access controller is shipped with the following items. If any of these items are missing or damaged, please contact your customer service representative.

- WAC-2004A Series wireless controller
- 2 AC power cords (C13 type, US and EU)
- 1 serial console cable (DB9 type, female-to-female)
- 2 RJ45 connector protective caps
- Rackmount kit
- Quick installation guide (printed)
- Warranty card

NOTE It is required to use an IEC C13 type connector for the AC power cord. The WAC-2004A package comes with two AC power cords, one US and one EU type. To connect the second power input to the WAC-2004A, an additional power cord of the same type can be purchased separately.

Product Features

Advanced Turbo Roaming Support

- Layer-3 Mobile IP tunneling roaming (Controller + HA)
- Millisecond level L2 and L3 handover
- Wireless security support:
  - ➢ WPA/WPA2-Personal/Enterprise
  - ➢ EAP methods: TLS, TTLS, PEAP
- Sub-50 ms inter-controller handover
- Sub-500 ms controller backup recovery
- WAC-Centralized CCoA assignment
- Inter-WAC security setting

Value-added Networking Functions

- Number of supported AP/Clients for Turbo Roaming
  - ➢ Layer 2 networks: Up to 190 clients roaming between 400 APs
  - ➢ Layer 3 networks: Up to 100 clients roaming between 190 APs
- Ethernet port-binding for Ethernet redundancy
- 450 Mbps of total tunneling bandwidth
- 1+1 WAC/HA hot swap redundancy
- Configuration back-up with ABC-01

Useful Utilities and Remote Configuration

- Serial/Telnet console management
- Web Console (HTTP/HTTPS) management
- Firmware upgrade from TFTP, Web Console, and utility
- Supports SNMP
- Configuration backup and reset

Industrial-grade Design

- Rackmount fanless design
- Redundant power

Product Specifications

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

ATTENTION

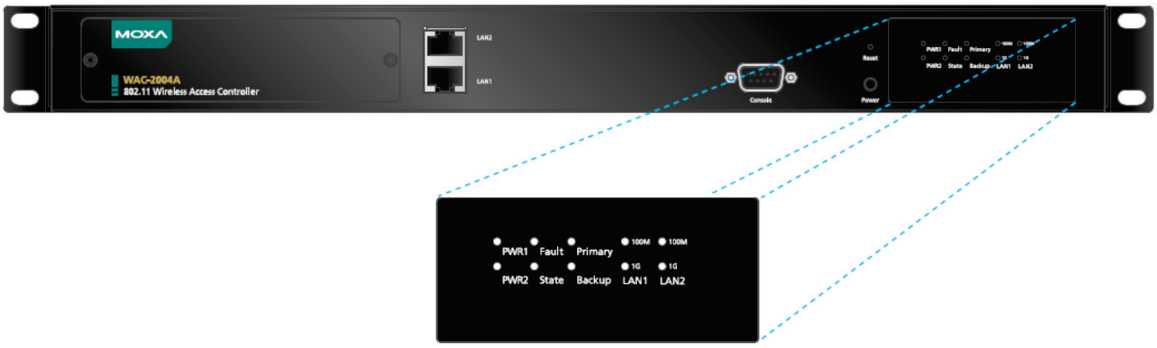
The WAC-2004A is NOT designed for use by the general public. A well-trained technician is required to safely deploy the WAC-2004A.

Interface Specifications

This section provides detailed introduction on the WAC-2004A interfaces.

LED Indicators

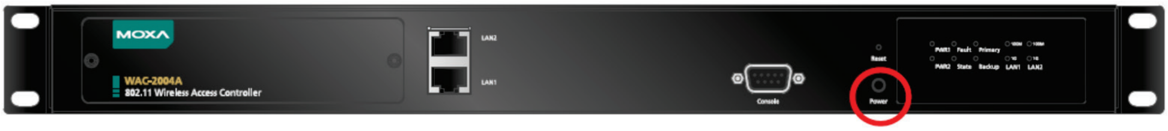
The LEDs on the front panel of the WAC-2004A provide quick and easy means of determining the current operational status and wireless settings.



LED	Color	State	Description
PWR1	Green	On	Power is being supplied from power input 1.
		Off	Power is not being supplied from power input 1.
PWR2	Green	On	Power is being supplied from power input 2.
		Off	Power is not being supplied from power input 2.
Fault	Red	On	Booting; System Error.
		Blinking (fast)	IP address conflict (interval: 0.5 sec).
		Off	Normal status.
State		Green	Software is ready.

LED	Color	State	Description
	Green/ Red	Green (Blinking)	The device has been located by the Search Utility (interval: 1 sec).
		Red	Booting error.
Primary	Green	On	The device is operating as the primary roaming controller.
		Off	The device is not operating as the primary roaming controller.
Backup	Green	On	The device is operating as the backup roaming controller.
		Off	The device is not operating as the backup roaming controller.
LAN 1,2 1G (2 reserved)	Green	On	1 Gbps link established on the port.
		Blinking	The device has been located by the Search Utility (interval: 1 sec).
		Off	No link detected on the port.
LAN 1,2 100M (2 reserved)	Amber	On	100 Mbps link established on the port.
		Blinking	The device has been located by the Search Utility (interval: 1 sec).
		Off	No link detected on the port.

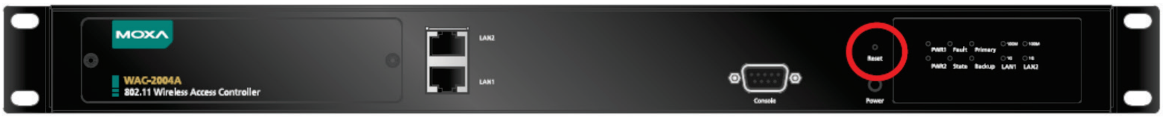
Power Button



The Power button located on the front panel of WAC-2004A is for **powering off the device ONLY**.

To power off the device, press the Power button for more than 5 seconds and release.

Reset Button

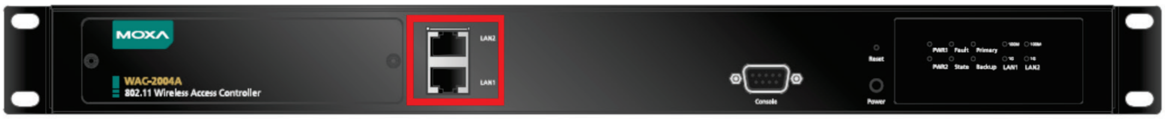


The RESET button located on the front panel of WAC-2004A is for **power reset ONLY**.

To reboot the WAC-2004A, press and release the RESET button with a pointed object, such as an unfolded paper clip.

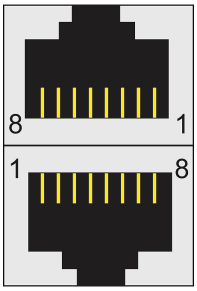
NOTE For configuration reset:
Web Console (HTTP/HTTPS): Maintenance → Load Factory Default
Telnet/Serial Console: System Maintenance → Load Factory Default

Gigabit Ethernet Port Connection



The WAC-2004A offers one pair of Gigabit Ethernet ports with the port binding feature enabled (LAN 1 and LAN 2) for Ethernet failover redundancy. When the cable is properly connected, the LED on the front panel will glow to indicate a proper connection.

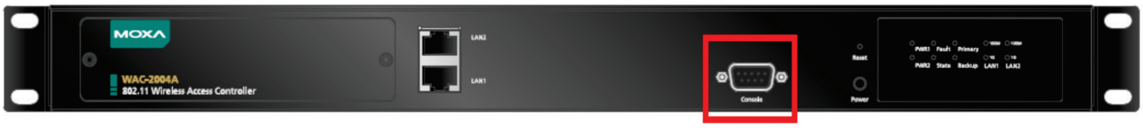
See below for detailed pin assignment and LED indication:



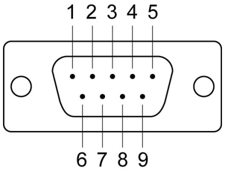
Pin	10/100 Mbps	1000 Mbps
1	ETx+	TRD(0)+
2	ETx-	TRD(0)-
3	ERx+	TRD(1)+
4	---	TRD(2)+
5	---	TRD(2)-
6	ERx-	TRD(1)-
7	---	TRD(3)+
8	---	TRD(3)-

NOTE The pin numbers for the 8-pin RJ45 connectors (and ports) are typically not labeled on the connector (or port). Refer to the diagram above to see how the RJ45 pins are numbered.

Serial Console Connection



The WAC-2004A offers a serial port with DB9 male connector for its console access. The pin assignments are shown in the following table:

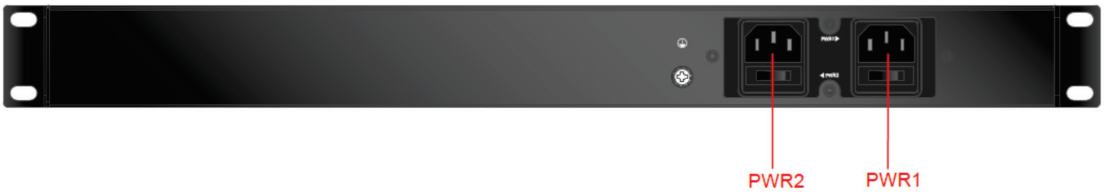


Pin	RS-232
1	DCD
2	RxD
3	TxD
4	DTR
5	GND
6	DSR
7	RTS
8	CTS

NOTE The pin numbers for the male DB9 connectors are stated in the table above. The pinhole numbers for the female DB9 connectors are usually labeled on the connector. However, the numbers are typically very small, so you may need to use a magnifying glass to see the numbers clearly.

Power Socket

The WAC-2004A offers a dual power supply for power failover redundancy. Input voltage ranges from **100 to 240 VAC/VDC, 47 to 63 Hz,** with two male **C14** inlets. The WAC-2004A is shipped with 2 power cords, one US type and one EU type. To connect the secondary power input on the WAC-2004A, an additional power cord of the same type can be purchased separately.



Beeper

The beeper emits one short beep when the power is turned on and two short beeps when the system is ready. When the device is located by the Search Utility, the beeper emits beeps every second to indicate its location.

2

Getting Started

This chapter explains how to access the WAC-2004A for the first time. There are three ways to access the controller: (1) Web Console, (2) Telnet Console, or (3) Serial Console. The Web and Telnet Consoles are suitable for remote management as the controller can be accessed over an existing network. The Serial Console can be used if you do not have the WAC-2004A's IP address; however it requires using a RS-232 serial cable to connect WAC-2004A to your PC's COM port.

In addition, the Web Console provides a more complete collection of functions for status monitoring and controller administration; where the Telnet and Serial Consoles only provide basic administration functions.

The following topics are covered in this chapter:

❒ **Using the Web Console to Access the WAC-2004A**

❒ **Using the Telnet Console to Access the WAC-2004A**

❒ **Using the Serial Console to Access the WAC-2004A**

Using the Web Console to Access the WAC-2004A

The WAC-2004A's Web Console provides a convenient way to modify controller configuration, monitor the controller and governed AP/Client status, and upgrade FW remotely over an existing network. The recommended web browser is Microsoft® Internet Explorer 8.0 or later releases with JVM (Java Virtual Machine).

Default Web Console access information	
IP	192.168.127.253
Submask	255.255.255.0
Username	admin
Password	moxa

NOTE To use the WAC-2004A's management and monitoring functions from a PC host connected to the same LAN as the WAC-2004A, you must make sure that the PC host and the WAC-2004A are on the same logical subnet. The WAC-2004A's default IP is 192.168.127.253.

Step 1: Connect the WAC-2004A to a notebook or PC with an Ethernet cable

The WAC-2004A supports MDI/MDI-X auto-sensing so you can use either a straight-through cable or crossover cable to connect the WAC-2004A to your computer.

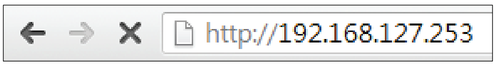
Step 2: Setting up the computer IP address

Choose an IP address on the same subnet as the WAC-2004A. Since the WAC-2004A'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/24.

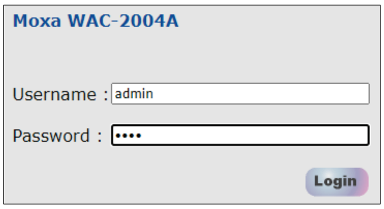
NOTE If you select Maintenance → Load Factory Default and click the Submit button, the WAC-2004A will be reset to factory default settings and the IP address will be reset back to 192.168.127.253/24.

Step 3: Use the web-based manager to configure the WAC-2004A

Open your computer web browser and type http://192.168.127.253 in the address field to access the homepage of the WAC-2004A Web Console. For first-time configuration, enter the default username **admin** and password **moxa** and click the Login button:



http://192.168.127.253



Moxa WAC-2004A

Username : admin

Password : ••••

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

ATTENTION

For security reasons, each authenticated login will have a 5-minute idle timeout. If your session is left idle for more than 5 minutes, you will need to re-authenticate your login.

NOTE After clicking **Submit** to apply changes, the web page will refresh and (Updated) will appear on the page, and at the same time, a flashing reminder on the upper-right corner of the web page will be displayed

To activate the changes, click the **Restart** button, and then the **Save** and **Restart** button. It will take about 40 seconds for the WAC-2004A to complete the reboot procedure.

Using the Telnet Console to Access the WAC-2004A

For basic configuration, Telnet is another option.

Default Telnet console access information	
IP	192.168.127.253
Submask	255.255.255.0
Username	admin
Password	moxa

Step 1: Connect the WAC-2004A to a notebook or PC with an Ethernet cable

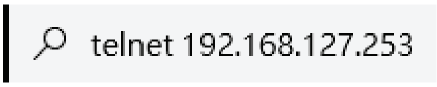
The WAC-2004A supports MDI/MDI-X auto-sensing so you can use either a **straight-through cable** or **crossover cable** to connect the WAC-2004A to your computer.

Step 2: Setting up the computer IP address

Choose an IP address on the same subnet as the WAC-2004A. Since the WAC-2004A'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/24.

Step 3: Establish Telnet connection.

On Windows 10, type "telnet [ip address]" in the search bar (see below)
(You may also issue the telnet command from the Windows command prompt.).

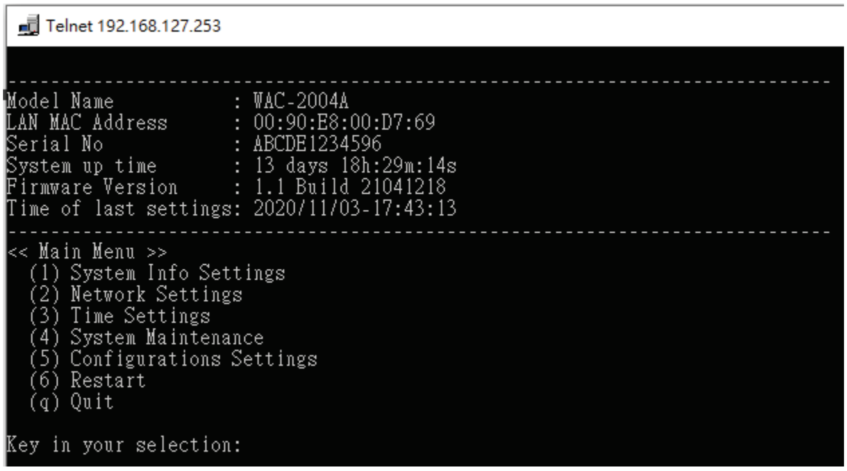


```
telnet 192.168.127.253
```

NOTE The Telnet client built into Windows 10 is disabled by default. To enable it, type "Turn Windows Features on or off" in the search bar. Next, in the Windows Features list, check the box for **Telnet Client** and click **Ok**.

Step 4: Authentication for Telnet console access

After the Telnet connection is established, you will be asked to enter username and password. For first-time configuration, use the default username **admin** and password **moxa**.



Telnet 192.168.127.253

```
------------------------------------------------------------------------
Model Name          : WAC-2004A
LAN MAC Address     : 00:90:E8:00:D7:69
Serial No           : ABCDE1234596
System up time      : 13 days 18h:29m:14s
Firmware Version    : 1.1 Build 21041218
Time of last settings: 2020/11/03-17:43:13
------------------------------------------------------------------------
<< Main Menu >>
  (1) System Info Settings
  (2) Network Settings
  (3) Time Settings
  (4) System Maintenance
  (5) Configurations Settings
  (6) Restart
  (q) Quit

Key in your selection:
```

Step 5: Basic text-based management interface

Once authentication is complete, a list of text-based menu will be available to you. The following is a summary on the menu items:

Item	Label	Description
1	System Info Settings	Basic system information, such as Device name, Device location, Device description, Device contact information.
2	Network Settings	Basic network parameters, such as IP configuration (IP mode), IP address, subnet mask, gateway, and DNS settings.
3	Time Settings	Basic time settings, including Static Time and Time Server settings.
4	System Maintenance	Reset configuration back to factory default.
5	Configuration Settings	Show, configure, and save configuration and TFTP settings.
	Restart	Reboot the system.
q	Quit	Exit Telnet console.

Using the Serial Console to Access the WAC-2004A

If you do not have the WAC-2004A's IP address, but you can physically reach the device, use the Serial Console to manage the device or obtain the IP address.

Default Serial Console access information	
Baud Rate	115200
Data Bits	8
Parity	None
Stop Bits	1
Terminal	VT100
Username	admin
Password	moxa

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

Step 1: Connect the WAC-2004A to your computer

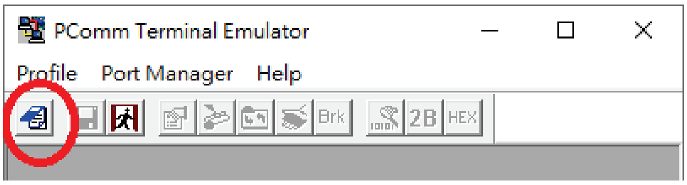
Before running PComm Terminal Emulator, use a DB9 female to DB9 female crossover serial cable to connect the WAC-2004A to your PC's COM port

Step 2: Connect to the WAC-2004A Serial Console

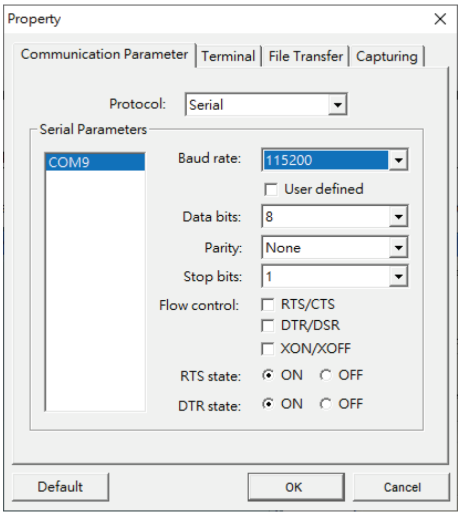
After installing the emulator software, type "PComm Terminal Emulator" in the search bar and open the software.

PComm Terminal Emulator

Use the Open icon or select Open in the Port Manager menu to establish a new connection.
The Communication Parameter page of the Property window will appear.



Select the appropriate COM port for Console Connection, 115200 for Baud Rate, 8 for Data Bits, None for Parity, and 1 for Stop Bits.



Protocol: Serial

Serial Parameters

COM9

Baud rate: 115200

□ User defined

Data bits: 8

Parity: None

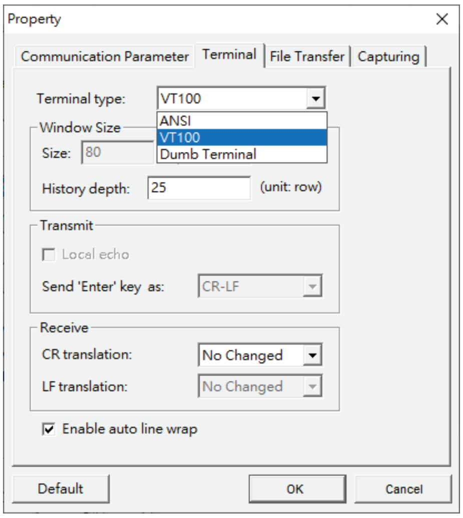
Stop bits: 1

Flow control: □ RTS/CTS □ DTR/DSR □ XON/XOFF

RTS state: ● ON ○ OFF

DTR state: ● ON ○ OFF

Click the Terminal tab, and select VT100 for Terminal Type. Click **OK** to establish the connection.



Terminal type: VT100

Window Size

Size: 80

History depth: 25 (unit: row)

Transmit

□ Local echo

Send 'Enter' key as: CR-LF

Receive

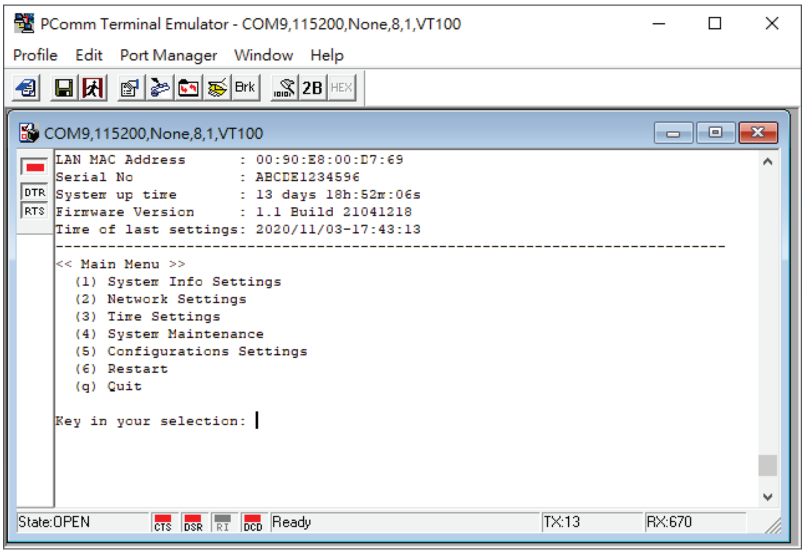
CR translation: No Changed

LF translation: No Changed

☑ Enable auto line wrap

Step 3: Authentication for Serial Console access

After the connection is established, you will be asked to enter username and password. For first-time configuration, please use the default username **admin** and password **moxa**.



```
LAN MAC Address      : 00:90:E8:00:D7:69
Serial No            : ABCDE1234596
System up time       : 13 days 18h:52m:06s
Firmware Version     : 1.1 Build 21041218
Time of last settings: 2020/11/03-17:43:13
-----------------------------------------------------------------------------
<< Main Menu >>
  (1) System Info Settings
  (2) Network Settings
  (3) Time Settings
  (4) System Maintenance
  (5) Configurations Settings
  (6) Restart
  (q) Quit

Key in your selection: 
```

Step 4: Basic text-based management interface

(Please refer to section: Using the Telnet Console to Access the WAC-2004A)

ATTENTION

If you unplug the RS-232 cable or turn off the DTR, the session will be disconnected and you will be automatically logged out to ensure network security. You will need to log in again to resume operation.

3

Web Console Configuration

The WAC-2004A's Web Console provides a convenient way to modify the controller's configuration, monitor the controller and governed AP/Client status, and upgrade FW remotely over an existing network. The recommended web browser is Microsoft® Internet Explorer 8.0 or later releases with JVM (Java Virtual Machine).

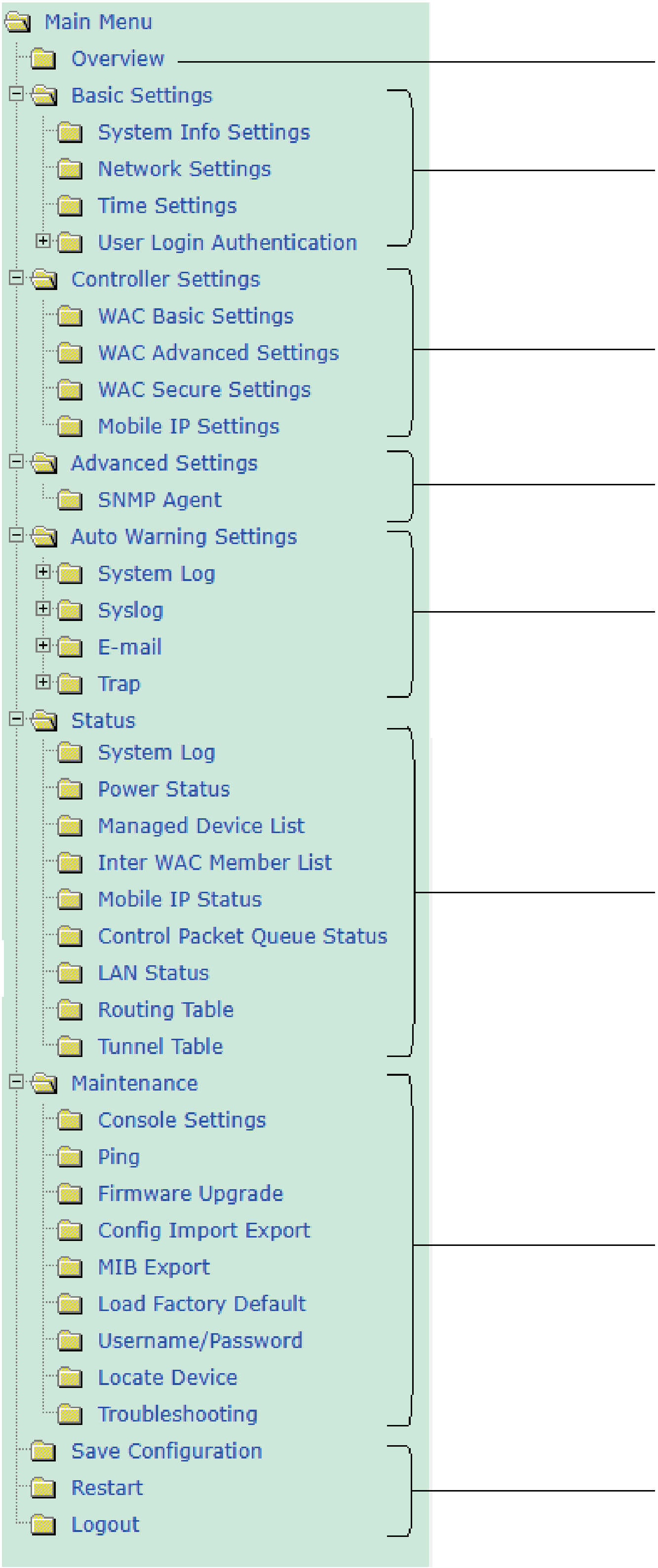
This chapter provides a detailed introduction and description to each WAC-2004A management function. For information on how to access Web Console, please refer to **Chapter 2: Using the Web Console to Access the WAC-2004A**.

The following topics are covered in this chapter:

- **Function Map**
- **Overview**
- **Basic Settings**
  - System Info Settings
  - Network Settings
  - Time Settings
  - User Login Authentication
- **Controller Settings**
  - WAC Basic Settings
  - WAC Advanced Settings
  - WAC Security Settings
  - Mobile IP Settings
- **Advanced Settings**
  - SNMP Agent
- **Auto Warning Settings**
  - System Log
  - Syslog
  - E-mail
  - Trap
- **Status**
  - System Log
  - Power Status
  - Managed Device List
  - Inter WAC Member List
  - Mobile IP Status
  - Control Packet Queue Status
  - LAN Status
  - Routing Table
  - Tunnel Table
- **Maintenance**
  - Console Settings
  - Ping
  - Firmware Upgrade
  - Config Import Export
  - MIB Export
  - Load Factory Default
  - Username/Password
  - Locate Device
  - Troubleshooting
- **Save Configuration**
- **Restart**
- **Logout**

Function Map

The Function Map provides a convenient means of determining which functions you need to use.



Quick overview of the WAC-2004A's status

Basic settings for administering the WAC-2004A

Essential settings for setting up the wireless access controller

Optional advanced features for additional network management

Optional application-oriented device management functions for setting up events logs, SNMP traps, and e-mail notifications

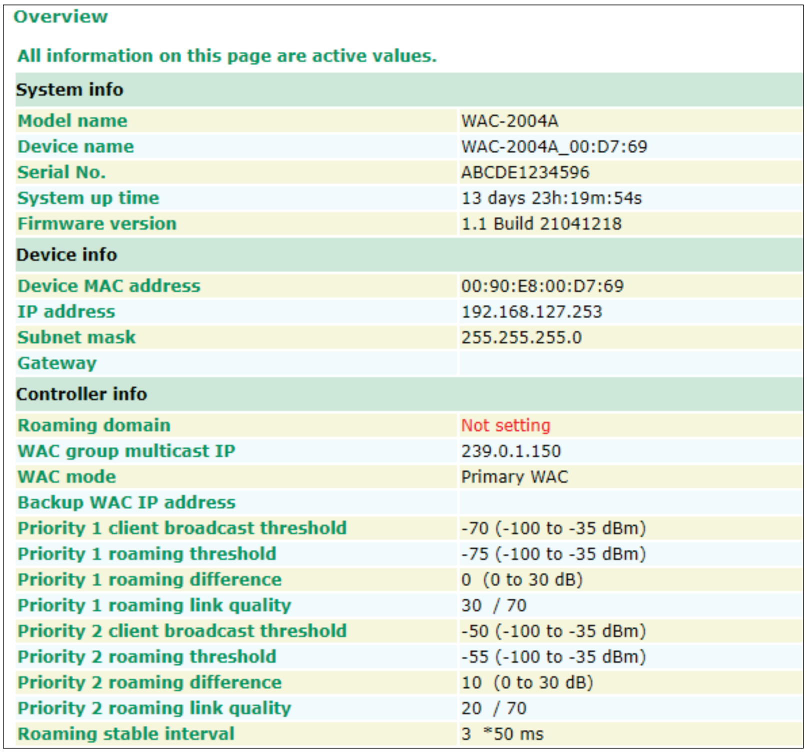
Real-time status information for performance monitoring and device management functions

Functions for maintaining the WAC-2004A and diagnosing the network

On-demand functions for web-based console operations

Overview

The **Overview** page summarizes the WAC-2004A's current status. The information is categorized into several groups: **System info**, **Device info**, and **Controller info**.



Overview

All information on this page are active values.

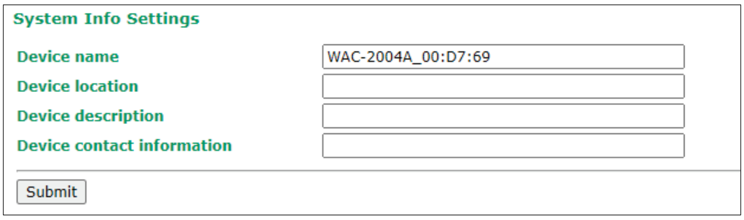
System info	
Model name	WAC-2004A
Device name	WAC-2004A_00:D7:69
Serial No.	ABCDE1234596
System up time	13 days 23h:19m:54s
Firmware version	1.1 Build 21041218
Device info	
Device MAC address	00:90:E8:00:D7:69
IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	
Controller info	
Roaming domain	Not setting
WAC group multicast IP	239.0.1.150
WAC mode	Primary WAC
Backup WAC IP address	
Priority 1 client broadcast threshold	-70 (-100 to -35 dBm)
Priority 1 roaming threshold	-75 (-100 to -35 dBm)
Priority 1 roaming difference	0 (0 to 30 dB)
Priority 1 roaming link quality	30 / 70
Priority 2 client broadcast threshold	-50 (-100 to -35 dBm)
Priority 2 roaming threshold	-55 (-100 to -35 dBm)
Priority 2 roaming difference	10 (0 to 30 dB)
Priority 2 roaming link quality	20 / 70
Roaming stable interval	3 *50 ms

Basic Settings

The Basic Settings group includes the most commonly used settings required by administrators to maintain and control the WAC-2004A.

System Info Settings

The **System Info** items, especially ***Device name** and **Device description**,* are displayed and included on the **Overview** page, in SNMP information, and in alarm emails. Setting **System Info** items makes it easier to identify the different WAC-2004A units connected to your network.



System Info Settings

Device name	WAC-2004A_00:D7:69
Device location	
Device description	
Device contact information	

Device name

Setting	Description	Factory Default
Max. 31 of characters	This option is useful for specifying the role or application of different WAC-2004A units.	WAC-2004A_<last 3 bytes of the device's MAC address>

Device location

Setting	Description	Factory Default
Max. of 31 characters	Specifies the location of different WAC-2004A units.	None

Device description

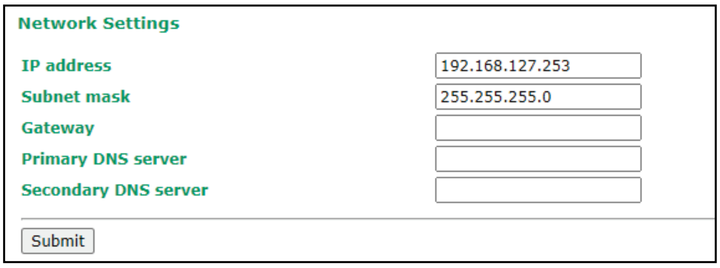
Setting	Description	Factory Default
Max. of 31 characters	Use this space to record a more detailed description of the WAC-2004A.	None

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 WAC-2004A.	None

Network Settings

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



Network Settings

IP address	192.168.127.253
Subnet mask	255.255.255.0
Gateway	
Primary DNS server	
Secondary DNS server	

IP address

Setting	Description	Factory Default
WAC-2004A IP address	Identifies the WAC-2004A on a TCP/IP network.	192.168.127.253

Subnet mask

Setting	Description	Factory Default
WAC-2004A subnet mask	Identifies the type of network to which the WAC-2004A 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

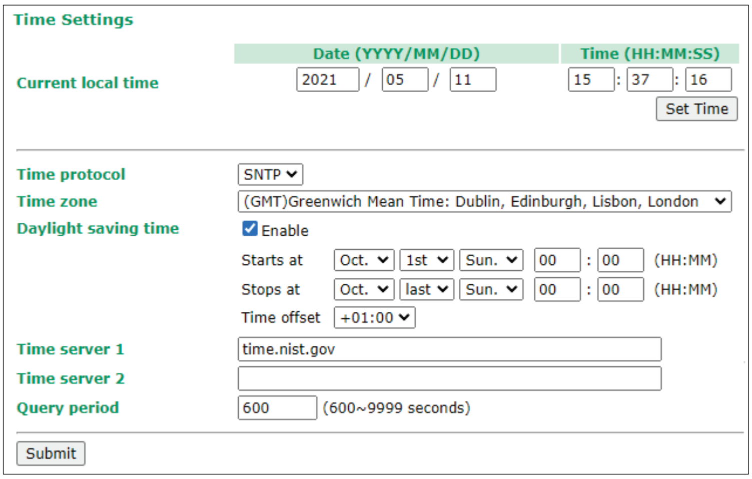
Setting	Description	Factory Default
WAC-2004A default gateway	The IP address of the router that connects the LAN to an outside network.	None

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 WAC-2004A's URL (e.g., http://ap11.abc.com) in your browser's address field instead of entering the IP address. The Secondary DNS server will be used if the Primary DNS server fails to connect.	None

Time Settings

The WAC-2004A has a time calibration function based on information from an NTP server or user specified Date and Time information. Functions such as Auto warning can add real-time information to the message.



Time Settings

	Date (YYYY/MM/DD)	Time (HH:MM:SS)
Current local time	2021 / 05 / 11	15 : 37 : 16

Time protocol: SNTP
Time zone: (GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
Daylight saving time: ☑ Enable
Starts at: Oct. 1st Sun. 00 : 00 (HH:MM)
Stops at: Oct. last Sun. 00 : 00 (HH:MM)
Time offset: +01:00
Time server 1: time.nist.gov
Time server 2:
Query period: 600 (600~9999 seconds)

The ***Current local time*** shows the WAC-2004A's system time when you open this web page. You can click on the **Set Time** button to activate the updated date and time parameters. An "(Updated)" string will appear to indicate that the change is complete. Local time settings will be immediately activated in the system without running Save and Restart.

NOTE The WAC-2004A has a built-in real time clock (RTC). We strongly recommend that users update the **Local time** for the WAC-2004A 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 if 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	Local time

Time protocol

Setting	Description	Factory Default
User-selectable time synchronization protocol	The time protocol setting allows the user to select the time synchronization protocol, either NTP or SNTP.	SNTP

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

Because the current local time will be adjusted automatically as the time zone is being adjusted, you will need to configure the time zone prior to inputting the current local time.

Daylight saving time

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

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

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

Time server 1/2

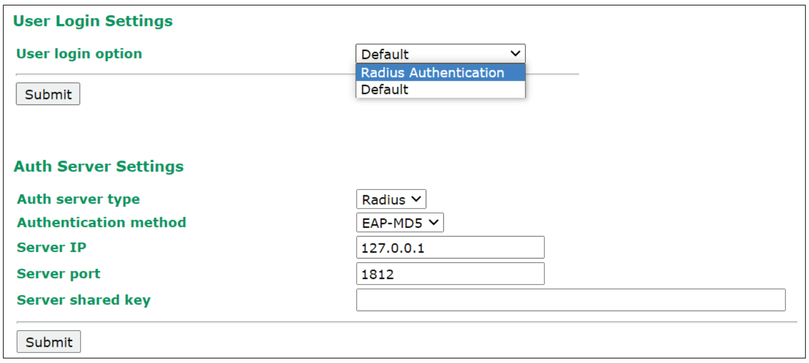
Setting	**Description**	**Factory Default**
IP/Name of Time Server 1/2	IP or Domain name of the NTP time server. The 2nd NTP server will be used if the 1st NTP server fails to connect.	time.nist.gov

Query period

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

User Login Authentication

The WAC-2004A supports user login authentication to verify users either locally or via a remote RADIUS server.



User Login Settings

User login option: Default

Auth Server Settings

Auth server type: Radius

Authentication method: EAP-MD5

Server IP: 127.0.0.1

Server port: 1812

Server shared key:

User login option

Setting	**Description**	**Factory Default**
User-selectable login option	The login method for users.	Default

Auth server type

Setting	**Description**	**Factory Default**
Server type	The type of server used for authenticating users.	Radius

Authentication method

Setting	**Description**	**Factory Default**
Protocol	The authentication protocol used by the remote RADIUS server to authenticate users.	EAP-MDS

Server IP

Setting	**Description**	**Factory Default**
IP address	The IP address of the remote RADIUS authentication server.	127.0.0.1

Server port

Setting	**Description**	**Factory Default**
Port number	The service port number of the remote RADIUS authentication server.	1812

Server shared key

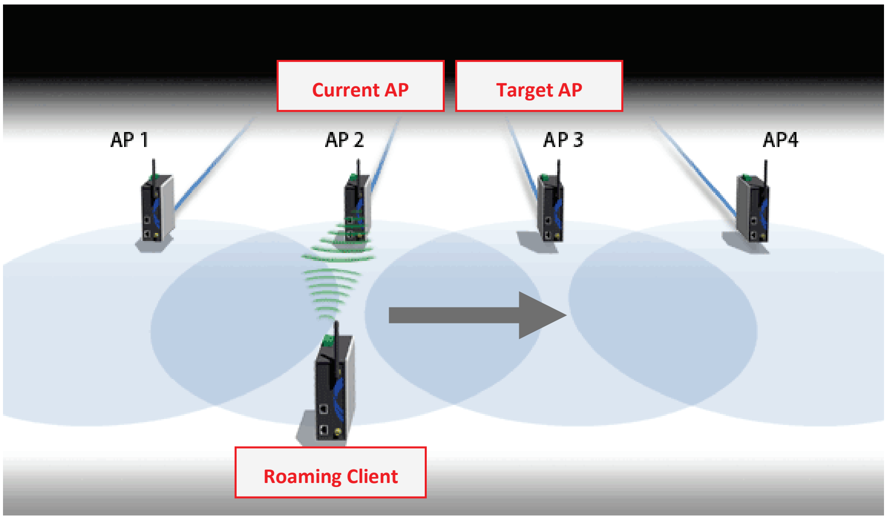
Setting	Description	Factory Default
Shared key value	The RADIUS login authentication key.	N/A

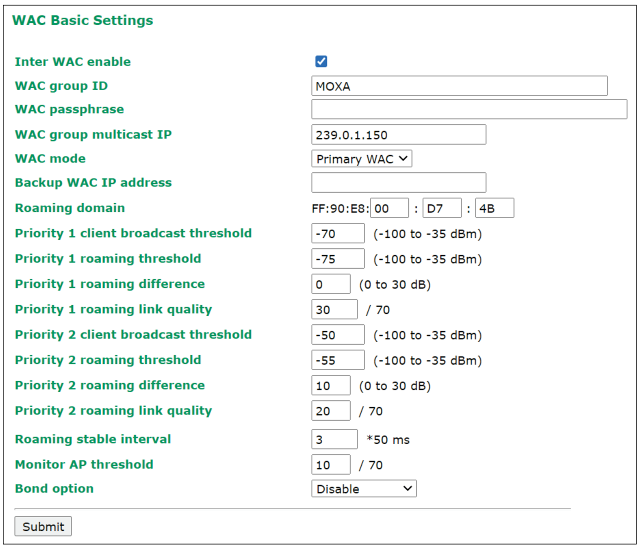
Controller Settings

The Controller Settings group includes the most important settings, which enable administrators to set up the Wireless Access Controller services.

WAC Basic Settings

The **controller information** (including Roaming domain, Roaming threshold, Roaming difference, etc…) are displayed on the **Overview** page.





WAC Basic Settings

Inter WAC enable	☑
WAC group ID	MOXA
WAC passphrase	
WAC group multicast IP	239.0.1.150
WAC mode	Primary WAC
Backup WAC IP address	
Roaming domain	FF:90:E8: 00 : D7 : 4B
Priority 1 client broadcast threshold	-70 (-100 to -35 dBm)
Priority 1 roaming threshold	-75 (-100 to -35 dBm)
Priority 1 roaming difference	0 (0 to 30 dB)
Priority 1 roaming link quality	30 / 70
Priority 2 client broadcast threshold	-50 (-100 to -35 dBm)
Priority 2 roaming threshold	-55 (-100 to -35 dBm)
Priority 2 roaming difference	10 (0 to 30 dB)
Priority 2 roaming link quality	20 / 70
Roaming stable interval	3 *50 ms
Monitor AP threshold	10 / 70
Bond option	Disable

Inter WAC enable

For WACs located in different areas or different subnets, the Inter WAC function creates a cluster/group of multiple WACs to service wireless clients, enabling clients to roam between WAC controllers in this group.

Setting	Description	Factory Default
Enable/Disable	Enable or disable the Inter WAC feature.	Disable

WAC group ID

Setting	Description	Factory Default
Max. 31 of characters	The group ID for WACs to recognize each other as a member of the same WAC community, and hence the inter WAC feature will operate properly.	MOXA

WAC passphrase

Setting	Description	Factory Default
Max. 63 of characters (masked)	The passphrase for inter WAC security and to prevent rouge WAC.	None

WAC group multicast IP

Setting	Description	Factory Default
Multicast IP	The multicast IP address for inter WAC communication.	239.0.1.150

WAC mode

Setting	Description	Factory Default
Primary WAC	Act as the primary WAC.	Primary WAC
Backup WAC	Act as a backup WAC.	

Primary/Backup WAC IP address

Setting	Description	Factory Default
IP address	The IP address of the pairing controller, when one fails, another controller will take over its function in the network (within 500ms).	None

Roaming domain

Setting	Description	Factory Default
6 Hex characters	This specifies the area served by the WAC-2004A. All related controllers, APs, and clients use this as identification to work and communicate with each other.	<The Mac address of the WAC-2004A>

NOTE The **Roaming domain** must be set at the time of initial (first time) installation.
Configure the priority 1 or 2 roaming settings for the access points.

The roaming priority should be set based on how the radios are deployed along the trackside.

Priority 1: For radios along the trackside that are deployed with leaky feeder-like coverage patterns.

Priority 2: For radios along the trackside that are deployed with open air radiating antennas.

Due to the differences in coverage patterns between different deployment scenarios, the roaming priority that user selects will impact roaming performance.

Priority 1/2 client Broadcast threshold

Setting	Description	Factory Default
Signal strength (dBm)	The signal strength of the current Client must be lower than this threshold.	Priority 1: -70 Priority 2: -55

Priority 1/2 roaming threshold

Setting	Description	Factory Default
Signal strength (dBm)	The signal strength of the current AP and Client must be lower than this threshold.	Priority 1: -75 Priority 2: -55

Priority 1/2 roaming difference

Setting	Description	Factory Default

Relative value (dB)	The signal strength between the target AP and Client must be greater than this value	Priority 1: 0 Priority 2: 10

Priority 1/2 roaming link quality

Setting	Description	Factory Default
Link quality (Integer)	The link quality (signal strength – Background noise) between the target AP and Client must be greater than this threshold	Priority 1: 30 Priority 2: 20

Roaming stable interval

Setting	Description	Factory Default
Multiple of 50ms (Integer)	The "roaming threshold", "roaming difference", and "roaming link quality" status must stay true for X amount of time to ensure a stable state.	3 (x 50 ms)

Monitor AP threshold

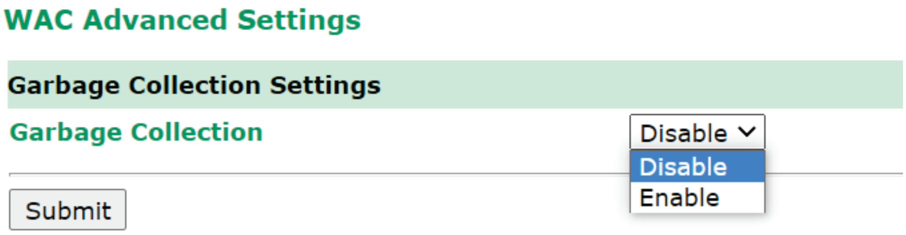
Setting	Description	Factory Default
Link quality (Integer)	The link quality (signal strength – background noise) between the Monitor AP and Client must be greater than this threshold.	10

Bond option

Setting	Description	Factory Default
Enable/Disable	Enable or disable the LAN1/2 port bonding feature for Ethernet connection redundancy.	disable

WAC Advanced Settings

The WAC Advanced Settings provide additional functions to monitor and manage some of the system resources. Unused data such as idle wireless clients, IP tunnels, routing table entries, will be detected and cleared automatically if the Garbage Collection Settings function is enabled.



WAC Advanced Settings

Garbage Collection Settings

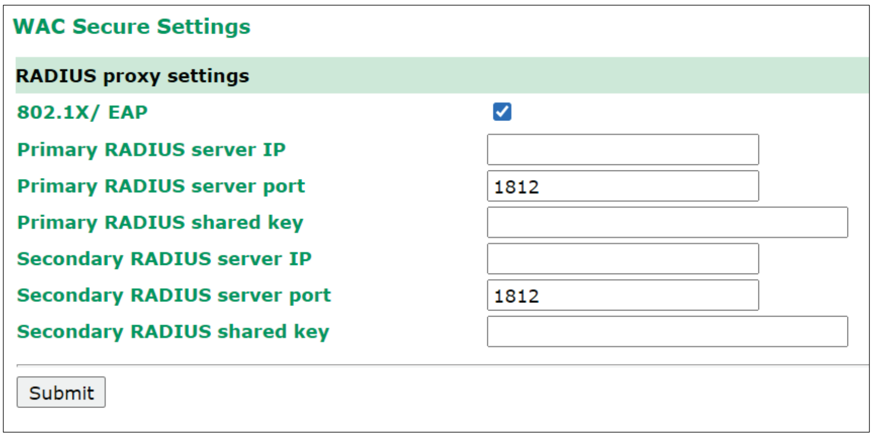
Garbage Collection: Disable

Garbage Collection

Setting	Description	Factory Default
Enable/Disable	Enable or disable the Garbage Collection function to clean up unused data.	Disable

WAC Security Settings

By enabling the 802.1X/EAP on the WAC-2004A, the controller acts as an **authentication proxy/relay** between the APs and the RADIUS server. So when configuring your RADIUS server, instead of entering IPs for every authentication requester (in normal cases, it will be your APs), you only need to enter the IP for the WAC-2004A.



WAC Secure Settings

RADIUS proxy settings

802.1X/ EAP	☑
Primary RADIUS server IP	
Primary RADIUS server port	1812
Primary RADIUS shared key	
Secondary RADIUS server IP	
Secondary RADIUS server port	1812
Secondary RADIUS shared key	

802.1X/ EAP

Setting	Description	Factory Default
Enable/Disable	Enables EAP proxy/relay support.	Disable

Primary/ Secondary RADIUS server IP

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

Primary/ Secondary RADIUS server port

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

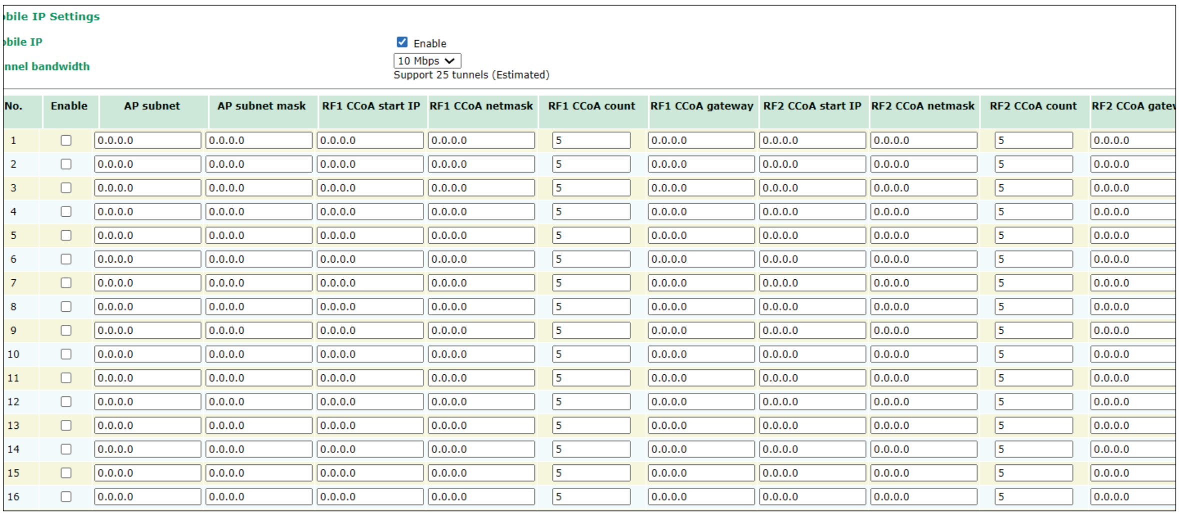
Primary/ Secondary RADIUS shared key

Setting	Description	Factory Default
Max. 63 characters	The secret key shared between the AP and RADIUS server.	None

NOTE The wireless security settings of all the APs that are deployed in the same **roaming domain** must be consistent and homogeneous. Different security settings in same-grouped APs may cause **Turbo Roaming** failures. Refer to the TAP-213 Series, TAP-323 Series, and AWK-RTG Series manual for detailed information about the wireless setting.

Mobile IP Settings

Mobile IP allows you to access the same IP address even when the Client is travelling across different subnets.



bile IP Settings

bile IP ☑ Enable

nnel bandwidth 10 Mbps
Support 25 tunnels (Estimated)

No.	Enable	AP subnet	AP subnet mask	RF1 CCoA start IP	RF1 CCoA netmask	RF1 CCoA count	RF1 CCoA gateway	RF2 CCoA start IP	RF2 CCoA netmask	RF2 CCoA count	RF2 CCoA gate
1	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
2	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
3	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
4	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
5	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
6	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
7	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
8	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
9	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
10	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
11	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
12	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
13	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
14	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
15	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0
16	□	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0	0.0.0.0	0.0.0.0	5	0.0.0.0

Mobile IP

Setting	Description	Factory Default
Enable/Disable	Enable or disable Mobile IP feature.	Disable

Tunnel bandwidth

Setting	Description	Factory Default
1-25 Mbps	Bandwidth per single Mobile IP tunnel (total bandwidth 450 Mbps).	10 Mbps

Enable

Setting	Description	Factory Default
Enable/Disable	Enable or disable a particular mobile rule.	Disable

AP subnet

Setting	Description	Factory Default
IP address	The IP address of the trackside access point.	0.0.0.0

AP subnet mask

Setting	Description	Factory Default
Subnet mask	The subnet mask of the trackside access point. Configure the subnet mask to limit the IP address range for the mobile IP network.	0.0.0.0

RF1/2 CCoA netmask

Setting	Description	Factory Default
Subnet mask	The subnet mask for CCoA IP Assignment.	0.0.0.0

RF1/2 CCoA start IP

Setting	Description	Factory Default
Starting CCoA IP address	The starting IP for CCoA IP Assignment for the specified subnet of each radio interface.	0.0.0.0

RF1/2 CCoA count

Setting	Description	Factory Default
Number of IPs	Number of IPs can be assigned in the specified subnet of each radio interface.	5

RF1/2 CCoA gateway

Setting	Description	Factory Default
Default gateway IP address	The default gateway for the specified CCoA subnet of each radio interface.	0.0.0.0

Advanced Settings

Advanced features to support additional network management.

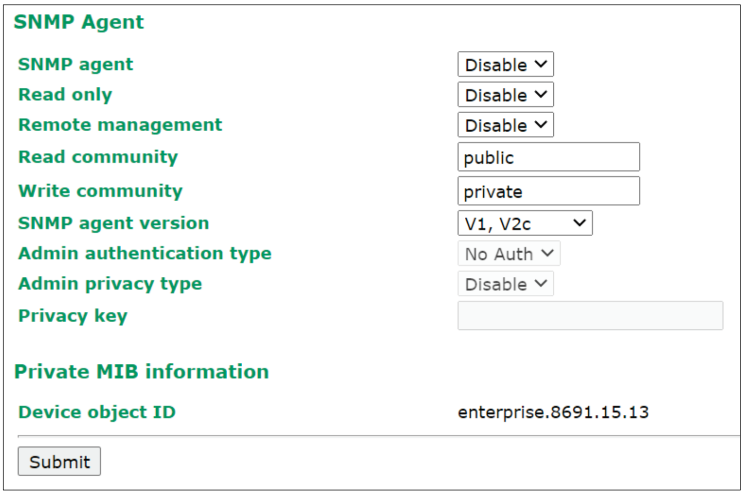
SNMP Agent

The WAC-2004A 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 WAC-2004A 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

SNMP agent	Disable
Read only	Disable
Remote management	Disable
Read community	public
Write community	private
SNMP agent version	V1, V2c
Admin authentication type	No Auth
Admin privacy type	Disable
Privacy key	

Private MIB information

Device object ID	enterprise.8691.15.13

SNMP Agent

Setting	Description	Factory Default
Enable/disable	Enable or disable the SNMP Agent.	Disable

Read only

Setting	Description	Factory Default
Enable/disable	Enable or disable the Read-only function for the SNMP Agent.	Disable

Remote management

Setting	Description	Factory Default
Enable/disable	Enable or disable the remote management through different subnets.	Disable

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 WAC.	V1, V2c

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

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

SHA	Provides authentication based on HMAC-SHA algorithms. 8-character passwords are the minimum requirement for authentication.	

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

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

Private Key

Setting	Description	Factory Default
Max. 63 characters	A data encryption key is the minimum requirement for data encryption.	None

Private MIB Information Device Object ID

Also known as ***OID***, this is the WAC-2004A's enterprise value and is fixed.

Auto Warning Settings

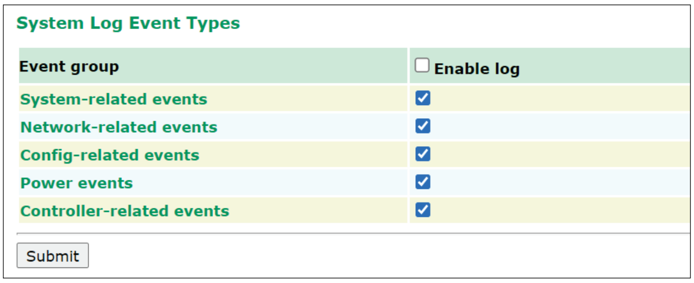
Since industrial-grade devices are often located at the endpoints of a system, these devices will not always know what is happening elsewhere on the network. This means that these devices, including wireless APs or clients, must provide system maintainers with real-time alarm messages. Even when system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

In addition to logging these events, the WAC-2004A supports different approaches to warn engineers automatically, such as SNMP trap, and e-mail.

System Log

System Log Event Types

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



System Log Event Types

Event group	□ Enable log
System-related events	☑
Network-related events	☑
Config-related events	☑
Power events	☑
Controller-related events	☑

System-related events	Event is triggered when…
System restart (warm start)	The WAC-2004A is rebooted, such as when settings are changed (IP address, subnet mask, etc.).
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).
Config-related events	**Event is triggered when…**
Configuration changed	A configuration item has been changed.
Configuration file import via Web Console	The configuration file is imported to the WAC-2004A.

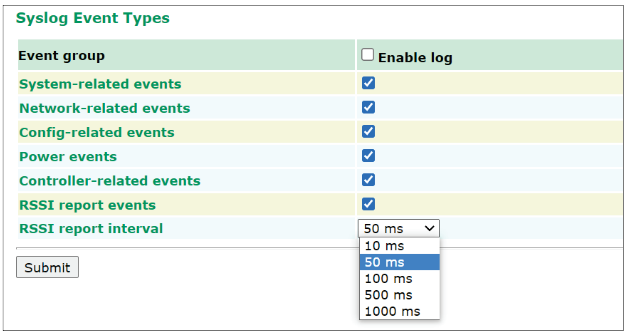
Console authentication failure	An incorrect password is entered.
Firmware upgraded	The WAC-2004A’s firmware is updated.
Power events (HW Rev. 1.1 only)	**Event is triggered when …**
Power on	The WAC-2004A is turned on.
Power off	The WAC-2004A is turned off.
Controller-related events	**Event is triggered when…**
CPU status	CPU over-temperature or overload.
AP status	AP joined/left.
STA status	Client joined/left.
Home Agent status	Home Agent overload and connection changed.
Controller status	Primary/Backup WAC up/down, Inter WAC joined/left.
Roaming status	Client roaming.

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

Detail information for the grouped events is shown in the following table. You can check the box for **Enable log** to enable the grouped events. All default values are enabled (checked). Details for each event group (except WAC RSSI report events) can be found on the “System log Event Types” table.



Syslog Event Types

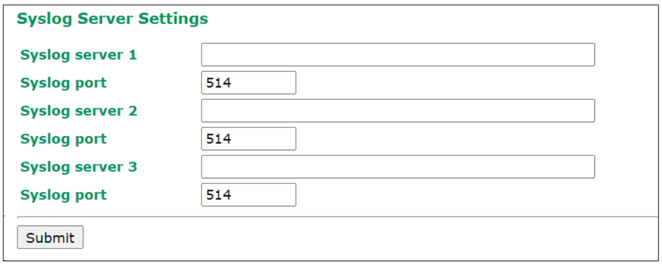
Event group	☐ Enable log
System-related events	☑
Network-related events	☑
Config-related events	☑
Power events	☑
Controller-related events	☑
RSSI report events	☑
RSSI report interval	50 ms

RSSI report events	Event is triggered when…
RSSI between governed Client and its monitor-APs.	Continuously reports the RSSI value between the governed Client and its monitor-APs. This report is used by “Moxa RSSI Transformer” to assist site surveying and system setup.

RSSI report Interval	Event is triggered when…
Report interval (10 to 1000 ms)	RSSI report events function is selected. (default: 50 ms)

Syslog Server Settings

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



Syslog Server Settings

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

Syslog server 1/ 2/ 3

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

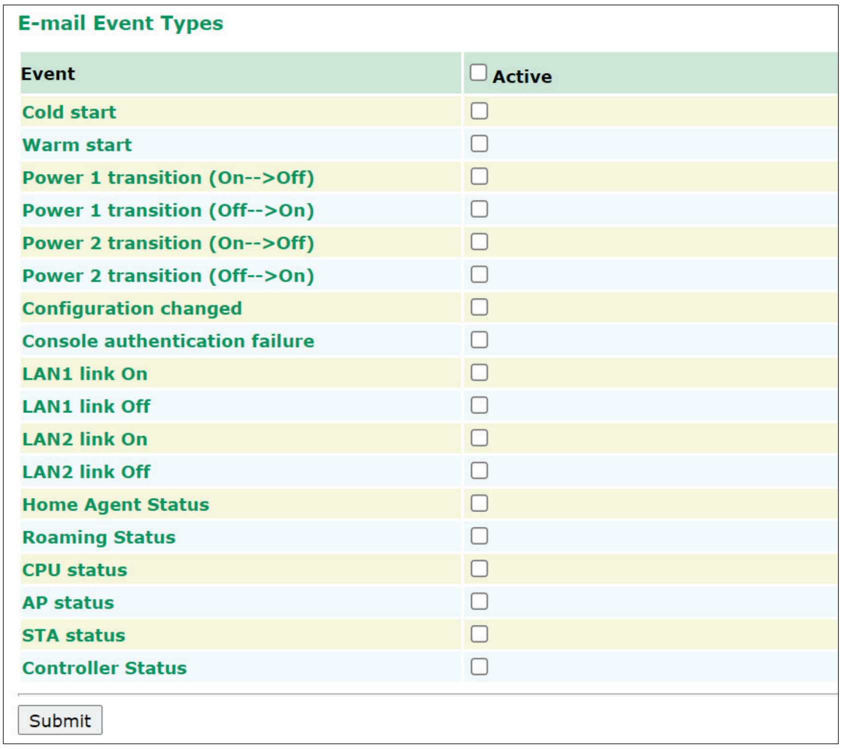
Syslog port

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

E-mail

E-mail Event Types

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

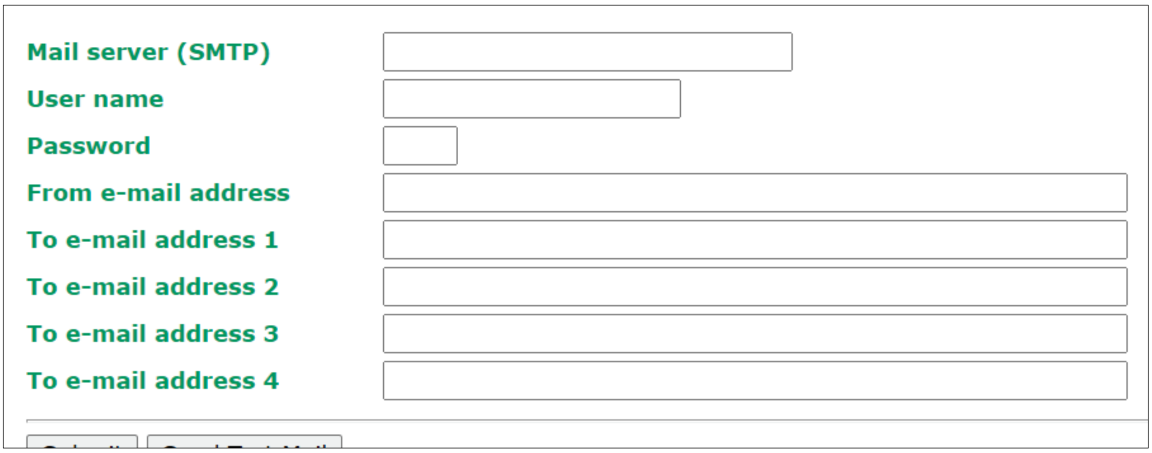


E-mail Event Types

Event	□ Active
Cold start	□
Warm start	□
Power 1 transition (On-->Off)	□
Power 1 transition (Off-->On)	□
Power 2 transition (On-->Off)	□
Power 2 transition (Off-->On)	□
Configuration changed	□
Console authentication failure	□
LAN1 link On	□
LAN1 link Off	□
LAN2 link On	□
LAN2 link Off	□
Home Agent Status	□
Roaming Status	□
CPU status	□
AP status	□
STA status	□
Controller Status	□

E-mail Server Settings

You can set up to 4 email addresses to receive alarm emails from the WAC-2004A. The following parameters can be configured on the **E-mail Server Settings** page. In addition, the **Send Test Mail** button can be used to test whether the Mail server and email addresses work well. More detailed explanations about these parameters are given after the following figure.



Mail server (SMTP)

User name

Password

From e-mail address

To e-mail address 1

To e-mail address 2

To e-mail address 3

To e-mail address 4

Mail server (SMTP)

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

User name & Password

Setting	Description	Factory Default
	The username and password used by the SMTP server.	None

From e-mail address

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

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

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

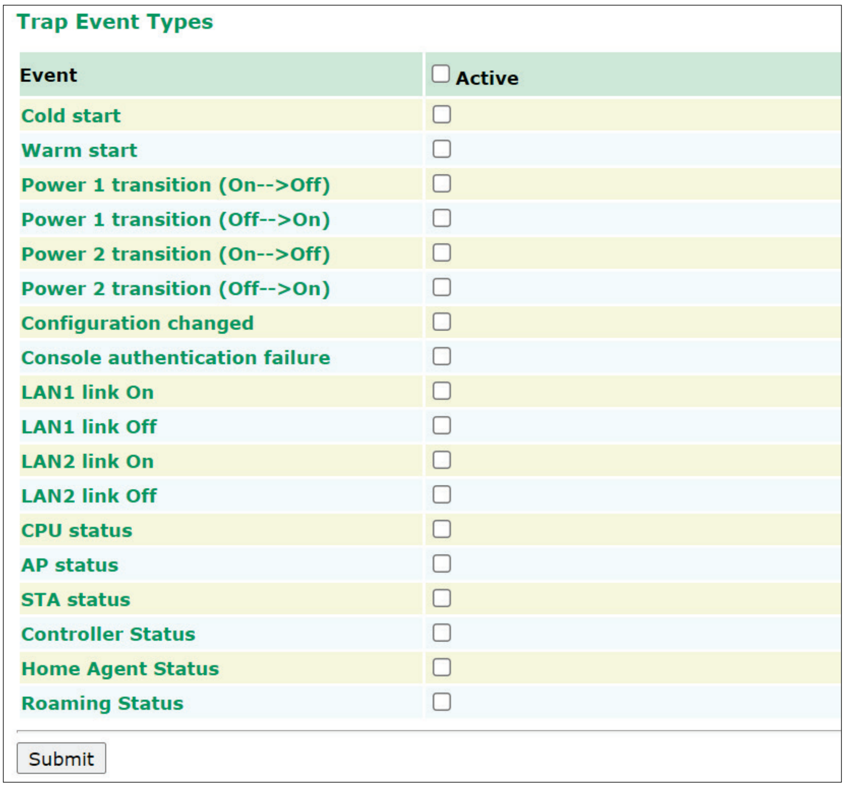
Trap

Traps can be used to signal abnormal conditions (notifications) to a management station. These trap-driven notifications 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

Details for each event group can be found in the "System log Event Types" table.

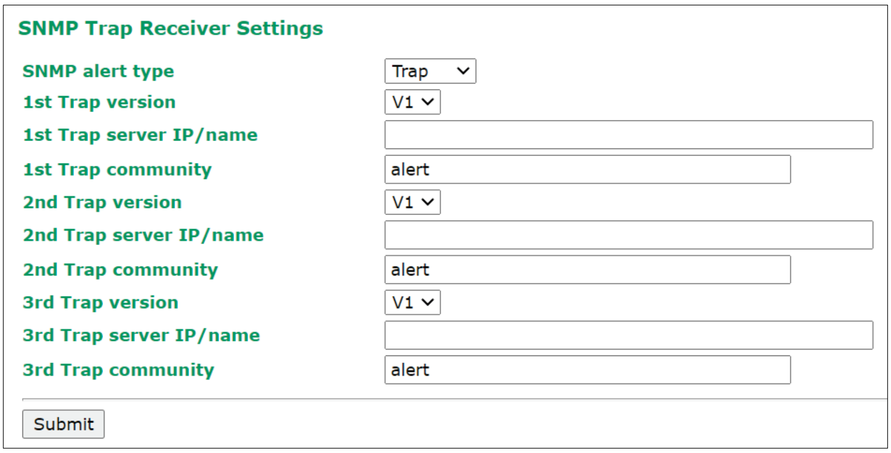


Trap Event Types

Event	□ Active
Cold start	□
Warm start	□
Power 1 transition (On-->Off)	□
Power 1 transition (Off-->On)	□
Power 2 transition (On-->Off)	□
Power 2 transition (Off-->On)	□
Configuration changed	□
Console authentication failure	□
LAN1 link On	□
LAN1 link Off	□
LAN2 link On	□
LAN2 link Off	□
CPU status	□
AP status	□
STA status	□
Controller Status	□
Home Agent Status	□
Roaming Status	□

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.



SNMP Trap Receiver Settings

SNMP alert type	Trap
1st Trap version	V1
1st Trap server IP/name	
1st Trap community	alert
2nd Trap version	V1
2nd Trap server IP/name	
2nd Trap community	alert
3rd Trap version	V1
3rd Trap server IP/name	
3rd Trap community	alert

SNMP alert type

Setting	Description	Factory Default
Trap	Send the event notification to the Trap Receiver only once.	Trap
Inform	Send the event notification to the Trap Receiver and receive an acknowledgement. If the acknowledgement is not received, the controller will resend the notification.	

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

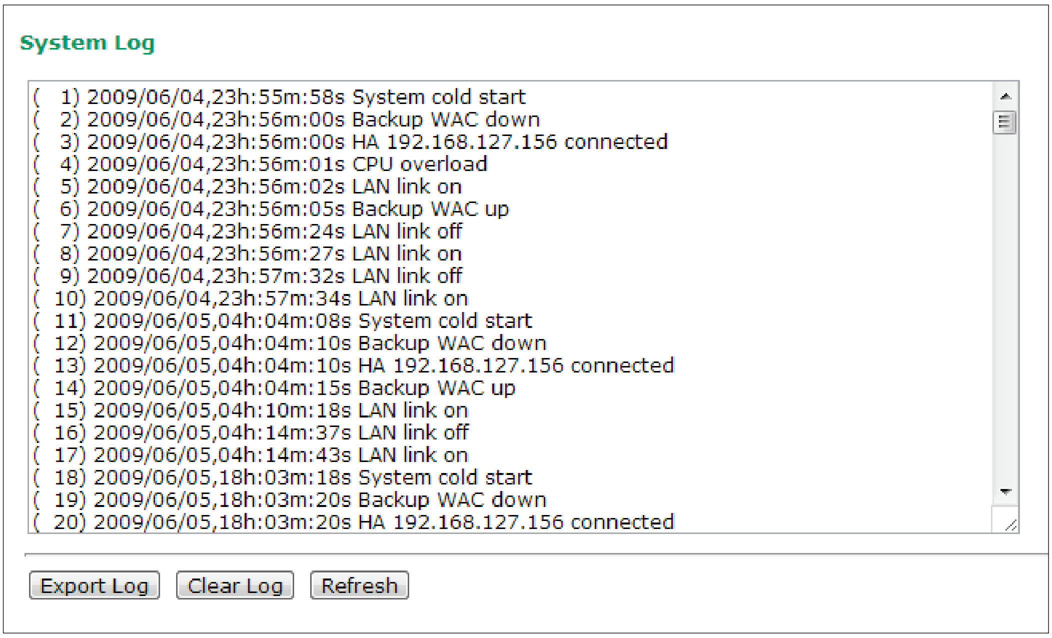
1st / 2nd Trap community

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

Status

System Log

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

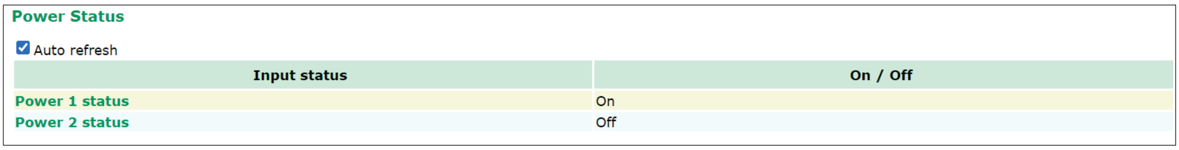


System Log

```
(  1) 2009/06/04,23h:55m:58s System cold start
(  2) 2009/06/04,23h:56m:00s Backup WAC down
(  3) 2009/06/04,23h:56m:00s HA 192.168.127.156 connected
(  4) 2009/06/04,23h:56m:01s CPU overload
(  5) 2009/06/04,23h:56m:02s LAN link on
(  6) 2009/06/04,23h:56m:05s Backup WAC up
(  7) 2009/06/04,23h:56m:24s LAN link off
(  8) 2009/06/04,23h:56m:27s LAN link on
(  9) 2009/06/04,23h:57m:32s LAN link off
( 10) 2009/06/04,23h:57m:34s LAN link on
( 11) 2009/06/05,04h:04m:08s System cold start
( 12) 2009/06/05,04h:04m:10s Backup WAC down
( 13) 2009/06/05,04h:04m:10s HA 192.168.127.156 connected
( 14) 2009/06/05,04h:04m:15s Backup WAC up
( 15) 2009/06/05,04h:10m:18s LAN link on
( 16) 2009/06/05,04h:14m:37s LAN link off
( 17) 2009/06/05,04h:14m:43s LAN link on
( 18) 2009/06/05,18h:03m:18s System cold start
( 19) 2009/06/05,18h:03m:20s Backup WAC down
( 20) 2009/06/05,18h:03m:20s HA 192.168.127.156 connected
```

Power Status

The **Power Status** page displays the status of power inputs 1 and 2.



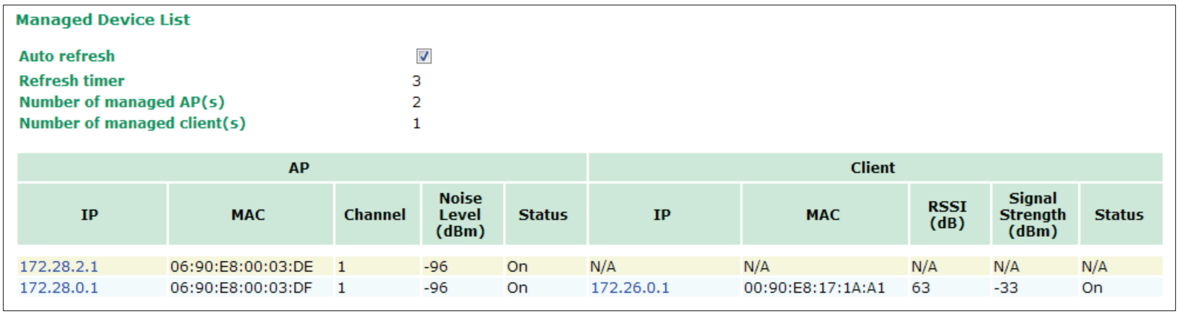
Power Status

☑ Auto refresh

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

Managed Device List

The **Managed Device List** displays all AWK APs, which are managed by the WAC-2004A; the associated clients are also displayed here. Select the **Auto refresh check box** to enable periodic updates.



Managed Device List

Auto refresh	☑
Refresh timer	3
Number of managed AP(s)	2
Number of managed client(s)	1

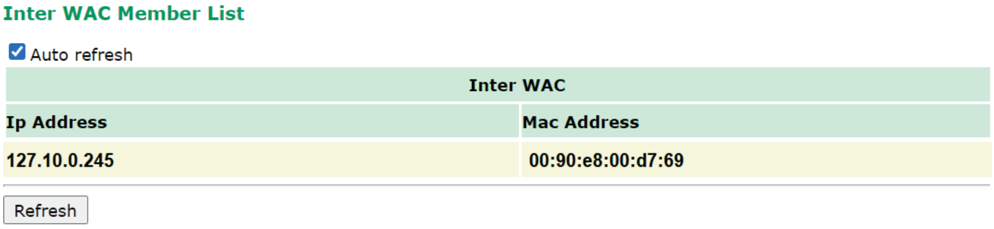
AP					Client				
IP	MAC	Channel	Noise Level (dBm)	Status	IP	MAC	RSSI (dB)	Signal Strength (dBm)	Status
172.28.2.1	06:90:E8:00:03:DE	1	-96	On	N/A	N/A	N/A	N/A	N/A
172.28.0.1	06:90:E8:00:03:DF	1	-96	On	172.26.0.1	00:90:E8:17:1A:A1	63	-33	On

All monitored APs will be listed on the left-hand side of the table, along with their IP addresses, MAC addresses, operating channels, noise level, and device status.

All monitored Clients will be listed on the right-hand side of the table, along with their IP addresses, MAC addresses, RSSI and Signal Strength values against the associated AP, as well as the status of the Client device.

Inter WAC Member List

The Inter WAC Member List displays all other WAC members that have been configured to work together in the same inter WAC group.



Inter WAC Member List

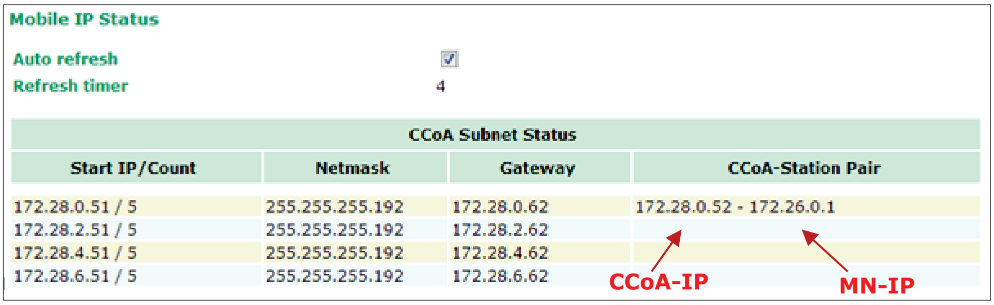
☑ Auto refresh

Inter WAC	
Ip Address	Mac Address
127.10.0.245	00:90:e8:00:d7:69

Mobile IP Status

The Mobile IP Status displays the status of all Mobile IP Clients, which are managed by this particular WAC-2004A. This page contains two main tables - **CCoA Subnet Status** and **Home Subnet Status**.

The CCoA Subnet Status table provides the Mobile IP Client's IP information from the CCoA's (Collocated Care-of-Address) point of view.

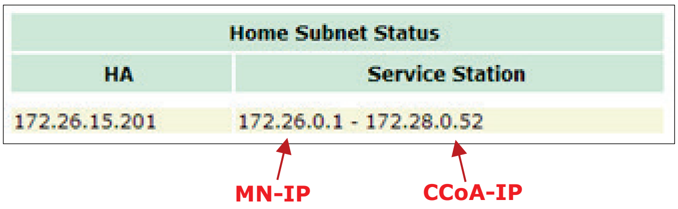


Mobile IP Status

Auto refresh	☑
Refresh timer	4

CCoA Subnet Status			
Start IP/Count	Netmask	Gateway	CCoA-Station Pair
172.28.0.51 / 5	255.255.255.192	172.28.0.62	172.28.0.52 - 172.26.0.1
172.28.2.51 / 5	255.255.255.192	172.28.2.62	
172.28.4.51 / 5	255.255.255.192	172.28.4.62	
172.28.6.51 / 5	255.255.255.192	172.28.6.62	

The **Home Subnet Status** table provides the Mobile IP Client's IP information from the HA's (Home Agent) point of view.

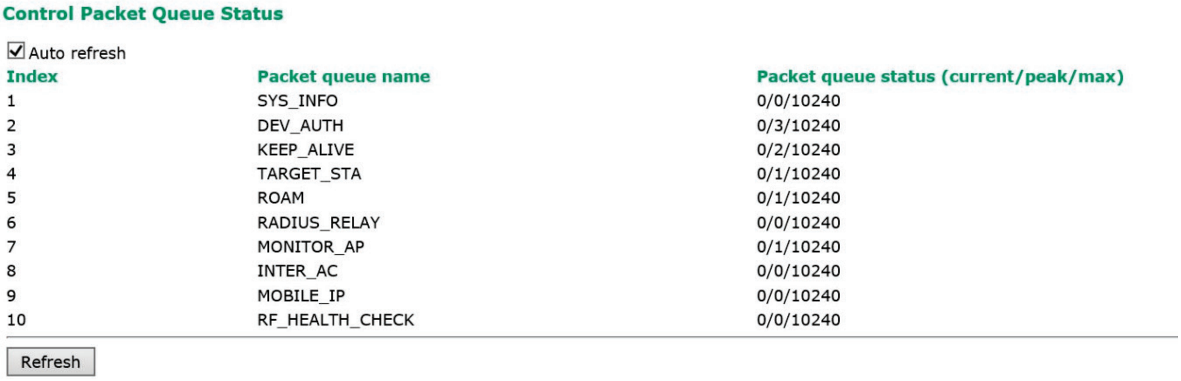


Home Subnet Status	
HA	Service Station
172.26.15.201	172.26.0.1 - 172.28.0.52

Control Packet Queue Status

The Control Packet Queue Status displays the number of unprocessed control packets in each queue along with the current, peak, and maximum number of packets for each queue.

These control packets carry different types of information including system information, authentication, roaming status, and corresponding AP information.



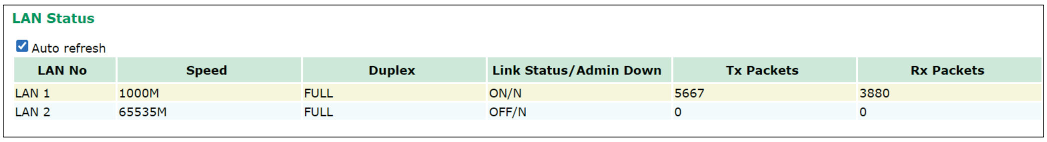
Control Packet Queue Status

☑ Auto refresh

Index	Packet queue name	Packet queue status (current/peak/max)
1	SYS_INFO	0/0/10240
2	DEV_AUTH	0/3/10240
3	KEEP_ALIVE	0/2/10240
4	TARGET_STA	0/1/10240
5	ROAM	0/1/10240
6	RADIUS_RELAY	0/0/10240
7	MONITOR_AP	0/1/10240
8	INTER_AC	0/0/10240
9	MOBILE_IP	0/0/10240
10	RF_HEALTH_CHECK	0/0/10240

LAN Status

The following table shows the status of each port, including the Speed, Duplex type, Link Status, and TX/RX Packets flow.



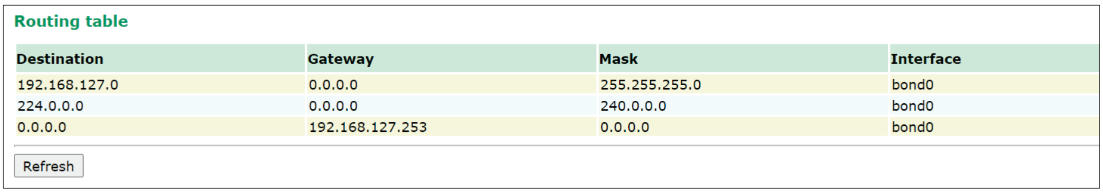
LAN Status

☑ Auto refresh

LAN No	Speed	Duplex	Link Status/Admin Down	Tx Packets	Rx Packets
LAN 1	1000M	FULL	ON/N	5667	3880
LAN 2	65535M	FULL	OFF/N	0	0

Routing Table

The Routing Table shows the status of the current routing information of each interface.

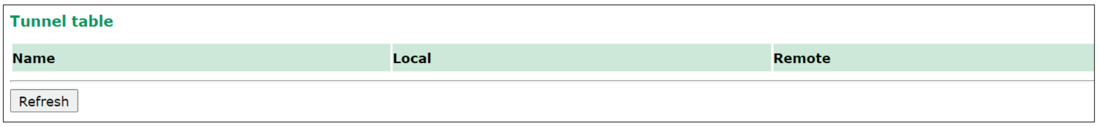


Routing table

Destination	Gateway	Mask	Interface
192.168.127.0	0.0.0.0	255.255.255.0	bond0
224.0.0.0	0.0.0.0	240.0.0.0	bond0
0.0.0.0	192.168.127.253	0.0.0.0	bond0

Tunnel Table

The Tunneling Table shows the status of the current tunnels between the WAC to Clients.



Tunnel table

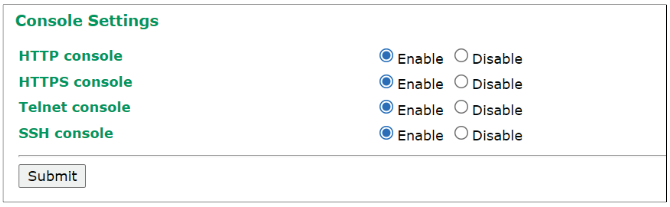
Name	Local	Remote

Maintenance

Maintenance functions provide the administrator with tools to manage the WAC-2004A and wired/wireless networks.

Console Settings

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

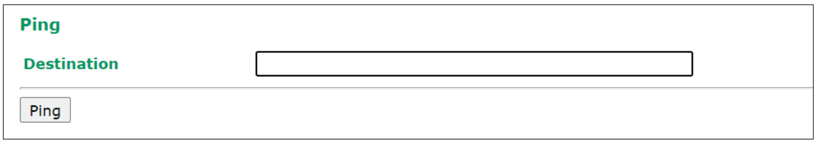


Console Settings

HTTP console	● Enable ○ Disable
HTTPS console	● Enable ○ Disable
Telnet console	● Enable ○ Disable
SSH console	● Enable ○ Disable

Ping

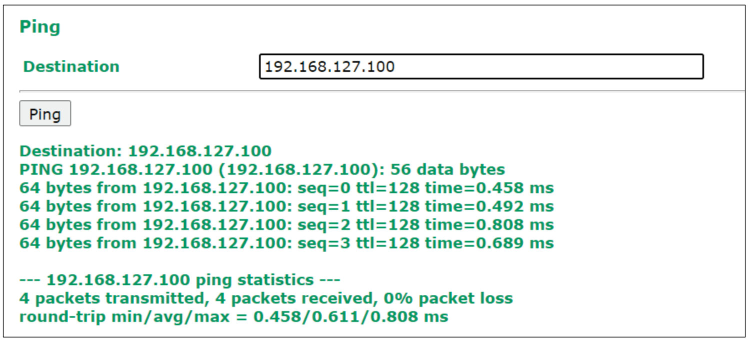
Ping helps to diagnose the integrity of wired or wireless networks. By inputting a node's IP address in the **Destination** field, you can use the **ping** command to make sure it exists and whether or not the access path is available.



Ping

Destination

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.



Ping

Destination 192.168.127.100

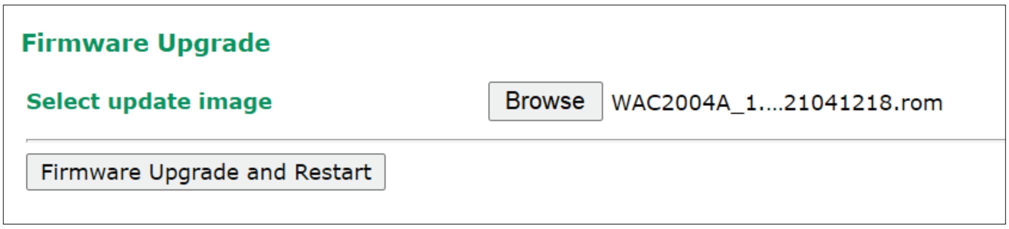
```
Destination: 192.168.127.100
PING 192.168.127.100 (192.168.127.100): 56 data bytes
64 bytes from 192.168.127.100: seq=0 ttl=128 time=0.458 ms
64 bytes from 192.168.127.100: seq=1 ttl=128 time=0.492 ms
64 bytes from 192.168.127.100: seq=2 ttl=128 time=0.808 ms
64 bytes from 192.168.127.100: seq=3 ttl=128 time=0.689 ms

--- 192.168.127.100 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.458/0.611/0.808 ms
```

Firmware Upgrade

The WAC-2004A can be enhanced with more value-added functions by installing firmware upgrades.

Note that while the firmware is being upgraded, all APs controlled by the WAC-2004A will be out of service. 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 WAC-2004A will reboot itself.

When upgrading your firmware, the WAC-2004A's other functions will be unavailable.



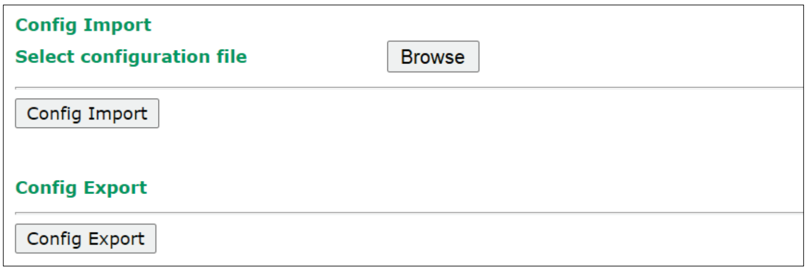
Select update image WAC2004A_1....21041218.rom

ATTENTION

Please make sure the power source is stable when you upgrade your firmware. An unexpected power breakup may damage your WAC-2004A.

Config Import Export

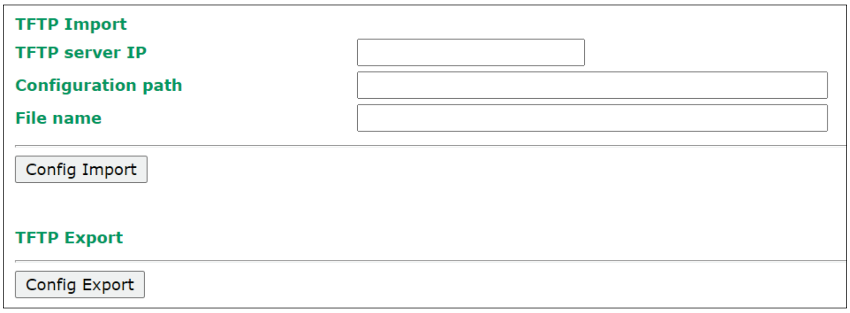
You can back up or restore the WAC-2004A's configuration with **Config Import Export**.



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

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

You can also back up or restore the WAC-2004A's configuration via **TFTP.**



TFTP server IP

Setting	Description	Factory Default
IP address	The IP address of the TFTP server.	None

Configuration path

Setting	Description	Factory Default
File system characters (a-z, A-Z, 0-9, etc…)	The relative path to the configuration file on the TFTP server.	None

File name

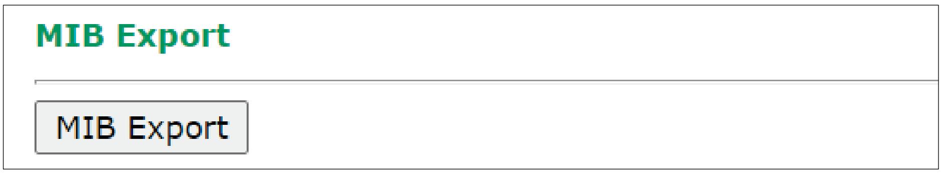
Setting	Description	Factory Default
File system characters (a-z, A-Z, 0-9, etc…)	The file name of the configuration file.	None

In the **Config Import** section, click **Config Import** button to begin importing the configuration.

In the **Config Export** section, click the **Config Export** button and the configuration file will be saved to the specified TFTP server as **"importTFTP.ini"**.

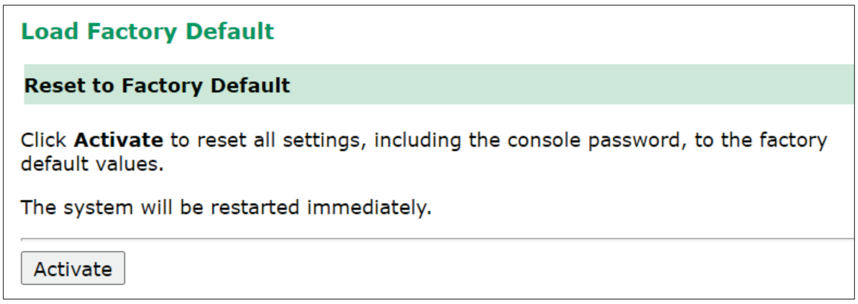
MIB Export

Click **MIB Export** to save a MIB file to your local storage. The configuration file is a **.my** file that you can import with a general SNMP tool. This operation allows you to control or configure the WAC-2004A remotely.



Load Factory Default

Use this function to reset the WAC-2004A and roll all settings back to the factory default values.


Load Factory Default

Reset to Factory Default

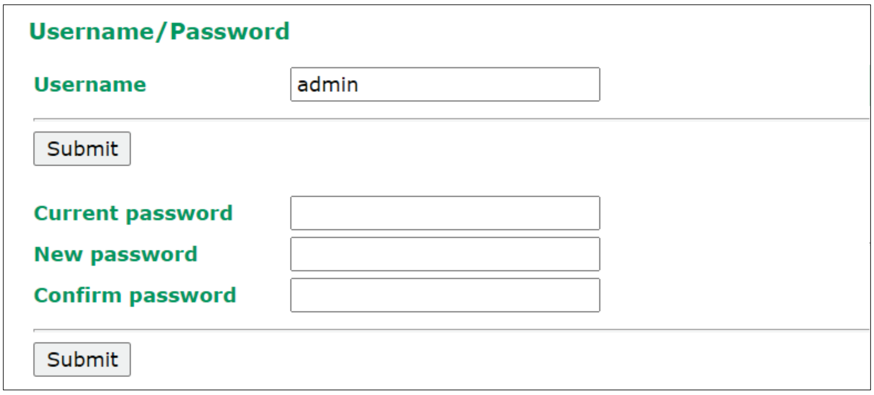
Click **Activate** to reset all settings, including the console password, to the factory default values.

The system will be restarted immediately.

Username/Password

You can change the administration username and password for each of the WAC-2004A's console managers by using the **Password** function. Before you set up a new password, you must input the current password and reenter the new password for confirmation. For your security, do not use the default password ***moxa***, and remember to change the administration password regularly.

NOTE The default password is "moxa".

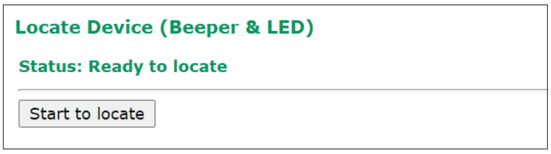


Username/Password

Username: admin

Locate Device

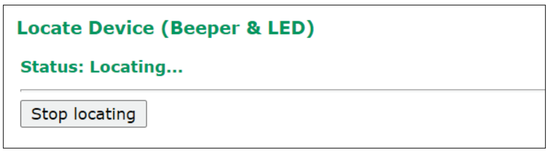
The Locate Device function allows you to easily find your device. When you click the "Start to locate" button, the beeper of the device you are looking for will start beeping, and the device's LED will blink continuously.



Locate Device (Beeper & LED)

Status: Ready to locate

After finding your device, you can click "Stop locating" to stop the beep and blinking of LED.

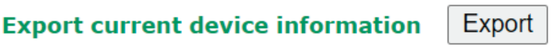


Locate Device (Beeper & LED)

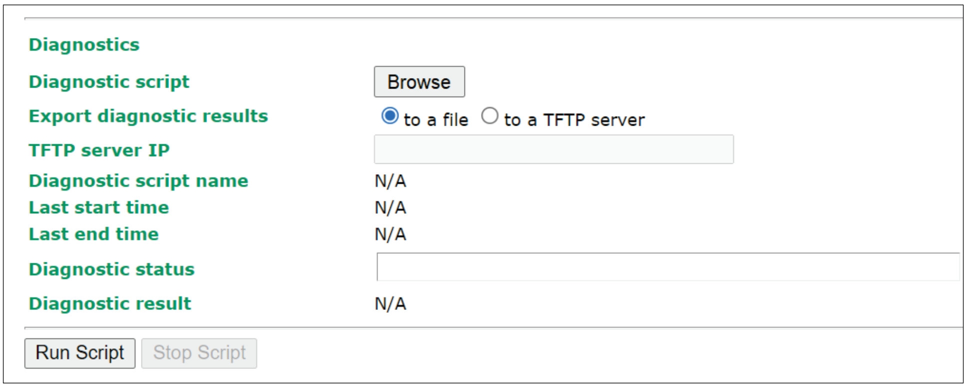
Status: Locating...

Troubleshooting

From the Troubleshooting screen, you can quickly obtain the current system status and provide diagnostics information to Moxa engineers. Click **Export** to export the current device information.



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



Diagnostics

Diagnostic script	Browse
Export diagnostic results	● to a file ○ to a TFTP server
TFTP server IP	
Diagnostic script name	N/A
Last start time	N/A
Last end time	N/A
Diagnostic status	
Diagnostic result	N/A

To use the script, navigate to the script file using **Browse**. Select the export method (file or TFTP) and click **Run Script**:

Export diagnostic results

Setting	Description
Export method	Choose to export the diagnostics results to a file or to a TFTP server.

TFTP server IP

Setting	Description
IP address	The IP address of the TFTP server.

Diagnostic script name

Setting	Description
Name	Displays the name of the selected script file.

Last start time

Setting	Description
Time	Displays the start time of the last time the script was executed.

Last end time

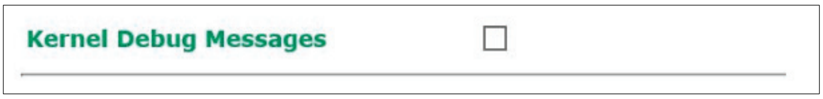
Setting	Description
Time	Displays the end time of the last time the script was executed.

Diagnostic status

Setting	Description
Status	Displays the progress of the system diagnostics.

Diagnostic result

Setting	Description
Test result	Displays the result of the system diagnostics. If you have selected the **to a file** export option, the system logs are packaged and encrypted into a file. The maximum log file size is 1 MB. If the log file exceeds the 1 MB file size, another file will be created. A maximum of 5 files (for a total of 5 MB) will be kept on the system for downloading. When the number of files exceeds five, the oldest file will be deleted first.



Kernel Debug Messages □

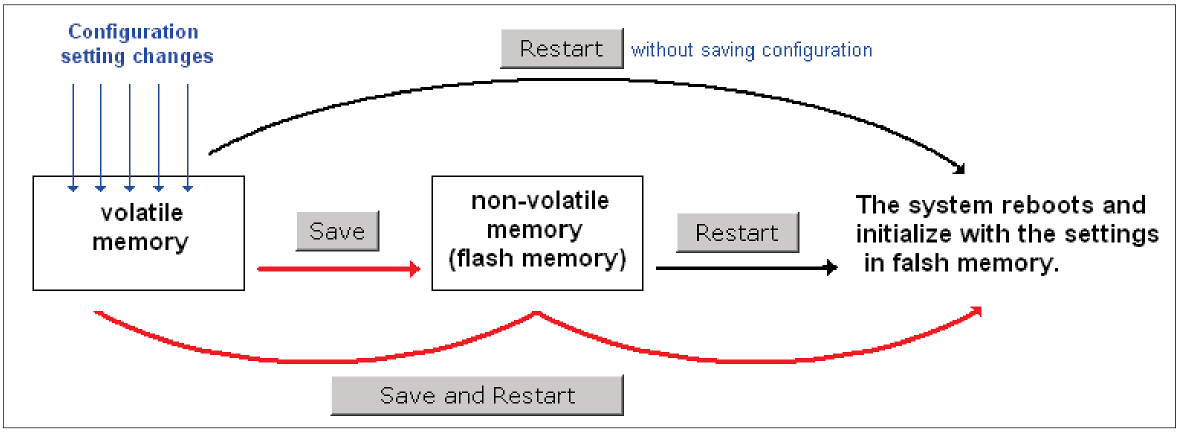
Kernel Debug Message

Setting	Description	Factory Default
Debug message	Select the checkbox to enable logging the kernel debug message.	None

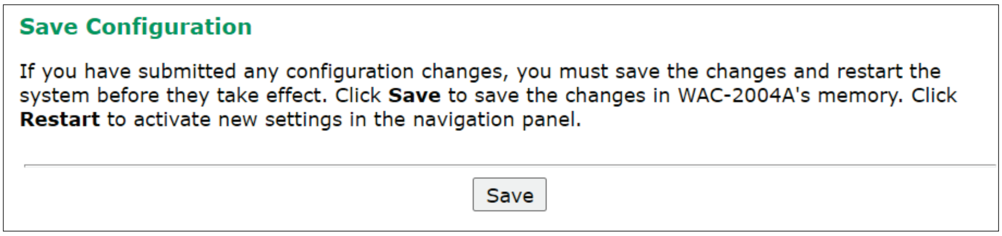
Save Configuration

The following figure shows how the WAC-2004A stores the setting changes into volatile and non-volatile memory. All data stored in volatile memory will disappear when the WAC-2004A is shutdown or rebooted unless they are saved onto the flash (non-volatile) memory. Because the WAC-2004A starts up and initializes with the settings stored in flash memory, all new changes must be saved to flash memory before restarting the WAC-2004A.

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


Configuration setting changes
Restart
without saving configuration
volatile memory
Save
non-volatile memory (flash memory)
Restart
The system reboots and initialize with the settings in falsh memory.
Save and Restart

After clicking on **Save Configuration** in the left menu box, the following screen will appear. Click **Save** 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.



Save Configuration

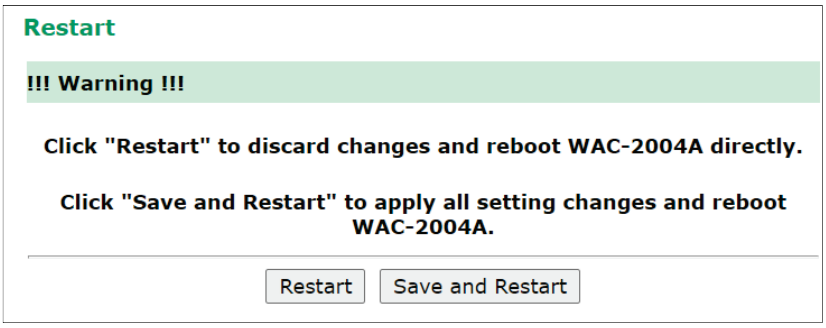
If you have submitted any configuration changes, you must save the changes and restart the system before they take effect. Click **Save** to save the changes in WAC-2004A's memory. Click **Restart** to activate new settings in the navigation panel.

Save

Restart

If you submitted configuration changes, you will see a blinking alert message on 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 WAC-2004A, and all setting changes will be ignored. Clicking the **Save and Restart** button will apply all setting changes and then reboot the WAC-2004A.



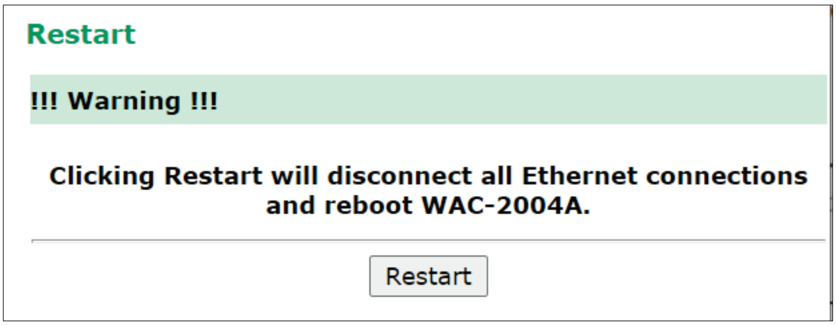
Restart

!!! Warning !!!

Click "Restart" to discard changes and reboot WAC-2004A directly.

Click "Save and Restart" to apply all setting changes and reboot WAC-2004A.

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.



Restart

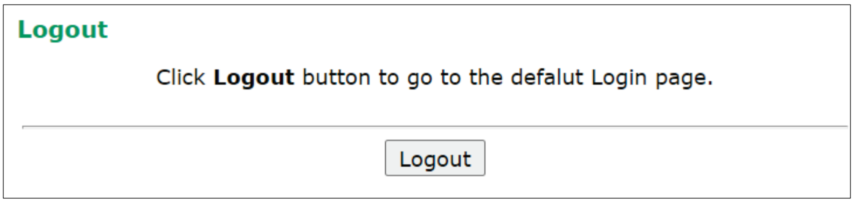
!!! Warning !!!

Clicking Restart will disconnect all Ethernet connections and reboot WAC-2004A.

You will not be able to use any of the WAC-2004A's functions while the system is rebooting.

Logout

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



Logout

Click **Logout** button to go to the defalut Login page.

4

Software Installation and Configuration

The following topics are covered in this chapter:

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

Overview

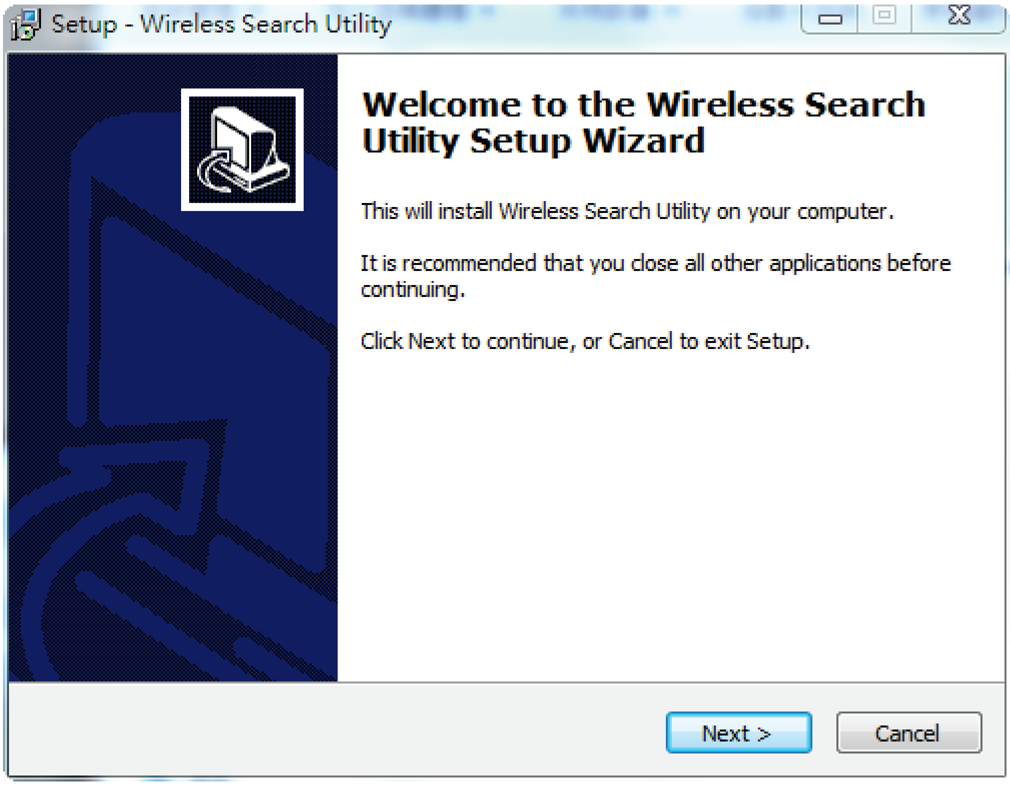
The Wireless Search Utility can be downloaded from the Moxa website at www.moxa.com.

Wireless Search Utility

Installing the 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.



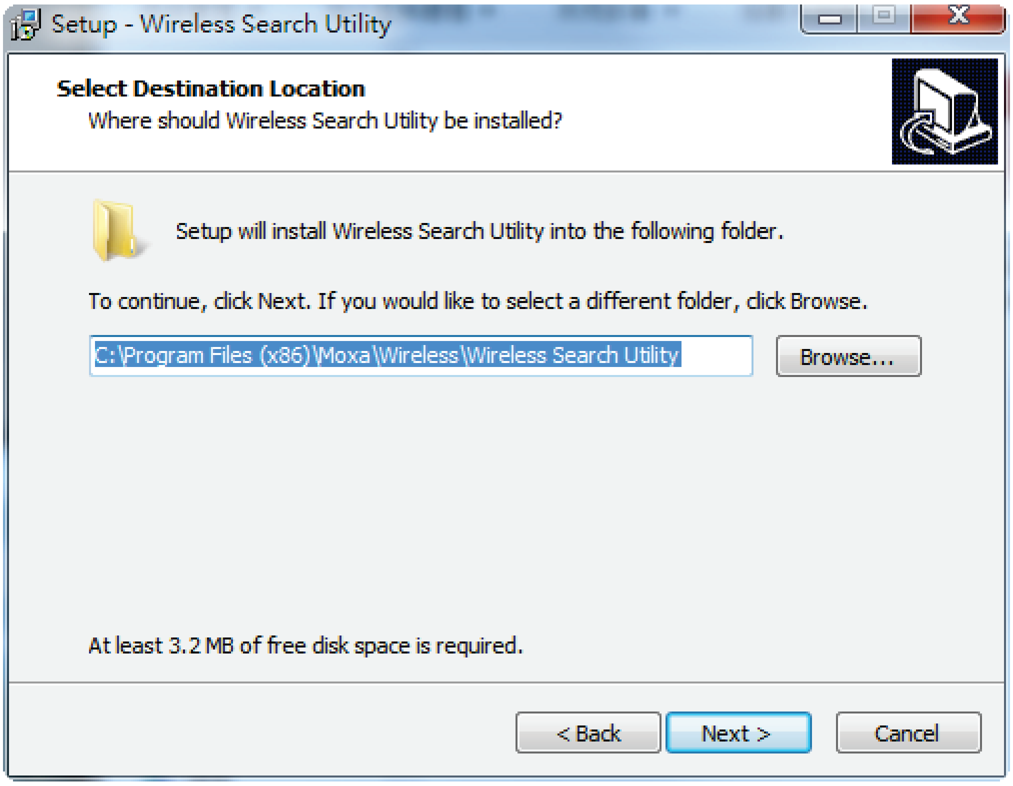
Welcome to the Wireless Search Utility Setup Wizard

This will install Wireless Search Utility on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

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



Setup - Wireless Search Utility

Select Destination Location

Where should Wireless Search Utility be installed?

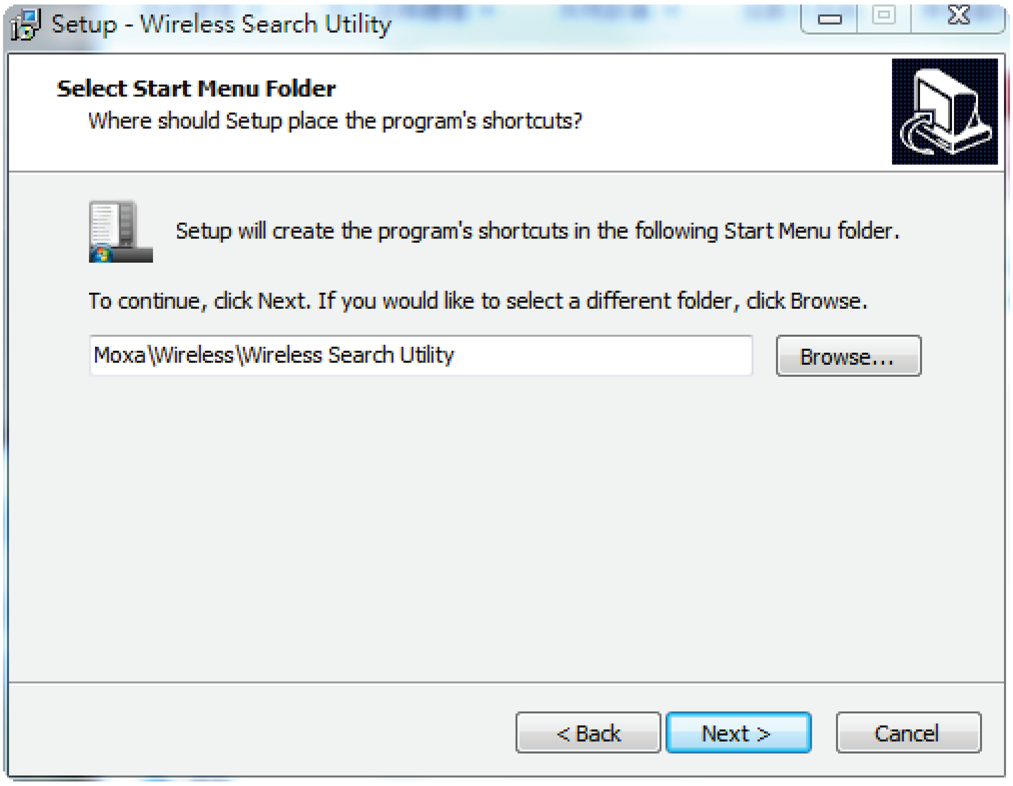
Setup will install Wireless Search Utility into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\Moxa\Wireless\Wireless Search Utility

At least 3.2 MB of free disk space is required.

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



Setup - Wireless Search Utility

Select Start Menu Folder

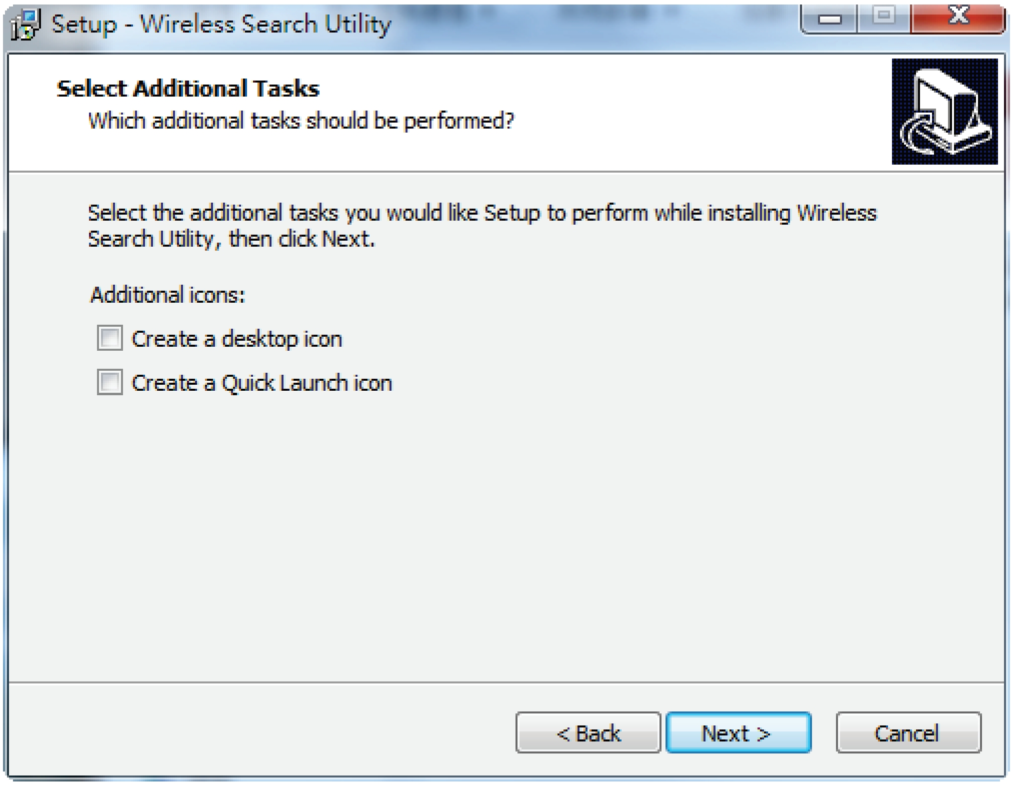
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

Moxa\Wireless\Wireless Search Utility

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



Setup - Wireless Search Utility

Select Additional Tasks

Which additional tasks should be performed?

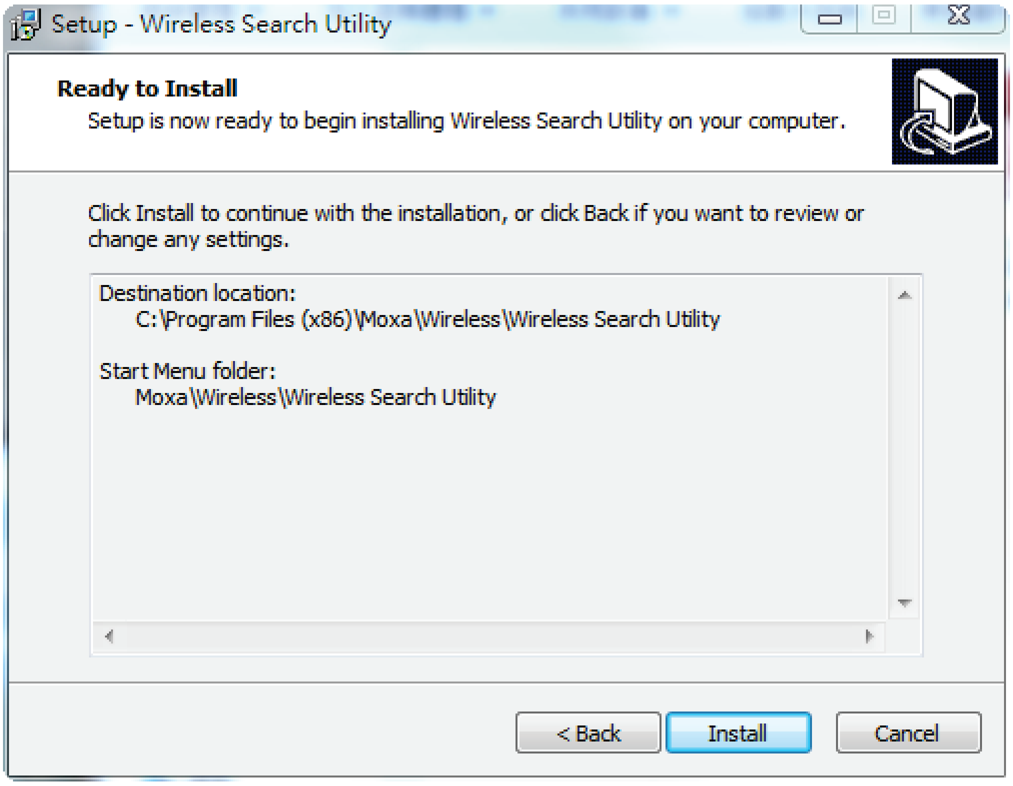
Select the additional tasks you would like Setup to perform while installing Wireless Search Utility, then click Next.

Additional icons:

□ Create a desktop icon

□ Create a Quick Launch icon

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



Setup - Wireless Search Utility

Ready to Install

Setup is now ready to begin installing Wireless Search Utility on your computer.

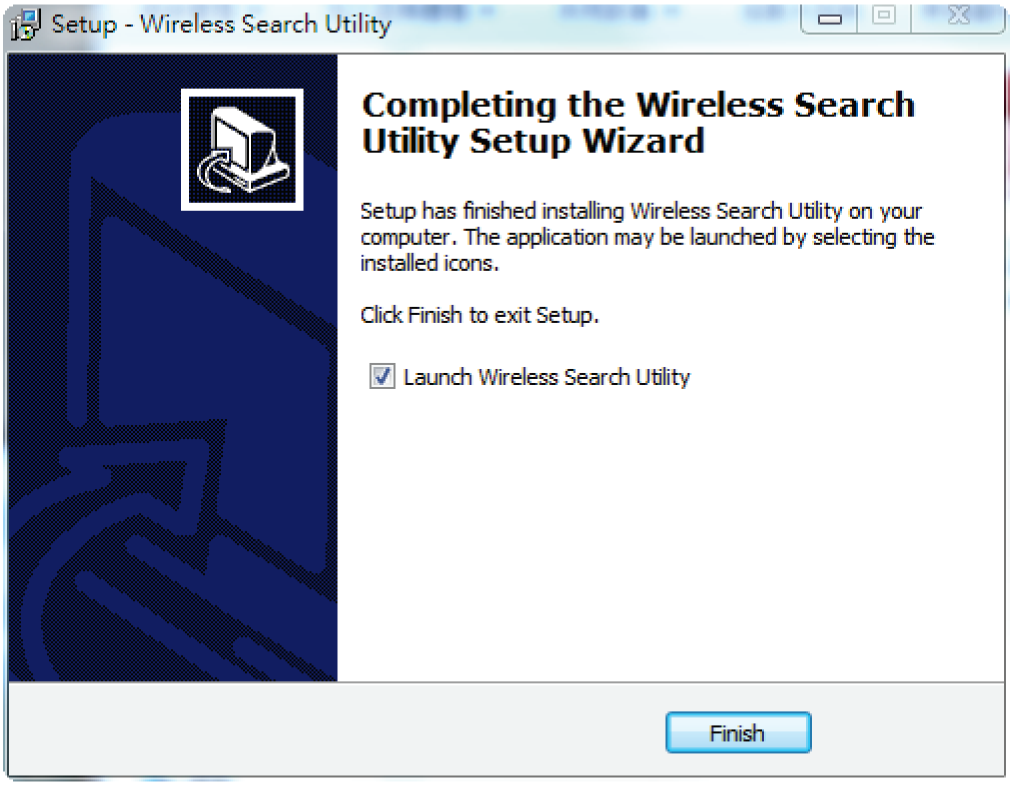
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files (x86)\Moxa\Wireless\Wireless Search Utility

Start Menu folder:
Moxa\Wireless\Wireless Search Utility

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.



Setup - Wireless Search Utility

Completing the Wireless Search Utility Setup Wizard

Setup has finished installing Wireless Search Utility on your computer. The application may be launched by selecting the installed icons.

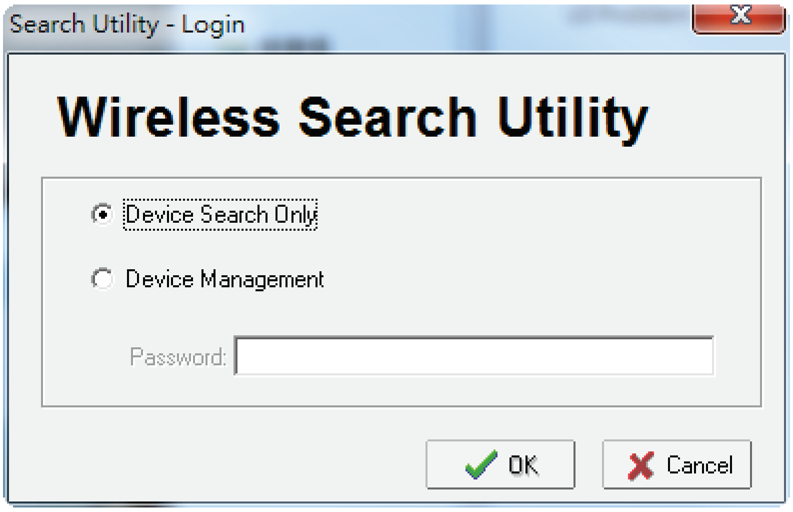
Click Finish to exit Setup.

☑ Launch Wireless Search Utility

Configuring the Wireless Search Utility

The Broadcast Search function is used to locate all AWK-3131A APs that are connected to the same LAN as your computer. After locating an AWK-3131A, 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-3131A 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.



Search Utility - Login

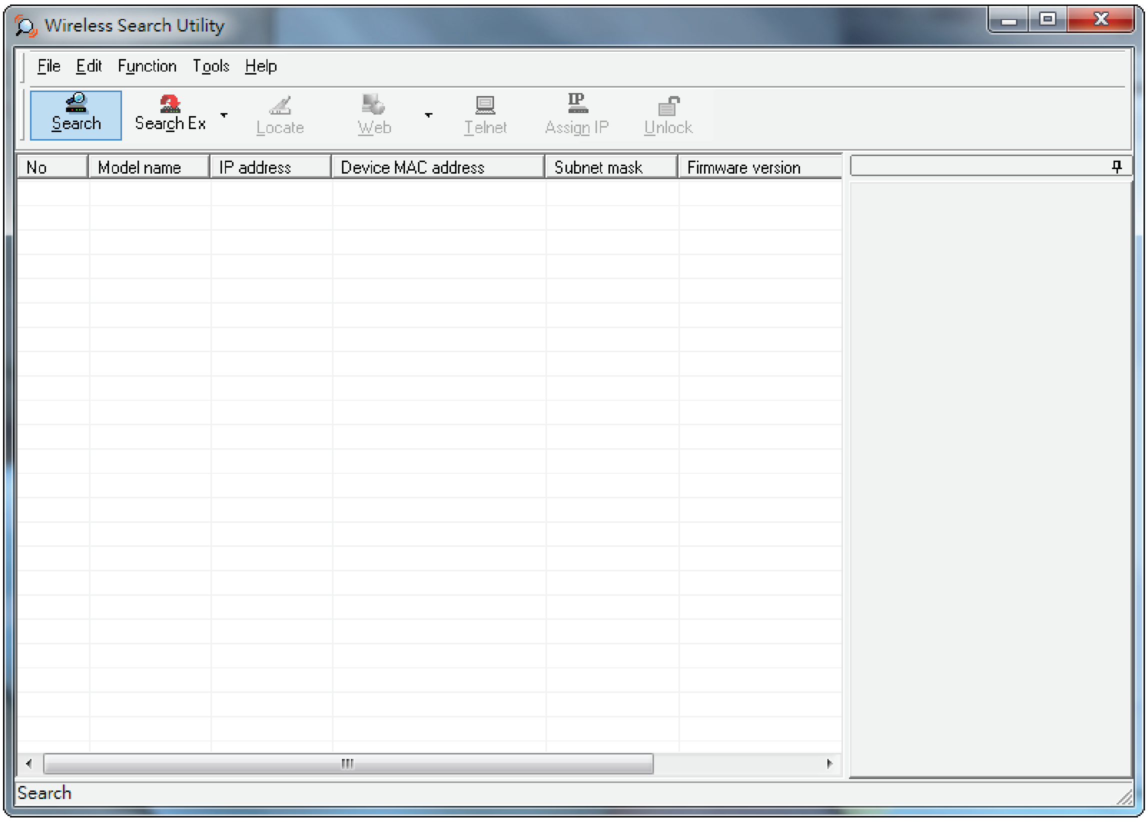
Wireless Search Utility

● Device Search Only

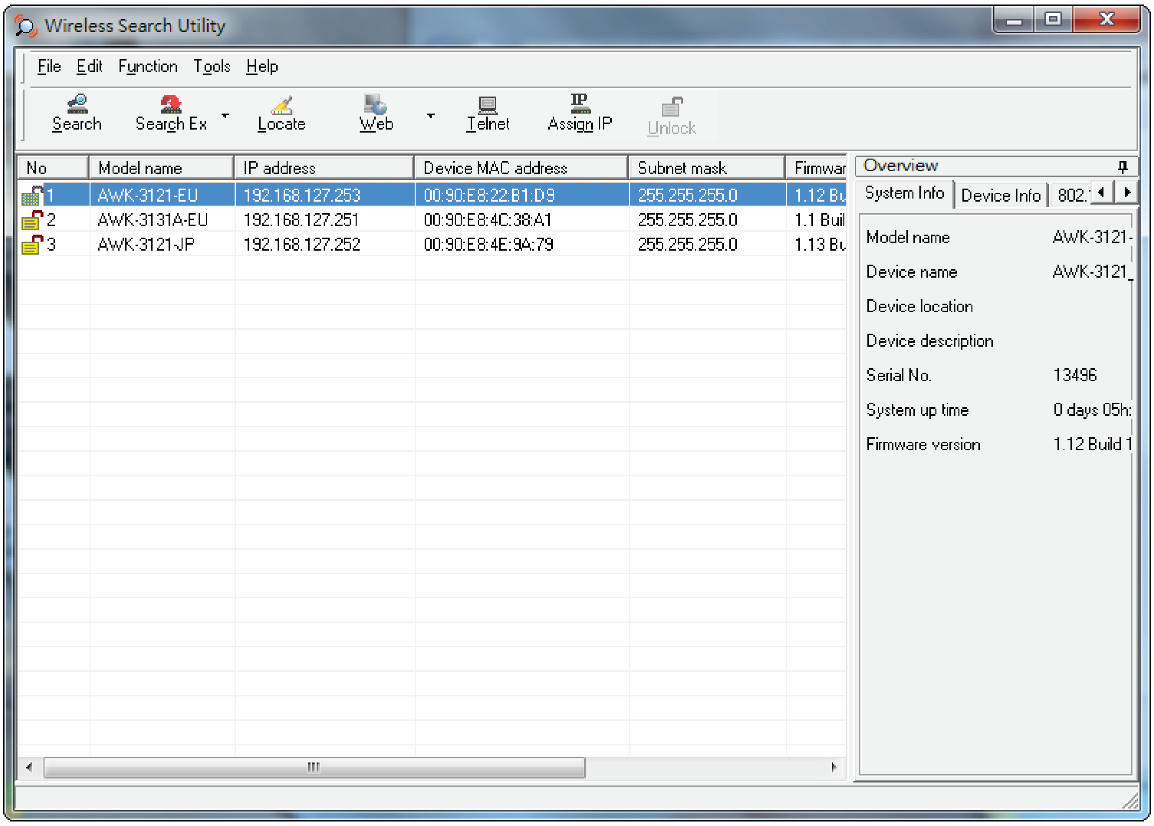
○ Device Management

Password:

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



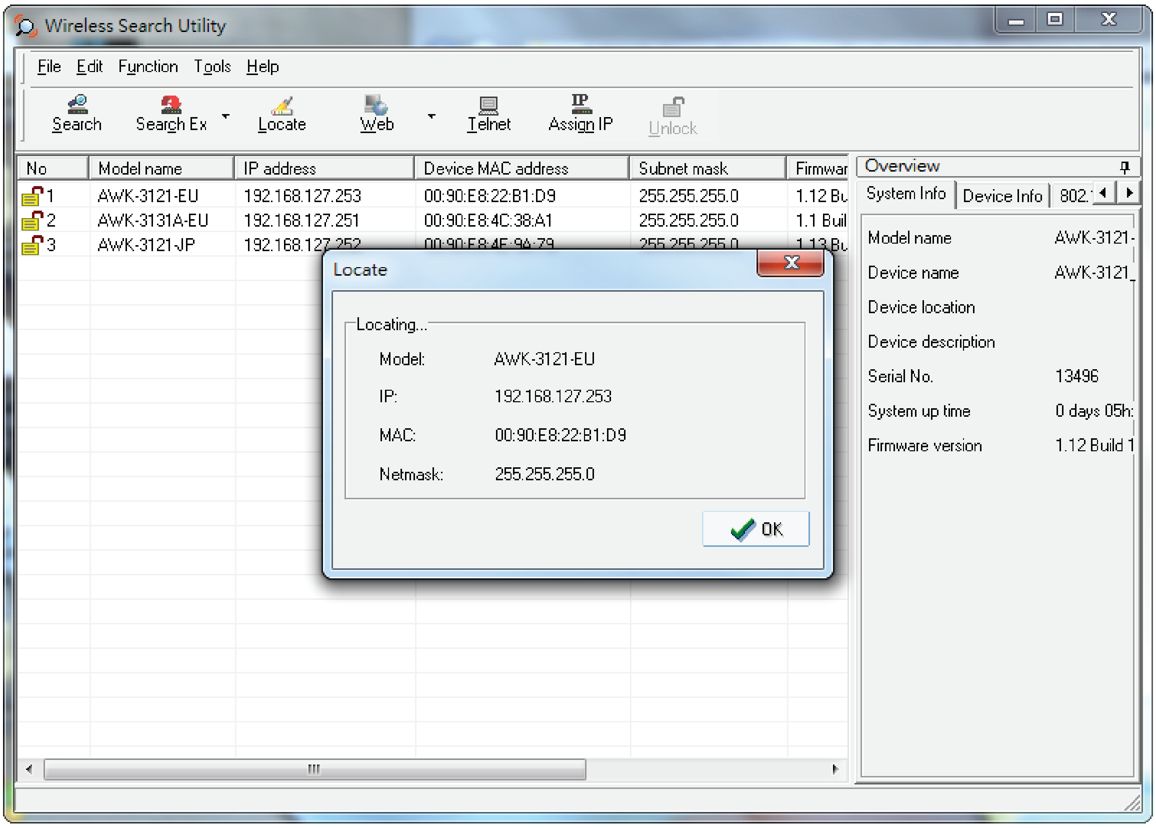
3. The "Searching" window indicates the progress of the search. When the search is complete, all AWKs that were located will be displayed in the Wireless Search Utility window.



No	Model name	IP address	Device MAC address	Subnet mask	Firmwar
1	AWK-3121-EU	192.168.127.253	00:90:E8:22:B1:D9	255.255.255.0	1.12 Bu
2	AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0	1.1 Buil
3	AWK-3121-JP	192.168.127.252	00:90:E8:4E:9A:79	255.255.255.0	1.13 Bu

Model name	AWK-3121-
Device name	AWK-3121_
Device location	
Device description	
Serial No.	13496
System up time	0 days 05h:
Firmware version	1.12 Build 1

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



No	Model name	IP address	Device MAC address	Subnet mask	Firmwar
1	AWK-3121-EU	192.168.127.253	00:90:E8:22:B1:D9	255.255.255.0	1.12 Bu
2	AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0	1.1 Buil
3	AWK-3121-JP	192.168.127.252	00:90:E8:4E:9A:79	255.255.255.0	1.13 Bu

Locate

Locating...

Model: AWK-3121-EU

IP: 192.168.127.253

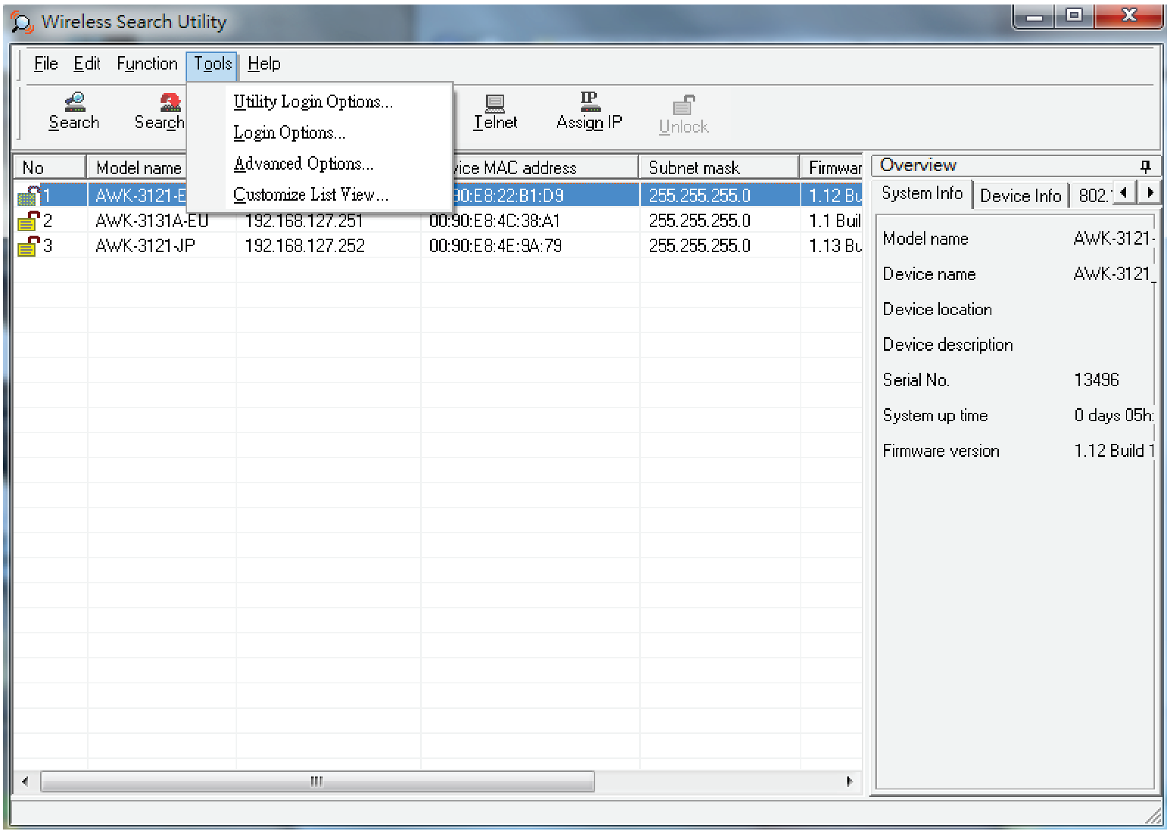
MAC: 00:90:E8:22:B1:D9

Netmask: 255.255.255.0

Model name	AWK-3121-
Device name	AWK-3121_
Device location	
Device description	
Serial No.	13496
System up time	0 days 05h:
Firmware version	1.12 Build 1

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.



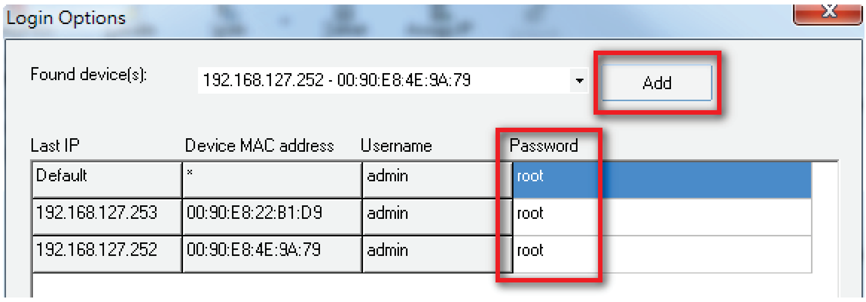
No	Model name		ice MAC address	Subnet mask	Firmwar
1	AWK-3121-E		90:E8:22:B1:D9	255.255.255.0	1.12 Bu
2	AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0	1.1 Buil
3	AWK-3121-JP	192.168.127.252	00:90:E8:4E:9A:79	255.255.255.0	1.13 Bu

Model name	AWK-3121-
Device name	AWK-3121_
Device location	
Device description	
Serial No.	13496
System up time	0 days 05h:
Firmware version	1.12 Build 1

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.

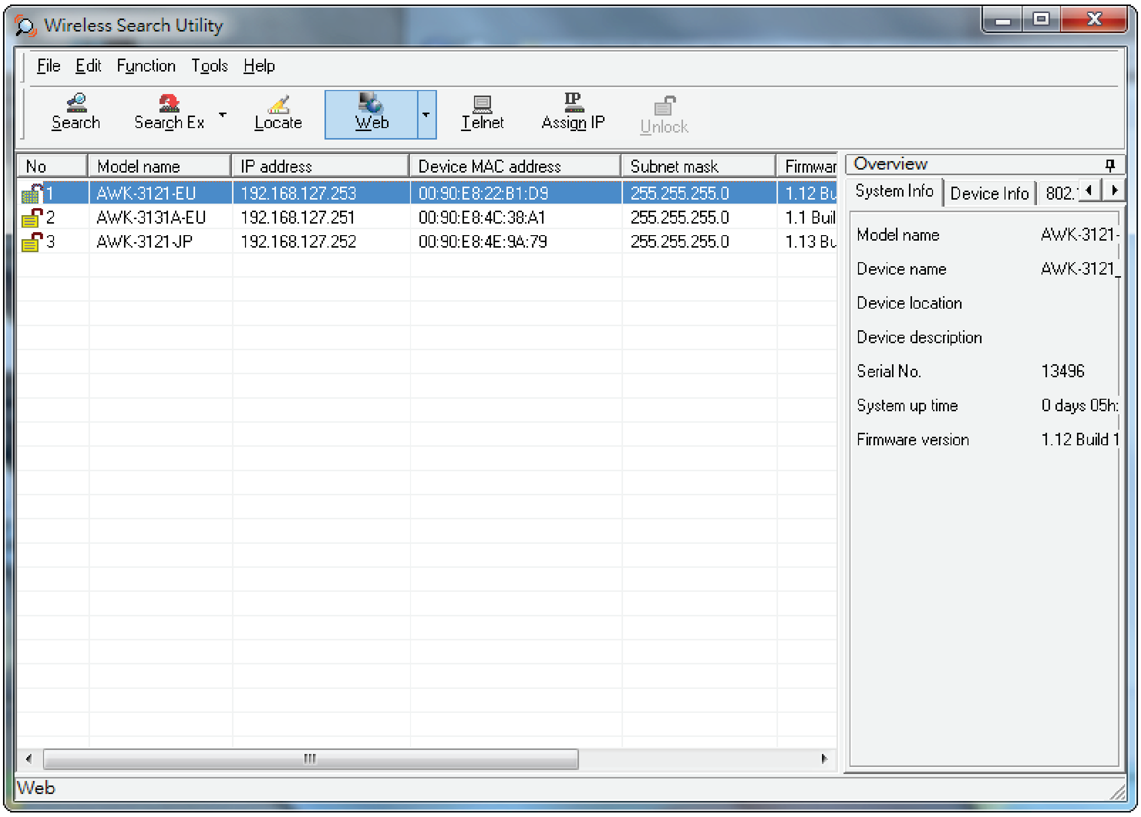


Found device(s): 192.168.127.252 - 00:90:E8:4E:9A:79

Last IP	Device MAC address	Username	Password
Default	*	admin	root
192.168.127.253	00:90:E8:22:B1:D9	admin	root
192.168.127.252	00:90:E8:4E:9A:79	admin	root

To modify the configuration of the highlighted AWK:

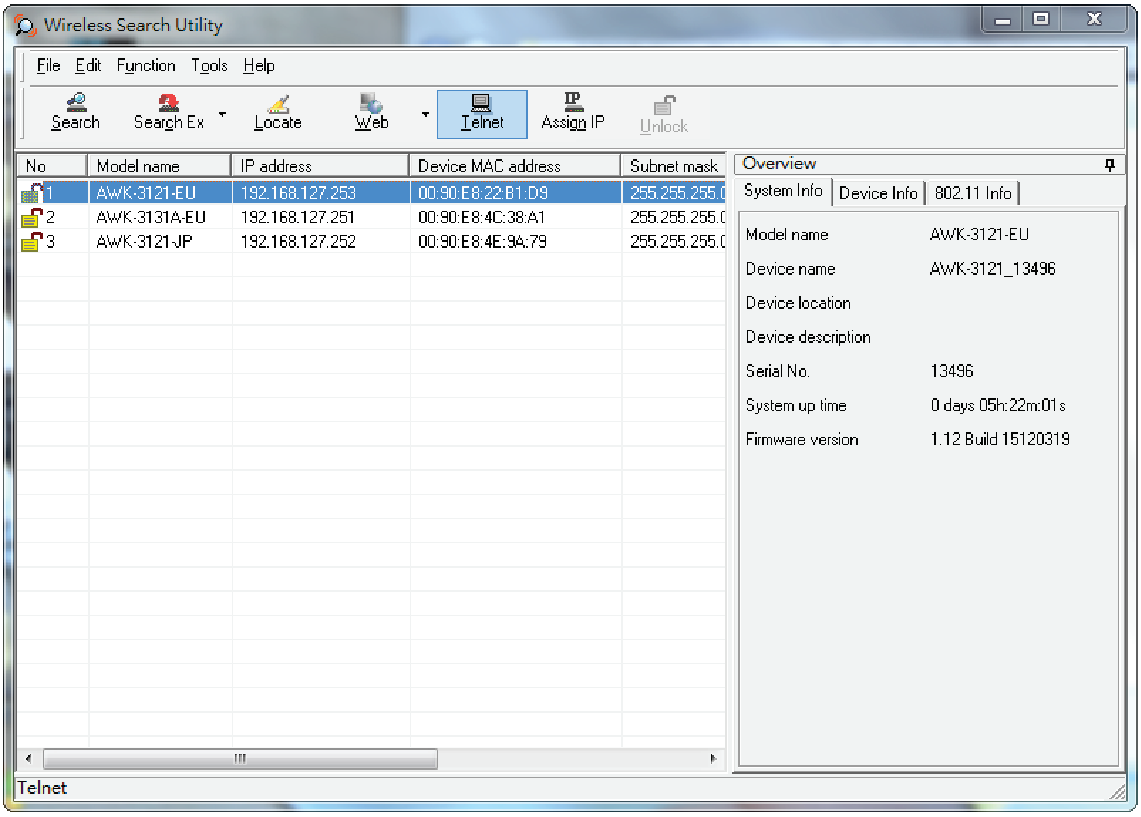
1. Click on the Web icon to open the web console.
   This will take you to the web console, where you can make all configuration changes. Refer to Chapter 3, “Using the Web Console,” for information on how to use the web console.



No	Model name	IP address	Device MAC address	Subnet mask	Firmwar
1	AWK-3121-EU	192.168.127.253	00:90:E8:22:B1:D9	255.255.255.0	1.12 Bu
2	AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0	1.1 Buil
3	AWK-3121-JP	192.168.127.252	00:90:E8:4E:9A:79	255.255.255.0	1.13 Bu

Model name	AWK-3121-
Device name	AWK-3121_
Device location	
Device description	
Serial No.	13496
System up time	0 days 05h:
Firmware version	1.12 Build 1

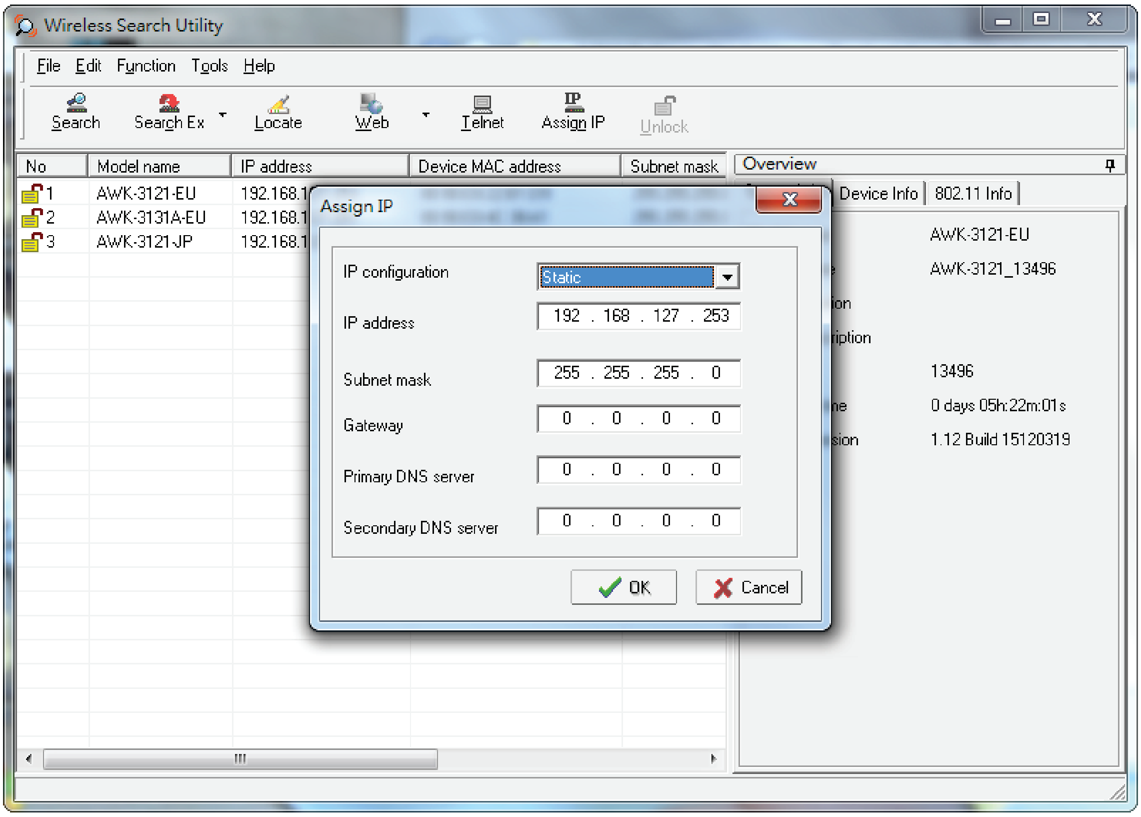
2. Click on **Telnet** if you would like to use telnet to configure your AWKs.



No	Model name	IP address	Device MAC address	Subnet mask
1	AWK-3121-EU	192.168.127.253	00:90:E8:22:B1:D9	255.255.255.0
2	AWK-3131A-EU	192.168.127.251	00:90:E8:4C:38:A1	255.255.255.0
3	AWK-3121-JP	192.168.127.252	00:90:E8:4E:9A:79	255.255.255.0

Model name	AWK-3121-EU
Device name	AWK-3121_13496
Device location	
Device description	
Serial No.	13496
System up time	0 days 05h:22m:01s
Firmware version	1.12 Build 15120319

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



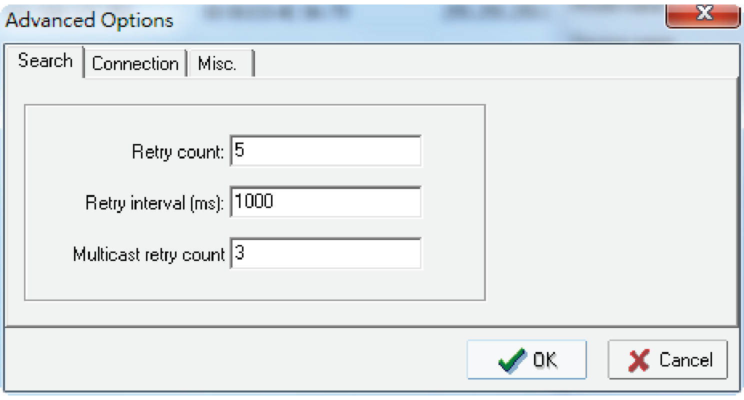
No	Model name	IP address
1	AWK-3121-EU	192.168.1
2	AWK-3131A-EU	192.168.1
3	AWK-3121-JP	192.168.1

IP configuration	Static
IP address	192 . 168 . 127 . 253
Subnet mask	255 . 255 . 255 . 0
Gateway	0 . 0 . 0 . 0
Primary DNS server	0 . 0 . 0 . 0
Secondary DNS server	0 . 0 . 0 . 0

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.



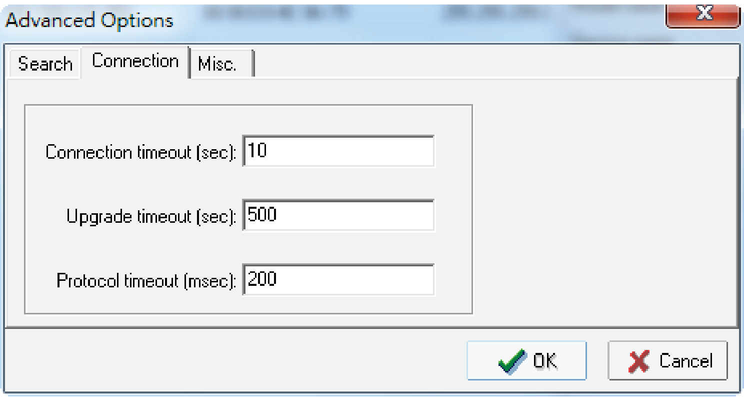
Retry count: 5

Retry interval (ms): 1000

Multicast retry count 3

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.



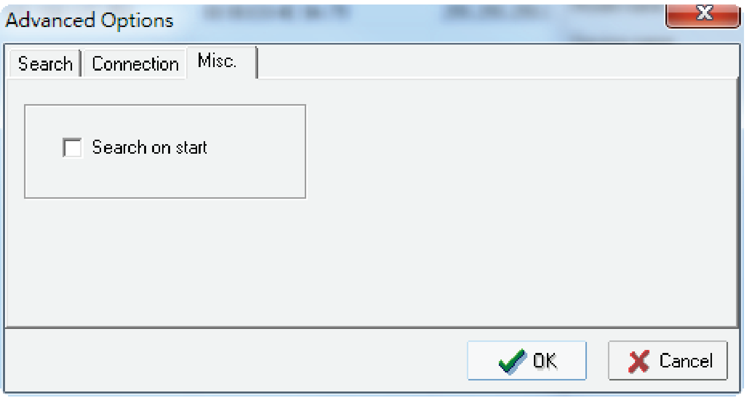
Connection timeout (sec): 10

Upgrade timeout (sec): 500

Protocol timeout (msec): 200

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.



□ Search on start

A

References

This chapter provides more detailed information about wireless-related technologies. The information in this chapter can help you administer your WAC-2004As and plan your industrial wireless network better.

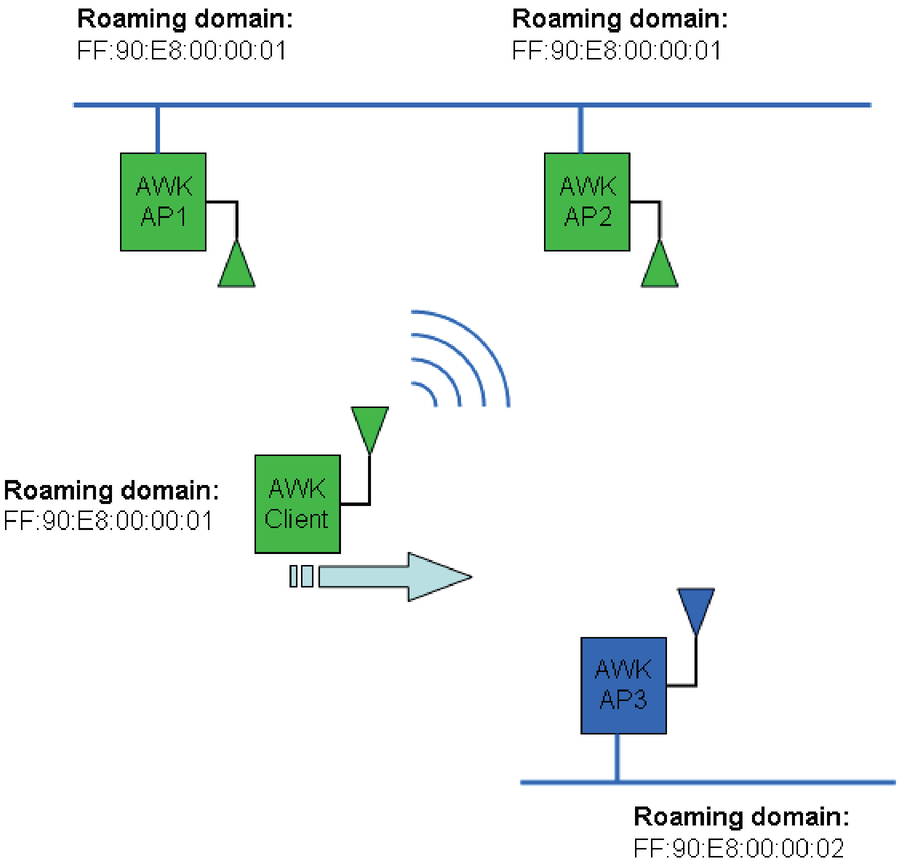
The following topics are covered in this appendix:

❒ **Roaming Domain**

Roaming Domain

A roaming domain defines an area where all related wireless controllers, APs, and clients work together to enable fast roaming. Such a domain is specified as six groups of two hexadecimal digits beginning with the fixed identifier, **FF:90:E8**.

Note that the default value of a roaming domain resembles a controller's MAC address; however, it is not necessary to take the last 3-bytes of a controller's MAC address to form a roaming domain. You may take any six hexadecimal digits to form a unique roaming domain; this will be dissimilar enough for other roaming domains to tell themselves apart.



The purpose of a roaming domain is to ensure that wireless clients roam in the same area, and do not jump onto unintended areas. For example, as illustrated above, a wireless client is disconnected from **AWK AP1** and is trying to connect to the next AP. Even though **AWK AP2** and **AWK AP3** have the same SSID, channel, and wireless settings, the client will not roam onto **AWK AP3** because it is in a different roaming domain. A **roaming domain** setting provides wireless clients with consistent roaming among specific APs.

B

Supporting Information

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

The following topics are covered in this appendix:

About This User’s Manual

This manual is mainly designed for, but not limited to, the following hardware and firmware for the WAC-2004A:

- Hardware Rev: **1.0 or above**
- Firmware Ver: **1.2 or above**

You are strongly recommended to check with your sales representative for the latest product datasheet, firmware, QIG (Quick Installation Guide), UM (User’s Manual), and related information.

Declaration of Conformity (DoC)

Federal Communication Commission Interference Statement

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

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

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

FCC Radiation Exposure Statement

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

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

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