

ARISTA

Quick Start Guide

O-235E Access Point

Arista Networks

www.arista.com

DOC-04357-03

Headquarters	Support	Sales
5453 Great America Parkway Santa Clara, CA 95054 USA		
408 547-5500	408547-5502 866 476-0000	408 547-5501 866 497-0000
www.arista.com	support-wifi@arista.com	sales@arista.com

© Copyright 2022 Arista Networks, Inc. The information contained herein is subject to change without notice. Arista Networks and the Arista logo are trademarks of Arista Networks, Inc in the United States and other countries. Other product or service names may be trademarks or service marks of others.

Contents

1 About This Guide.....	1
2 Package Content.....	1
3 Access Point Overview.....	3
3.1 Front Panel.....	3
3.2 Rear Panel.....	5
3.3 Side Panel.....	6
4 Install the Access Point.....	7
4.1 Pole Mount the AP.....	8
4.2 Power On the AP.....	11
4.3 Connect the AP to the Network.....	12
4.3.1 Connect the AP using PoE.....	13
4.4 Connect External Antennas to O-235E.....	13
5 Access Point Troubleshooting.....	14
6 Appendix A: AP-Server Mutual Authentication.....	15

1 About This Guide

This installation guide explains how to deploy the O-235E access point (AP).

 **Important:** Please read the EULA before installing O-235E. 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-235E outdoor access point.

Document Overview

This guide contains the following chapters:

- [Package Content](#)
- [O-235E Overview](#)
- [Installing O-235E](#)
- [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.

This equipment conforms to the requirements of the NCC.

- 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
- 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前項合法通信，指依電信法規定作業之無線電通信。低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。
- 無線資訊傳輸設備避免影響附近雷達系統之操作。
- 本器材須經專業工程人員安裝及設定，始得設置使用，且不得直接販售給一般消費者。

2 Package Content

The access point (AP) package must contain the components shown in the following figure.



Figure 1: Package Components

Table 1: Labels: Package Components

Label	Description
1	O-235E Access Point
2	2 metal clamps for fixing the mounting bracket to the pole
3	Mounting bracket

Label	Description
4	4 steel bosses for fixing AP in the bracket
5	Philips screw to secure the AP to the bracket
6	Earthing screw fitted at the back of AP with dimension 6.8 ± 0.2 mm
7	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 \times 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.

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

3 Access Point Overview

The O-235E is a tri radio (4X4 5GHz, 2X2 2.4GHz, 2x2 Dual-band scan radio), Wi-Fi 6 access point.

This chapter provides an overview of the O-235E and describes the:

- [Front Panel of the AP](#)
- [Rear Panel of the AP](#)
- [Side Panel of the AP](#)

3.1 Front Panel

The front panel of the O-235E has 6 LEDs that indicate the status of various device functions.

Figure 2: Front Panel LEDs



Table 2: Labels: Front Panel LEDs

Label	Description
1	Power
2	2.4 GHz Radio
3	5 GHz Radio
4	Third Radio
5	LAN1
6	LAN2

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

Table 3: Power LED States Description

	Green	Orange
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, i.e., 802.3af instead of 802.3at.

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 Rear Panel

The rear panel of the AP has LAN/PoE+ connectors that enable you to connect the AP to a wired LAN through a switch or a hub. The ports provide power to the AP by using the 802.3at standard. Use an active wrench to open the LAN cap.

Figure 3: O-235E Rear Panel

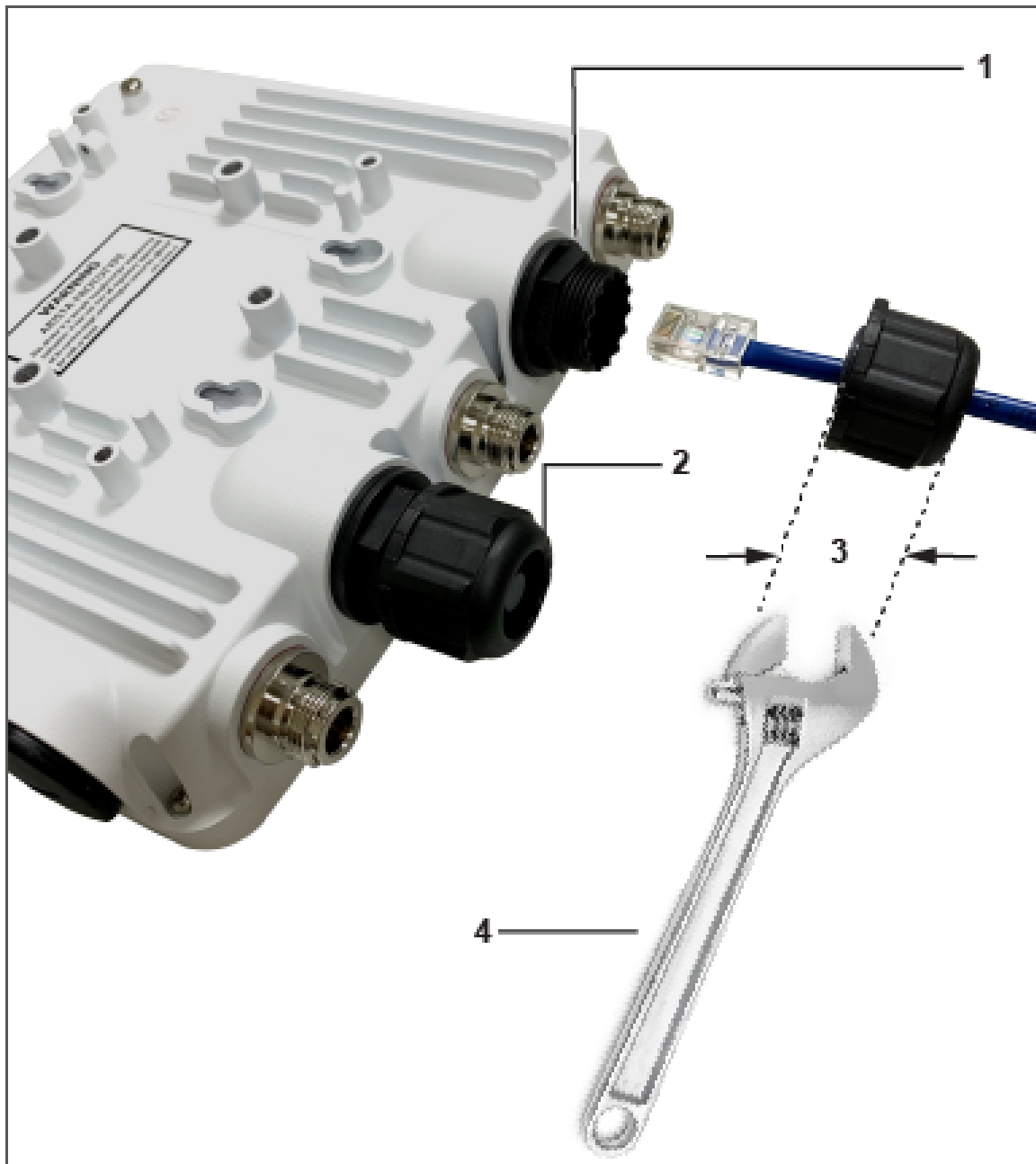


Table 4: Labels: Ports

Label	Description
1	LAN1 (PoE+)

Label	Description
2	LAN2
3	Width of the LAN cap is 29 mm
4	Wrench to open the LAN cap

Table 5: O-235E Port Details

Port/Button	Description	Connector Type	Speed/Protocol
LAN1	5 Gigabit Ethernet with 802.3at compliant PoE	IP67-rated, weatherproof RJ-45	100/1000 Mbps Ethernet, 1/2.5/5 Gbps Ethernet
LAN2	1 Gigabit Ethernet with 802.3at compliant PoE	IP67-rated, weatherproof RJ-45	100/1000 Mbps Ethernet

3.3 Side Panel

The side panel of the AP has a console port, a USB port, and a Reset pin.

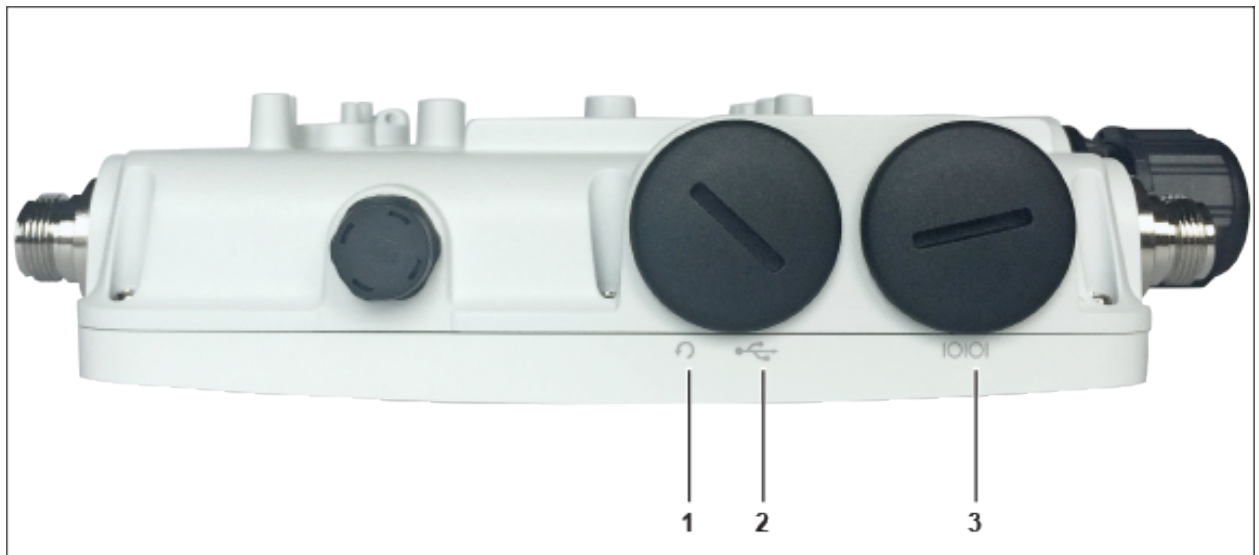


Figure 4: Side Panel

Table 6: Labels: Side Panel

Label	Description
1	Reset
2	USB
3	Console

Port	Description	Connector Type	Speed/Protocol
------	-------------	----------------	----------------

Console	Establish 'config shell' terminal session via serial connection	RJ-45	<ul style="list-style-type: none"> • RS 232 Serial (115200 bits per second) • Data bits:8; Stop bits: 1 • Parity: None • Flow Control: None
USB	USB 2.0 port	USB	Future Use
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.


4 Install the Access Point

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

Zero-Configuration of O-235E as 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.

 **Important:** If the AP is on a network segment that is separated from the server by a firewall, you must first open the 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 Configuration 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. Before you install the AP in a hard-to-reach location, note the MAC address and the IP address of the AP for later use. The MAC address is printed on a label at the bottom of the AP.

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

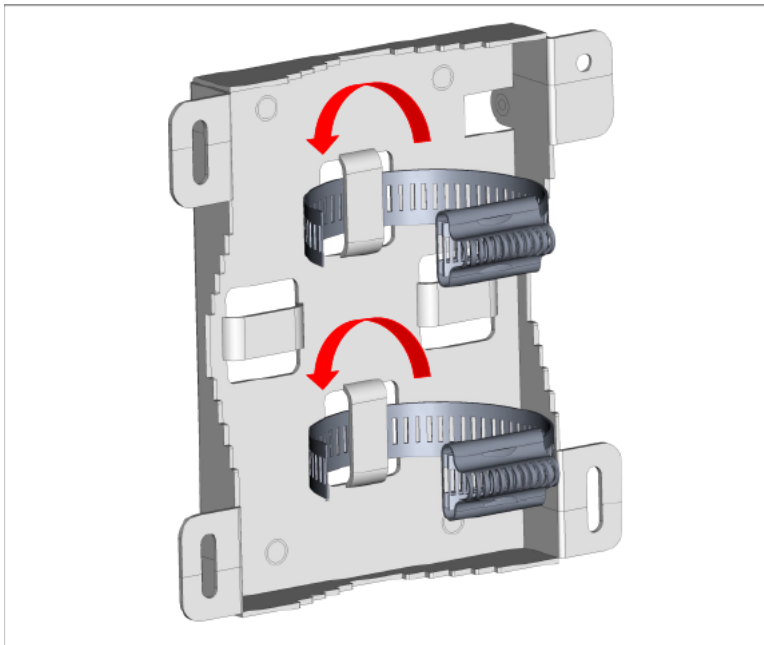
1. [Pole Mount the AP](#)
2. [Connect External Antennas](#)
3. [Power On the AP](#)
4. [Connect the AP to the Network](#)

4.1 Pole Mount the AP

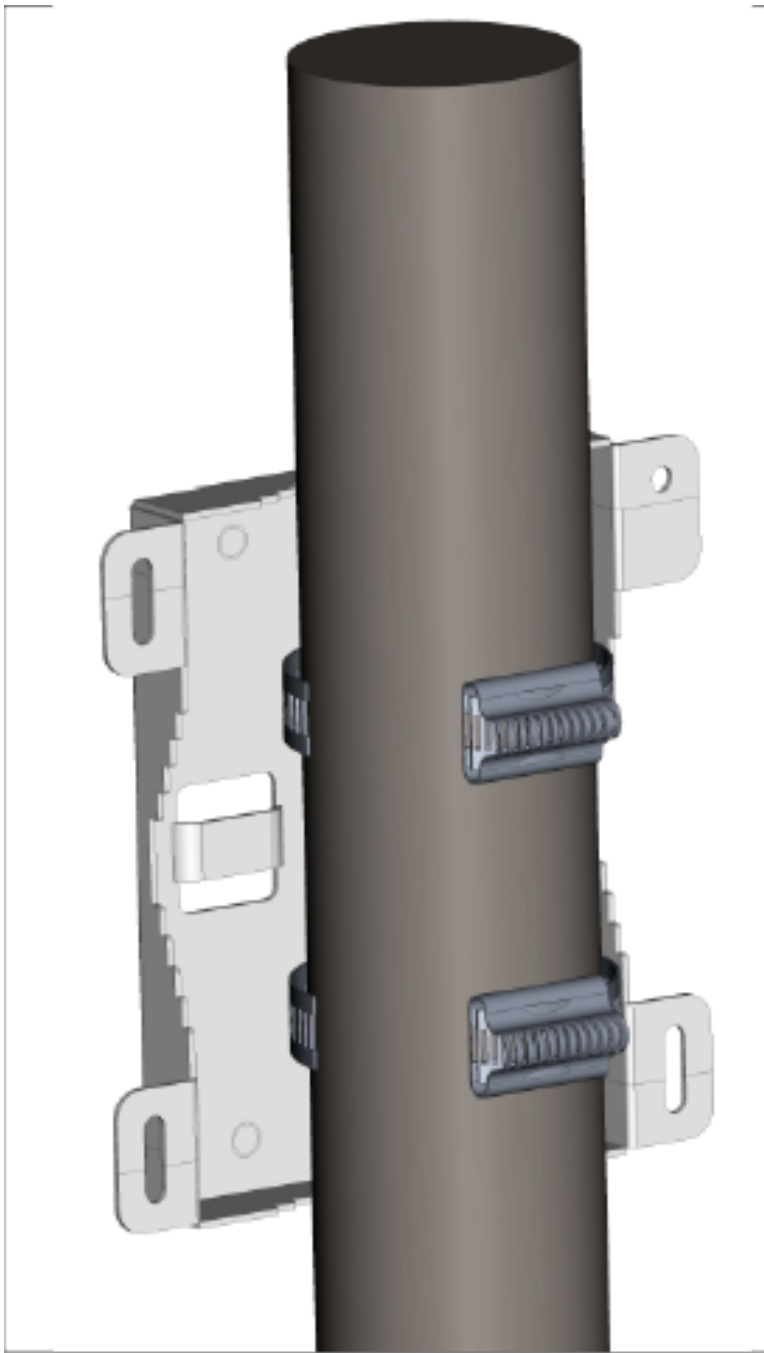
Use the mounting bracket and metal clamps to install the O-235E AP on a pole. Standard accessories include the mounting bracket and two metal clamps.

To mount the AP:

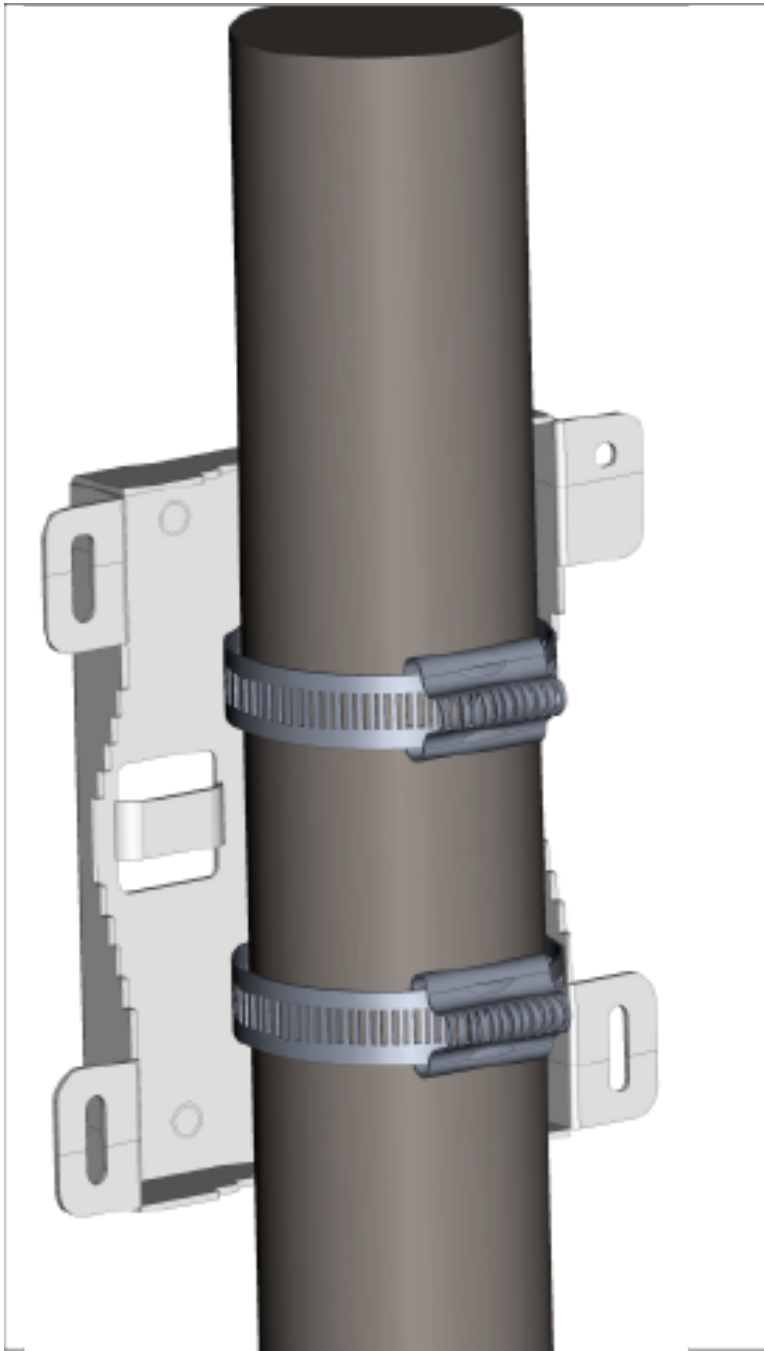
1. Insert the two metal clamps into the bracket. You can insert the clamps either in the horizontal or vertical slots depending on the position the pole-mount bracket for use on a vertical or horizontal pole.



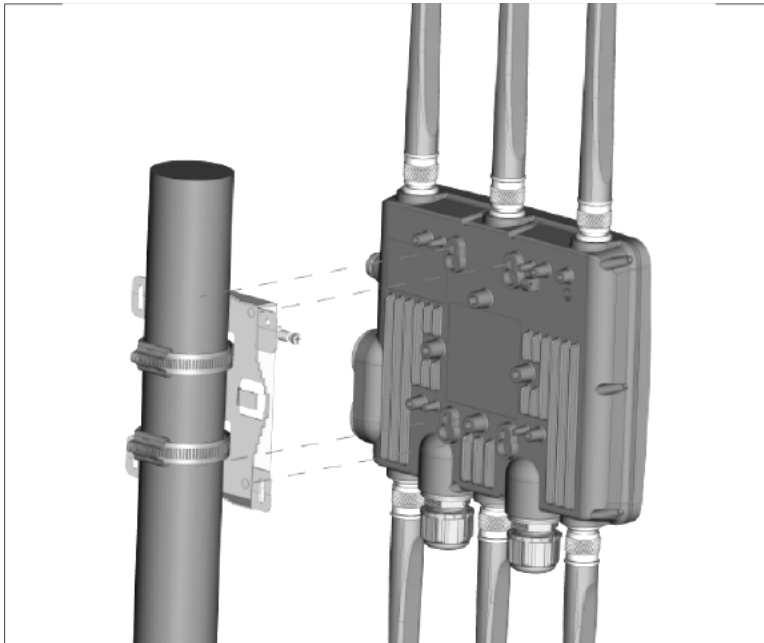
2. Fix the bracket to a pole. You can position the pole-mount bracket for use on a vertical or horizontal pole.



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.

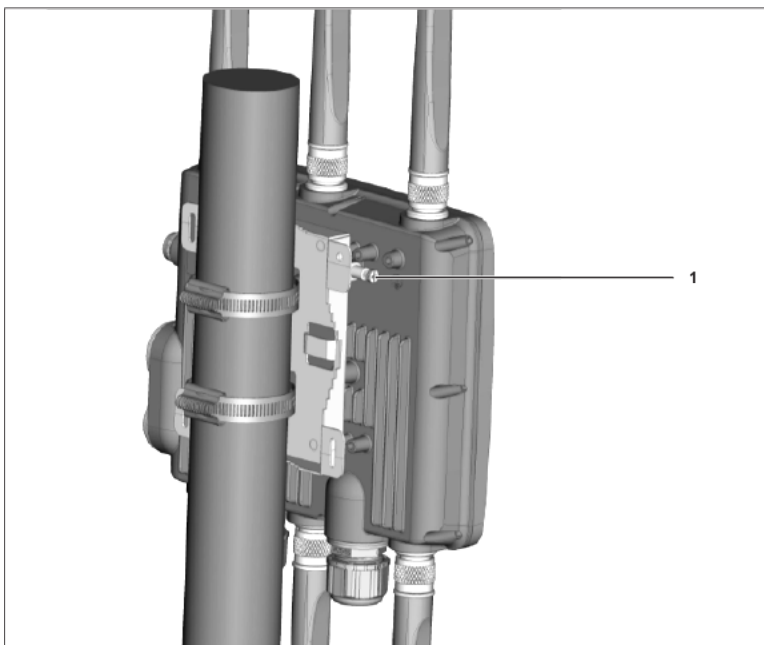


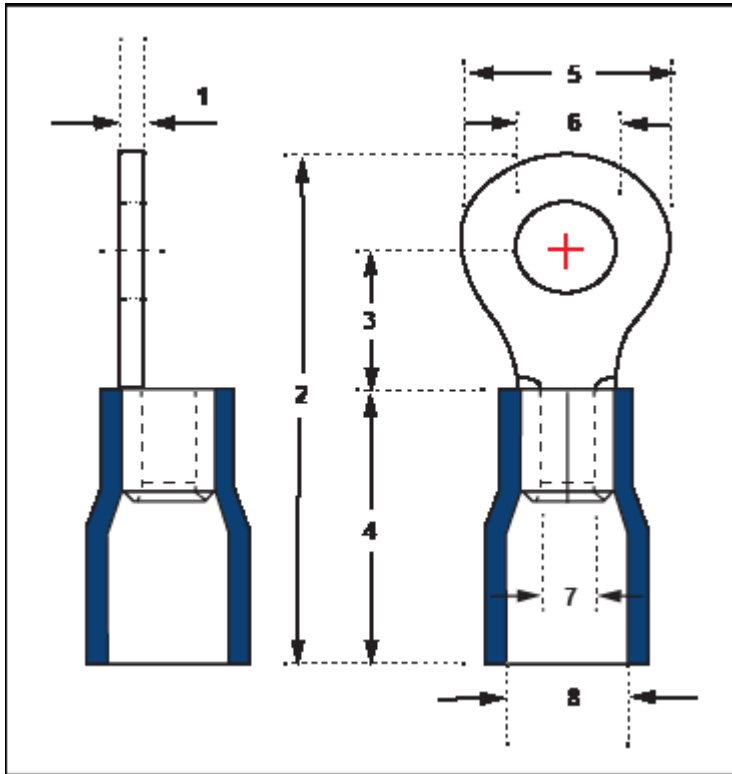
Table 7: Labels: Parts

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

4.2 Power On the AP

Plug one end of the Ethernet cable into the PoE+ switch or compatible PoE injector (a Single-port High Power Midspan, 802.3at compliant, up to Gigabit PoE with 30W minimum power output) and the other end into the LAN1 (PoE+) on the O-235E. Make sure the PoE+ source you are using is turned ON.

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: O-235E 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 48V DC (0.5A minimum).

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

Item	1	2	3	4	5	6	7	8
Tolerance	± 0.5	± 0.5	± 0.5	± 0.5	± 0.5	± 0.2	± 0.2	± 0.2
Size	1.0	21.50	5.90	13.0	7.20	4.30	3.40	6.70



4.3 Connect the AP to the Network

To connect the access point (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.

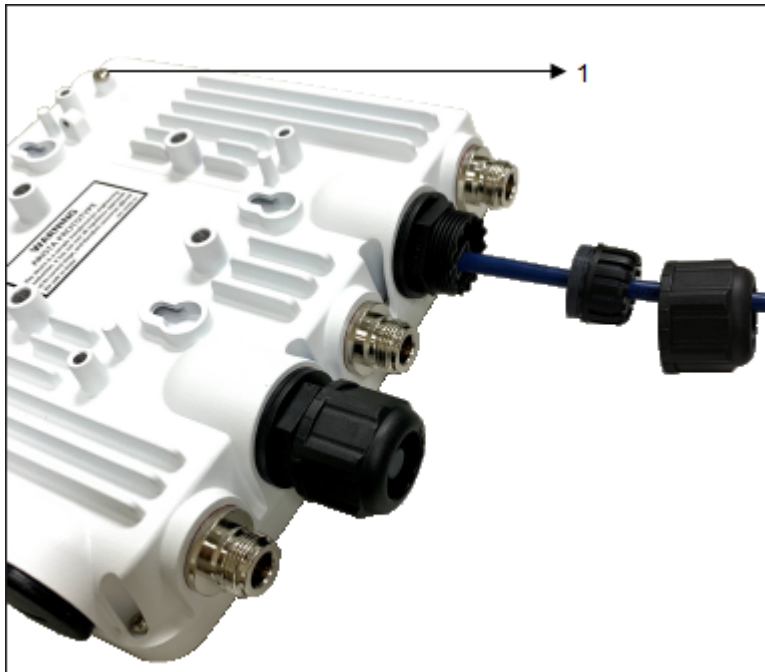
You will see a list of all Arista devices that are recognized by the server. Single Sign-On users can go to the **Monitor** tab in CloudVision Cognitive Unified Edge and check whether the device is visible under the **Monitor** tab.

The AP is connected and operational.

-  **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>.

4.3.1 Connect the AP 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.



The following table shows the position of the earthing screw in the access point:

Item	Description
1	Earthing screw

4.4 Connect External Antennas to O-235E

Connect the external antennas to their respective ports using "N Type" connectors.

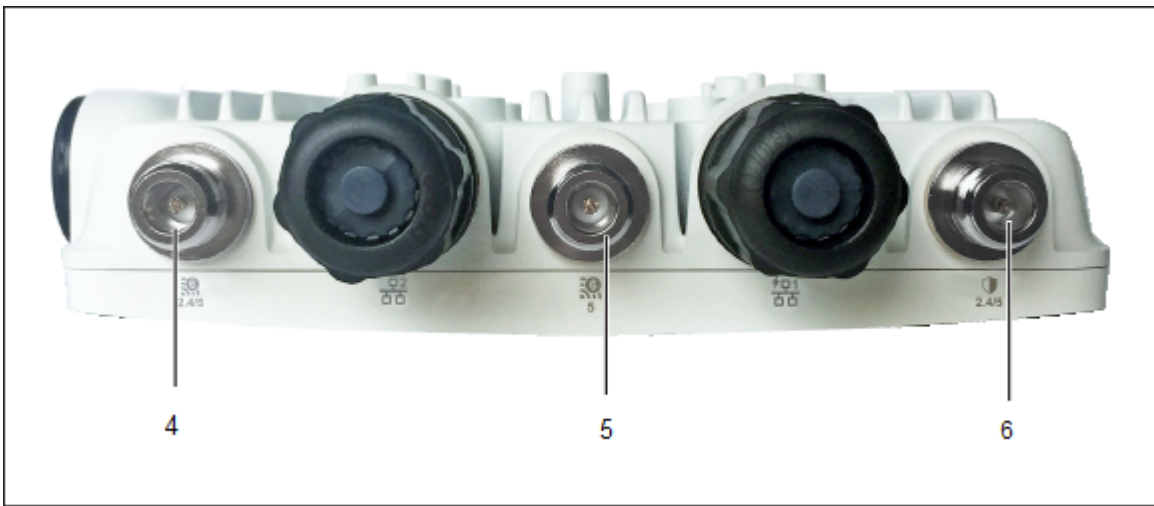
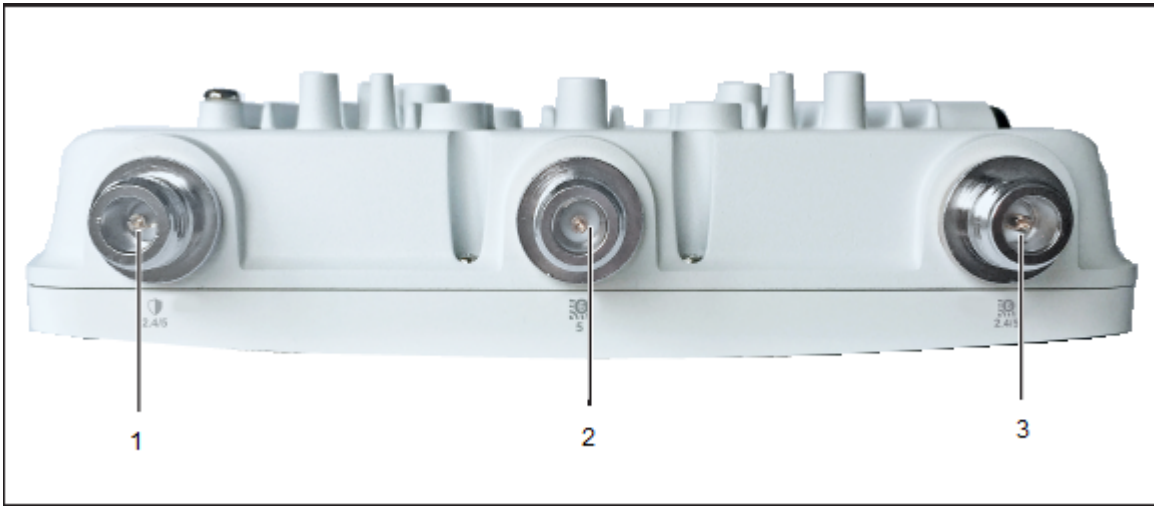


Table 8: Labels: Antenna Ports

Label	Description
1	Scanning radio, 2.4/5 GHz
2	Access radio, 5 GHz
3	Access radio, 2.4/5 GHz
4	Access radio, 2.4/5 GHz
5	Access radio, 5 GHz
6	Scanning radio, 2.4/5 GHz

5 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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 http://support-wifi@arista.com.

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. 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.