Quick Start Guide

O-105 Access Point

Arista Networks

DOC-03489-01

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA		
+1 408 547-5500	+1 408 547-5502+ 1 866 476-0000	+1 408 547-5501 +1 866 497-0000
www.arista.com	support-wifi@arista.com	sales@arista.com

Contents

Chapter 1. About This Guide

This installation guide explains how to deploy the O-105 access point (AP).

Important: Please read the EULA before installing O-105. You can download and read the EULA from https://www.arista.com/en/support/product-documentation.

Installation constitutes your acceptance of the terms and conditions of the EULA.

Intended Audience

This guide can be referred to by anyone who wants to install and configure the O-105 outdoor access point.

Document Overview

This guide contains the following chapters:

- Package Content
- O-105 Overview
- Installing O-105
- O-105 Troubleshooting

Note: All instances of the term 'server' in this document refer to the Wireless Manager, unless the server name or type is explicitly stated.

Product and Documentation Updates

To receive important news on product updates, please visit our website at . We continuously enhance our product documentation based on customer feedback.

Contact Information

Arista Networks, Inc.

339 N, Bernardo Avenue, Suite #200, Mountain View, CA 94043

Tel: +1 650-961-1111 Fax: +1 650-963-3388

For technical support, send an email to support-wifi@arista.com .

Chapter 2. Package Content

Please ensure that the items shown in Figure 1-1 are included in the O-105 device package:

Figure 1: O-105 Mounting Accessories

Important: The MAC address of the device is printed on a label at the bottom of the product and the packaging box. Note down the MAC address, before mounting the device.

If the package is not complete, please contact Arista Networks Technical Support Team on www.support-wifi@arista.com or return the package to the vendor or dealer where you purchased the product.

Chapter 3. O-105 Overview

The O-105/WP9331-MJ is two radios, dual band, 802.11ac wave 2 access point. It provides powerful WLAN supporting wireless speed up to 400Mbps on 2.4GHz and 867Mbps on 5GHz, one Ethernet port to connect to the backbone network, one Ethernet port can be aggregated to connect to one computer through the network cables. It also supports fiber as one of uplink options. Besides, the O-105/WP9331-MJ supports 802.3at/af PoE PD to allow the device powered by PoE switch remotely.

To protect data during wireless transmission, the device supports WEP data encryption and WPA/WPA2 wireless security to ensure network safely.

The O-105/WP9331-MJ is ideal for a variety of medium density enterprise and hotspot environments.

Note: Optional features are not included in default SKU and to be quoted separately if required afterwards.

This chapter provides an overview of the O-105 and describes:

- The Side Panel of O-105 *(page 6)*
- The Bottom Panel of O-105 *(page 5)*

Bottom Panel of O-105

The bottom panel of the O-105 has LAN/PoE connectors that enable you to connect the device to a wired LAN through a switch or a hub. The ports provide power for the device by using the 802.3at standard.

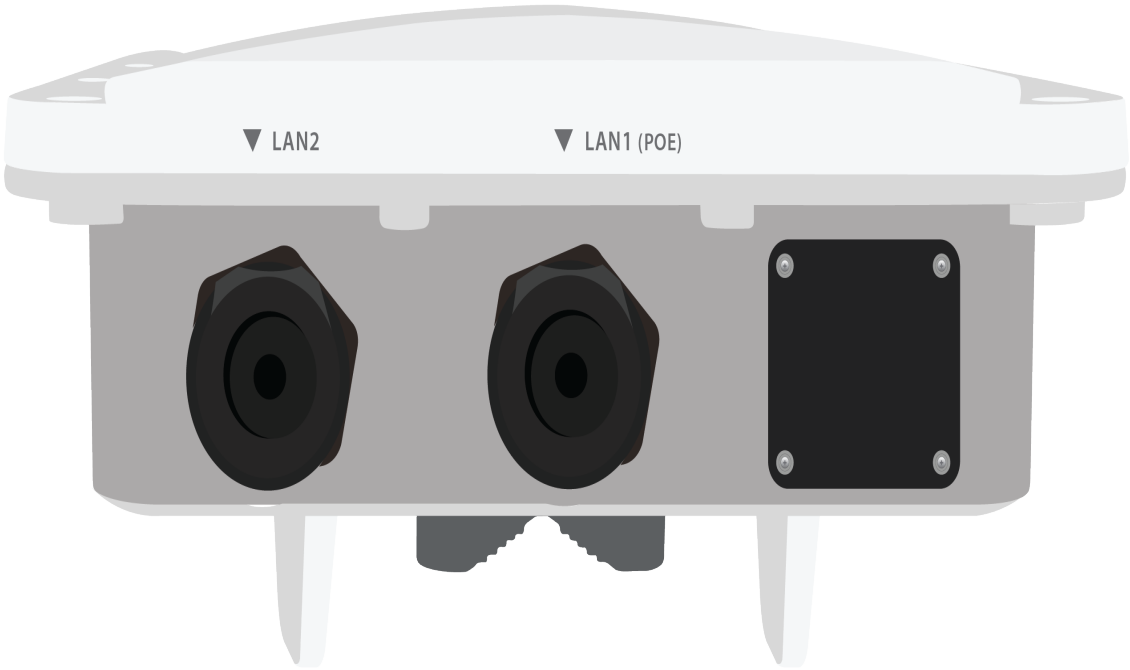


Figure 2: O-105 Bottom Panel

Port/Button	Description	Connector Type	Speed/Protocol
Ethernet (LAN2)	Enables you to connect the device to a wired LAN through a switch or a hub. The device can then communicate with the server. This port also provides the power for the device using the 802.3at standard	RJ-45	10/100/1000 Mbps Ethernet Power over Ethernet

LAN1 (PoE)	Enables you to connect the device to a wired LAN through a switch or a hub. The device can then communicate with the server. This port also provides the power for the device using the 802.3at standard	RJ-45	10/100/1000 Mbps Ethernet Power over Ethernet
Reset	Enables you to reset the O-105	--	--

Side Panel of O-105

The side panel of the O-105 has LEDs that indicate the working of the device.

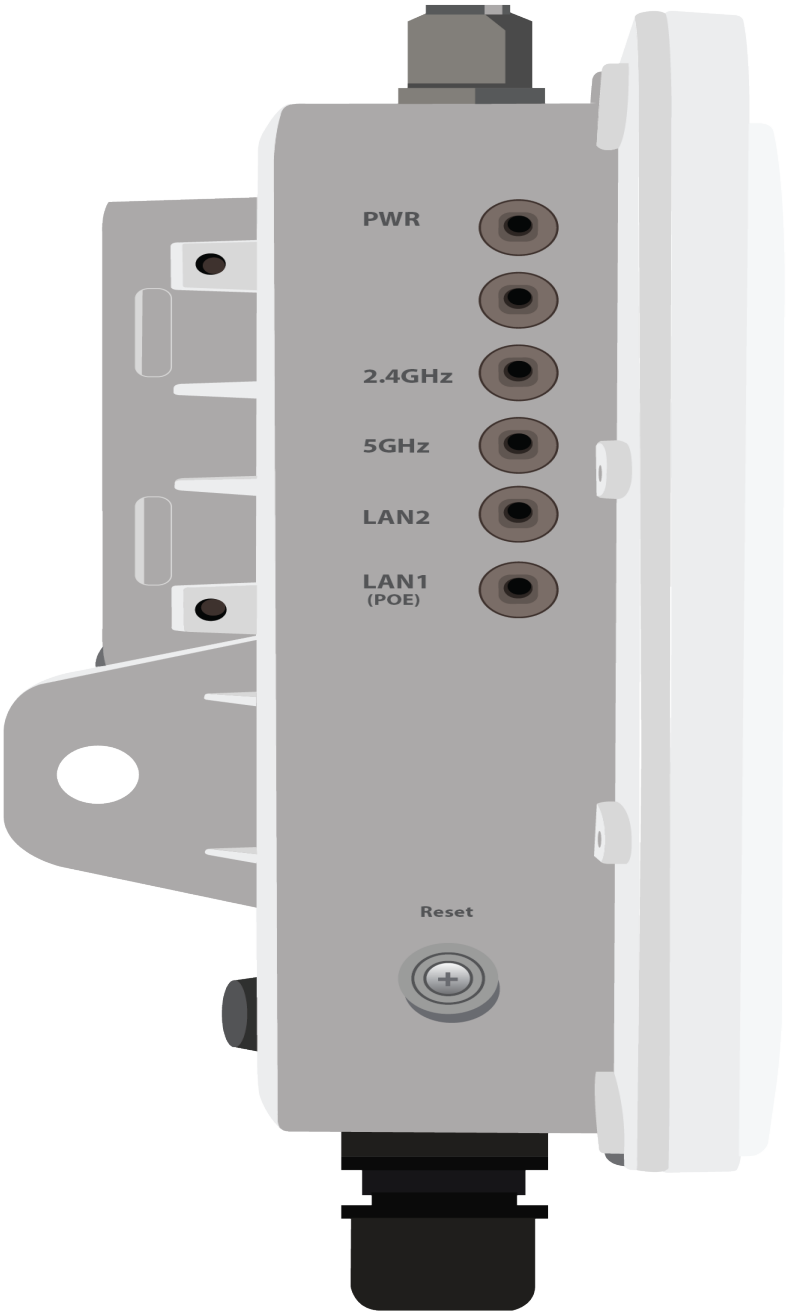


Figure 3: O-105 Side Panel

The following table indicates the device states based on the LEDs

Table 1: O-105 LED Status Description

LED	Status	Description
Power(PWR)	Solid Green	Power ON
	OFF	Power OFF
5 GHz	Solid Green	No clients connected
	Blinking Green	Wireless activity on 5 GHz radio
2.4 GHz	Solid Green	No activity on 2.4 GHz
	Blinking Green	Wireless activity on 2.4 GHz
LAN1/2	Solid Green	Wired Extension/VLAN Extension enabled
	Blinking Green	Connectivity Issues

Note : LAN2 is On when the link is up and it is Off when the link is down. WLAN1 and WLAN2 LEDs blink when there is activity on the respective radios.

[1] *(page)* If the Ethernet connection for the AP switches to 10/100 Mbps mode while in operation, the Orange LED for LAN1 starts blinking, while the state of the Green LED for LAN1 is retained. The Orange LED for LAN1 might continue to blink even if the Ethernet switches back to 10/1000 Mbps mode and would stop only on rebooting the device.

[1] *(page)* If the Ethernet connection for the AP switches to 10/100 Mbps mode while in operation, the Orange LED for LAN1 starts blinking, while the state of the Green LED for LAN1 is retained. The Orange LED for LAN1 might continue to blink even if the Ethernet switches back to 10/1000 Mbps mode and would stop only on rebooting the device.

Chapter 4. Install the O-105

When the O-105 functions as a WIPS sensor, it monitors your network and communicates with the server to guard your corporate network against over-the-air attacks. When the O-105 functions as an access point (AP), clients can connect to your corporate network in wireless mode through the AP(s). The O-105 must be plugged into your corporate network to perform the above-mentioned operations.

Zero-Configuration of O-105 as Access Point

Zero-configuration is supported under the following conditions:

- The device is in sensor mode.
- A DNS entry **wifi-security-server** is set up on all the DNS servers. This entry should point to the IP address of the server. By default, the device looks for the DNS entry **wifi-security-server**.
- The sensor is placed on a subnet that is DHCP enabled.

Important: If the device is placed on a network segment that is separated from the server by a firewall, you must first open port 3851 for User Datagram Protocol (UDP) and Transport Control Protocol (TCP) bidirectional traffic on that firewall. This port number is assigned to Arista Networks. If multiple devices are set up to connect to multiple servers, zero-configuration is not possible. In this case, you must manually configure the APs. See the Access Point Configuration Guide on our website.

Take a configured O-105, that is, ensure that a static IP is assigned to the device or the settings have been changed for DHCP. Note the MAC address and the IP address of the device is in a safe place before it is installed in a hard-to-reach location. The MAC address of the device is printed on a label at the bottom of the product. With two extra mounting brackets and the screws, O-105/WP9331-MJ can be mounted on pole with the ability of being 90D to the ground. **Recommended-** *You should label the devices using MAC addresses or at least your own convention. For example, use serial numbers, so that you can easily identify the devices.*

The steps to install the device with no configuration (zero-configuration) are as follows:

1. Mount the device. *(page 8)*
2. Power on the O-105 *(page 11)*
3. Connect the O-105 to the network *(page 11)*

Mount the O-105

Take a configured O-105, that is, ensure that a static IP is assigned to the device or the settings have been changed for DHCP. Note the MAC address and the IP address of the device in a safe place before it is installed in a hard-to-reach location. The MAC address of the device is printed on a label at the bottom of the product.

Recommended : You should label the devices using MAC addresses or at least your own convention. For example, use serial numbers, so that you can easily identify the devices.

There are 2 ways to mount the device:

1. Wall Mounting *(page 9)*
2. Pole Mounting *(page 8)*

Pole Mount the O-105

Use the pole-mount bracket and pole strap to install the O-105 device on a pole. The proposal only supports pole mounting. Standard accessories include two metal clamps.:

Use the mounting base to install the O-105 device on the wall. To mount the device:

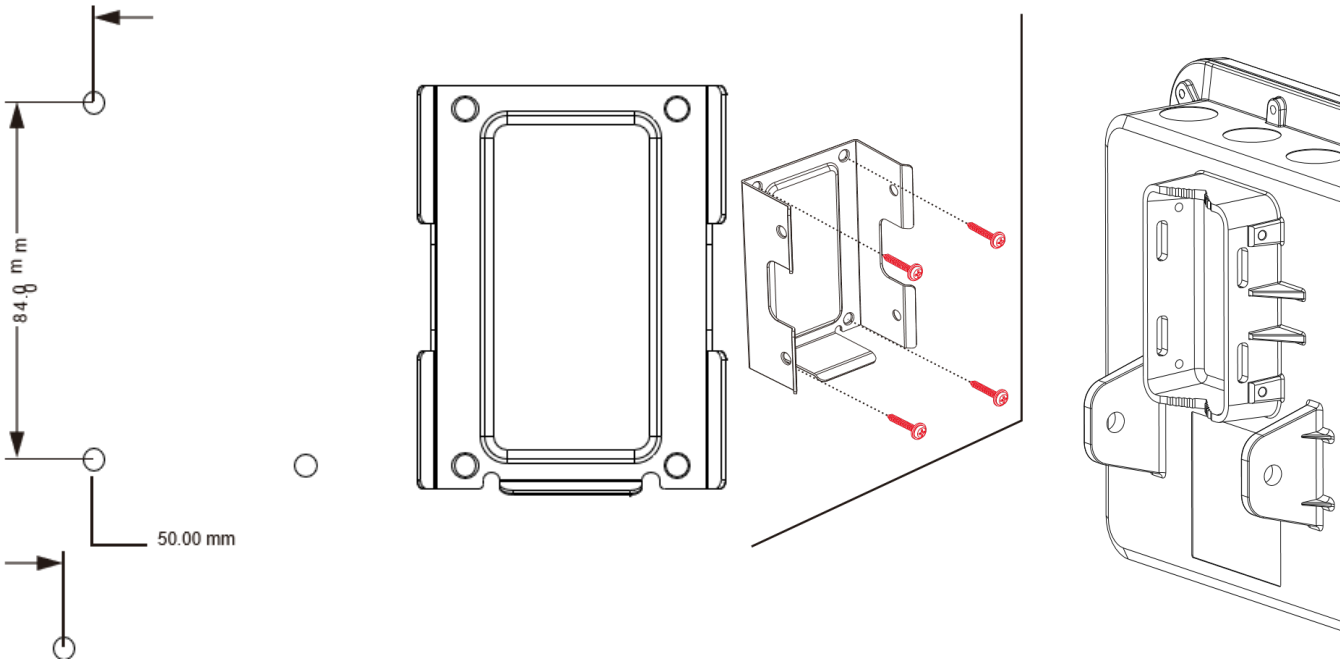
1. Attach the device to the mounting base.

2. Attach the pole-mount bracket to the mounting base. You can position the pole-mount bracket for use on a vertical or horizontal pole. Insert the pole strap in to the pole-mount bracket.
3. Mount the device securely to the pole by using the pole strap.

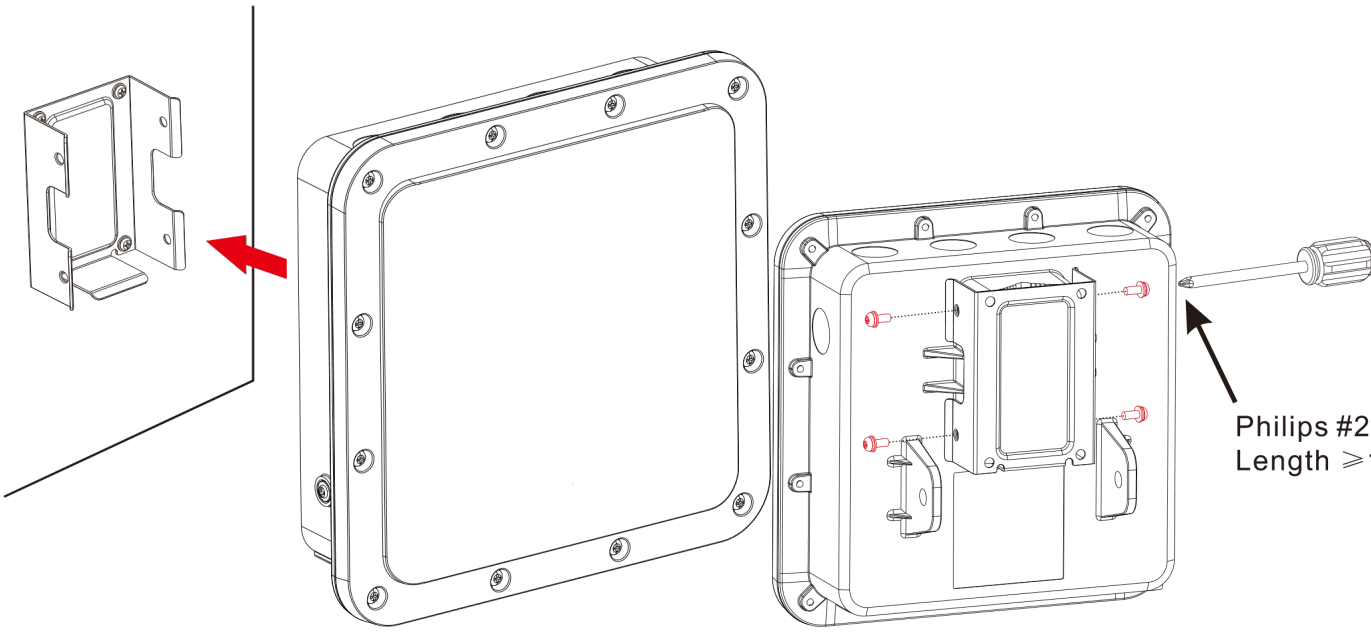
Wall Mount the O-105

Use the pole-mount bracket and pole strap to install the O-105 device on a pole. The proposal only supports pole mounting. Standard accessories include two metal clamps.

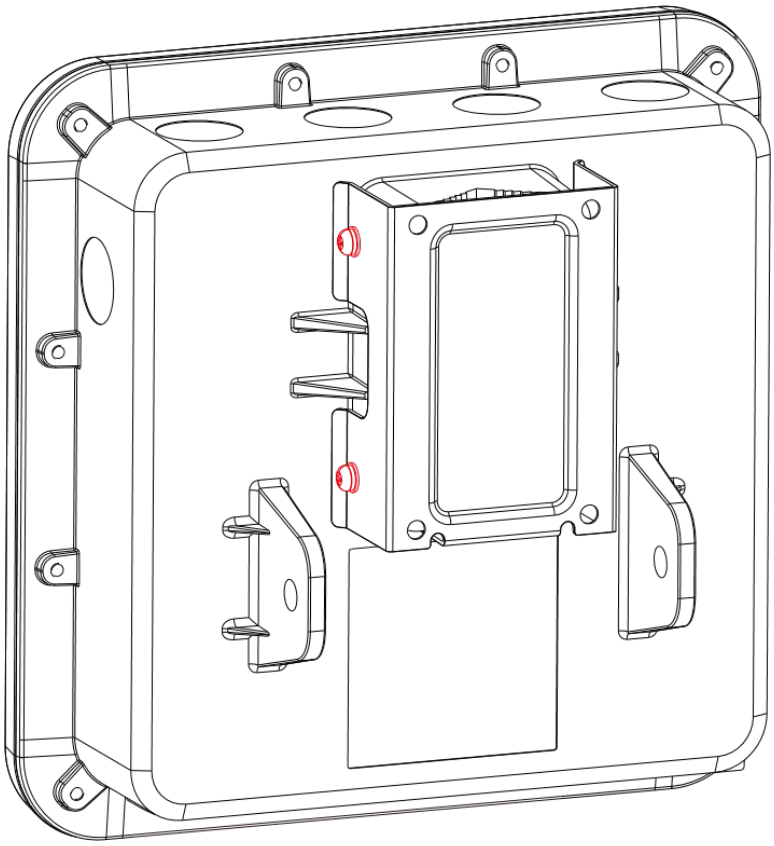
1. Affix the expansion bolts on the wall such that the holes on the mounting base can be perfectly placed over them.



2. Attach the mounting base to the bottom cover of the O-105 device.



3. Mount the device on the expansion bolts.



Power On the O-105

An O-105 device can be powered on by plugging one end of the Ethernet cable into the 802.3af/at Power Over Ethernet+ (PoE +) switch or injector and the other end into the Ethernet/PoE part on O-105 of nominal input voltage 48V DC.

Note: If you are not using PoE, ensure that you use only an AC power adaptor supported by the O-105 access point (AP).

Connect the O-105 to the Network

To connect O-105 to the network, perform the following steps:

1. Ensure that the server is already running on your network.
2. Add the DNS entry **wifi-security-server** on all DNS servers. This entry should point to the IP address of the server.
3. Ensure that DHCP is running on the subnet to which the device will be connected.
4. Ensure that a DHCP server is available on the network to enable network configuration of the O-105
5. Connect one end of the network interface cable to the Ethernet port at the bottom of the O-105.
6. Connect the other end of the network interface cable to an Ethernet jack on the desired subnet.
7. Log on to the server through SSH and run the get sensor list command. You would see a list of all Arista devices that are recognized by the server. You can also check whether the device is recognized by the server from the **Devices** tab in Wireless Manager.

The device is connected and ready to go operational.

Note: If the zero configuration is not successful, the device must be configured manually.

Important: If DHCP is not enabled on a subnet, devices cannot connect to that subnet with zero-configuration. If the DNS entry is not present on the DNS servers or you do not have the DHCP server running on the subnet, you must manually configure the device. See the Access Point Configuration guide on our website.

Connect the O-105 using PoE

If you are using a PoE injector, make sure the data connection is plugged into a suitable switch port with proper network connectivity.

Chapter 5. O-105 Troubleshooting

The table below lists some of the troubleshooting guidelines for O-105.

Diagnosis	Solution
The device did not receive a valid IP address via the DHCP.	Ensure that the DHCP server is On and available on the VLAN/subnet to which the device is connected. If the device still fails to get a valid IP address, you can reboot it to see if the problem is resolved.
The Ethernet cable is loose. The device is probably disconnected from the network.	Ensure that the Ethernet cable is connected.
Unable to connect to the server.	Ensure that the server is running and is reachable from the network to which the device is attached. If there is a firewall or a router with ACLs enabled between the device and the server, ensure that the traffic is allowed on UDP port 3851. Use the server IP-based discovery and ensure that you have correctly entered the DNS name, **wifi-security-server** , on the DNS server. Also, ensure that the DNS server IP addresses are either correctly configured on the, or are provided by the DHCP server. It is also possible that the AP is unable to connect to the server because it has failed to authenticate with the server. In this case, an 'Authentication failed for ' event is raised on the server. Refer to the event for recommended action.
The AP has encountered a problem.	If you are using Arista Cloud Services, then open the TCP port 443 (SSL). If you have an on-premises installation, then open the ports UDP 3851 and port 80. If you are using a Proxy, Web Accelerator or URL Content Filter in between the AP and the Internet, ensure the settings allow communication between the AP and Arista Cloud Services. If your configuration requires you to specify an exact IP address or IP range for Arista Cloud Services, please contact Technical Support at support-wifi@arista.com.

Chapter 6. Appendix A: AP-Server Mutual Authentication

The AP-server communication begins with a mutual authentication step in which the AP and server authenticate each other using a shared secret. The AP-server communication takes place only if this authentication succeeds.

After the authentication succeeds, a session key is generated. All communication between the AP and server from this point on is encrypted using the session key.

The AP and server are shipped with the same default value of the shared secret. The CLI commands are provided on both server and AP for changing the shared secret.

Note: After the shared secret (communication key) is changed on the server, all APs connected to the server will automatically be set up to use the new communication key. APs that are not connected to the server at this time must be manually set up with the same communication key to enable communication with this server.

Note: Although the server is backward compatible, that is, older version APs can connect to a newer version server, this is not recommended.