



# Configuring and Deploying the Access Point

This section describes how to connect the AP to a controller. For instructions on how to configure the AP, see the relevant release *Cisco Wireless Controller Configuration Guide*.

- [The Controller Discovery Process, on page 1](#)
- [Deploying the Access Point on the Wireless Network, on page 2](#)
- [Checking the Access Point LEDs, on page 2](#)

## The Controller Discovery Process

To support C9136AXI AP, the controller must be running Cisco IOS-XE 17.7.1 or a later release. For more information, see the access point data sheet at: <https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/nb-06-cat9136-access-point-ds-cte-en.html>

### Guidelines and Limitations

- It is not possible to edit or query an access point using the controller CLI if the name of the access point contains a space.
- Make sure that the controller is set to the current time. If the controller is set to a time that has already occurred, the access point might not join the controller because its certificate may not be valid for that time.

The controller must discover AP before it can become an active part of the network. The AP supports the following controller discovery processes:

- **Locally stored controller IP address discovery:** If the access point was previously joined to a controller, the IP addresses of the primary, secondary, and tertiary controllers are stored in the access point's nonvolatile memory. This process of storing controller IP addresses on an access point for later deployment is called priming the access point. For more information about priming, see the [Performing a Preinstallation Configuration \(Optional\)](#).
- **DHCP server discovery:** This feature uses DHCP option 43 to provide controller IP addresses to the access points. Cisco switches support a DHCP server option that is typically used for this capability. For more information about DHCP option 43, see the [Configuring DHCP Option 43](#).
- **DNS discovery:** The access point can discover controllers through your domain name server (DNS). For the access point to do so, you must configure your DNS to return controller IP addresses in response to CISCO-CAPWAP-CONTROLLER.localdomain, where localdomain is the access point domain name.

Configuring the CISCO-CAPWAP-CONTROLLER provides backwards compatibility in an existing customer deployment. When an access point receives an IP address and DNS information from a DHCP server, it contacts the DNS to resolve CISCO-CAPWAP-CONTROLLER.localdomain. When the DNS sends a list of controller IP addresses, the access point sends discovery requests to the controllers.

## Deploying the Access Point on the Wireless Network

After you have mounted the access point, follow these steps to deploy it on the wireless network:

### Procedure

---

**Step 1** Connect and power up the access point.

**Step 2** Observe the access point LED.

For LED status descriptions, see [Checking the Access Point LEDs, on page 2](#).

- When you power up the access point, it begins a power-up sequence that you can verify by observing the access point LED. If the power-up sequence is successful, the discovery and join process begins. During this process, the LED blinks green, red, and off sequentially. When the access point joins a controller, the LED is green if no clients are associated, or blue if one or more clients are associated.
- If the LED is not on, the access point is most likely not receiving power.
- If the LED blinks sequentially for more than five minutes, the access point is unable to find its primary, secondary, and tertiary controller. Check the connection between the access point and the Cisco Wireless Controller, and be sure that the access point and the Cisco Wireless Controller are either on the same subnet or that the access point has a route back to its primary, secondary, and tertiary Cisco Wireless Controller. Also, if the access point is not on the same subnet as the Cisco Wireless Controller, ensure that there is a properly configured DHCP server on the same subnet as the access point.

For more information, see [Configuring DHCP Option 43](#).

**Step 3** Reconfigure the Cisco Wireless Controller so that it is not the primary.

**Note** A primary Cisco Wireless Controller should be used only for configuring access points and not in a working network.

---

## Checking the Access Point LEDs

The location of the access point status LED is shown in [C9136I Face View](#).










**Note** Regarding LED status colors, it is expected that there will be small variations in color intensity and hue from unit to unit. This is within the normal range of the LED manufacturer's specifications and is not a defect. However, the intensity of the LED can be changed through the controller.

---

The access point status LED indicates various conditions, which are described in the following table.

**Table 1: LED Status Indications**

Message Type	LED State	Message Meaning
Association status	Green 	Normal operating condition, but no wireless client associated
	Blue 	Normal operating condition, at least one wireless client association
Boot loader status	Green 	Executing boot loader
Boot loader error	Blinking Green 	Boot loader signing verification failure
Operating status	Blinking Blue 	Software upgrade in progress
	Alternating between Green and Red 	Discovery or join process in progress
Access point operating system errors	Cycling through Red-Off-Green-Off-Blue-Off 	General warning; insufficient inline power

