



Bridge AP User Guide

© 2026 TP-Link 1900004320 REV1.0.0

Note: Features available in the AP may vary by model and software version. All images, steps, and descriptions in this guide are only examples and may not reflect your actual product experience.

CONTENTS

About This Guide	1
Overview	2
1 Quick Start.....	3
1.1 Determine the Management Method.....	4
1.2 Set Up a Bridge Network	5
1.2.1 Auto Pairing	5
1.2.2 Pairing with the Pair Button	6
1.2.3 Pairing with the Pairing Code Switches	6
1.3 Manage the Network.....	7
2 System Overview	12
3 Monitor Network Status.....	15
3.1 Monitor the Bridge AP	16
3.2 Monitor Wireless Status	17
3.3 Monitor the Clients	19
4 Manage the Bridge Network.....	21
4.1 View the Network Topology.....	22
4.2 Manage Bridge APs	22
4.3 Add Client APs	24
4.4 Run a Speed Test	25
4.5 Configure Channel Optimization	26
5 Configure Wireless Settings	27
5.1 Configure Wireless Radio Settings	28
5.1.1 Configure the SSID.....	28
5.1.2 Configure Wireless Advanced Settings	31
5.1.3 Configure the Wireless VLAN.....	33
5.2 Configure Bridging Radio Settings.....	34

5.2.1	Configure Radio Settings.....	34
5.2.2	Configure TDMA.....	36
5.3	Configure Rogue AP Detection.....	37
6	Configure PoE.....	39
6.1	Configure PoE Parameters.....	40
6.2	Configure the PoE Profile.....	41
7	Manage the Bridge AP	43
7.1	Manage Bridge APs	44
7.2	Manage the IP Address of the Bridge AP	45
7.3	Manage System Logs	46
7.4	Configure Web Server.....	49
7.5	Configure Management Access.....	50
7.6	Configure LED Control.....	51
7.7	Configure LAN Port	51
7.8	Configure SSH.....	52
7.9	Configure SNMP	52
8	Manage the System.....	55
8.1	Configure the User Account	56
8.2	Configure Controller Settings.....	56
8.3	Configure the System Time.....	58
8.3.1	Configure the System Time	58
8.3.2	Configure Daylight Saving Time.....	60
8.4	Run a Network Diagnostic.....	61
8.5	Reboot and Reset the Bridge AP	62
8.6	Backup and Restore the Configuration.....	63
8.7	Update the Firmware	63

About This Guide

When using this guide, notice that features available in the Bridge AP may vary by model and firmware version. Availability of the Bridge AP may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit <https://www.omadanetworks.com>.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure the 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 product.

Ethernet Port Limitation Disclaimer

Actual network speed may be limited by the rate of the product's Ethernet WAN or LAN port, the rate supported by the network cable, Internet service provider factors and other environmental conditions.

Lightning and Electro-Static Discharge Protection Disclaimer

Protection against lightning and electro-static discharge may be achieved through proper product setup, grounding and cable shielding. Refer to the instruction manual and consult an IT professional to assist with setting up this product.

More Info

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit <https://www.omadanetworks.com>.

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

The Quick Installation Guide can be found where you find this guide or inside the package of the Bridge AP.

The authentication information can be found where you find this guide.

Specifications can be found on the product page at <https://www.omadanetworks.com>.

Overview

Omada Bridge APs are access points designed for point-to-point (PtP) and point-to-multipoint (PtMP) wireless bridging. They extend your network to another building or remote area without running cables, perfect for scenarios like remote surveillance monitoring and Wi-Fi extension.

Bridge APs can either work independently as standalone bridge groups (Standalone Mode) or be centrally managed by a controller (Controller Mode), providing a flexible, richly-functional but easily configured bridge network.

This guide introduces how to quickly set up Bridge APs in Standalone Mode.

1 *Quick Start*

This chapter introduces how to set up and manage the Bridge network. Follow the steps below:

1.1 Determine the Management Method

1.2 Set Up a Bridge Network

1.3 Manage the Network

1.1 Determine the Management Method

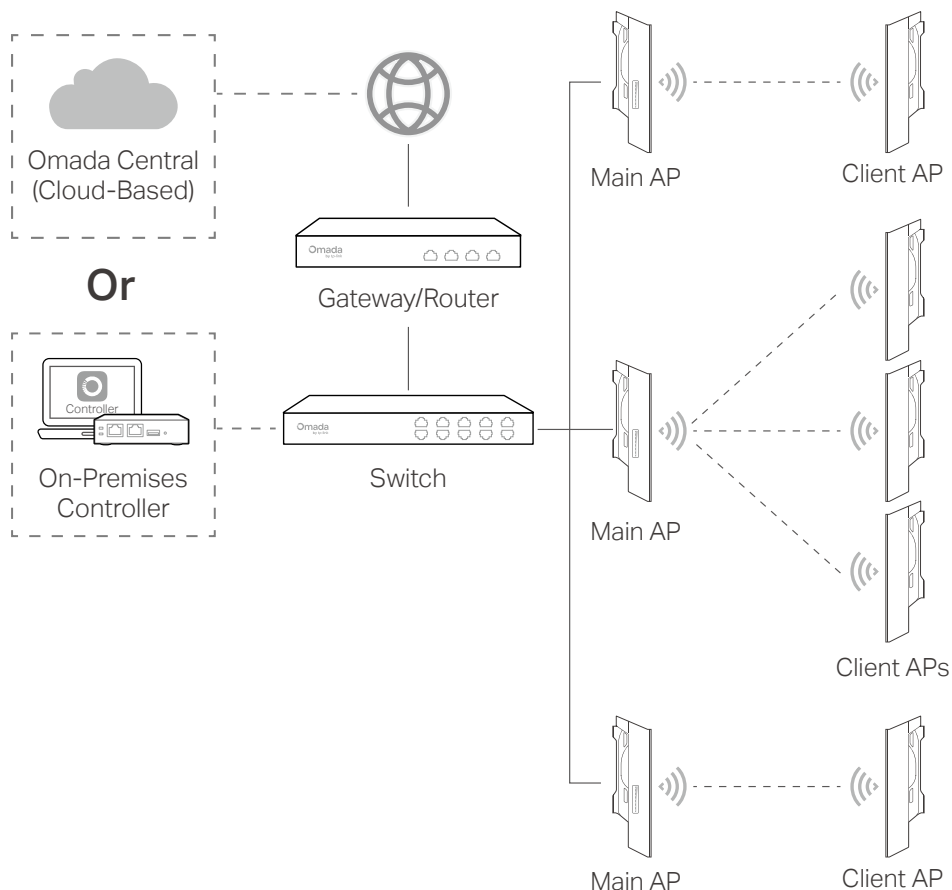
Before building your network, choose a proper method to manage your Bridge APs. You have the following options:

■ Controller Mode

If you want to manage a large-scale network centrally, choose Controller Mode. In Controller Mode, you can configure and monitor mass APs, switches, gateways, and more centrally via a compatible controller.

Note:

The figure below uses EAP211-Bridge for demonstration. Other types of Bridge APs can be used in a similar manner.



For more information, go to <https://www.omadanetworks.com/en/business-networking/omada/controller/>.

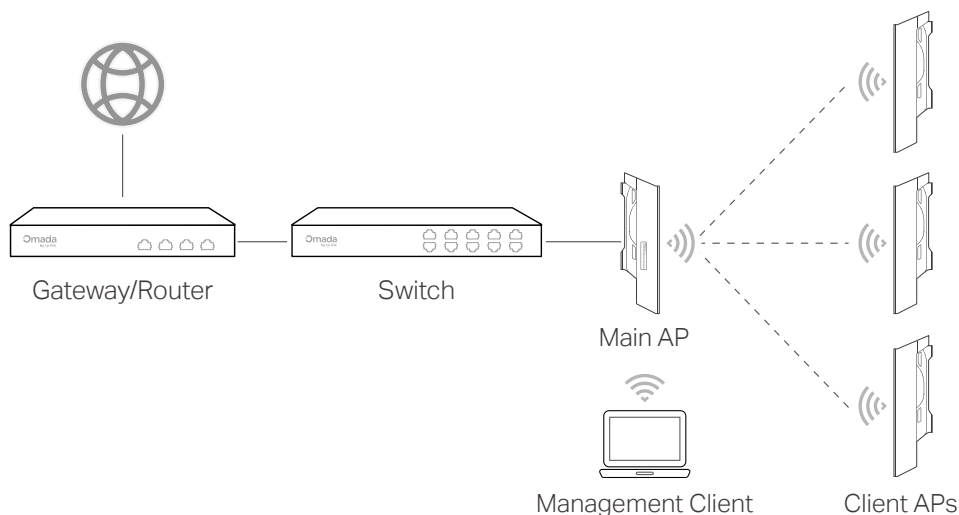
■ Standalone Mode

If you want to manage only a few Bridge APs, choose Standalone Mode. In Standalone Mode, you can singly configure and monitor your Bridge APs via Omada app or a web browser, and each Bridge AP has its own management page. For a bridge network, you can

configure and manage Bridge APs through the Main AP.

Note:

The figure below uses EAP211-Bridge for demonstration. Other types of Bridge APs can be used in a similar manner.



This guide introduces how to quickly set up Bridge APs in Standalone Mode.

Note:

- Standalone Mode is inaccessible while the Bridge AP is managed by a controller. To turn the Bridge AP back to Standalone Mode, you can forget the Bridge AP on the controller or reset the Bridge AP.
- To make your Bridge APs discovered by the controller, you need to configure [8.2 Configure Controller Settings](#) in certain scenarios.

1.2 Set Up a Bridge Network

Bridge APs support both PtP and PtMP networking via auto pairing, pairing with the Pair button, and/or pairing with the Pairing Code switches.

This section briefly introduces the pairing methods.

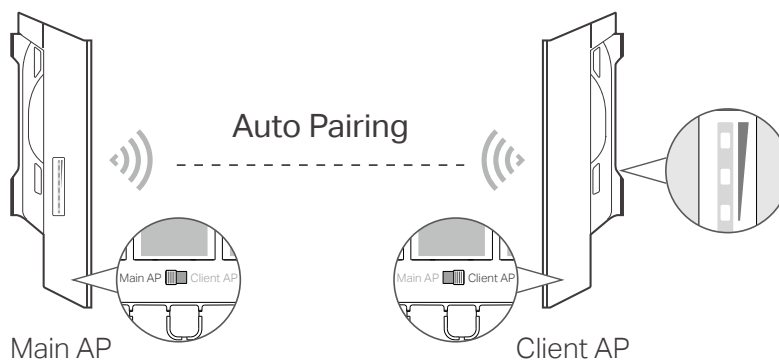
For detailed instructions, refer to the Installation Guide included in the product package or on the product support page (<https://support.omadanetworks.com/product/>). You can also refer to the Bridge AP Start Guide on the official website (<https://support.omadanetworks.com/document/27792/>).

1.2.1 Auto Pairing

For a Bridge KIT product, the Main AP and Client AP in the same kit will automatically form a PtP bridge network after powering on.

Note:

The figure below uses EAP211-Bridge KIT for demonstration. Other types of Bridge kits can be used in a similar manner.



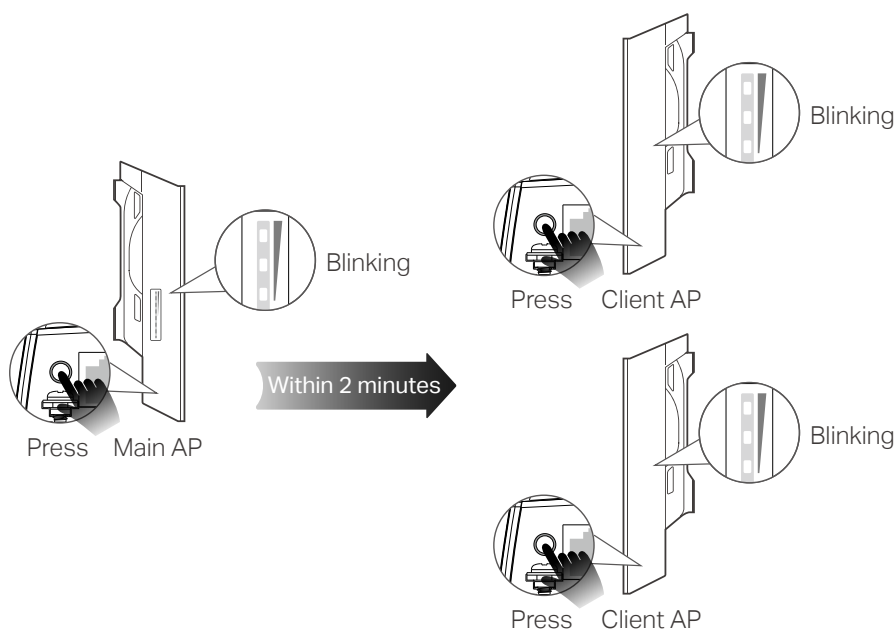
1.2.2 Pairing with the Pair Button

For models that feature the Pair button, you can pair multiple Client APs with the Main AP to form a PtMP network.

Note:

Flex Bridge 5 and Sector Bridge 5 do not provide the Pair button.

The figure below uses EAP211-Bridge for demonstration. Other types of Bridge kits can be used in a similar manner.



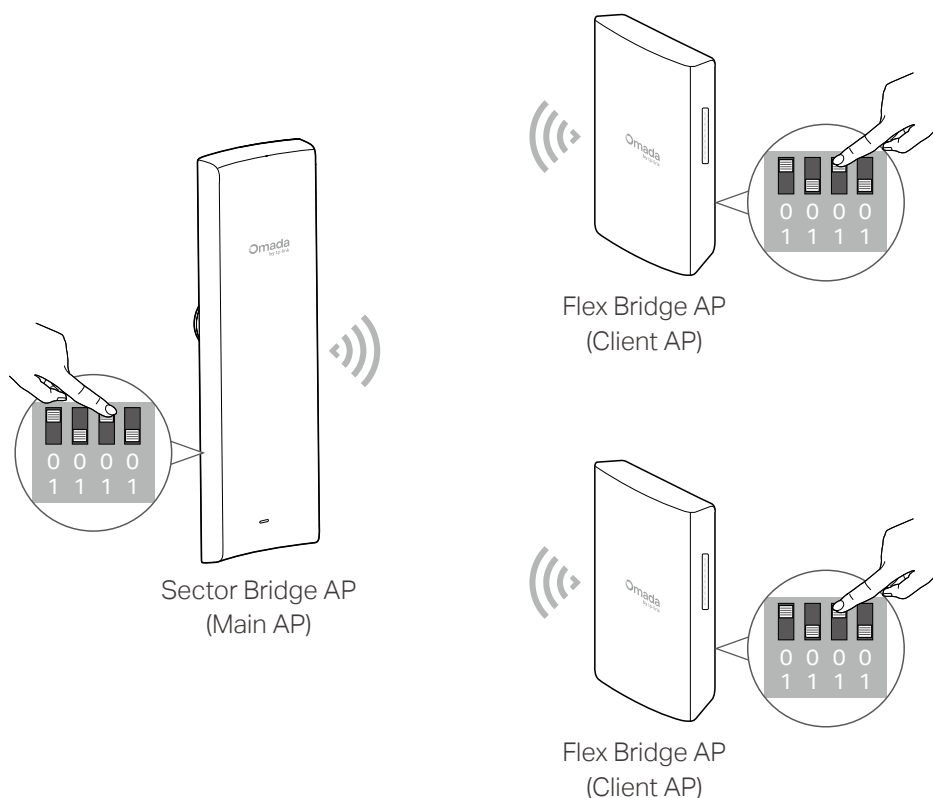
1.2.3 Pairing with the Pairing Code Switches

For models that feature Pairing Code switches, you can set the same pairing code for multiple Client APs and the Main AP to form a PtMP network.

Note:

Currently only Flex Bridge 5 and Sector Bridge 5 provide the Pairing Code switches.

The figure below uses Sector Bridge 5 (Main AP) and Flex Bridge 5 (Client AP) for demonstration. Other types of Bridge APs with Pairing Code switches can be used in a similar manner.



1.3 Manage the Network

If you want to manage the network, set up the Bridge AP using either the Omada app on your mobile device or the web browser on your PC. Choose a method from the following sections and follow the instructions.

Notes:

- Only one user is allowed to log in to the Bridge AP at one time.
- Omada app is designed to help you quickly configure some basic settings. To configure advanced functions, use the web browser on your PC.
- Omada app is only compatible with certain firmware versions of the Bridge AP. To check the firmware versions of the supported Bridge APs, please refer to https://www.omadanetworks.com/omada_compatibility_list/.

• Method 1: Set Up via the Omada App

1. Download and install the TP-Link Omada App from the App Store or Google Play.



2. Connect your mobile device to the Wi-Fi of the Main AP.

Note:

The default SSID is printed on the product and is only for device access and management.

3. Launch the Omada app, go to **Standalone Mode > Bridge**. The Omada app will discover and list all the Bridge APs in the current bridge network.
4. Tap on the Main AP and follow the app instructions to complete the initial setup.

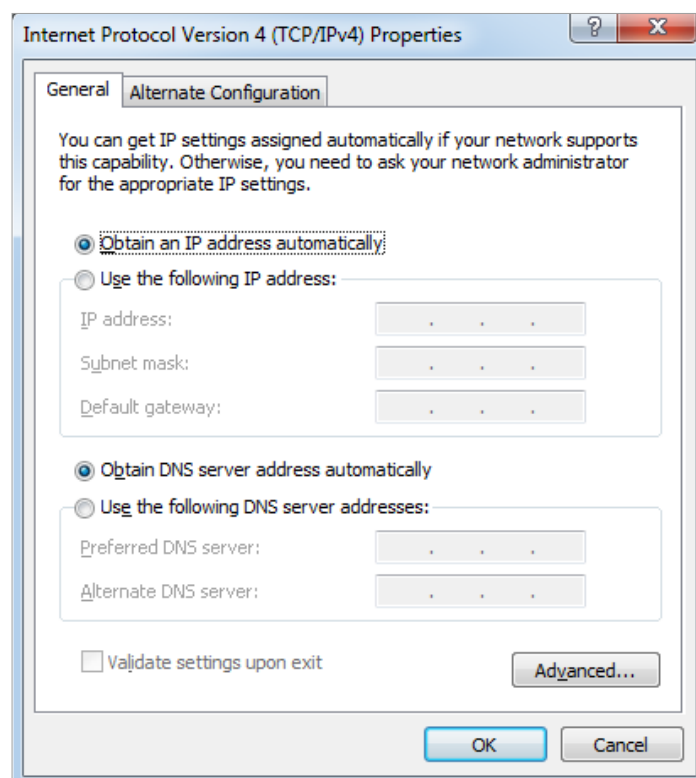
The app will automatically scan for the Client AP in the same kit as the Main AP and connect it to the network.

Note:

If you cannot access the internet, refer to [Troubleshooting of wireless issues for Omada AP products](#).

• **Method 2: Set Up via a Web Browser (login via the AP domain name)**

1. Make sure your PC is set to obtain an IP address automatically.

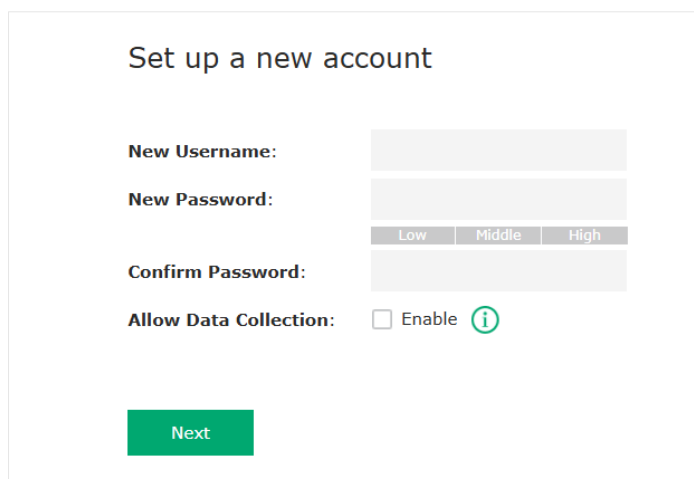


2. Connect your PC to the Main AP via the AP Wi-Fi or an Ethernet cable.

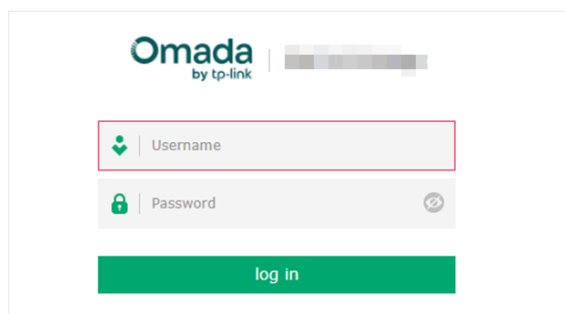
Note:

The default SSID is printed on the product and is only for device access and management.

3. Launch a web browser and enter <https://omadaeap.net> in the address bar. The web page will be displayed.
4. Set up the username and password for login to the web page.

**Note:**

For some models with earlier firmware, the initial web page may require the default login username and password. In this case, enter **admin / admin** to log in, then set up a new username and password.



5. Follow the step-by-step web instructions to complete the initial setup.

If you connect to the Main AP of a Bridge kit product, the system will automatically scan for the Client AP in the kit and connect it to the network.

Note:

If you cannot access the internet, refer to [Troubleshooting of wireless issues for Omada AP products](#).

- **Method 3: Set Up via a Web Browser (login via the AP IP address)**

1. Connect your PC to the Main AP via the AP Wi-Fi or an Ethernet cable.

2. Get the IP address of the Main AP. In a network without a DHCP Server, the Main AP will use the DHCP fallback IP address **192.168.0.254**. In other cases, get the IP address using one of the following methods.

- Using the DHCP Client List of the Gateway/Router

Log in to your gateway/router which acts as the DHCP server. In the DHCP client list, find the IP address of your Bridge AP according to its MAC address. The MAC address can be found on the Bridge AP. In the following figure, for example, the IP address of the Bridge AP is **192.168.0.118**.

DHCP Client List				
Total Clients: 1				Refresh
ID	Client Name	MAC Address	Assigned IP Address	Lease Time
1	[REDACTED]	B0-4E-26-[REDACTED]	192.168.0.118	01:59:30

- Using the Omada Discovery Utility

Go to <https://support.omadanetworks.com/download/software/omada-discovery-utility/> to download, install and launch AP Discovery Utility on your PC. AP Discovery Utility can scan all APs in the same network segment, and find the IP address of the AP. In the following figure, for example, the IP address of the Bridge AP is **192.168.0.5**.

[illegible]

Note:

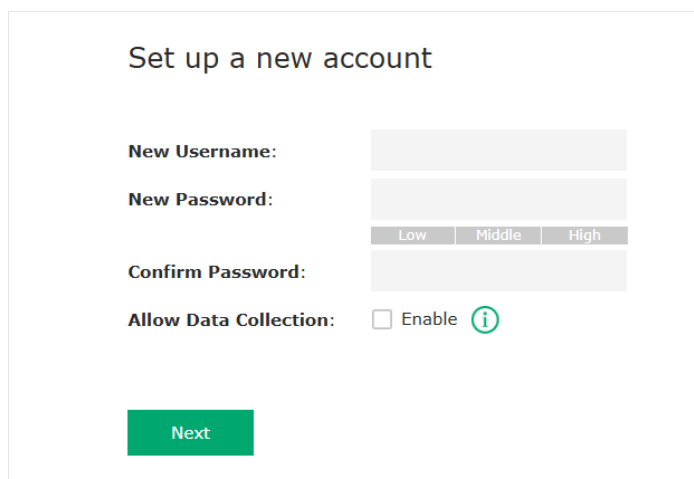
Some Bridge AP models only works with certain software version of Discovery Utility. If your Discovery Utility can't discover your Bridge AP anyway, try a different software version.

3. Launch a web browser and enter the IP address of the Main AP in the address bar. The web page will be displayed.

Tip:

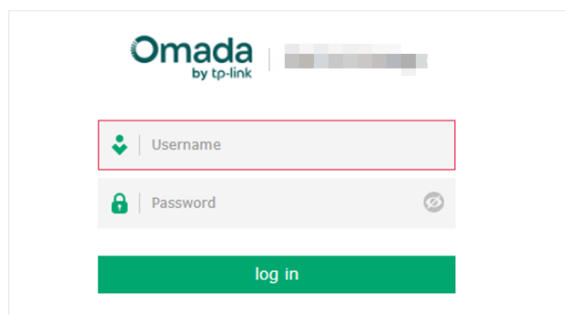
To facilitate access to the Bridge AP, you can set a static IP address for the Bridge AP and remember it well or write it down. But make sure that this IP address is not being used by other devices in the same LAN. For detailed instructions about how to set a static IP address for the Bridge AP, refer to [7.2 Manage the IP Address of the Bridge AP](#).

4. Set up the username and password for login to the web page.



Note:

For some models with earlier firmware, the initial web page may require the default login username and password. In this case, enter **admin / admin** to log in, then set up a new username and password.



5. Follow the step-by-step web instructions to complete the initial setup.

The system will automatically scan for the Client AP in the same kit as the Main AP and connect it to the network.

Note:

If you cannot access the internet, refer to [Troubleshooting of wireless issues for Omada AP products](#).

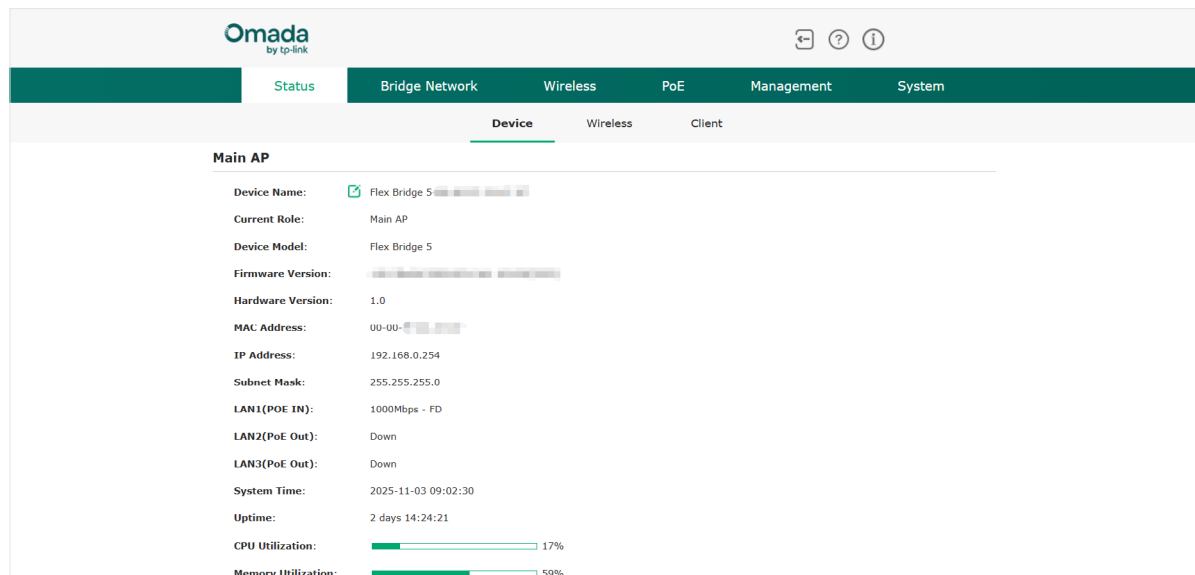
2 *System Overview*

This chapter provides a brief introduction to the web management page so you can quickly find the functions you need under the corresponding tabs:

If you use the web browser to configure your Bridge AP, you can configure more advanced functions according to your needs, and manage it conveniently on the web page.

Note:

Features available in the Bridge AP and the UI layout may vary by model and software version.



In the upper right of the page, you can:

Click  to log out.

Click  to go to the technical support page.

Click  to open the About page.

The tabs on the page allow you to access different configurations. The following table introduces what you can configure under each tab, and the following chapters discuss these topics in detail.

Status	View the information of the device, wireless traffic, and clients.
Bridge Network	View the topology and manage the Bridge APs in the Bridge network, run a speed test, and optimize channels.
Wireless	Configure management and bridging radio settings and detect rogue APs.
PoE (Only for Bridge APs with PoE Out ports)	Configure the PoE Out power and port settings and set the PoE profile.
Management	Manage the Bridge AP and network, and configure management features, such as System Logs, Web Server, LED Control, and more.

System

Configure system parameters, such as the login account, controller settings, and system time. In addition, you can diagnose device issues, reboot and reset the Bridge AP, backup and restore configurations, and update the firmware.

3

Monitor Network Status

This chapter introduces how to monitor the running status and statistics of the wireless network, including:

- *3.1 Monitor the Bridge AP*
- *3.2 Monitor Wireless Status*
- *3.3 Monitor the Clients*

3.1 Monitor the Bridge AP

To monitor the Bridge AP, go to **Status > Device**.

Main AP

Device Name:

 Flex Bridge 5 

Current Role:

Main AP

Device Model:

Flex Bridge 5

Firmware Version:



Hardware Version:

1.0

MAC Address:

00-00-

IP Address:

192.168.0.254

Subnet Mask:

255.255.255.0

LAN1(PoE IN):

1000Mbps - FD

LAN2(PoE Out):

Down

LAN3(PoE Out):

Down

System Time:

2025-11-03 09:02:30

Uptime:

2 days 14:24:21

CPU Utilization:

17%

Memory Utilization:

59%

The following device information will be displayed:

Device Name	Displays the name of the Bridge AP. The name consists of the product model followed with the MAC address of the Bridge AP by default.
Current Role	Displays the current role of the Bridge AP: Main AP or Client AP.
Device Model	Displays the product model of the Bridge AP.
Firmware Version	Displays the current firmware version the Bridge AP. To update the firmware, you can refer to 8.7 Update the Firmware .
Hardware Version	Displays the hardware version the Bridge AP.
MAC Address	Displays the MAC address of the Bridge AP.
IP Address	Displays the IP address of the Bridge AP.
Subnet Mask	Displays the subnet mask of the Bridge AP.
LAN	Displays the LAN port status of the Bridge AP.
System Time	Displays the current system time. To configure the system time, you can refer to 8.3 Configure the System Time .
Uptime	Displays how long the Bridge AP has been working since it starts up.

CPU Utilization	Displays the CPU occupancy. If this value is too high, the Bridge AP may work abnormally.
Memory Utilization	Displays the memory occupancy.

3.2 Monitor Wireless Status

You can monitor wireless status of the Bridge AP, including SSID lists, radio settings, radio traffic, and LAN traffic.

To monitor wireless status, go to **Status > Wireless**.

SSID List							
							 Refresh
ID	SSID Name	Clients	Band	Security	VLAN ID	Down (Byte)	Up (Byte)
1	dqdq		5GHz	WPA-PSK	Disable	0	0

Radio Settings	
5GHz Wireless Radio:	Enable
Channel Frequency:	44 / 5220MHz
Channel Width:	80MHz
IEEE802.11 Mode:	a/n/ac/ax mixed
Max TX Rate:	2402.0Mbps
Tx Power:	30dBm

Radio Traffic			
Rx Packets:	7	Tx Packets:	9769
Rx Bytes:	731	Tx Bytes:	85518
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

LAN Traffic			
Rx Packets:	12303	Tx Packets:	14365
Rx Bytes:	3117371	Tx Bytes:	11218841
Rx Dropped Packets:	0	Tx Dropped Packets:	0
Rx Errors:	0	Tx Errors:	0

- **Monitor the SSIDs**

You can monitor the SSID information of the Bridge AP.

SSID Name	Displays the SSID name.
Clients	Displays the number of clients currently connected to the SSID.
Band	Displays the frequency band the SSID is currently using.
Security	Displays the security mode of the SSID.
VLAN ID	Displays the VLAN ID of the SSID.
Down (Byte)	Displays the total download traffic since the SSID starts working.
Up (Byte)	Displays the total upload traffic since the SSID starts working.

- **Monitor the Radio Settings**

You can monitor the radio settings of the Bridge AP.

Wireless Radio	Displays whether wireless function is enabled on the radio band.
Channel Frequency	Displays the channel and frequency which are currently used by the Bridge AP.
Channel Width	Displays the channel width which is currently used by the Bridge AP.
IEEE802.11 Mode	Displays the IEEE802.11 protocol currently used by the Bridge AP.
Max TX Rate	Displays the maximum physical rate of the Bridge AP.
Tx Power	Displays the transmit power of the Bridge AP.

- **Monitor Radio Traffic**

You can monitor the radio traffic of the Bridge AP.

Rx Packets	Displays the total number of the received packets on the current band since the Bridge AP starts up.
Tx Packets	Displays the total number of the sent packets on the current band since the Bridge AP starts up.
Rx Bytes	Displays the total received traffic on the current band since the Bridge AP starts up.
Tx Bytes	Displays the total sent traffic on the current band since the Bridge AP starts up.

Rx Dropped Packets	Displays the total number of the dropped packets which are received on the current band since the Bridge AP starts up.
Tx Dropped Packets	Displays the total number of the dropped packets which are sent on the current band since the Bridge AP starts up.
Rx Errors	Displays the total number of error packets which are received on the current band since the Bridge AP starts up.
Tx Errors	Displays the total number of error packets which are sent on the current band since the Bridge AP starts up.

- **Monitor LAN Traffic**

You can view the LAN traffic of Bridge AP.

Rx Packets	Displays the total number of received packets in the LAN since the Bridge AP starts up.
Tx Packets	Displays the total number of sent packets in the LAN since the Bridge AP starts up.
Rx Bytes	Displays the total received traffic in the LAN since the Bridge AP starts up.
Tx Bytes	Displays the total sent traffic in the LAN since the Bridge AP starts up.
Rx Dropped Packets	Displays the total number of the dropped packets which are received by the Bridge AP since it starts up.
Tx Dropped Packets	Displays the total number of the dropped packets which are sent by the Bridge AP since it starts up.
Rx Errors	Displays the total number of the received error packets since the Bridge AP starts up.
Tx Errors	Displays the total number of the sent error packets since the Bridge AP starts up.

3.3 Monitor the Clients

You can monitor the clients connected to the Bridge AP.

To monitor the clients, go to **Status > Client**.

Client List										
										 Refresh
ID	Hostname	IP Address	MAC Address	Band	SSID	Active Time	Up (Byte)	Down (Byte)	RSSI (dBm)	Rate (Mbps)
1	Unknown	192.168.5.101		2.4GHz	603	0 days 00:00:50	3k	476	-54	1.0

The following client information will be displayed:

Hostname	Displays the hostname of the user.
IP Address	Displays the IP address of the user.
MAC Address	Displays the MAC address of the user.
Band	Displays the frequency band the user is working on.
SSID	Displays the SSID the user is connecting to.
Active Time	Displays how long the user has been connected to the SSID.
Up (Byte)	Displays the user's total uploaded traffic to the Bridge AP since the last connection.
Down (Byte)	Displays the user's total downloaded traffic from the Bridge AP since the last connection.
RSSI (dBm)	Displays the RSSI(Received Signal Strength Indication) of the user.
Rate (Mbps)	Displays the wireless transmission rate of the user.

4 *Manage the Bridge Network*

This chapter introduces how to manage the bridge network, including:

- *4.1 View the Network Topology*
- *4.2 Manage Bridge APs*
- *4.3 Add Client APs*
- *4.4 Run a Speed Test*
- *4.5 Configure Channel Optimization*

4.1 View the Network Topology

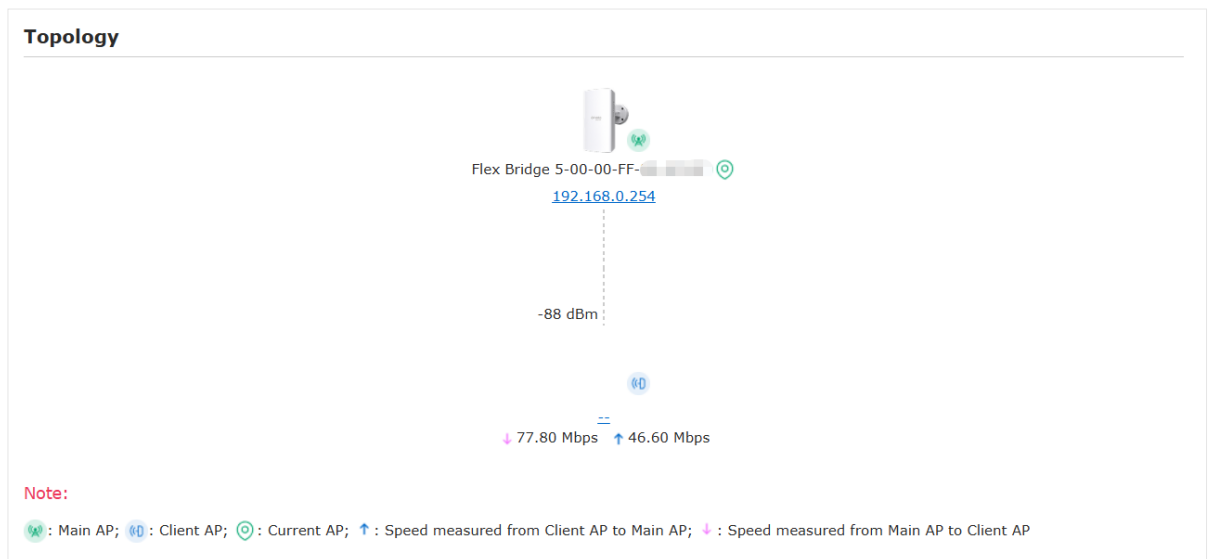
The topology displays the Bridge APs in the bridge network and their connection information graphically.

To view the topology, go to **Bridge Network > Topology**.

In the topology, you can view the Main AP and Client AP(s) in the current network, the signal strength of the connection, and the link speed between them.

Note:

The UI layout may vary by model and software version.



4.2 Manage Bridge APs

The Bridge AP list displays the basic information about the Bridge APs in the bridge network in a table.

To view the list, go to **Bridge Network > Bridge APs List**.

In the list, you can view the basic information about Main AP and Client AP(s) in the current network.

Bridge APs List (2/9)

 Refresh

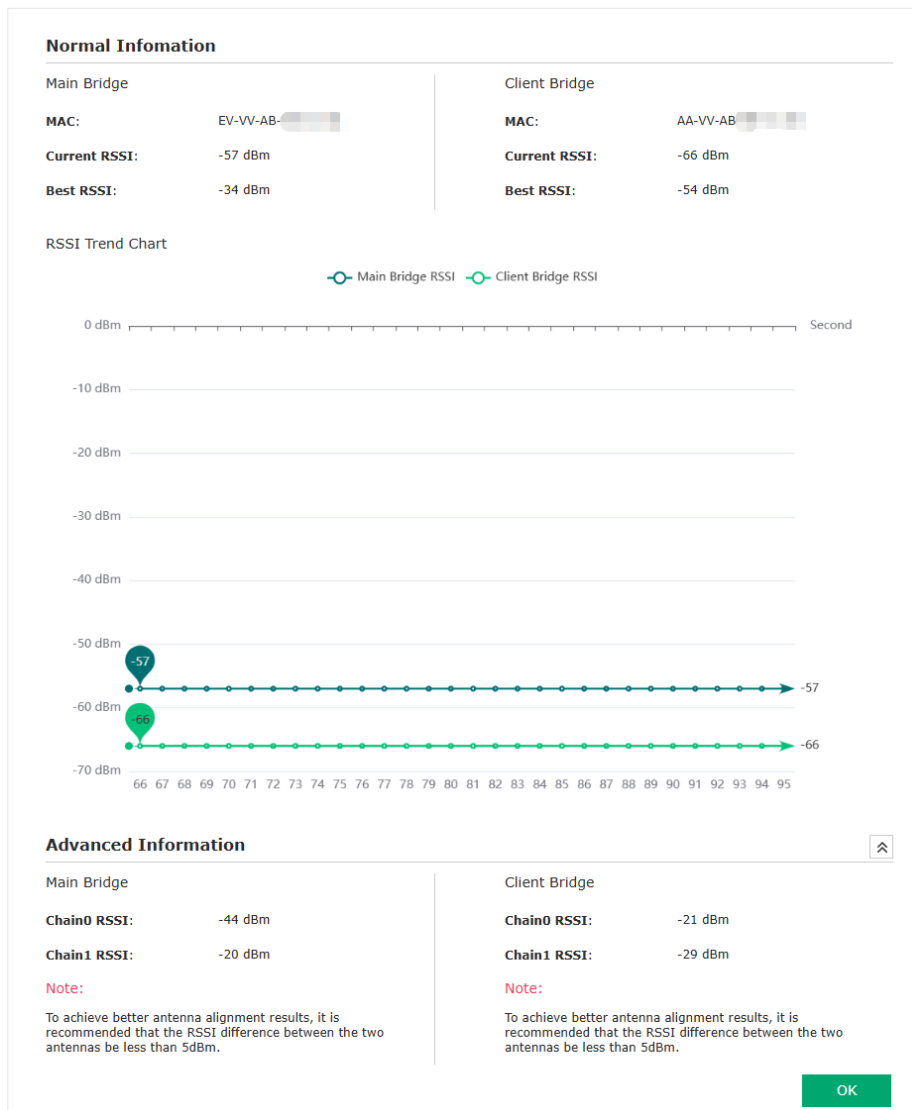
ID	Device	Type	IP Address	MAC Address	Action
1	Sector Bridge 5- (Current AP)	Main AP	192.168.0.254	00-5A- 	
2	Flex Bridge 5- 	Client-AP	192.168.0.100	DC-62- 	 

Note:

You can also use the Bridge Pairing Window to batch add Client APs set with the same pairing code as the Main AP. [Start Pairing Window](#)

[Add Client-AP](#)

For a Client AP, you can click the Launch icon in the Action column to open its web page, or click the Antenna Alignment icon to check the real-time RSSI values to assist in antenna calibration.



4.3 Add Client APs

Bridge APs support both PtP and PtMP networking. Apart from pairing via the physical button (such as the Pair button or Pairing Code switches), you can also add Client APs via the web page.

To add more Client APs, go to **Bridge Network > Bridge APs List**, and click the **Add Client AP** button.

Bridge APs List (2/9)

Refresh

ID	Device	Type	IP Address	MAC Address	Action
1	Sector Bridge 5 (Current AP)	Main AP	192.168.0.254	00-5A- 	
2	Flex Bridge 5- 	Client-AP	192.168.0.100	DC-62- 	 

Note:
You can also use the Bridge Pairing Window to batch add Client APs set with the same pairing code as the Main AP. [Start Pairing Window](#)

Add Client-AP

The system will automatically scan for Bridge APs nearby.

Select Client-APs to Add

Note:
You can also use the Bridge Pairing Window to batch add Client APs set with the same pairing code as the Main AP. [Start Pairing Window](#)

Device MAC	RSSI	Action
 Flex Bridge 5 00-FF- 	-73	☐

Cancel

Confirm

Select the Client AP to add and confirm the settings.

Tip:

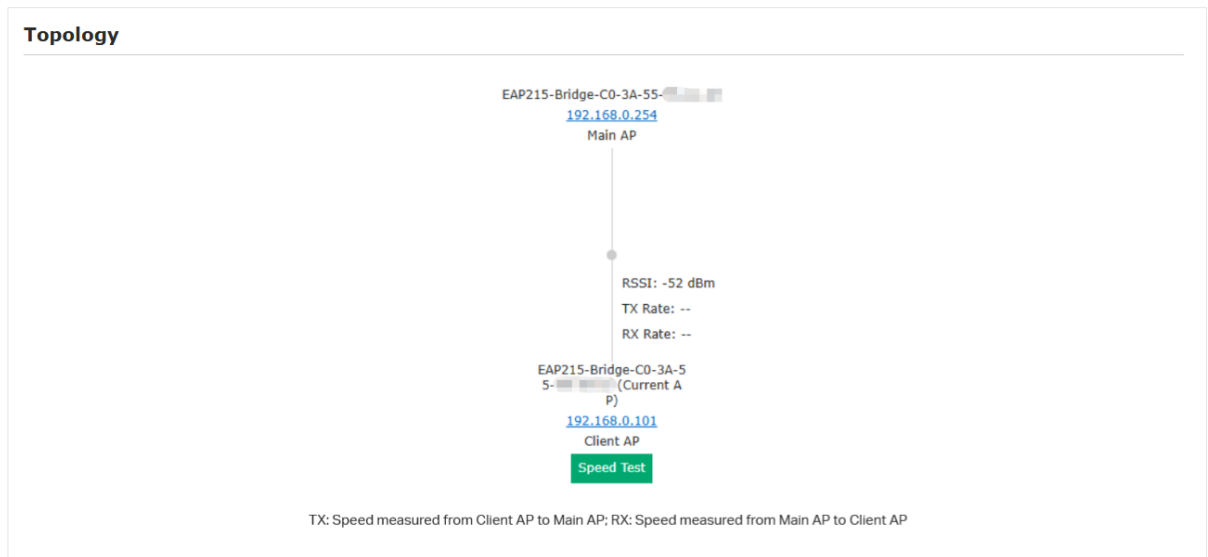
For models with Pairing Code switches, you can also use the Bridge Pairing Window to batch add Client APs set with the same pairing code as the Main AP.

4.4 Run a Speed Test

After setting up a Bridge network, you can test the speed between the Main AP and Client AP.

- **Method 1: Initiate a speed test on a Client AP**

Access the Client AP's web page, go to **Bridge Network > Topology**, then click the **Speed Test** button to test the link speed.



- **Method 2: Initiate a speed test on the Main AP**

Note:

Only for models supporting two-way speed measurement.

Access the Main AP's web page, go to **Bridge Network > Speed Test**, then select a Client AP and click **Start Speed Test**.

Speed Test

Client AP: - Please Select -

Start Speed Test

Note:

Speed test can be performed only after the Bridge AP is networked.
Up: Speed measured from Client AP to Main AP; Down: Speed measured from Main AP to Client AP

Speed Test History

Refresh

Client AP	Down	Up	Time
00:00:	77.80 Mbps	46.60 Mbps	

4.5 Configure Channel Optimization

DFS (Dynamic Frequency Selection) allows Wi-Fi device to use radar-shared 5 GHz channels. If radar is detected, the device automatically switches to another channel to avoid interference. You can enable the Bridge AP to scan for DFS channels if needed.

Note:

Using DFS channels in wireless bridge may lead to connection instability due to radar-triggered switching, comparability problems, and potential security threats during channel transitions.

To enable this feature, go to **Bridge Network > Channel Optimization**. Enable **Scan DFS Channel** and save the settings.

Scan DFS Channel

Scan DFS Channel: ☒ Enable ⓘ

Save

5

Configure Wireless Settings

This chapter introduces how to configure wireless settings of the Bridge AP, including:

- *5.1 Configure Wireless Radio Settings*
- *5.2 Configure Bridging Radio Settings*
- *5.3 Configure Rogue AP Detection*

5.1 Configure Wireless Radio Settings

In Wireless Settings, you can configure the SSID, wireless advanced settings, and wireless VLAN of the Bridge AP.

To configure wireless radio settings, go to **Wireless > Wireless Settings** (for common Bridge APs) or **Wireless > Wireless Settings > Management Radio** (for Flex Bridge 5 and Sector Bridge 5).

Note:

1. Client APs in the network will synchronize management wireless settings from the Main AP.
 2. The UI layout and available bands may vary by model.
- Example 1:

5GHz Wireless Radio

5GHz Wireless Radio: ☐ Enable

Save

VLAN ID

ID	SSID Name	Band	VLAN	VLAN ID
1	dqdq	5GHz	Disable ▼	0

Save

- Example 2:

Management Radio Bridging Radio

2.4GHz Wireless Radio

2.4GHz Wireless Radio: ☐ Enable

Save

VLAN ID

ID	SSID Name	Band	VLAN	VLAN ID
1	2g123456789	2.4GHz	Disable ▼	0

Save

5.1.1 Configure the SSID

Management SSID (Service Set Identifier) is used for wireless access of the management

client.

To configure the management SSID, follow the steps below:

1. Go to **Wireless > Wireless Settings** (for common Bridge APs) or **Wireless > Wireless Settings > Management Radio** (for Flex Bridge 5 and Sector Bridge 5).
2. Enable the wireless radio and save the settings.
3. Click **Add** to add an SSID.

ID	SSID	VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
--	--	--	--	--	--	--

SSID:

SSID Broadcast: ☒ Enable

Security Mode: None ▼

4. Configure the following parameters for this SSID:

SSID	Specify a name for the wireless network.
SSID Broadcast	With the option enabled, the device will broadcast the SSID to the nearby hosts, so that those hosts can find the wireless network identified by this SSID. If this option is disabled, users must enter the SSID manually to connect to the device.

5. Set the security mode. For network security, we recommend that you encrypt your wireless network.

Security Mode	Select the security mode of the wireless network. There are four options: None: Clients can access the wireless network without authentication. WPA-Enterprise: Clients need to pass the WPA-Enterprise (Wi-Fi Protected Access-Enterprise) authentication before accessing the wireless network. WPA-Enterprise (Wi-Fi Protected Access-Enterprise) is a safer encryption method compared with WEP and WPA-Personal. It requires a RADIUS server to authenticate the clients via 802.1X and AP (Extensible Authentication Protocol). WPA-Enterprise can generate different passwords for different clients, which ensures higher network security. But it also costs more to maintain the network, so it is more suitable for business networks. WPA-Personal: Clients need to pass the WPA-Personal authentication before accessing the wireless network. WPA-Personal is based on a pre-shared key. It is characterized by high safety and simple settings, so it is mostly used by common households and small businesses.
---------------	---

■ If you select **WPA-Enterprise**, configure the following parameters:

Version	Select the version of WPA-Enterprise according to your needs. If you select WPA/WPA2-Enterprise, the device automatically decides whether to use WPA-Enterprise or WPA2-Enterprise during the authentication process.
Encryption	Select the Encryption type. Note that some encryption type is only available under certain circumstances. Auto: The default setting is Auto and the device will select TKIP or AES automatically based on the client device's request. AES: Advanced Encryption Standard. It is securer than TKIP.
RADIUS Server IP	Enter the IP address of the RADIUS Server.
RADIUS Port	Enter the port number of the RADIUS Server.
RADIUS Password	Enter the shared secret key of the RADIUS server.
RADIUS Accounting	Enable or disable RADIUS accounting feature.
Accounting Server IP	Enter the IP address of the accounting server.
Accounting Server Port	Enter the port number of the accounting server.
Accounting Server Password	Enter the shared secret key of the accounting server.

Interim Update	With this option enabled, you can specify the duration between accounting information updates. By default, the function is disabled. Enter the appropriate duration between updates for devices in Interim Update Interval .
Interim Update Interval	With Interim Update enabled, specify the appropriate duration between updates for devices. The default duration is 600 seconds.
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the device should change the encryption key. 0 means that the encryption key does not change at anytime.

- If you select **WPA-Personal**, configure the following parameters:

Version	Select the version of WPA-Personal according to your needs. If you select WPA/WPA2-PSK, the device automatically decides whether to use WPA-PSK or WPA2-PSK during the authentication process.
Encryption	Select the Encryption type. Note that some encryption type is only available under certain circumstances. Auto: The default setting is Auto and the device will select TKIP or AES automatically based on the client device's request. AES: Advanced Encryption Standard. It is securer than TKIP.
Wireless Password	Configure the wireless password with ASCII characters. For ASCII, the length should be between 8 and 63 and the valid characters contain numbers, letters (case-sensitive) and common punctuations.
Group Key Update Period	Specify an update period of the encryption key. The update period instructs how often the device should change the encryption key. 0 means that the encryption key does not change at anytime.

6. Save the settings to create the SSID.

5.1.2 Configure Wireless Advanced Settings

Proper wireless advanced parameters for the management radio can improve the performance of your management network.

To configure wireless advanced settings, follow the steps below:

1. Go to **Wireless > Wireless Settings** (for common Bridge APs) or **Wireless > Wireless Settings > Management Radio** (for Flex Bridge 5 and Sector Bridge 5).
2. In the **Wireless Advanced Settings** section, configure the parameters.

Note:

Available bands and parameters may vary by model.

5GHz Wireless Advanced Settings

Radio Settings

Wireless Mode:

802.11a/n/ac mixed

Channel Width:

Auto

Channel Limit:

☐ Enable

Note:

With this feature enabled, the frequency ranging from 5150MHz to 5350MHz will not be used to meet the local laws and regulations when the EAP works outdoors.

Channel:

Auto

Tx Power(EIRP):

30

dBm(15-30)

Note:

The EIRP transmit power includes the antenna gain.

Save

Wireless Mode

Select the IEEE 802.11 mode the radio uses.

- For 2.4 GHz:

802.11b/g/n mixed is recommended so that all of 802.11b, 802.11g, and 802.11n clients operating in the 2.4 GHz frequency can connect to the device.

- For 5 GHz:

802.11a/n/ac mixed is recommended so that all of 802.11a, 802.11n, and 802.11ac clients operating in the 5 GHz frequency can connect to the device.

Channel Width

Select the channel width of the device. The available options differ among different devices.

We recommend you keep the default value **Auto** to improve the transmission speed. However, you may choose a lower bandwidth due to the following reasons:

- To increase the available number of channels within the limited total bandwidth.
- To avoid interference from overlapping channels occupied by other devices in the environment.
- Lower bandwidth can concentrate higher transmit power, increasing stability of wireless links over long distances.

Channel Limit	Check the box to enable the function. With this function enabled, the wireless frequency 5150MHz~5350MHz will be disabled. This function can influence the available options in Channel. Note: This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.
Channel	Select the channel used by the device. For example, 44/5220MHz for 5 GHz band means that the channel is 44 and the frequency is 5220MHz. We recommend you keep the default value Auto so the device can automatically select the channel.
Tx Power (EIRP)	Specify the transmit power value. If this value is set to be larger than the maximum transmit power that is allowed by the local regulation, the regulated maximum transmit power will be applied in the actual situation. Note: 1. This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface. 2. In most cases, it is unnecessary to use the maximum transmit power. Specifying a larger transmit power than needed may cause interference to the neighborhood. Also it consumes more power and reduces longevity of the device.

3. Save the settings.

5.1.3 Configure the Wireless VLAN

Wireless VLAN is used to set VLANs for the wireless networks. With this feature, the AP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks will be added with different VLAN tags according to the VLAN settings of the wireless networks. The wireless clients in different VLANs cannot directly communicate with each other. Note that the traffic from the wired clients will not be added with VLAN tags.

To configure the wireless VLAN on the Bridge AP, follow the steps below:

1. Go to **Wireless > Wireless Settings**.
2. In the **VLAN ID** section, enable the VLAN and set the VLAN ID.

Note:

Available bands may vary by model.

VLAN ID

ID	SSID Name	Band	VLAN	VLAN ID
1	2g123456789	2.4GHz	Enable ▼	1

Save

- Save the settings. Now traffic from the clients in this wireless network will be added with the VLAN tag corresponding to the specified VLAN ID.

5.2 Configure Bridging Radio Settings

For some dual-band models, you can configure radio settings and TDMA (Time-Division Multiple Access) to optimize connections between Bridge APs.

Note:

Currently only Flex Bridge 5 and Sector Bridge 5 support bridge radio settings.

To configure bridging radio settings, go to **Wireless > Wireless Settings > Bridging Radio**.

Management Radio

Bridging Radio

5GHz Wireless Advanced Settings

Radio Settings

Wireless Mode:

802.11a/n/ac mixed ▼

Channel Width:

Auto ▼

Channel:

Auto ▼

Tx Power:

23

dBm(4-23)

Save

TDMA:

☒ Enable ⓘ

☐	Client AP	TDMA Priority
☐	00-00-FF- 	Low Mode ▼ ⓘ

Save

5.2.1 Configure Radio Settings

Proper radio settings can improve the performance of your bridge network.

To configure radio settings, follow the steps below:

1. Go to **Wireless > Wireless Settings > Bridging Radio**.

Note:

Currently only Flex Bridge 5 and Sector Bridge 5 support bridge radio settings.

2. Configure radio settings.

5GHz Wireless Advanced Settings

Radio Settings

Wireless Mode:

802.11a/n/ac mixed

▼

Channel Width:

Auto

▼

Channel:

Auto

▼

Tx Power:

23

dBm(4-23)

Save

Wireless Mode

Select the IEEE 802.11 mode the radio uses.

802.11a/n/ac mixed is recommended so that all of 802.11a, 802.11n, and 802.11ac Bridge APs operating in the 5 GHz frequency can connect to this device.

Channel Width

Select the channel width of this device. The available options differ among different models.

We recommend you keep the default value **Auto** to improve the transmission speed. However, you may choose a lower bandwidth due to the following reasons:

- To increase the available number of channels within the limited total bandwidth.
- To avoid interference from overlapping channels occupied by other devices in the environment.
- Lower bandwidth can concentrate higher transmit power, increasing stability of wireless links over long distances.

Channel

Select the channel used by this device. For example, 44/5220MHz for 5 GHz band means that the channel is 44 and the frequency is 5220MHz.

We recommend you keep the default value **Auto** so the device can automatically select the channel.

Tx Power

Specify the transmit power value.

If this value is set to be larger than the maximum transmit power that is allowed by the local regulation, the regulated maximum transmit power will be applied in the actual situation.

Note:

In most cases, it is unnecessary to use the maximum transmit power. Specifying a larger transmit power than needed may cause interference to the neighborhood. Also it consumes more power and reduces longevity of the device.

3. Save the settings.

5.2.2 Configure TDMA

TDMA (Time-Division Multiple Access) optimizes wireless communication in PtMP bridge scenarios by eliminating signal interference between devices, ensuring stable and efficient data transmission across multiple wireless links.

Note:

The bridge network requires consistent TDMA status of Bridge APs. Do not enable TDMA if your Client APs do not support TDMA.

To configure TDMA, follow the steps below:

1. Go to **Wireless > Wireless Settings > Bridging Radio**.

Note:

Currently only Flex Bridge 5 and Sector Bridge 5 support bridge radio settings.

2. Enable TDMA and set the priority.

TDMA:

☒ Enable ?

☐	Client AP	TDMA Priority
☐	00-00-FF- 	Low Mode ?

Save

TDMA Priority

Select the TDMA priority for the Client AP.

Low Mode: Allocates fewer time slots. Network performance and latency may be less optimal, suitable for non-critical or background traffic.

Base Mode: Provides a balanced allocation of time slots. Network performance and latency remain stable and consistent, suitable for general-purpose bridge connection.

High Mode: Allocates a larger share of slots, delivering higher throughput and lower latency. Recommended for Client APs requiring prioritized performance.

3. Save the settings.

5.3 Configure Rogue AP Detection

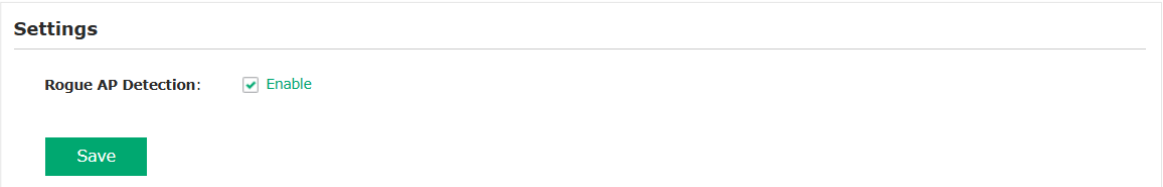
A Rogue AP is an access point that is installed on a secure network without explicit authorization from the network administrator. With Rogue AP Detection, the Bridge AP can scan all channels to detect the nearby APs and display the detected APs in the **Detected Rogue AP** list.

Note:

The Rogue AP Detection feature is only used for collecting information of the nearby wireless network and does not impact the detected APs, no matter what operations you have executed in this feature.

To configure Rogue AP Detection, follow the steps below:

1. Go to **Wireless > Rogue AP Detection**.
2. In the **Settings** section, check the box to enable **Rogue AP Detection**. Save the settings.



Settings

Rogue AP Detection: ☒ Enable

Save

3. In the **Detected Rogue AP List** section, click **Scan**.
4. Wait for a few seconds without any operation. After detection is finished, the detected APs will be displayed in the list.

Detected Rogue AP List							Scan
MAC	SSID	Band	Channel	Security	Beacon Interval	Signal	
00:00:00:00:00:00	!!!test1111	5GHz	149	ON	100		
60:3A:09:00:00:00	!!!!!!Solution	5GHz	149	ON	100		
82:3A:09:00:00:00		5GHz	149	ON	100		
0C:EF:15:00:00:00	BT_Office	5GHz	149	ON	300		
16:EF:15:00:00:00	BT_Technical	5GHz	149	ON	300		
00:00:FF:00:00:00		5GHz	153	ON	100		
3C:78:95:00:00:00		5GHz	153	ON	100		
82:3A:08:00:00:00		5GHz	149	ON	100		
3C:6A:D2:00:00:00	Omada_5GHz_05075E	5GHz	44	OFF	100		
5E:6A:D2:00:00:00		5GHz	44	ON	100		

The following table introduces the displayed information of the APs:

MAC	Displays the MAC address of the AP.
SSID	Displays the SSID of the AP.
Band	Displays the frequency band the AP is working on.
Channel	Displays the channel the AP is using.
Security	Displays whether the security mode is enabled on the AP.
Beacon Interval	Displays the Beacon Interval value of the AP. Beacon frames are sent periodically by the AP to announce to the stations the presence of a wireless network. Beacon Interval determines the time interval of the beacon frames sent by the AP device.
Signal	Displays the signal strength of the AP.

6

Configure PoE

PoE Out ports can transmit data and supply power to the powered devices (PDs) simultaneously. With the PoE feature, you can configure PoE settings for the PoE Out ports.

Note:

Currently only Flex Bridge 5 supports the PoE feature.

This chapter introduces how to configure PoE settings, including:

- *6.1 Configure PoE Parameters*
- *6.2 Configure the PoE Profile*

6.1 Configure PoE Parameters

To configure PoE parameters, follow the steps below:

1. Go to **PoE > PoE Config**.
2. In the **PoE Config** section, click the Edit icon of the device and set the **System Power Limit** if needed.

PoE Config

Refresh Auto Refresh

Device	System Power Limit(W)	System Power Consumption(W)	System Power Remain(W)	Action
Flex Bridge 5	10	0	10	

Device: Flex Bridge 5

System Power Limit: 10 W(3-10)

OK Cancel

System Power Limit (w)

Specify the maximum power the device can supply.

3. In the **Port Config** section, select the port(s) you want to configure and specify the parameters.

Port Config

Refresh Auto Refresh

Port	PoE Profile	PoE Status	PoE Priority	Power Limit	Power Limit Value(0.1-10W)	Time Range	Power(W)	Current(mA)	Voltage(V)	Power Status	Action
LAN2	Default None	Disabled	High	Manual	10	any	0	0	0	OFF	
LAN3	Default None	Disabled	High	Manual	10	any	0	0	0	OFF	

PoE Profile: Default None

PoE Status: ☐ Enable

PoE Priority: High

Power Limit: Manual

Power Limit Value: 10 W(0.1-10)

OK Cancel

Note:

When the output power margin is less than 3W, the remaining PoE Out port will be unable to output power.

The PoE Out function is unavailable due to insufficient input power (DC power or PoE power less than 48V). The configuration will take effect when the power supply is sufficient.

PoE Profile	Select Default None if you want to configure PoE settings manually, or select a PoE profile to apply preconfigured PoE settings automatically. To configure a PoE profile, refer to 6.2.
PoE Status	Specify the PoE status for the port. When enabled, the port can supply power to the PD.
PoE Priority	Specify the priority level for the port. When the supply power exceeds the system power limit, the device will power off PDs on low-priority ports to ensure stable running of other PDs.
Power Limit	Specify the maximum power the port can supply. Auto: The device will allocate the maximum power that the port can supply automatically. Class1: 4W Class2: 7W Manual: Set the Power Limit Value manually.

4. Save the settings.

6.2 Configure the PoE Profile

You can configure the PoE profile with the desired parameters and bind the profile to the corresponding ports to quickly configure PoE parameters.

To configure the PoE profile, follow the steps below:

1. Go to **PoE > PoE Profile**. Click **Add**.
2. Specify the desired PoE parameters.

PoE Profile Config

+

Add

↺

Refresh

Profile Name	PoE Status	PoE Priority	Power Limit	Action
--	--	--	--	--

Profile Name:

(1-16 characters)

PoE Status:

☐
Enable

PoE Priority:

High

▼

Power Limit:

Auto

▼

OK

Cancel

sample	Disabled	High	Auto	✎ 🗑
--------	----------	------	------	---------------------------

PoE Status	Specify the PoE status for the port. When enabled, the port can supply power to the PD.
PoE Priority	Specify the priority level for the port. When the supply power exceeds the system power limit, the device will power off PDs on low-priority ports to ensure stable running of other PDs.
Power Limit	Specify the maximum power the port can supply. Auto: The device will allocate the maximum power that the port can supply automatically. Class1: 4W Class2: 7W Manual: Set the Power Limit Value manually.

3. Save the settings. Now you can bind the profile when configuring a PoE port in **PoE > PoE Config > Port Config**.

7

Manage the Bridge AP

The Bridge AP provides powerful functions of device management and maintenance. This chapter introduces how to manage the Bridge AP, including:

- *7.1 Manage Bridge APs*
- *7.2 Manage the IP Address of the Bridge AP*
- *7.3 Manage System Logs*
- *7.4 Configure Web Server*
- *7.5 Configure Management Access*
- *7.6 Configure LED Control*
- *7.7 Configure LAN Port*
- *7.8 Configure SSH*
- *7.9 Configure SNMP*

7.1 Manage Bridge APs

To manage Bridge AP settings, go to **Management > Bridge AP Management**.

Note:

Features available in the Bridge AP may vary by model and firmware version.

Bridge AP Role

Current Role:

Main AP

Current IP:

192.168.0.254

DIP Switch:

☒ Enable

Set the Bridge AP's role:

☒ Main AP

☐ Client AP

i

Pair Code:

Save

Bridge Information

Bridge SSID:

Omada_Bridge_15

Bridging Password:

.....

🔒

Edit

Bridge Pairing Window

Hour

Minutes

02

00

Stop Pairing

Note:

During the countdown, Client APs set with the same pairing code as the Main AP will automatically join the network. Paired Client AP: 0

MAC Address	RSSI
--	--

Current Role	Displays the current working role of the Bridge AP: Main AP or Client AP.
Current IP	Displays the current IP address of the Bridge AP.
Hardware Role Switch	(For Bridge APs with the hardware Role switch) Control the hardware Role switch on the Bridge AP. If disabled, the hardware Role switch will no longer take effect.
DIP Switch	(For Bridge APs with hardware DIP switches) Control the hardware DIP switches on the Bridge AP, such as the Role switch and Pairing code switches. If disabled, the hardware DIP switches will no longer take effect.

Set the Bridge AP's Role	Configure the Bridge AP to work as the Main AP or Client AP. This option is unavailable when Hardware Role Switch or DIP Switch is enabled.
Bridge SSID / Password	Displays the Bridge SSID and password of the Bridge AP. Bridge APs with the same Bridge SSID and password will form a Bridge network. If needed, you can click the Edit button to change them. This option is unavailable when DIP Switch is enabled.
Bridge Pairing Window	(For Bridge APs with hardware DIP switches) This option is displayed on the Main AP only when DIP Switch is enabled. When the first Client AP connects to the Main AP, a 2-hour countdown begins on the Main AP. During the countdown, Client APs with the same Pairing Code as the Main AP can automatically join the network. To stop the countdown, click Stop Pairing . To start the pairing window again, click Start Pairing .

7.2 Manage the IP Address of the Bridge AP

The IP address of the Bridge AP can be a dynamic IP address assigned by the DHCP server or a static IP address manually specified by yourself. By default, the Bridge AP gets a dynamic IP address from the DHCP server. You can also specify a static IP address according to your needs.

To configure the IP address of the Bridge AP, follow the steps below:

1. Go to **Management > Network**.

IP Settings

☒ Dynamic
☐ Static

Fallback IP:

☒ Enable

DHCP Fallback IP:

192.168.0.254

DHCP Fallback IP Mask:

255.255.255.0

DHCP Fallback Gateway:

Save

2. Choose your desired IP address mode: **Dynamic** or **Static**.
3. Configure the related parameters according to your selection.

- **Dynamic**

If you choose Dynamic as the IP address mode, make sure that there is a reachable DHCP server on your network and the DHCP server is properly configured to assign IP address and the other network parameters to the Bridge AP.

For network stability, you can also configure the fallback IP parameters for the Bridge AP:

Fallback IP	With the fallback IP configured, if the Bridge AP fails to get an IP address from a DHCP server within 10 seconds, the fallback IP will work as the IP address of the Bridge AP. After that, however, the Bridge AP will keep trying to obtain an IP address from the DHCP server until it succeeds.
DHCP Fallback IP	Specify a fallback IP address for the Bridge AP. Make sure that this IP address is not being used by any other device in the same LAN. The default DHCP fallback IP is 192.168.0.254.
DHCP Fallback IP MASK	Specify the network mask of the fallback IP. The default DHCP fallback IP mask is 255.255.255.0.
DHCP Fallback Gateway	Specify the network gateway.

- **Static**

If you choose Static as the IP address mode, you need to manually specify an IP address and the related network parameters for the Bridge AP. Make sure that the specified IP address is not being used by any other device in the same LAN.

Configure the IP address and network parameters as the following table shows:

IP Address	Specify a static IP address for the Bridge AP.
IP Mask	Specify the network mask.
Gateway	Specify the network gateway.
Primary DNS	Specify the primary DNS server.
Secondary DNS	Specify the secondary DNS server. (Optional)

4. Click **Save**.

7.3 Manage System Logs

System logs record information about hardware, software as well as system issues and

monitors system events. With the help of system log, you can get informed of system running status and detect the reasons for failure.

To manage system logs, go to **Management > System Log**.

Log

 Refresh

Index	Time	Type	Level	Log Content
2	1970-01-01 08:00:52	DEV_IP_C	WARNING	The LAN IP address/mask of [ap:12-45-23-12-73-15] were changed to 192.168.0.38/255.255.255.0.
1	1970-01-01 00:00:22	OTHER	INFO	System started

Log Settings

Enable Auto Mail:☐ Enable

Enable Server:☐ Enable

Save

On this page, you can view the system logs and configure the way of receiving system logs.

- **View System Logs**

In the **Log** section, you can click **Refresh** to refresh the logs and view them in the table.

- **Configure the Way of Receiving Logs**

In the **Log Settings** section, you can configure the ways of receiving system logs.

To configure this feature, follow the steps below:

1. Check the corresponding box to enable one or more ways of receiving system logs, and configure the related parameters. Two ways are available: **Auto Mail** and **Server**.

Log Settings

Enable Auto Mail:

☒ Enable

From:

To:

SMTP Server:

Enable SSL:

☐ Enable

SMTP Port:

25

(1-65535)

Enable Authentication:

☐ Enable

Time:

☒ Fixed Time ☐ Period

Fixed Time:

00

:

00

(HH:MM)

Enable Server:

☒ Enable

System Log Server IP:

0.0.0.0

System Log Server Port:

514

(514, 1025-65535)

More Client Detail Log:

☐ Enable

Save

■ Auto Mail

If Auto Mail is configured, system logs will be sent to a specified mailbox. Check the box to enable the feature and configure the related parameters.

The following table introduces how to configure these parameters:

From	Enter the sender's E-mail address.
To	Enter the receiver's E-mail address.
SMTP Server	Enter the IP address of the sender's SMTP server. Note: At present, the domain name of SMTP server is not supported in this field.
Enable Authentication	If the sender's mailbox is configured with You can check the box to enable mail server authentication. Enter the sender's username and password.
Time Mode	Select Time Mode: Fixed Time or Period Time . Fixed Time means that the system logs will be sent at the specific time every day. Period Time means that the system logs will be sent at the specific time interval.
Fixed Time	If you select Fixed Time , specify a fixed time to send the system log mails. For example, 08:30 indicates that the mail will be sent at 8:30 am everyday.

Period Time	If you select Period Time , specify a period time to regularly send the system log mail. For example, 6 indicates that the mail will be sent every six hours.
--------------------	--

■ Server

If Server is configured, system logs will be sent to the specified system log server, and you can use the syslog software to view the logs on the server.

Enable this feature and enter the IP address and port of the system log server.

System Log Server IP	Enter the IP address of the server.
System Log Server Port	Enter the port of the server.
More Client Detail Log	With the option enabled, the logs of clients will be sent to the server.

2. Click **Save**.

7.4 Configure Web Server

With the web server, you can log in to the management web page of the Bridge AP. You can configure the web server parameters of the Bridge AP according to your needs.

To configure the web server, go to **Management > Web Server**, configure the parameters, and save the settings.

Web Server

Secure Server Port:	443	
Server Port:	80	
Session Timeout:	15	minutes
Layer-3 Accessibility:	☐ Enable	
TLS Version 1.0/1.1:	☐ Enable ⓘ	
Older Security Kits:	☐ Enable ⓘ	
HTTP Server:	☐ Enable	

Note:
Please enter the EAP's IP address to access the web-based configuration utility via an HTTPS connection.

Save

Secure Server Port	Designate a secure server port for web server in HTTPS mode. By default the port is 443.
Server Port	Designate a server port for web server in HTTP mode. By default the port is 80.

Session Timeout	Set the session timeout. If you do nothing with the web page within the timeout, the system will log out automatically. You can log in again if you want to go back to web page.
Layer-3 Accessibility	With this feature enabled, devices from a different subnet can access Omada managed devices via the management web page. With this feature disabled, only the devices in the same subnet can access Omada managed devices via the management web page.
TLS Version 1.0/1.1	The Bridge AP management page uses TLS v1.2 by default. You can enable the feature if you prefer TLS v1.0/1.1. This feature is only available on certain devices. To check whether your device supports this feature, refer to the actual web interface.

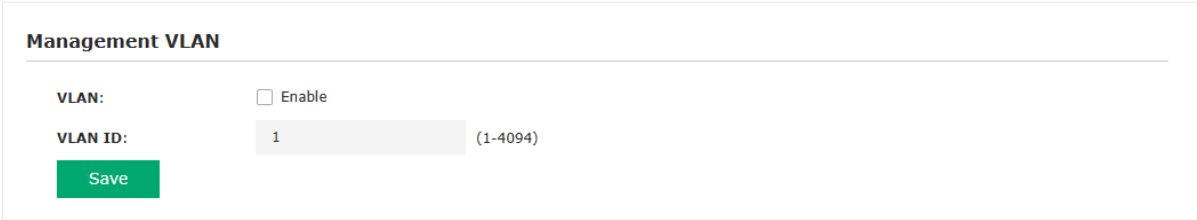
7.5 Configure Management Access

By default, all hosts in the LAN can log in to the management web page of the Bridge AP with the correct username and password. To control the hosts' access to the web page of the Bridge AP, you can specify the management VLAN of the hosts that are allowed to access the web page.

Management VLAN provides a safer method to manage the Bridge AP. With Management VLAN enabled, only the hosts in the Management VLAN can access the web page of the Bridge AP. Since most hosts cannot process VLAN TAGs, you can connect the management host to the network via a switch, and set up correct VLAN settings for the switches on the network to ensure the communication between the host and the Bridge AP in the Management VLAN.

To configure the Management VLAN, follow the steps below:

1. Go to **Management > Management Access**.



Management VLAN

VLAN: ☐ Enable

VLAN ID: (1-4094)

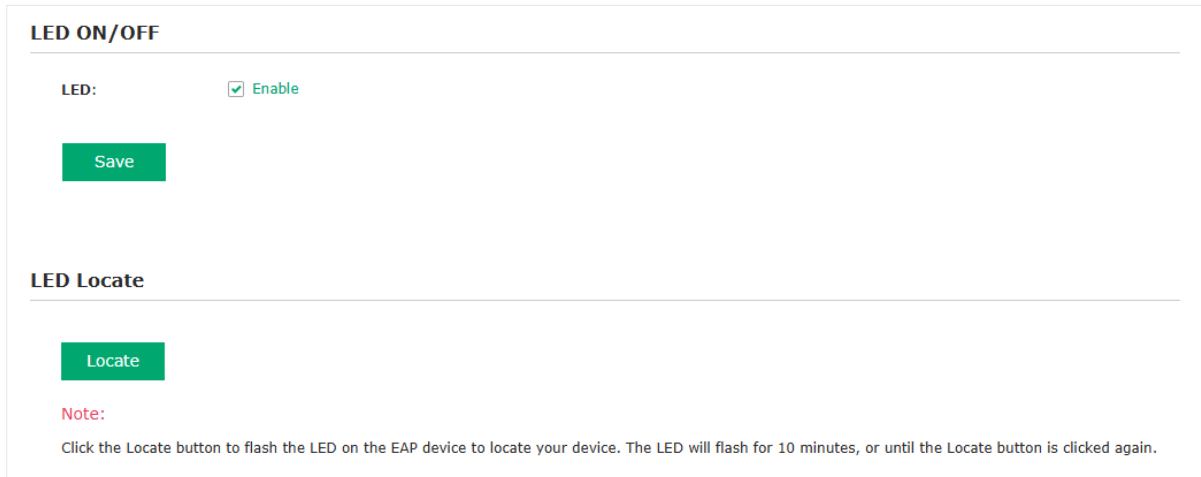
Save

2. Check the box to enable **VLAN**.
3. Specify the VLAN ID of the management VLAN. Only the hosts in the Management VLAN can log in to the Bridge AP via the Ethernet port.
4. Click **Save**.

7.6 Configure LED Control

You can turn on or off the LED light of the Bridge AP and flash the LED to locate your device.

To configure LED control, go to **Management > LED Control**.



LED ON/OFF

LED: ☒ Enable

Save

LED Locate

Locate

Note:

Click the Locate button to flash the LED on the EAP device to locate your device. The LED will flash for 10 minutes, or until the Locate button is clicked again.

Check the **LED** box to turn on or turn off the LED light of the Bridge AP, and click **Save**.

To flash the LED, click **Locate**. Then the LED will flash for 10 minutes or until the locate button is clicked again.

7.7 Configure LAN Port

Note:

Currently only Flex Bridge 5 supports this features.

If you want the Bridge AP's LAN port to forward data with VLAN tags, you can configure the port VLAN for it.

Port VLAN is used to set VLANs for the LAN ports. With this feature, the Bridge AP can work together with the switches supporting 802.1Q VLAN. Traffic from the clients connected to different LAN ports will be added with different VLAN tags according to the VLAN settings of the ports. The wired clients in different VLANs cannot directly communicate with each other.

To configure the port VLAN, follow the steps below:

1. Go to **Management > LAN Port Config**.

VLAN Config

ETH Port	VLAN	VLAN ID
LAN2	Enable ▼	1
LAN3	Disable ▼	0

Save

2. Select your desired port, select **Enable** in the **VLAN** column.
3. Set the VLAN ID for the port. Every VLAN ID represents a different VLAN.
4. Click **Save**.

7.8 Configure SSH

If you want to remotely log in to the Bridge AP via SSH, you can deploy an SSH server on your network and configure the SSH feature on the Bridge AP.

To configure SSH, go to **Management > SSH**, configure the parameters, and save the settings.

SSH Server

Server Port:

22

(22,1025-65535)

Layer-3 Accessibility:

☐ Enable

SSH Login:

☐ Enable

Save

Server Port Designate a server port for SSH. By default the port is 22.

Layer-3 Accessibility With this feature enabled, devices from a different subnet can access Omada managed devices via SSH. With this feature disabled, only the devices in the same subnet can access Omada managed devices via SSH.

SSH Login Enable or disable SSH Login globally.

7.9 Configure SNMP

The Bridge AP can be configured as an SNMP agent and work together with the SNMP manager. Once the Bridge AP has become an SNMP agent, it is able to receive and process request messages from the SNMP manager. At present, the Bridge AP supports

SNMP v1 and v2c.

To configure the Bridge AP as an SNMP agent, follow the steps below:

1. Go to **Management > SNMP**.

SNMP Agent

SNMP Agent:

☐ Enable

SysContact:

SysName:

SysLocation:

Get Community:

public

Get Source:

0.0.0.0

Set Community:

private

Set Source:

0.0.0.0

Save

2. Check the box to enable **SNMP Agent**.

3. Refer to the following table to configure the required parameters:

SysContact	Enter the textual identification of the contact person for this managed node.
SysName	Enter an administratively-assigned name for this managed node.
SysLocation	Enter the physical location of this managed node.
Get Community	Community refers to a host group aiming at network management. Get Community only has the read-only right of the device's SNMP information. The community name can be considered a group password. The default setting is public.
Get Source	Defines the IP address (for example, 10.10.10.1) for management systems that can serve as Get Community to read the SNMP information of this device. The default is 0.0.0.0, which means all hosts can read the SNMP information of this device.
Set Community	Set Community has the read and write right of the device's SNMP information. Enter the community name that allows read/write access to the device's SNMP information. The community name can be considered a group password. The default setting is private.
Set Source	Defines the IP address (for example, 10.10.10.1) for management systems that can serve as Set Community to read and write the SNMP information of this device. The default is 0.0.0.0, which means all hosts can read and write the SNMP information of this device.

4. Click **Save**.

Note:

Defining community can allow management systems in the same community to communicate with the SNMP Agent. The community name can be seen as the shared password of the network hosts group. Thus, for the security, we recommend that modify the default community name before enabling the SNMP Agent service. If the field of community is blank, the SNMP Agent will not respond to any community name.

8

Manage the System

This chapter introduces how to configure the system of the Bridge AP, including:

- *8.1 Configure the User Account*
- *8.2 Configure Controller Settings*
- *8.3 Configure the System Time*
- *8.4 Run a Network Diagnostic*
- *8.5 Reboot and Reset the Bridge AP*
- *8.6 Backup and Restore the Configuration*
- *8.7 Update the Firmware*

8.1 Configure the User Account

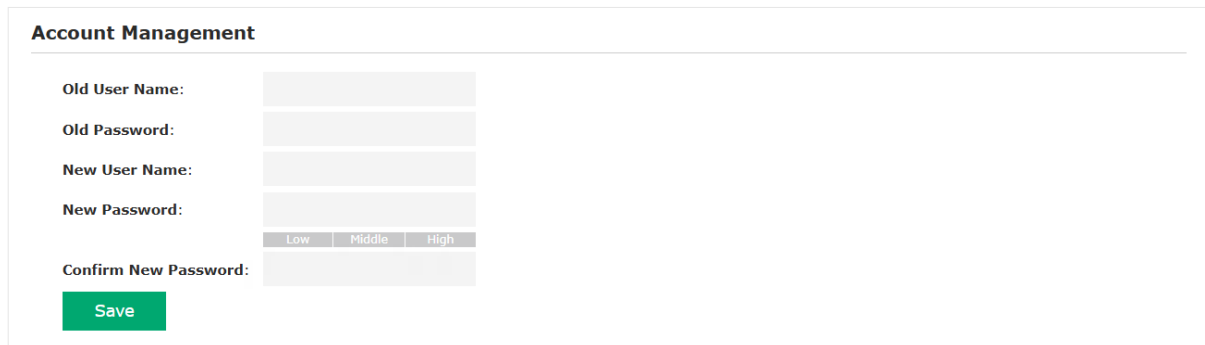
Every Bridge AP has a user account, which is used to log in to the management page of the Bridge AP. When you start the Bridge AP at the first time, the username and password of the user account are both admin. After the first login, the system will require you to set a new username and a new password for the user account. And then you can use the new user account to log in to the Bridge AP. Also, you can change your user account as needed.

Tip:

Please remember your user account well. If you forget it, reset the Bridge AP to the factory defaults and log in with the default user account (username and password are both admin).

To configure the user account, follow the steps below:

1. Go to **System > User Account** page.



The screenshot shows the 'Account Management' page. It contains the following fields and controls:

- Old User Name:** A text input field.
- Old Password:** A text input field.
- New User Name:** A text input field.
- New Password:** A text input field with a strength indicator below it showing 'Low', 'Middle', and 'High' levels.
- Confirm New Password:** A text input field.
- Save:** A green button at the bottom left.

2. Enter the old username and old password of your user account.
3. Specify a new username and a new password for your user account. The system will automatically detect the strength of your entered password. For security, we recommend that you set a password with high strength.
4. Retype the new password.
5. Click **Save**.

8.2 Configure Controller Settings

To make your controller adopt your Bridge AP, make sure the Bridge AP can be discovered by the controller. Controller Settings enable your Bridge AP to be discovered in either of

the following scenarios.

Cloud-Based Controller Management

Connection Status: Disabled

Cloud-Based Controller Management: ☐ Enable

Note:

To enjoy centralized management on Omada Cloud-Based Controller, enable Cloud-Based Controller Management and add the device to the controller via its serial number.
You can disable this feature if you do not need to manage the device with the Omada Cloud-Based Controller.

Controller Inform URL

Inform URL/IP Address: 0.0.0.0?dPort=29810&mPort=29814&omadacId=c21f969b5f03d3

Note:

Enter the inform URL or IP address of your controller to tell the device where to discover the controller.
This feature is commonly used for the device to be managed by the controller in Layer 3 deployments.

Save

- If you are using Omada Cloud-Based Controller, refer to [Enable Cloud-Based Controller Management](#).
- If your Bridge AP and controller are located in the same network, LAN and VLAN, the controller can discover and adopt the Bridge AP without any controller settings. Otherwise, you need to inform the Bridge AP of the controller's URL/IP address. Refer to [Configure Controller Inform URL](#).

To adopt and manage Bridge APs with a controller, refer to the Omada SDN Controller User Guide on our Documents page: <https://support.omadanetworks.com/document>

- **Enable Cloud-Based Controller Management**

Go to **System > Controller Settings**. In the Cloud- Based Controller Management section, enable **Cloud-Based Controller Management** and click **Save**. After you add the Bridge AP to your Omada Cloud-Based Controller, you can check the connection status on this page.

- **Configure Controller Inform URL**

Go to **System > Controller Settings**. In the Controller Inform URL section, inform the Bridge AP of the controller's URL/IP address, and click **Save**. Then the Bridge AP make contact with the controller so that the controller can discover the Bridge AP.

8.3 Configure the System Time

System time is the standard time for Scheduler and other time-based functions. The Bridge AP supports the basic system time settings and the Daylight Saving Time (DST) feature.

To configure the system time, go to **System > Time Settings**.

Time Settings

Time zone:

(GMT-08:00) Pacific Time

Date:

01/01/2025

MM/DD/YYYY

Time:

08

:

02

:

26

(HH/MM/SS)

Primary NTP Server:

(Optional)

Secondary NTP Server:

(Optional)

Get GMT

Synchronize with PC

Save

Daylight Saving

Daylight Saving:

☐ Enable

Mode:

☒ Predefined Mode

☐ Recurring Mode

Predefine Country:

USA

Save

The following two sections introduce how to configure the basic system time settings and the Daylight Saving Time feature.

8.3.1 Configure the System Time

In the **Time Settings** section, you can configure the system time. There are three methods to set the system time: *Set the System Time Manually*, *Acquire the System Time From an NTP Server*, and *Synchronize the System Time with PC's Clock*.

Determine the way of setting the system time and follow the steps below to complete the configurations:

- **Set the System Time Manually**

To set the system time manually, follow the steps below:

1. Configure the following three options on the page: **Time Zone**, **Date** and **Time**.

Time Zone	Select your time zone from the drop-down list. Here GMT means Greenwich Mean Time.
-----------	--

Date	Specify the current date in the format MM/DD/YYYY. MM means month, DD means day and YYYY means year. For example: 06/01/2026.
Time	Specify the current time in the format HH/MM/SS. HH means hour, MM means minute and SS means second. It uses 24-hour system time. For example: 14:36:21.

2. Click **Save**.

Note:

The system time set manually will be lost after the Bridge AP is rebooted.

- **Acquire the System Time From an NTP Server**

To get the system time from an NTP server, follow the steps below:

1. Build an NTP server on your network and make sure that it is reachable by the Bridge AP. Or you can simply find an NTP server on the internet and get its IP address.
2. Specify the NTP server for the Bridge AP. If you have two NTP servers, you can set one of them as the primary NTP server, and the other as the secondary NTP server. Once the primary NTP server is down, the Bridge AP can get the system time from the secondary NTP server.

Primary NTP Server	Enter the IP address of the primary NTP server. Note: If you have only one NTP server on your network, enter the IP address of the NTP server in this field.
Secondary NTP Server	Enter the IP address of the secondary NTP server.

3. Click the button **Get GMT** and the acquired system time will be displayed in the **Date** and **Time** fields.
4. Click **Save**.

- **Synchronize the System Time with PC's Clock**

To synchronize the system time with the clock of your currently logged-in host, follow the steps below:

1. Click the button **Synchronize with PC** and the synchronized system time will be displayed in the **Date** and **Time** fields.
2. Click **Save**.

Note:

The system time synchronized with PC's clock will be lost after the Bridge AP is rebooted.

8.3.2 Configure Daylight Saving Time

Daylight saving time is the practice of advancing clocks during summer months so that evening daylight lasts longer, while sacrificing normal sunrise times. The Bridge AP provides daylight saving time configuration.

Follow the steps below to configure daylight saving time:

1. Check the box to enable **Daylight Saving**.
2. Select the mode of daylight saving time. Three modes are available: **Predefined Mode**, **Recurring Mode** and **Date Mode**.
3. Configure the related parameters of the selected mode.

■ Predefined Mode

If you select Predefined Mode, choose your region from the drop-down list and the Bridge AP will use the predefined daylight saving time of the selected region.

There are four regions provided: **USA**, **European**, **Australia** and **New Zealand**. The following table introduces the predefined daylight saving time of each region.

USA	From 2: 00 a.m. on the Second Sunday in March to 2:00 a.m. on the First Sunday in November.
European	From 1: 00 a.m. on the Last Sunday in March to 1:00 a.m. on the Last Sunday in October.
Australia	From 2:00 a.m. on the First Sunday in October to 3:00 a.m. on the First Sunday in April.
New Zealand	From 2: 00 a.m. on the Last Sunday in September to 3:00 a.m. on the First Sunday in April.

■ Recurring Mode

If you select Recurring Mode, manually specify a cycle time range for the daylight saving time of the Bridge AP. This configuration will be used every year.

The following table introduces how to configure the cycle time range.

Time Offset	Specify the time to set the clock forward by.
-------------	---

Start	Specify the start time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).
End	Specify the end time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).

■ Date Mode (Only for certain models)

If you select Date Mode, manually specify an absolute time range for the daylight saving time of the Bridge AP. This configuration will be used only once.

The following table introduces how to configure the absolute time range.

Time Offset	Specify the time to set the clock forward by.
Start	Specify the start time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).
End	Specify the end time of daylight saving time. The interval between the start time and end time should be more than 1 day and less than 1 year (365 days).

4. Click **Save**.

8.4 Run a Network Diagnostic

The Bridge AP provides many diagnostic tools for you to analyze your network.

Note:

Firmware update may be required for earlier devices to support this feature.

To diagnose network problems, follow the steps below:

1. Go to **System > Diagnostic**.
2. Select a diagnostic tool, configure the test parameters.

• Ping

Tests the connectivity between the Bridge AP and specified destination, and measures the round-trip time.

Diagnostic

Diagnostic Tool:

Ping

Destination IP/Domain:

0.0.0.0

Packet Count:

4

(1-100)

Packet Size:

32

bytes (10-2000)

Output:

Run

Destination IP/
Domain

Select the destination IP address or domain to test.

Packet Count

Specify the number of ping packets.

Packet Size

Specify the size of ping packets.

• Traceroute

Tests the route (path) the Bridge AP passes to reach the specified destination, and measures transit delays of packets across an Internet Protocol network.

Diagnostic

Diagnostic Tool:

Traceroute

Destination IP/Domain:

0.0.0.0

Output:

Run

Destination IP/
Domain

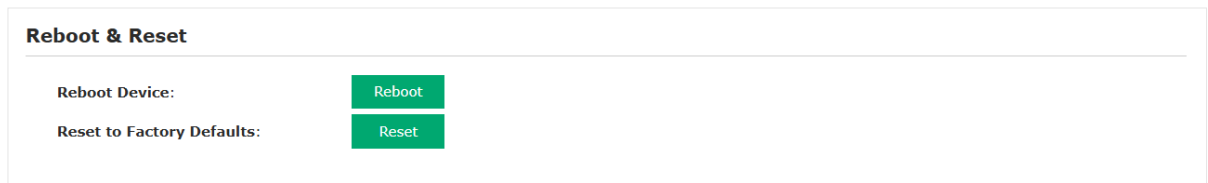
Select the destination IP address or domain to test.

- Click **Run** to start the diagnostic. The result will be displayed in the **Output** field.

8.5 Reboot and Reset the Bridge AP

You can reboot and reset the Bridge AP according to your need.

To reboot and reset the Bridge AP, go to **System > Reboot/Reset**.



Reboot & Reset

Reboot Device:

Reset to Factory Defaults:

- To reboot the Bridge AP, click the **Reboot** button, and the Bridge AP will be rebooted automatically. Please wait without any operation.
- To reset the Bridge AP, click the **Reset** button, and the Bridge AP will be reset to the factory defaults automatically. Please wait without any operation.

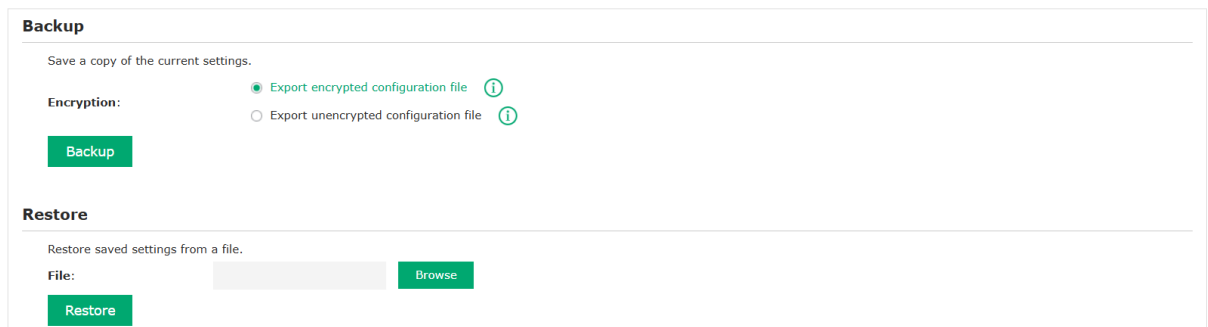
Note:

After reset, all the current configuration of the Bridge AP will be lost. We recommend that you check whether you have any configuration that needs to be backed up before resetting the Bridge AP.

8.6 Backup and Restore the Configuration

You can save the current configuration of the Bridge AP as a backup file and save the file to your host. And if needed, you can use the backup file to restore the configuration. We recommend that you backup the configuration before resetting or upgrading the Bridge AP.

To backup and restore the configuration, go to **System > Backup & Restore**.



Backup

Save a copy of the current settings.

Encryption: ☒ Export encrypted configuration file ⓘ ☐ Export unencrypted configuration file ⓘ

Restore

Restore saved settings from a file.

File:

- To backup the configuration, specify whether to export an encrypted or unencrypted configuration file, then click the **Backup** button. The backup file will be saved to the host automatically.
- To restore the configuration, click the **Browse** button, choose the backup file from the host, then click the **Restore** button. The configuration will be restored.

8.7 Update the Firmware

We occasionally provide the firmware update files for the Bridge AP products on our

official website. To get new functions of the Bridge AP, you can check our official website and download the update files to update the firmware of your Bridge AP.

To update the firmware, go to **System > Firmware Update**.

Firmware Update

New Firmware File:

Browse

Warning:

The firmware update process takes a couple of minutes. Please do not power off the device until the process finishes.

Update

Follow the steps below to update the firmware of your Bridge AP:

1. Go to our website <https://www.omadanetworks.com> and search for your Bridge AP model. Download the proper firmware file on the support page of the Bridge AP.
2. Click the **Browse** button, locate and choose the correct firmware file from your host.
3. Click the **Update** button to update the firmware of the Bridge AP. After updated, the Bridge AP will be rebooted automatically.

Note:

The update process takes several minutes. To avoid damage to the Bridge AP, please wait without any operation until the update is finished.