WAC-M300 Series User Manual

Version 1.0, July 2025

www.moxa.com/products

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

Trademarks

Disclaimer

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

Technical Support Contact Information

www.moxa.com/support

Table of Contents

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:

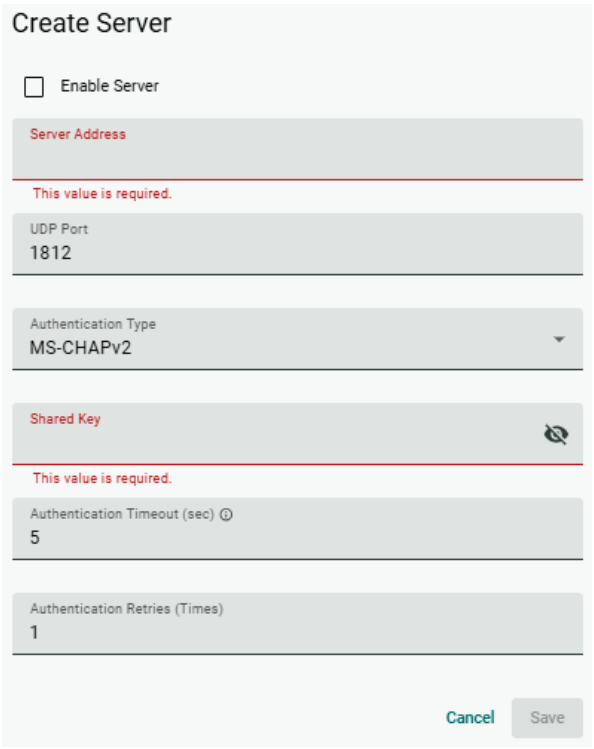
WARNING

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



- 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 (`).

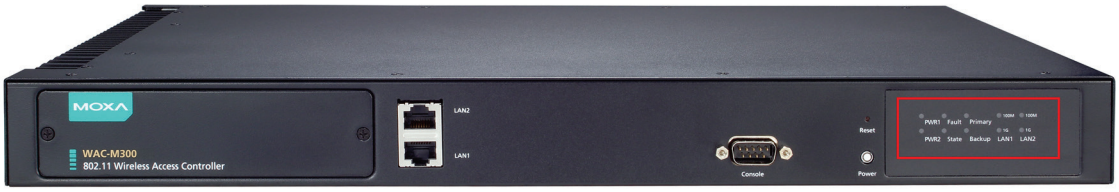
2. Getting Started

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.

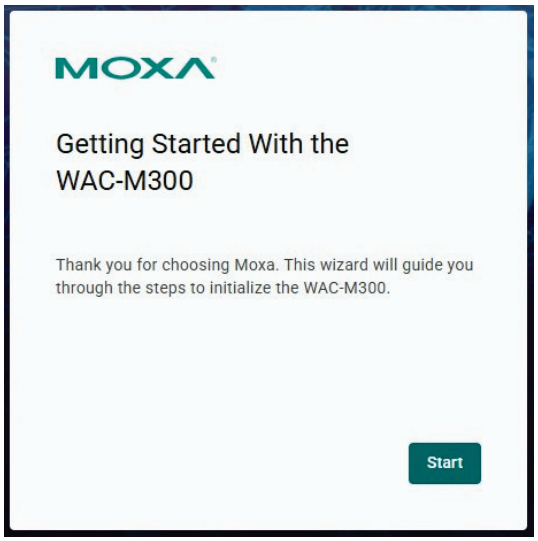
The LED indicator on the WAC Series' LAN port will light up when a connection is established.

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**.

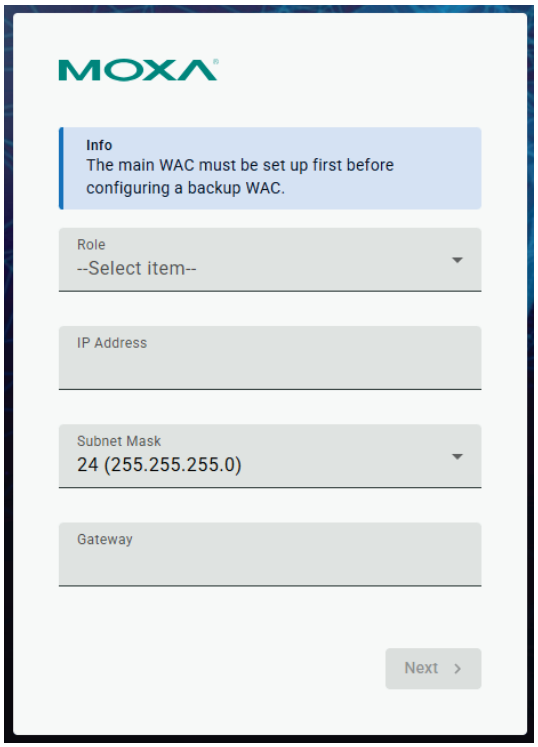


Step 5: Configure the WAC's role and network parameters.

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

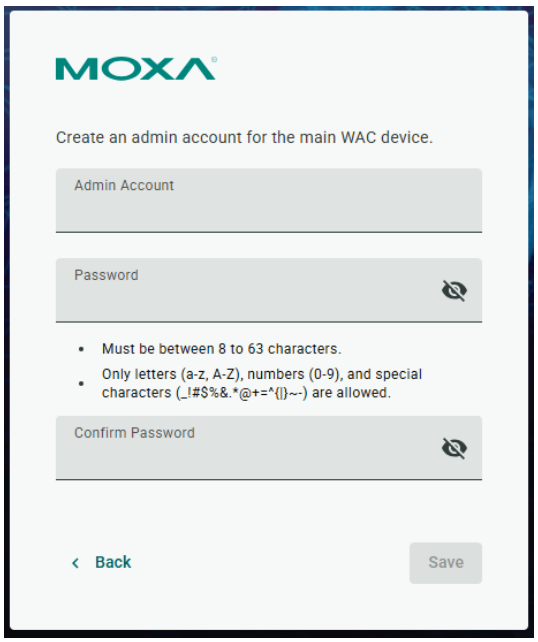
The Main WAC must be set up first before a WAC can be designated as a Backup WAC.



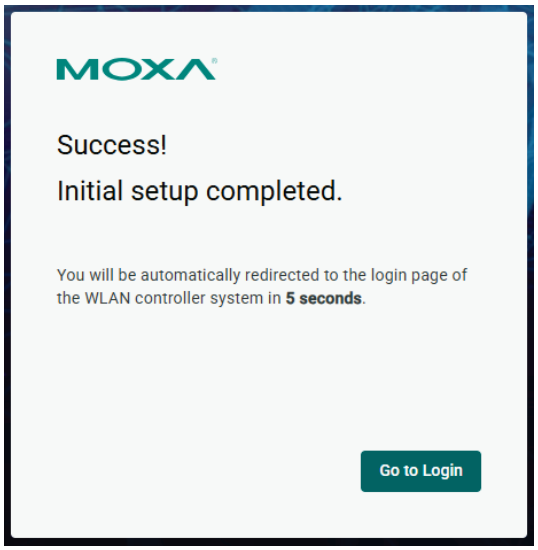
Step 6: Create a user account and password.

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.

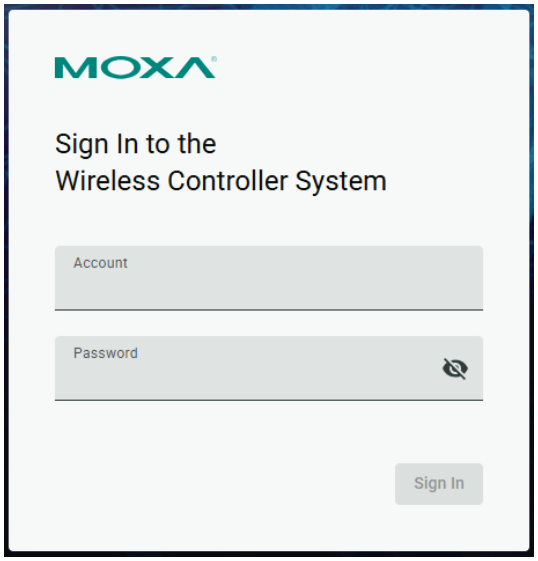


After creating your account, you will be automatically redirected to the login screen.



Step 7: Log in to the device.

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

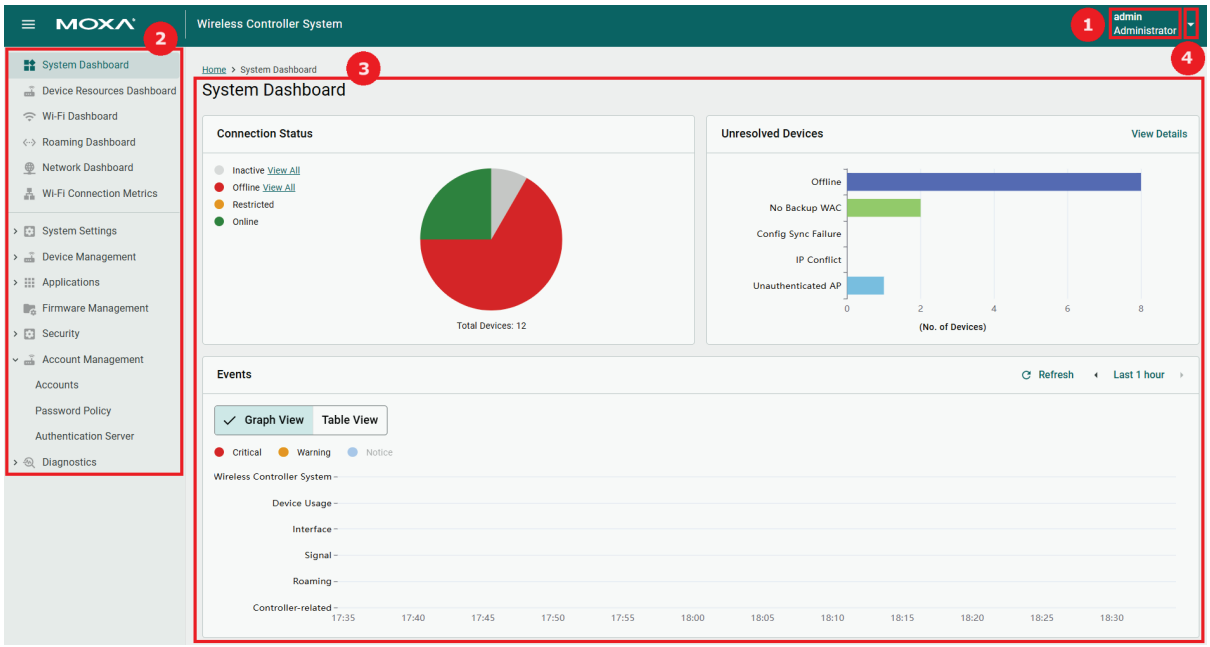


3. Web Interface Configuration

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

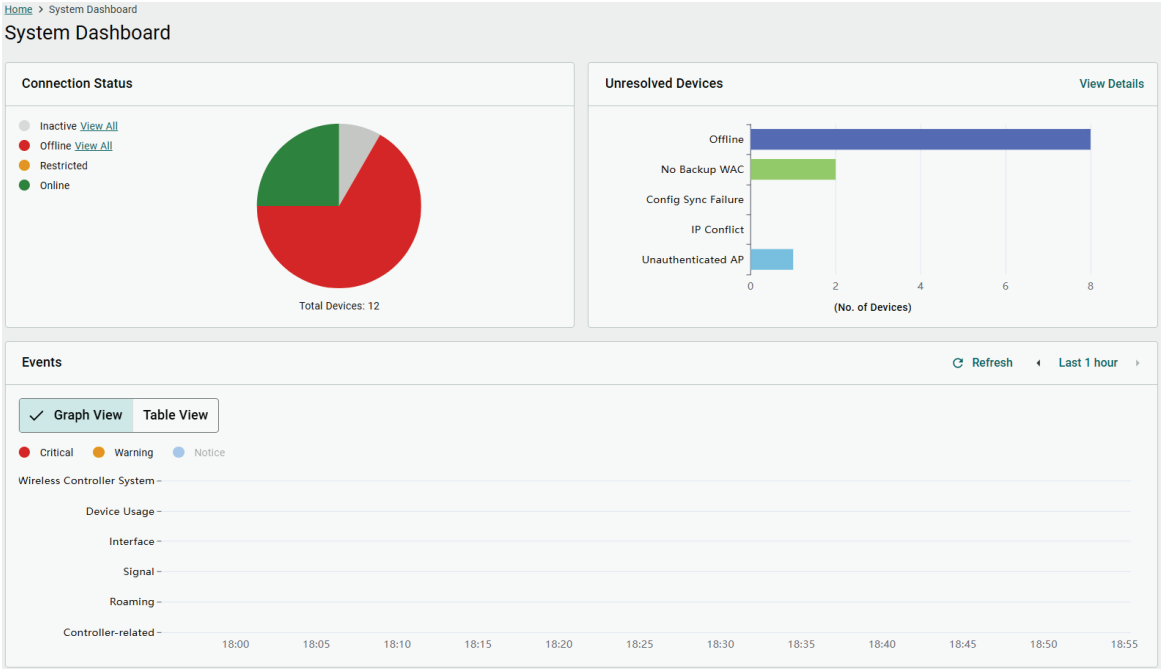
This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



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

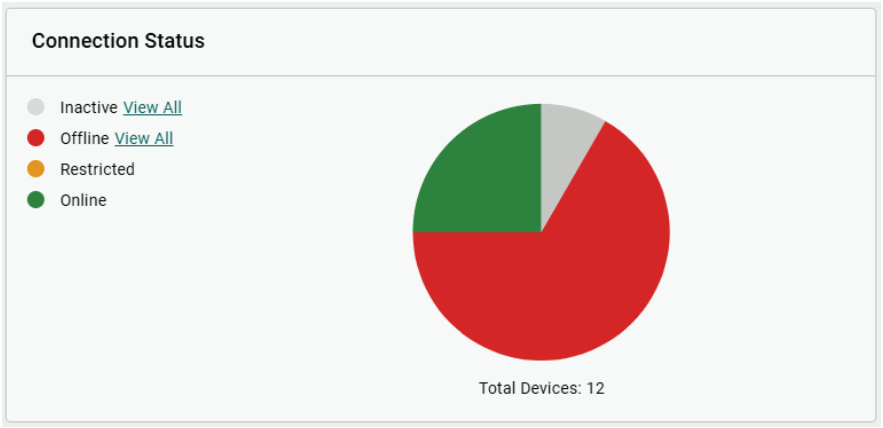
After successfully connecting to the WAC-M300 Series, the **System Dashboard** will automatically appear. To view the device summary from anywhere in the interface, click **System Dashboard** on the Function Menu.



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

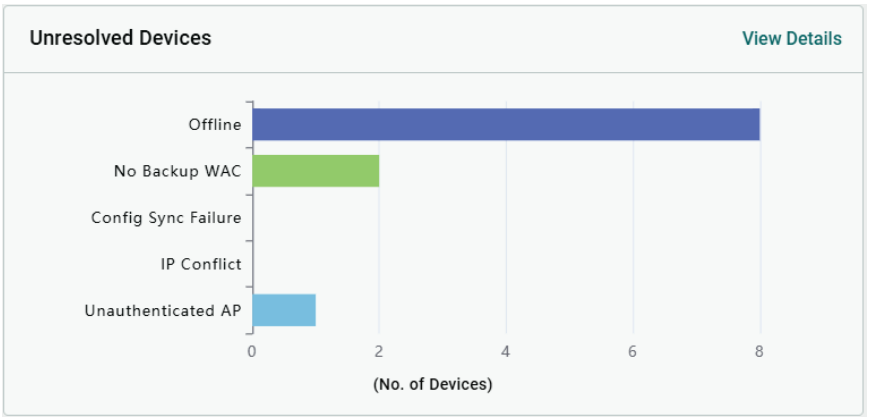
Connection Status

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

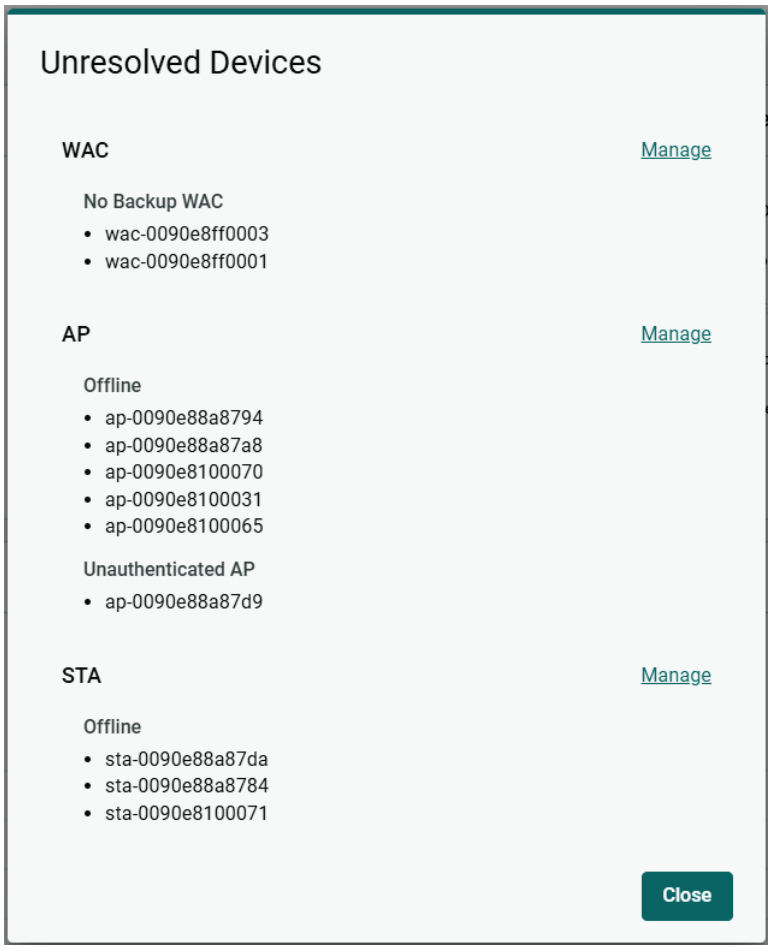


Unresolved Devices

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.



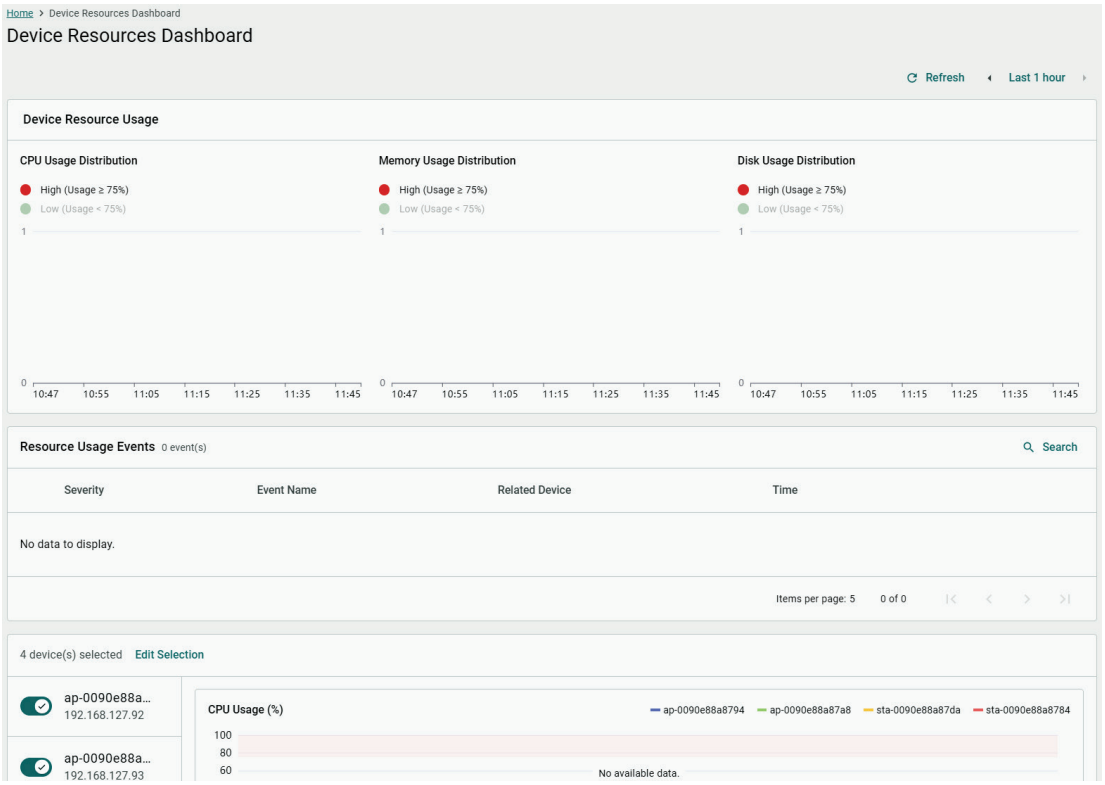
Events

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

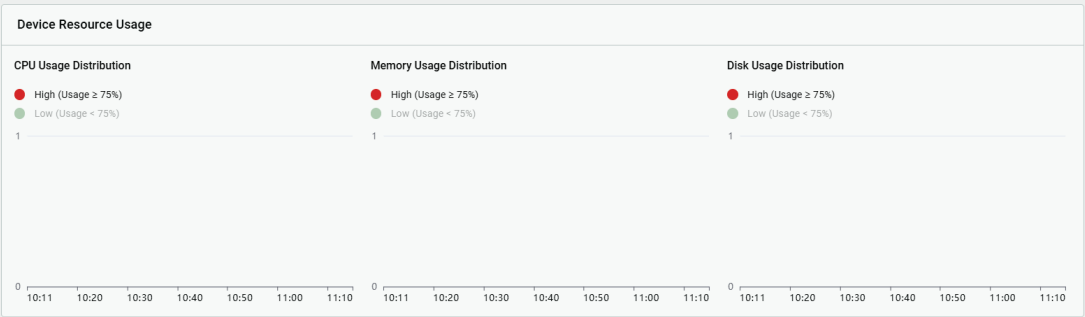
From the **Device Resources Dashboard** screen, you can view the resource usage of the device.



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

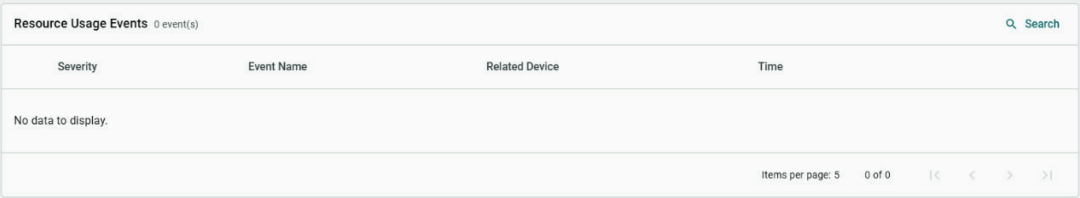
Device Resource Usage

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.



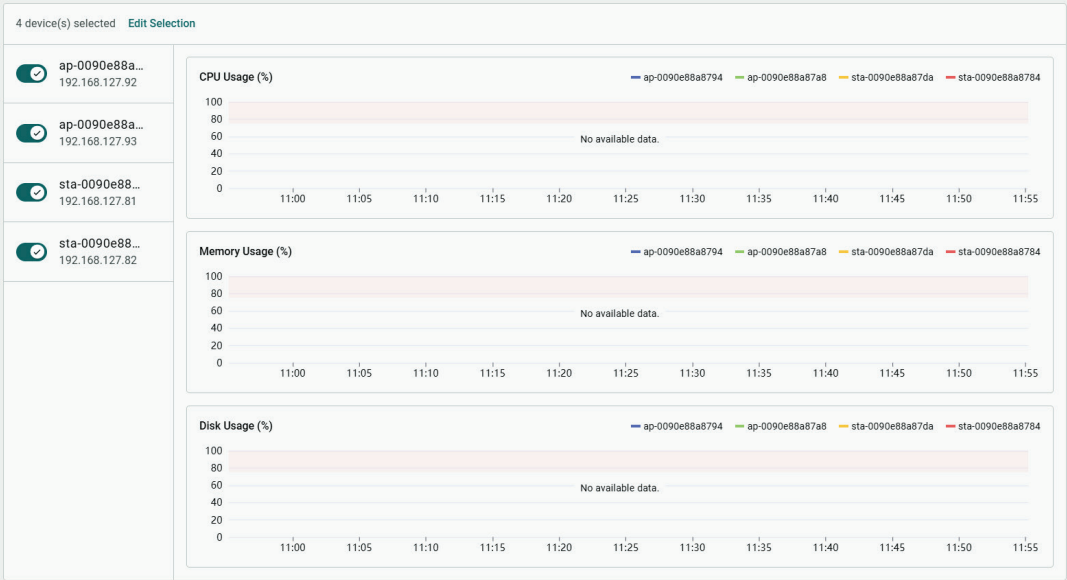
Resource Usage Events

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.



Compare Device Usage

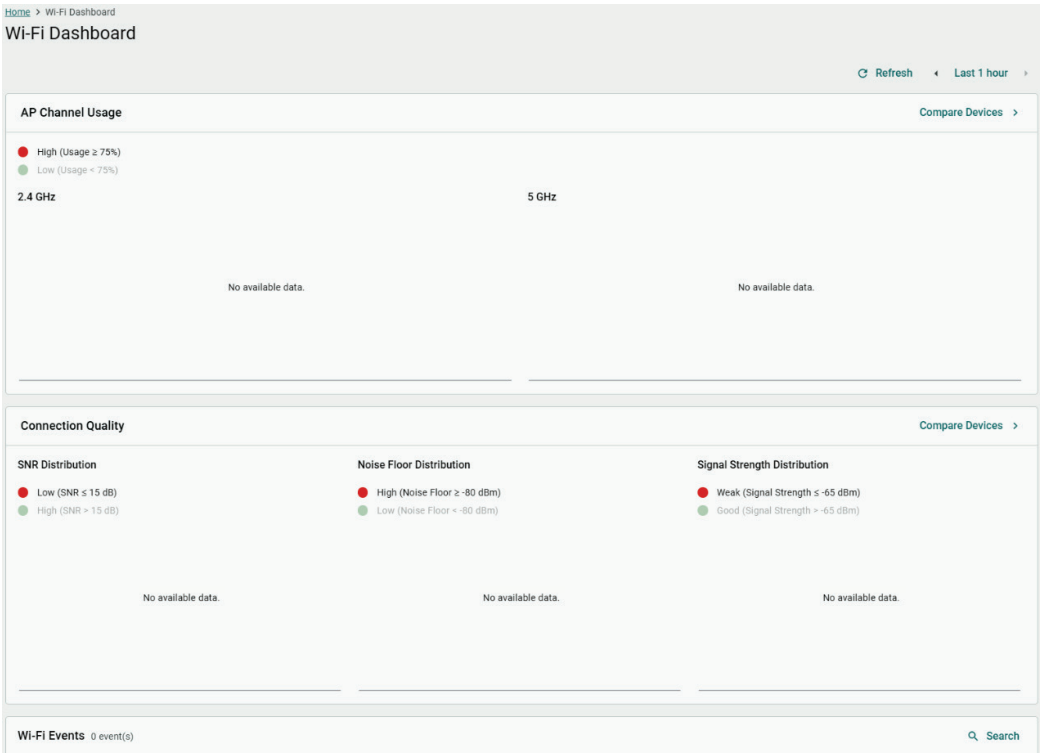
This widget lets you compare the resource usage history of up to 8 selected devices.



Wi-Fi Dashboard

Menu Path: Wi-Fi Dashboard

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



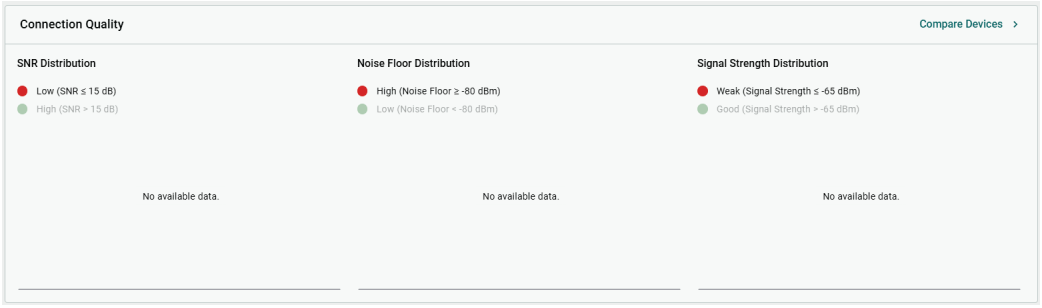
Refer to the following sections for more details about each widget.

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.



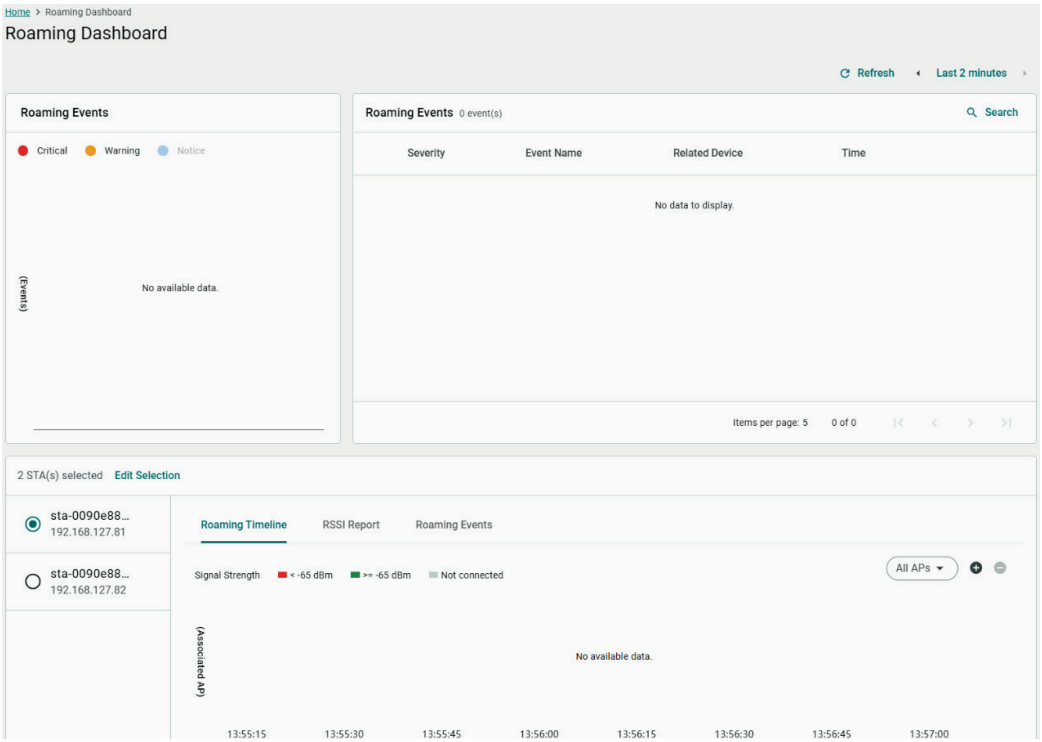
Wi-Fi Events

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.

Roaming Dashboard

Menu Path: Roaming Dashboard

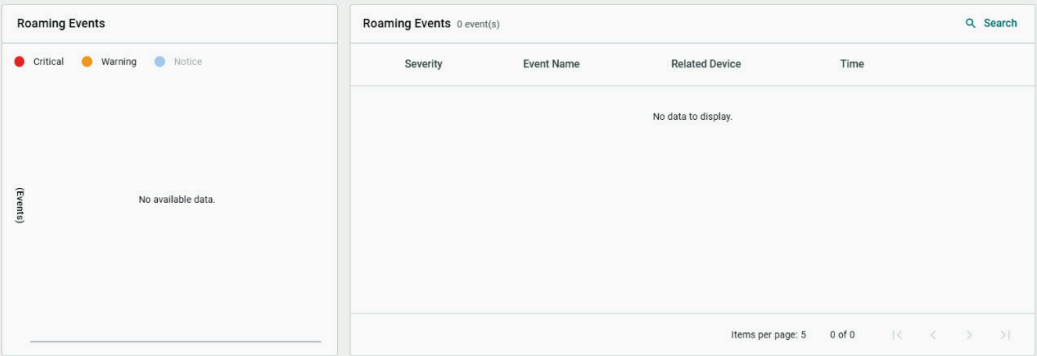
From the **Roaming Dashboard** screen, you can view the roaming status of managed devices.



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

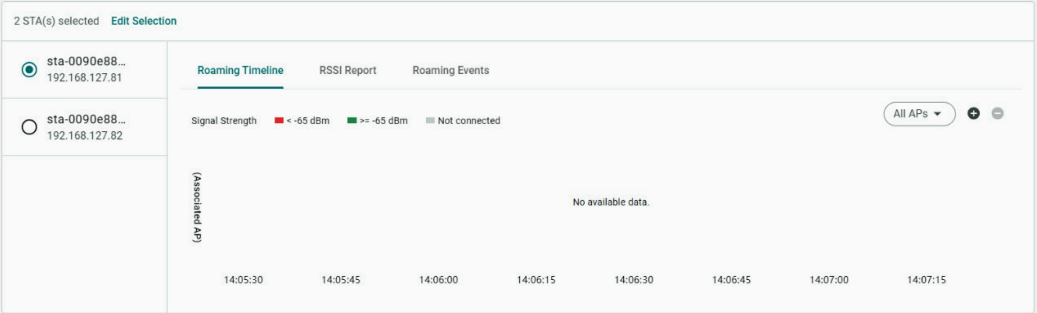
Roaming Events

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



Monitoring Roaming Status

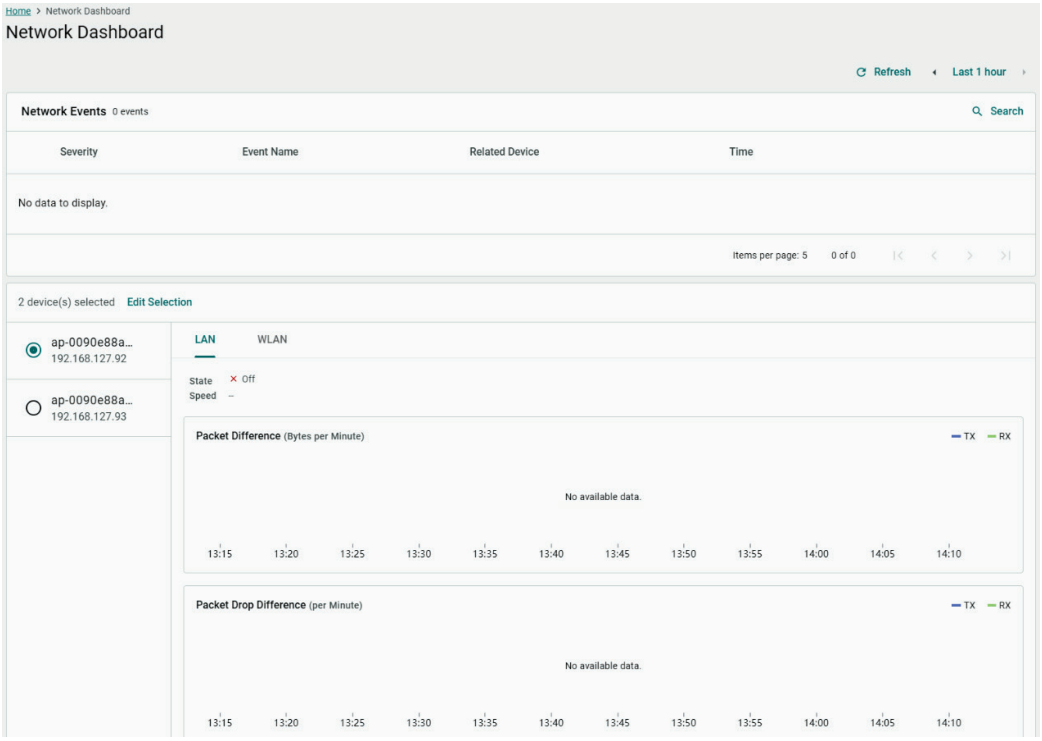
This widget shows the roaming status of managed devices. Click **Compare Devices** to compare and view more detailed roaming information for up to 8 selected devices.



Network Dashboard

Menu Path: Network Dashboard

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



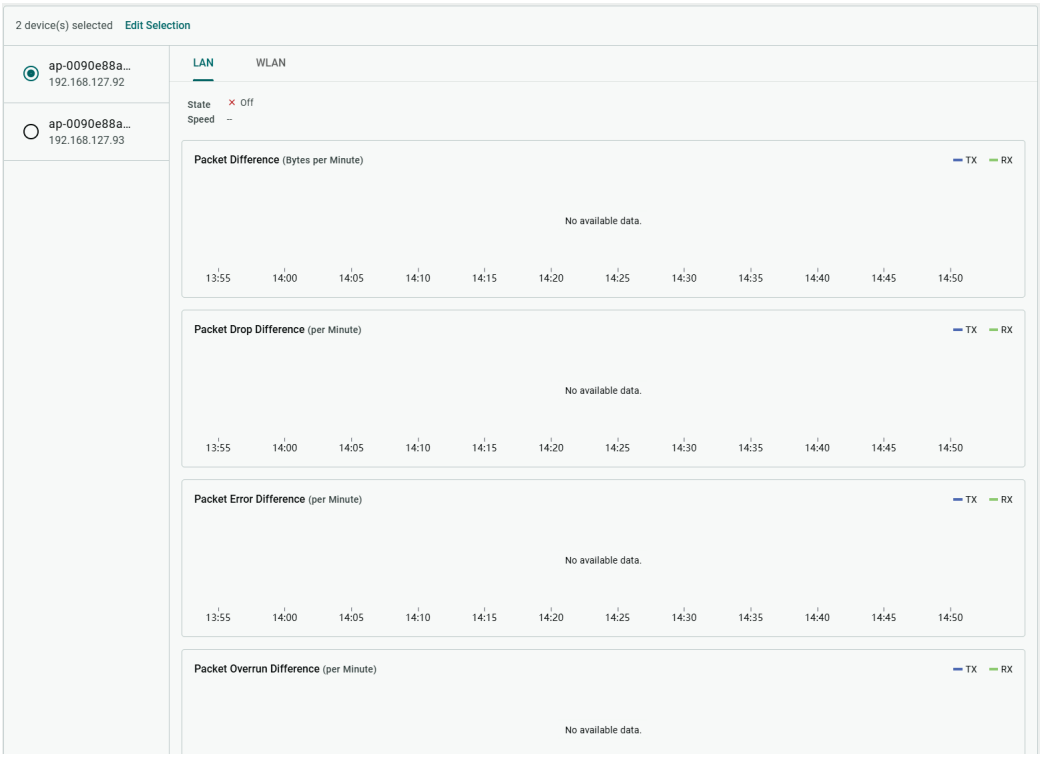
Refer to the following sections for more details about each widget.

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

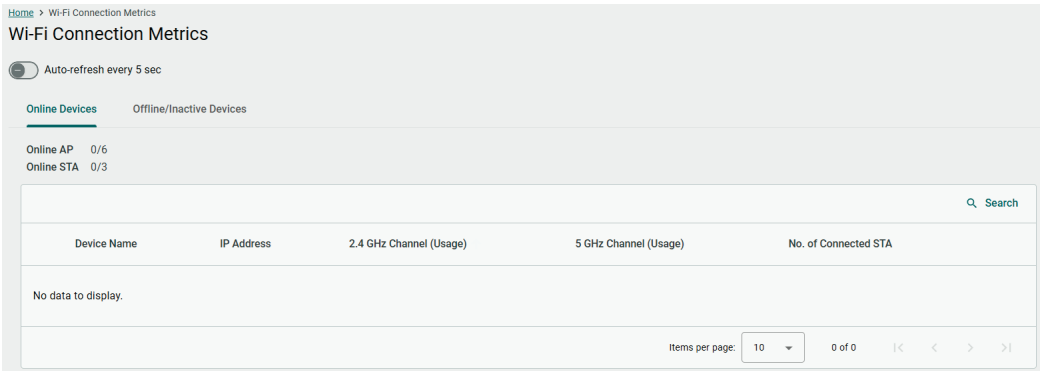
Menu Path: Wi-Fi Connection Metrics

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**.

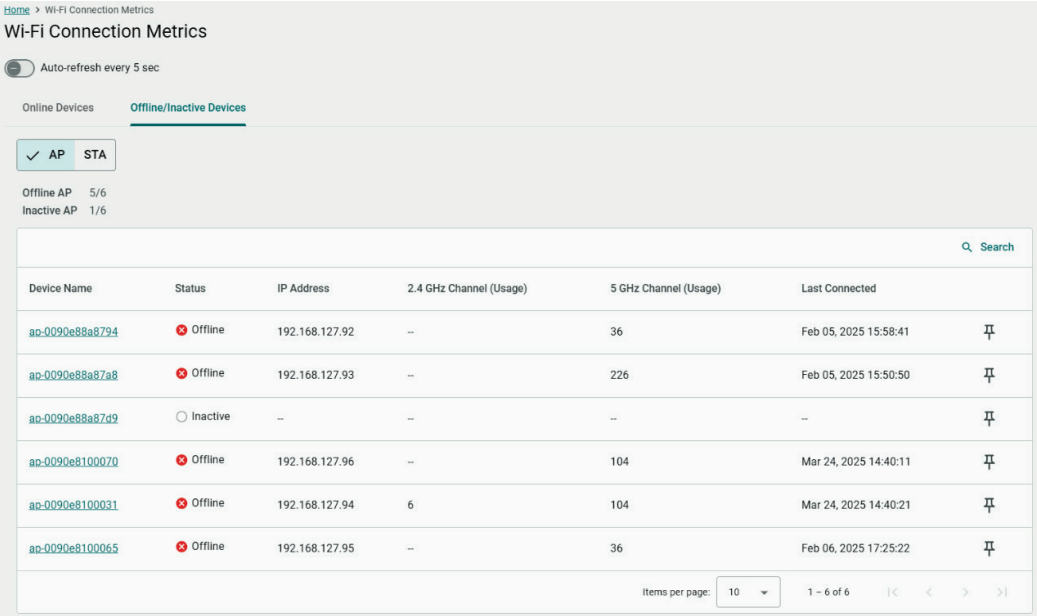
Online Devices

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.



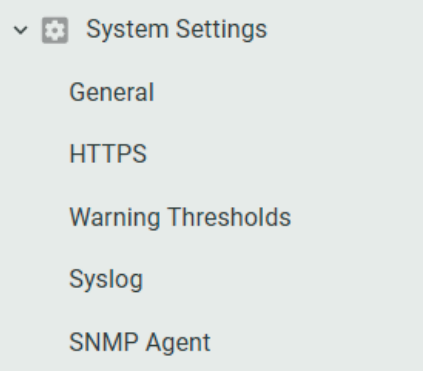
Offline/Inactive Devices

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.



System Settings

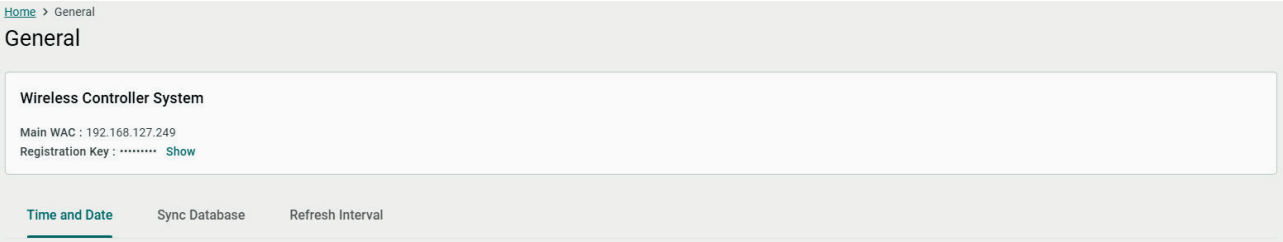
The **System Settings** section covers system configuration functions. From here, you can configure the **General**, **HTTPS**, **Warning Thresholds**, **Syslog**, and **SNMP Agent** settings.



General

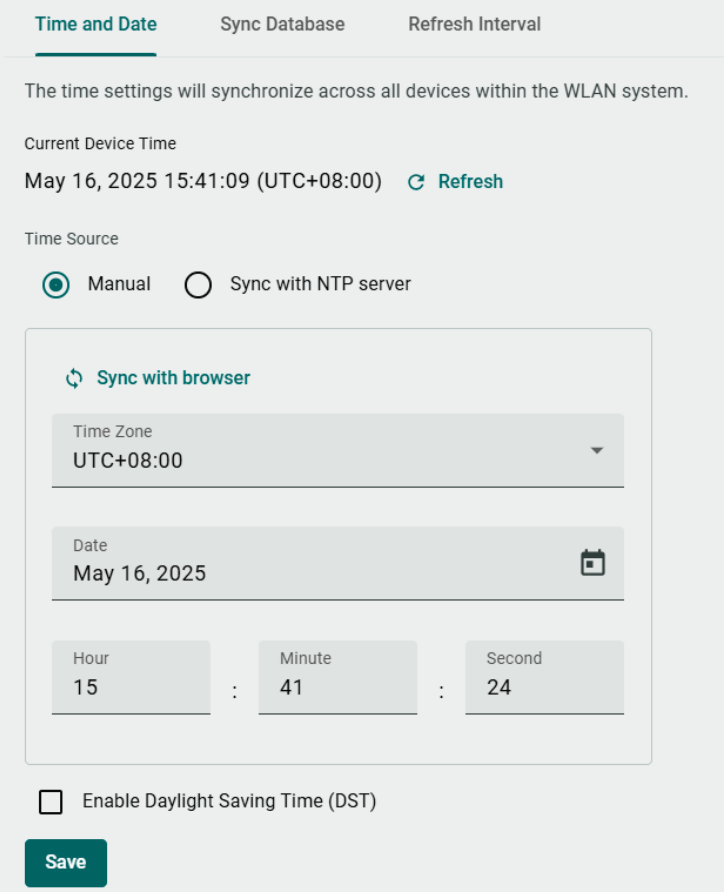
Menu Path: System Settings > General

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 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

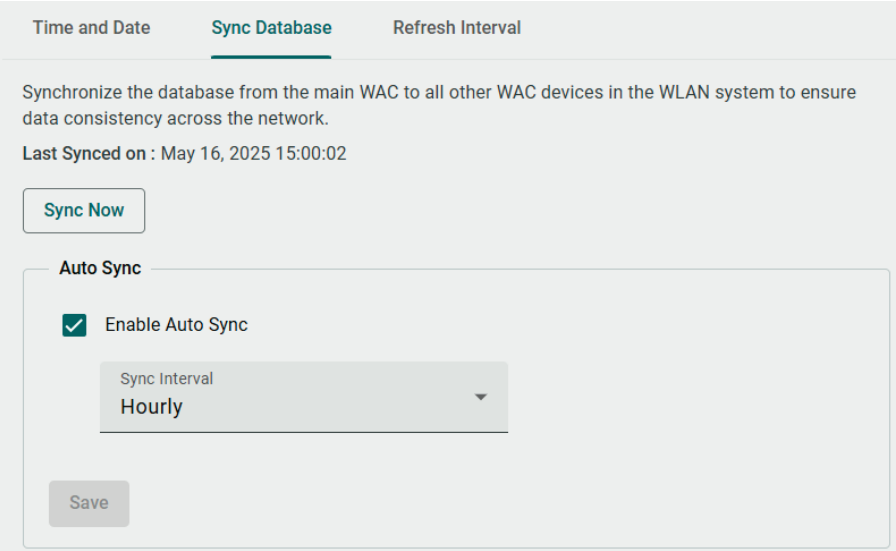
Setting	Description	Factory Default
Month, Week, Day, Hour	Specify the start and end date and time for daylight saving.	Jan 1st week, Sun. 00

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**.



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

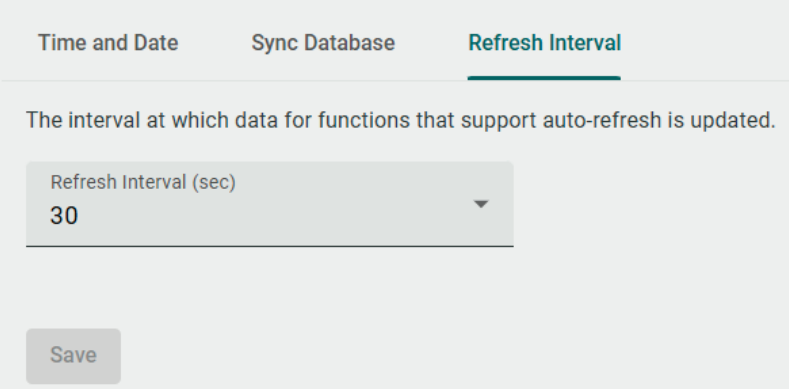
Sync Interval

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.



Refresh Interval (sec)

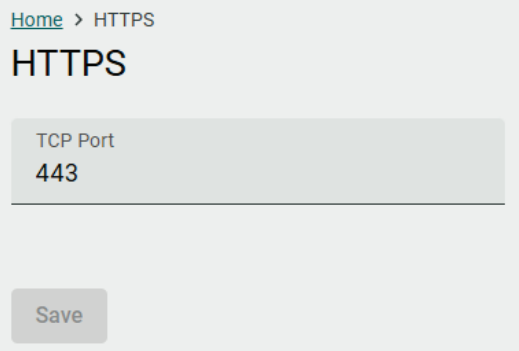
Setting	Description	Factory Default
Interval	Select the data refresh interval (in seconds).	30

When finished, click **Save**.

HTTPS

Menu Path: System Settings > HTTPS

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



TCP Port

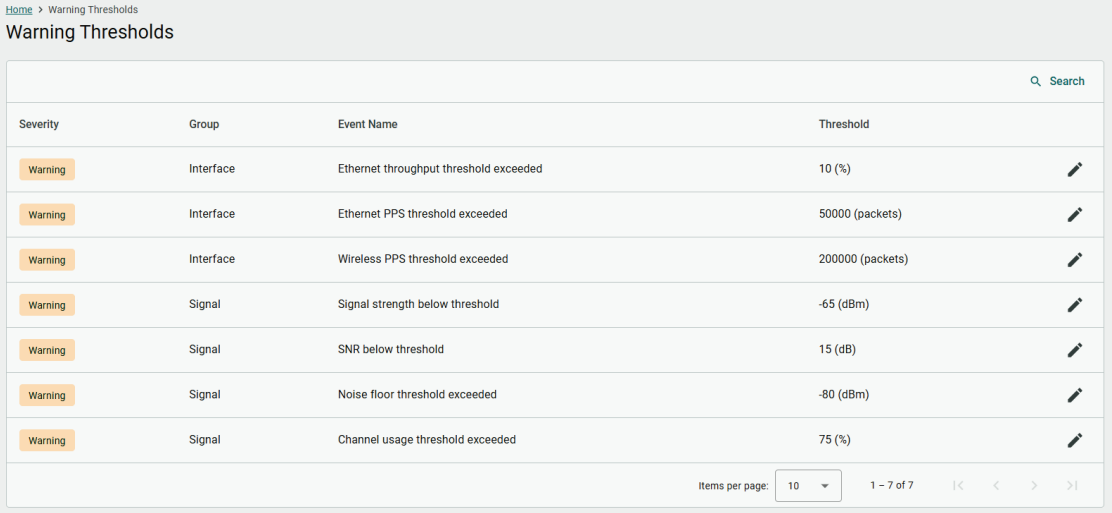
Setting	Description	Factory Default
1 to 43999, 45000 to 65535	Specify the TCP port number for the HTTPS interface used to access the main WAC.	443

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.



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

When finished, click **Save**.

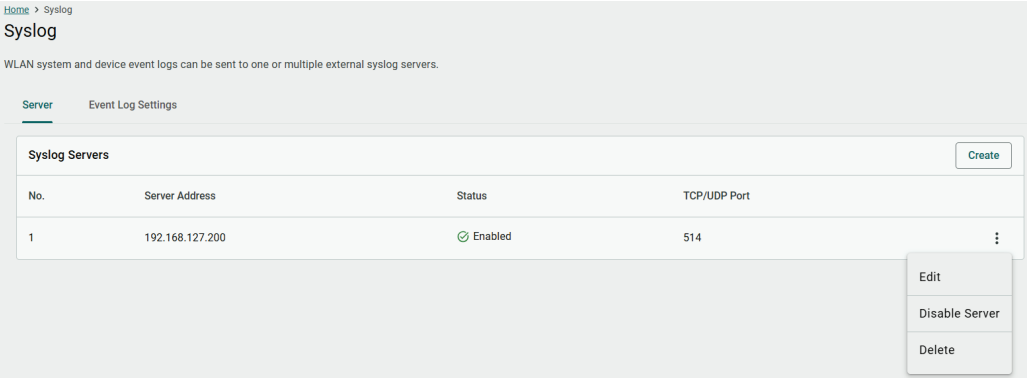
Syslog

Menu Path: System Settings > Syslog

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

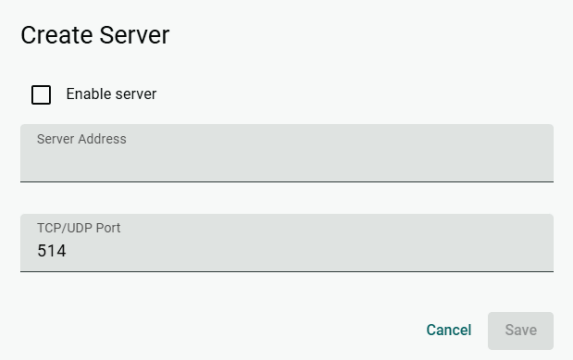
Server

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.



Create a New Syslog Server

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



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

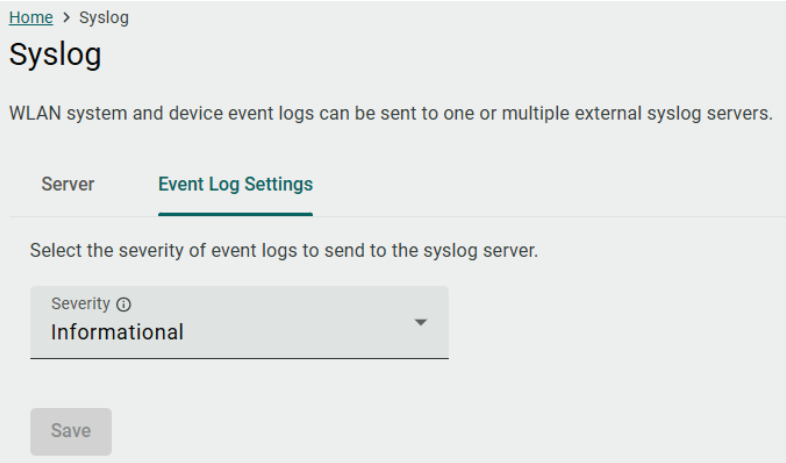
Click the **menu** (⋮) icon next to the server you want to disable and click **Disable**.

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

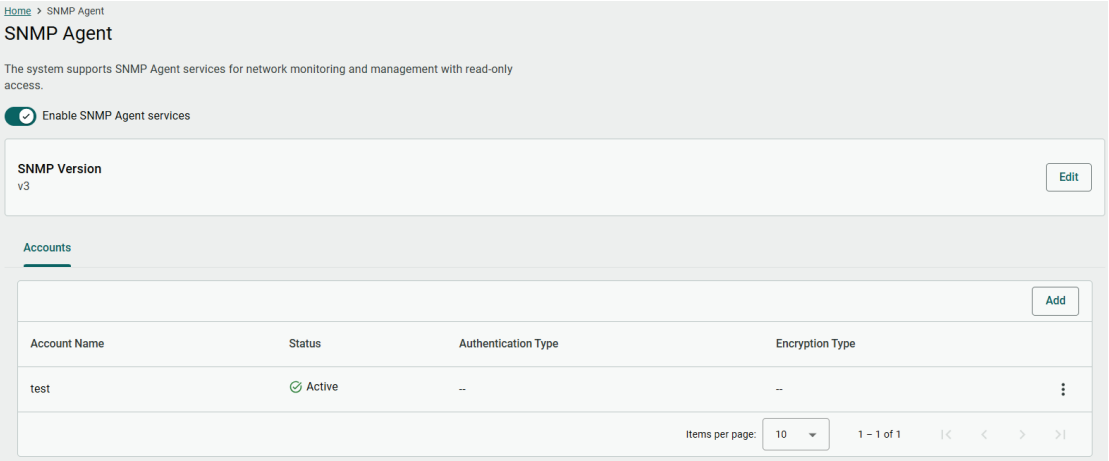
Setting	Description	Factory Default
Emergency, Alert, Critical, Error, Warning, Notice, Informational	Select the severity level of event logs to send to the syslog server. Logs with severity levels under the selected level will also be sent to the syslog server.	Informational

When finished, click **Save**.

SNMP Agent

Menu Path: System Settings > SNMP Agent

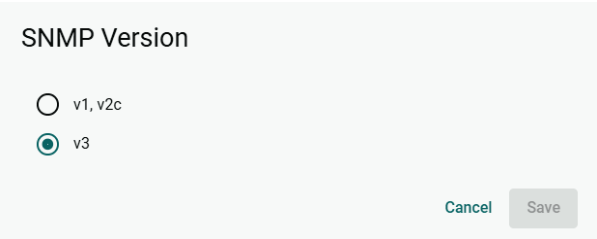
From the **SNMP Agent** section, you can enable SNMP Agent services for network monitoring and read-only management. This page is also used to manage SNMP accounts.



Enable SNMP Agent Services

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

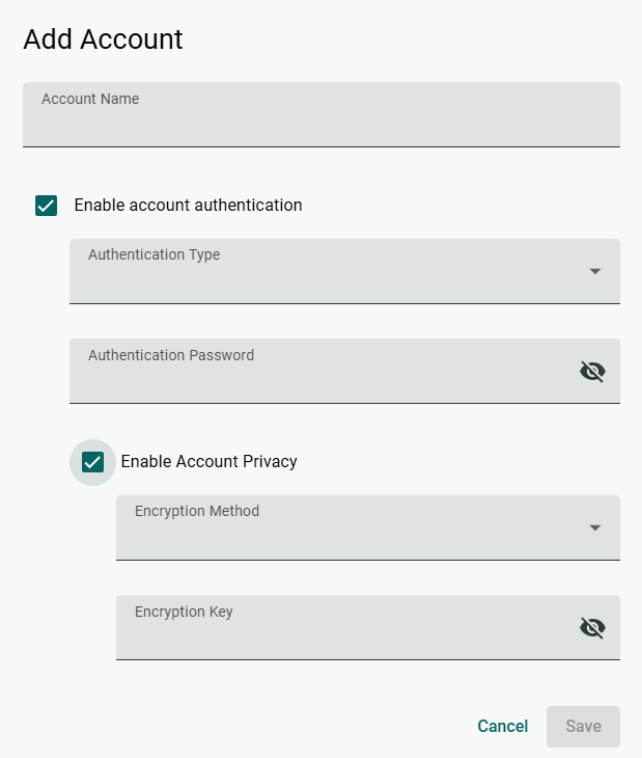
To change the SNMP version, click the **Edit** button and select the desired SNMP version.



When finished, click **Save**.

Create an SNMP Account

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



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

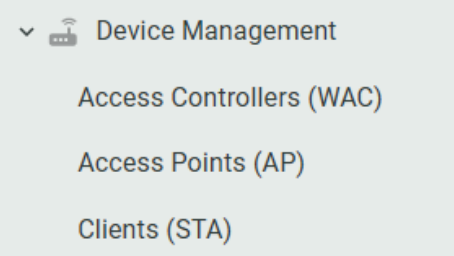
If **Account Privacy** is enabled, configure the encryption method.

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

When finished, click **Save**.

Device Management

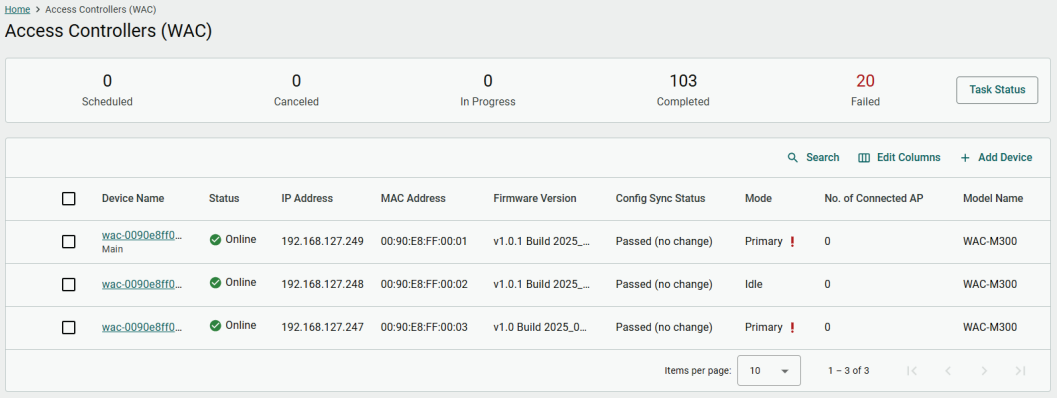
From the **Device Management** section, you can manage settings for the different device types, including access controllers (WAC), access points (AP), and clients (STA).



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.



Task Status

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

NOTE

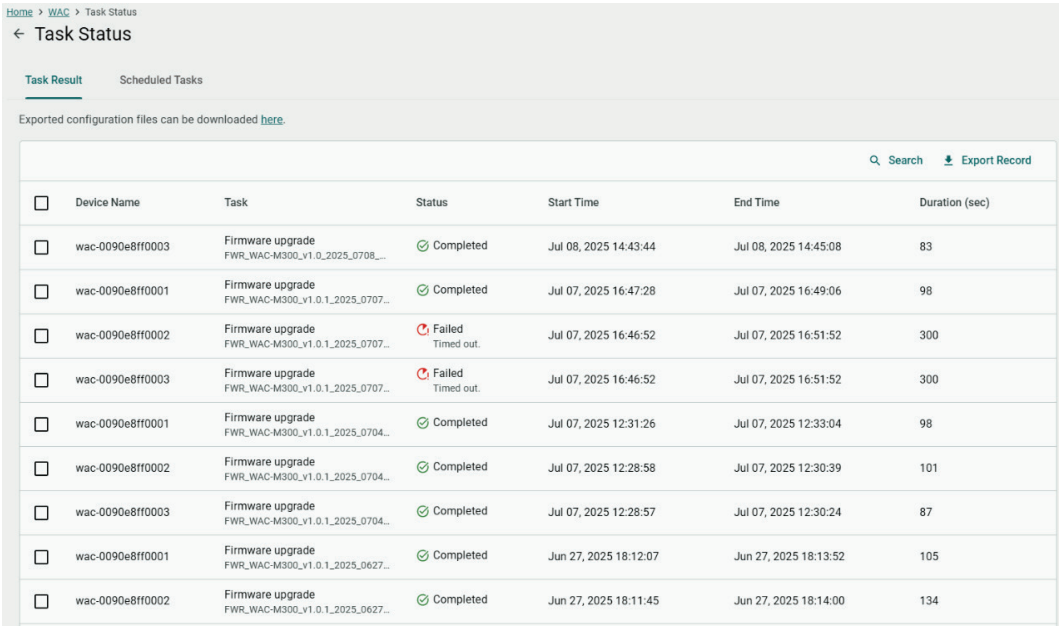
All device types (WAC, AP, STA) have a dedicated Task Status page. While task types may differ, the Task Status page behaves the same for all devices.

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.

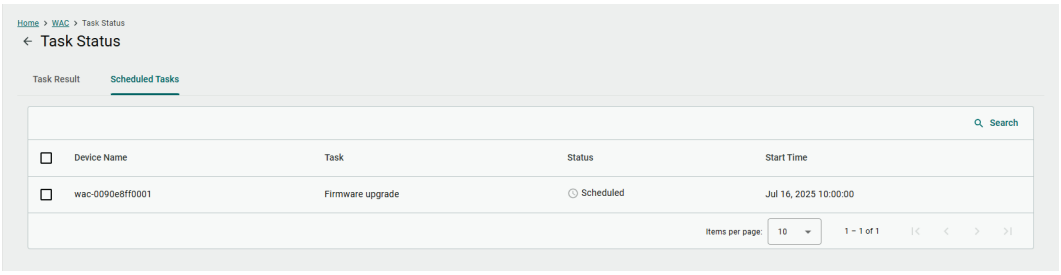
To delete records, check the box of the task record(s) you want to delete and click **Clear Record**.



Scheduled Tasks

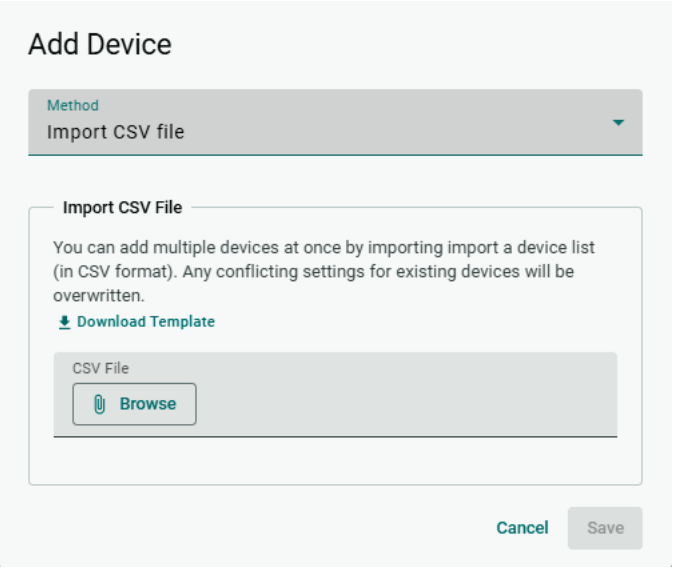
The **Scheduled Result** tab shows a list of all currently pending scheduled tasks. Once a scheduled task is finished, a record will be added to the **Task Result** table.

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



Add a WAC Device

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



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

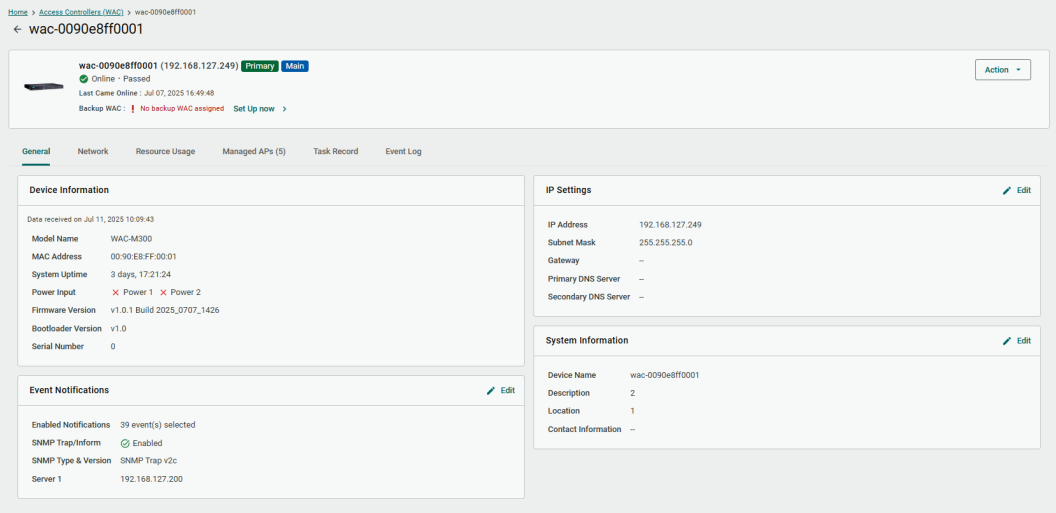
Assign as Primary WAC (Manually Add Device Only)

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

When finished, click **Save**.

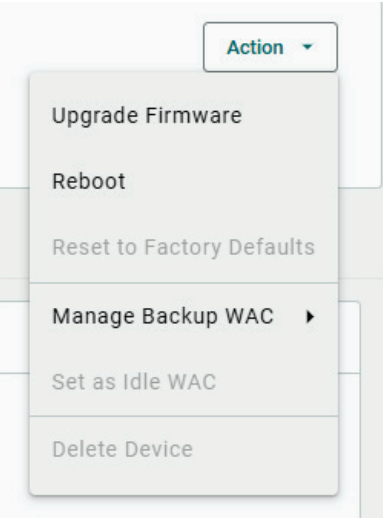
WAC Device Page

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.



Command Actions

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

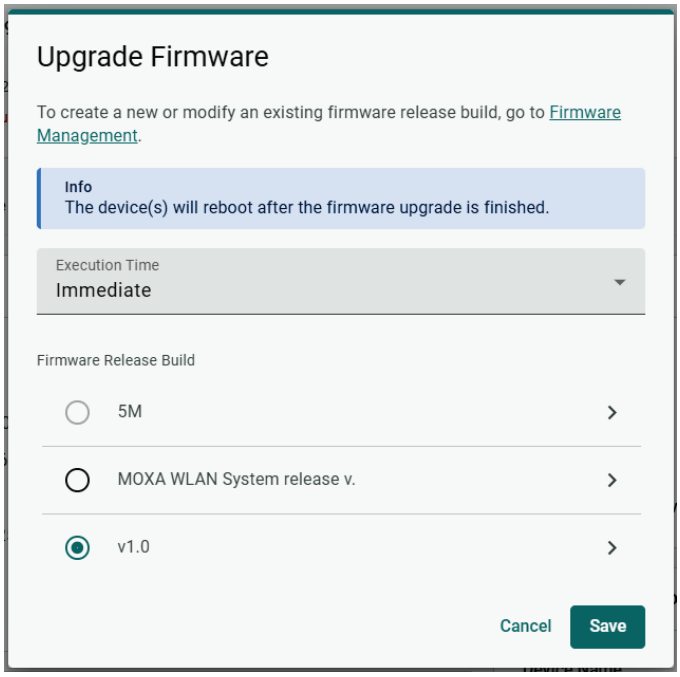


Upgrade Firmware

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

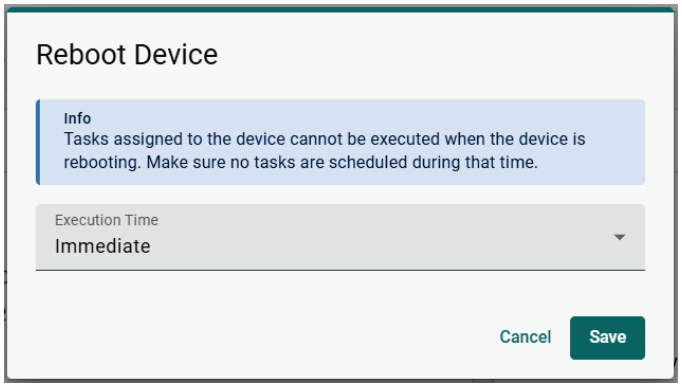
Firmware Release Build

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.	

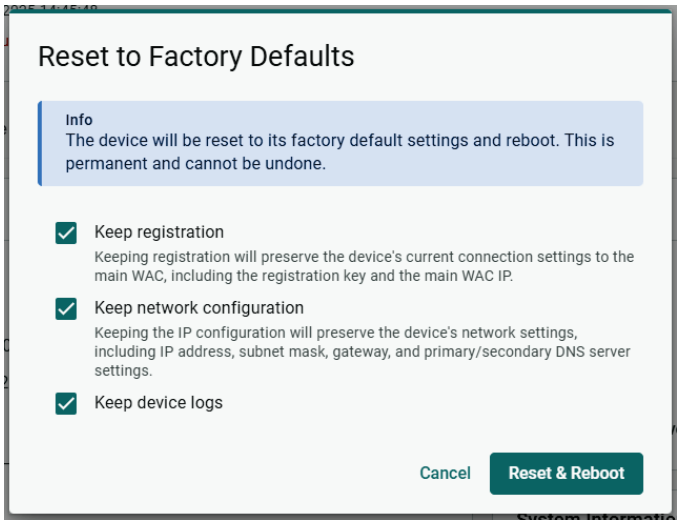
Date and Time (Scheduled Only)

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.

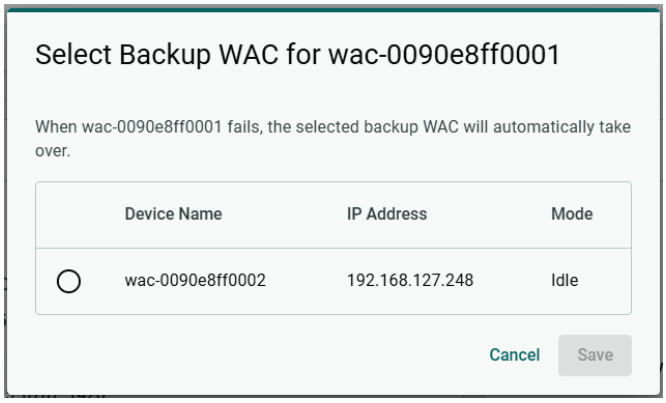
Available options depend on the current status and role of the device.

Assign a Backup WAC

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

NOTE

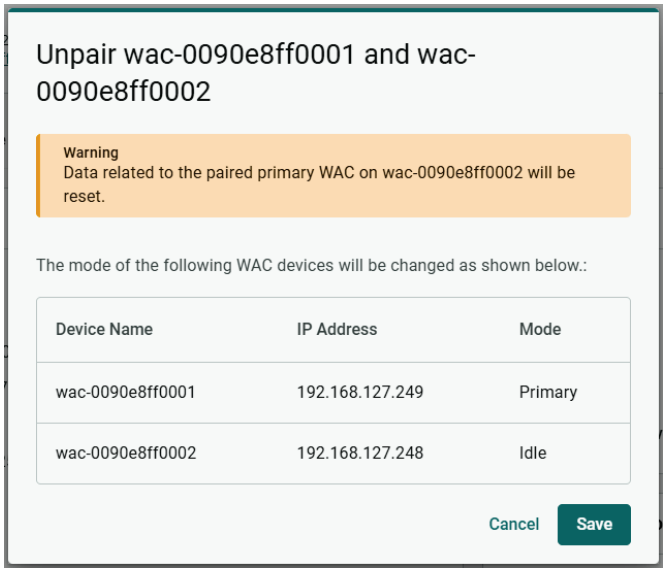
Only idle WAC devices can be assigned as a backup WAC. To designate a WAC device as idle, refer to Set as Idle WAC.



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

Unpair a Backup WAC

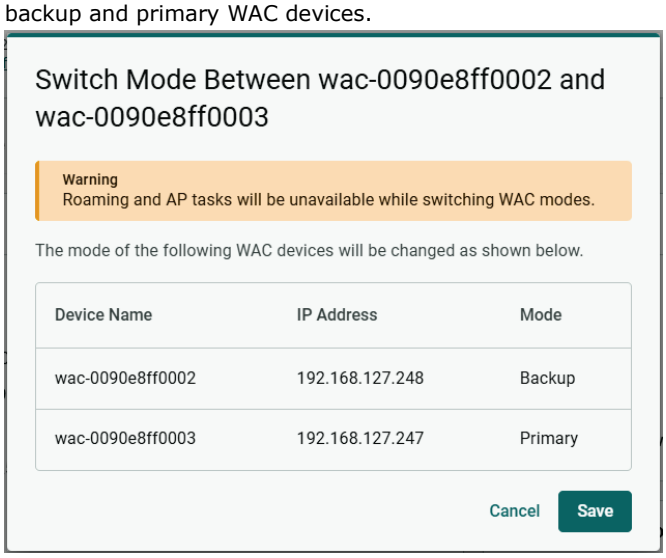
If a backup WAC is already assigned, click **Unpair** to unpair the backup WAC device. Once unpaired, the backup WAC will become idle.



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.



When finished, click **Save**.

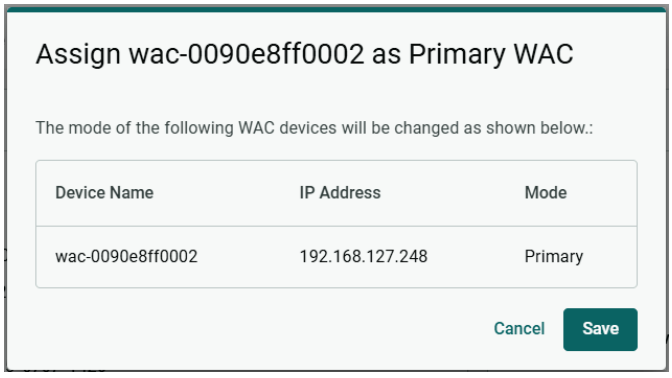
Set as Idle WAC

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.

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.



When finished, click **Save**.

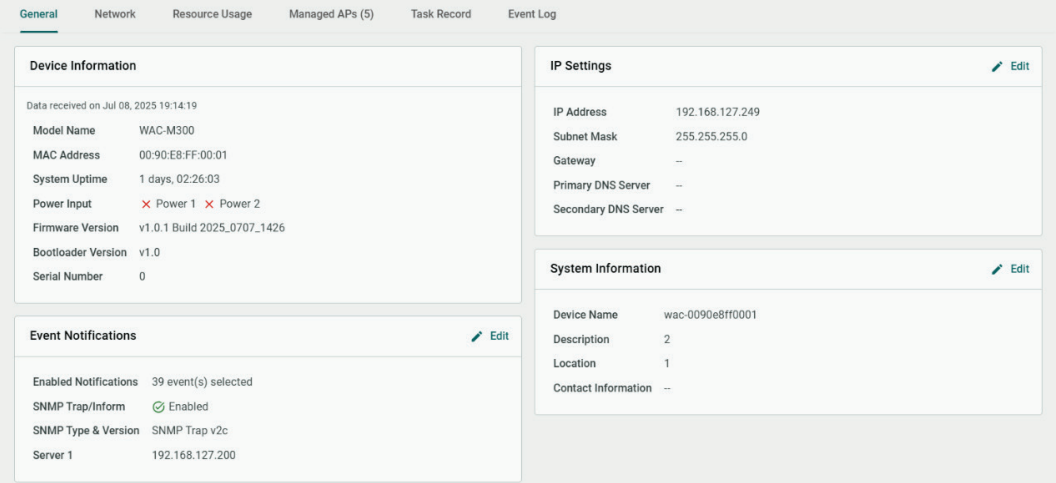
Delete Device

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.



Edit IP Settings

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

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.

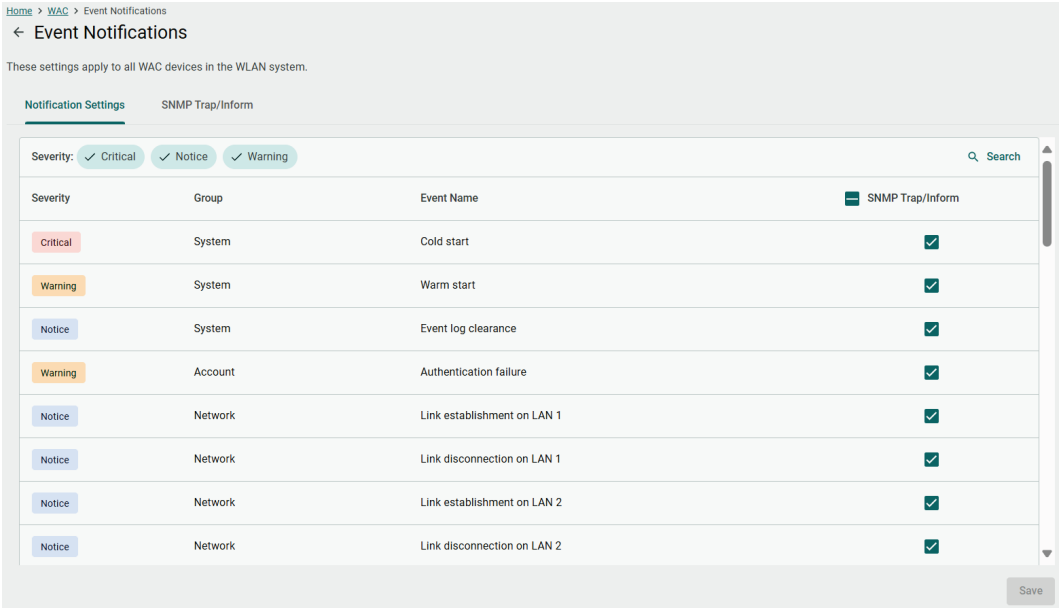
NOTE

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.

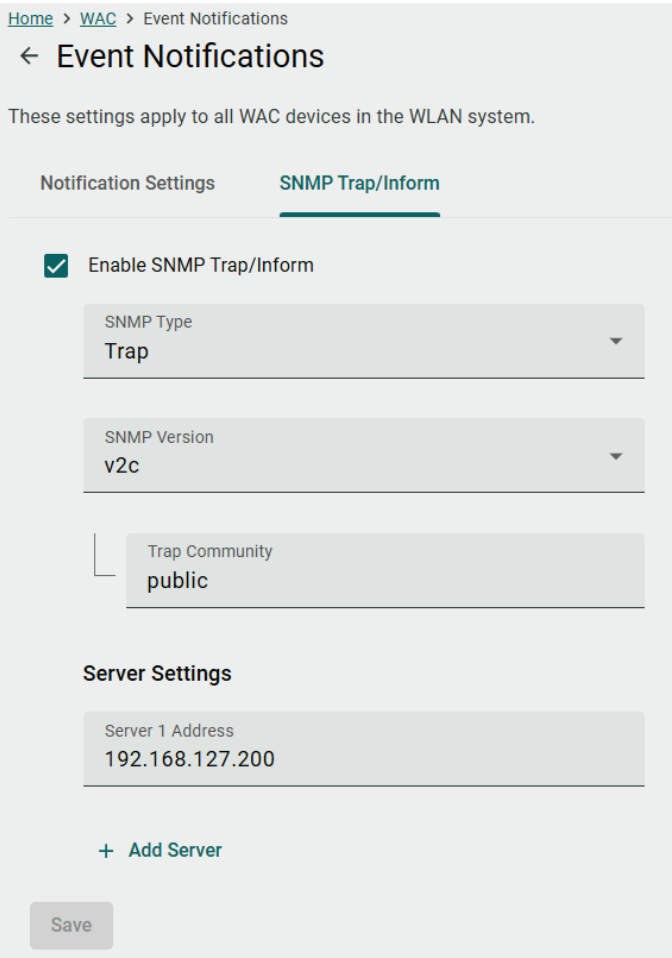
Check the **SNMP Trap/Inform** checkbox for the event(s) you want to receive notifications for.



When finished, click **Save**.

SNMP Trap/Inform

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



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

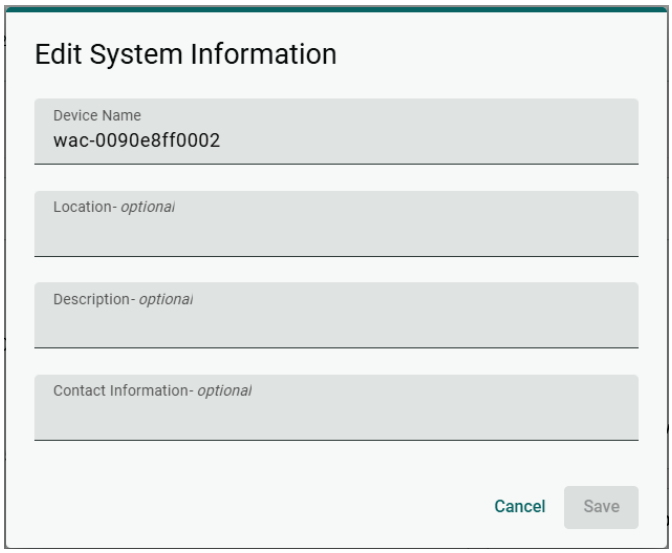
Server 1/2 Address

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.



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

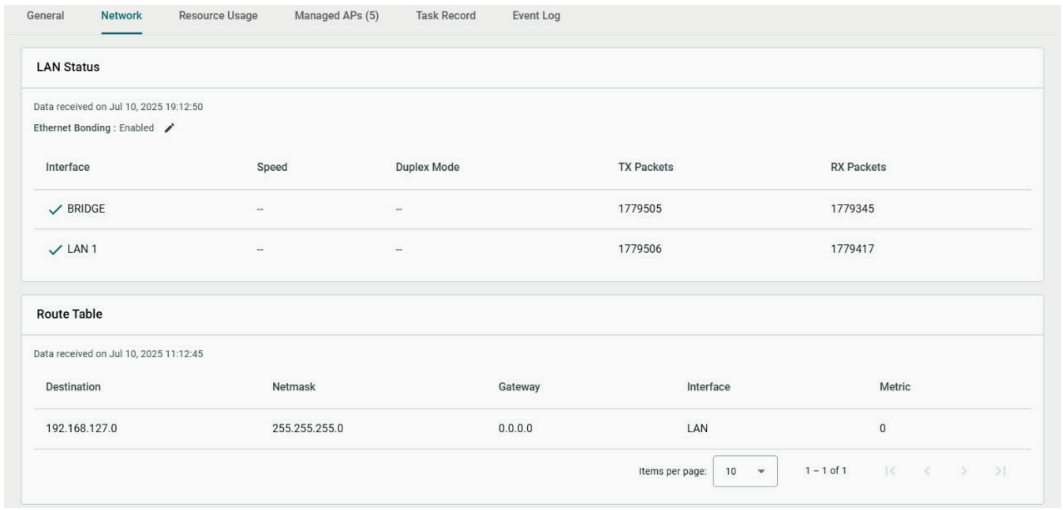
Contact Information - optional

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

When finished, click **Save**.

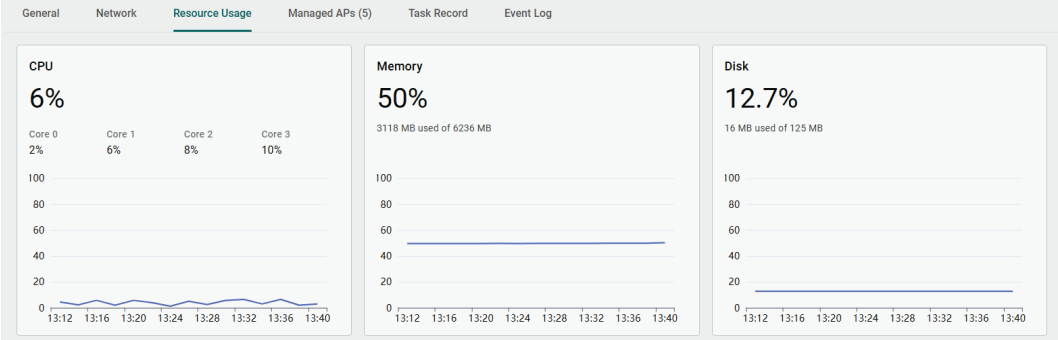
Network

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



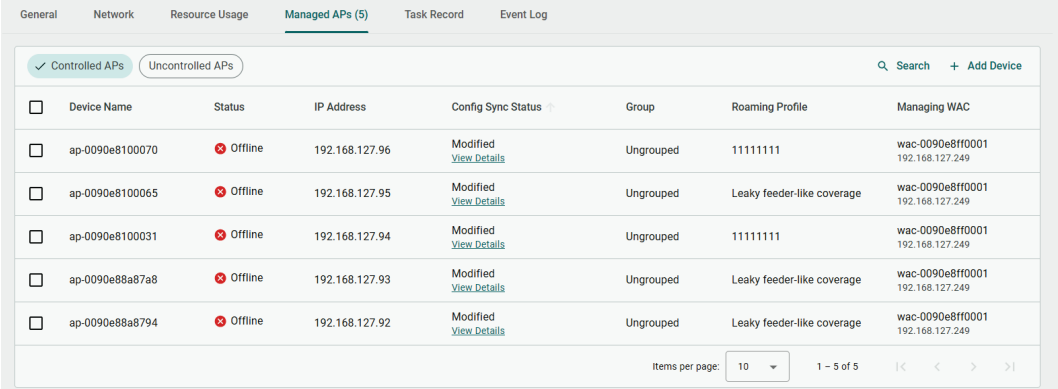
Resource Usage

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



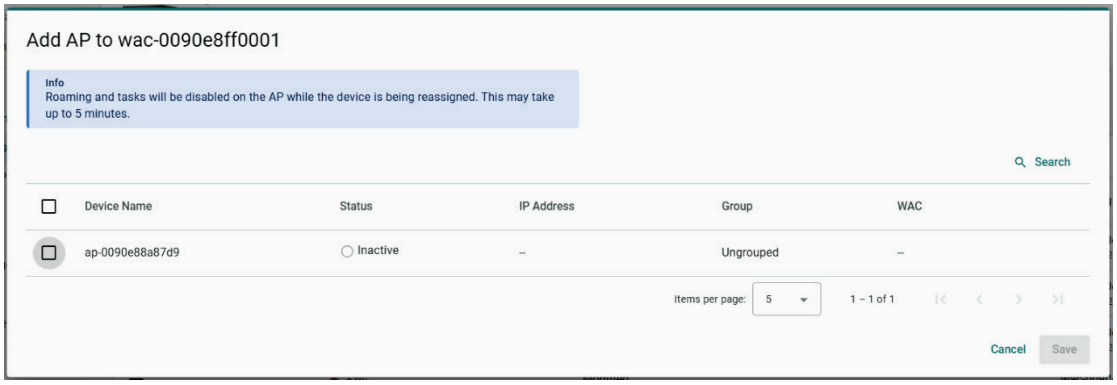
Managed APs

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



Add Managed AP

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

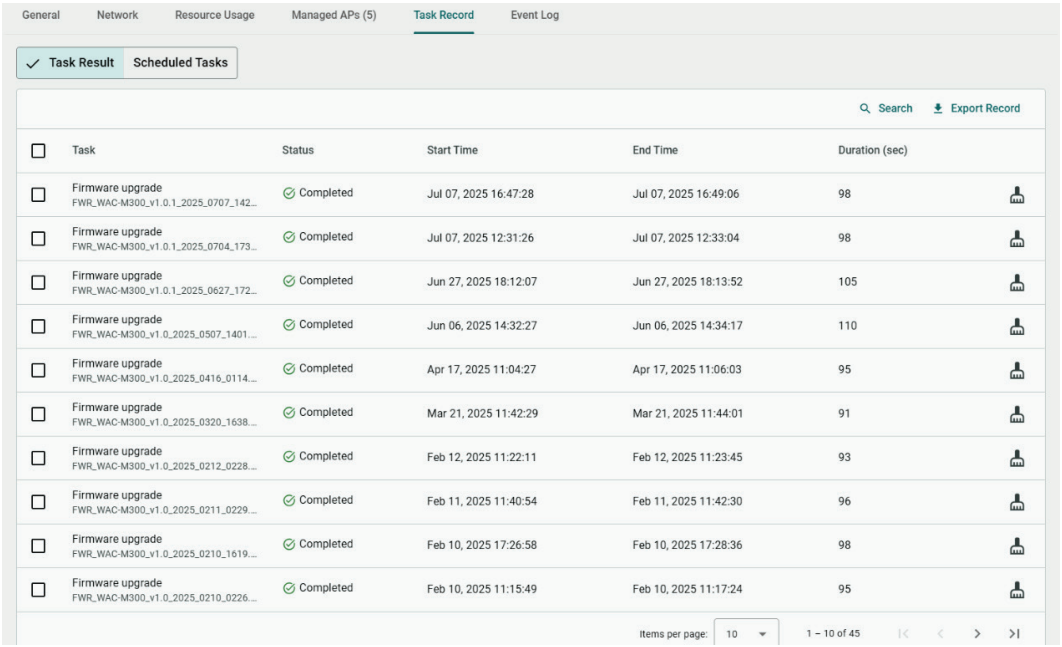


Check the box of the AP(s) you want to add.

When finished, click **Save**.

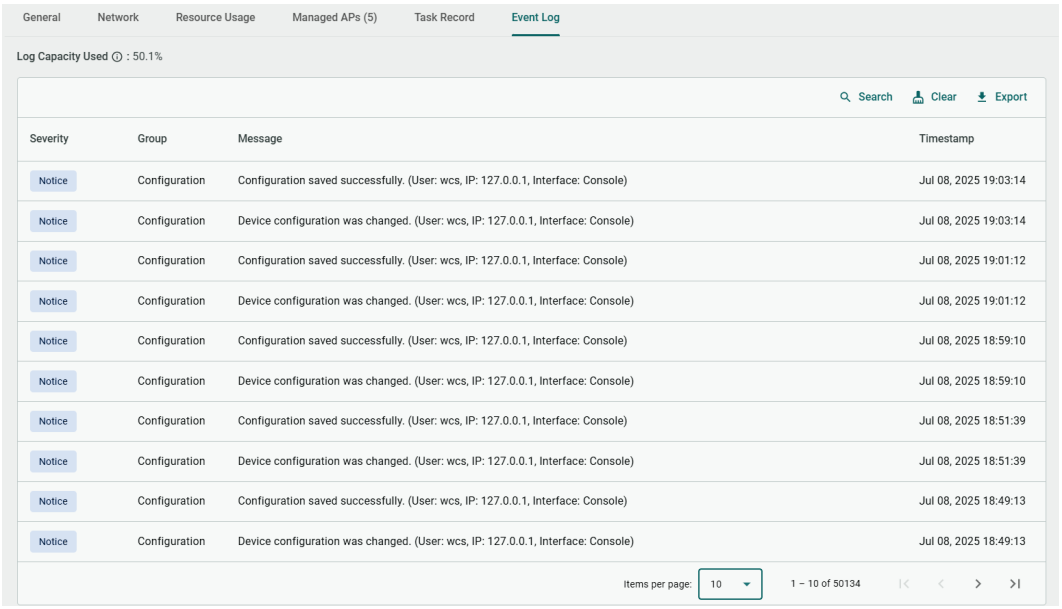
Task Record

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



Event Log

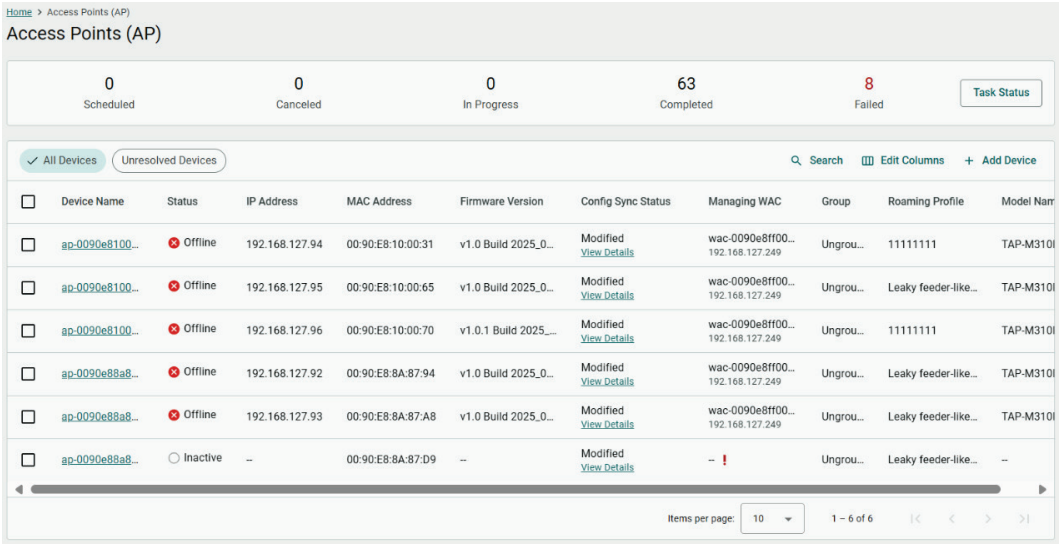
The **Event Log** tab shows a list of event logs recorded on the device.



Access Points (AP)

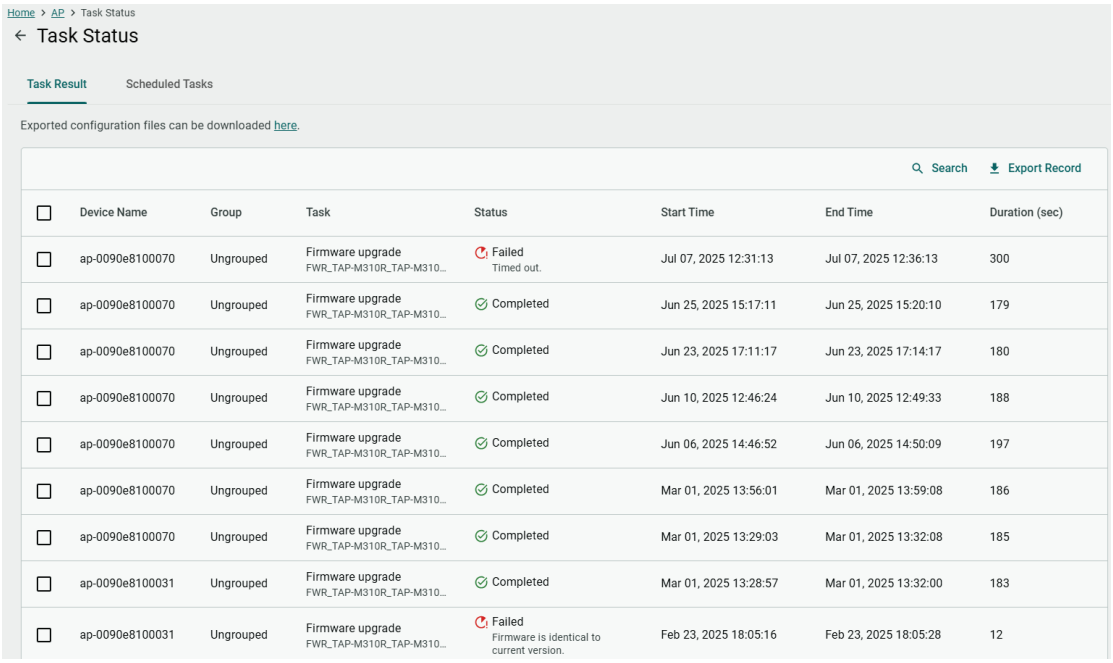
Menu Path: Device Management > Access Points (AP)

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



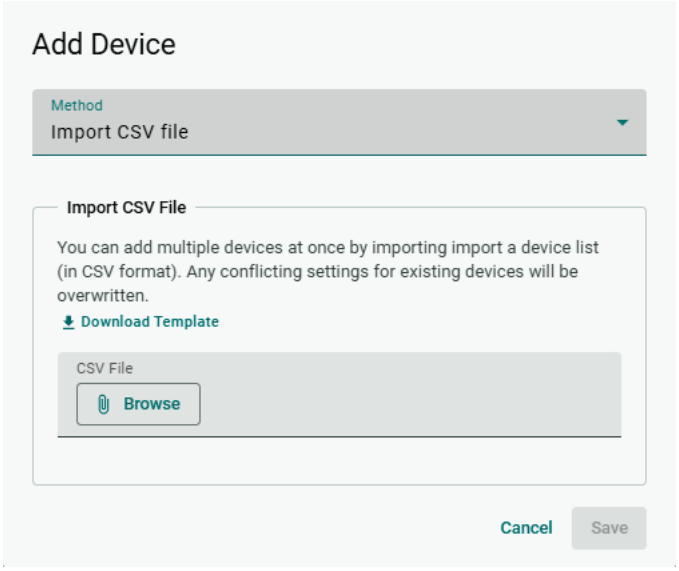
Task Status

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



Add an AP Device

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



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

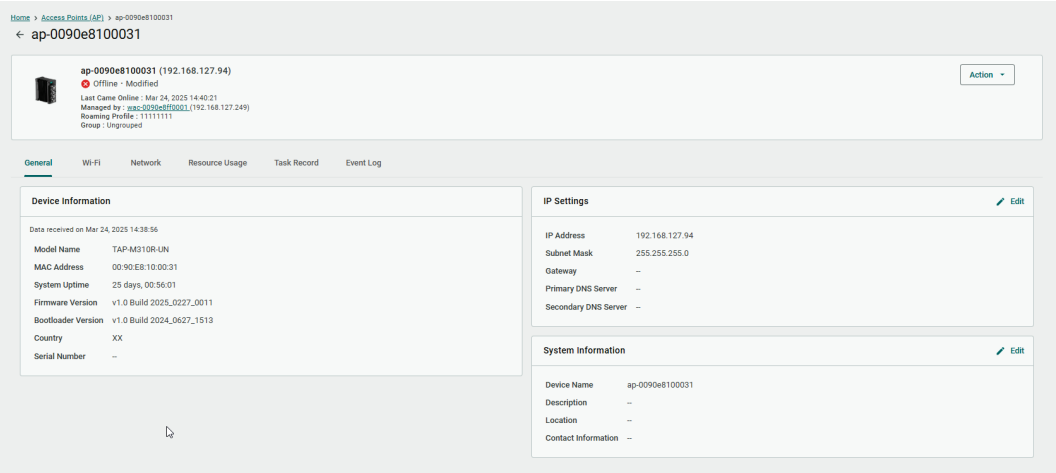
Group - optional (Manually Add Device Only)

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

When finished, click **Save**.

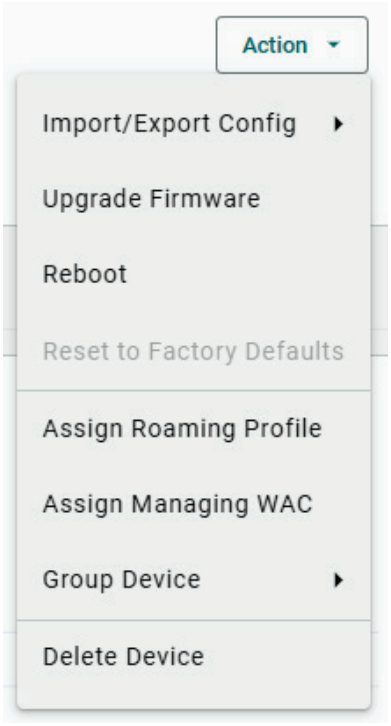
AP Device Page

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.



Command Actions

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

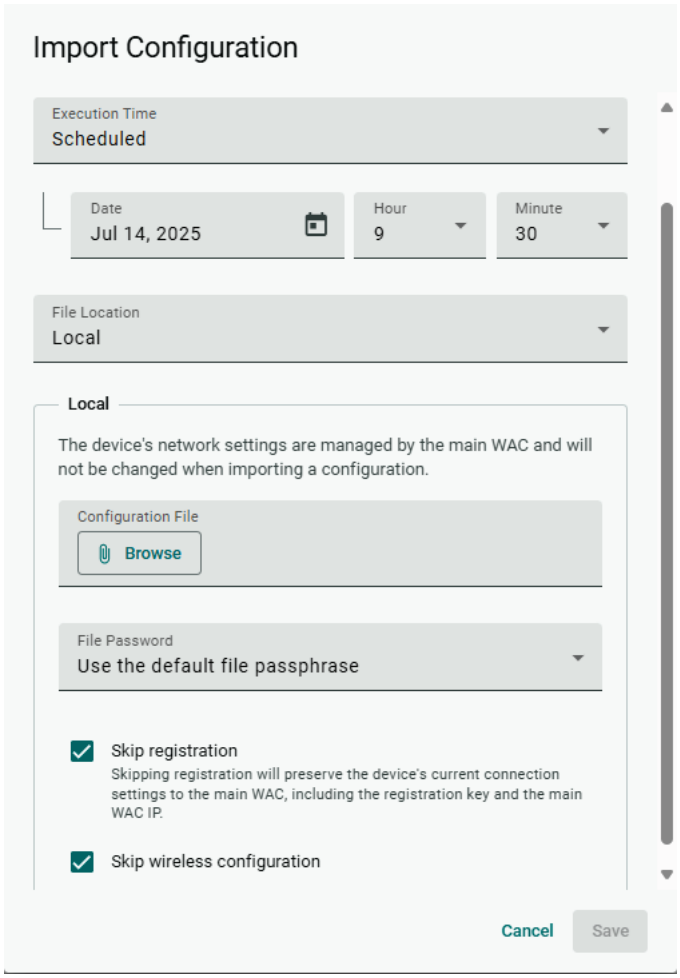


Import/Export Config

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.



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

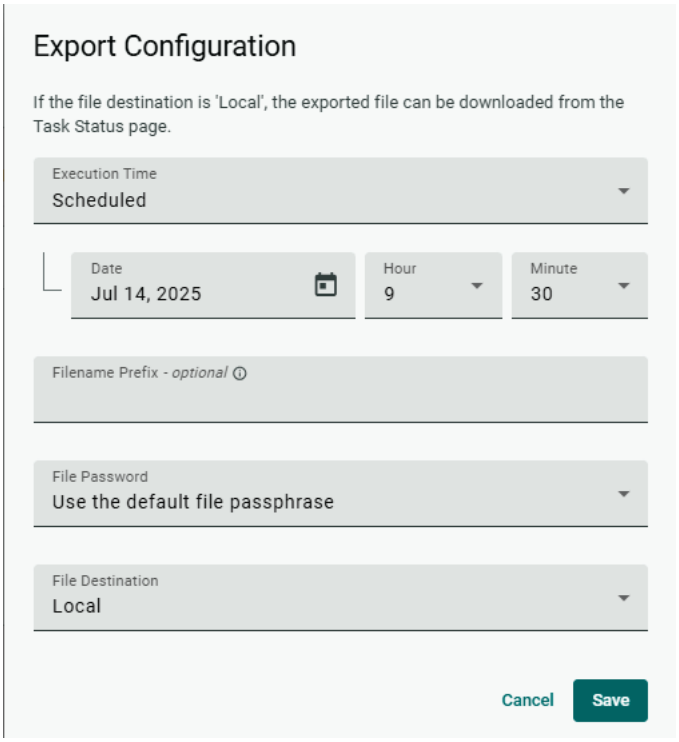
Skip wireless configuration

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.



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.

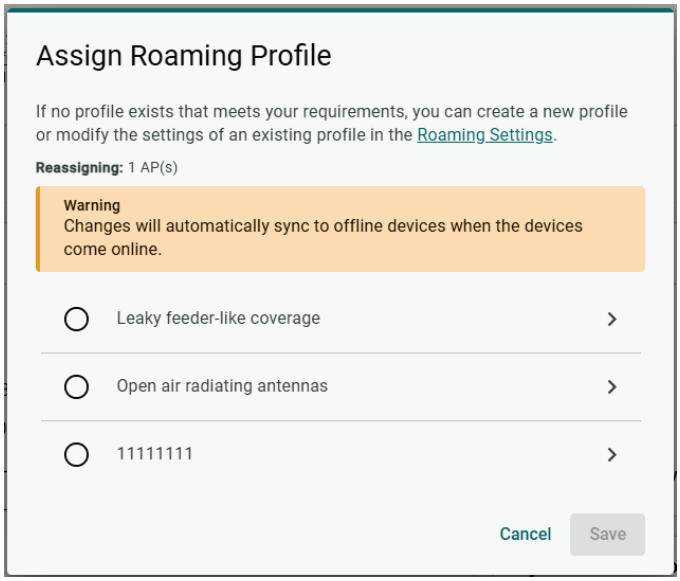
This process is the same as for WAC devices. Refer to Reset to Factory Defaults.

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.



Configure the following settings:

Roaming Profile

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

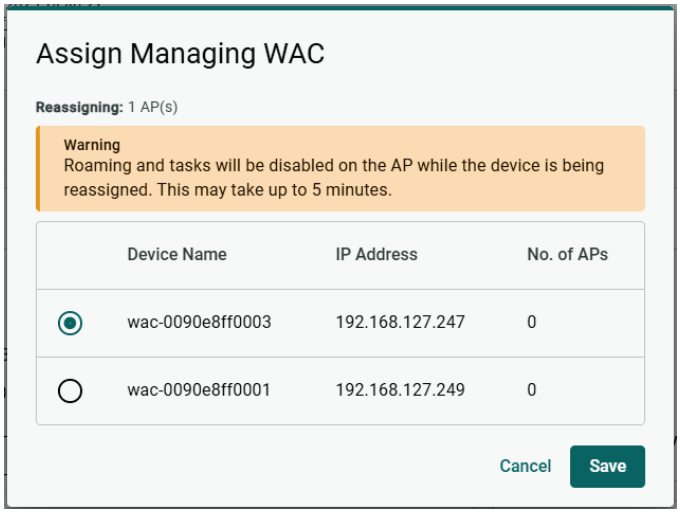
When finished, click **Save**.

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.



Configure the following settings:

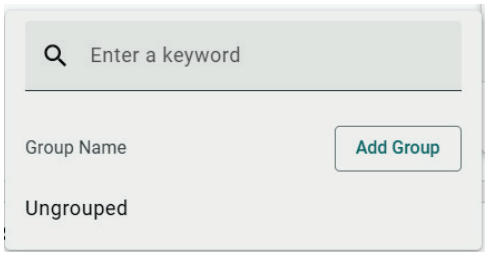
Managing WAC

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

When finished, click **Save**.

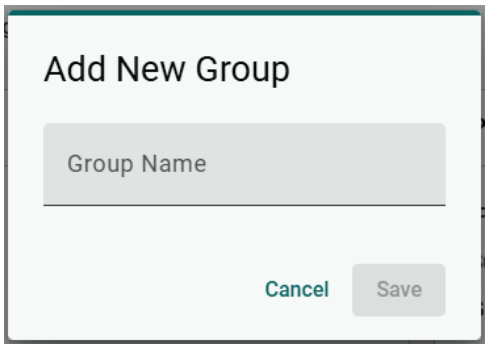
Group Device

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



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**.



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**.

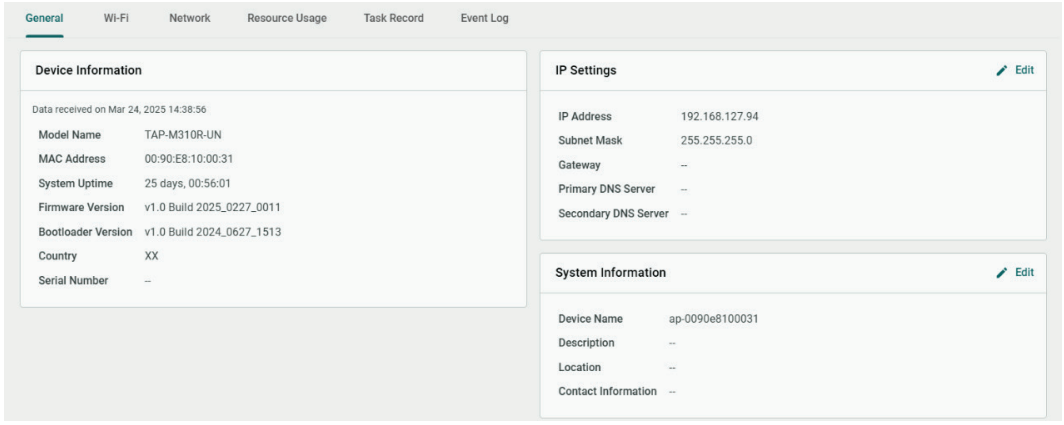
Delete Device

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.



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.

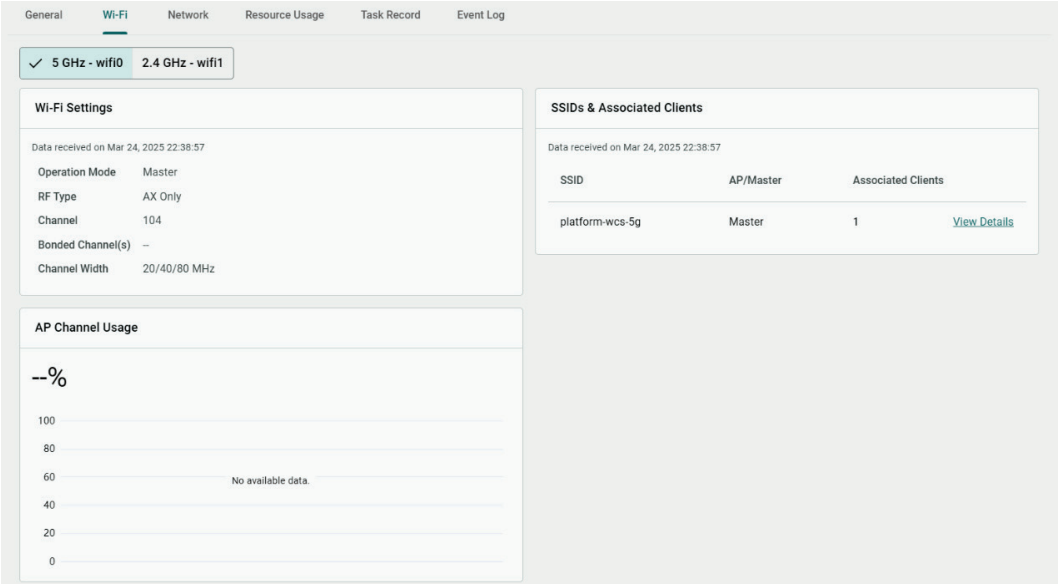
Edit System Information

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.

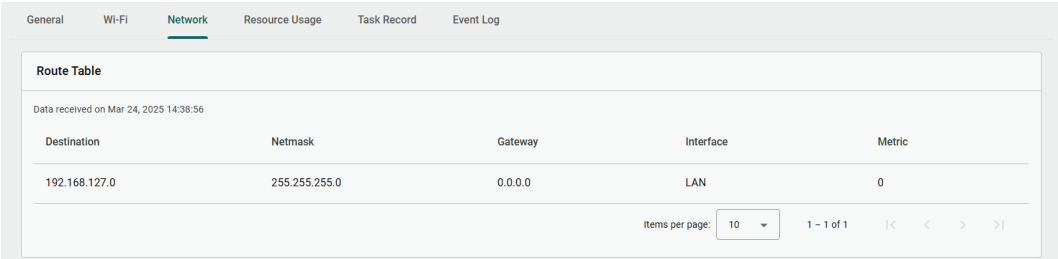
Wi-Fi

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.



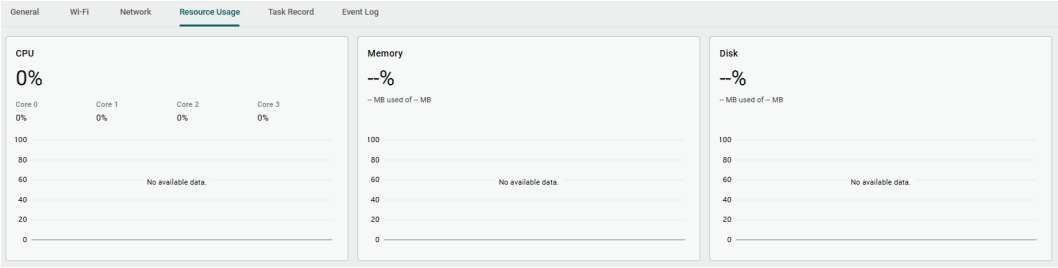
Network

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



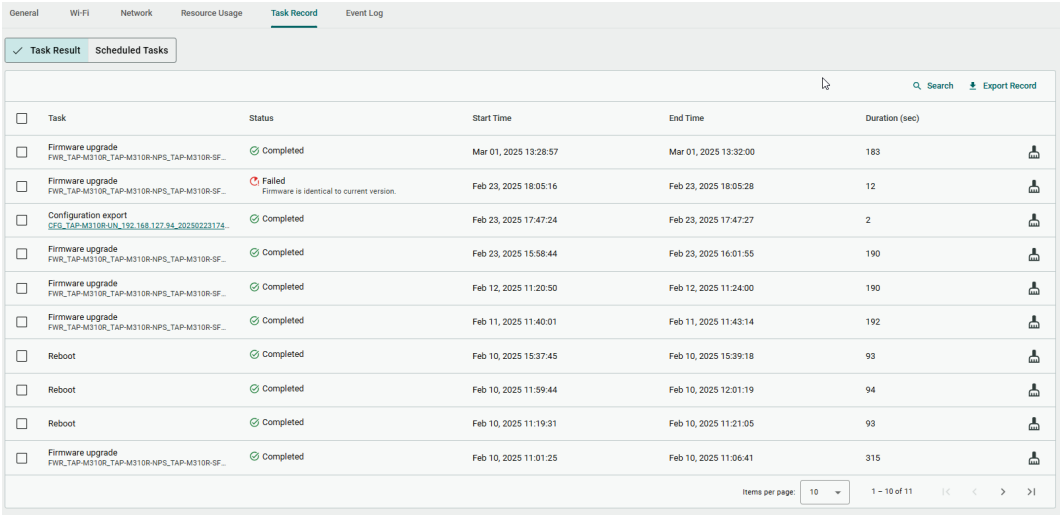
Resource Usage

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



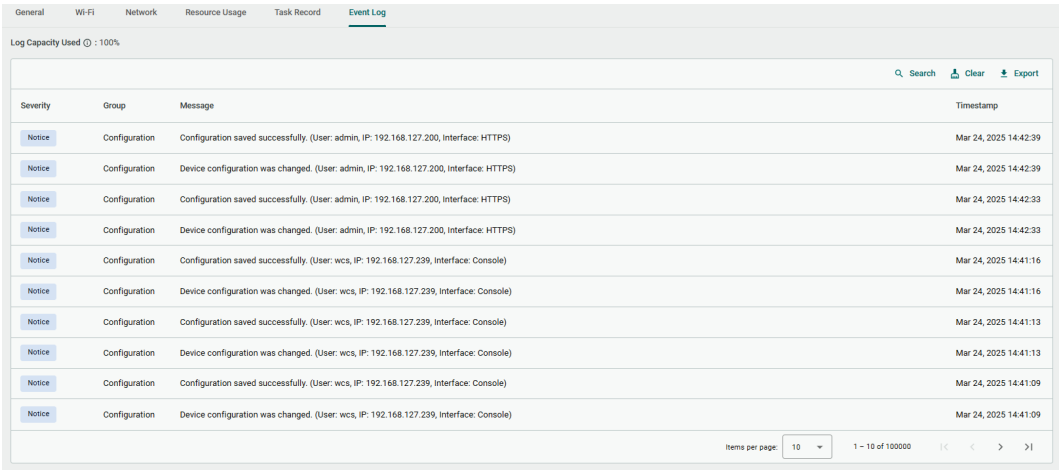
Task Record

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



Event Log

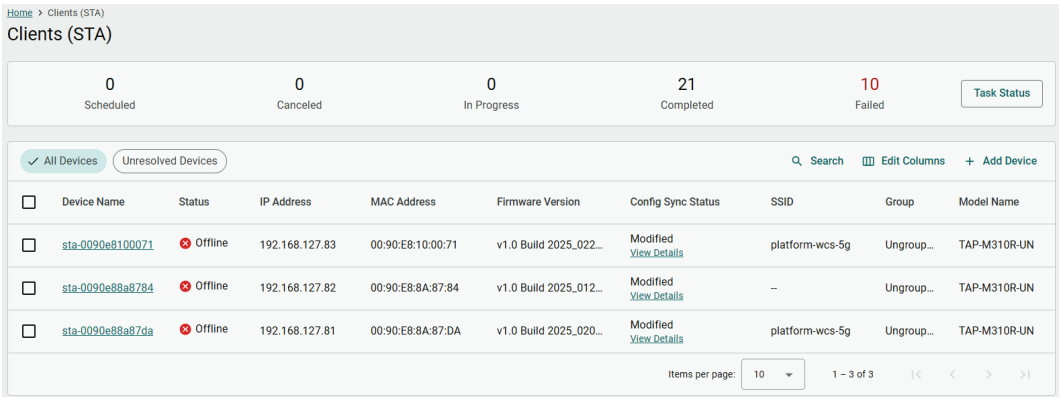
The **Event Log** tab shows a list of event logs recorded on the device.



Clients (STA)

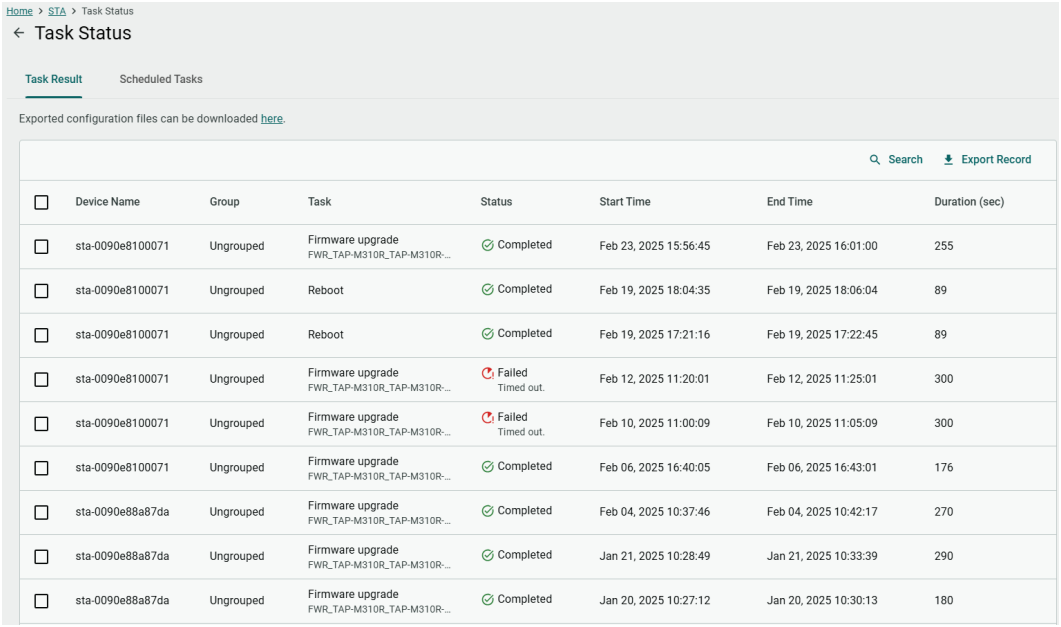
Menu Path: Device Management > Clients (STA)

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



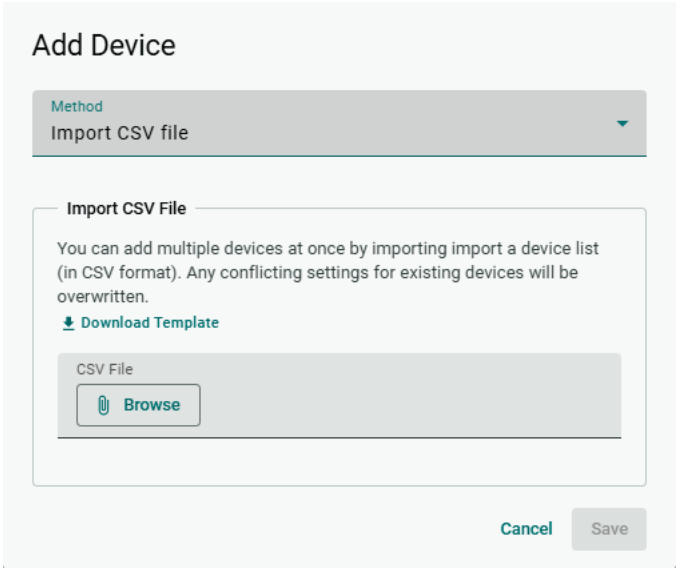
Task Status

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



Add a Client Device

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



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

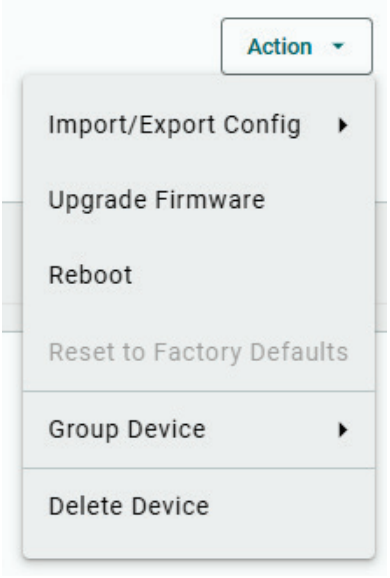
When finished, click **Save**.

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.

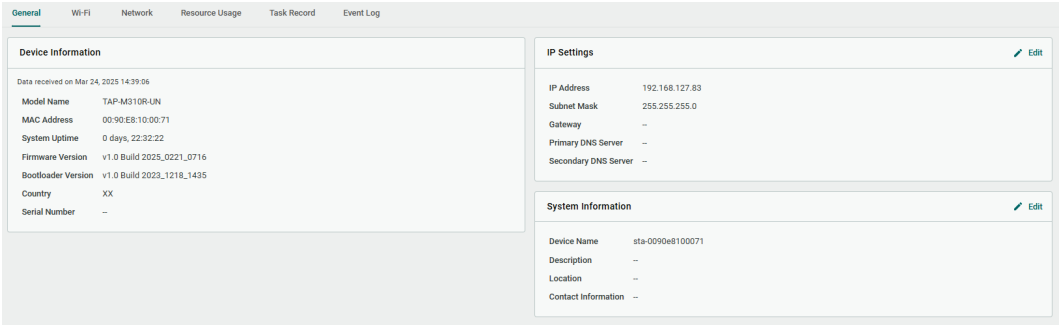
Delete Device

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.

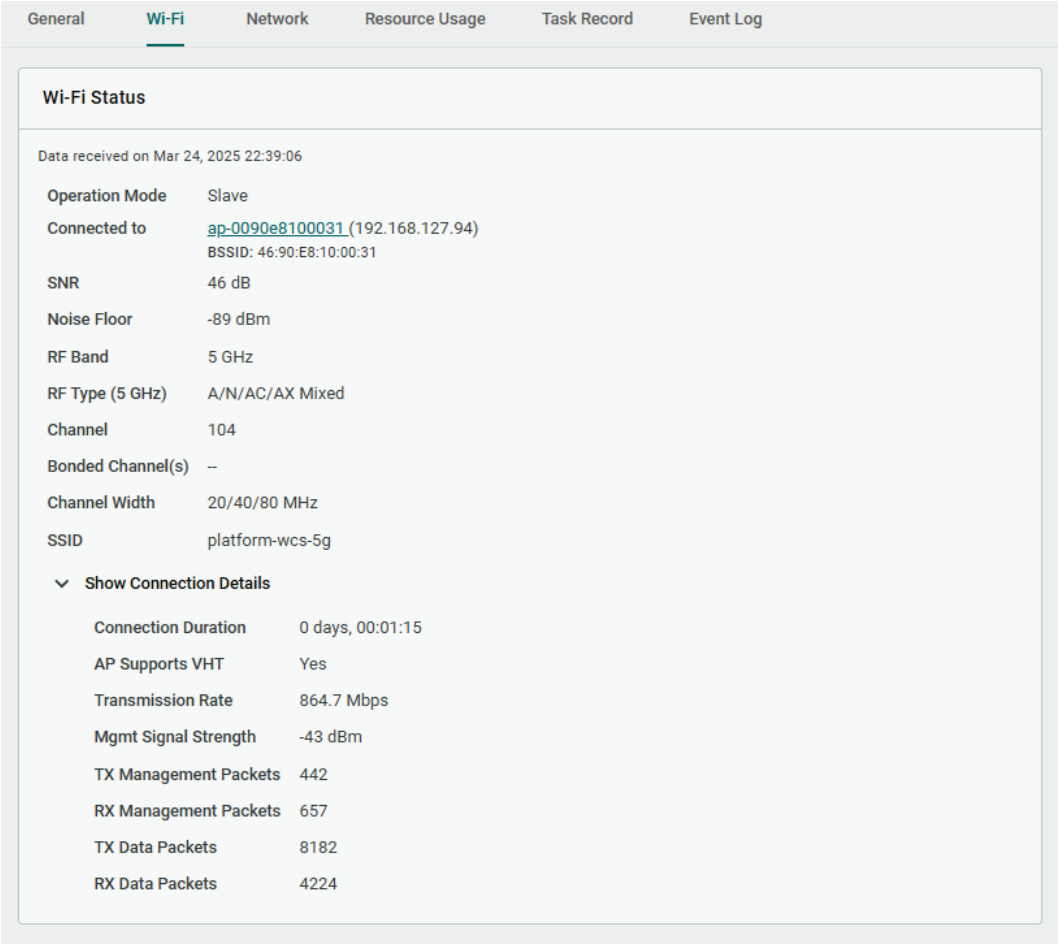
Edit System Information

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.

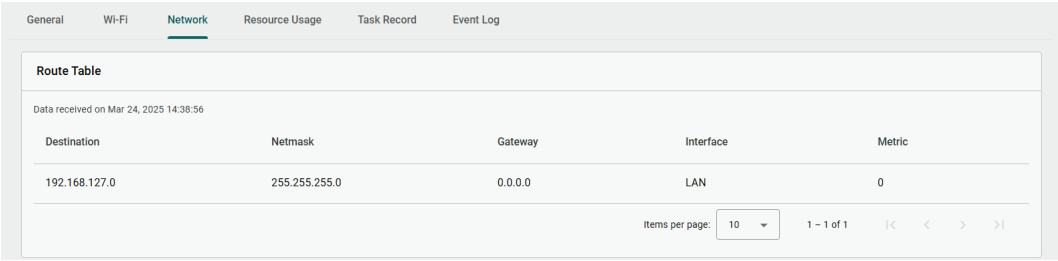
Wi-Fi

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



Network

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

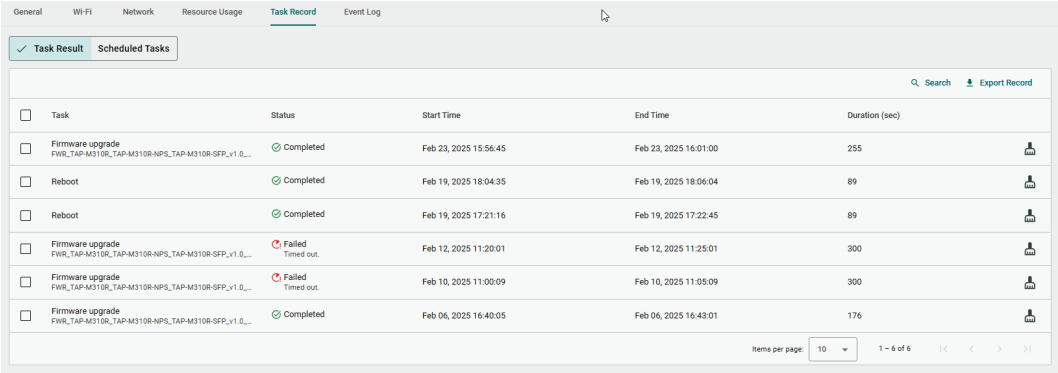


Resource Usage

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

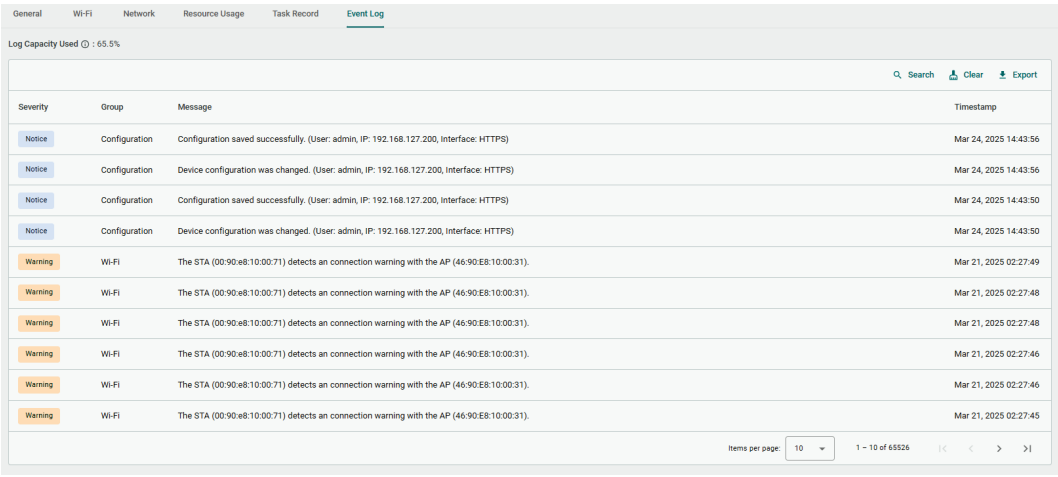
Task Record

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



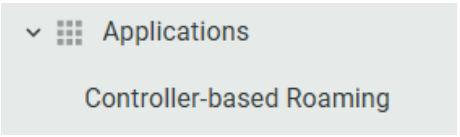
Event Log

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



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.

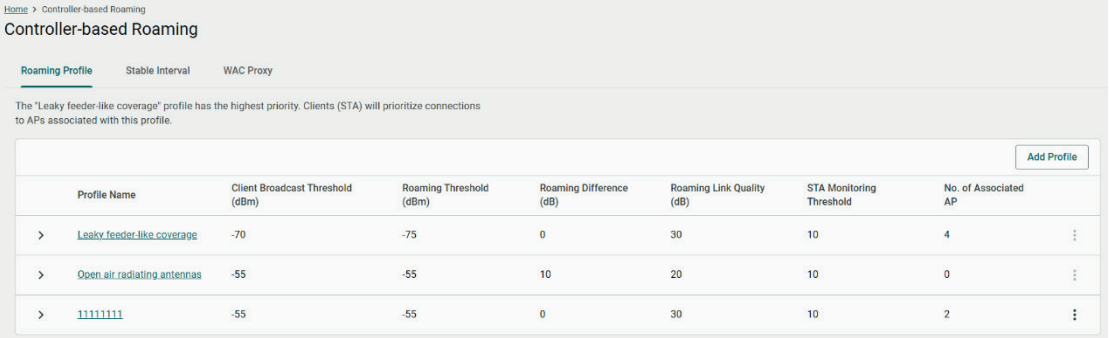
Roaming Profile

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

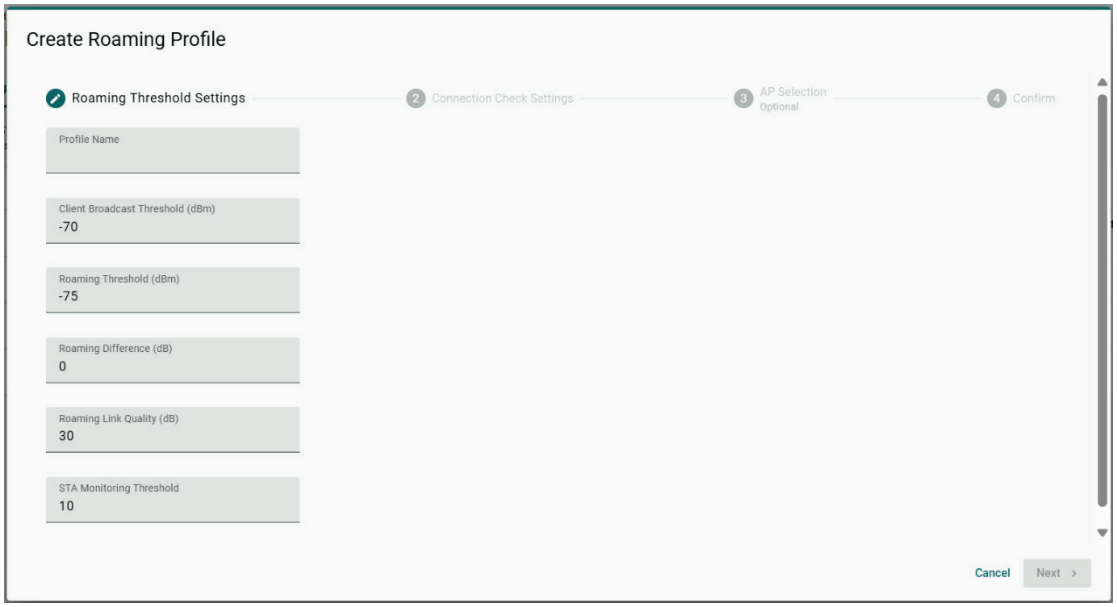
The "Leaky feeder-like coverage" and "Open air radiating antennas" profiles are default profiles and cannot be modified or deleted.

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



Create a New Roaming Profile

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



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

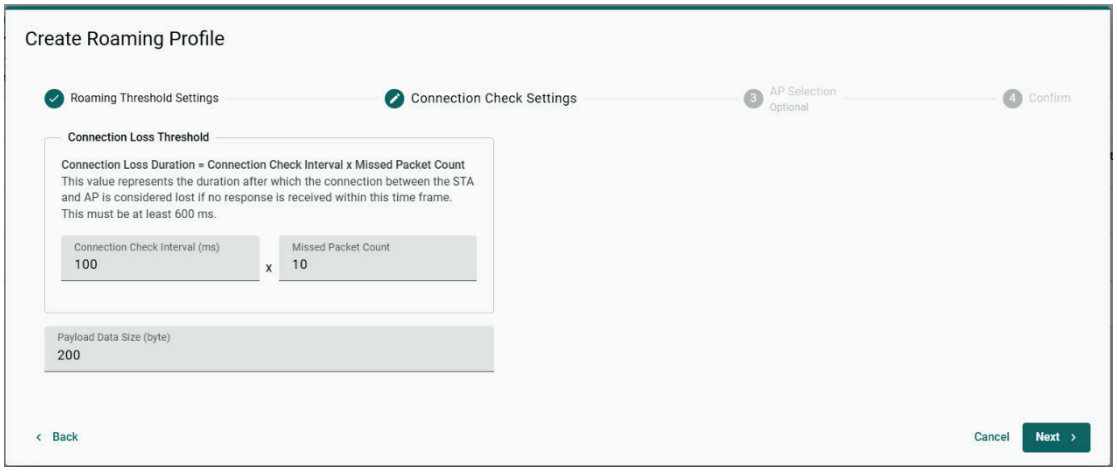
Roaming Link Quality

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

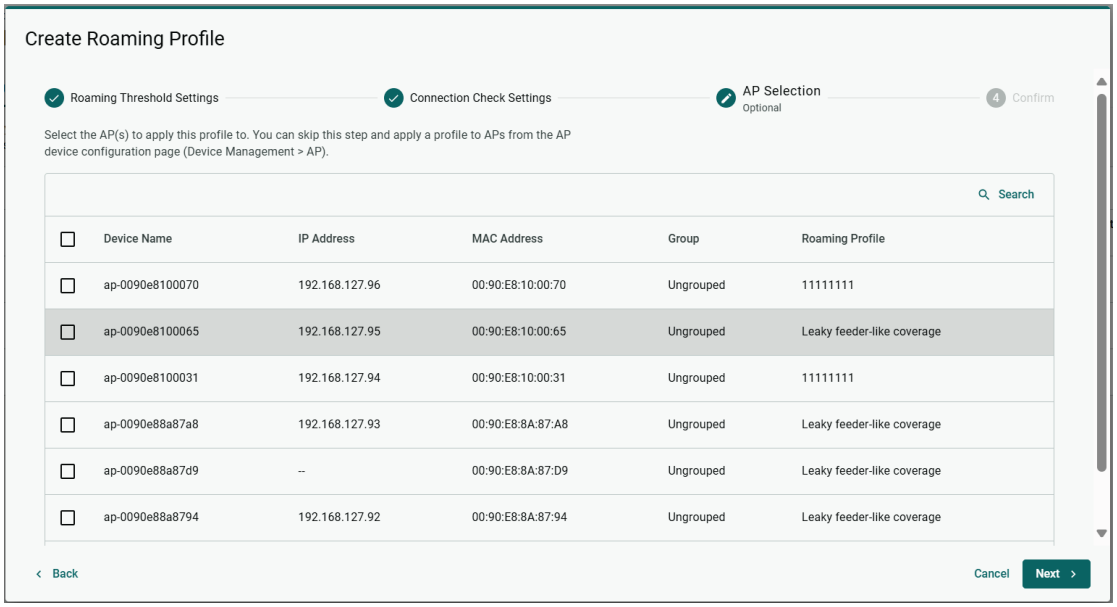
Missed Packet Count

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

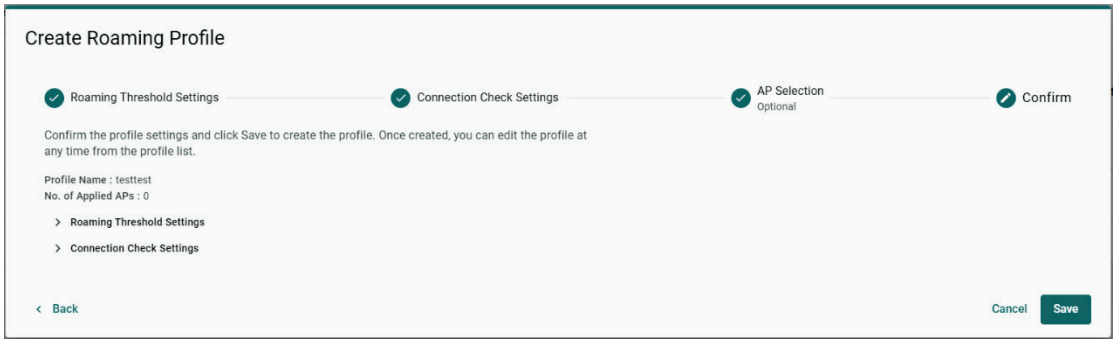
Setting	Description	Factory Default
200 to 1000 (byte)	Specify the size of data packets sent during connection alive checks.	200

When finished, click **Next**.



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**.



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.

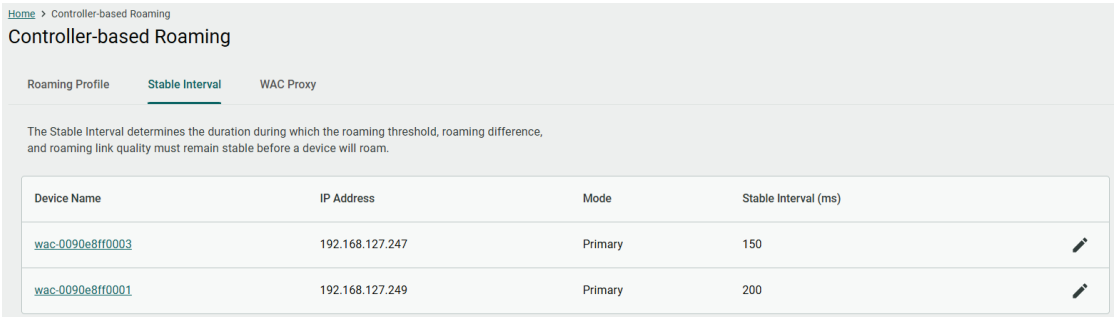
Click the **menu** (⋮) icon next to the profile you want to delete and click **Delete**.

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.



Edit the Stable Interval

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

Configure the following settings:

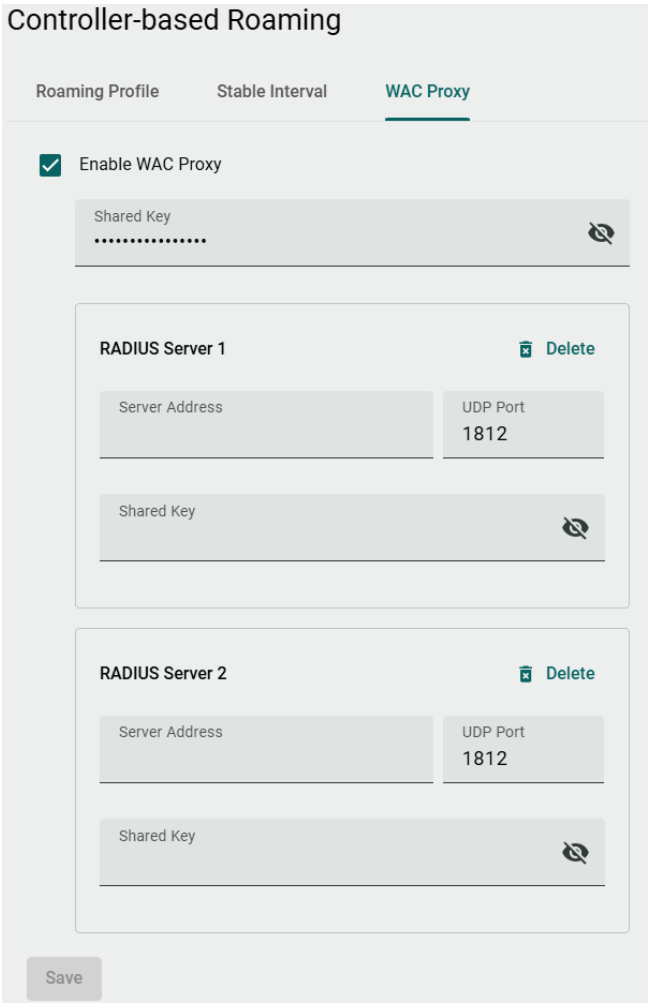
Stable Interval

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.



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)

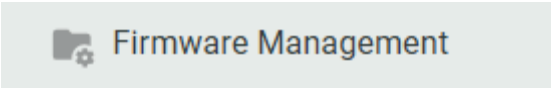
Setting	Description	Factory Default
1 to 65535	Specify the UDP port of the RADIUS server.	1812

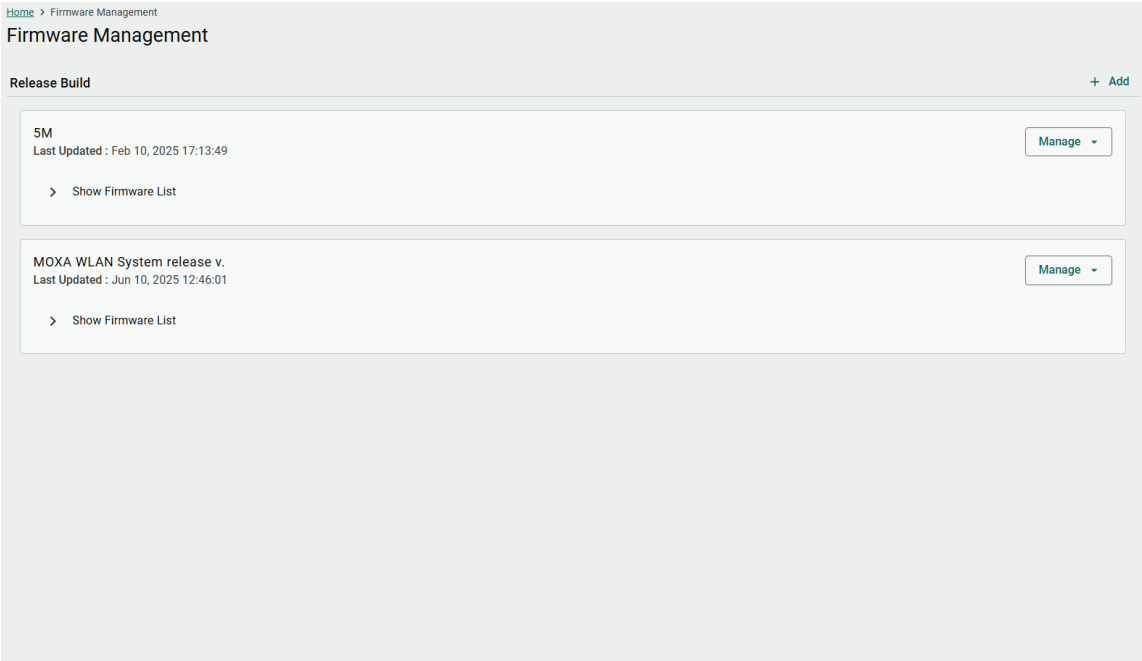
When finished, click **Save**.

Firmware Management

Menu Path: Firmware Management

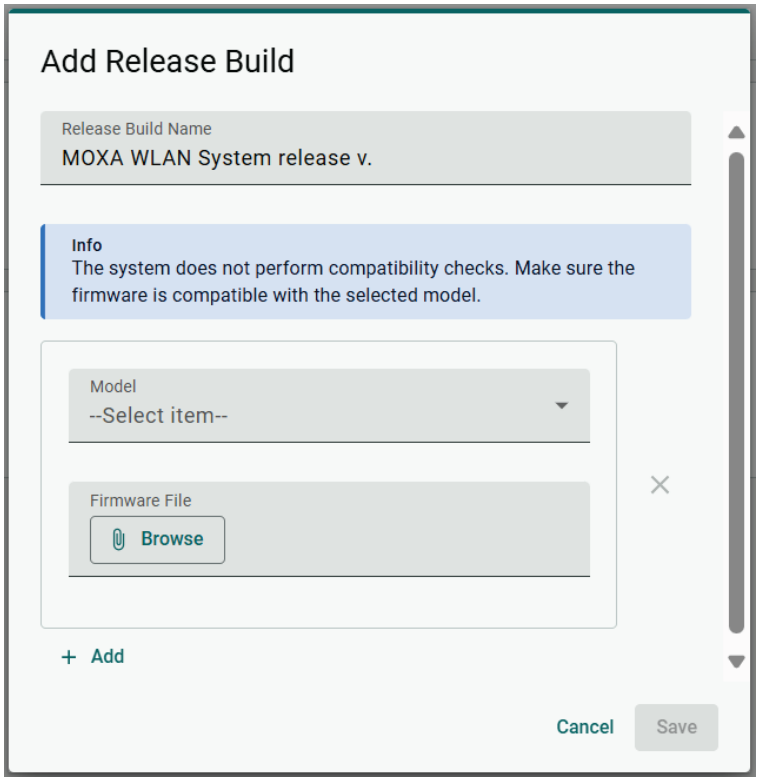
The **Firmware Management** page allows you to create new release builds, upload firmware files, and select compatible device models.





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

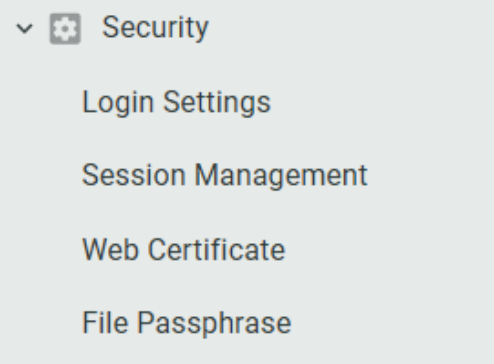
The system will not perform a compatibility check on the uploaded firmware file. To avoid issues, make sure the uploaded firmware file is compatible with the selected product model(s).

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 Passphrase** settings.



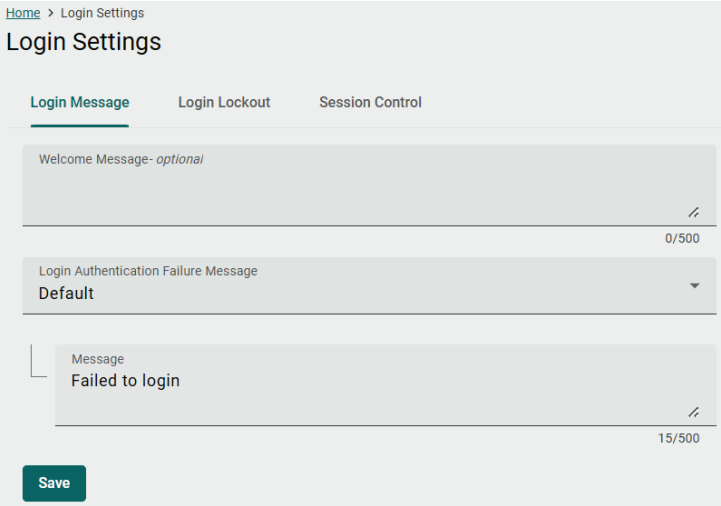
Login Settings

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.	

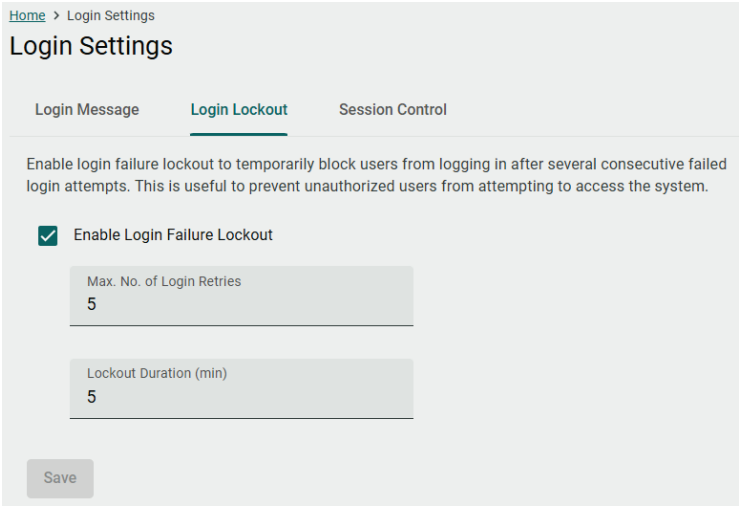
Message (Custom Only)

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.



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

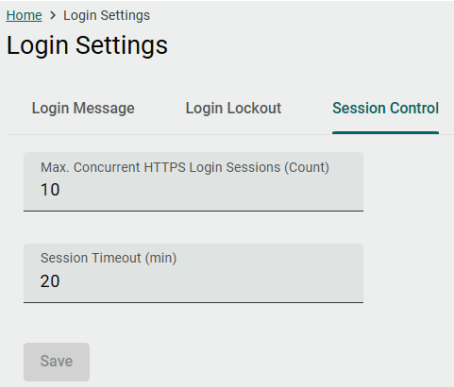
Lockout Duration (min)

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

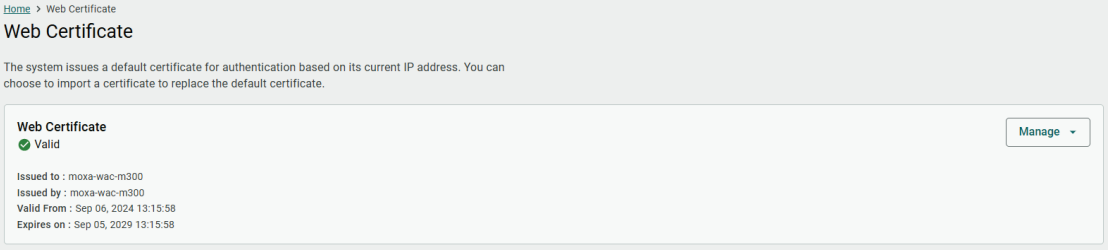
From the **Session Management** screen, you can view the login sessions of all enabled user accounts and can manually terminate active sessions.

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.

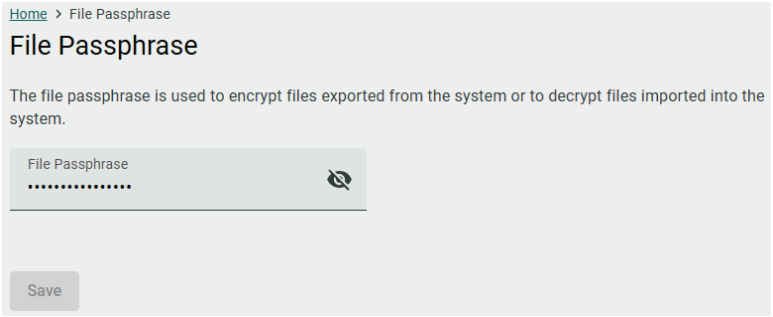
To import a new certificate, click **Manage > Import Certificate** and browse to the web certificate file on the local host.

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.



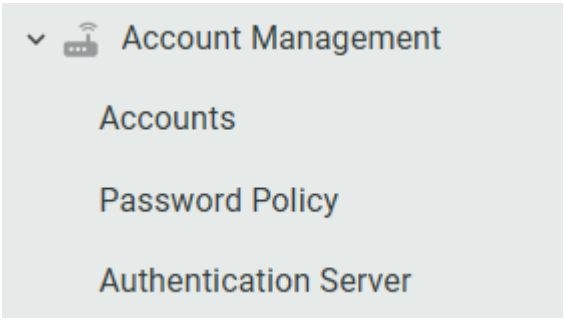
File Passphrase

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.



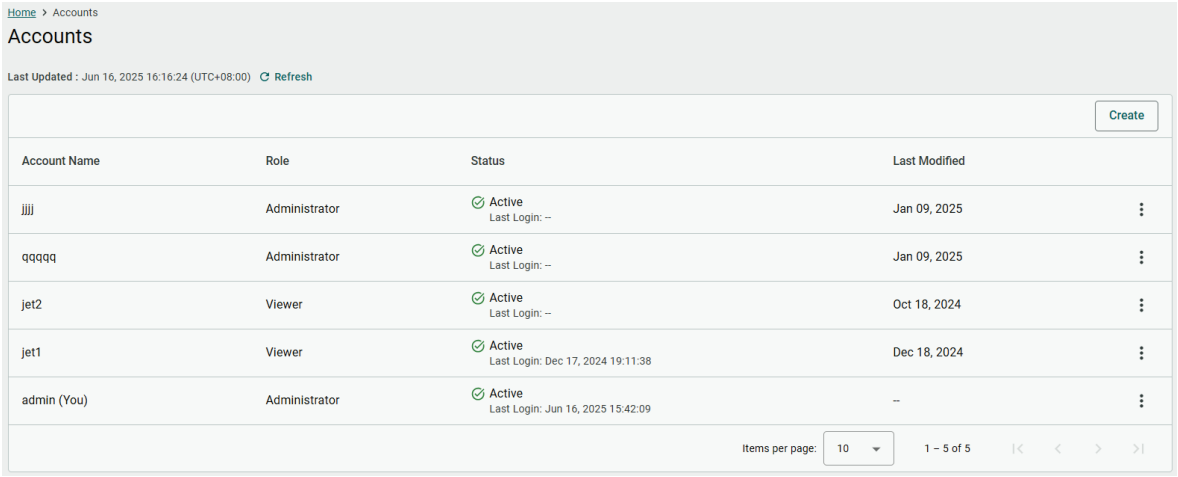
Accounts

Menu Path: Account Management > Accounts

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

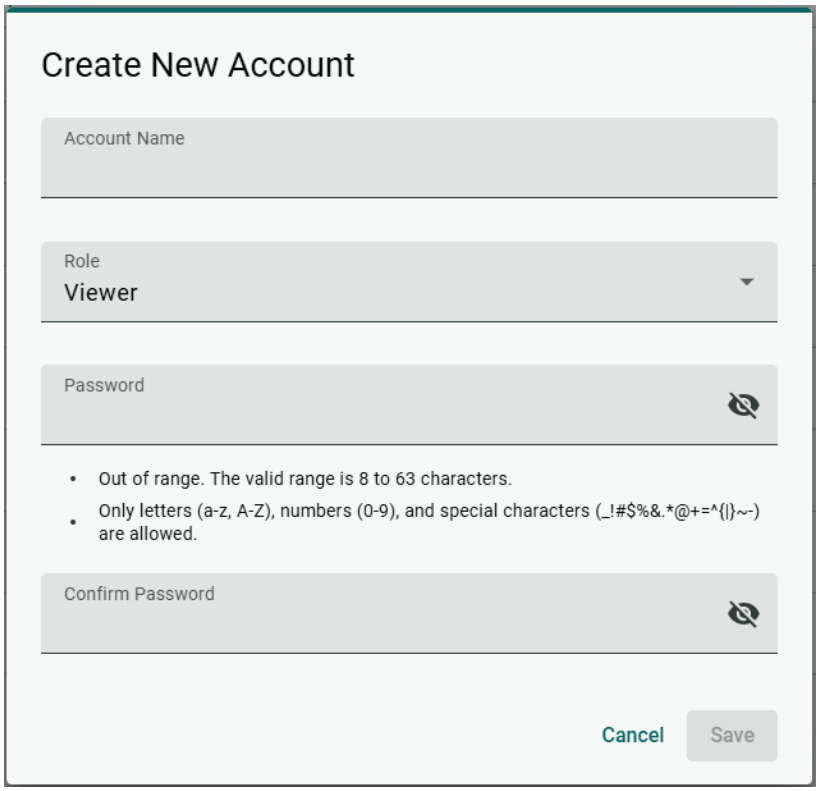
NOTE

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



Create a New Account

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



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.

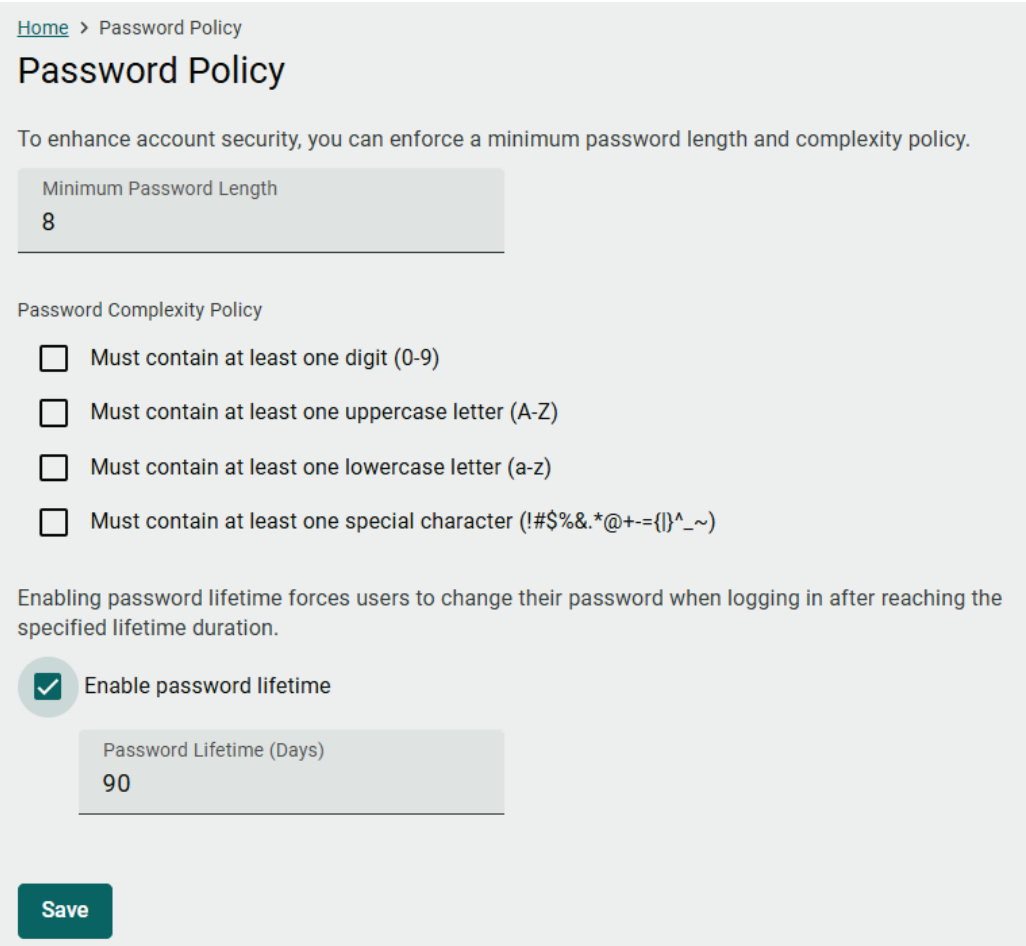
Click the **Menu** ( ) icon next to the account you want to delete and click **Delete**.

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.



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**.

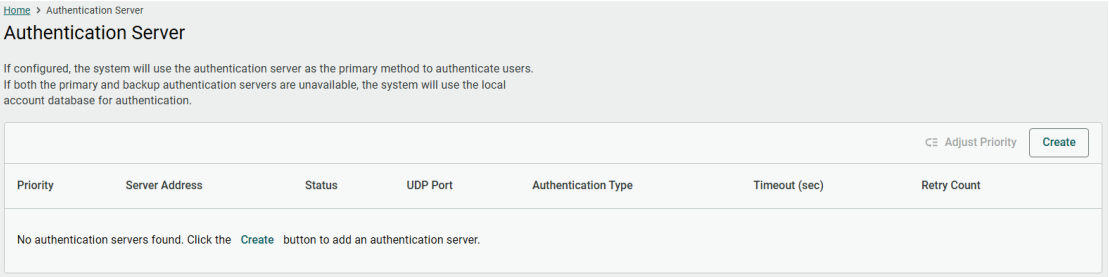
Authentication Server

Menu Path: Account Management > Authentication Server

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

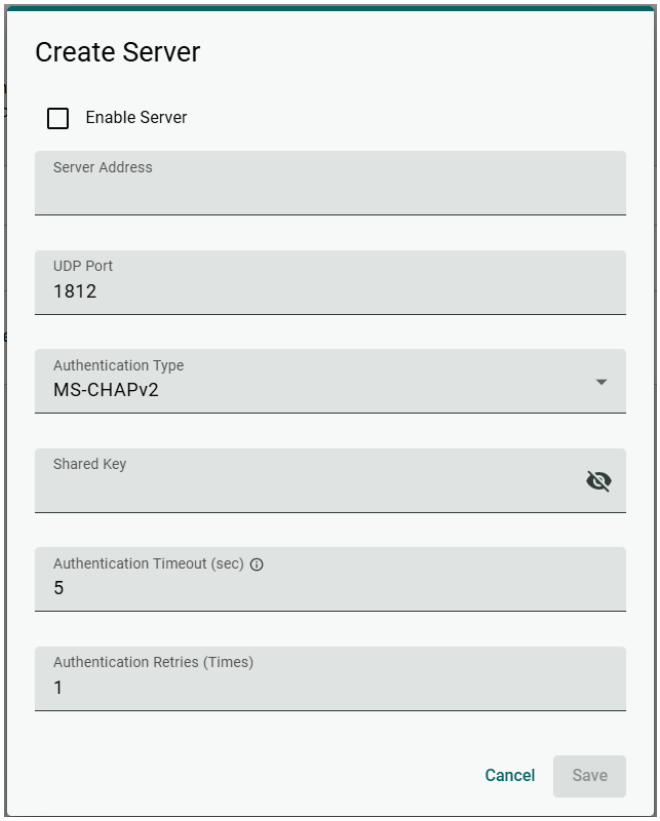
NOTE

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



Add an Authentication Server

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



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)

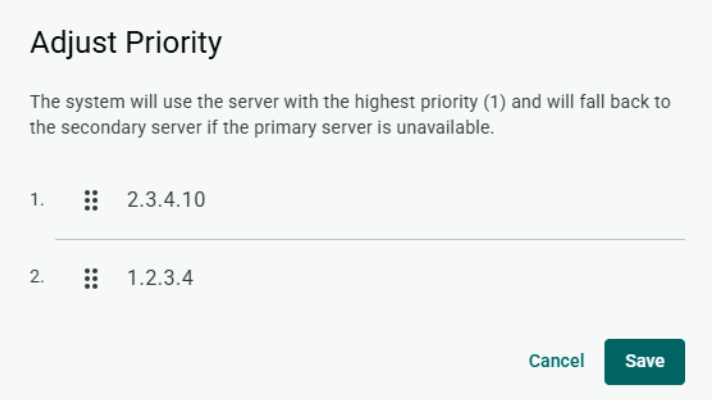
Setting	Description	Factory Default
0 to 5	Specify the number of times the device will attempt to authenticate with the RADIUS server if no response is received.	1

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**.



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**.

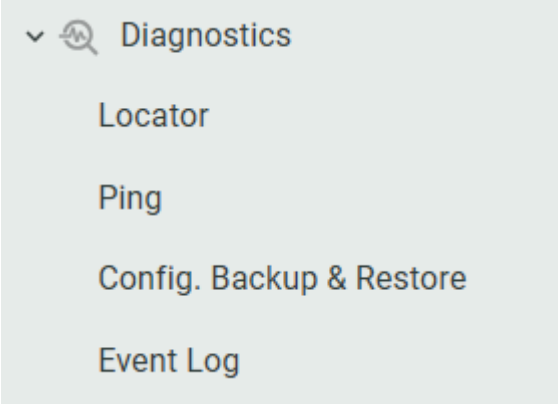
Delete an Authentication Server

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.

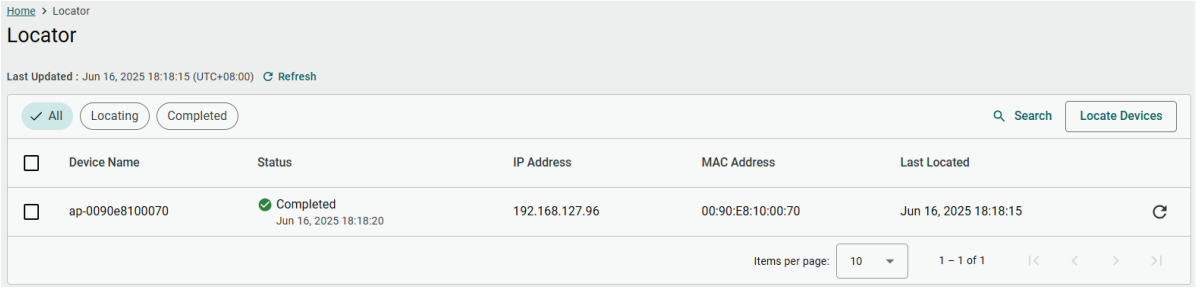


Locator

Menu Path: Diagnostics > Locator

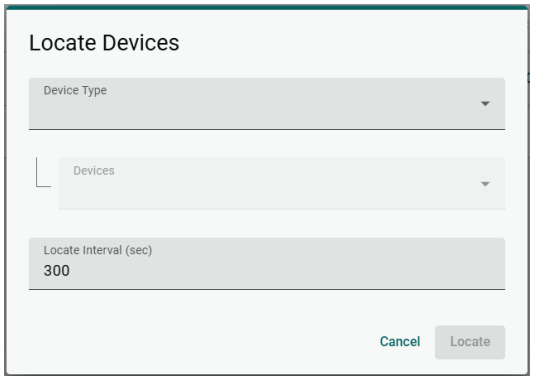
From the **Locator** screen, you can trigger an LED sequence and an audible beep on specified devices to identify their physical location.

> **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.



Locate Devices

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



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)

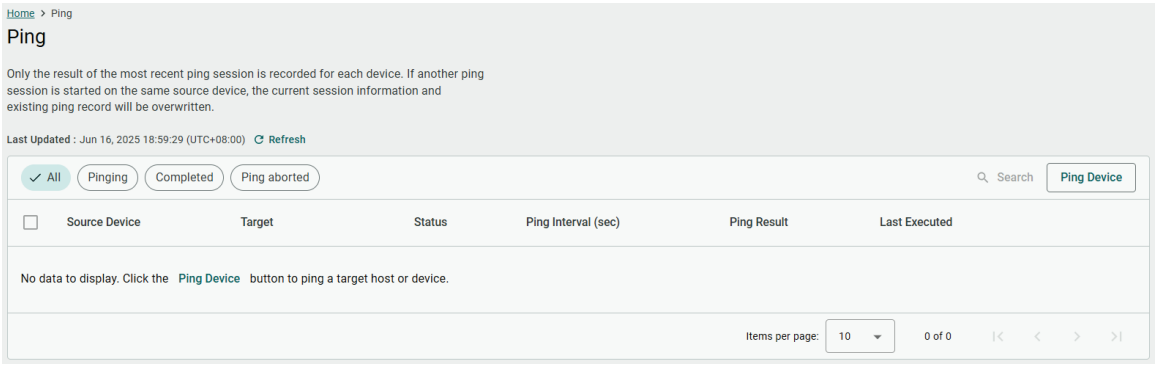
Setting	Description	Factory Default
1 to 3600	Specify the duration of the audible locator beep and LED sequence on the device(s) (in sec).	300

When finished, click **Locate**.

Ping

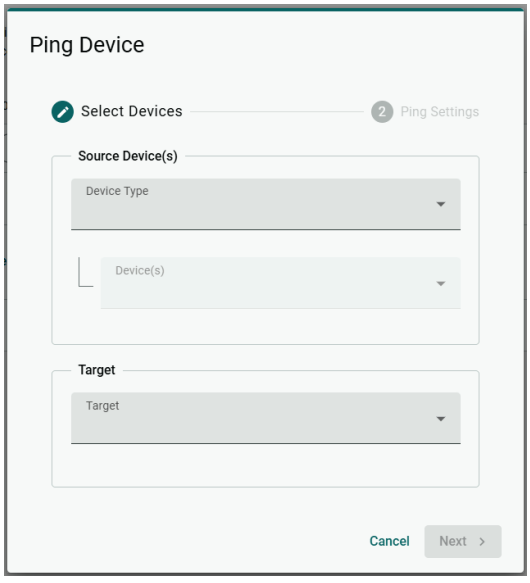
Menu Path: Diagnostics > Ping

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

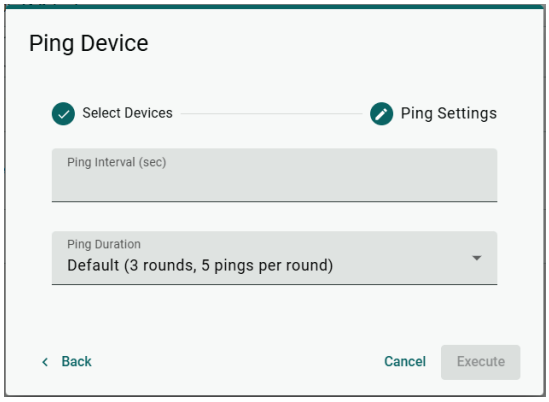
Devices

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**.



Configure the following settings:

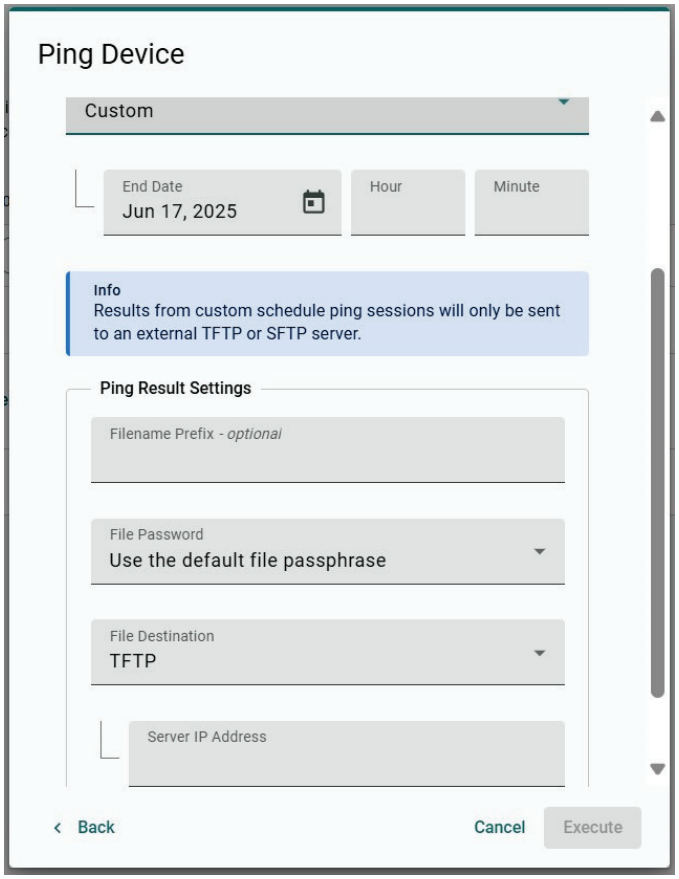
Ping Interval (sec)

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**.

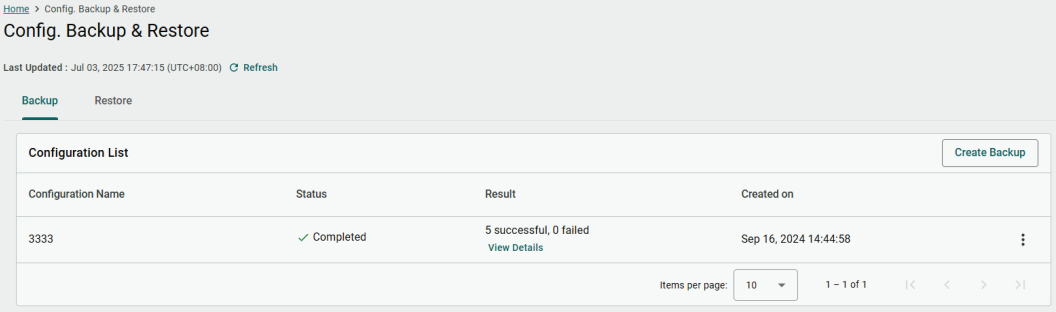
Config. Backup & Restore

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.

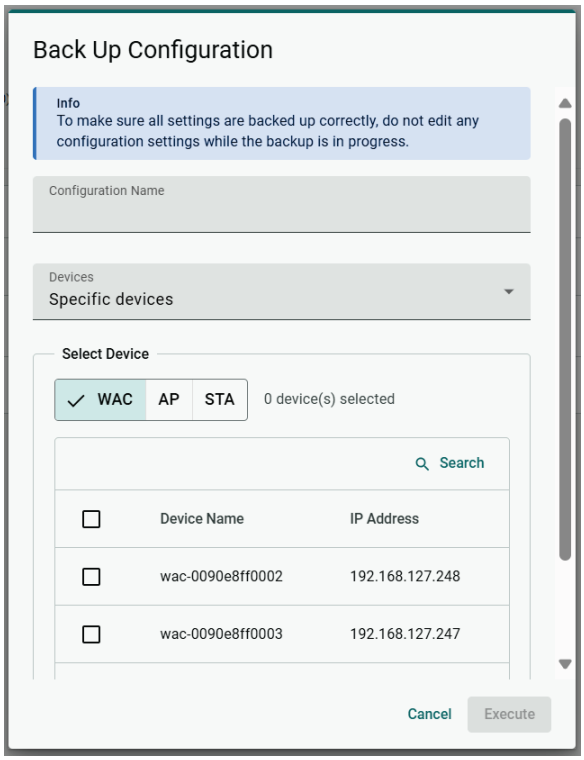


Create a Configuration Backup

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

NOTE

You can create a maximum of 10 configuration backups.



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**.

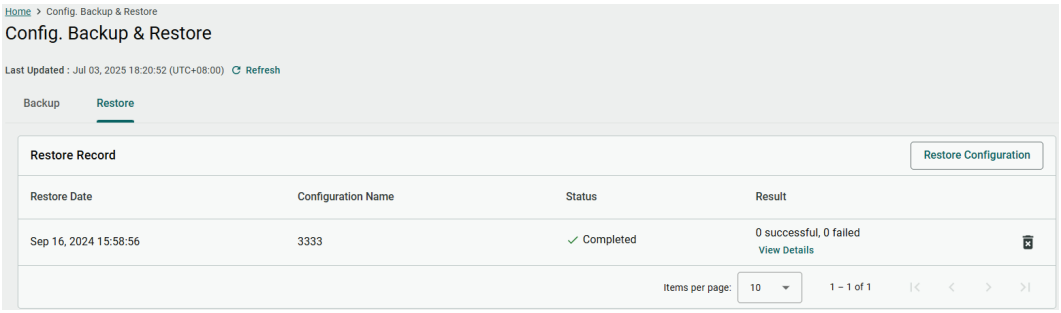
Deleting a Configuration Backup

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

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

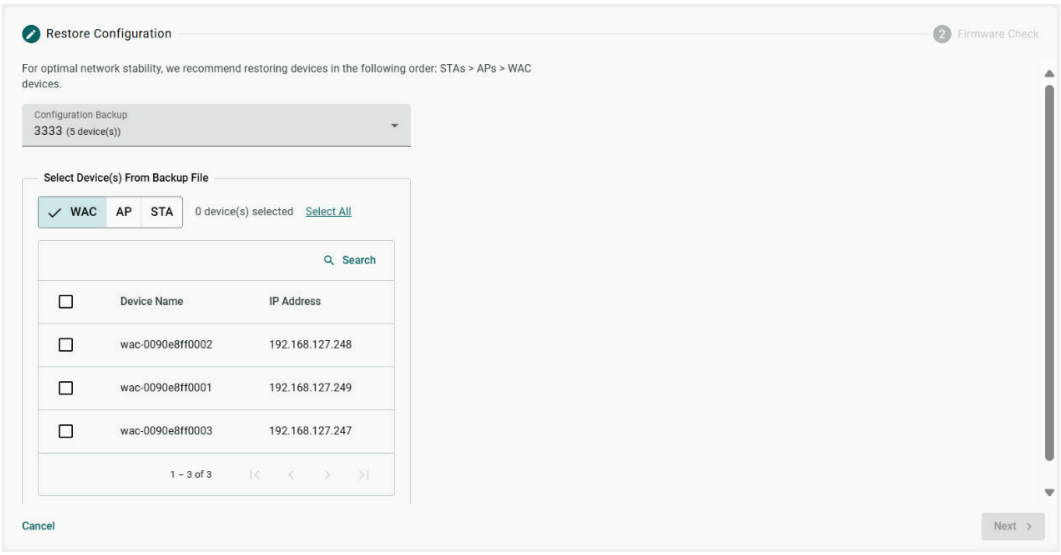
Restore

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:

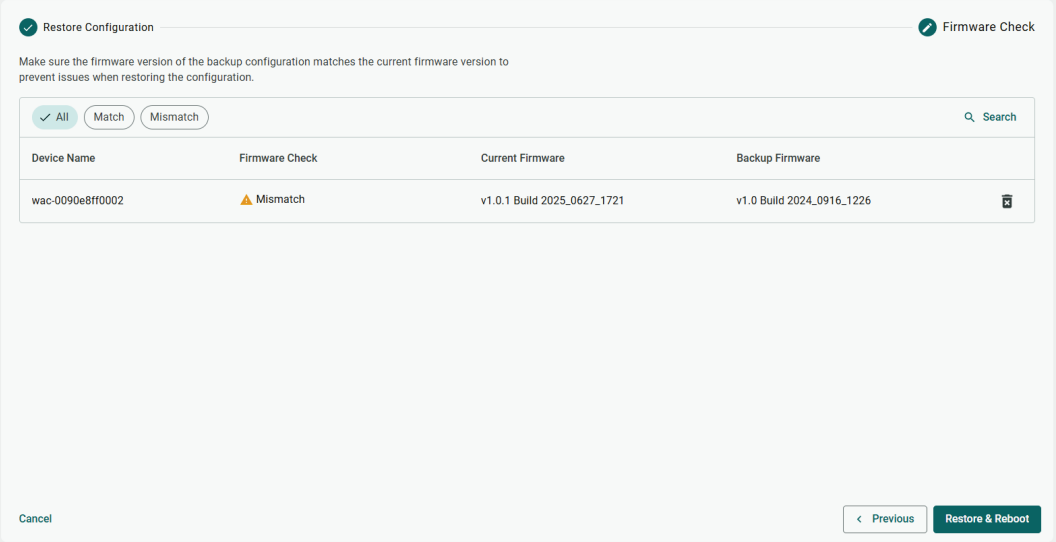
Configuration Backup

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**.



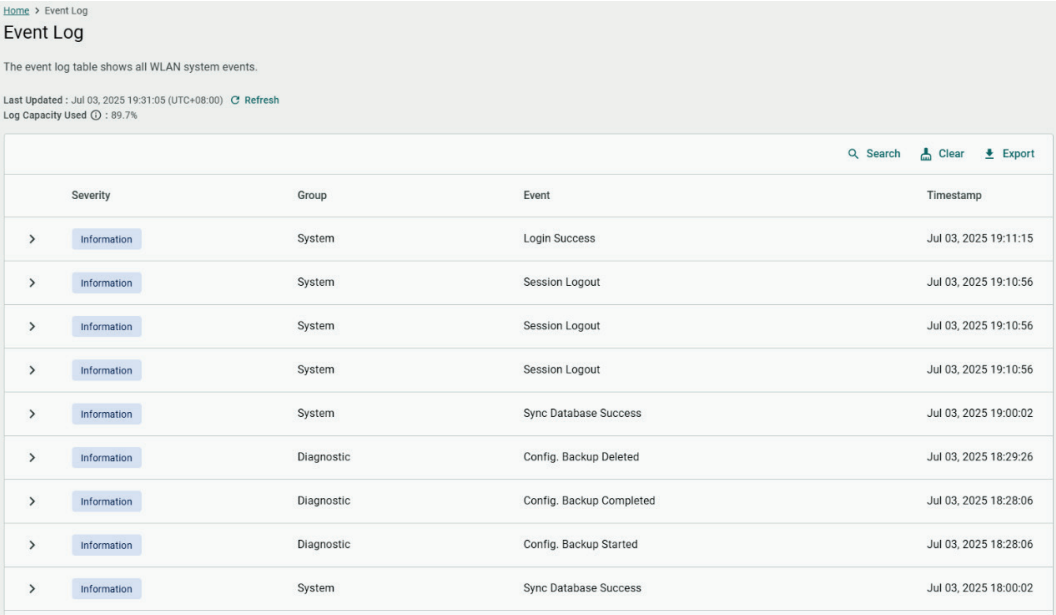
The system will perform a firmware check to see if the current device firmware matches the firmware version in the configuration backup. Any devices with a mismatching firmware version will be shown. While it is possible to restore the configuration across different firmware versions, it is recommended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

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

Event Log

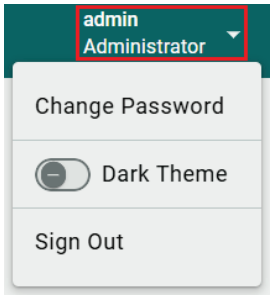
Menu Path: Diagnostics > Event Log

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



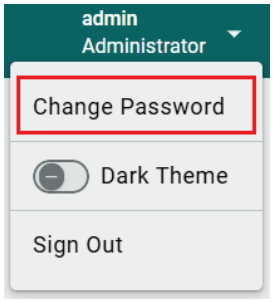
Maintenance and Tools

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.

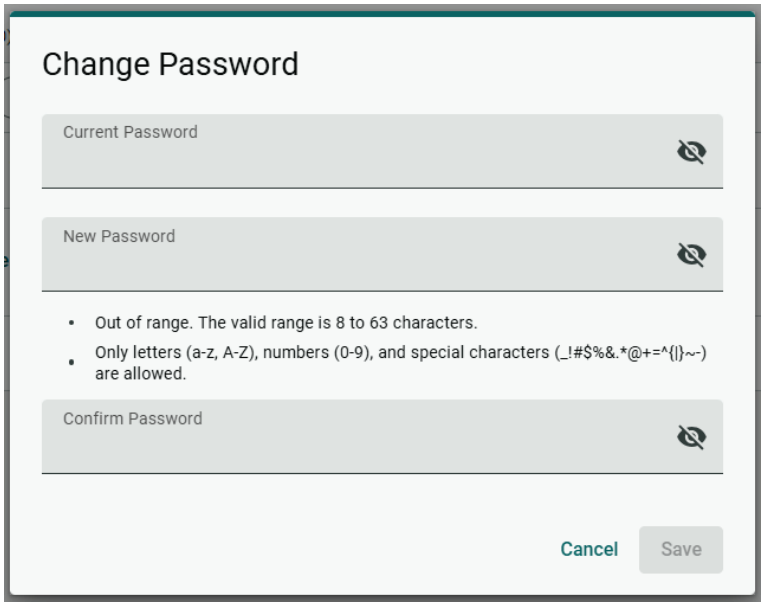


Change Password

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



Configure the following settings:



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

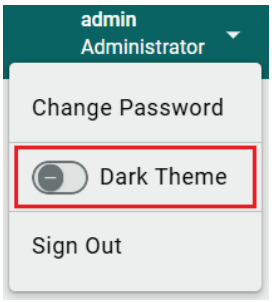
Confirm Password

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.