ARISTA

Quick Start Guide

C-100 Access Point

Arista Networks
DOC-03480-01

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 C-100 access point (AP).

⚠️ **Important:** Please read the EULA before installing C-100. 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 in this document.

Intended Audience

This guide can be referred by anyone who wants to install and configure the C-100 access point.

Document Overview

This guide contains the following chapters:

📝 **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.
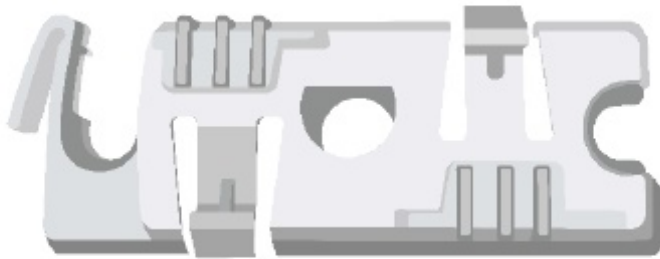
Chapter 2. Package Content

The C-100 package must contain the components shown in the figure below.

Figure 1: C-100 Package Components

C-100

15/16" (24mm) Mounting Bracket

⚠️ **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 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.

Chapter 3. C-100 Overview
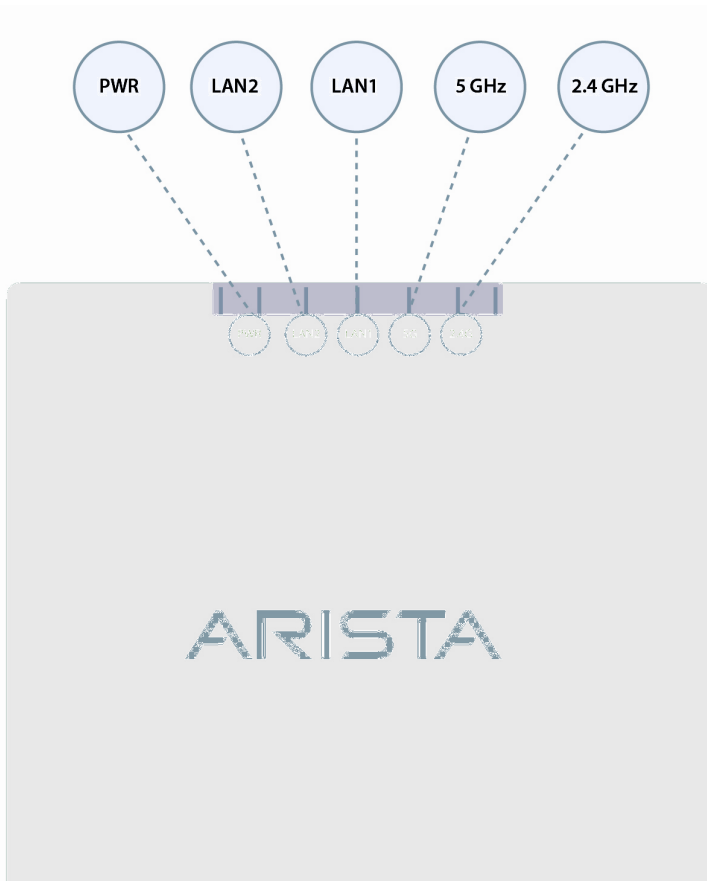
C-100 is a 2x2 802.11a/b/g/n/ac access point.

This chapter provides an overview of the C-100 and describes:

- The Front Panel of the C-100 *(page 5)*.
- The Rear Panel of the C-100 *(page 6)*.

Front Panel of C-100

The front panel of the C-100 has 5 functional LEDs that indicate the working of the device.

Figure 2: C-100 Front Panel LEDs

The following table indicates the device states based on the LEDs.

Table 1: C-100 LED Status Description

LED	Status	Description
Power	Solid Green	Power ON
	OFF	Power OFF
5 GHz	Solid Green	No activity on 5 GHz radio
	Blinking Green	Wireless activity on 5 GHz radio
2.4 GHz	Solid Amber	No activity on 2.4 GHz radio
	Blinking Amber	Wireless activity on 2.4 GHz radio

LED	Status		Description
LAN1 /2	Solid Green	Enabled	

Rear Panel of C-100

The rear panel of the C-100 provides an PoE Ethernet port that enables you to connect the device to a wired LAN through a switch or a hub and power the device by using the 802.3af standard.

Figure 3: C-100 Rear Panel
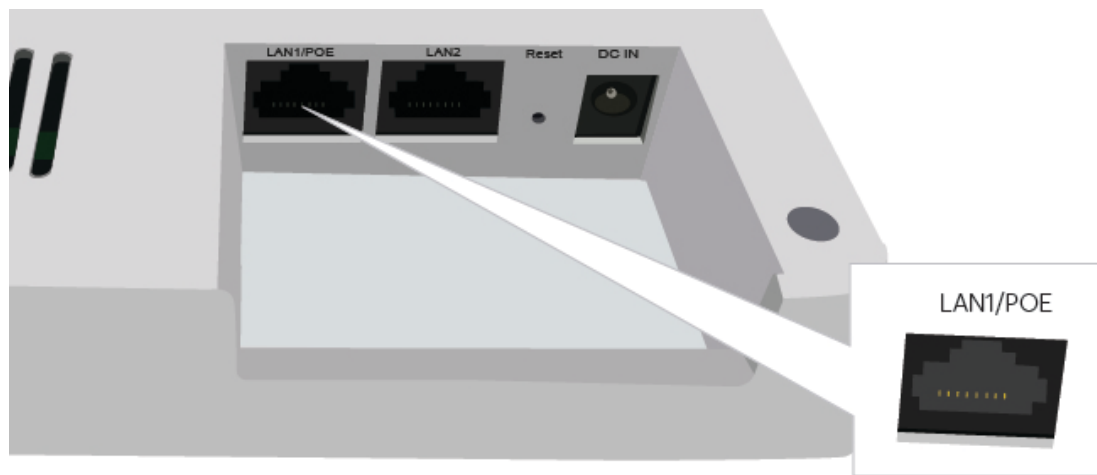
Port	Description	Connector Type	Speed/Protocol
Ethernet (LAN1/PoE)	Gigabit Ethernet port used to connect to the wired LAN and communicate with the Arista Cloud or Server. This port can also be used to power the device using the 802.3af Power over Ethernet (PoE) standard.	RJ45	• 10/100/1000 Mbps Gigabit Ethernet • 802.3af Class 0 PoE • PoE input voltage: 48V
Ethernet (LAN2)	Gigabit Ethernet port that can be used for wired extension for an SSID.	RJ45	10/100/1000 Mbps Gigabit Ethernet
Reset Pin Hole	Reset to factory default settings.	Pin hole push button	Hold down and power cycle the device to reset.
DC IN	Enables you to connect to and power on device using 12 V DC power with 1.5 ampere.	6.3 mm barrel	--

The Reset Pin Hole resets the C-100 device to factory defaults. To reset the device, press and hold the Reset Pin Hole for 10 sec until all LEDs go off which indicates that the device has rebooted. Pressing the Reset Pin Hole while the device is booting up will not have any effect. You should perform this operation only when the device is running.

When you reset the device, 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 static IP is configured on the device, the IP address is erased and DHCP mode is set. The factory default IP address of the device is 169.254.11.74.

Chapter 4. Install the C-100

This chapter contains the stepwise procedure to install the C-100 device.

Zero-Configuration of C-100 as Access Point

Zero-configuration is supported under the following conditions:

- The device is in AP mode with background scanning on with 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 device looks for the DNS entry **wifi-security-server**.

- The device 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 at https://www.arista.com/en/support/product-documentation.

Take a configured C-100, that is, ensure that a static IP is assigned to the device or the settings have been changed for DHCP. Note down 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.

📝 **Note:** 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 7)*
2. Power On the device. *(page 8)*
3. Connect device to the network. *(page 9)*

Mount the C-100

The C-100 mounting procedure can be divided into two parts:

1. **Affix the bracket to the T -grid:** Use the mounting bracket to install the C-100 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. Refer to the images given below.
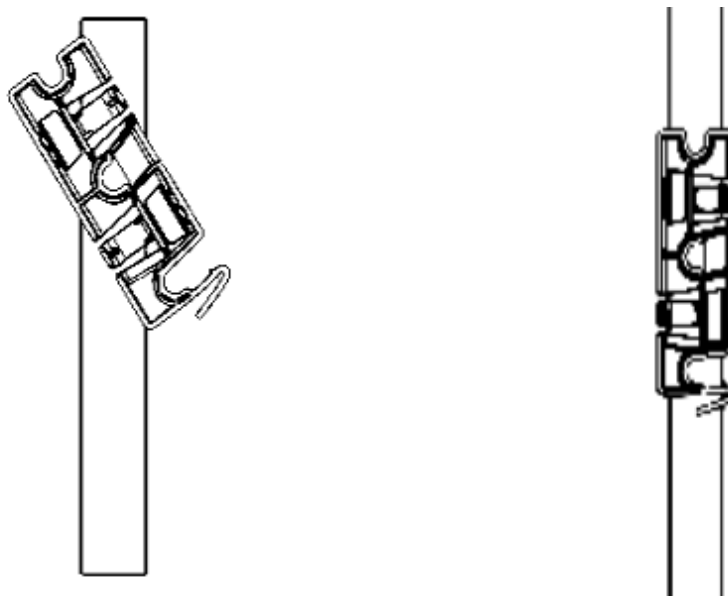
2. **Mounting C-100 on the bracket:** Place the first mounting post on the rear-side of the device on to the lower notch of the bracket. Rotate the device such that the center mounting post fits in to the center notch on the bracket. Ensure that all the mounting posts on the rear-side of the device are snapped in to the respective notches on the bracket. The mounting posts on the rear-side of the device are now properly fit in the respective notches of the bracket and device is mounted properly.
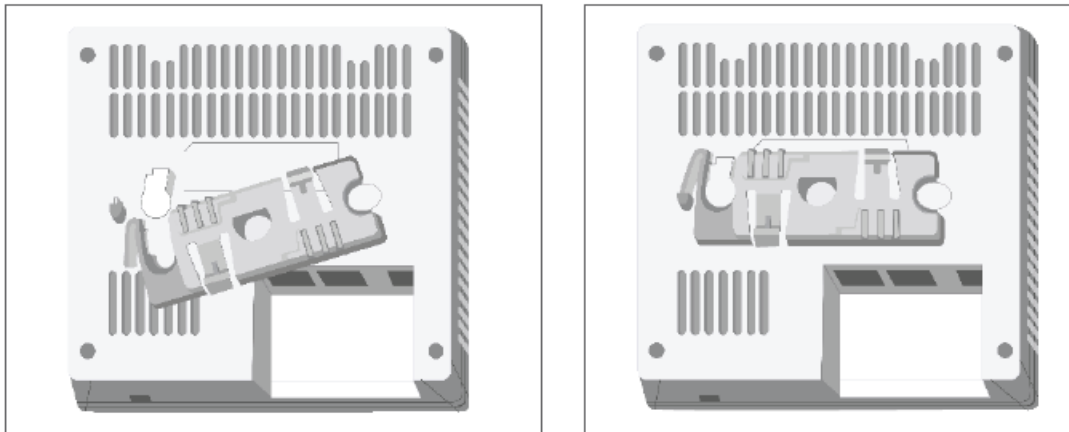
Mounting Instructions using the Silhouette/Interlude Bracket Mount: The Silhouette/Interlude mounting bracket is not a part of the standard package and must be procured separately. The mounting instructions for the Silhouette/ Interlude Bracket Mount are very similar to the Standard Package Content's mounting instructions.

Power On the C-100

The C-100 device can be powered on by plugging one end of the Ethernet cable into the PoE (802.3af) switch or injector and the other end into the Ethernet/PoE port on the C-100. 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 C-100.

> 📝 **Note:** If you are not using PoE, ensure that you use only an AC power adaptor supported by the C-100 access point (AP).

Connect the C-100 to the Network

To connect C-100 to the network, perform the following steps:

1. Ensure that a DHCP server is available on the network to enable network configuration of the C-100.
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. Check the status LEDs on the device. If all LEDs glow green, then the device is operational and 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 **Devices** tab in Wireless Manager and check whether the device is visible under the **Devices** tab.

The device is connected and ready to go operational.

> 📝 **Note:** If the zero configuration is not successful, the device must be configured manually. See the Access Point Configuration Guide on our website at https://www.arista.com/en/support/product-documentation.

> ⚠️ **Important:** If DHCP is not enabled on a subnet, the device 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 device.

Connect the C-100 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.
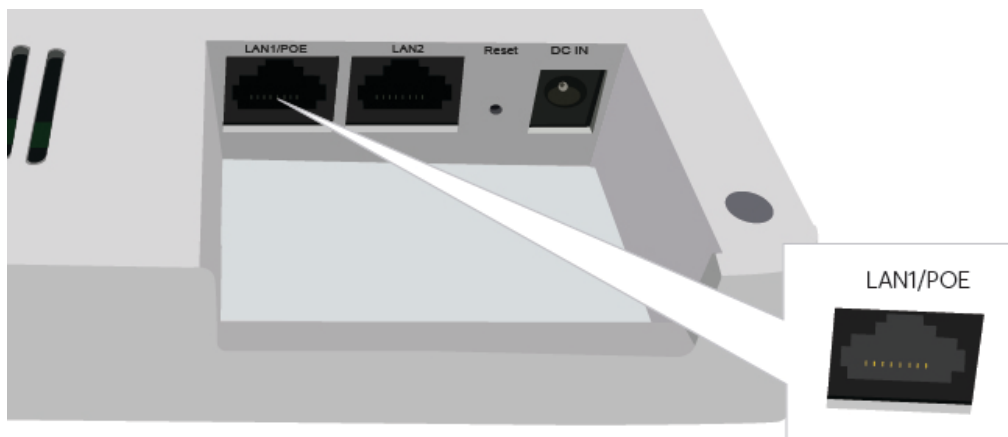
Using the C-100 with Power Adapter

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 details table.

Chapter 5. C-100 Troubleshooting

The table below lists some of the troubleshooting guidelines for C-100.

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 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.