ARISTA

Quick Start Guide

O-435 Access Point

Arista.com

Arista Networks

DOC-07524-01

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/en/	support@arista.com	sales@arista.com

Contents

Chapter 1

About This Guide

This installation guide explains how to deploy the O-435 access point (AP).

Important: Please read the EULA before installing the access point (AP). You can download and read the EULA from: https://www.arista.com/en/support/product-documentation

Installing the AP constitutes your acceptance of the terms and conditions of the EULA mentioned above.

Intended Audience

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

Document Overview

This guide contains the following chapters:

- Package Content
- Access Point Overview
- Install the Access Point
- Access Point 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 https://www.arista.com/en/support/product-documentation. We continuously enhance our product documentation based on customer feedback

FCC Advisory

O-435 is prohibited for control of or communications with unmanned aircraft systems, including drones.

Chapter 2

Package Content

The access point (AP) package contains the components shown in the following figure:

Figure 2-1: Package Components

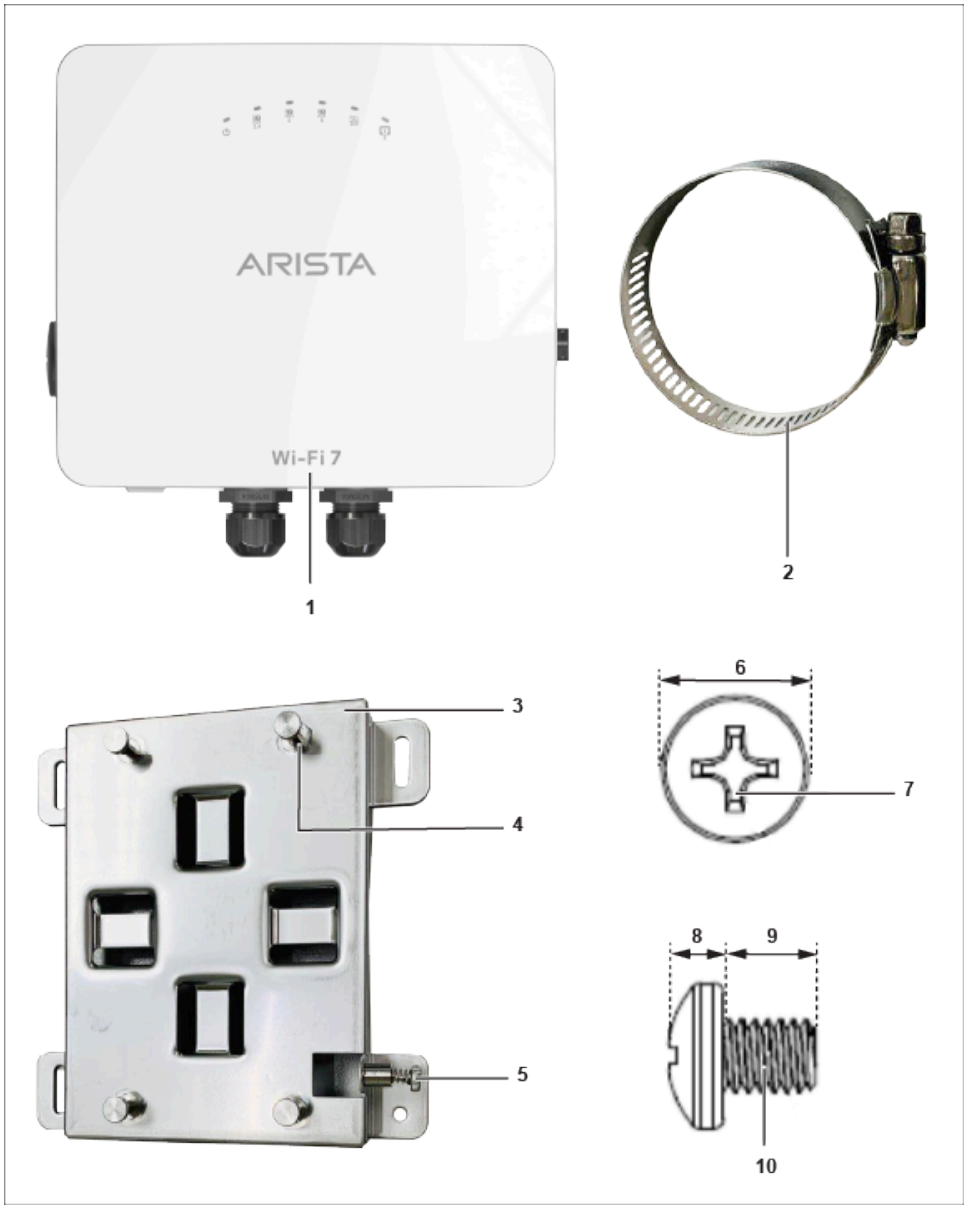


Table 1: Labels: Package Components

Label	Description
1	O-435 Access Point
2	2 metal clamps for fixing the mounting bracket to the pole
3	Mounting bracket
4	4 steel bosses for fixing AP in the bracket
5	Philips screw driver to secure the AP to the bracket
6	Earthing screw fitted at the back of AP with dimension 6.8 ±0.2 mm
7	Use Philips #2 screwdriver to tighten the screw
8	Earthing screw - 2.6 ±0.2 mm
9	Earthing screw - 5.8 ±0.2 mm
10	Earthing screw thread - M4 × 0.5 mm

Important: The MAC address of the AP is printed on a label at the bottom of the product and the packaging box. Note down the MAC address before mounting the AP on the ceiling or at a location that is difficult to access.

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

Chapter 3

Access Point Overview

O-435 is a multi-radio 802.11be (Wi-Fi 7) access point. Refer the datasheet for more information.

Note: This equipment is suitable for use in environment air spaces (plenums).

This chapter provides an overview of the access point (AP) and describes:

- Front Panel
- Side Panel - Left
- Bottom Panel

3.1 Front Panel

The front panel of the AP has 6 LEDs that indicate the status of various AP functions.

Figure 3-1: Front Panel LED

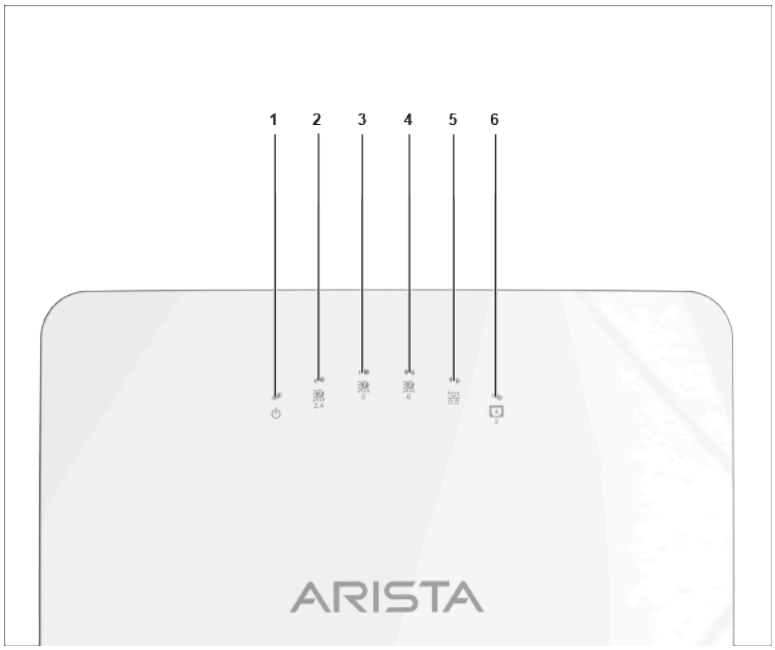


Table 2: Labels: Front Panel LEDs

Label	Description
1	Power
2	2.4 GHz Radio
3	5 GHz Radio
4	6 GHz Radio
5	LAN1 PoE PD
6	LAN2 PoE PSE (802.3af)

Power LED: The following table describes the Power LED states.

Table 3: Power LED States Description

	Green	Red
Solid	Running at full capability	Running at reduced capability
Blinking	Received IP address, but not connected to the server	Did not receive an IP address

Reduced capability indicates that the AP is getting lower than the required maximum power from the PoE++ switch. It means the AP is getting 802.3at instead of 802.3bt.

LAN1 LED: ON when the corresponding interface is up.

LAN2 LED: ON when the corresponding interface is up, and either wired guest or link aggregation is configured.

Radio LEDs: ON when the corresponding radio is operational.

3.2 Side Panel - Left

The side panel of the AP has a reset pinhole, USB port, and console port.

Figure 3-2: Side Panel

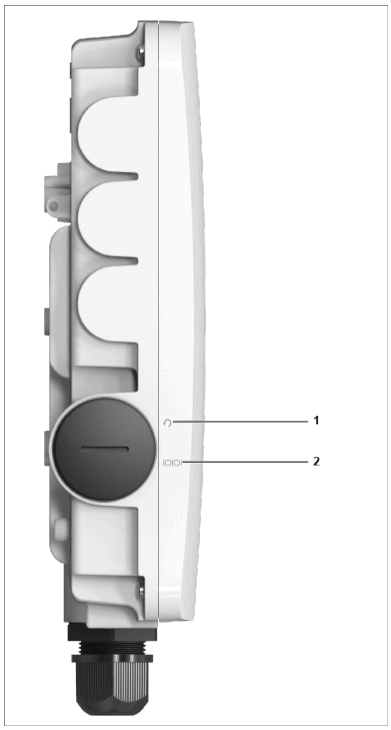


Table 4: Labels: Side Panel

Label	Description
1	Reset
2	Console

Port	Description	Connector Type	Speed/Protocol
Console	Establish ‘config shell’ terminal session via serial connection	RJ-45	• RS 232 Serial (115200 bits per second) • Data bits:8; Stop bits: 1 • Parity: None • Flow Control: None
Reset	Reset to factory default settings port. Hold down and power cycle the device to reset.	Pinhole push button	N/A

When you reset the AP, the following settings are reset:

- Config shell password is reset to **config**.

- Server discovery value is erased and changed to the default, **redirector.online.spectraguard.net** (primary) and **wifi-security-server** (secondary).
- All the VLAN configurations are lost.
- If a static IP is configured on the AP, the IP address is erased and DHCP mode is set. The factory default IP address of the AP is 169.254.11.74.

3.3 Bottom Panel

The left side panel of the AP has two ports LAN1 and LAN2. Conect a wired LAN from a Switch or a hub to the LAN1/PoE++ port of the AP to power-on the AP. The LAN1 port supports the 802.3bt power standard. Use an active wrench to open the LAN cap. Width of the LAN cap is 27 mm. LAN2 acts as a PoE Power Sourcing Equipment (PSE) that provides power to any devices connected thorugh LAN2. Note that LAN2 cannot be used to provide power to the AP.

Figure 3-3: Rear Panel

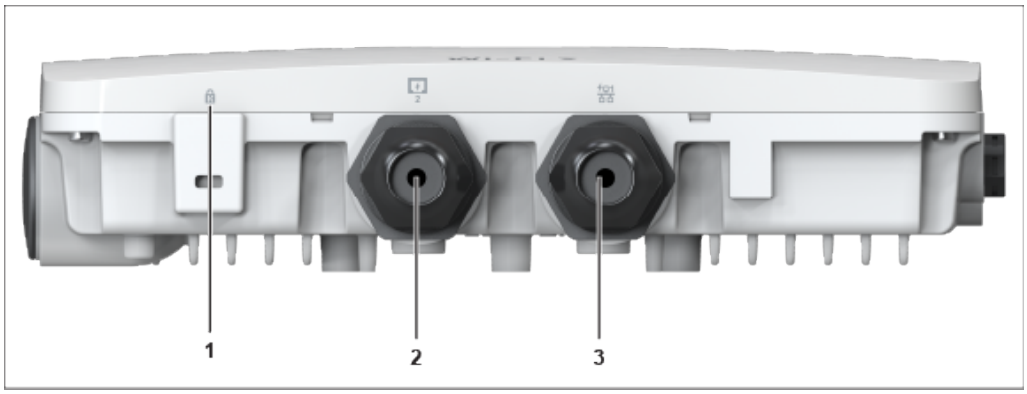


Table 5: Labels: Ports

Label	Description
1	Kensington lock
2	LAN2 (PoE PSE)
3	LAN1 (PoE+ PD)

Table 6: Port Details

Port	Description	Connector Type	Speed/Protocol
LAN 1	5Gbps Ethernet with 802.3bt compliant PoE PD. LAN 1 is used to power the AP.	RJ-45	10M/100M/1000Mbps/2.5G/5Gbps Ethernet
LAN 2	5Gbps Ethernet with 802.3af compliant PoE PSE. LAN 2 is used to power other connected devices. LAN 2 cannot be used to power the AP.	RJ-45	10M/100M/1000Mbps/2.5G/5Gbps Ethernet

Chapter 4

Install the Access Point

This chapter contains the stepwise procedure to install the access point (AP).

Zero-Configuration of the Access Point

Zero-configuration is supported under the following conditions:

- The device is in AP mode with background scanning on and no SSID configured.
- 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 AP looks for the DNS entry **wifi-security-server**.
- The AP is on a subnet that is DHCP enabled.

Refer to these articles to understand how APs communicate with the server, and the ports that you need to open to enable the communication:

- Wi-Fi Access Points-Server Comunication
- TCP Ports and UDP Ports Used by Access Points

Important: If the AP is on a network segment that is separated from the server by a firewall, you must first open port 3851 for bidirectional User Datagram Protocol (UDP) and Transport Control Protocol (TCP) traffic on that firewall. This port number is assigned to Arista Networks. Zero-configuration cannot work if multiple APs are set up to connect to multiple servers. In this case, the APs must be configured manually. For details on how to configure an AP manually, see the Access Point CLI Guide on our website at https://www.arista.com/en/support/product-documentation .

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

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

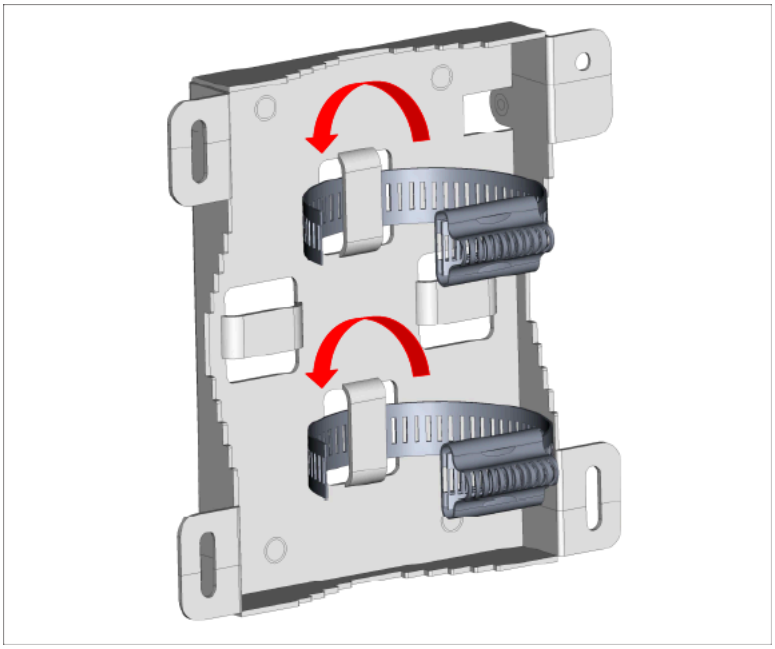
1. Pole Mount the AP
2. Connect the Access Point to the Network
3. Power the Access Point On

4.1 Pole Mount the AP

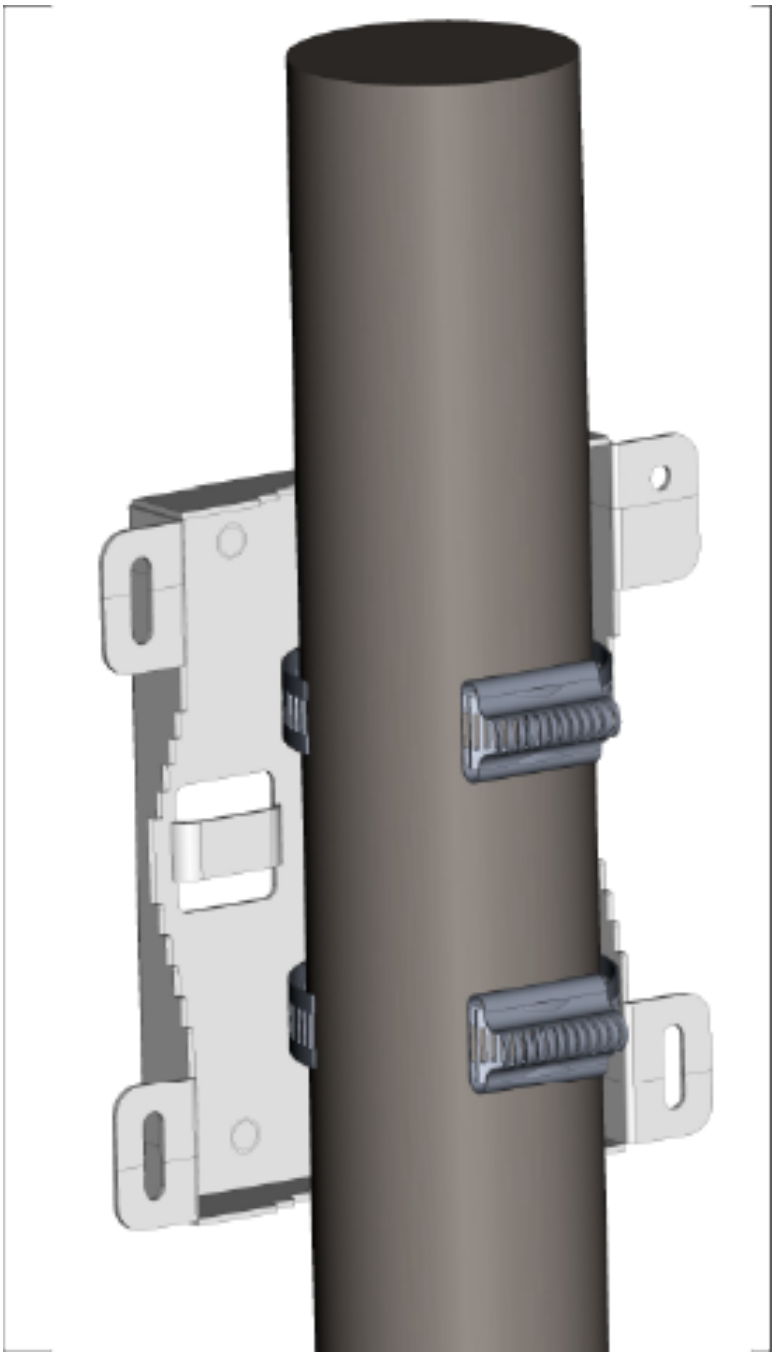
Use the mounting bracket and metal clamps to install the AP on a pole. Standard accessories include the mounting bracket and two metal clamps.

To mount the AP:

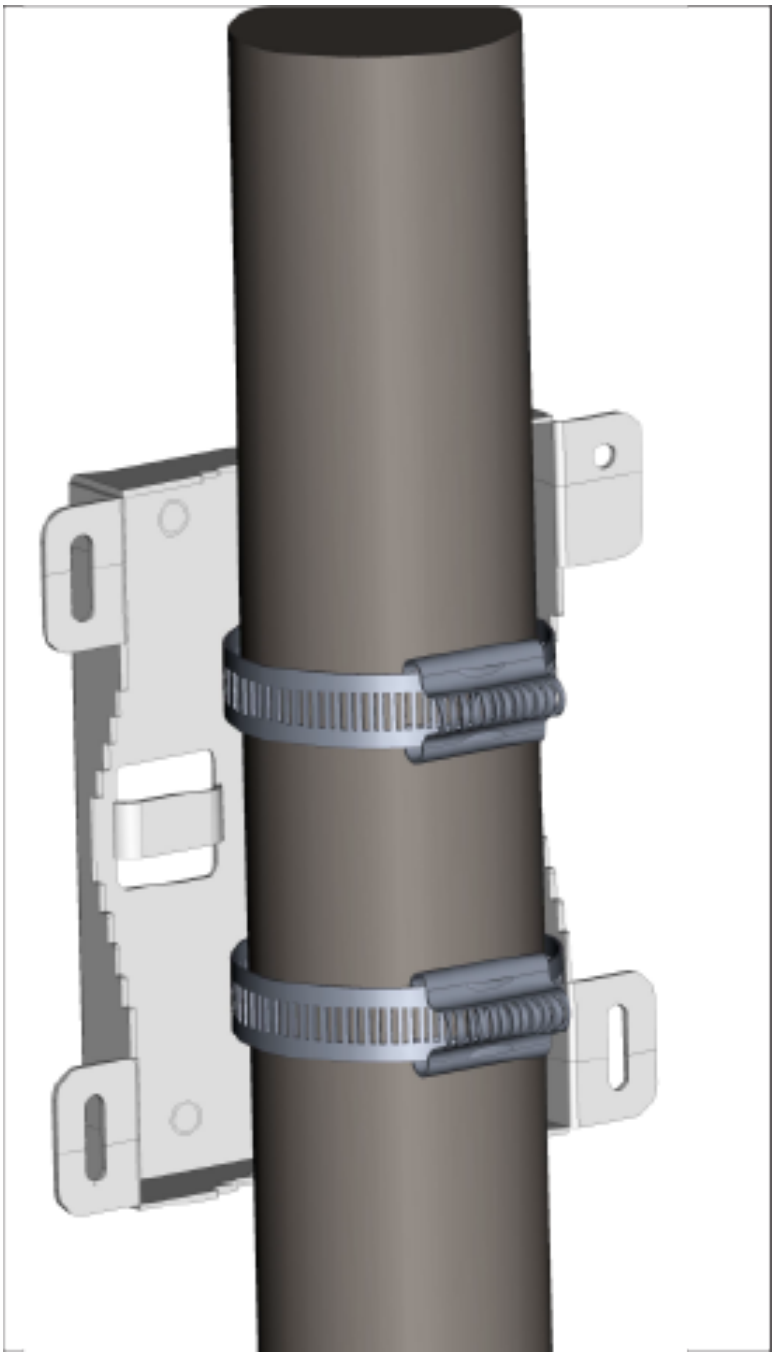
1. Insert the two metal clamps into the bracket. You can insert the clams either in the horizontal or vertical slots depending on the position the pole-mount bracket for use on a vertical or horizontal pole.



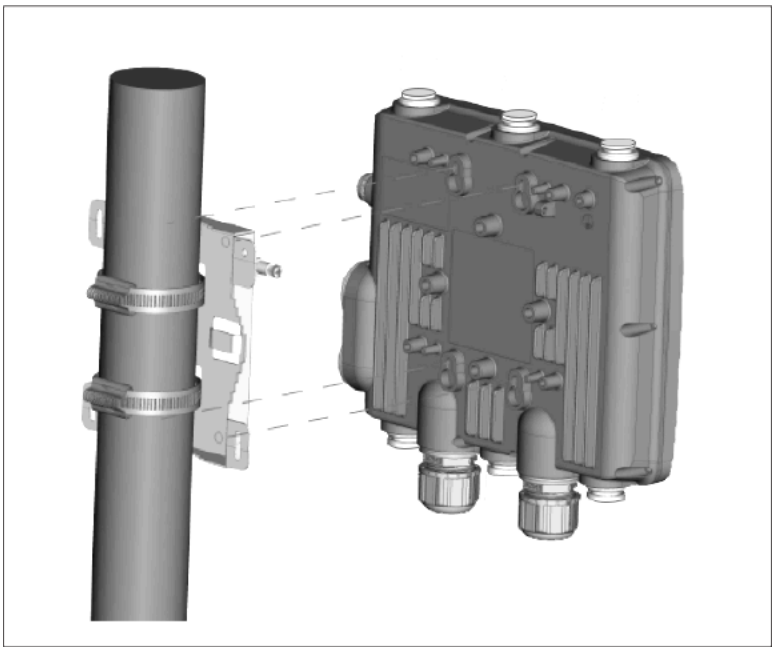
2. Fix the bracket to a pole. You can position the pole-mount bracket for use on a vertical or horizontal pole.



3. Fasten the two metal clamps into the slotted driver.



4. Mount the AP to the bracket.



5. Tighten the thumb screw using Philips# 2 screwdriver.

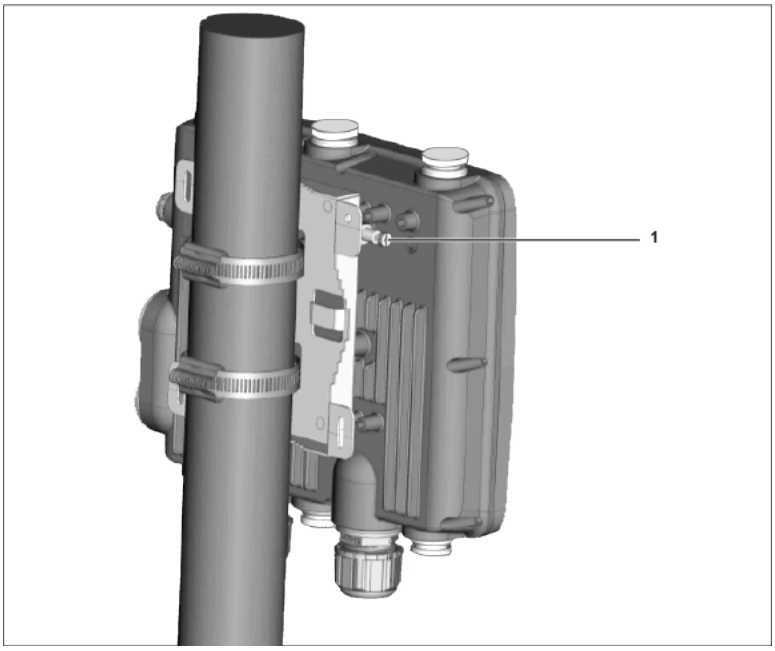


Table 7: Labels: Parts

Label	Description
1	Use a Philips #2 screwdriver to fasten the screw.

Chapter 5

Power the Access Point On

Plug one end of the Ethernet cable into the PoE++ switch or compatible PoE injector (a Single-port High Power Midspan, 802.3bt compliant, up to 5Gigabit PoE with PD54V in power output) and the other end into the LAN1 (PoE++) on the AP. Make sure the PoE++ source you are using is turned ON. Use an active wrench with 27 mm opening to open the LAN (PoE++) port cap.

Figure 5-1: Use Active Wrench

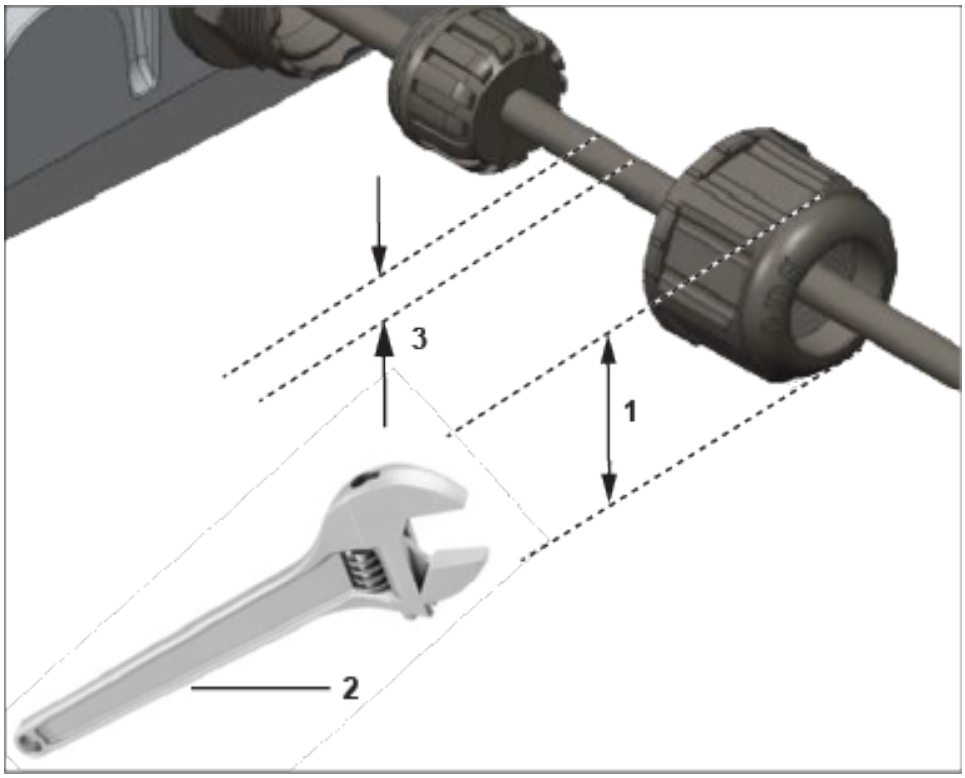


Table 8: Labels: Measurements

Label	Description
1	The width of the LAN port cap is 27mm.
2	Use an active wrenchto open the LAN port cap.
3	LAN cable of 6 ~ 8mm width

Earthing or Grounding: The AP must be properly grounded using a copper earthing wire (12 ~ 10 AWG) and a tin-plated lug as shown in the following image. The wire and the lug must be tightened at the earthing screw on the AP.

Note: Connect the power cord of the power adapter (if used) to a socket outlet with an earthing connection.

The folowing two images show the position of the Earthing screw on the AP (shown as serial number 1 in the image) and the dimension of the lug that attaches to the earthing screw.

Figure 5-2: Position of Earthing Screw on AP

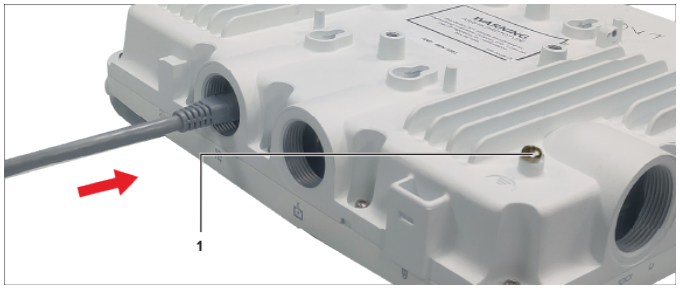
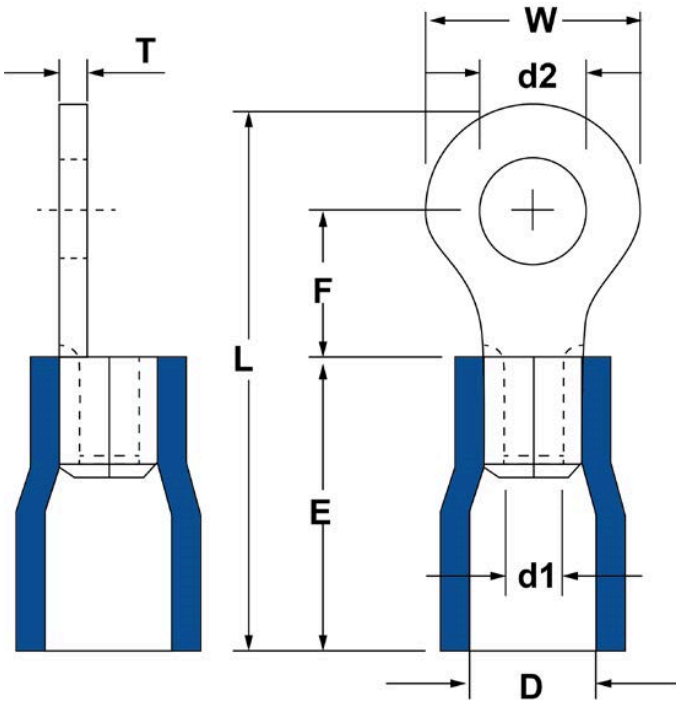


Figure 5-3: Lug Nut Dimensions



Note: The O-435 APs are intended to be supplied with UL-listed PoE+ power source suitable for use at 65 degree Celsius, and whose output meets LPS requirements or PS2, with a rating of 54V DC (0.8A or 800mA minimum).

The following table shows the dimension of the earthing screw and lug.

Item	1	2	3	4	5	6	7	8
Tolerance	W: ± 0.5	d2: ± 0.2	L: ± 0.5	F: ± 0.5	E: ± 0.5	d1: ± 0.2	D: ± 0.2	T: ± 0.5
Size	7.20	4.30	21.50	5.90	13.00	3.40	6.70	1.00

Chapter 6

Connect the Access Point to the Network

To connect the AP to the network, perform the following steps:

1. Ensure that a DHCP server is available on the network to enable network configuration of the AP.
2. Add the DNS entry **wifi-security-server** on all DNS servers. This entry must point to the IP address of the server.
3. Ensure that DHCP is running on the subnet to which the AP is connected.
4. Check the LEDs on the AP to ensure that it is connected to the server.
5. Log on to the server using ssh and run the `get sensor list` command.

   You will see a list of all Arista devices that are recognized by the server. Single Sign-On users can go to the **Monitor** tab in CloudVision Cognitive Unified Edge and check whether the access point is visible under the **Monitor** tab.

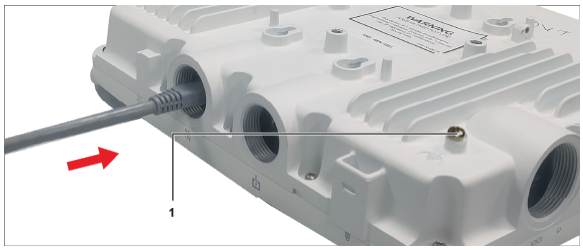
Note: If zero configuration fails, the AP must be configured manually.

Important: If DHCP is not enabled on a subnet, the AP cannot connect to that subnet with zero-configuration. If the DNS entry is not present on the DNS servers, or if you do not have the DHCP server running on the subnet, you must manually configure the AP. For details on configuring an AP manually, see the Access Point Configuration guide on our website at https://www.arista.com/en/support/product-documentation .

6.1 Connect the Access Point 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.

Figure 6-1: LAN Port



The figure shows the LAN cable inserted to the LAN1 Port. Labe l points to the relative position of the earthing screw on the AP.

For PoE port details, see the Bottom Panel section.

Chapter 7

Access Point Troubleshooting

The table below lists some of the troubleshooting guidelines for the access point (AP).

Problem	Solution
The AP 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 AP is connected. If the AP still fails to get a valid IP address, you can reboot it to see if the problem is resolved.
Unable to connect to the server.	• Ensure that the server is running and is reachable from the network to which the AP is connected. If a firewall or a router has Access Control Lists (ACLs) enabled between the AP and the server, ensure that traffic on UDP port 3851 is allowed. • Use the IP-based server discovery method and ensure that you have correctly entered the DNS name, **wifi-security-server** , on the DNS server. • Ensure that the DNS server IP addresses are either correctly configured, or are provided by the DHCP server. • The AP might fail to authenticate with the server. In this case, an 'Authentication failed ' 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 UDP port 3851 and port 80. • If you are using a Proxy, Web Accelerator, or URL Content Filter between the AP and the Internet, ensure that 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 support-campus@arista.com.

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. From this point on, all communication between the AP and server is encrypted using the session key.

The AP and server are shipped with the same default value of the shared secret. Both the server and the AP have CLI commands to change 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. You must manually configure the new communication key on an AP if it is not connected to the server when the key is changed on the server.

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

Appendix B: Product Compliance

Singapore IMDA Registration Mark

Figure 9-1: Singapore IMDA Registration Mark

IP67 Mark