Configuring and Deploying the Access Point

This section describes subsequent discovery process for day 1 after the AP has successfully completed the initial discovery. For instructions on how to configure the AP, see the *Cisco Wireless Controller Configuration Guide* for the relevant release.

Note
- To configure a fresh out of the box AP to the Meraki Dashboard or Cisco Catalyst 9800 Controller, see Cisco Wireless Global Use AP Deployment Guide.
- If the organisation policy does not allow and the AP intends to join the controller, use fast offline migration technique.

The Controller Discovery Process

To support the CW9176I AP, the controller must be running Cisco IOS XE 17.15.2 or a later release. For more information, see the Cisco Catalyst 9176 Series Access Points Data Sheet.

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 AP must discover the controller 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 Performing a Preinstallation Configuration.

- 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 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 these controllers.

Deploying the Access Point on a Wireless Network

After you mount the access point, follow these steps to deploy it on a 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, it is most likely that the access point is 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.

Checking the Access Point LEDs

The location of the access point status LED is shown in Connectors and Ports on the AP.

Note
- Regarding LED status colors, it is expected that there might 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.

- When the AP is in Meraki management mode, the LED status indicators convey the status differently from the Cisco APs. For more information, see the CW9176I Installation Guide.

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 is associated
	Blue	Normal operating condition, at least one wireless client is associated
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 powe

Message Type	LED State	Message Meaning
Top right ethernet LED	Off	Link speed is 10 Mb, 100 Mb, or disconnected
	Orange	Link speed is 1000 Mb
	Green	Link speed is 2.5 Gb, 5 Gb, or 10 Gb
Top left ethernet LED	Blinking Green	Activity indicator for received signal or transmitted signal