Quick Start Guide

C-250 Access Point

C-260 Access Point

Arista Networks

www.arista.com

DOC-03846-04
Contents

1 About This Guide................................................................................ 1
2 Package Content.................................................................................. 1
3 Access Point Overview....................................................................... 2
4 Install the Access Point...................................................................... 6
5 Access Point Troubleshooting........................................................... 11
6 Appendix A: AP-Server Mutual Authentication................................. 12
1 About This Guide

This installation guide explains how to deploy the C-250 or C-260 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](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
- Installing the 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**


This telecommunication equipment conforms to the technical standards or requirements of NBTC.

2 Package Content

The access point (AP) package must contain the components shown in the following figure.
Table 1: Labels: Package Components

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>C-250 or C-260 Access Point</td>
</tr>
<tr>
<td>2</td>
<td>15/16&quot; (24 mm) Mounting Bracket</td>
</tr>
</tbody>
</table>

**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-wifi@arista.com or return the package to the vendor or dealer where you purchased the product.

### 3 Access Point Overview

C-250 or C-260 is a tri-radio 802.11ax access point.

This chapter provides an overview of the C-250 or C-260 access point (AP) and describes:
3.1 Front Panel

The front panel of the C-250 or C-260 has 6 LEDs that indicate the status of various device functions.

![Front Panel LEDs](image)

**Table 2: Labels: Front Panel LEDs**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Power</td>
</tr>
<tr>
<td>2</td>
<td>2.4 GHz Radio</td>
</tr>
<tr>
<td>3</td>
<td>5 GHz Radio</td>
</tr>
<tr>
<td>4</td>
<td>Third Radio</td>
</tr>
<tr>
<td>5</td>
<td>LAN1</td>
</tr>
<tr>
<td>6</td>
<td>LAN2</td>
</tr>
</tbody>
</table>

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

**Table 3: Power LED States Description**

<table>
<thead>
<tr>
<th></th>
<th>Green</th>
<th>Orange</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solid</td>
<td>Running at full capability</td>
<td>Running at reduced capability</td>
</tr>
<tr>
<td>Blinking</td>
<td>Received IP address, but not connected to the server</td>
<td>Did not receive an IP address</td>
</tr>
</tbody>
</table>

Reduced capability indicates that the AP is getting lower than the required maximum power from the PoE switch, i.e., 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 Rear Panel

The rear panel of the AP has its DC power port and 802.3bt compliant PoE LAN ports to power the device and connect it to a wired LAN.

![Rear Panel Diagram]

**Figure 3: Rear Panel**

**Table 4: Labels: Rear Panel**

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>LAN1</td>
</tr>
<tr>
<td>2</td>
<td>LAN2</td>
</tr>
<tr>
<td>3</td>
<td>Power</td>
</tr>
</tbody>
</table>

The first of the following tables shows port details for C-250, and the second one shows port details for C-260.
### Table 5: C-250 Port Details

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Connector Type</th>
<th>Speed/Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>12V DC</td>
<td>5.5 mm overall diameter / 2.1 mm center pinhole</td>
<td>N/A</td>
</tr>
<tr>
<td>LAN 1</td>
<td>2.5 Gigabit Ethernet with 802.3bt compliant PoE</td>
<td>RJ-45</td>
<td>100/1000 Mbps / 2.5 Gbps Ethernet</td>
</tr>
<tr>
<td>LAN 2</td>
<td>2.5 Gigabit Ethernet with 802.3bt compliant PoE</td>
<td>RJ-45</td>
<td>100/1000 Mbps / 2.5 Gbps Ethernet</td>
</tr>
</tbody>
</table>

### Table 6: C-260 Port Details

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Connector Type</th>
<th>Speed/Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>12V DC</td>
<td>5.5 mm overall diameter / 2.1 mm center pinhole</td>
<td>N/A</td>
</tr>
<tr>
<td>LAN 1</td>
<td>5 Gigabit Ethernet with 802.3bt compliant PoE</td>
<td>RJ-45</td>
<td>100/1000 Mbps / 2.5 /5 Gbps Ethernet</td>
</tr>
<tr>
<td>LAN 2</td>
<td>5 Gigabit Ethernet with 802.3bt compliant PoE</td>
<td>RJ-45</td>
<td>100/1000 Mbps / 2.5/5 Gbps Ethernet</td>
</tr>
</tbody>
</table>

### 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](image-url)
Table 7: Labels: Side Panel

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Reset</td>
</tr>
<tr>
<td>2</td>
<td>USB</td>
</tr>
<tr>
<td>3</td>
<td>Console</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
<th>Connector Type</th>
<th>Speed/Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Console</td>
<td>Establish ‘config shell’ terminal session via serial connection</td>
<td>RJ-45</td>
<td>• RS 232 Serial (115200 bits per second) &lt;br&gt;• Data bits:8; Stop bits: 1 &lt;br&gt;• Parity: None &lt;br&gt;• Flow Control: None</td>
</tr>
<tr>
<td>USB</td>
<td>USB 2.0 port</td>
<td>USB</td>
<td>Future Use</td>
</tr>
<tr>
<td>Reset</td>
<td>Reset to factory default settings port. Hold down and power cycle the device to reset.</td>
<td>Pinhole push button</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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 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.

**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 Configuration Guide on our website at [https://www.arista.com/en/support/product-documentation](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. Ceiling Mount the AP or Wall Mount the AP.
2. Connect the AP to the network.
3. Power ON the AP.

### 4.1 Ceiling Mount the Access Point

Mounting the access point (AP) on the ceiling consists of the following steps:

1. **Affix the bracket to the T-grid:** Use the mounting bracket to install the AP on the ceiling. Fix the bracket to the T-grid and rotate the bracket so that it snaps on the T-grid. The bracket is now parallel to an arm of the T-grid. Ensure that the bracket is properly snapped to the T-grid, as shown below.

2. **Mounting C-250 on the bracket:** Place the first mounting post on the rear-side of the AP on to the lower notch of the bracket. Rotate the AP such that the center mounting post fits in to the center notch on the bracket. Ensure that all the mounting posts on the rear-side of the AP are snapped in to the respective notches on the bracket. The mounting posts now properly fit in the respective notches of the bracket and the AP is mounted properly.
Mounting Instructions using the Silhouette/Interlude Bracket Mount: The Silhouette/Interlude mounting bracket is not a part of the standard package and must be procured separately. The mounting instructions for the Silhouette/Interlude Bracket Mount are similar to the Standard Package Content's mounting instructions.

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

4.2 Wall Mount the Access Point

Note: The wall mounting accessory SKU can be ordered and purchased separately.

Mounting the access point (AP) on a wall consists of the following steps:

1. Drill four mounting holes in the wall, as shown below.

![Diagram of drilling holes](image)

Table 8: Labels: Dimensions to drill holes

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>46 mm</td>
</tr>
<tr>
<td>2</td>
<td>83.4 mm</td>
</tr>
<tr>
<td>3</td>
<td>Diameter: 6.5 mm, Depth: 30 mm</td>
</tr>
</tbody>
</table>

2. Insert four anchors.

![Diagram of anchors](image)

3. Affix the mounting bracket on the wall.
4. Attach the AP to the mounting bracket. Pull the release key outward. Attach the AP stubs to the bracket holder, ensuring a firm fit.

5. Once attached, push in the release key to lock the hooks and make sure all the hooks are locked in place.

6. Fasten the release key screw with a tamper-resistant T10 torx screwdriver to lock the AP to the bracket.
4.3 **Power the Access Point On**

You can power the access point (AP) on by plugging one end of the Ethernet cable into the PoE switch or injector and the other end into the Ethernet/PoE port on the AP. Ensure the PoE source you are using is turned on.

As an alternative to PoE, you can insert a compatible power adaptor plug into an AC power outlet and the other end into the power input port on the AP.

---

**Note:** If you are not using PoE, ensure that you use only an AC power adaptor supported by the AP.

4.3.1 **Using the C-250 with Power Adapter**

To power up the device with power adapter, perform the following steps:

1. Plug the power cable into the DC power receptacle at the rear of the device.
2. Plug the other end of the power cable into an 110V~240V 50/60 Hz AC power source.
3. Wait until the device is ready. Refer to the LED status table.

4.4 **Connect the Access Point 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](https://www.arista.com/en/support/product-documentation).
4.4.1 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.

For PoE port details, see the Rear Panel section.

5 Access Point Troubleshooting

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

<table>
<thead>
<tr>
<th>Problem</th>
<th>Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>The AP did not receive a valid IP address via the DHCP.</td>
<td>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.</td>
</tr>
</tbody>
</table>
| 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-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.