User Guide

Manage EAPs via the Omada Controller

 1900002156 REV6.1.0

About this Guide

Omada Controller offers centralized and efficient management for configuring enterprise networks comprised of gateways, switches, wireless access points (APs), optical line terminals (OLTs), and more. This guide provides information for centrally managing EAPs via the Omada Controller. Please read this guide carefully before operation.

For instructions about how to use the Omada Controller, refer to the Omada Controller User Guide.

For instructions about how to manage other types of devices via the Omada Controller, refer to the relevant user guides.

Intended Readers

This guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

When using this guide, notice that:

- Features available in the Omada Controller may vary due to your region, controller type and version, and device model. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.
- The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.
- This guide uses the specific formats to highlight special messages. The following table lists the notice icons that are used throughout this guide.

In this guide, the following conventions are used:

Controller	Stands for the Omada On-Premises Controller and the Omada Cloud-Based Controller.
On-Premises Controller	Includes the Omada Software Controller (also referred to as the Omada Network Application), Omada Hardware Controller, and Omada Integrated Gateway (Controller).
Cloud-Based Controller/ Omada Central	The Omada Cloud-Based Controller is now referred to as the Omada Network system on the Omada Central. Note that the Omada Central integrates the Omada Network system and Omada Guard system. The Omada Network system works as an Omada Controller to manage network devices (gateways, switches, access points, OLTs, and more), while the Omada Guard system works as a VMS system to manage surveillance devices (security cameras, NVRs, and more). This guide involves instructions about the Omada Network system. For instructions about the Omada Guard system, refer to the Omada Guard User Guide.
OLT	Stands for the DeltaStream GPON Optical Line Terminal.

Note:	The note contains the helpful information for a better use of the controller.
Configuration Guidelines:	Provide guidelines for the feature and its configurations.

More Resources

Main Site	https://www.omadanetworks.com/
Video Center	https://support.omadanetworks.com/video/
Documents	https://support.omadanetworks.com/document/
Product Support	https://support.omadanetworks.com/product/
Technical Support	https://support.omadanetworks.com/contact-support/

For technical support, the latest software, and management app, visit https://support.omadanetworks.com/.

CONTENTS

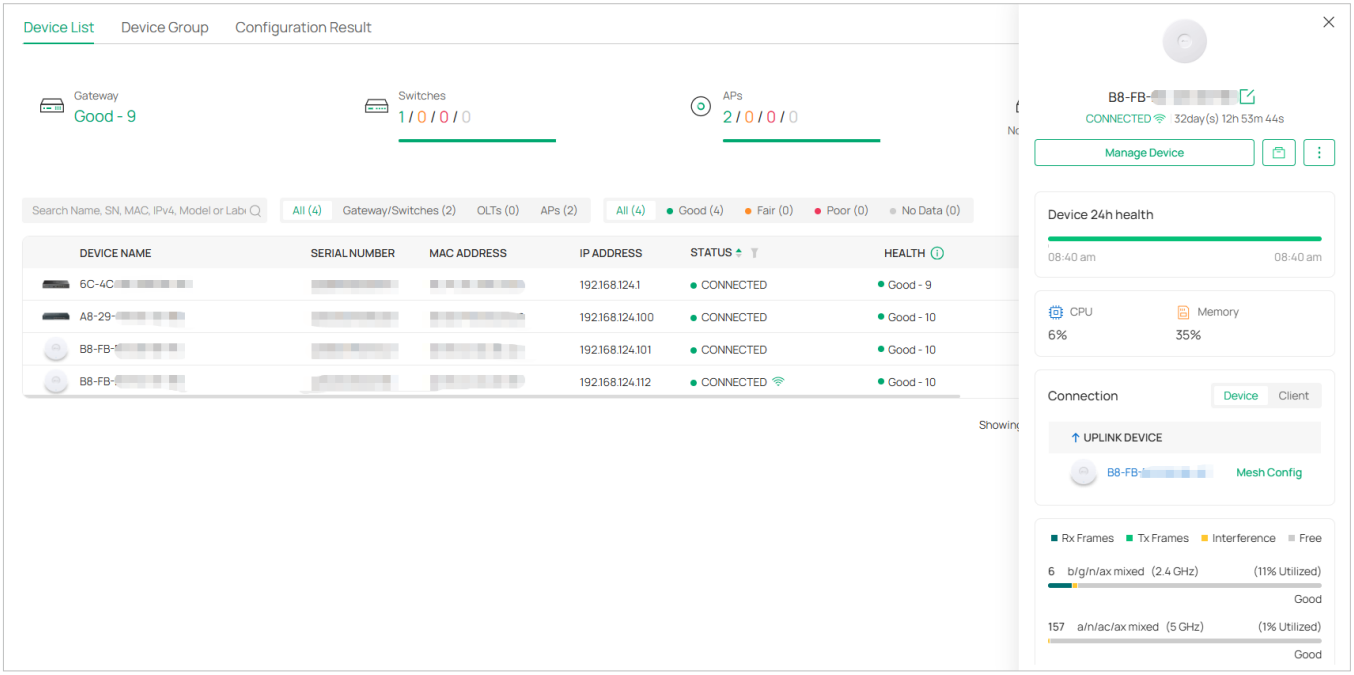
1 Manage the AP

Launch the controller and access a site. Go to Devices > Device List. In the device list, click an AP, then you can monitor and manage it in the Properties window and Device Management window.

1.1 Properties Window

The Properties window displays the device's basic information, health status, connection information, and more.

Note: The available functions in the window may vary by device model and status.



Quick Operations

Click the ⋮ icon and choose an operation to quickly operate the device.

Custom Upgrade	Click Browse and choose a file from your computer to upgrade the device. After upgraded, the device will reboot and be readopted by the controller.
Copy Configuration	Select another device at the current site to copy its configurations. **Note:** Only devices of the same model as the current device will be displayed.
Download Device Info	If the device has an abnormality, you can download the device information and provide it to our R&D personnel to analyze the problem. **Note:** Firmware updates are required for earlier devices to obtain complete information.
Move to Site	Select a site which the device will be moved to. After moving to another site, device configurations on the prior site will be replaced by that on the new site, and its traffic history will be cleared.

Force Provision	Click Force Provision to synchronize the configurations of the device with the controller. The device will lose connection temporarily, and be adopted to the controller again to get the configurations from the controller.
IntelliRecover	(Only for the EAP directly connected to the PoE switch) Click to enable the IntelliRecover function for the device so that it can be added to the IntelliRecover monitoring list. IntelliRecover can help you monitor the status of PoE devices, automatically repairing abnormal devices.
Forget This Device	Click Forget and then the device will be removed from the controller. Once forgotten, all configurations and history related to the device will be wiped out.

Network Tools

Click the  icon and choose a network tool to analyze the network.

Network Check	Test the device connectivity via ping or traceroute.
Packet Capture	Capture packets for network troubleshooting.
Terminal	Open Terminal to execute CLI or Shell commands.
Link Speed Test	(Only for Bridge APs supporting link speed test and already form a bridge group) Click to test the link speed between the Main AP and Client AP.

1.2 Device Management Window

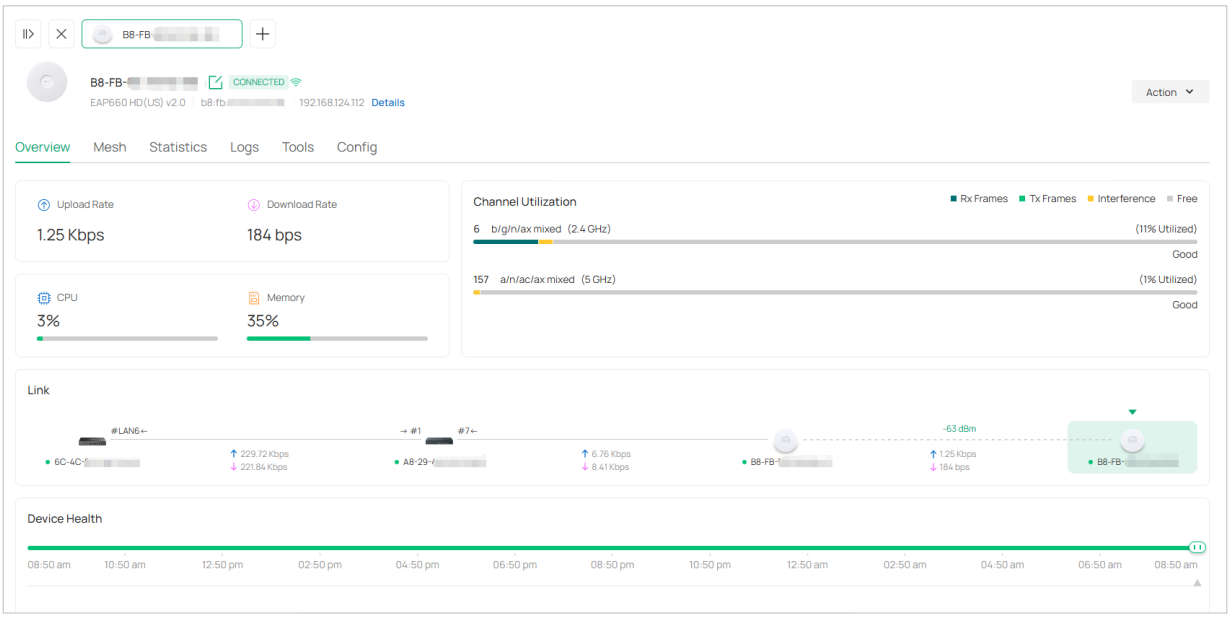
Click Manage Device to open the Device Management window to view more device details and change device settings.

In the management window, you can click + and select one or more devices to open new management windows, click the icon in the top left to minimize the windows to the  icon in the right side, and click the  icon to reopen the minimized windows.

You can also click each tab to monitor and manage the device. The tabs available may vary by model.

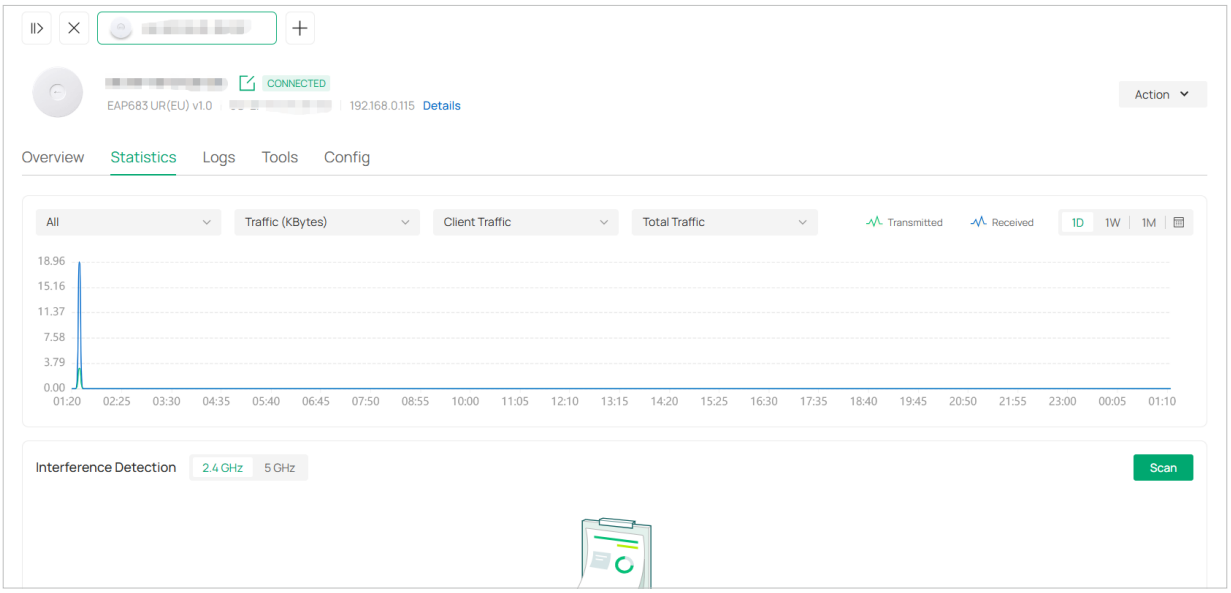
Overview

In Overview, you can get an overview of the device, such as device status, device health, link status, online time, current clients, and more.



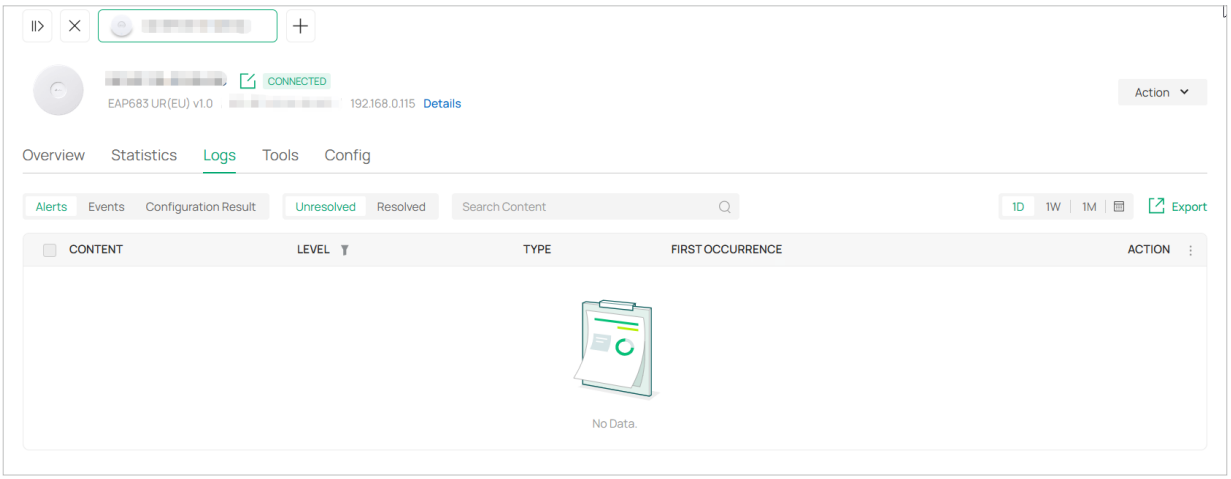
Statistics

In Statistics, you can check the traffic statistics of the device. You can also perform RF Scanning, interface detection, and/or spectral analysis if the device firmware supports these functions.



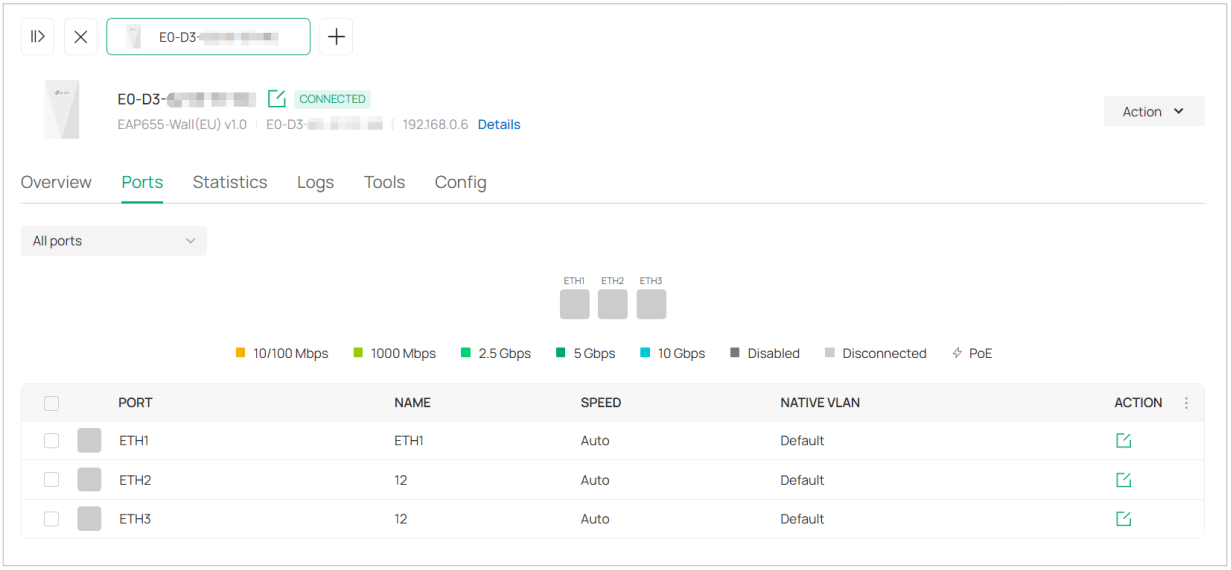
Logs

In Logs, you can check the logs of the device, such as alerts, events, and configuration result.



Ports (Only for APs with multiple LAN ports)

In Ports, you can view the port status and statistics and edit port settings.



To configure a port, click the edit icon in the Action column. Port settings may vary by port type.

Name	Specify the name of the port.
Status	Click the box to enable or disable the port.
VLAN	Configure the uplink port VLAN corresponding to the SSID. Default: Using untagged transmission. Custom: Enter the PVID (Port VLAN Identifier). When a port receives an untagged frame, the AP inserts a VLAN tag to the frame based on the PVID before forwarding it.
PoE Out	(Only for APs with the PoE out port) Enable this function to supply power to the connected device on this port.

Mesh (Only for pending/connected/isolated devices supporting Mesh)

Mesh is used to establish a wireless network or expand a wired network through wireless connection on 5 GHz radio band. In practical application, it can help users to conveniently deploy APs without requiring Ethernet cable. After mesh network establishes, the APs can be configured and managed in the controller in the same way as wired APs. Meanwhile, because of the ability to self-organize and self-configure, mesh also can efficiently reduce the configuration.

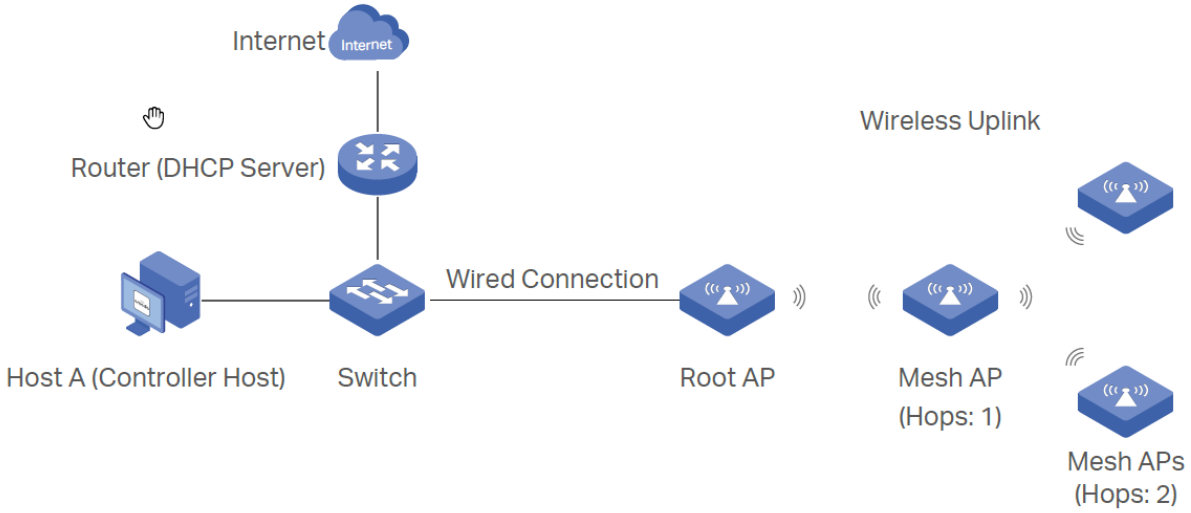
Note that only certain AP models support Mesh, and the APs should be in the same site to establish a Mesh network.

To understand how mesh can be used, the following terms used in the Controller will be introduced:

Root AP	The AP is managed by the Controller with a wired data connection that can be configured to relay data to and from mesh APs (downlink AP).
Isolated AP	When the AP which has been managed by the Controller before connects to the network wirelessly and cannot reach the gateway, it goes into the Isolated state.
Mesh AP	An isolated AP will become a mesh AP after establishing a wireless connection to the AP with network access.
Uplink AP/Downlink AP	Among mesh APs, the AP that offers the wireless connection for other APs is called uplink AP. A Root AP or an intermediate AP can be the uplink AP. And the AP that connects to the uplink AP is called downlink AP. An uplink AP can offer direct wireless connection for 4 downlink APs at most.
Wireless Uplink	The action that a downlink AP connects to the uplink AP.
Hops	In a deployment that uses a root AP and more than one level of wireless uplink with intermediate APs, the uplink tiers can be referred to by root, first hop, second hop and so on. The hops should be no more than 3.

A common mesh network is shown as below. Only the root AP is connected by an Ethernet cable, while other APs have no wired data connection. Mesh allows the isolated APs to communicate with pre-configured root AP on the network. Once powered up, factory default or unadopted APs can detect the

AP in range and make itself available for adoption in the controller.



After all the APs are adopted, a mesh network is established. The APs connected to the network via wireless connection also can broadcast SSIDs and relay network traffic to and from the network through the uplink AP.

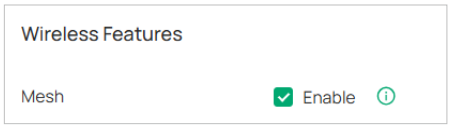
To build a mesh network, follow the steps below:

1) Enable Mesh function.

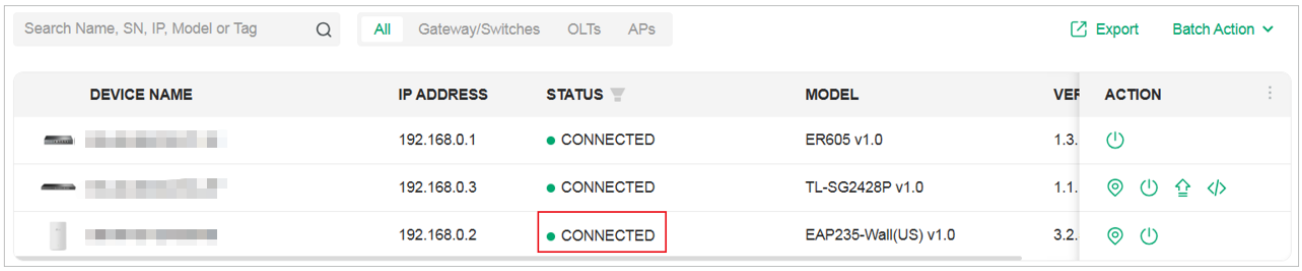
2) Adopt the Root AP.

3) Set up wireless uplink by adopting APs in Pending (Wireless) or Isolated status.

1. Go to Network Config > General Settings > Site Settings > Wireless Features and make sure Mesh is enabled.

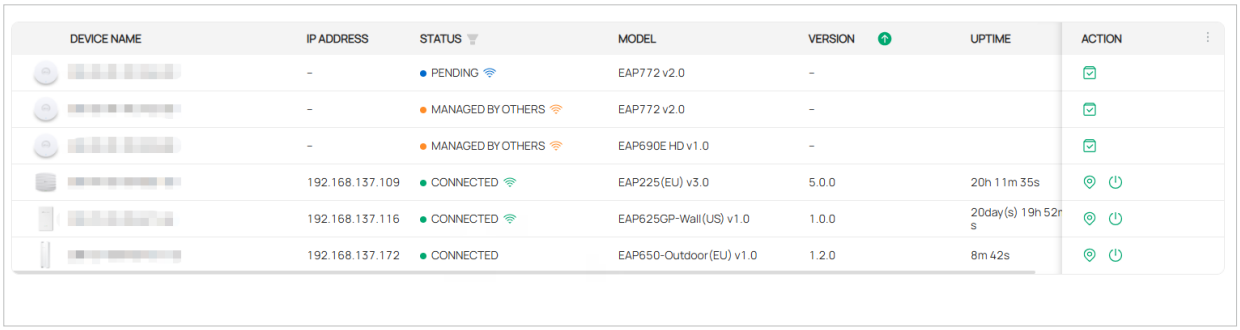


2. Go to Devices to make sure that the Root AP has been adopted by the controller. The status of the Root AP is Connected.



3. Install the AP that will uplink the Root AP wirelessly. Make sure the intended location is within the range of Root AP. The APs that is waiting for Wireless Uplink includes two cases: factory default APs and APs that has been managed by the controller before. Go to Devices to adopt an AP in

Pending (Wireless) status or link an isolated AP.

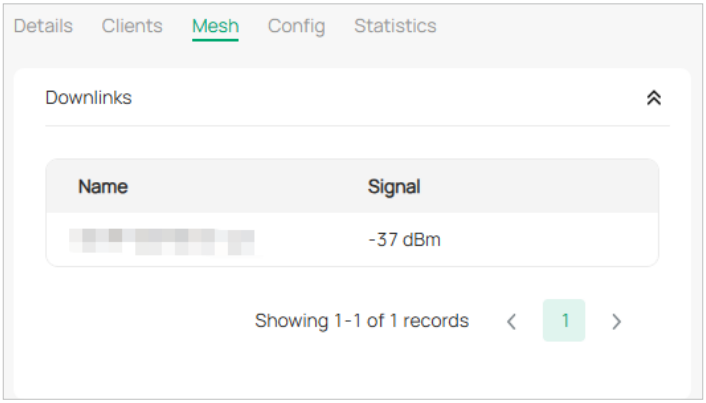


1) For the factory default AP, after powering on the device, the AP will be in Pending (Wireless) status. Go to Devices, click Add Devices, choose Auto Find, then click the adopt icon in the Action column to adopt the AP.
2) For the AP that has been managed by the Controller before and cannot reach the gateway, it goes into Isolated status in the Devices list when it is discovered by controller again. Click the adopt icon in the Action column to connect the Uplink AP.

Once mesh network has been established, the AP can be managed by the controller in the same way as a wired AP.

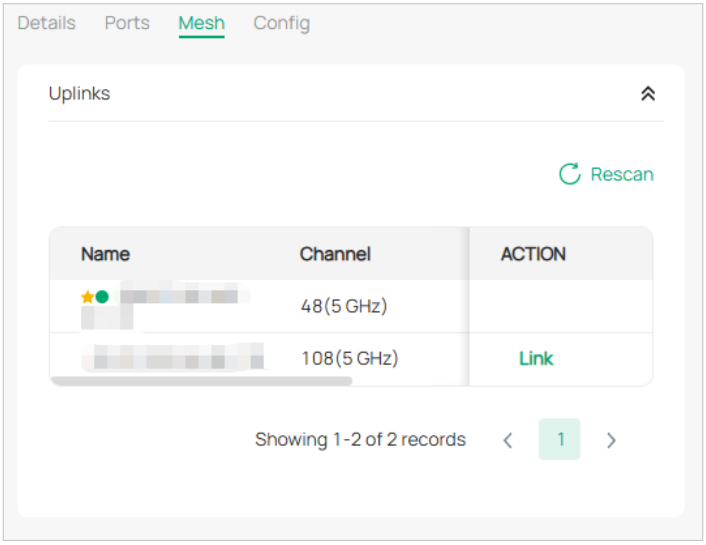
To view mesh info, click the mesh AP in the device list, click Manage Device, and go to the Mesh page.

In Mesh, if the selected AP is an uplink AP, this page lists all downlink APs connected to the AP.



If the selected AP is a downlink AP, this page lists all available uplink APs and their channel, signal strength, hop, and the number of downlink APs. You can click Rescan to search the available uplink APs

and refresh the list, and click Link to connect the uplink AP and build up a mesh network.

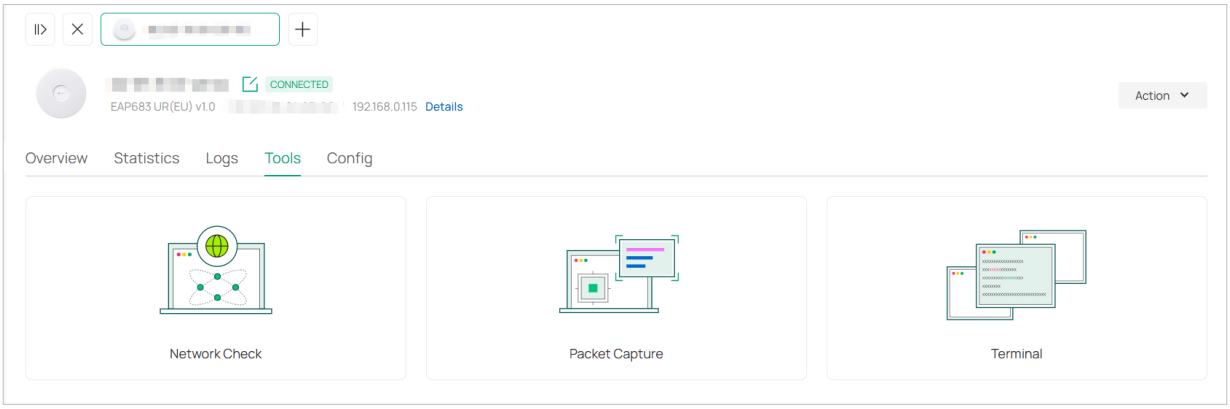


Tips:

- You can manually select the priority uplink AP that you want to connect in the uplink AP list. To build a mesh network with better performance, we recommend that you select the uplink AP with the strongest signal, least hop and least downlink AP.
- Auto Failover is enabled by default in Site Settings, and it allows the controller automatically select an uplink AP for the isolated AP to establish Wireless Uplink. And the controller will automatically select a new uplink AP for the mesh APs when the original uplink fails.

Tools

In Tools, you can use network tools to test the device connectivity or Open Terminal to execute CLI or Shell commands.



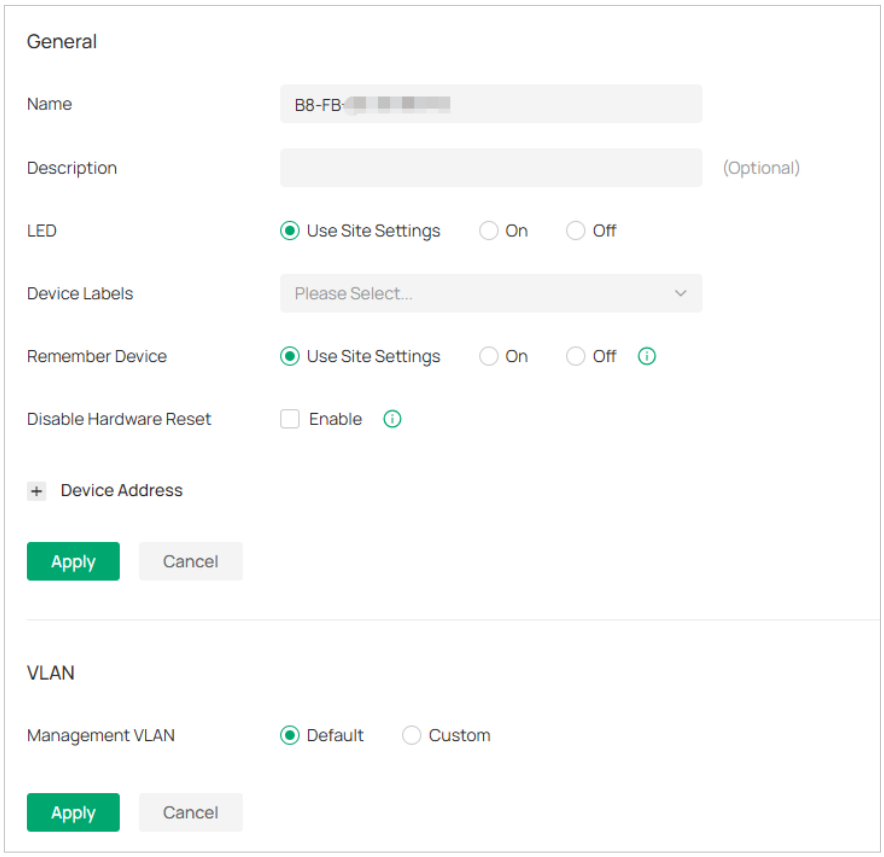
2 Configure General Settings

In General Settings, you can specify the device name, control the LED and Wi-Fi, configure the device address, and more.

To configure general settings of an AP, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > General.

3. Configure the parameters.



Name	Specify a name of the device.
Description	(Optional) Enter a description for identification.
LED	Select the way that device's LEDs work. Use Site Settings: The device's LED will work following the settings of the site. On/Off: The device's LED will keep on/off.
Wi-Fi Control	(Only for Certain APs) Enable Wi-Fi Control, and it will take effect only when the LED feature is enabled. After enabling Wi-Fi Control, you can press the LED button on the AP to turn on/off the Wi-Fi and LED at the same time.
Device Labels	Select a tag from the drop-down list or create a new tag to categorize the device.
Remember Device	With this function, the controller will remember this device. After device reset and power-on, the controller will automatically adopt the device if the controller can find it.
Disable Hardware Reset	When enabled, the hardware reset button will be ineffective when the device is managed by the controller, and it will be effective again when the device is disconnected from the controller.

Device Address	GPS Enable: (Only for models with the with GPS chip) When enabled, the device can actively obtain GPS data and update its location. Address/Longitude/Latitude: Configure the parameters according to where the site is located. These fields are optional.
Management VLAN	Specify the VLAN ID of the management VLAN. Only the hosts in the Management VLAN can log in to the AP via the Ethernet port. This provides a safer method to manage the AP. Note that the controller will fail to manage your devices with wrong Management VLAN configurations. If you are not sure about your network conditions and the potential impact of any configurations, we recommend that you keep the default configurations. Refer to the Management VLAN Configuration Guide before you configure this feature.

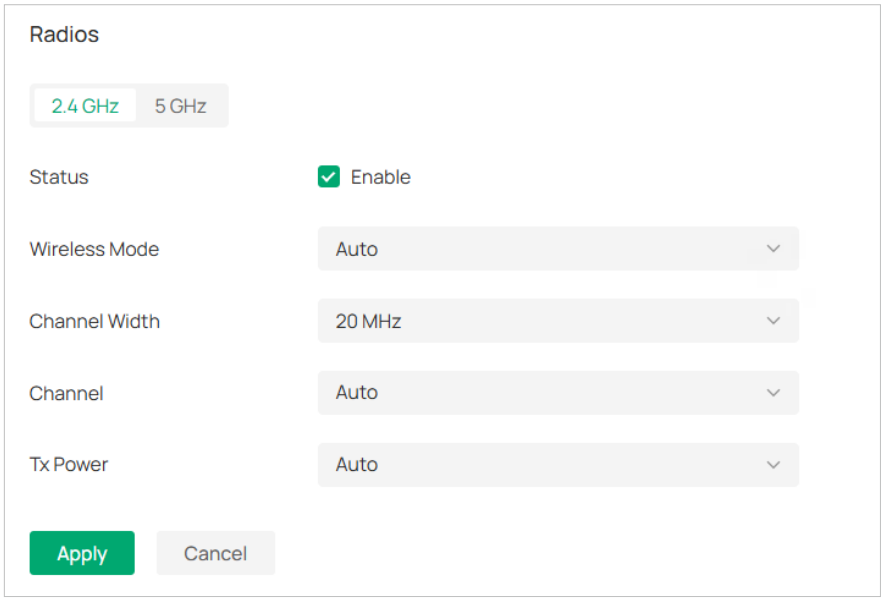
3 Configure Wireless Settings

3.1 Radio Settings

In Radios, you can control how and what type of radio signals the AP emits.

To configure radio settings of an AP, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Wireless > Radios.
3. Select each band and configure the parameters. Different models support different bands.



AFC	(For Wi-Fi 7 APs of US version) Enable this feature to use the 6GHz band. The AFC (Automated Frequency Coordination) feature adjusts the transmission power of the 6 GHz band according to your geographic location to meet regulatory requirements.

Installation Type	(For Indoor/Outdoor Wi-Fi 7 APs of EU version) Choose the installation mode of the device. Default Mode: In this mode, the device will adjust the Indoor/Outdoor mode of the 5GHz/6GHz band according to local regulations. This mode is recommended. Indoor Mode / Outdoor Mode: If selected, the device will adjust 5GHz/6GHz channel power bandwidth parameters for indoor / outdoor usage.
Status	If you disable the frequency band, the radio on it will turn off.
Wireless Mode	Specify the wireless mode of the band. Different bands have different available options. We recommend using the default value.
Channel Width	Specify the channel width of the band. Different bands have different available options. We recommend using the default value.
Channel	Specify the operation channel of the device to improve wireless performance. If you select Auto for the channel setting, the device scans available channels and selects the channel where the least amount of traffic is detected.
Channel Range	(Only for certain models) Specify the channel range of the device to improve wireless performance.
Tx Power	Specify the Tx Power (Transmit Power) in the 4 options: Low, Medium, High and Custom. The actual power of Low, Medium and High are based on the minimum transmit power (Min. Txpower) and maximum transmit power (Max. TxPower), which may vary in different countries and regions. Low: Min. TxPower + (Max. TxPower-Min. TxPower) * 20% (round off the value) Medium: Min. TxPower + (Max. TxPower-Min. TxPower) * 60% (round off the value) High: Max. TxPower Custom: Specify the value manually.

3.2 WLAN Settings

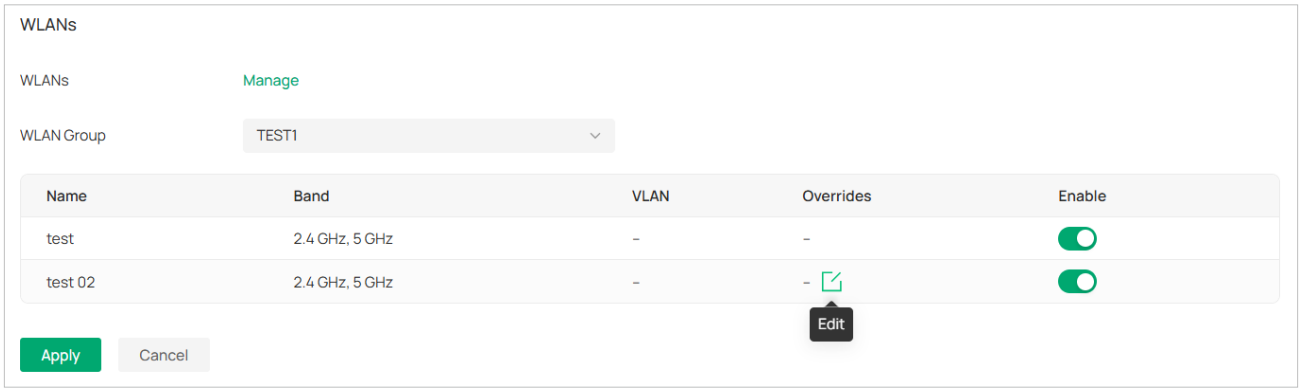
Each site has a default WLAN group, and APs adopted to the site will be applied with the default WLAN group by default.

In WLANs, you can change the WLAN group of the AP or specify a different SSID and password to override the SSID in the WLAN group. After that, clients can access the AP's network via the new SSID and password.

To configure WLAN settings of an AP, follow the steps below:

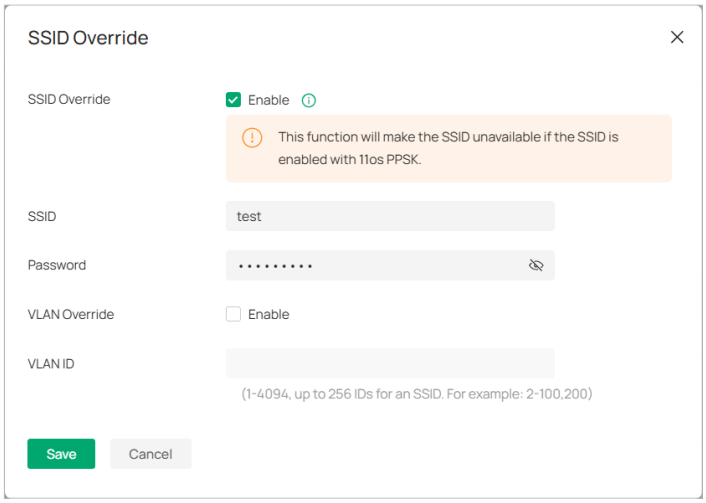
1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Wireless > WLANs.

3. Configure the parameters.



WLANs	Click Manage to redirect to the WLAN group page of the site to create and edit WLAN groups. For detailed instructions about WLAN groups, refer to the Omada Controller User Guide.
WLAN Group	Choose a WLAN group to apply its preset wireless network settings to the AP.

If you want to override an SSID of the WLAN group, hover on it, then click the edit icon in the Overrides column. Set the parameters.



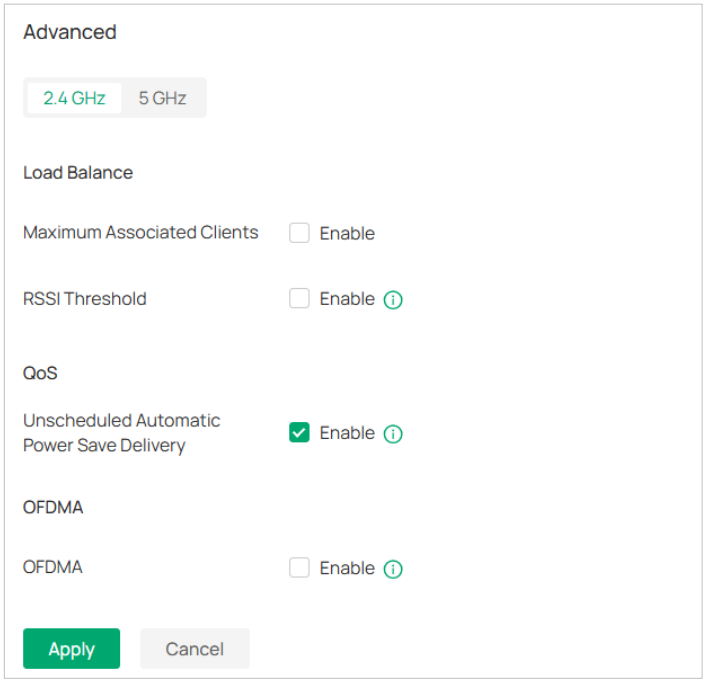
SSID Override	Enable or disable SSID Override on the AP. If enabled, specify the new SSID and password to override the current one. Note: If the SSID is enabled with 11os PPSK, the override function will make the SSID unavailable!
VLAN Override	Enable or disable VLAN Override on the AP. If enabled, enter a VLAN ID to override the current one.

3.3 Advanced Settings

In Advanced, you can configure Load Balance, QoS, and OFDMA to improve network performance.

To configure advanced wireless settings of an AP, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Wireless > Advanced.
3. Select each band and configure the parameters. Different models support different bands.



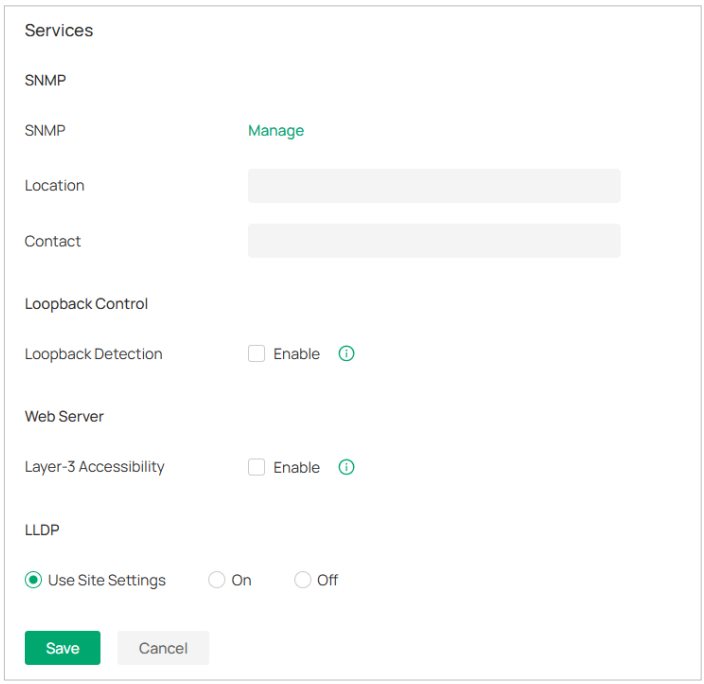
Load Balance	Load Balance controls the clients associated to the device. Max Associated Clients: Enable this function and specify the maximum number of connected clients. If the number of connected clients reaches the specified value, the device will disconnect those with weaker signals to make room for other clients requesting connections. RSSI Threshold: Enable this function and enter the threshold of RSSI (Received Signal Strength Indication). If a client's signal strength is weaker than the threshold, the client will lose connection with the device.
QoS	QoS optimize the performance when handling differentiated wireless traffics, including traditional IP data, VoIP (Voice-over Internet Protocol), and other types of audio, video, streaming media. Unscheduled Automatic Power Save Delivery: Abbreviation as U-APSD, this function greatly improves the energy-saving capacity of clients to extend their battery life, and reduces the latency of traffic flow that is delivered over the wireless media.
OFDMA	(Only for AP supporting 802.11 ax or later standards) Enable this feature to enable multiple users to transmit data simultaneously, and it will greatly improves speed and efficiency. Note that the benefits of OFDMA can be fully enjoyed only when the clients support OFDMA.

4 Configure Service Settings

In Services, you can configure SNMP and LLDP for the AP.

To configure service settings of an AP, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Services.
3. Configure the parameters.



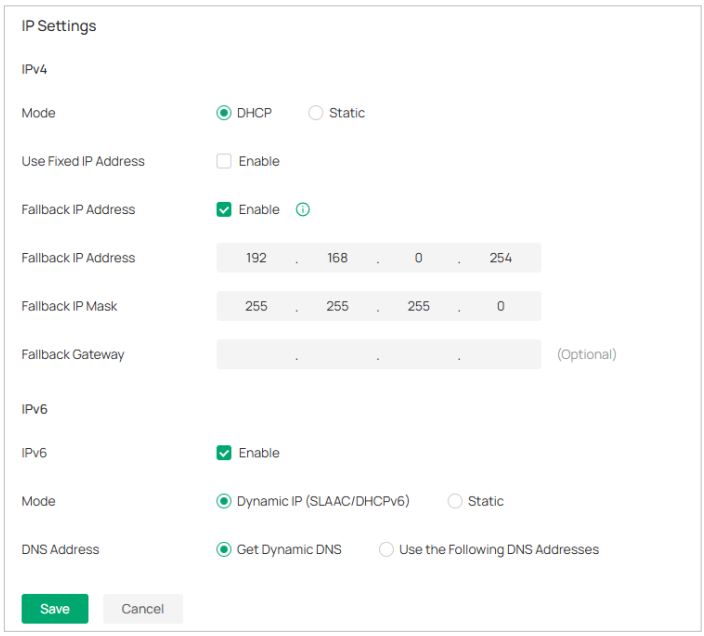
SNMP	Configure SNMP to write down the Location and Contact detail. You can click Manage to redirect to the SNMP setting page of the site.
Loopback Control	(Only for EAPs with multiple LAN ports) Loopback refers to the routing of data streams back to their source in the network. You can disable loopback control for the network or enable Loopback Detection to help detect loops that occur on a specific port. When a loop is detected on a port, the port will be blocked.
Web Server	With the web server, you can access and manage the AP. Layer-3 Accessibility: With this feature enabled, devices from a different subnet can access controller-managed devices.
LLDP	LLDP (Link Layer Discovery Protocol) can help discover devices.

5 Configure IP Settings

In IP Settings, you can configure the IP address of the AP.

To configure IP settings of an AP, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > IP Settings.
3. Configure the parameters.



IPv4 Mode	Select an IP mode and configure the parameters for the device. DHCP: In this mode, make sure there is a DHCP server in the network and then the device will obtain dynamic IP address from the DHCP server automatically. If you want to let the device use a fixed IP address, enable Use Fixed IP Address, and set the network and IP address according to site needs. If you want to hold an IP address in reserve for the situation in which the device fails to get a dynamic IP address, enable Fallback IP Address and set the IP address, IP mask, and gateway. Static: In this mode, set the IP address, IP mask, gateway, and DNS server for the static address.
IPv6	Enable this option if you want to set up an IPv6 address.

IPv6 Mode	Select the IPv6 mode. Dynamic IP (SLAAC/DHCPv6): Select this mode if your ISP uses Dynamic IPv6 address assignment, either DHCPv6 or SLAAC+Stateless DHCP. In this mode, set the DNS Address to determine whether to get dynamic DNS or use the specified DNS addresses. Static: In this mode, set the IP address, prefix length, gateway, and DNS server for the static address.

6 Bridge Settings (Only for Bridge APs)

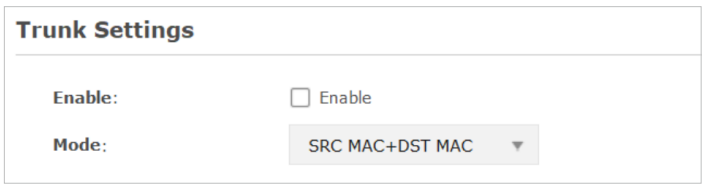
Bridge SSID / Password	Set the Bridge SSID and password of the AP. APs with the same Bridge SSID and password will form a Bridge network.

7 Configure Trunk Settings (Only for certain models)

The trunk function can bundle multiple Ethernet links into a logical link to increase bandwidth and improve network reliability.

To configure trunk settings of an AP, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Trunk.
3. Enable this function and select the trunk algorithm mode.



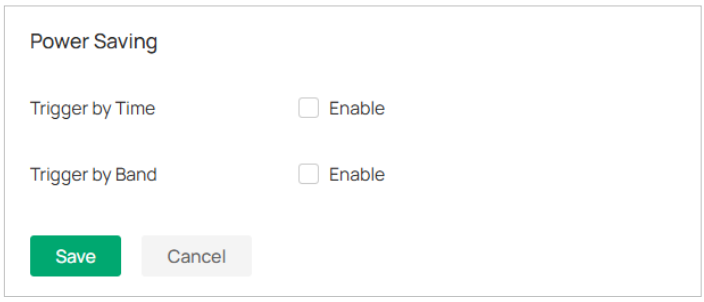
Mode	Select the trunk algorithm mode. Based on the selected algorithm mode, the AP determines which physical port is used to send out the received packet. SRC MAC+DST MAC: The AP determines the outgoing port based on both the source and destination MAC addresses of the packet. DST MAC: The AP determines the outgoing port based on the destination MAC address of the packet. SRC MAC: The AP determines the outgoing port based on the source MAC address of the packet.

8 Configure Power Saving (Only for Certain Models)

Power saving can reduce the AP's power usage.

To configure power saving settings of an AP, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Power Saving.
3. Configure the parameters.



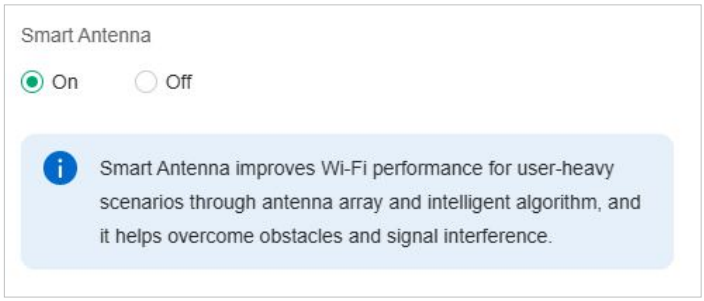
Trigger by Time	With this option enabled, you can specify the start and end time to enable power saving every day within the time period.
Trigger by Band	With this option enabled, you can specify the bands and idle duration to enable power saving when there are no connections for the specified duration on the bands.

9 Configure Smart Antenna (Only for Certain Models)

Smart Antenna improves Wi-Fi performance for user-heavy scenarios through antenna array and intelligent algorithm. This helps overcome obstacles and signal interference.

To enable or disable Smart Antenna of an AP, follow the steps below:

1. Launch the controller and access a site.
2. Go to Devices > Device List. In the device list, click an AP, click Manage Device and go to Config > Smart Antenna.
3. Enable or disable Smart Antenna according to site needs.



10 Configure EoGRE Tunnel

Overview

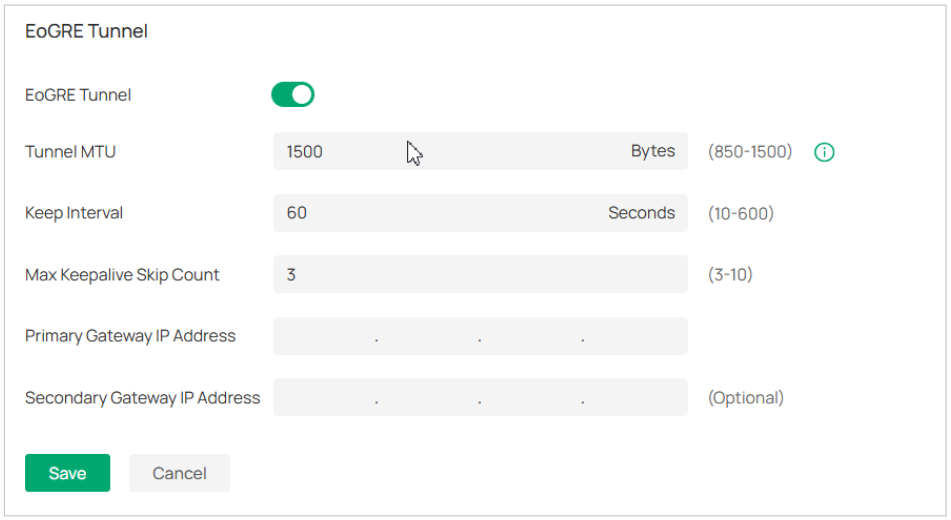
You can configure the EoGRE (Ethernet over GRE) tunnel for APs on a site. Set the IP address to the gateway IP of the peer-end EoGRE Server. Ensure that the topology meets the point-to-point structure and that the two points are connected across Layer 3 wired connections. In this configuration, the following two conditions must be met to make the AP tunnel interface up:

- The function is enabled.
- There is a client connection.

Configuration

To configure the EoGRE tunnel for APs on a site, follow the steps below:

1. Launch the controller and access a site.
2. Go to Device Config > EAP > EoGRE Tunnel.
3. Enable EoGRE Tunnel and configure the parameters.



Tunnel MTU	Specify the MTU (Maximum Transmission Unit) of the tunnel.
Keep Interval	Specify the time interval for the device to send Keepalive packets to confirm the link status.
Max Keepalive Skip Count	Specify the maximum number of times the keepalive message is not replied. If the number of times exceeds this value, the device will consider the peer to be offline.
Primary Gateway IP Address	Specify the Gateway IP address of the peer.
Secondary Gateway IP Address	Specify the secondary Gateway IP address of the peer. This field is optional.

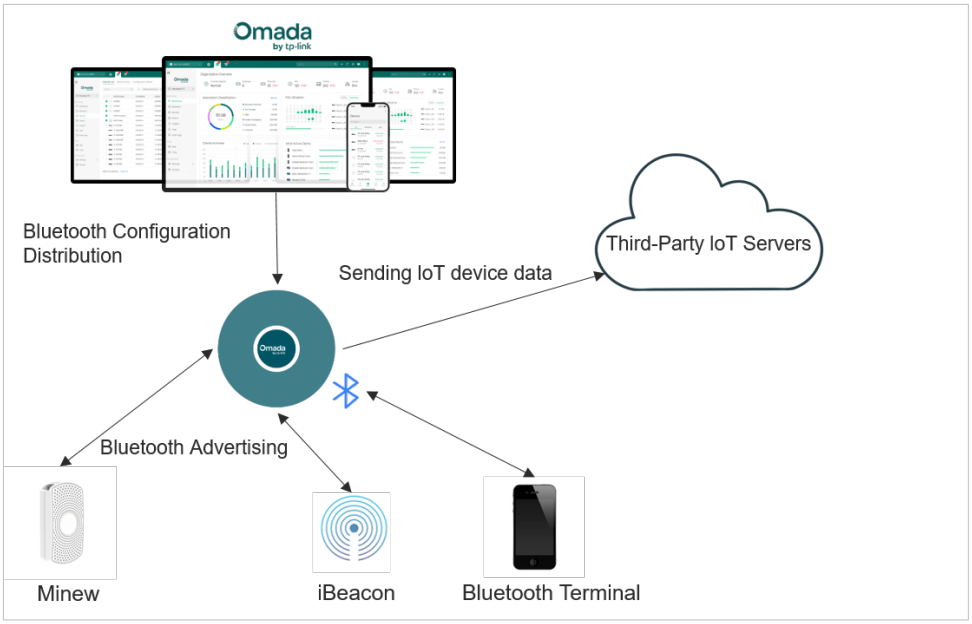
11 Configure Bluetooth Settings

11.1 Overview

Omada supports Bluetooth settings to provide IoT (Internet of Things) solutions compatible with the Omada EAP for applications in healthcare, nursing homes, and more.

The Bluetooth Advertising with iBeacon technology turns the Omada EAP into a Bluetooth beacon, enabling location features for iOS apps using the Apple Core Location API.

Bluetooth IoT utilizes the Omada EAP Bluetooth module to easily collect Bluetooth data from third-party beacons and sensors, seamlessly connecting to external IoT servers for improved applications.



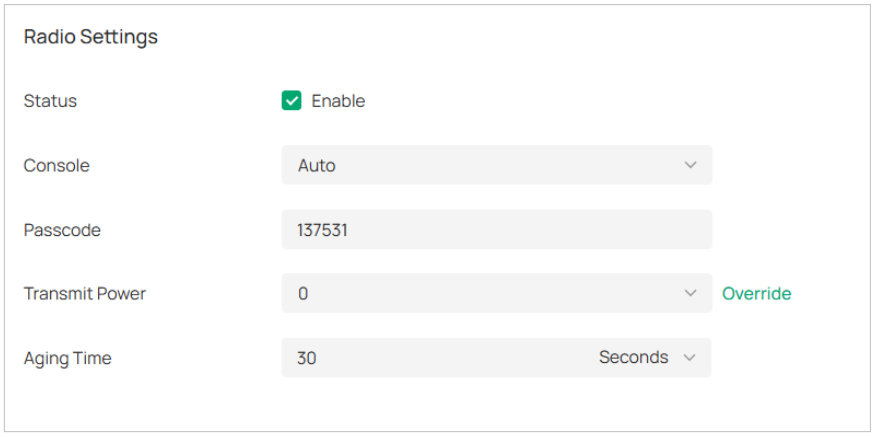
11.2 Configure Radio Settings

The Radio Settings module allows you to configure the broadcasting and connection behavior of Bluetooth devices. By adjusting these parameters, you can control the effective transmission power of Bluetooth broadcasts, device aging time, and other Bluetooth-related settings to optimize the network performance and connection stability of Bluetooth devices.

To configure radio settings of Bluetooth devices, follow the steps below:

1. Launch the controller and access a site.
2. Go to Device Config > EAP > Bluetooth > Radio Settings.

3. Configure the parameters.



Status	Toggle to enable Bluetooth radio. Configurations on the IoT Transport Streams and Bluetooth Advertising pages are effective only when this option is enabled. When disabled, Bluetooth disables all TX and RX activities.
Console	A Bluetooth Console allows you to communicate with a device over a wireless Bluetooth connection using serial protocols. Set the Bluetooth console mode: Auto: Automatically enables the Bluetooth console if a network error or device disconnection occurs and disables it when the device reconnects normally. On: Always on. Off: Always off.
Passcode	Specify the 6-digit pairing code used to establish a Bluetooth connection.
Transmit Power	Specify the broadcast transmission power (dB).
Aging Time	Set the time in seconds, minutes, or hours to control the aging time of devices. If an AP does not receive the data sent by a device within the aging time, it will delete the device entry and no longer forward it to the IoT application server. If the AP receives the data sent by the device again, it will re-add the device entry and continue to report the Bluetooth data of the device.

11.3 Configure IoT Transport Streams

IoT Transport Streams allow Bluetooth-enabled APs to scan BLE Advertising frames in its surrounding environment, collect the required BLE data, and then report the data to the designated third-party IoT server. IoT Transport Streams can be divided into two functions: BLE Periodic Telemetry and BLE Data Forwarding.

BLE Periodic Telemetry: The APs will parse the scanned BLE Advertising frames, extract the valid data, and save the data to their BLE device lists. They will populate BLE device list data into the messages at set intervals and report to the designated third-party IoT server.

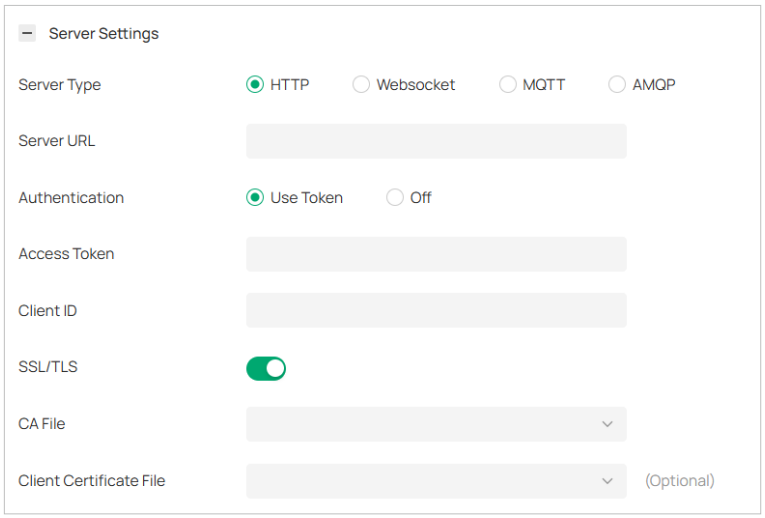
BLE Data Forwarding: The APs will automatically forward the scanned BLE Advertising frames of the specified protocol. The forwarded data is the raw data received by the APs, which is forwarded in real time.

To configure IoT Transport Streams, follow the steps below:

1. Launch the controller and access a site.
2. Go to Device Config > EAP > Bluetooth > IoT Transport Streams.
3. Click Create New Entry to create a new IoT Transport Streams profile.
4. Configure basic information.

Name	Enter the name of the profile.
Status	Toggle on to enable this profile on Bluetooth-enabled APs.

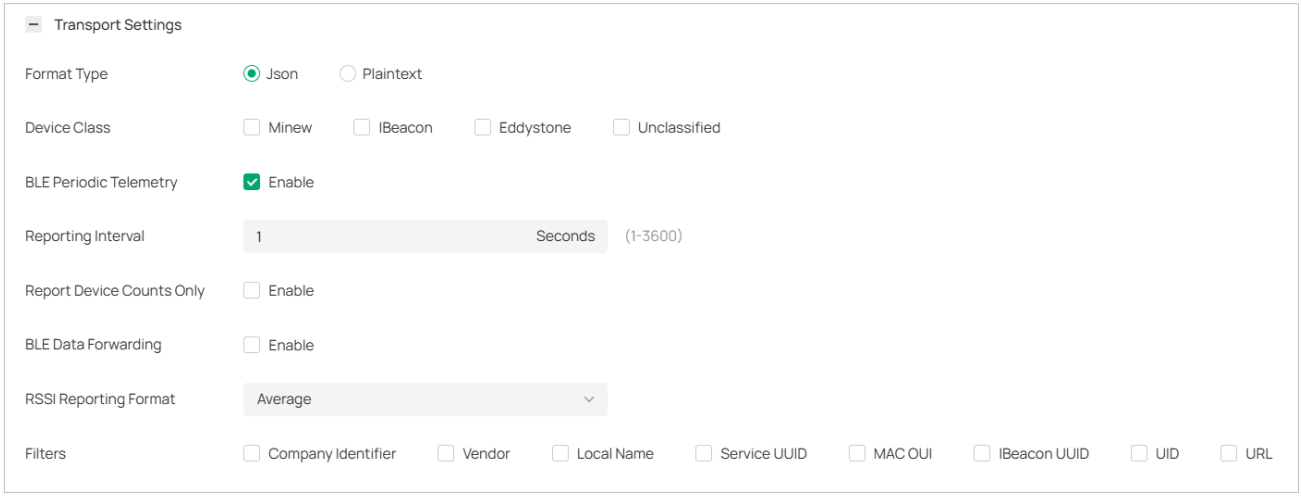
5. Configure server settings.



Server Type	Specify the type of server receiving IoT data. Available options include HTTP, WebSocket, MQTT, and AMQP.
Server URL	Enter the server address for IoT data reporting. Currently, the URL path with http as the prefix is supported.
Authentication	Specify the authentication method. Currently, token authentication is supported.
Access Token	Specify the token used for identity authentication.
Client ID	Specify the ID used for identity authentication.
SSL/TLS	Specify whether to enable SSL/TLS.
CA File	Upload the certificate from a CA authority or a self-signed certificate.

Client Certificate File	Upload the certificate issued by a CA authority or generated locally, which will be sent to the server to authenticate the client's identity.

6. Configure transport settings.



Format Type	Specify the format type of the reported data. Available options are Json, Plaintext.
Device Class	Specify the vendors and protocols. Currently, only iBeacon, Eddystone, and Minew protocols are supported. More protocols will be supported in the future.
BLE Periodic Telemetry	Toggle on if you want to enable the periodic reporting of the AP.
Reporting Interval	Specify the interval period for the AP to report IoT data.
Report Device Counts Only	When enabled, the AP only reports the number of IoT devices.
BLE Data Forwarding	Toggle on if you want to enable the transparent transmission of the AP data.
RSSI Reporting Format	Specify the signal strength reporting format. Currently, Average, Max, Last, Smooth, and Bulk are supported.
Filters	Specify the custom configuration items that control the AP to filter IoT devices. Currently, Company Identifier, Vendor, Local Name, Service UUID, MAC OUI, iBeacon UUID, UID, and URL are supported.

7. Click Apply. The profile will be added and applied to Bluetooth-enabled APs. You can go to Devices > Configuration Result to check whether the configuration is applied to the corresponding APs successfully.

11.4 Configure Bluetooth Advertising

The Bluetooth Advertising function allows Bluetooth-enabled APs to send out specific BLE broadcast

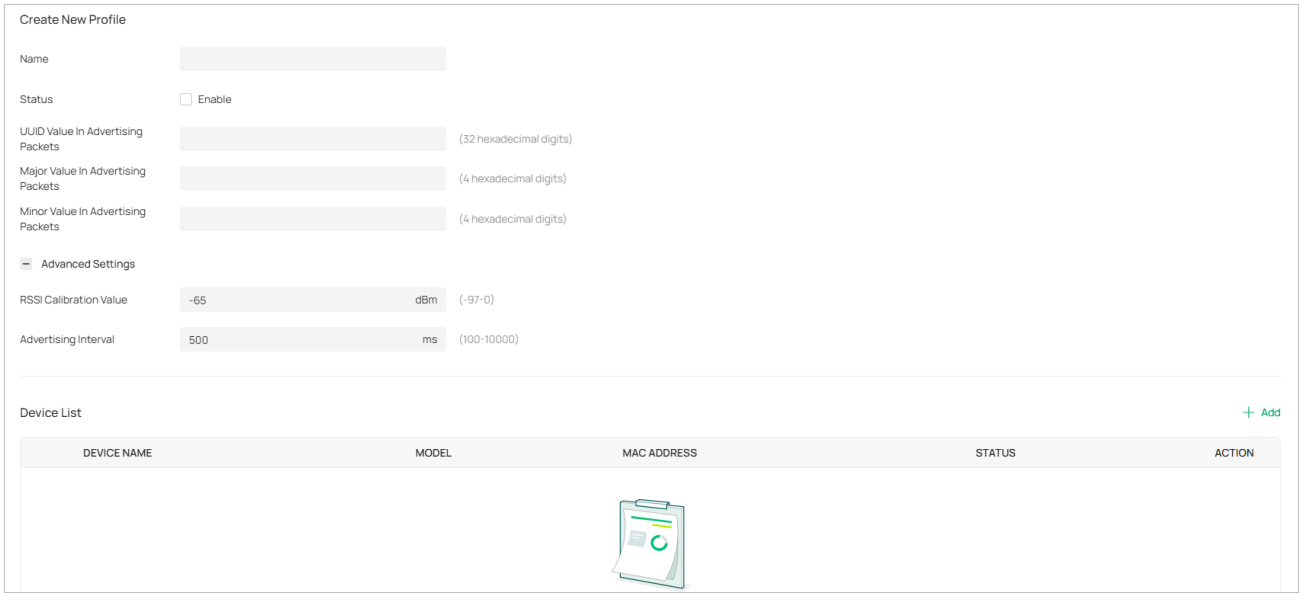
frames according to the set configuration. Currently, it only supports broadcasting iBeacon frames, and more protocols will be supported in the future.

There is a default rule in the initial interface, which can be turned off but cannot be deleted.

You can also add Bluetooth Advertising profiles and apply them to specific APs.

To add a Bluetooth Advertising profile, follow the steps below:

1. Launch the controller and access a site.
2. Go to Device Config > EAP > Bluetooth > Bluetooth Advertising.
3. Click Create New Profile to create a Bluetooth Advertising profile. Configure the parameters.



Name	Enter the name of the profile.
Status	Toggle on to enable this profile on Bluetooth-enabled APs.
UUID Value In Advertising Packets	Specify the Universally Unique Identifier (UUID) of the broadcast iBeacon device, which is the unique identifier of the universal device.
Major Value In Advertising Packets	Specify the major value of the broadcast iBeacon device, used to mark larger groups.
Minor Value In Advertising Packets	Specify the minor value of the broadcast iBeacon device, used to mark smaller groups.
RSSI Calibration Value	Specify the RSSI calibration value (dB).
Advertising Interval	Specify the interval of advertising frames.

Device List	Click Add and select devices to apply this profile. Only Bluetooth-enabled APs will be listed for selection. Notes: 1. The default site-level entry does not have this configuration item. Only custom entries support the configuration of specific devices. 2. Currently, a single device is supported to configure a Bluetooth Custom configuration entry for advertising.

4. Click Create. The profile will be added and applied to the Bluetooth-enabled APs you selected. You can go to Devices > Configuration Result to check whether the configuration is applied to the corresponding APs successfully.