

WAC-M300 Series User Manual

Version 1.0, July 2025

www.moxa.com/products



© 2025 Moxa Inc. All rights reserved.

WAC-M300 Series User Manual

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

Copyright Notice

© 2025 Moxa Inc. All rights reserved.

Trademarks

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

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. About This Manual	5
Symbol Definition for Web Interface Configurations	5
About Note, Attention, and Warning	6
Configuration Reminders	7
A: About Mandatory Parameters	7
2. Getting Started	8
Functional Design	8
LED Indicators	8
Reset Button	8
First-time Installation and Configuration	9
3. Web Interface Configuration	12
Function Introduction	12
System Dashboard	13
Connection Status	13
Unresolved Devices	13
Events	14
Device Resources Dashboard	15
Device Resource Usage	15
Resource Usage Events	16
Compare Device Usage	16
Wi-Fi Dashboard	16
AP Channel Usage	17
Connection Quality	17
Wi-Fi Events	18
Roaming Dashboard	18
Roaming Events	18
Monitoring Roaming Status	19
Network Dashboard	19
Network Events	20
Monitoring Network Packets	20
Wi-Fi Connection Metrics	21
Online Devices	21
Offline/Inactive Devices	21
System Settings	22
General	22
HTTPS	25
Warning Thresholds	25
Syslog	26
SNMP Agent	28
Device Management	30
Access Controllers (WAC)	30
Access Points (AP)	44
Clients (STA)	55
Applications	60
Controller-based Roaming	60
Firmware Management	66
Add a New Release Build	66
Security	67
Login Settings	68
Session Management	70
Web Certificate	70
File Passphrase	71
Account Management	71
Accounts	71
Password Policy	73
Authentication Server	74
Diagnostics	77
Locator	77

Ping	78
Config. Backup & Restore	81
Event Log	84
Maintenance and Tools	84
Change Password	85
Dark Theme.....	86
Sign Out	86

1. About This Manual

Thank you for purchasing a Moxa WAC-M300 Series product. Read this user's manual to learn how to connect your Moxa product with various interfaces and how to configure all settings and parameters via the user-friendly web interface.

Three methods can be used to connect to the Moxa's device, which all will be described in the next two chapters. See the following descriptions for each chapter's main functions.

Chapter 2: Getting Started

In this chapter, we provide instructions on how to initialize the configuration of your Moxa product. We provide two interfaces to access the configuration settings: CLI (Command Line Interface) via the RS-232 console or SSH/Telnet interfaces and web interface.

Chapter 3: Web Interface Configuration

In this chapter, we explain how to access the WAC-M300 Series' various configuration, monitoring, and management functions. These functions can be accessed through a web browser or through the command line console (CLI). In this manual, we describe how to configure the WAC-M300 Series functions via the web interface, which provides the most user-friendly way to configure a Moxa device.

Symbol Definition for Web Interface Configurations

The Web Interface Configuration includes various symbols. For your convenience, refer to the following table for the meanings of the symbols.

Symbols	Meanings
	Add
	Read detailed information
	Clear all
	Column selection
	Refresh
	Enable/Disable Auto Save When Auto Save is disabled, users need to click this icon to save the configuration.
	Export
	Edit
	Perform a Wi-Fi site survey (Client mode only)
	Re-authentication
	Delete
	Panel View
	Expand
	Collapse

Symbols	Meanings
	Hint or additional information
	Settings
	Data comparison
	Menu icon
	Change mode
	Locator
	Reboot
	Reset to defaults
	Logout
	Increase
	Decrease
	Equal
	Menu
	Search
	Hide text that is typed into a text box (usually used when typing a password)
	Show text typed into a text box (usually used when checking a password)

About Note, Attention, and Warning

Throughout the whole manual, you may see notes, attentions, and warnings. The definition of each type is explained below.

Note: This is used to provide additional information for a function, feature, or scenario. Here is an example:



NOTE

The Reset to Default button is disabled by default; users need to enable it in the web console if they want to use it.

Attention: This is used to notify readers of matters or situations that require extra attention to avoid possible issues. Here is an example:



ATTENTION

When a different type of module has been inserted into the WAC-M300 Series, we suggest you configure the settings, or use reset-to-default.

Warning: This is used to notify readers of matters or situations that require extra attention to avoid serious harm to the user or the device. Here is an example:



WARNING

There is a risk of explosion if the battery is replaced by an incorrect type.

Configuration Reminders

In this section, several examples will be used to remind users when configuring the settings for Moxa's WAC-M300 Series.

A: About Mandatory Parameters

Create Server

Enable Server

Server Address

This value is required.

UDP Port

1812

Authentication Type

MS-CHAPv2

Shared Key

This value is required.

Authentication Timeout (sec) ⓘ

5

Authentication Retries (Times)

1

Cancel Save

- If a field is marked in red indicates this mandatory field was skipped. You need to provide the required value in order to save or apply the configuration.
- Some parameter values will be limited to a specific range. If the values exceed the range, it cannot be applied or created.
- Configuration input fields universally do not allow the following special characters: backslash (\), apostrophe ('), double quotes ("), backtick (`).

2. Getting Started

In this chapter, we provide an overview of the WAC-M300 Series and explain how to log into the Moxa WAC-M300 Series for the first time through the web-based interface.

Functional Design

LED Indicators

The LEDs on the front panel of the WAC-M300 Series provide a quick and easy means of determining the current operational status of the device.



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.
		Blinking	Power is not being supplied from power input 2.
Fault	Red	On	System error.
		Blinking	IP address conflict (interval: 0.5 sec).
		Off	The device is operating normally.
State	Green	On	Software is ready.
		Blinking	The WAC has been located by the Search Utility (interval: 1 sec).
	Red	On	Booting error.
Primary	Green	On	This WAC is operating as the primary roaming controller.
		Off	This WAC is not operating as the primary roaming controller.
Backup	Green	On	This WAC is operating as the backup roaming controller.
		Off	This WAC is not operating as the backup roaming controller.
LAN1/2 1G (2-reserved)	Green	On	The LAN port's 1000 Mbps link is active.
		Blinking	Data is being transmitted at 1000 Mbps.
		Off	The LAN port's 1000 Mbps link is inactive.
LAN 1/2 100M (2-reserved)	Amber	On	The LAN port's 100 Mbps link is active.
		Blinking	Data is being transmitted at 100 Mbps.
		Off	The LAN port's 100 Mbps link is inactive.

Reset Button

The reset button is located on the front panel of the device and is used exclusively to reboot the device. Use a pointed object such as an unfolded paper clip to press down the reset button.

Resetting the WAC-M300 to factory default settings can only be done via the device's web interface or CLI command.

First-time Installation and Configuration

Before installing the WAC-M300 Series, make sure that all items in the Package Checklist listed in the Quick Installation Guide are in the box. You will need access to a notebook computer or PC equipped with an Ethernet port.

Step 1: Connect the power inputs and power on the device.

The WAC-M300 Series supports dual redundant power supplies. Connect the power input to a power source using power cords with an IEC C13 connector.

Step 2: Connect the WAC Series to a notebook or PC via the WAC's LAN1 port.

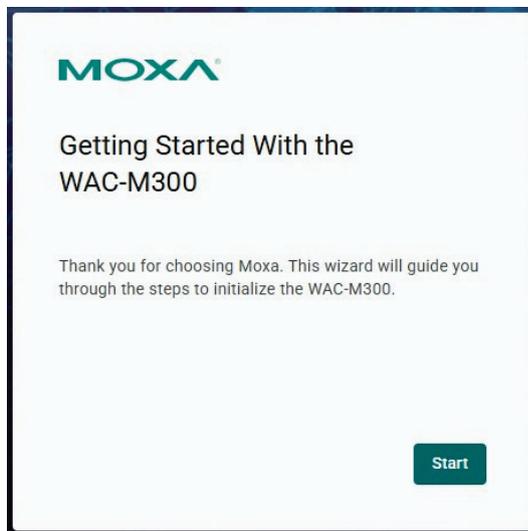
The LED indicator on the WAC Series' LAN port will light up when a connection is established.

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

Choose an IP address on the same subnet as the WAC Series. Since the WAC Series' default IP address is **192.168.127.250**, and the subnet mask is **255.255.255.0**, you should set the IP address of the computer to **192.168.127.xxx**.

Step 4: Access the homepage of the WAC.

Open your computer's web browser and type **https://192.168.127.250** in the address field to access the WAC's homepage. If successfully connected, the WAC's interface homepage will appear. Click **Start**.



Step 5: Configure the WAC's role and network parameters.

Set the WAC role as either the **Main WAC** or **Extended WAC**. If set to **Main WAC**, also configure the **Registration Key**. Configure the IP address, subnet, and gateway parameters according to the network needs.



NOTE

The Main WAC must be set up first before a WAC can be designated as a Backup WAC.

MOXA

Info
The main WAC must be set up first before configuring a backup WAC.

Role
--Select item--

IP Address

Subnet Mask
24 (255.255.255.0)

Gateway

Next >

Step 6: Create a user account and password.

There is no default user account and password. Enter the username and password for the admin account and click **Save**.



NOTE

The username and password are case-sensitive.

MOXA

Create an admin account for the main WAC device.

Admin Account

Password

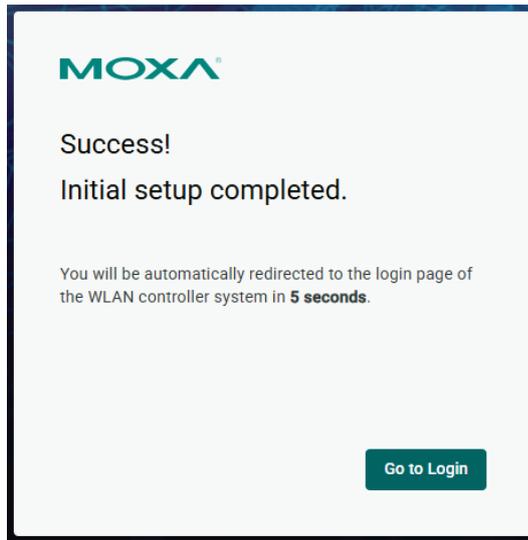
- Must be between 8 to 63 characters.
- Only letters (a-z, A-Z), numbers (0-9), and special characters (_!#\$%&.*@+^{}|--) are allowed.

Confirm Password

< Back

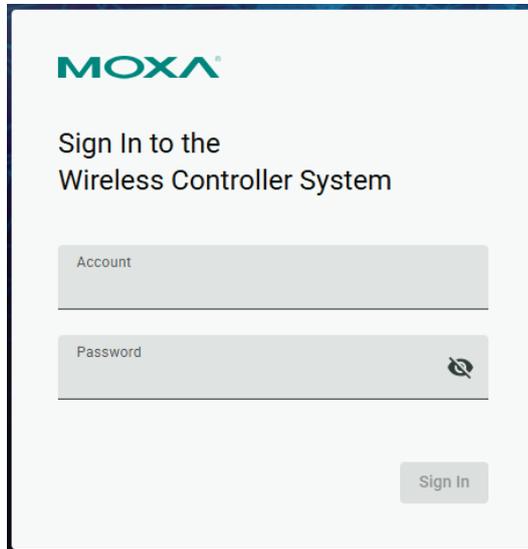
Save

After creating your account, you will be automatically redirected to the login screen.



Step 7: Log in to the device.

Enter your username and password and click **Sign In**.

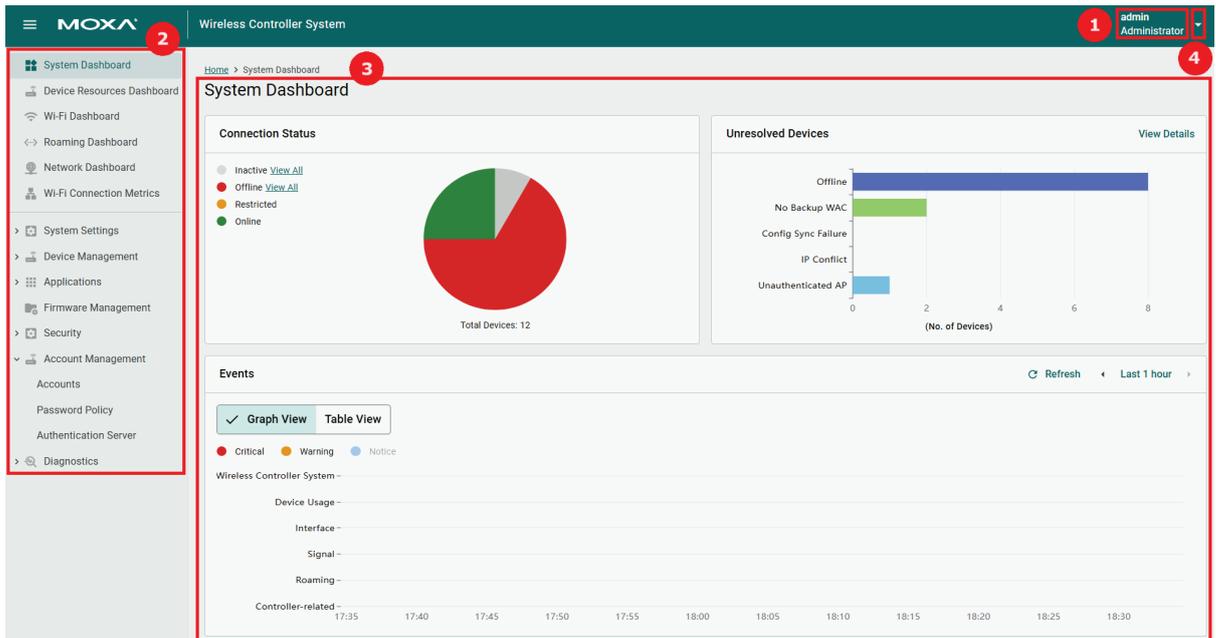


3. Web Interface Configuration

Moxa's WAC-M300 Series offers a user-friendly web interface for easy configuration. All functions of the WAC-M300 Series can be configured via this web interface.

Function Introduction

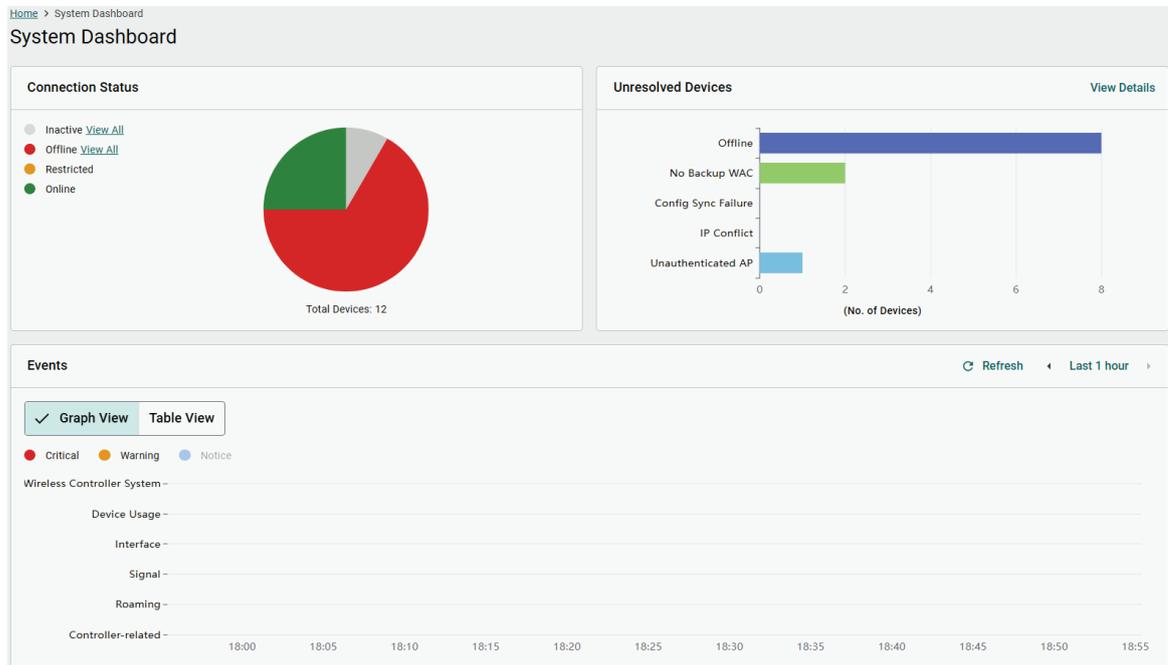
This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



1. **Login Name:** This shows the name of the user that is currently logged in.
2. **Function Menu:** All functions of the WAC-M300 Series are shown here. Click the function you want to view or configure.
3. **System Dashboard:** All important system information and statistics are shown here.
4. **Account Status:** This menu is for changing your password, toggling dark theme, and signing out.

System Dashboard

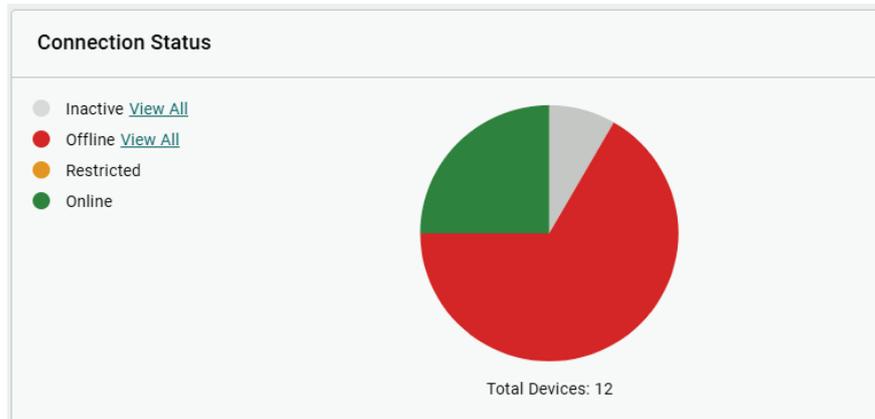
After successfully connecting to the WAC-M300 Series, the **System Dashboard** will automatically appear. To view the device summary from anywhere in the interface, click **System Dashboard** on the Function Menu.



See the following sections for a detailed description of each widget.

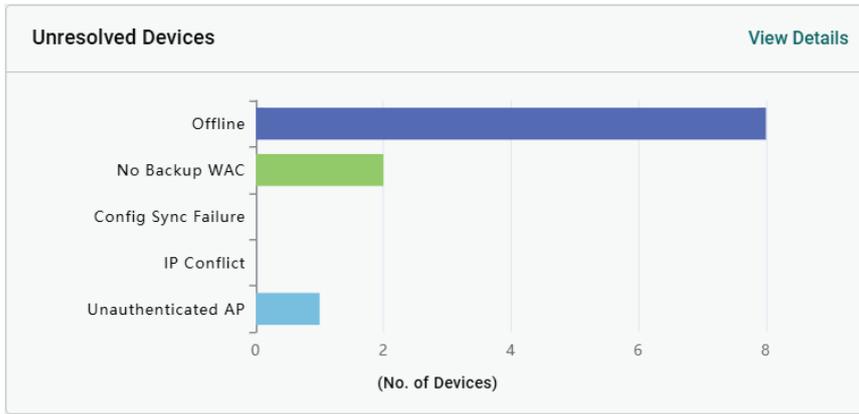
Connection Status

This widget shows the connection status of managed devices, including the number of inactive, offline, restricted, and online devices.



Unresolved Devices

This widget shows the number of unresolved devices. These are devices with pending issues, including offline devices, devices with no assigned backup WAC, devices with failed configuration sync, devices with IP conflicts, and unauthenticated APs.



Click **View Details** to see more detailed information about the affected devices. Click **Manage** to navigate to the relevant configuration page.

Unresolved Devices

WAC [Manage](#)

No Backup WAC

- wac-0090e8ff0003
- wac-0090e8ff0001

AP [Manage](#)

Offline

- ap-0090e88a8794
- ap-0090e88a87a8
- ap-0090e8100070
- ap-0090e8100031
- ap-0090e8100065

Unauthenticated AP

- ap-0090e88a87d9

STA [Manage](#)

Offline

- sta-0090e88a87da
- sta-0090e88a8784
- sta-0090e8100071

[Close](#)

Events

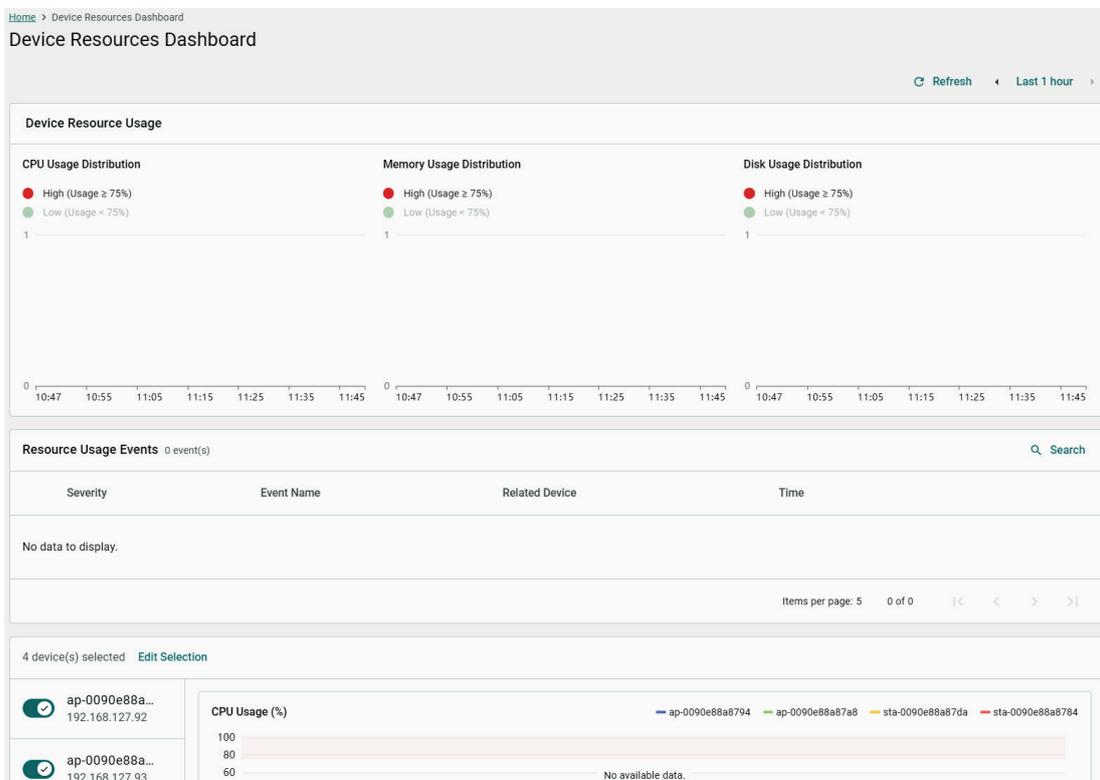
This widget shows all types of critical, warning, and informational events recorded by the system in a graph or table format.



Device Resources Dashboard

Menu Path: Device Resources Dashboard

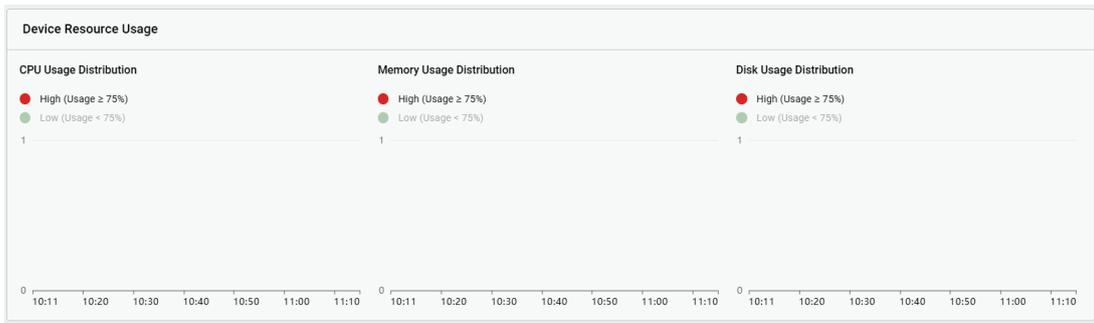
From the **Device Resources Dashboard** screen, you can view the resource usage of the device.



Refer to the following sections for more details about each widget.

Device Resource Usage

This widget shows the CPU, memory, and disk usage status of managed devices. The bar charts only show abnormal (high usage) devices by default. Click the **Low** in each chart to view resource usage information for all other devices.



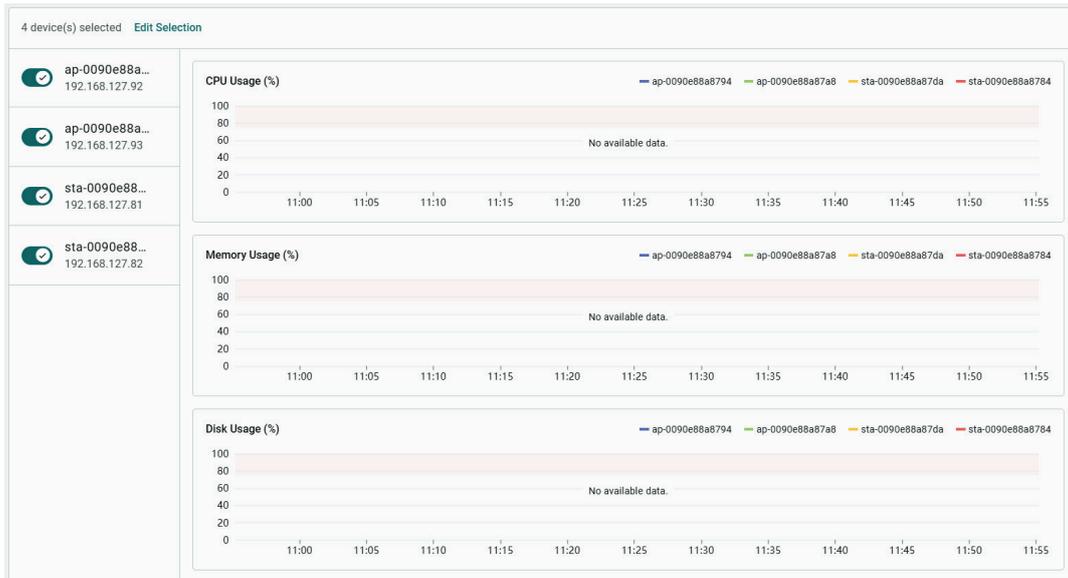
Resource Usage Events

This widget shows resource usage events. These events are triggered when the specified threshold is exceeded. Refer to [Warning Thresholds](#) to configure the threshold for each event type.

Resource Usage Events 0 event(s) 🔍 Search			
Severity	Event Name	Related Device	Time
No data to display.			
Items per page: 5 0 of 0 < > >			

Compare Device Usage

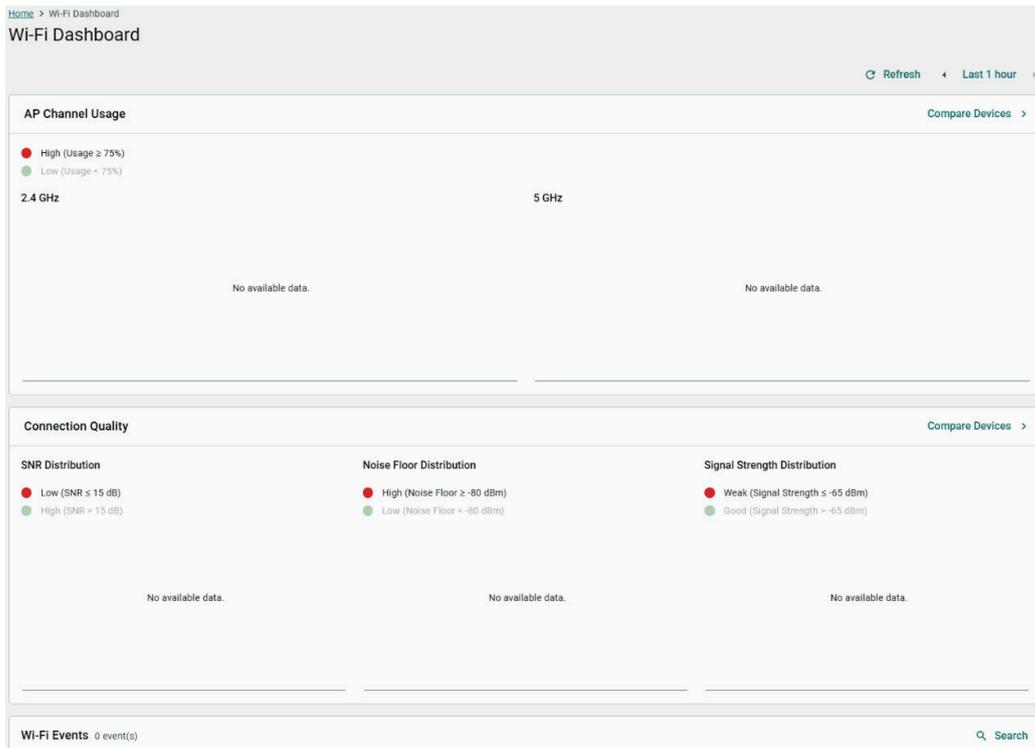
This widget lets you compare the resource usage history of up to 8 selected devices.



Wi-Fi Dashboard

Menu Path: Wi-Fi Dashboard

From the **Wi-Fi Dashboard** screen, you can view the Wi-Fi status of managed devices.



Refer to the following sections for more details about each widget.

AP Channel Usage

This widget shows the AP channel usage of managed devices on the wireless controller system. Click **Compare Devices** to compare and view more detailed AP channel usage information for up to 8 selected APs.



Connection Quality

This widget shows the connection quality status of managed devices. Click **Compare Devices** to compare and view more detailed connection quality information for up to 8 selected devices.



Wi-Fi Events

This widget shows Wi-Fi-related events. These events are triggered when the specified threshold is exceeded. Refer to [Warning Thresholds](#) to configure the threshold for each event type.

Severity	Event Name	Related Device	Time
No data to display.			

Roaming Dashboard

Menu Path: Roaming Dashboard

From the **Roaming Dashboard** screen, you can view the roaming status of managed devices.

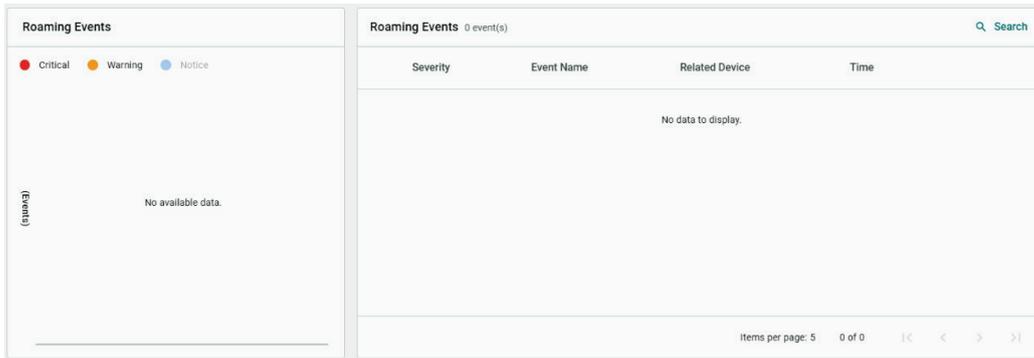
The screenshot displays the 'Roaming Dashboard' interface. At the top, there is a breadcrumb 'Home > Roaming Dashboard' and a title 'Roaming Dashboard'. Below the title are 'Refresh' and 'Last 2 minutes' options. The dashboard is divided into several sections:

- Roaming Events (Left):** A legend with 'Critical' (red), 'Warning' (orange), and 'Notice' (blue) categories. Below it, a vertical bar chart area shows '(0 items)' and 'No available data.'
- Roaming Events (Table):** A table with columns 'Severity', 'Event Name', 'Related Device', and 'Time'. It shows '0 event(s)' and 'No data to display.'
- Selected STAs:** A section titled '2 STA(s) selected' with an 'Edit Selection' link. It lists two STAs: 'sta-0090e88... 192.168.127.81' and 'sta-0090e88... 192.168.127.82'.
- Roaming Timeline:** A chart area for the selected STAs. It includes a legend for 'Signal Strength' with categories: '<-65 dBm' (red), '>= -65 dBm' (green), and 'Not connected' (grey). The chart shows '(0 items)' and 'No available data.' with a time axis from 13:55:15 to 13:57:00.

Refer to the following sections for more details about each widget.

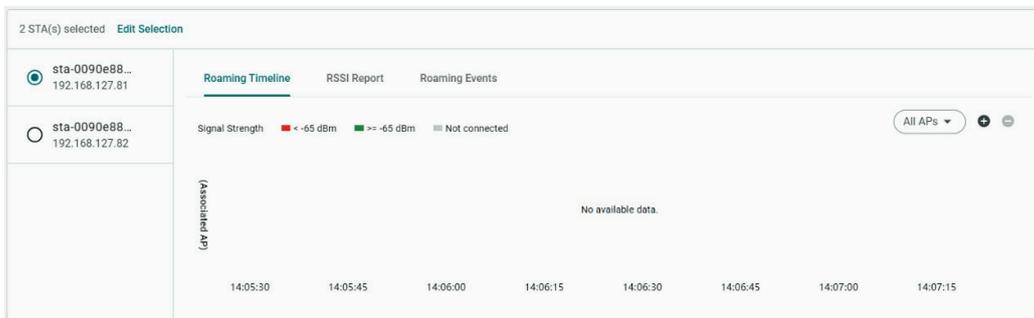
Roaming Events

This widget shows roaming-related events in bar chart and table format.



Monitoring Roaming Status

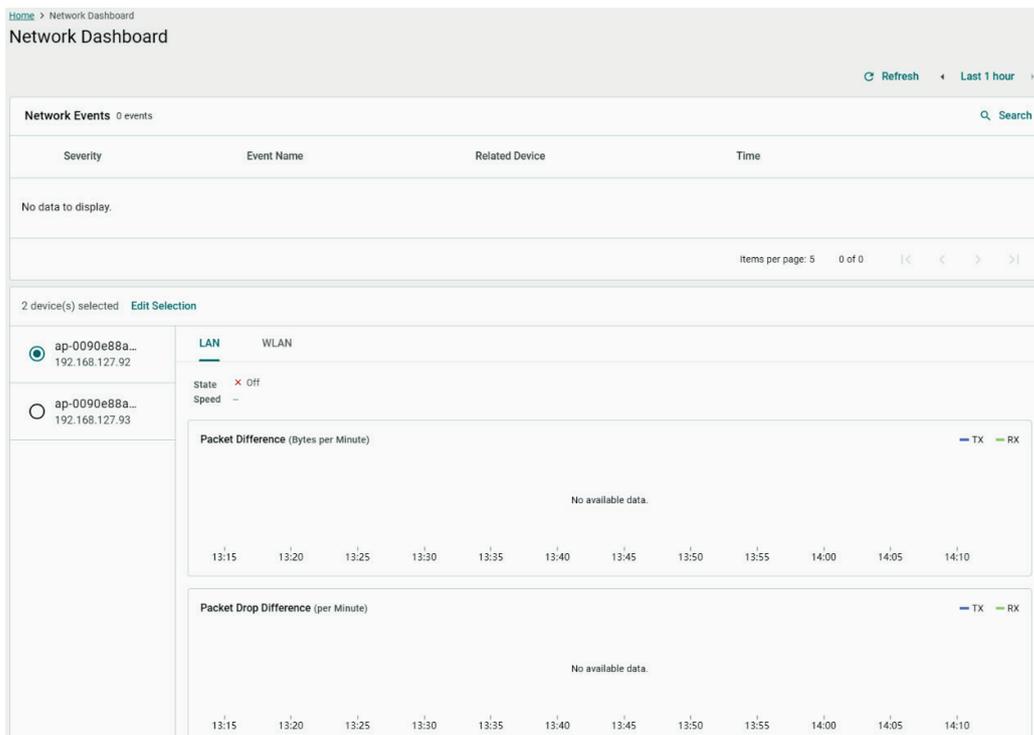
This widget shows the roaming status of managed devices. Click **Compare Devices** to compare and view more detailed roaming information for up to 8 selected devices.



Network Dashboard

Menu Path: Network Dashboard

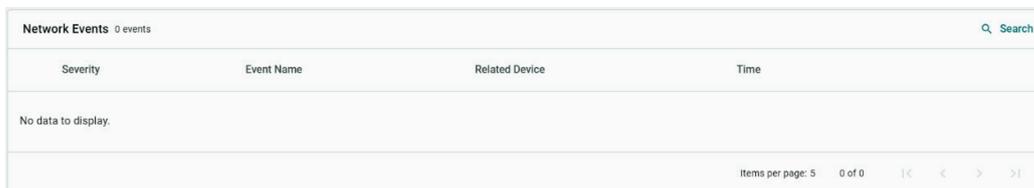
From the **Network Dashboard** screen, you can view real-time data and historical event logs of the network.



Refer to the following sections for more details about each widget.

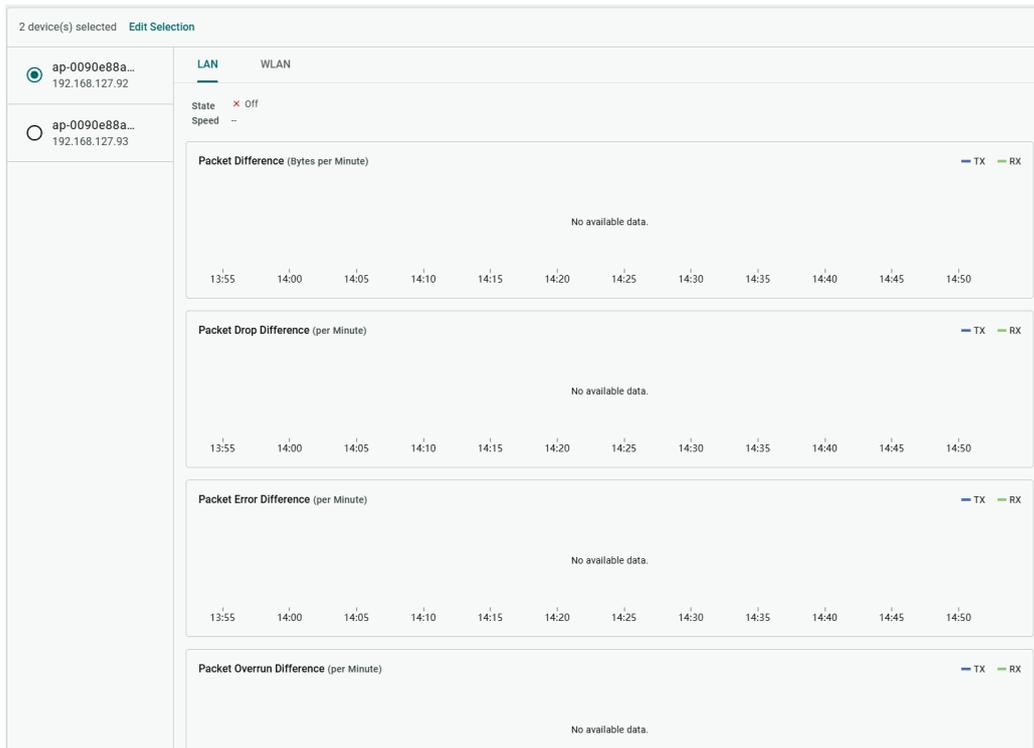
Network Events

This widget shows network-related events. These events are triggered when the specified threshold is exceeded. Refer to [Warning Thresholds](#) to configure the threshold for each event type.



Monitoring Network Packets

This widget shows the packet difference, packet drop difference, packet error difference, and packet overrun difference for selected devices. Click **Compare Devices** to compare and view more detailed packet information for up to 8 selected devices.



Wi-Fi Connection Metrics

Menu Path: Wi-Fi Connection Metrics

From the **Wi-Fi Connection Metrics** screen, you can view real-time AP-client connections and the hierarchical relationship between WACs and APs. If auto-refresh is enabled, the information on this page automatically refreshes every 5 seconds to reflect changes to device connections and roaming events.

This page is further separated into two tabs: **Online Devices** and **Offline/Inactive Devices**.

Online Devices

This tab shows the current connection relationship between online APs and stations, including AP channel usage. To view this page, click the **Online Devices** tab.

Home > Wi-Fi Connection Metrics

Wi-Fi Connection Metrics

Auto-refresh every 5 sec

Online Devices Offline/Inactive Devices

Online AP 0/6

Online STA 0/3

Search

Device Name	IP Address	2.4 GHz Channel (Usage)	5 GHz Channel (Usage)	No. of Connected STA
No data to display.				

Items per page: 10 0 of 0 < >

Offline/Inactive Devices

This tab shows the last known connection relationship between offline and inactive devices to the WAC device. To view this page, click the **Offline/Inactive Devices** tab.

Home > Wi-Fi Connection Metrics

Wi-Fi Connection Metrics

Auto-refresh every 5 sec

Online Devices **Offline/Inactive Devices**

AP STA

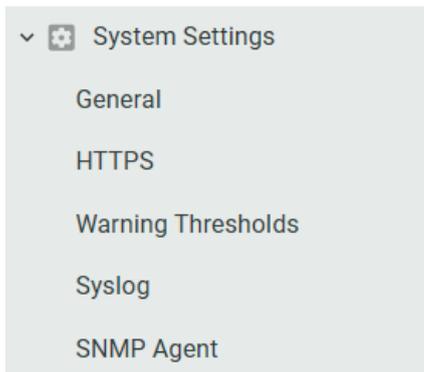
Offline AP 5/6
Inactive AP 1/6

Device Name	Status	IP Address	2.4 GHz Channel (Usage)	5 GHz Channel (Usage)	Last Connected	
ap-0090e88a8794	Offline	192.168.127.92	--	36	Feb 05, 2025 15:58:41	⌵
ap-0090e88a87a8	Offline	192.168.127.93	--	226	Feb 05, 2025 15:50:50	⌵
ap-0090e88a87d9	Inactive	--	--	--	--	⌵
ap-0090e8100070	Offline	192.168.127.96	--	104	Mar 24, 2025 14:40:11	⌵
ap-0090e8100031	Offline	192.168.127.94	6	104	Mar 24, 2025 14:40:21	⌵
ap-0090e8100065	Offline	192.168.127.95	--	36	Feb 06, 2025 17:25:22	⌵

Items per page: 10 1 - 6 of 6 |< < > >|

System Settings

The **System Settings** section covers system configuration functions. From here, you can configure the **General**, **HTTPS**, **Warning Thresholds**, **Syslog**, and **SNMP Agent** settings.



General

Menu Path: System Settings > General

The **General** section houses three subsections: **Time and Date**, **Sync Database**, and **Refresh Interval**. The top of this page shows the IP address and registration key of the associated main WAC.



Time and Date

On the **Time and Date** screen, you can configure the time and date parameters. These settings will synchronize to all devices within the WLAN system. Click the **Time and Date** tab to access this screen.

Time and Date Sync Database Refresh Interval

The time settings will synchronize across all devices within the WLAN system.

Current Device Time
 May 16, 2025 15:41:09 (UTC+08:00) [Refresh](#)

Time Source
 Manual Sync with NTP server

[Sync with browser](#)

Time Zone
 UTC+08:00

Date
 May 16, 2025

Hour : Minute : Second
 15 : 41 : 24

Enable Daylight Saving Time (DST)

[Save](#)

Time Source

Setting	Description	Factory Default
Manual	Manually specify the device time and date.	Manual
Sync with NTP server	Synchronize the device time with the specified NTP server.	

Time Zone

Setting	Description	Factory Default
UTC	Select the UTC time zone the device is located in.	UTC+00:00

Date and Time (Manual Only)

Setting	Description	Factory Default
Date, Hour, Minute, Second	Specify the device's date and time.	Current device date and time

Sync Interval (Sync with NTP server Only)

Setting	Description	Factory Default
10 to 1440	Specify the time interval (in minutes) at which the system will sync the device time with the NTP server.	10

Primary/Secondary NTP Server (Sync with NTP server Only)

Setting	Description	Factory Default
IP address	Specify the NTP server to sync the device time with. The secondary server will be used if the primary server is unavailable.	None

If **Enable Daylight Saving Time (DST)** is checked, also configure the following options:

Offset

Setting	Description	Factory Default
1, 0.5	Specify the daylight saving time offset (in hours).	1

Start/End Date

Setting	Description	Factory Default
Month, Week, Day, Hour	Specify the start and end date and time for daylight saving.	Jan 1st week, Sun. 00

When finished, click **Save**.

Sync Database

From the **Sync Database** screen, you can enable auto-synchronizing the database of the main WAC to all other WAC devices on the wireless controller system (WCS) to ensure data consistency across the network. Click the **Sync Database** tab to access this screen.

To manually sync the database, click **Sync Now**.

Time and Date **Sync Database** Refresh Interval

Synchronize the database from the main WAC to all other WAC devices in the WLAN system to ensure data consistency across the network.

Last Synced on : May 16, 2025 15:00:02

Sync Now

Auto Sync

Enable Auto Sync

Sync Interval
Hourly

Save

Enable Auto Sync

Setting	Description	Factory Default
Checkbox	Enable or disable auto database syncing. If enabled, the system will automatically sync the main WAC's database to all devices in the WCS at the selected interval.	Checked

Sync Interval

Setting	Description	Factory Default
Hourly, Daily	Select the auto-sync interval. If set to Daily, also specify the time of day.	Hourly

When finished, click **Save**.

Refresh Interval

From the **Refresh Interval** screen, you can select the default refresh time interval for all functions that support auto-refresh. Click the **Refresh Interval** tab to access this screen.

Time and Date Sync Database **Refresh Interval**

The interval at which data for functions that support auto-refresh is updated.

Refresh Interval (sec)
30

Save

Refresh Interval (sec)

Setting	Description	Factory Default
Interval	Select the data refresh interval (in seconds).	30

When finished, click **Save**.

HTTPS

Menu Path: System Settings > HTTPS

From this section, you can configure the system's HTTPS TCP port number.

[Home](#) > HTTPS

HTTPS

TCP Port
443

Save

TCP Port

Setting	Description	Factory Default
1 to 43999, 45000 to 65535	Specify the TCP port number for the HTTPS interface used to access the main WAC.	443

When finished, click **Save**.

Warning Thresholds

Menu Path: System Settings > Warning Thresholds

From the **Warning Thresholds** section, you can adjust the warning thresholds for triggering interface-related and signal-related events.

Home > Warning Thresholds

Warning Thresholds

Search

Severity	Group	Event Name	Threshold	
Warning	Interface	Ethernet throughput threshold exceeded	10 (%)	
Warning	Interface	Ethernet PPS threshold exceeded	50000 (packets)	
Warning	Interface	Wireless PPS threshold exceeded	200000 (packets)	
Warning	Signal	Signal strength below threshold	-65 (dBm)	
Warning	Signal	SNR below threshold	15 (dB)	
Warning	Signal	Noise floor threshold exceeded	-80 (dBm)	
Warning	Signal	Channel usage threshold exceeded	75 (%)	

Items per page: 10 1 - 7 of 7 < >

Click the **Edit** () icon to modify the threshold value for the corresponding event.

When finished, click **Save**.

Syslog

Menu Path: System Settings > Syslog

The **Syslog** section houses two subsections: **Server** and **Event Log Settings**.

Server

The **Server** screen lets you configure up to 5 external syslog servers for sending the WAC's event logs to. Click the **Server** tab to access this screen.

Home > Syslog

Syslog

WLAN system and device event logs can be sent to one or multiple external syslog servers.

Server Event Log Settings

Syslog Servers Create

No.	Server Address	Status	TCP/UDP Port	
1	192.168.127.200	Enabled	514	

Edit

Disable Server

Delete

Create a New Syslog Server

Click **Create** to add a new syslog server.

Create Server

Enable server

Server Address

TCP/UDP Port
514

Cancel Save

Enable server

Setting	Description	Factory Default
Checkbox	Check to enable or disable the syslog server.	Unchecked

Server Address

Setting	Description	Factory Default
IP address	Enter the IP address of the syslog server.	None

TCP/UDP Port

Setting	Description	Factory Default
1 to 65535	Specify the TCP/UDP port of the syslog server.	514

When finished, click **Save**.

Edit a Syslog Server

Click the **menu** (☰) icon next to the server you want to modify and click **Edit**.

For configuration settings, refer to [Create a New Syslog Server](#).

When finished, click **Save**.

Disable a Syslog Server

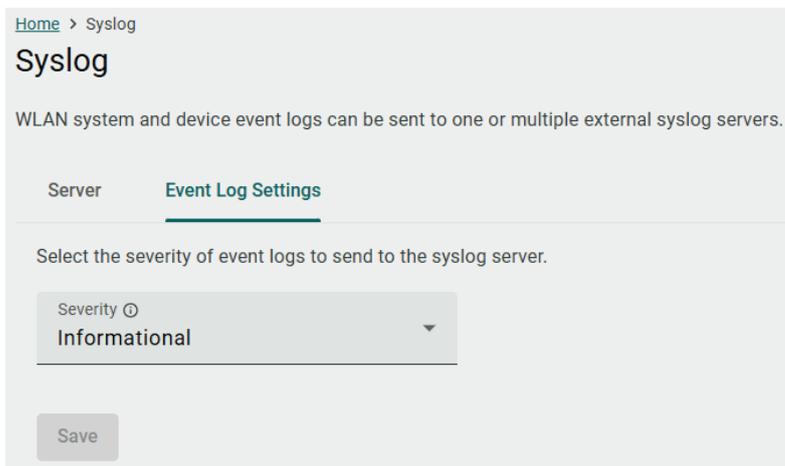
Click the **menu** (☰) icon next to the server you want to disable and click **Disable**.

Delete a Syslog Server

Click the **menu** (☰) icon next to the server you want to delete and click **Delete**.

Event Log Settings

The **Event Log Settings** screen lets you configure the severity of event logs to send to the syslog server. Syslog severity levels are inclusive, meaning logs will be sent for the selected severity level and all levels below it. For example, selecting 'Warning' will also send logs with "Notice" or "Informational" severity.



Configure the following settings:

Server Address

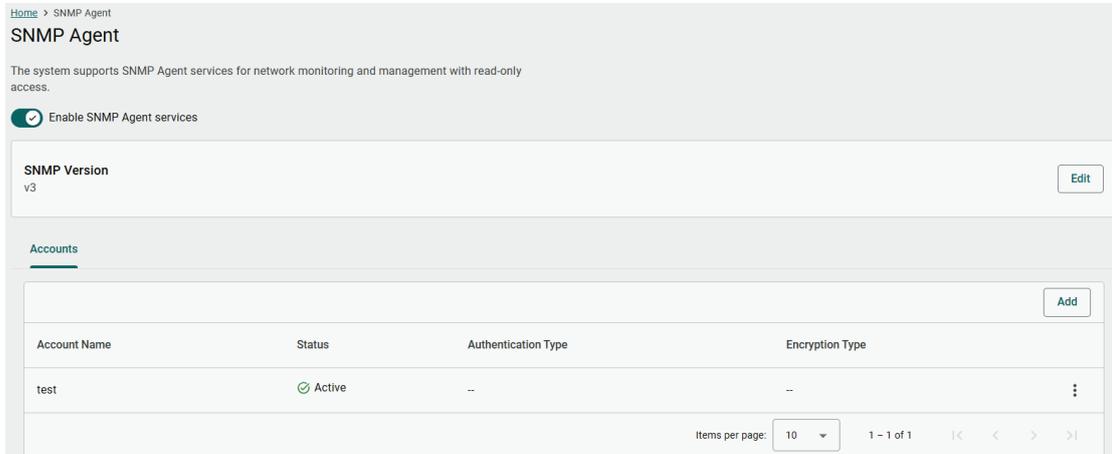
Setting	Description	Factory Default
Emergency, Alert, Critical, Error, Warning, Notice, Informational	Select the severity level of event logs to send to the syslog server. Logs with severity levels under the selected level will also be sent to the syslog server.	Informational

When finished, click **Save**.

SNMP Agent

Menu Path: System Settings > SNMP Agent

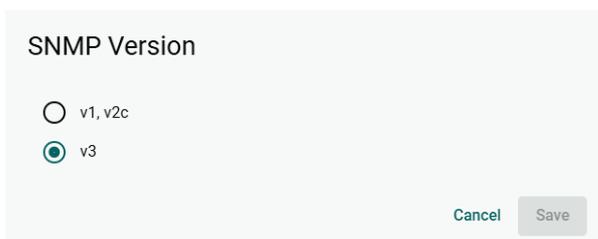
From the **SNMP Agent** section, you can enable SNMP Agent services for network monitoring and read-only management. This page is also used to manage SNMP accounts.



Enable SNMP Agent Services

Setting	Description	Factory Default
Enable/Disable	Use the toggle to enable or disable SNMP Agent services.	Enabled

To change the SNMP version, click the **Edit** button and select the desired SNMP version.



When finished, click **Save**.

Create an SNMP Account

To add an SNMP account, click **Add** in the Accounts table.

Add Account

Enable account authentication

Enable Account Privacy

Configure the following settings:

Account Name

Setting	Description	Factory Default
4 to 32 characters	Enter the username for the SNMP account.	None

Account Authentication

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable account authentication.	Disabled

Authentication Type

If **Account Authentication** is enabled, configure the authentication type.

Setting	Description	Factory Default
MD5	Use MD5 as the authentication type.	None
SHA	Use SHA as the authentication type.	
SHA256	Use SHA256 as the authentication type.	
SHA384	Use SHA384 as the authentication type.	
SHA512	Use SHA512 as the authentication type.	

Authentication Password

If **Account Authentication** is enabled, configure the authentication password.

Setting	Description	Factory Default
8 to 63 characters	Enter the password for the SNMP account.	None

Account Privacy

If **Account Authentication** is enabled, configure account privacy.

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable account privacy. If enabled, the SNMP account will use encryption.	Disabled

Encryption Method

If **Account Privacy** is enabled, configure the encryption method.

Setting	Description	Factory Default
AES	Use AES as the encryption method.	None
DES	Use DES as the encryption method.	

Encryption Key

If **Account Privacy** is enabled, configure the encryption method.

Setting	Description	Factory Default
1 to 63 characters	Enter the encryption key.	None

When finished, click **Save**.

Device Management

From the **Device Management** section, you can manage settings for the different device types, including access controllers (WAC), access points (AP), and clients (STA).



Access Controllers (WAC)

Menu Path: Device Management > Access Controllers (WAC)

From the **Access Controllers (WAC)** page, you can view the status of tasks and manage WAC devices.

Home > Access Controllers (WAC)

Access Controllers (WAC)

0	0	0	103	20	Task Status
Scheduled	Canceled	In Progress	Completed	Failed	

<input type="checkbox"/>	Device Name	Status	IP Address	MAC Address	Firmware Version	Config Sync Status	Mode	No. of Connected AP	Model Name
<input type="checkbox"/>	wac-0090e8ff0... Main	Online	192.168.127.249	00:90:E8:FF:00:01	v1.0.1 Build 2025_...	Passed (no change)	Primary !	0	WAC-M300
<input type="checkbox"/>	wac-0090e8ff0...	Online	192.168.127.248	00:90:E8:FF:00:02	v1.0.1 Build 2025_...	Passed (no change)	Idle	0	WAC-M300
<input type="checkbox"/>	wac-0090e8ff0...	Online	192.168.127.247	00:90:E8:FF:00:03	v1.0 Build 2025_0...	Passed (no change)	Primary !	0	WAC-M300

Items per page: 10 1 - 3 of 3

Task Status

To view details about task results and a list of scheduled tasks for WAC access controller devices, click **Task Status**.



NOTE

All device types (WAC, AP, STA) have a dedicated Task Status page. While task types may differ, the Task Status page behaves the same for all devices.

Task Result

The **Task Result** tab shows details of all finished tasks.

Click **Export Record** to export all task records to the local host in CSV format.

To delete records, check the box of the task record(s) you want to delete and click **Clear Record**.

Home > WAC > Task Status

← Task Status

Task Result Scheduled Tasks

Exported configuration files can be downloaded [here](#).

Search Export Record

<input type="checkbox"/>	Device Name	Task	Status	Start Time	End Time	Duration (sec)
<input type="checkbox"/>	wac-0090e8ff0003	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0708_...	Completed	Jul 08, 2025 14:43:44	Jul 08, 2025 14:45:08	83
<input type="checkbox"/>	wac-0090e8ff0001	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0707_...	Completed	Jul 07, 2025 16:47:28	Jul 07, 2025 16:49:06	98
<input type="checkbox"/>	wac-0090e8ff0002	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0707_...	Failed Timed out.	Jul 07, 2025 16:46:52	Jul 07, 2025 16:51:52	300
<input type="checkbox"/>	wac-0090e8ff0003	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0707_...	Failed Timed out.	Jul 07, 2025 16:46:52	Jul 07, 2025 16:51:52	300
<input type="checkbox"/>	wac-0090e8ff0001	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0704_...	Completed	Jul 07, 2025 12:31:26	Jul 07, 2025 12:33:04	98
<input type="checkbox"/>	wac-0090e8ff0002	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0704_...	Completed	Jul 07, 2025 12:28:58	Jul 07, 2025 12:30:39	101
<input type="checkbox"/>	wac-0090e8ff0003	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0704_...	Completed	Jul 07, 2025 12:28:57	Jul 07, 2025 12:30:24	87
<input type="checkbox"/>	wac-0090e8ff0001	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0627_...	Completed	Jun 27, 2025 18:12:07	Jun 27, 2025 18:13:52	105
<input type="checkbox"/>	wac-0090e8ff0002	Firmware upgrade FWR_WAC-M300_v1.0.1_2025_0627_...	Completed	Jun 27, 2025 18:11:45	Jun 27, 2025 18:14:00	134

Scheduled Tasks

The **Scheduled Result** tab shows a list of all currently pending scheduled tasks. Once a scheduled task is finished, a record will be added to the **Task Result** table.

To cancel a scheduled task, check the box of the task(s) you want to cancel and click **Cancel Task**.

Home > WAC > Task Status

← Task Status

Task Result Scheduled Tasks

Search

<input type="checkbox"/>	Device Name	Task	Status	Start Time
<input type="checkbox"/>	wac-0090e8ff0001	Firmware upgrade	Scheduled	Jul 16, 2025 10:00:00

Items per page: 10 1 - 1 of 1 < >

Add a WAC Device

Click **Add Device** in the device list to add a WAC device.

Add Device

Method
Import CSV file

Import CSV File

You can add multiple devices at once by importing a device list (in CSV format). Any conflicting settings for existing devices will be overwritten.

[Download Template](#)

CSV File

Configure the following settings:

Method

Setting	Description	Factory Default
Import CSV file	Add one or multiple devices in bulk by importing the device information as a CSV file. Click Download Template to download an example file.	Import CSV file
Manually add device	Manually add a single device.	

CSV File (Import CSV File Only)

Setting	Description	Factory Default
CSV File	Click Browse and navigate to the CSV file on the local host.	None

MAC Address (Manually Add Device Only)

Setting	Description	Factory Default
MAC Address	Enter the MAC address of the device.	None

IP Address (Manually Add Device Only)

Setting	Description	Factory Default
IP Address	Enter the IP address of the device.	None

Device Name - optional (Manually Add Device Only)

Setting	Description	Factory Default
CSV File	Enter a name for the device.	None

Assign as Primary WAC (Manually Add Device Only)

Setting	Description	Factory Default
Checkbox	Designate the device as a primary WAC.	Unchecked

When finished, click **Save**.

WAC Device Page

Click the name of a WAC device in the Device Name column on the **Access Controllers (WAC)** page to open the device details page. From this screen, you can view the current WAC device status and device details including general settings, resource usage, managed AP devices, and event records. You can also perform several access controller-related actions from this screen.

Home > Access Controllers (WAC) > wac-0090e8ff0001

← wac-0090e8ff0001

wac-0090e8ff0001 (192.168.127.249) **Primary** **Main** Action ▾

Online - Passed
Last Came Online: Jul 07, 2025 16:49:48
Backup WAC: **No backup WAC assigned** [Set Up now >](#)

General Network Resource Usage Managed APs (5) Task Record Event Log

Device Information Edit

Data received on Jul 11, 2025 10:09:43

Model Name WAC-M300

MAC Address 00:90:E8:FF:00:01

System Uptime 3 days, 17:21:24

Power Input **X** Power 1 **X** Power 2

Firmware Version v1.0.1 Build 2025_0707_1426

Bootloader Version v1.0

Serial Number 0

IP Settings Edit

IP Address 192.168.127.249

Subnet Mask 255.255.255.0

Gateway --

Primary DNS Server --

Secondary DNS Server --

System Information Edit

Device Name wac-0090e8ff0001

Description 2

Location 1

Contact Information --

Event Notifications Edit

Enabled Notifications 39 event(s) selected

SNMP Trap/Inform Enabled

SNMP Type & Version SNMP Trap v2c

Server 1 192.168.127.200

Command Actions

The **Action** menu allows you to perform several actions. Available actions depend on the WAC device's status and role.

Action ▾

- Upgrade Firmware
- Reboot
- Reset to Factory Defaults
- Manage Backup WAC ▶
- Set as Idle WAC
- Delete Device

Upgrade Firmware

Click **Upgrade Firmware** in the **Action** menu to upgrade the WAC device's firmware.



NOTE

To upgrade device firmware, a firmware release build with the target firmware version needs to be created first. Refer to [Firmware Management](#).

Configure the following settings:

Execution Time

Setting	Description	Factory Default
Immediate	Perform the firmware upgrade immediately.	Immediate
Scheduled	Perform the firmware upgrade at the specified date and time. A scheduled task will be created and added to the Scheduled Task list. Refer to Scheduled Tasks .	

Date and Time (Scheduled Only)

Setting	Description	Factory Default
Date, Hour, Minute	Specify the date, hour, and minute to execute the scheduled task. The Minute value can only be set as 30-minute intervals (00, 30).	Based on current device date and time

Firmware Release Build

Setting	Description	Factory Default
Firmware Release Build	Select the release build to upgrade the device firmware.	None

When finished, click **Save**.

Reboot Device

Click **Reboot Device** in the **Action** menu to restart the device.

Configure the following settings:

Execution Time

Setting	Description	Factory Default
Immediate	Reboot the device immediately.	Immediate
Scheduled	Perform the reboot at the specified date and time. A scheduled task will be created and added to the Scheduled Task list. Refer to Scheduled Tasks .	

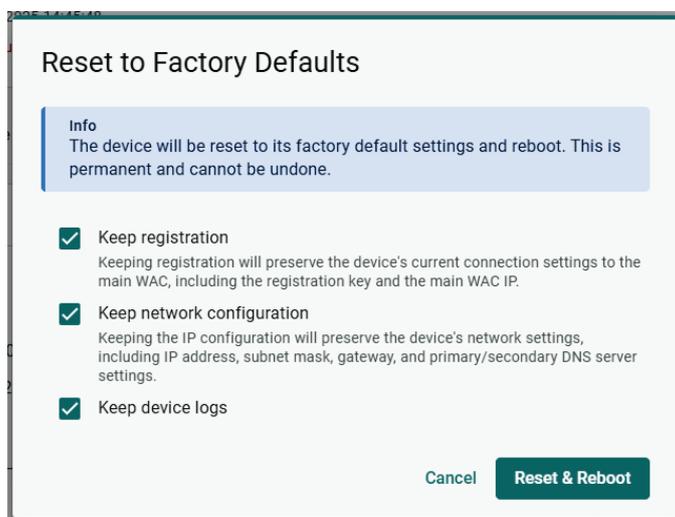
Date and Time (Scheduled Only)

Setting	Description	Factory Default
Date, Hour, Minute	Specify the date, hour, and minute to execute the scheduled task. The Minute value can only be set as 30-minute intervals (00, 30).	Based on current device date and time

When finished, click **Save**.

Reset to Factory Defaults

Click **Reset to Factory Defaults** in the **Action** menu to reset the WAC device's configuration to the factory default settings. Depending on the selected options, certain types of data can be kept.



Configure the following settings:

Keep Registration

Setting	Description	Factory Default
Checkbox	Keeping the registration information will preserve the device's current connection settings to the main WAC, including the registration key and the main WAC IP. The WAC device will register to the original main WAC after resetting the device. If unchecked, the device will need to be registered again with the main WAC.	Checked

Keep Network Information

Setting	Description	Factory Default
Checkbox	Keeping the IP configuration will preserve the device's network settings, including IP address, subnet mask, gateway, and primary/secondary DNS server settings.	Checked

Keep Device Logs

Setting	Description	Factory Default
Checkbox	Keeping device logs will preserve all logs of the device.	Checked

When finished, click **Reset & Reboot**.

Manage Backup WAC

Click **Manage Backup WAC** in the **Action** menu to assign or unpair a backup WAC device, and swap roles. Assigning a backup WAC is recommended for redundancy. When the WAC device becomes unavailable, the assigned backup WAC will take over operations until the original WAC is restored to a working state.

Available options depend on the current status and role of the device.

Assign a Backup WAC

If no backup is assigned, click **Assign Backup WAC** to assign a backup WAC device to the primary WAC.



NOTE

Only idle WAC devices can be assigned as a backup WAC. To designate a WAC device as idle, refer to [Set as Idle WAC](#).

Select Backup WAC for wac-0090e8ff0001

When wac-0090e8ff0001 fails, the selected backup WAC will automatically take over.

Device Name	IP Address	Mode
<input type="radio"/> wac-0090e8ff0002	192.168.127.248	Idle

[Cancel](#) [Save](#)

Select the WAC device to assign as the backup and click **Save**.

Unpair a Backup WAC

If a backup WAC is already assigned, click **Unpair** to unpair the backup WAC device. Once unpaired, the backup WAC will become idle.

Unpair wac-0090e8ff0001 and wac-0090e8ff0002

Warning
Data related to the paired primary WAC on wac-0090e8ff0002 will be reset.

The mode of the following WAC devices will be changed as shown below.:

Device Name	IP Address	Mode
wac-0090e8ff0001	192.168.127.249	Primary
wac-0090e8ff0002	192.168.127.248	Idle

[Cancel](#) [Save](#)

When finished, click **Save**.

Switch WAC Roles

If a backup WAC device is assigned, click **Switch With Backup WAC** to swap the currently assigned backup and primary WAC devices.

Switch Mode Between wac-0090e8ff0002 and wac-0090e8ff0003

Warning
Roaming and AP tasks will be unavailable while switching WAC modes.

The mode of the following WAC devices will be changed as shown below.

Device Name	IP Address	Mode
wac-0090e8ff0002	192.168.127.248	Backup
wac-0090e8ff0003	192.168.127.247	Primary

When finished, click **Save**.

Set as Idle WAC

Click **Set as Idle WAC** in the **Action** menu to turn the primary WAC device into an idle WAC that can be assigned as a backup to another primary WAC device.

Set wac-0090e8ff0002 as Idle WAC

The mode of the following WAC devices will be changed as shown below.:

Device Name	IP Address	Mode
wac-0090e8ff0002	192.168.127.248	Idle

When finished, click **Save**.

Set as Primary WAC

Click **Set as Primary WAC** in the **Action** menu to turn the idle WAC device into a primary WAC to manage access points and clients.

Assign wac-0090e8ff0002 as Primary WAC

The mode of the following WAC devices will be changed as shown below.:

Device Name	IP Address	Mode
wac-0090e8ff0002	192.168.127.248	Primary

When finished, click **Save**.

Delete Device

Click **Delete Device** in the **Action** menu to delete the WAC device. This will delete all relevant device information from the WLAN system and tasks can no longer be assigned to the WAC device.

When prompted, click **Delete**.

General

The **General** tab contains general information about the WAC device including IP settings, event notifications, and system information.

The screenshot shows the 'General' tab of the WAC device configuration interface. It features several sections: 'Device Information' with fields for Model Name (WAC-M300), MAC Address (00:90:E8:FF:00:01), System Uptime (1 days, 02:26:03), Power Input (Power 1 and Power 2), Firmware Version (v1.0.1 Build 2025_0707_1426), Bootloader Version (v1.0), and Serial Number (0). 'Event Notifications' shows 39 event(s) selected and SNMP Trap/Inform is enabled. 'IP Settings' displays IP Address (192.168.127.249), Subnet Mask (255.255.255.0), Gateway, Primary DNS Server, and Secondary DNS Server. 'System Information' shows Device Name (wac-0090e8ff0001), Description (2), Location (1), and Contact Information.

Edit IP Settings

To edit the device's IP settings, click the **Edit** icon in the **IP Settings** widget.

The screenshot shows the 'Edit IP Settings' dialog box. It contains input fields for IP Address (192.168.127.249), Subnet Mask (24 (255.255.255.0)), Gateway (optional), Primary DNS Server (optional), and Secondary DNS Server (optional). At the bottom, there are 'Cancel' and 'Save' buttons.

Configure the following settings:

IP Address

Setting	Description	Factory Default
IP address	Specify the IP address of the device.	Current IP address

Subnet Mask

Setting	Description	Factory Default
1 (128.0.0.0) to 32 (255.255.255.255)	Specify the subnet mask of the device.	Current subnet mask

Gateway - optional

Setting	Description	Factory Default
IP address	Enter the gateway IP address.	None

Primary/Secondary DNS Server - optional

Setting	Description	Factory Default
IP address	Enter the primary and secondary DNS server address. The secondary DNS server acts as a redundant server and will take over if the primary server becomes unavailable.	None

When finished, click **Save**.

Edit Event Notifications

To edit the system event notifications and SNMP Trap settings, click the **Edit** icon in the **Even Notifications** widget.



NOTE

The notification settings apply to all WAC devices in the WLAN system.

Notification Settings

From the **Notification Settings** tab, you can enable or disable SNMP Trap/Inform notifications for specific notification types.

Check the **SNMP Trap/Inform** checkbox for the event(s) you want to receive notifications for.

Home > WAC > Event Notifications
← Event Notifications

These settings apply to all WAC devices in the WLAN system.

Notification Settings SNMP Trap/Inform

Severity: Critical Notice Warning

Severity	Group	Event Name	SNMP Trap/Inform
Critical	System	Cold start	<input checked="" type="checkbox"/>
Warning	System	Warm start	<input checked="" type="checkbox"/>
Notice	System	Event log clearance	<input checked="" type="checkbox"/>
Warning	Account	Authentication failure	<input checked="" type="checkbox"/>
Notice	Network	Link establishment on LAN 1	<input checked="" type="checkbox"/>
Notice	Network	Link disconnection on LAN 1	<input checked="" type="checkbox"/>
Notice	Network	Link establishment on LAN 2	<input checked="" type="checkbox"/>
Notice	Network	Link disconnection on LAN 2	<input checked="" type="checkbox"/>

Save

When finished, click **Save**.

SNMP Trap/Inform

From the **SNMP Trap/Inform** tab, you can configure SNMP Trap/Inform server settings for receiving notifications.

[Home](#) > [WAC](#) > Event Notifications

← Event Notifications

These settings apply to all WAC devices in the WLAN system.

Notification Settings **SNMP Trap/Inform**

Enable SNMP Trap/Inform

SNMP Type
Trap

SNMP Version
v2c

Trap Community
public

Server Settings

Server 1 Address
192.168.127.200

+ Add Server

Save

Configure the following settings:

Enable SNMP Trap/Inform

Setting	Description	Factory Default
Checkbox	Enable or disable SNMP Trap/Inform functionality.	Checked

SNMP Type

Setting	Description	Factory Default
Trap	Set the SNMP type to Trap.	Trap
Inform	Set the SNMP type to Inform.	

SNMP Version

Setting	Description	Factory Default
v1	Set the SNMP version to v1. This option is not available if the SNMP type is set to Inform.	v2c
v2c	Set the SNMP version to v2c.	
v3	Set the SNMP version to v3.	

Trap Community (SNMP v1/v2c Only)

Setting	Description	Factory Default
1 to 32 characters	Specify the Trap community string.	public

Account Name (SNMP v3 Only)

Setting	Description	Factory Default
4 to 32 characters	Enter the username of the SNMP account.	None

Account Authentication (SNMP v3 Only)

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable account authentication.	Disabled

Authentication Type

If **Account Authentication** is enabled, select the authentication type.

Setting	Description	Factory Default
MD5	Use MD5 as the authentication type.	None
SHA	Use SHA as the authentication type.	
SHA256	Use SHA256 as the authentication type.	
SHA384	Use SHA384 as the authentication type.	
SHA512	Use SHA512 as the authentication type.	

Authentication Password

If **Account Authentication** is enabled, configure the authentication type.

Setting	Description	Factory Default
8 to 63 characters	Enter the password for the SNMP account.	None

Account Privacy

If **Account Authentication** is enabled, configure account privacy.

Setting	Description	Factory Default
Enabled/Disabled	Enable or disable account privacy. If enabled, the SNMP account will use encryption.	Disabled

Encryption Method

If **Account Privacy** is enabled, select the encryption method.

Setting	Description	Factory Default
AES	Use AES as the encryption method.	None
DES	Use DES as the encryption method.	

Encryption Key

If **Account Privacy** is enabled, configure the encryption key.

Setting	Description	Factory Default
1 to 63 characters	Enter the encryption key.	None

Device Name

Setting	Description	Factory Default
1 to 255 characters	Enter a name for the device.	[device type]-[MAC address]

Inform Retries (Count) (SNMP Inform Only)

Setting	Description	Factory Default
1 to 99	Specify the maximum number of Inform retries.	3

Inform Timeout (sec) (SNMP Inform Only)

Setting	Description	Factory Default
1 to 300	Specify the duration (in seconds) after which an Inform attempt is considered timed out.	10

Server 1/2 Address

Setting	Description	Factory Default
IP address	Specify the IP address of the server to receive SNMP trap/inform notifications. Click Add Server to add a second server.	192.168.127.200

When finished, click **Save**.

Edit System Information

To edit the device's system information, click the **Edit** icon in the **System Information** widget.

Edit System Information

Device Name
wac-0090e8ff0002

Location- *optional*

Description- *optional*

Contact Information- *optional*

Cancel Save

Configure the following settings:

Device Name

Setting	Description	Factory Default
1 to 255 characters	Enter a name for the device.	[device type]-[MAC address]

Location - optional

Setting	Description	Factory Default
0 to 255 characters	Enter the location of the device.	None

Description - optional

Setting	Description	Factory Default
0 to 255 characters	Enter a description for the device. This helps identify the device more easily.	None

Contact Information - optional

Setting	Description	Factory Default
0 to 255 characters	Enter the contact information of the device's administrator.	None

When finished, click **Save**.

Network

The **Network** tab shows information about the current LAN status and routing table.

General **Network** Resource Usage Managed APs (5) Task Record Event Log

LAN Status

Data received on Jul 10, 2025 19:12:50

Ethernet Bonding : Enabled

Interface	Speed	Duplex Mode	TX Packets	RX Packets
✓ BRIDGE	--	--	1779505	1779345
✓ LAN 1	--	--	1779506	1779417

Route Table

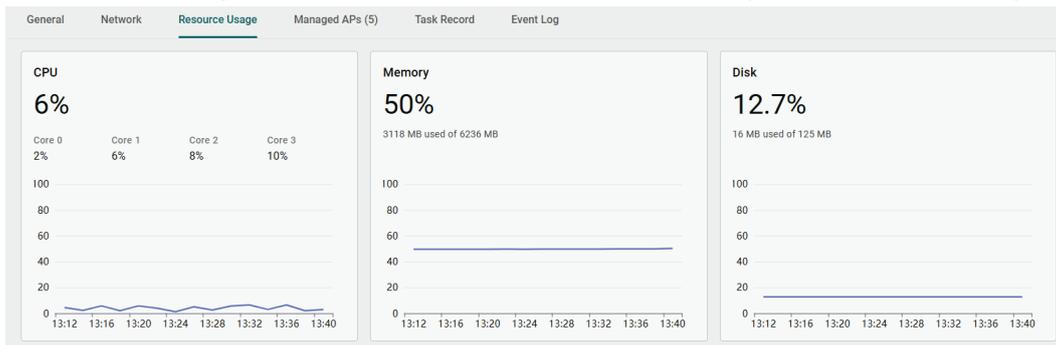
Data received on Jul 10, 2025 11:12:45

Destination	Netmask	Gateway	Interface	Metric
192.168.127.0	255.255.255.0	0.0.0.0	LAN	0

Items per page: 10 1 - 1 of 1 < >

Resource Usage

The **Resource Usage** tab shows the device's real-time CPU, memory, and disk resource usage.



Managed APs

The **Managed APs** tab shows information about the APs managed by this WAC device.

The Managed APs table displays a list of 5 managed APs, all of which are currently offline. The table includes columns for Device Name, Status, IP Address, Config Sync Status, Group, Roaming Profile, and Managing WAC.

<input type="checkbox"/>	Device Name	Status	IP Address	Config Sync Status	Group	Roaming Profile	Managing WAC
<input type="checkbox"/>	ap-0090e8100070	Offline	192.168.127.96	Modified View Details	Ungrouped	11111111	wac-0090e8ff0001 192.168.127.249
<input type="checkbox"/>	ap-0090e8100065	Offline	192.168.127.95	Modified View Details	Ungrouped	Leaky feeder-like coverage	wac-0090e8ff0001 192.168.127.249
<input type="checkbox"/>	ap-0090e8100031	Offline	192.168.127.94	Modified View Details	Ungrouped	11111111	wac-0090e8ff0001 192.168.127.249
<input type="checkbox"/>	ap-0090e88a87a8	Offline	192.168.127.93	Modified View Details	Ungrouped	Leaky feeder-like coverage	wac-0090e8ff0001 192.168.127.249
<input type="checkbox"/>	ap-0090e88a8794	Offline	192.168.127.92	Modified View Details	Ungrouped	Leaky feeder-like coverage	wac-0090e8ff0001 192.168.127.249

Add Managed AP

To add an unmanaged AP, click **Add Device**. Once added, the AP will be managed by this WAC.

The Add Managed AP dialog box shows the process of adding an AP to the WAC-0090e8ff0001. It includes an information message, a search bar, and a table of available APs.

Info: Roaming and tasks will be disabled on the AP while the device is being reassigned. This may take up to 5 minutes.

<input type="checkbox"/>	Device Name	Status	IP Address	Group	WAC
<input checked="" type="checkbox"/>	ap-0090e88a87d9	Inactive	--	Ungrouped	--

Check the box of the AP(s) you want to add.

When finished, click **Save**.

Task Record

The **Task Record** tab shows an overview of all completed and scheduled tasks for this WAC device.

General						Network	Resource Usage	Managed APs (5)	Task Record	Event Log
✓ Task Result		Scheduled Tasks								
						<input type="text"/> Search <input type="button" value="Export Record"/>				
<input type="checkbox"/>	Task	Status	Start Time	End Time	Duration (sec)					
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_1_2025_0707_142...	Completed	Jul 07, 2025 16:47:28	Jul 07, 2025 16:49:06	98	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_1_2025_0704_173...	Completed	Jul 07, 2025 12:31:26	Jul 07, 2025 12:33:04	98	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_1_2025_0627_172...	Completed	Jun 27, 2025 18:12:07	Jun 27, 2025 18:13:52	105	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_2025_0507_1401...	Completed	Jun 06, 2025 14:32:27	Jun 06, 2025 14:34:17	110	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_2025_0416_0114...	Completed	Apr 17, 2025 11:04:27	Apr 17, 2025 11:06:03	95	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_2025_0320_1638...	Completed	Mar 21, 2025 11:42:29	Mar 21, 2025 11:44:01	91	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_2025_0212_0228...	Completed	Feb 12, 2025 11:22:11	Feb 12, 2025 11:23:45	93	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_2025_0211_0229...	Completed	Feb 11, 2025 11:40:54	Feb 11, 2025 11:42:30	96	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_2025_0210_1619...	Completed	Feb 10, 2025 17:26:58	Feb 10, 2025 17:28:36	98	<input type="button" value="Info"/>				
<input type="checkbox"/>	Firmware upgrade FWR_WAC-M300_v1.0_2025_0210_0226...	Completed	Feb 10, 2025 11:15:49	Feb 10, 2025 11:17:24	95	<input type="button" value="Info"/>				
						Items per page: <input type="text" value="10"/> 1 - 10 of 45 <input type="button" value="Previous"/> <input type="button" value="Next"/>				

Event Log

The **Event Log** tab shows a list of event logs recorded on the device.

General						Network	Resource Usage	Managed APs (5)	Task Record	Event Log
Log Capacity Used <input type="text" value="50.1%"/>										
						<input type="text"/> Search <input type="button" value="Clear"/> <input type="button" value="Export"/>				
Severity	Group	Message				Timestamp				
Notice	Configuration	Configuration saved successfully. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 19:03:14				
Notice	Configuration	Device configuration was changed. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 19:03:14				
Notice	Configuration	Configuration saved successfully. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 19:01:12				
Notice	Configuration	Device configuration was changed. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 19:01:12				
Notice	Configuration	Configuration saved successfully. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 18:59:10				
Notice	Configuration	Device configuration was changed. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 18:59:10				
Notice	Configuration	Configuration saved successfully. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 18:51:39				
Notice	Configuration	Device configuration was changed. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 18:51:39				
Notice	Configuration	Configuration saved successfully. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 18:49:13				
Notice	Configuration	Device configuration was changed. (User: wcs, IP: 127.0.0.1, Interface: Console)				Jul 08, 2025 18:49:13				
						Items per page: <input type="text" value="10"/> 1 - 10 of 50134 <input type="button" value="Previous"/> <input type="button" value="Next"/>				

Access Points (AP)

Menu Path: Device Management > Access Points (AP)

From the **Access Points (AP)** page, you can view the status of tasks and manage AP devices.

Home > Access Points (AP)

Access Points (AP)

0 Scheduled 0 Canceled 0 In Progress 63 Completed 8 Failed [Task Status](#)

All Devices Unresolved Devices [Search](#) [Edit Columns](#) [+ Add Device](#)

<input type="checkbox"/>	Device Name	Status	IP Address	MAC Address	Firmware Version	Config Sync Status	Managing WAC	Group	Roaming Profile	Model Name
<input type="checkbox"/>	ap-0090e8100...	Offline	192.168.127.94	00-90:E8:10:00:31	v1.0 Build 2025_0...	Modified View Details	wac-0090e8ff00... 192.168.127.249	Ungrou...	11111111	TAP-M310
<input type="checkbox"/>	ap-0090e8100...	Offline	192.168.127.95	00-90:E8:10:00:65	v1.0 Build 2025_0...	Modified View Details	wac-0090e8ff00... 192.168.127.249	Ungrou...	Leaky feeder-like...	TAP-M310
<input type="checkbox"/>	ap-0090e8100...	Offline	192.168.127.96	00-90:E8:10:00:70	v1.0.1 Build 2025_...	Modified View Details	wac-0090e8ff00... 192.168.127.249	Ungrou...	11111111	TAP-M310
<input type="checkbox"/>	ap-0090e88a8...	Offline	192.168.127.92	00-90:E8:8A:87:94	v1.0 Build 2025_0...	Modified View Details	wac-0090e8ff00... 192.168.127.249	Ungrou...	Leaky feeder-like...	TAP-M310
<input type="checkbox"/>	ap-0090e88a8...	Offline	192.168.127.93	00-90:E8:8A:87:A8	v1.0 Build 2025_0...	Modified View Details	wac-0090e8ff00... 192.168.127.249	Ungrou...	Leaky feeder-like...	TAP-M310
<input type="checkbox"/>	ap-0090e88a8...	Inactive	--	00-90:E8:8A:87:D9	--	Modified View Details	-- !	Ungrou...	Leaky feeder-like...	--

Items per page: 10 1 - 6 of 6 << < > >>

Task Status

To view details about task results and a list of scheduled tasks for access points, click **Task Status**. Refer to [Task Status](#).

Home > AP > Task Status

Task Status

[Task Result](#) [Scheduled Tasks](#)

Exported configuration files can be downloaded [here](#).

[Search](#) [Export Record](#)

<input type="checkbox"/>	Device Name	Group	Task	Status	Start Time	End Time	Duration (sec)
<input type="checkbox"/>	ap-0090e8100070	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Failed Timed out.	Jul 07, 2025 12:31:13	Jul 07, 2025 12:36:13	300
<input type="checkbox"/>	ap-0090e8100070	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Completed	Jun 25, 2025 15:17:11	Jun 25, 2025 15:20:10	179
<input type="checkbox"/>	ap-0090e8100070	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Completed	Jun 23, 2025 17:11:17	Jun 23, 2025 17:14:17	180
<input type="checkbox"/>	ap-0090e8100070	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Completed	Jun 10, 2025 12:46:24	Jun 10, 2025 12:49:33	188
<input type="checkbox"/>	ap-0090e8100070	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Completed	Jun 06, 2025 14:46:52	Jun 06, 2025 14:50:09	197
<input type="checkbox"/>	ap-0090e8100070	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Completed	Mar 01, 2025 13:56:01	Mar 01, 2025 13:59:08	186
<input type="checkbox"/>	ap-0090e8100070	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Completed	Mar 01, 2025 13:29:03	Mar 01, 2025 13:32:08	185
<input type="checkbox"/>	ap-0090e8100031	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Completed	Mar 01, 2025 13:28:57	Mar 01, 2025 13:32:00	183
<input type="checkbox"/>	ap-0090e8100031	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310...	Failed Firmware is identical to current version.	Feb 23, 2025 18:05:16	Feb 23, 2025 18:05:28	12

Add an AP Device

Click **Add Device** in the device list to add an AP device.

Add Device

Method
Import CSV file

Import CSV File

You can add multiple devices at once by importing import a device list (in CSV format). Any conflicting settings for existing devices will be overwritten.

[Download Template](#)

CSV File
[Browse](#)

[Cancel](#) [Save](#)

Configure the following settings:

Method

Setting	Description	Factory Default
Import CSV file	Add one or multiple devices in bulk by importing the device information as a CSV file. Click Download Template to download an example file.	Import CSV file
Manually add device	Manually add a single device.	

CSV File (Import CSV File Only)

Setting	Description	Factory Default
CSV File	Click Browse and navigate to the CSV file on the local host.	None

MAC Address (Manually Add Device Only)

Setting	Description	Factory Default
MAC Address	Enter the MAC address of the device.	None

IP Address (Manually Add Device Only)

Setting	Description	Factory Default
IP Address	Enter the IP address of the device.	None

Device Name - optional (Manually Add Device Only)

Setting	Description	Factory Default
CSV File	Enter a name for the device.	None

Managing WAC IP - optional (Manually Add Device Only)

Setting	Description	Factory Default
IP Address	Enter the IP address of the WAC device managing this AP.	None

Group - optional (Manually Add Device Only)

Setting	Description	Factory Default
CSV File	Select the group to assign the device to.	None

When finished, click **Save**.

AP Device Page

Click the name of an access point in the Device Name column on the **Access Points (AP)** page to open the device details page. From this screen, you can view the current AP device status and device details, including general settings, resource usage, and event records. You can also perform several access point-related actions from this screen.

Home > Access Points (AP) > ap-0090e8100031
 < ap-0090e8100031

ap-0090e8100031 (192.168.127.94)
 Offline - Modified
 Last Came Online - Mar 24, 2025 14:40:21
 Managed by - wac0209e8100031 (192.168.127.249)
 Roaming Profile - 11111111
 Group - Ungrouped

General | WiFi | Network | Resource Usage | Task Record | Event Log

Device Information		IP Settings	
Data received on Mar 24, 2025 14:38:56		IP Address 192.168.127.94	
Model Name	TAP-M310R-LIN	Subnet Mask	255.255.255.0
MAC Address	00:90:EB:10:00:31	Gateway	-
System Uptime	25 days, 00:56:01	Primary DNS Server	-
Firmware Version	v1.0 Build 2025_0227_0011	Secondary DNS Server	-
Bootloader Version	v1.0 Build 2024_0627_1513		
Country	XX		
Serial Number	-		

System Information	
Device Name	ap-0090e8100031
Description	-
Location	-
Contact Information	-

Command Actions

The **Action** menu allows you to perform several actions. Available actions depend on the access point's status and configuration.

Action ▾

- Import/Export Config ▸
- Upgrade Firmware
- Reboot
- Reset to Factory Defaults
- Assign Roaming Profile
- Assign Managing WAC
- Group Device ▸
- Delete Device

Import/Export Config

Import Configuration

Click **Import** to upload a configuration file to the access point.



NOTE

The access point's network settings are managed by the main WAC. Importing a configuration file will not override these settings.

Import Configuration

Execution Time
Scheduled

Date Jul 14, 2025  Hour 9 Minute 30

File Location
Local

Local

The device's network settings are managed by the main WAC and will not be changed when importing a configuration.

Configuration File
 **Browse**

File Password
Use the default file passphrase

Skip registration
Skipping registration will preserve the device's current connection settings to the main WAC, including the registration key and the main WAC IP.

Skip wireless configuration

Cancel Save

Configure the following settings:

Execution Time

Setting	Description	Factory Default
Immediate	Import the configuration immediately.	Immediate
Scheduled	Import the configuration at the specified date and time. A scheduled task will be created and added to the Scheduled Task list. Refer to Scheduled Tasks .	

Date and Time (scheduled Only)

Setting	Description	Factory Default
Date, Hour, Minute	Specify the date, hour, and minute to execute the scheduled task. The Minute value can only be set as 30-minute intervals (00, 30).	Based on current device date and time

File Location

Setting	Description	Factory Default
Local	Import the configuration file from the local storage.	Local
TFTP	Import the configuration file from a TFTP server.	
SFTP	Import the configuration file from an SFTP server.	

Configuration File (Local Only)

Setting	Description	Factory Default
Configuration file	Click Browse and navigate to the configuration file on the local host.	None

Server IP Address (TFTP and SFTP Only)

Setting	Description	Factory Default
IP Address	Enter the IP address of the TFTP or SFTP server.	None

Account (SFTP Only)

Setting	Description	Factory Default
8 to 255 characters	Enter the account name of the SFTP server.	None

Password (SFTP Only)

Setting	Description	Factory Default
Account	Enter the account name of the SFTP server.	None

Filename

Setting	Description	Factory Default
Filename	Enter the name of the configuration file to import from the TFTP or SFTP server.	Filename

File Password

Setting	Description	Factory Default
Use the default file passphrase	Use the file encryption password configured in the File Passphrase section as the default password. Refer to File Passphrase .	Use the default file passphrase
Custom	Specify a custom file encryption password.	

Password (Custom Only)

Setting	Description	Factory Default
8 to 127 characters	Enter the file encryption password.	None

Skip registration

Setting	Description	Factory Default
Checkbox	If checked, this will maintain the AP's original connection settings to the main WAC. If unchecked, the device will need to be registered to the main WAC again after importing the configuration.	Checked

Skip wireless configuration

Setting	Description	Factory Default
Checkbox	If checked, this will maintain the device's original wireless configuration settings. If unchecked, the wireless settings will need to be reconfigured.	Checked

When finished, click **Save**.

Export Configuration

Click **Export** to export the access point's configuration settings.

Export Configuration

If the file destination is 'Local', the exported file can be downloaded from the Task Status page.

Execution Time
Scheduled

Date: Jul 14, 2025 | Hour: 9 | Minute: 30

Filename Prefix - optional

File Password
Use the default file passphrase

File Destination
Local

Cancel Save

Configure the following settings:

Execution Time

Setting	Description	Factory Default
Immediate	Export the configuration immediately.	Immediate
Scheduled	Export the configuration at the specified date and time. A scheduled task will be created and added to the Scheduled Task list. Refer to Scheduled Tasks .	

Date and Time (scheduled Only)

Setting	Description	Factory Default
Date, Hour, Minute	Specify the date, hour, and minute to execute the scheduled task. The Minute value can only be set as 30-minute intervals (00, 30).	Based on current device date and time

Filename Prefix - optional

Setting	Description	Factory Default
1 to 64 characters	Enter a prefix for the exported configuration filename.	None

File Password

Setting	Description	Factory Default
Use the default file passphrase	Use the file encryption password configured in the File Passphrase section as the default password. Refer to File Passphrase .	Use the default file passphrase
Custom	Specify a custom file encryption password.	

Password (Custom Only)

Setting	Description	Factory Default
8 to 127 characters	Enter the file encryption password.	None

File Location

Setting	Description	Factory Default
Local	Export the configuration file to the local storage.	Local
TFTP	Export the configuration file to a TFTP server.	
SFTP	Export the configuration file to an SFTP server.	

Server IP Address (TFTP and SFTP Only)

Setting	Description	Factory Default
IP Address	Enter the IP address of the TFTP or SFTP server.	None

Account (SFTP Only)

Setting	Description	Factory Default
8 to 255 characters	Enter the account name of the SFTP server.	None

Password (SFTP Only)

Setting	Description	Factory Default
Account	Enter the account name of the SFTP server.	None

When finished, click **Save**.

Upgrade Firmware

Click **Upgrade Firmware** in the **Action** menu to upgrade the AP's firmware.

This process is the same as for WAC devices. Refer to [Upgrade Firmware](#).

Reboot

Click **Reboot** in the **Action** menu to restart the device.

This process is the same as for WAC devices. Refer to [Reboot Device](#).

Reset to Factory Defaults

Click **Reset to Factory Defaults** in the **Action** menu to reset the AP's configuration to the factory default settings. Depending on the selected options, certain types of data can be kept.

This process is the same as for WAC devices. Refer to [Reset to Factory Defaults](#).

Assign Roaming Profile

Click **Assign Roaming Profile** to assign a pre-configured roaming profile to the access point. The roaming behavior of the access point will be determined by the parameters configured in the associated roaming profile.



NOTE

If the default "Leaky feeder-like coverage" and "Open air radiating antennas" profiles do not meet your requirements, you can create a custom roaming profile. Refer to [Roaming Profile](#).

Assign Roaming Profile

If no profile exists that meets your requirements, you can create a new profile or modify the settings of an existing profile in the [Roaming Settings](#).

Reassigning: 1 AP(s)

Warning
Changes will automatically sync to offline devices when the devices come online.

- Leaky feeder-like coverage >
- Open air radiating antennas >
- 11111111 >

[Cancel](#) [Save](#)

Configure the following settings:

Roaming Profile

Setting	Description	Factory Default
Roaming Profile	Select the roaming profile to assign to the device.	None

When finished, click **Save**.

Assign Managing WAC

Click **Assign Managing WAC** to assign the AP to a managing WAC device. If assigned, the AP's configuration will be managed by the corresponding WAC device.



WARNING

Assigning the access point to a managing WAC device will temporarily disable roaming and all tasks on the access point while the device is being assigned. To avoid interruptions, make sure the device is not required for operations when performing this action.

Device Name	IP Address	No. of APs
<input checked="" type="radio"/> wac-0090e8ff0003	192.168.127.247	0
<input type="radio"/> wac-0090e8ff0001	192.168.127.249	0

Configure the following settings:

Managing WAC

Setting	Description	Factory Default
WAC device	Select the managing WAC device to assign the AP to.	None

When finished, click **Save**.

Group Device

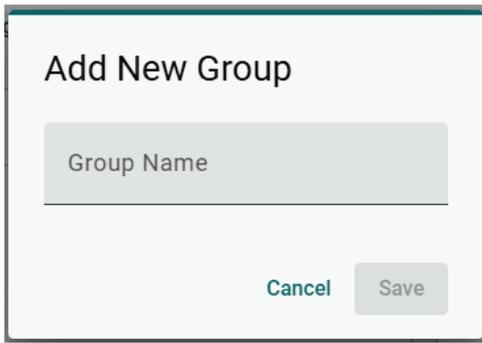
Click **Group Device** to add the access point to a device group. Devices are ungrouped by default.

Group Name

Ungrouped

Enter the partial or full name of the group in the search bar. Click the group name to add the device to the group.

If the group does not exist, click **Add Group**.



The dialog box is titled "Add New Group". It features a text input field labeled "Group Name". At the bottom right, there are two buttons: "Cancel" and "Save".

Configure the following settings:

Group Name

Setting	Description	Factory Default
1 to 32 characters	Enter a name for the group.	None

When finished, click **Save**.

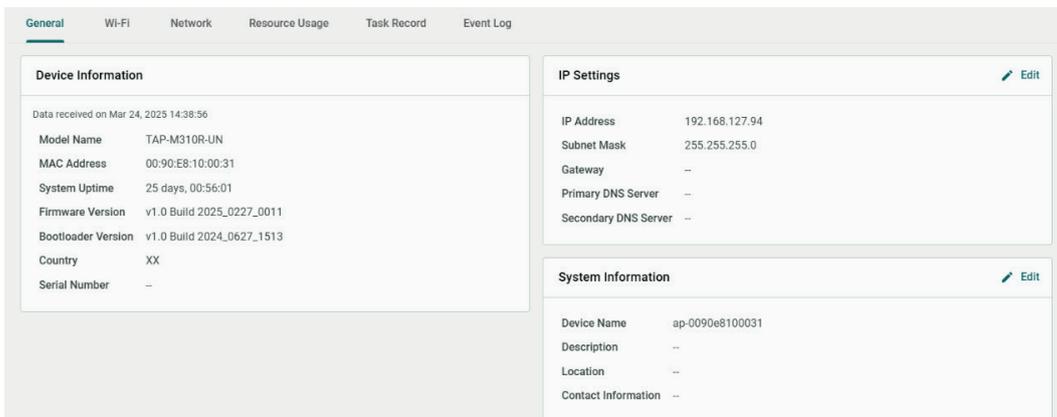
Delete Device

Click **Delete Device** in the **Action** menu to delete the AP. This will delete all relevant device information from the WLAN system and tasks can no longer be assigned to the AP.

When prompted, click **Delete**.

General

The **General** tab contains general information about the access point, including IP settings, device, and system information.



The screenshot shows the "General" tab of a configuration interface. It has a navigation bar with tabs: General, Wi-Fi, Network, Resource Usage, Task Record, and Event Log. The main content area is divided into two columns. The left column is titled "Device Information" and contains a table with the following data:

Data received on Mar 24, 2025 14:38:56	
Model Name	TAP-M310R-UN
MAC Address	00:90:E8:10:00:31
System Uptime	25 days, 00:56:01
Firmware Version	v1.0 Build 2025_0227_0011
Bootloader Version	v1.0 Build 2024_0627_1513
Country	XX
Serial Number	--

The right column contains two sections: "IP Settings" and "System Information", each with an "Edit" icon. The "IP Settings" section contains:

IP Address	192.168.127.94
Subnet Mask	255.255.255.0
Gateway	--
Primary DNS Server	--
Secondary DNS Server	--

The "System Information" section contains:

Device Name	ap-0090e8100031
Description	--
Location	--
Contact Information	--

Edit IP Settings

To edit the device's IP settings, click the **Edit** icon in the **IP Settings** widget.

For a description of each setting, refer to [Edit IP Settings](#).

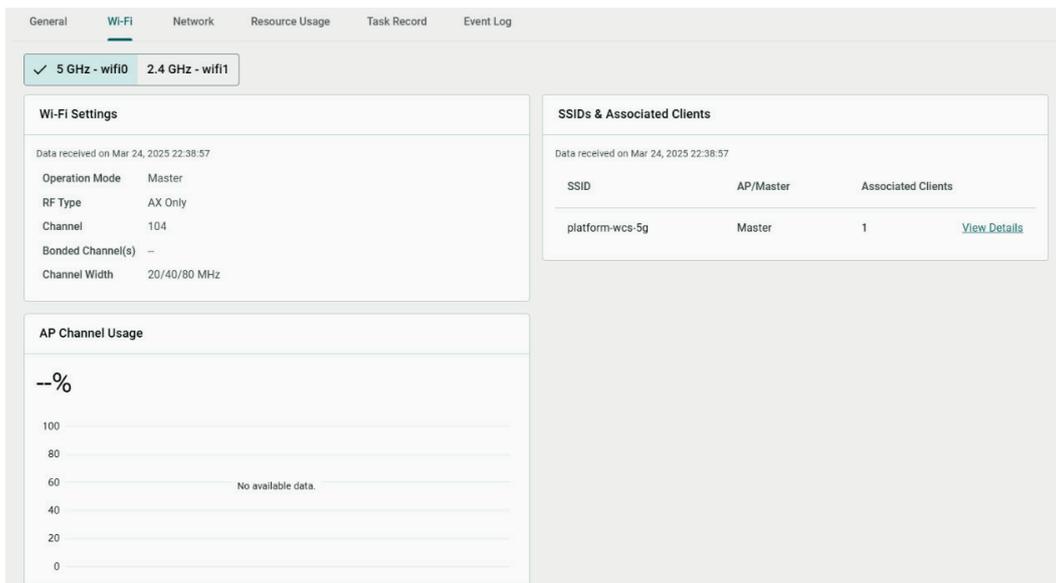
Edit System Information

To edit the device's system information, click the **Edit** icon in the **System Information** widget.

For a description of each setting, refer to [Edit System Information](#).

Wi-Fi

The **Wi-Fi** tab shows information about the Wi-Fi configuration settings, channel usage, and configured SSIDs. Click the 5 GHz or 2.4 GHz tab to view relevant information for the corresponding wireless band.



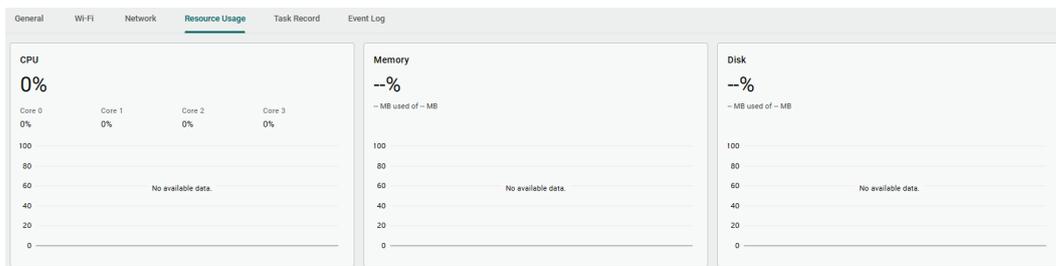
Network

The **Network** tab shows information about the routing table.

Destination	Netmask	Gateway	Interface	Metric
192.168.127.0	255.255.255.0	0.0.0.0	LAN	0

Resource Usage

The **Resource Usage** tab shows the device's real-time CPU, memory, and disk resource usage.



Task Record

The **Task Record** tab shows an overview of all completed and scheduled tasks for this access point.

Task Record					
Task	Status	Start Time	End Time	Duration (sec)	
Firmware upgrade FWL_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SF...	Completed	Mar 01, 2025 13:28:57	Mar 01, 2025 13:32:00	183	
Firmware upgrade FWL_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SF...	Failed Firmware is identical to current version.	Feb 23, 2025 18:05:16	Feb 23, 2025 18:05:28	12	
Configuration export CFS_TAP-M310R-UN_192.168.127.34_20250223174...	Completed	Feb 23, 2025 17:47:24	Feb 23, 2025 17:47:27	2	
Firmware upgrade FWL_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SF...	Completed	Feb 23, 2025 15:58:44	Feb 23, 2025 16:01:55	190	
Firmware upgrade FWL_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SF...	Completed	Feb 12, 2025 11:20:50	Feb 12, 2025 11:24:00	190	
Firmware upgrade FWL_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SF...	Completed	Feb 11, 2025 11:40:01	Feb 11, 2025 11:43:14	192	
Reboot	Completed	Feb 10, 2025 15:37:45	Feb 10, 2025 15:39:18	93	
Reboot	Completed	Feb 10, 2025 11:59:44	Feb 10, 2025 12:01:19	94	
Reboot	Completed	Feb 10, 2025 11:19:31	Feb 10, 2025 11:21:05	93	
Firmware upgrade FWL_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SF...	Completed	Feb 10, 2025 11:01:25	Feb 10, 2025 11:06:41	315	

Event Log

The **Event Log** tab shows a list of event logs recorded on the device.

Event Log			
Severity	Group	Message	Timestamp
Notice	Configuration	Configuration saved successfully. (User: admin, IP: 192.168.127.200, Interface: HTTPS)	Mar 24, 2025 14:42:39
Notice	Configuration	Device configuration was changed. (User: admin, IP: 192.168.127.200, Interface: HTTPS)	Mar 24, 2025 14:42:39
Notice	Configuration	Configuration saved successfully. (User: admin, IP: 192.168.127.200, Interface: HTTPS)	Mar 24, 2025 14:42:33
Notice	Configuration	Device configuration was changed. (User: admin, IP: 192.168.127.200, Interface: HTTPS)	Mar 24, 2025 14:42:33
Notice	Configuration	Configuration saved successfully. (User: wcs, IP: 192.168.127.239, Interface: Console)	Mar 24, 2025 14:41:16
Notice	Configuration	Device configuration was changed. (User: wcs, IP: 192.168.127.239, Interface: Console)	Mar 24, 2025 14:41:16
Notice	Configuration	Configuration saved successfully. (User: wcs, IP: 192.168.127.239, Interface: Console)	Mar 24, 2025 14:41:13
Notice	Configuration	Device configuration was changed. (User: wcs, IP: 192.168.127.239, Interface: Console)	Mar 24, 2025 14:41:13
Notice	Configuration	Configuration saved successfully. (User: wcs, IP: 192.168.127.239, Interface: Console)	Mar 24, 2025 14:41:09
Notice	Configuration	Device configuration was changed. (User: wcs, IP: 192.168.127.239, Interface: Console)	Mar 24, 2025 14:41:09

Clients (STA)

Menu Path: Device Management > Clients (STA)

From the **Clients (STA)** page, you can view the status of tasks and manage client devices.

Clients (STA)									
0 Scheduled		0 Canceled		0 In Progress		21 Completed		10 Failed	
Device Name	Status	IP Address	MAC Address	Firmware Version	Config Sync Status	SSID	Group	Model Name	
sta-0090e8100071	Offline	192.168.127.83	00:90:E8:10:00:71	v1.0 Build 2025_022...	Modified View Details	platform-wcs-5g	Ungroup...	TAP-M310R-UN	
sta-0090e88a8784	Offline	192.168.127.82	00:90:E8:8A:87:84	v1.0 Build 2025_012...	Modified View Details	--	Ungroup...	TAP-M310R-UN	
sta-0090e88a87da	Offline	192.168.127.81	00:90:E8:8A:87:DA	v1.0 Build 2025_020...	Modified View Details	platform-wcs-5g	Ungroup...	TAP-M310R-UN	

Task Status

To view details about task results and a list of scheduled tasks for clients, click **Task Status**. Refer to [Task Status](#).

Home > STA > Task Status

← Task Status

Task Result Scheduled Tasks

Exported configuration files can be downloaded [here](#).

Search Export Record

<input type="checkbox"/>	Device Name	Group	Task	Status	Start Time	End Time	Duration (sec)
<input type="checkbox"/>	sta-0090e8100071	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310R...	Completed	Feb 23, 2025 15:56:45	Feb 23, 2025 16:01:00	255
<input type="checkbox"/>	sta-0090e8100071	Ungrouped	Reboot	Completed	Feb 19, 2025 18:04:35	Feb 19, 2025 18:06:04	89
<input type="checkbox"/>	sta-0090e8100071	Ungrouped	Reboot	Completed	Feb 19, 2025 17:21:16	Feb 19, 2025 17:22:45	89
<input type="checkbox"/>	sta-0090e8100071	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310R...	Failed Timed out.	Feb 12, 2025 11:20:01	Feb 12, 2025 11:25:01	300
<input type="checkbox"/>	sta-0090e8100071	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310R...	Failed Timed out.	Feb 10, 2025 11:00:09	Feb 10, 2025 11:05:09	300
<input type="checkbox"/>	sta-0090e8100071	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310R...	Completed	Feb 06, 2025 16:40:05	Feb 06, 2025 16:43:01	176
<input type="checkbox"/>	sta-0090e88a87da	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310R...	Completed	Feb 04, 2025 10:37:46	Feb 04, 2025 10:42:17	270
<input type="checkbox"/>	sta-0090e88a87da	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310R...	Completed	Jan 21, 2025 10:28:49	Jan 21, 2025 10:33:39	290
<input type="checkbox"/>	sta-0090e88a87da	Ungrouped	Firmware upgrade FWR_TAP-M310R_TAP-M310R...	Completed	Jan 20, 2025 10:27:12	Jan 20, 2025 10:30:13	180

Add a Client Device

Click **Add Device** in the device list to add a client device.

Add Device

Method

Import CSV file

Import CSV File

You can add multiple devices at once by importing import a device list (in CSV format). Any conflicting settings for existing devices will be overwritten.

[Download Template](#)

CSV File

[Cancel](#)

Configure the following settings:

Method

Setting	Description	Factory Default
Import CSV file	Add one or multiple devices in bulk by importing the device information as a CSV file. Click Download Template to download an example file.	Import CSV file
Manually add device	Manually add a single device.	

CSV File (Import CSV File Only)

Setting	Description	Factory Default
CSV File	Click Browse and navigate to the CSV file on the local host.	None

MAC Address (Manually Add Device Only)

Setting	Description	Factory Default
MAC Address	Enter the MAC address of the device.	None

IP Address (Manually Add Device Only)

Setting	Description	Factory Default
IP Address	Enter the IP address of the device.	None

Device Name - optional (Manually Add Device Only)

Setting	Description	Factory Default
CSV File	Enter a name for the device.	None

Group - optional (Manually Add Device Only)

Setting	Description	Factory Default
CSV File	Select a group to assign the device to.	None

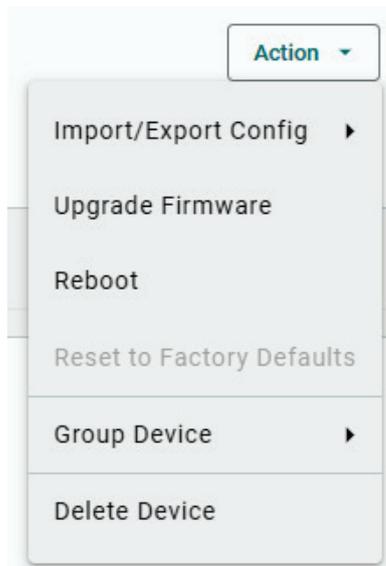
When finished, click **Save**.

Client Device Page

Click the name of a client device in the Device Name column on the **Clients (STA)** page to open the device details page. From this screen, you can view the current client device status and device details including general settings, resource usage, and event records. You can also perform several client-related actions from this screen.

Command Actions

The **Action** menu allows you to perform several actions. Available actions depend on the client's status and configuration.



Import/Export Config

Import Configuration

Click **Import** to upload a configuration file to the client.

For a description of each setting, refer to [Import Configuration](#).

Export Configuration

Click **Export** to export the client's configuration settings.

For a description of each setting, refer to [Export Configuration](#).

Upgrade Firmware

Click **Upgrade Firmware** in the **Action** menu to upgrade the client's firmware.

This process is the same as for WAC devices. Refer to [Upgrade Firmware](#).

Reboot

Click **Reboot** in the **Action** menu to restart the device.

This process is the same as for WAC devices. Refer to [Reboot Device](#).

Reset to Factory Defaults

Click **Reset to Factory Defaults** in the **Action** menu to reset the client's configuration to the factory default settings. Depending on the selected options, certain types of data can be kept.

This process is the same as for WAC devices. Refer to [Reset to Factory Defaults](#).

Group Device

Click **Group Device** to add the client to a device group. Devices are ungrouped by default.

This process is the same as for AP devices. Refer to [Group Device](#).

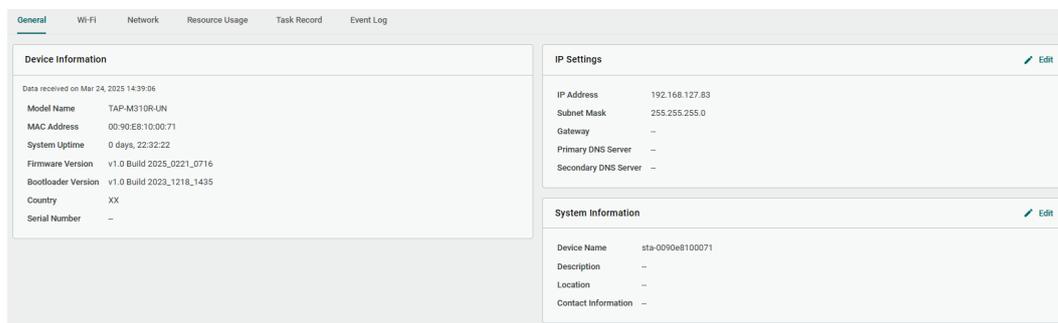
Delete Device

Click **Delete Device** in the **Action** menu to delete the client. This will delete all relevant device information from the WLAN system and tasks can no longer be assigned to the AP.

When prompted, click **Delete**.

General

The **General** tab contains general information about the client, including IP settings, device, and system information.



Edit IP Settings

To edit the device's IP settings, click the **Edit** icon in the **IP Settings** widget.

For a description of each setting, refer to [Edit IP Settings](#).

Edit System Information

To edit the device's system information, click the **Edit** icon in the **System Information** widget.

For a description of each setting, refer to [Edit System Information](#).

Wi-Fi

The **Wi-Fi** tab shows information about the Wi-Fi configuration settings and the connection to the AP it's currently associated with.

General **Wi-Fi** Network Resource Usage Task Record Event Log

Wi-Fi Status

Data received on Mar 24, 2025 22:39:06

Operation Mode Slave

Connected to [ap-0090e8100031](#) (192.168.127.94)
BSSID: 46:90:E8:10:00:31

SNR 46 dB

Noise Floor -89 dBm

RF Band 5 GHz

RF Type (5 GHz) A/N/AC/AX Mixed

Channel 104

Bonded Channel(s) --

Channel Width 20/40/80 MHz

SSID platform-wcs-5g

▼ **Show Connection Details**

Connection Duration 0 days, 00:01:15

AP Supports VHT Yes

Transmission Rate 864.7 Mbps

Mgmt Signal Strength -43 dBm

TX Management Packets 442

RX Management Packets 657

TX Data Packets 8182

RX Data Packets 4224

Network

The **Network** tab shows information about the routing table.

General Wi-Fi **Network** Resource Usage Task Record Event Log

Route Table

Data received on Mar 24, 2025 14:38:56

Destination	Netmask	Gateway	Interface	Metric
192.168.127.0	255.255.255.0	0.0.0.0	LAN	0

Items per page: 10 1 - 1 of 1 << < > >>

Resource Usage

The **Resource Usage** tab shows the device's real-time CPU, memory, and disk resource usage.

General Wi-Fi Network **Resource Usage** Task Record Event Log

CPU

0%

Core 0 0% Core 1 0% Core 2 0% Core 3 0%

No available data.

Memory

--%

-- MB used of -- MB

No available data.

Disk

--%

-- MB used of -- MB

No available data.

Task Record

The **Task Record** tab shows an overview of all completed and scheduled tasks for this access point.

Task	Status	Start Time	End Time	Duration (sec)
Firmware upgrade FWR_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SFP_v1.0...	Completed	Feb 23, 2025 15:56:45	Feb 23, 2025 16:01:00	255
Reboot	Completed	Feb 19, 2025 18:04:35	Feb 19, 2025 18:06:04	89
Reboot	Completed	Feb 19, 2025 17:21:16	Feb 19, 2025 17:22:45	89
Firmware upgrade FWR_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SFP_v1.0...	Failed Timed out.	Feb 12, 2025 11:20:01	Feb 12, 2025 11:25:01	300
Firmware upgrade FWR_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SFP_v1.0...	Failed Timed out.	Feb 10, 2025 11:00:09	Feb 10, 2025 11:05:09	300
Firmware upgrade FWR_TAP-M310R_TAP-M310R-NPS_TAP-M310R-SFP_v1.0...	Completed	Feb 06, 2025 16:40:05	Feb 06, 2025 16:43:01	176

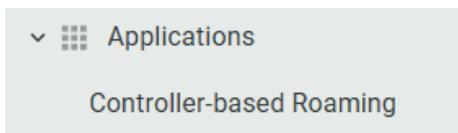
Event Log

The **Event Log** tab shows a list of event logs recorded on the device.

Severity	Group	Message	Timestamp
Notice	Configuration	Configuration saved successfully. (User: admin, IP: 192.168.127.200, Interface: HTTPS)	Mar 24, 2025 14:43:56
Notice	Configuration	Device configuration was changed. (User: admin, IP: 192.168.127.200, Interface: HTTPS)	Mar 24, 2025 14:43:56
Notice	Configuration	Configuration saved successfully. (User: admin, IP: 192.168.127.200, Interface: HTTPS)	Mar 24, 2025 14:43:50
Notice	Configuration	Device configuration was changed. (User: admin, IP: 192.168.127.200, Interface: HTTPS)	Mar 24, 2025 14:43:50
Warning	Wi-Fi	The STA (00:90:e8:10:00:71) detects a connection warning with the AP (46:90:E8:10:00:31).	Mar 21, 2025 02:27:49
Warning	Wi-Fi	The STA (00:90:e8:10:00:71) detects a connection warning with the AP (46:90:E8:10:00:31).	Mar 21, 2025 02:27:48
Warning	Wi-Fi	The STA (00:90:e8:10:00:71) detects a connection warning with the AP (46:90:E8:10:00:31).	Mar 21, 2025 02:27:48
Warning	Wi-Fi	The STA (00:90:e8:10:00:71) detects a connection warning with the AP (46:90:E8:10:00:31).	Mar 21, 2025 02:27:46
Warning	Wi-Fi	The STA (00:90:e8:10:00:71) detects a connection warning with the AP (46:90:E8:10:00:31).	Mar 21, 2025 02:27:46
Warning	Wi-Fi	The STA (00:90:e8:10:00:71) detects a connection warning with the AP (46:90:E8:10:00:31).	Mar 21, 2025 02:27:45

Applications

From the **Applications** section, you can configure **Controller-based Roaming**.



Controller-based Roaming

Menu Path: Wi-Fi > Controller-based Roaming

The WAC-M300 Series leverages Moxa's controller-based Turbo Roaming technology to enable clients to roam seamlessly between access points with millisecond-level handover times. The advanced roaming algorithm and customizable roaming profiles allow wireless stations (STAs) to move between APs while upholding stringent security requirements in demanding environments.

The **Controller-based Roaming** page is used to configure the controller-based roaming behavior, roaming profiles, the stable interval, and WAC proxy settings.

Roaming Profile

The **Roaming Profile** tab is used to manage roaming profiles. When assigned to APs, clients will roam to and from the AP based on the thresholds configured in the associated roaming profile. A roaming profile will determine the roaming conditions for both clients and access points. Each profile can be customized according to the roaming requirements for the device or application.



NOTE

The "Leaky feeder-like coverage" and "Open air radiating antennas" profiles are default profiles and cannot be modified or deleted.

Click the **Roaming Profile** tab to access this screen.

Home > Controller-based Roaming

Controller-based Roaming

Roaming Profile Stable Interval WAC Proxy

The "Leaky feeder-like coverage" profile has the highest priority. Clients (STA) will prioritize connections to APs associated with this profile.

[Add Profile](#)

Profile Name	Client Broadcast Threshold (dBm)	Roaming Threshold (dBm)	Roaming Difference (dB)	Roaming Link Quality (dB)	STA Monitoring Threshold	No. of Associated AP	
> Leaky feeder-like coverage	-70	-75	0	30	10	4	⋮
> Open air radiating antennas	-55	-55	10	20	10	0	⋮
> 11111111	-55	-55	0	30	10	2	⋮

Create a New Roaming Profile

To add a new roaming profile, click **Add Profile**.

Create Roaming Profile

1 Roaming Threshold Settings 2 Connection Check Settings 3 AP Selection Optional 4 Confirm

Profile Name

Client Broadcast Threshold (dBm)
-70

Roaming Threshold (dBm)
-75

Roaming Difference (dB)
0

Roaming Link Quality (dB)
30

STA Monitoring Threshold
10

Cancel Next >

Configure the following settings:

Profile Name

Setting	Description	Factory Default
8 to 255 characters	Enter a name for the profile.	None

Client Broadcast Threshold

Setting	Description	Factory Default
-100 to -35 (dBm)	Specify the client broadcast threshold value. When the signal strength of the connection from the client to the current associated AP falls below this threshold, it will periodically send out Action frames to nearby APs.	-70

Roaming Threshold

Setting	Description	Factory Default
-100 to -35 (dBm)	Specify the roaming threshold value. When the signal strength of the current AP and client are below this threshold, the client will roam to a stronger-signal AP.	-75

Roaming Difference

Setting	Description	Factory Default
0 to 35 (dB)	Specify the threshold for the RSSI difference between the current AP and the monitored AP. If the monitored AP exceeds the Roaming Difference and Roaming Link Quality values, it will be considered a candidate AP suitable for roaming.	0

Roaming Link Quality

Setting	Description	Factory Default
0 to 70 (dB)	Specify the threshold for the link quality (signal strength - background noise) between the client and the monitored AP. If the monitored AP exceeds the Roaming Difference and Roaming Link Quality values, it will be considered a candidate AP suitable for roaming.	30

STA Monitoring Threshold

Setting	Description	Factory Default
0 to 70	Specify the link quality threshold (signal strength - background noise) for identifying a monitored AP. When an AP receives an Action frame from a client, and its link quality exceeds this threshold, the WAC will acknowledge this AP as a monitored AP for the client. When all conditions are met, the monitored AP will be designated as a candidate AP for the client.	10

When finished, click **Next**.

Configure the following settings:

Connection Check Interval

Setting	Description	Factory Default
50 to 1000 (ms)	Specify the interval (in ms) the system will check the client-AP connection status.	100

Missed Packet Count

Setting	Description	Factory Default
3 to 50	Specify the number of consecutive missed packets to count before the system determines the presence of interference.	10

Payload Data Size

Setting	Description	Factory Default
200 to 1000 (byte)	Specify the size of data packets sent during connection alive checks.	200

When finished, click **Next**.

Create Roaming Profile

Roaming Threshold Settings ✓ Connection Check Settings ✓ AP Selection Optional 4 Confirm

Select the AP(s) to apply this profile to. You can skip this step and apply a profile to APs from the AP device configuration page (Device Management > AP).

Device Name	IP Address	MAC Address	Group	Roaming Profile
ap-0090e8100070	192.168.127.96	00:90:E8:10:00:70	Ungrouped	11111111
ap-0090e8100065	192.168.127.95	00:90:E8:10:00:65	Ungrouped	Leaky feeder-like coverage
ap-0090e8100031	192.168.127.94	00:90:E8:10:00:31	Ungrouped	11111111
ap-0090e88a87a8	192.168.127.93	00:90:E8:8A:87:A8	Ungrouped	Leaky feeder-like coverage
ap-0090e88a87d9	--	00:90:E8:8A:87:D9	Ungrouped	Leaky feeder-like coverage
ap-0090e88a8794	192.168.127.92	00:90:E8:8A:87:94	Ungrouped	Leaky feeder-like coverage

< Back Cancel Next >

Select the AP(s) to apply the roaming profile to. This step is optional. You can assign a roaming profile to APs at any time from the **Device Management > AP** page. Refer to [Assign Roaming Profile](#).

When finished, click **Next**.

Create Roaming Profile

Roaming Threshold Settings ✓ Connection Check Settings ✓ AP Selection Optional ✓ Confirm

Confirm the profile settings and click Save to create the profile. Once created, you can edit the profile at any time from the profile list.

Profile Name : testtest
No. of Applied APs : 0

- > Roaming Threshold Settings
- > Connection Check Settings

< Back Cancel Save

Confirm the roaming profile settings.

When finished, click **Save**.

Edit a Roaming Profile

Click the **menu** (☰) icon next to the profile you want to modify and click **Edit**.

For configuration settings, refer to [Create a New Roaming Profile](#).

When finished, click **Save**.

Delete a Roaming Profile



NOTE

The "Leaky feeder-like coverage" and "Open air radiating antennas" profiles are default profiles and cannot be modified or deleted.

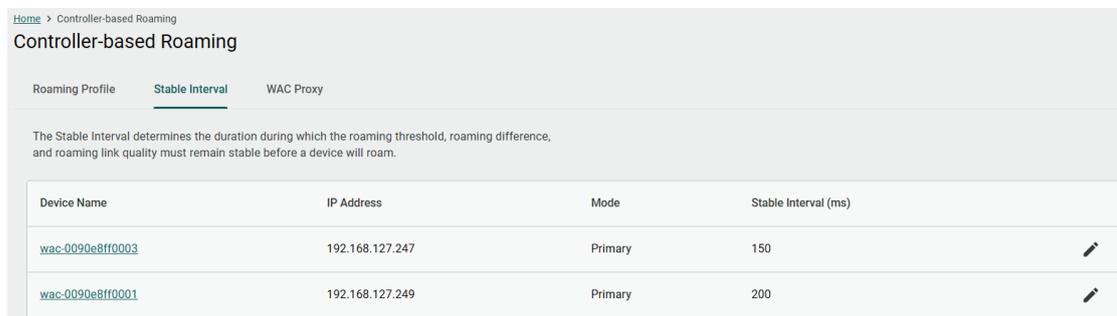
Click the **menu** () icon next to the profile you want to delete and click **Delete**.

When prompted to confirm, click **Delete**.

Stable Interval

The **Stable Interval** tab is used to manage stable interval parameters for roaming. The stable interval defines the period, measured in milliseconds, during which a STA will not attempt to roam again after associating with a new AP.

Click the **Stable Interval** tab to access this screen.



Home > Controller-based Roaming

Controller-based Roaming

Roaming Profile **Stable Interval** WAC Proxy

The Stable Interval determines the duration during which the roaming threshold, roaming difference, and roaming link quality must remain stable before a device will roam.

Device Name	IP Address	Mode	Stable Interval (ms)	
wac-0090e8ff0003	192.168.127.247	Primary	150	
wac-0090e8ff0001	192.168.127.249	Primary	200	

Edit the Stable Interval

Click the **Edit** () icon next to the device you want to modify the stable interval for.

Configure the following settings:

Stable Interval

Setting	Description	Factory Default
150 to 500	Specify the stable interval (in ms).	150

WAC Proxy

The **WAC Proxy** page is used to enable device authentication and configure RADIUS server settings.

Click the **WAC Proxy** tab to access this page.

Controller-based Roaming

Roaming Profile Stable Interval **WAC Proxy**

Enable WAC Proxy

Shared Key
 

RADIUS Server 1  Delete

Server Address UDP Port
1812

Shared Key 

RADIUS Server 2  Delete

Server Address UDP Port
1812

Shared Key 

Configure the following settings:

Enable WAC Proxy

Setting	Description	Factory Default
Checkbox	Check to enable or disable WAC proxy functionality.	Disabled

If enabled, also configure the following settings:

Shared Key

Setting	Description	Factory Default
Max. 128 characters	Specify the shared key which is used for encryption and to authenticate the device with the RADIUS server.	None

Server Address (RADIUS Server 1/2)

Setting	Description	Factory Default
IP address	Specify the IP address of the RADIUS server.	None

UDP Port (RADIUS Server 1/2)

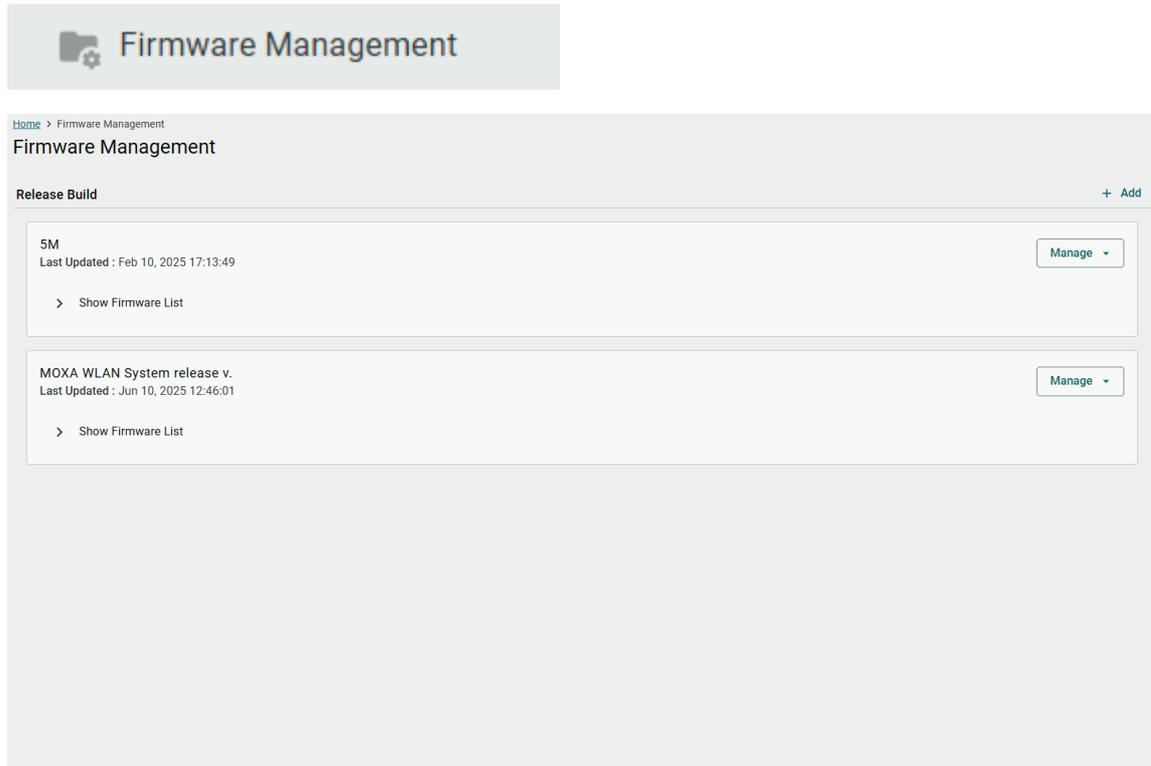
Setting	Description	Factory Default
1 to 65535	Specify the UDP port of the RADIUS server.	1812

When finished, click **Save**.

Firmware Management

Menu Path: Firmware Management

The **Firmware Management** page allows you to create new release builds, upload firmware files, and select compatible device models.



Add a New Release Build

To create a new release build, click **Add**.

Configure the following settings:

Release Build Name

Setting	Description	Factory Default
1 to 255 characters	Enter a name for the release build.	MOXA WLAN System release v.

Model

Setting	Description	Factory Default
TAP-M310R, WAC-M300	Select the product model to upload firmware for. Only upload firmware compatible with the selected product model.	N/A

Firmware File

Click **Browse** and navigate to the firmware file (in .rom format) to upload.



NOTE

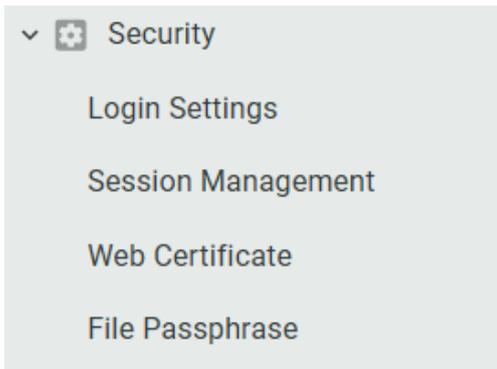
The system will not perform a compatibility check on the uploaded firmware file. To avoid issues, make sure the uploaded firmware file is compatible with the selected product model(s).

Click **Add** to add another firmware file to the release build.

When finished, click **Save**.

Security

From the **Security** section, you can configure **Login Settings**, **Session Management**, **Web Certificate**, and **File Password** settings.



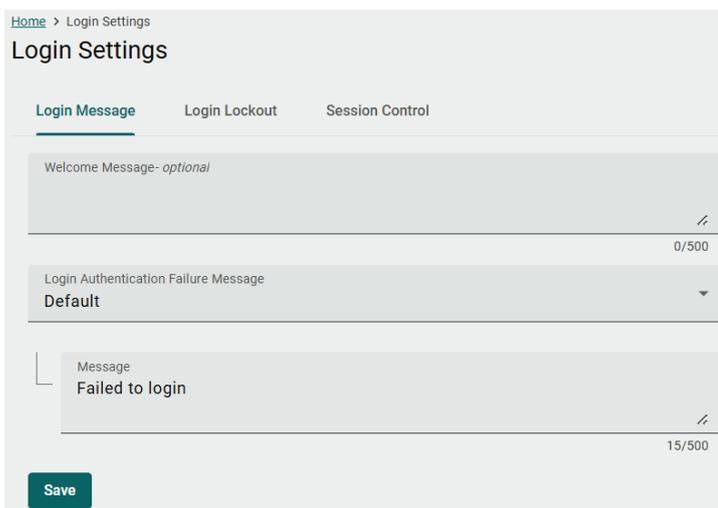
Login Settings

Menu Path: Security > Login Settings

The **Login Settings** section is used to configure login-related settings.

Login Message

The **Login Message** tab lets you configure the message for successful and failed login attempts. Click the **Login Message** tab to access this screen.



Configure the following settings:

Welcome Message - optional

Setting	Description	Factory Default
0 to 500 characters	Enter a welcome message. This message will appear when a user successfully logs in to the web interface.	None

Login Authentication Failure Message

Setting	Description	Factory Default
Default	Use the default login failure message "Failed to login". This message cannot be modified.	Default
Custom	Enter a custom login failure message.	

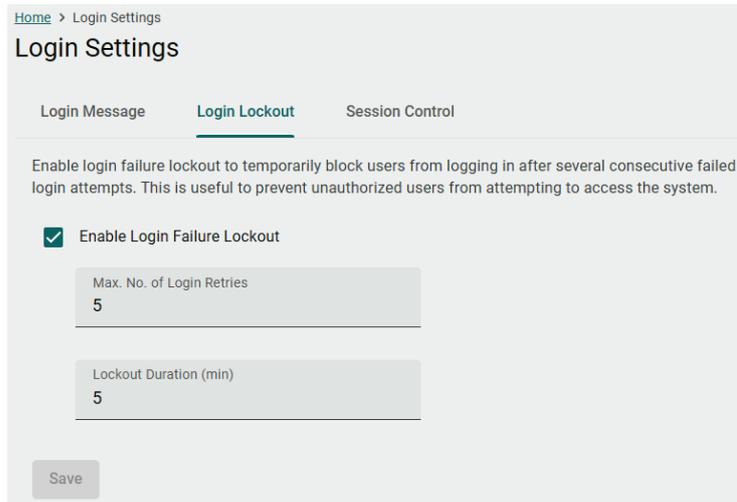
Message (Custom Only)

Setting	Description	Factory Default
0 to 500 characters	Enter the failure message that will appear after an unsuccessful login attempt.	None

When finished, click **Save**.

Login Lockout

The **Login Lockout** tab lets you configure login failure lockout settings. If enabled, a user will be locked out of the web interface after failing several consecutive login attempts. Click the **Login Lockout** tab to access this screen.



Home > Login Settings

Login Settings

Login Message **Login Lockout** Session Control

Enable login failure lockout to temporarily block users from logging in after several consecutive failed login attempts. This is useful to prevent unauthorized users from attempting to access the system.

Enable Login Failure Lockout

Max. No. of Login Retries
5

Lockout Duration (min)
5

Save

Configure the following settings:

Enable Login Failure Lockout

Setting	Description	Factory Default
Checkbox	Enable or disable login failure lockout. If enabled, the system will temporarily block users from logging in after several consecutive failed login attempts.	Checked

Max. No. of Login Retries

Setting	Description	Factory Default
1 to 10	Specify the maximum number of consecutive failed login attempts are allowed before the user account is locked out.	5

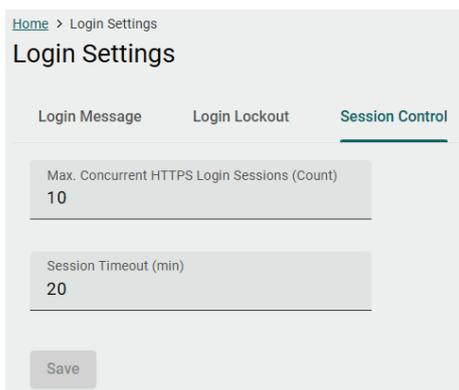
Lockout Duration (min)

Setting	Description	Factory Default
1 to 10	Specify the duration (in minutes) an account will remain locked out after the maximum number of consecutive failed login attempts has been reached. During this time, the user will be unable to log in to the system. Once the lockout time has expired, the user may attempt to log in again.	5

When finished, click **Save**.

Session Control

The **Session Control** tab lets you configure the HTTPS login session settings. Click the **Session Control** tab to access this screen.



Configure the following settings:

Max. Concurrent HTTPS Login Sessions (Count)

Setting	Description	Factory Default
1 to 128	Specify the maximum number of concurrent sessions allowed on the portal WAC.	10

Session Timeout (min)

Setting	Description	Factory Default
5 to 1440	Specify the duration of inactivity after which a user will be automatically logged out.	20

When finished, click **Save**.

Session Management

Menu Path: Security > Session Management

From the **Session Management** screen, you can view the login sessions of all enabled user accounts and can manually terminate active sessions.

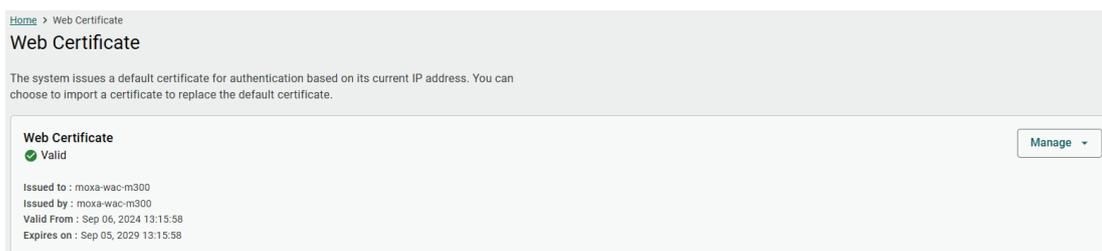


To terminate an active user session, click the **X** icon next to the session you want to terminate.

Web Certificate

Menu Path: Security > Web Certificate

The **Web Certificate** section is used to check certificate information. From this screen you can also export, import, and generate the web certificate.



To export the current web certificate, click **Manage > Export to CSR**. This will download the certificate file to the local host.

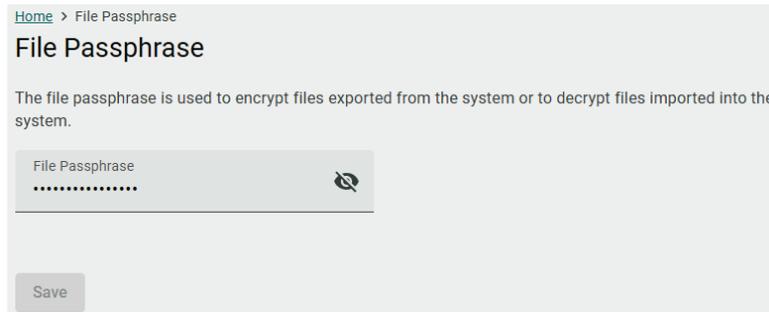
To import a new certificate, click **Manage > Import Certificate** and browse to the web certificate file on the local host.

To generate a new web certificate, click **Manage > Generate Certificate**. The system will generate a new certificate for authentication based on the device's current IP address.

File Passphrase

Menu Path: Security > File Passphrase

The **File Passphrase** section is used to configure the passphrase for encryption and decryption when importing and exporting files.



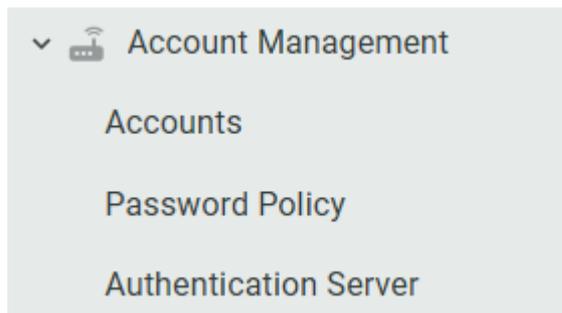
File Passphrase

Setting	Description	Factory Default
8 to 64 characters	Enter the password for encryption and decryption when importing or exporting files, respectively. It is highly recommended to change the default passphrase.	m0x@_w!an_systeM

When finished, click **Save**.

Account Management

From the **Account Management** section, you can configure **Accounts**, **Password Policy**, and **Authentication Server** settings.



Accounts

Menu Path: Account Management > Accounts

The **Accounts** section is used to manage user accounts on the system.



NOTE

The system supports a maximum number of 32 accounts. At least one administrator must be active at any given time.

Home > Accounts

Accounts

Last Updated : Jun 16, 2025 16:16:24 (UTC+08:00) [Refresh](#)

[Create](#)

Account Name	Role	Status	Last Modified	
jiji	Administrator	Active Last Login: --	Jan 09, 2025	⋮
qqqqq	Administrator	Active Last Login: --	Jan 09, 2025	⋮
jet2	Viewer	Active Last Login: --	Oct 18, 2024	⋮
jet1	Viewer	Active Last Login: Dec 17, 2024 19:11:38	Dec 18, 2024	⋮
admin (You)	Administrator	Active Last Login: Jun 16, 2025 15:42:09	--	⋮

Items per page: 10 1 - 5 of 5 < < > >

Create a New Account

Click **Create** to create a new user account.

Create New Account

Role

Viewer

- Out of range. The valid range is 8 to 63 characters.
- Only letters (a-z, A-Z), numbers (0-9), and special characters (_!#\$%&.*@+=^{}|~) are allowed.

Cancel Save

Configure the following settings:

Account Name

Setting	Description	Factory Default
4 to 32 characters	Enter a name for the account.	None

Role

Setting	Description	Factory Default
Viewer	Set the account role to Viewer. This role has view-only access and cannot modify any settings.	Viewer
Administrator	Set the account role to Administrator. This role has full viewing and editing rights.	

Password

Setting	Description	Factory Default
8 to 63 characters	Enter a password for the account.	None

Confirm Password

Setting	Description	Factory Default
8 to 63 characters	Enter the password again for confirmation.	None

When finished, click **Save**.

Edit an Account



NOTE

The account username cannot be modified, and users cannot modify the role of their own account.

To change the account role, click the **Menu** (⋮) icon next to the account and click **Change Role**. Select the desired role and click **Save**.

To change the account password, click the **Menu** (⋮) icon next to the account and click **Change Password**. Enter the password and click **Save**.

To disable or enable an account, click the **Menu** (⋮) icon next to the account and click **Disable** or **Enable**, respectively.

Delete an Account



NOTE

Users cannot deactivate or delete their own account. At least one administrator account must be active at any given time.

Click the **Menu** (⋮) icon next to the account you want to delete and click **Delete**.

When prompted to confirm, click **Delete**.

Password Policy

Menu Path: Account Management > Password Policy

The **Password Policy** section is used to configure the password strength requirements to enhance account security.

Password Policy

To enhance account security, you can enforce a minimum password length and complexity policy.

Minimum Password Length
8

Password Complexity Policy

- Must contain at least one digit (0-9)
- Must contain at least one uppercase letter (A-Z)
- Must contain at least one lowercase letter (a-z)
- Must contain at least one special character (!#\$%&.*@+={}|^_~)

Enabling password lifetime forces users to change their password when logging in after reaching the specified lifetime duration.

- Enable password lifetime

Password Lifetime (Days)
90

Save

Configure the following settings:

Minimum Password Length

Setting	Description	Factory Default
8 to 63	Specify the minimum character length for passwords.	8

Password Complexity Policy

Setting	Description	Factory Default
Checkbox	Enable or disable the corresponding password complexity requirements. Passwords need to comply with all the enabled requirements.	Unchecked

Enable Password Lifetime

Setting	Description	Factory Default
Checkbox	Enable or disable password lifetime. If enabled, passwords will automatically expire after the specified duration, requiring to update their password.	Checked

Password Lifetime (Days)

Setting	Description	Factory Default
0 to 360	Specify the password lifetime (in days). If set to 0, passwords will not expire.	90

When finished, click **Save**.

Authentication Server

Menu Path: Account Management > Authentication Server

The **Authentication Server** section is used to configure RADIUS server settings for remote authentication.



NOTE

The system supports two RADIUS authentication servers for redundancy and failover.

Home > Authentication Server

Authentication Server

If configured, the system will use the authentication server as the primary method to authenticate users. If both the primary and backup authentication servers are unavailable, the system will use the local account database for authentication.

⌵ Adjust Priority Create

Priority	Server Address	Status	UDP Port	Authentication Type	Timeout (sec)	Retry Count
No authentication servers found. Click the Create button to add an authentication server.						

Add an Authentication Server

Click **Create** to add a new server.

Create Server

Enable Server

Server Address

UDP Port
1812

Authentication Type
MS-CHAPv2

Shared Key 🔑

Authentication Timeout (sec) ⓘ
5

Authentication Retries (Times)
1

Cancel Save

Configure the following settings:

Enable Server

Setting	Description	Factory Default
Checkbox	Enable or disable the authentication server.	Unchecked

Server Address

Setting	Description	Factory Default
IP Address	Specify the IP address of the authentication server.	None

UDP Port

Setting	Description	Factory Default
1 to 65535	Specify the UDP port of the authentication server.	1812

Authentication Type

Setting	Description	Factory Default
MS-CHAPv2	Set the RADIUS authentication type to MS-CHAPv2.	MS-CHAPv2
MS-CHAPv1	Set the RADIUS authentication type to MS-CHAPv1.	
CHAP	Set the RADIUS authentication type to CHAP.	
PAP	Set the RADIUS authentication type to PAP.	

Shared Key

Setting	Description	Factory Default
Password	Enter the shared key for the authentication server.	None

Authentication Timeout (sec)

Setting	Description	Factory Default
5 to 30	Specify the duration (in sec) the device will wait for a response from the RADIUS authentication server before it will time out.	5

Authentication Retries (Times)

Setting	Description	Factory Default
0 to 5	Specify the number of times the device will attempt to authenticate with the RADIUS server if no response is received.	1

When finished, click **Save**.

Adjust Authentication Server Priority

By default, the authentication server with index 1 acts as the primary server. The server with index 2 acts as a failover server in the event the primary server is unavailable.

To change the authentication server priority, click **Adjust Priority**.

Adjust Priority

The system will use the server with the highest priority (1) and will fall back to the secondary server if the primary server is unavailable.

1.  2.3.4.10

2.  1.2.3.4

Cancel Save

Click and drag the server cards to the desired priority.

When finished, click **Save**.

Edit an Authentication Server

Click the **Menu** () icon next to the authentication server you want to edit and click **Edit**.

For a description of each setting, refer to [Add an Authentication Server](#).

When finished, click **Save**.

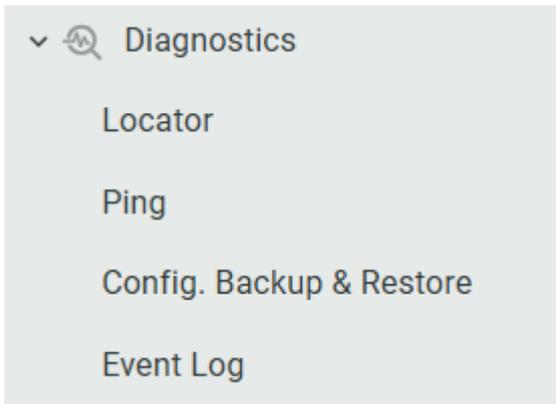
Delete an Authentication Server

Click the **Menu** () icon next to the authentication server you want to delete and click **Delete**.

When prompted to confirm, click **Delete**.

Diagnostics

The **Diagnostics** section contains the **Locator**, **Ping**, **Config. Backup & Restore**, and **Event Log** configuration pages.



Locator

Menu Path: Diagnostics > Locator

From the **Locator** screen, you can trigger an LED sequence and an audible beep on specified devices to identify their physical location.



NOTE

WAC Series devices do not support a beeper mechanism. When performing a location check on WAC Series devices, only the LED sequence will be triggered.



Home > Locator
Locator

Last Updated : Jun 16, 2025 18:18:15 (UTC+08:00) Refresh

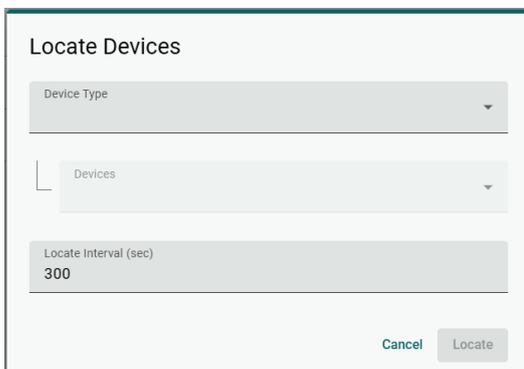
✓ All Locating Completed Search Locate Devices

Device Name	Status	IP Address	MAC Address	Last Located
ap-0090e8100070	Completed Jun 16, 2025 18:18:20	192.168.127.96	00:90:E8:10:00:70	Jun 16, 2025 18:18:15

Items per page: 10 1 - 1 of 1

Locate Devices

To locate one or more devices, click **Locate Devices**.



Locate Devices

Device Type

Devices

Locate Interval (sec)
300

Cancel Locate

Configure the following settings:

Device Type

Setting	Description	Factory Default
WAC, AP, STA	Select the type of the device you want to locate.	None

Devices

Setting	Description	Factory Default
Device Name	Depending on the selected device type, select the device(s) you want to locate.	None

Locate Interval (sec)

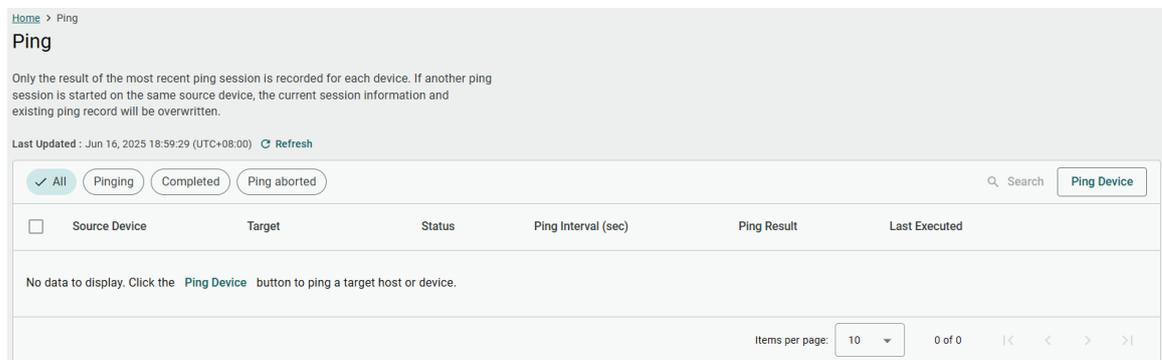
Setting	Description	Factory Default
1 to 3600	Specify the duration of the audible locator beep and LED sequence on the device(s) (in sec).	300

When finished, click **Locate**.

Ping

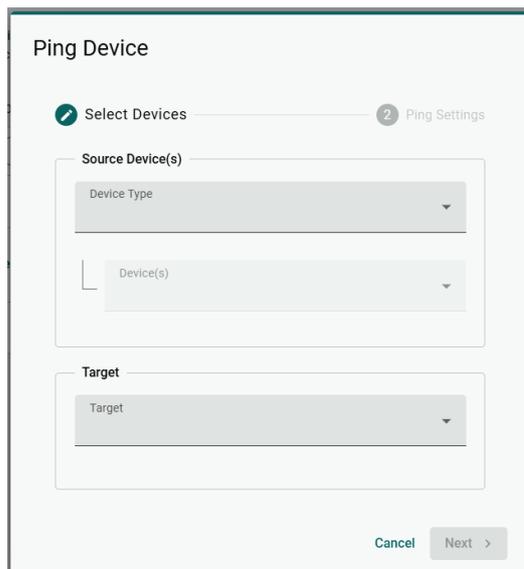
Menu Path: Diagnostics > Ping

From the **Ping** screen, you can ping devices and get detailed reports for network connectivity analysis.



Ping Devices

To ping one or more devices, click **Ping Device**.



Configure the following settings:

Device Type

Setting	Description	Factory Default
WAC, AP, STA	Select the type of the device you want to ping.	None

Devices

Setting	Description	Factory Default
Device Name	Depending on the selected device type, select the source device(s) for the ping test.	None

Target

Setting	Description	Factory Default
IP Address, Domain Name	Specify the IP address or domain name of the ping target.	None
WLAN System	Select a target device in the WLAN system to ping.	

When finished, click **Next**.

The screenshot shows a configuration window titled "Ping Device". At the top, there is a progress indicator with two steps: "Select Devices" (marked with a checkmark) and "Ping Settings" (marked with a pencil icon). Below this, there are two input fields: "Ping Interval (sec)" and "Ping Duration" (set to "Default (3 rounds, 5 pings per round)"). At the bottom, there are three buttons: "Back", "Cancel", and "Execute".

Configure the following settings:

Ping Interval (sec)

Setting	Description	Factory Default
1 to 30	Specify the ping interval (in sec).	None

Ping Duration

Setting	Description	Factory Default
Default (3 rounds, 5 pings per round)	Execute the default 3 rounds of 5 pings.	Default (3 rounds, 5 pings per round)
Custom	Specify a custom ping duration.	

If Custom is selected as the Ping Duration, configure the following settings:

End Date, Hour, Minute

Setting	Description	Factory Default
Date, Hour, Minute	Specify the date and time the ping test will end.	Current device date

Filename Prefix - optional

Setting	Description	Factory Default
1 to 64 characters	Enter a name for the ping result file.	None

File Password

Setting	Description	Factory Default
Use the default file passphrase	Use the file encryption password configured in the File Passphrase section as the default password. Refer to File Passphrase .	Use the default file passphrase
Custom	Specify a custom file encryption password.	

Password (Custom Only)

Setting	Description	Factory Default
8 to 127 characters	Enter the file encryption password.	None

File Destination

Setting	Description	Factory Default
TFTP	Send the ping result to a TFTP server.	TFTP
SFTP	Send the ping result to an SFTP server.	

Server IP Address

Setting	Description	Factory Default
IP Address	Enter the IP address of the TFTP or SFTP server.	None

Account (SFTP Only)

Setting	Description	Factory Default
Account	Enter the account name of the SFTP server.	None

Password (SFTP Only)

Setting	Description	Factory Default
Password	Enter the account password of the SFTP server.	None

When finished, click **Execute**.

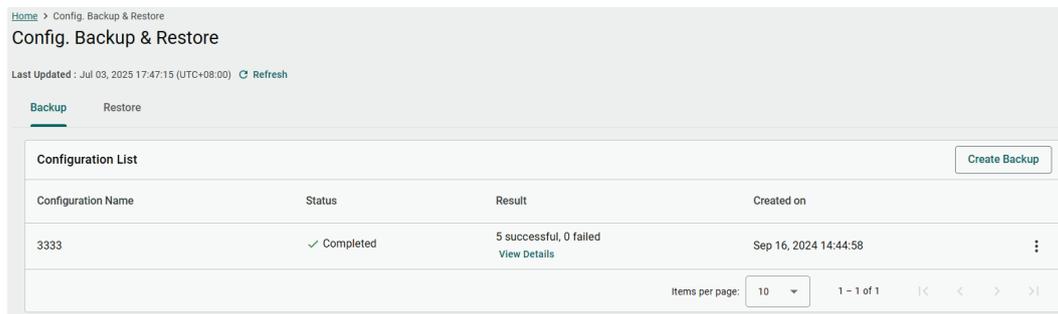
Config. Backup & Restore

Menu Path: Diagnostics > Config. Backup & Restore

From the **Config. Backup & Restore** screen, you can create configuration backups and restore the system configuration from a previous backup.

Backup

The **Backup** tab lets you create and manage configuration backups. Click the **Backup** tab to access this screen.



The screenshot shows the 'Config. Backup & Restore' interface. At the top, there are tabs for 'Backup' and 'Restore'. Below the tabs is a 'Configuration List' table with a 'Create Backup' button. The table has columns for 'Configuration Name', 'Status', 'Result', and 'Created on'. One entry is shown with Configuration Name '3333', Status 'Completed', Result '5 successful, 0 failed', and Created on 'Sep 16, 2024 14:44:58'. There is also a 'View Details' link under the result. At the bottom right, there is a pagination control showing 'Items per page: 10' and '1 - 1 of 1'.

Create a Configuration Backup

Click **Create Backup** to create a new configuration backup.



NOTE

You can create a maximum of 10 configuration backups.

Back Up Configuration

Info
To make sure all settings are backed up correctly, do not edit any configuration settings while the backup is in progress.

Configuration Name

Devices
Specific devices

Select Device

WAC AP STA 0 device(s) selected

Search

<input type="checkbox"/>	Device Name	IP Address
<input type="checkbox"/>	wac-0090e8ff0002	192.168.127.248
<input type="checkbox"/>	wac-0090e8ff0003	192.168.127.247

Cancel Execute

Configure the following settings:

Configuration Name

Setting	Description	Factory Default
1 to 255 characters	Enter a name for the configuration backup.	None

Devices

Setting	Description	Factory Default
All online devices	Back up the configuration for all online devices.	Specific devices
Specific devices	Back up the configuration for specific devices. In the Select Device section, check the box of the device(s) you want to back up the configuration for. You can select across device types (WAC, AP, STA).	

When finished, click **Execute**.

Renaming a Configuration Backup

Click the **Menu** (⋮) icon next to the configuration backup you want to edit and click **Edit Configuration Name**.

Configure the following settings:

Configuration

Setting	Description	Factory Default
1 to 255 characters	Enter a name for the configuration backup.	None

When finished, click **Save**.

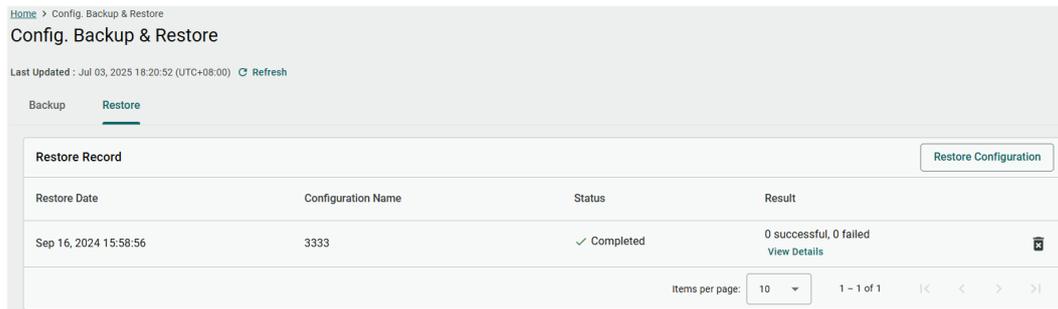
Deleting a Configuration Backup

Click the **Menu** (⋮) icon next to the configuration backup you want to delete and click **Delete**.

When prompted to confirm, click **Delete**.

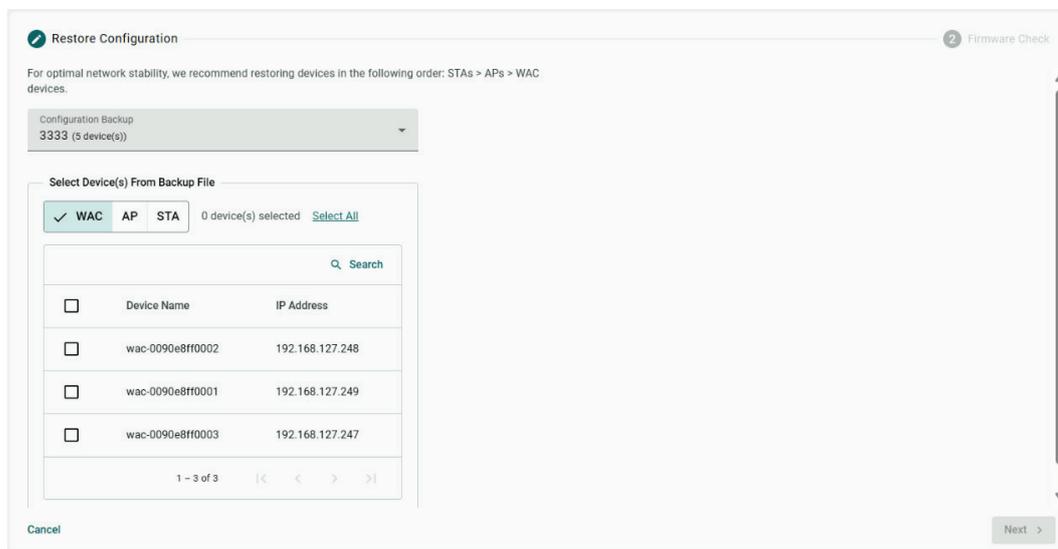
Restore

The **Restore** tab lets you restore the configuration of selected devices from a previously backed up configuration and view configuration restore records. Click the **Restore** tab to access this screen.



Restore a Configuration Backup

Click **Restore Configuration** to restore a configuration.



Configure the following settings:

Configuration Backup

Setting	Description	Factory Default
Configuration File	Select a previously created configuration backup to restore. To create a configuration backup, refer to Create a Configuration Backup .	

Select Device(s) From Backup File

Check the box of the device(s) to restore the configuration for. You can select across device types (WAC, AP, STA). Only devices included in the configuration backup file can be selected.

When finished, click **Next**.

Restore Configuration Firmware Check

Make sure the firmware version of the backup configuration matches the current firmware version to prevent issues when restoring the configuration.

All
 Match
 Mismatch
 Search

Device Name	Firmware Check	Current Firmware	Backup Firmware
wac-0090e8ff0002	▲ Mismatch	v1.0.1 Build 2025_0627_1721	v1.0 Build 2024_0916_1226

Cancel

The system will perform a firmware check to see if the current device firmware matches the firmware version in the configuration backup. Any devices with a mismatching firmware version will be shown. While it is possible to restore the configuration across different firmware versions, it is recommended to use firmware that matches that of the configuration backup to avoid potential issues or system instability.

When finished, click **Restore & Reboot**.

Event Log

Menu Path: Diagnostics > Event Log

From the **Event Log** screen, you can view a list of all WLAN system event logs.

Home > Event Log

Event Log

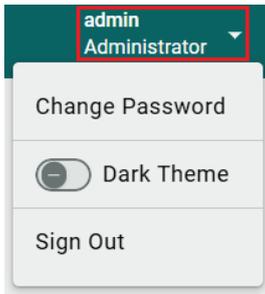
The event log table shows all WLAN system events.

Last Updated : Jul 03, 2025 19:31:05 (UTC+08:00) [Refresh](#)
 Log Capacity Used : 89.7%

Severity	Group	Event	Timestamp
> Information	System	Login Success	Jul 03, 2025 19:11:15
> Information	System	Session Logout	Jul 03, 2025 19:10:56
> Information	System	Session Logout	Jul 03, 2025 19:10:56
> Information	System	Session Logout	Jul 03, 2025 19:10:56
> Information	System	Sync Database Success	Jul 03, 2025 19:00:02
> Information	Diagnostic	Config. Backup Deleted	Jul 03, 2025 18:29:26
> Information	Diagnostic	Config. Backup Completed	Jul 03, 2025 18:28:06
> Information	Diagnostic	Config. Backup Started	Jul 03, 2025 18:28:06
> Information	System	Sync Database Success	Jul 03, 2025 18:00:02

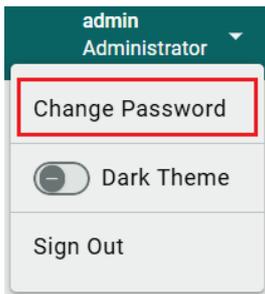
Maintenance and Tools

The user tools and functions are located at the top-right of the interface. Click the triangle icon in the upper-right corner of the page to open the user menu.



Change Password

Click **Change Password** to change the password of the account that is currently logged in.



Configure the following settings:

Change Password

- Out of range. The valid range is 8 to 63 characters.
- Only letters (a-z, A-Z), numbers (0-9), and special characters (_!#\$%&.*@+={})~) are allowed.

Cancel Save

Current Password

Setting	Description	Factory Default
8 to 63 characters	Enter the current password.	None

New Password

Setting	Description	Factory Default
8 to 63 characters	Enter the new password.	None

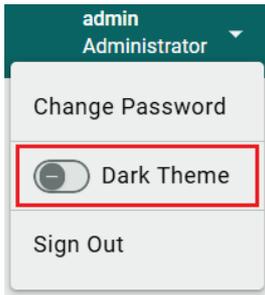
Confirm Password

Setting	Description	Factory Default
8 to 63 characters	Enter the new password again.	None

When finished, click **Save**.

Dark Theme

Click the **Dark Theme** toggle to enable or disable the dark theme for the interface.



Sign Out

To sign out of the WAC, click **Sign Out**. No confirmation prompt will appear. You will be immediately logged out of the system.

