Network Deployment

This section provides information about network deployment options, and how to include the 6 GHz access points in the network.

Cisco On-Premises Deployment

You can associate the CW9163E AP to a Cisco On-premises deployed network.

Initializing an Access Point

Perform the following procedure for an out-of-the-box (OOB) AP. This procedure prepares the AP to associate with a network.

Procedure

Step 1 Connect the power supply and power up the AP.

The switch port connected to the access point can be a trunk or access port.

Note The mGig or GE port can be used for the AP's connection.

Step 2 (Optional) Configure the switch port to trunk the VLANs when multiple VLANs are used for client traffic in FlexConnect deployment. Use the access mode in Local Mode/Centralized deployments.

Step 3 Configure the VLAN as a native VLAN.

When the management traffic is untagged, the VLAN is used for management.

Example: Configuring the port on a switch

```
interface GigabitEthernet1/0/37
    switchport trunk native VLAN 122
    switchport trunk allowed VLAN 10,20,122
    switchport mode trunk
```

Example: For Flexconnect/Distributed deployments

```
Switch(config)# interface GigabitEthernet 0/0/10
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 1,2,3,4
```

Example: For Local Mode/Centralized deployments

```
Switch(config)# interface GigabitEthernet 0/0/10
Switch(config)# switchport mode access
Switch(config)# switchport access vlan 10
```

Step 4 VLAN associated with the AP must have DHCP scope enabled.

The DHCP scope can be active in the switch or in an external DHCP server.

Step 5 AP's LED should be solid green and with a valid IP address.

In this state, the AP is ready to join a controller. The process should take about five minutes to complete. For LED descriptions, see Checking the Access Point LEDs.

Associating an Access Point with a Controller

The Cisco access points need to associate themselves with a controller in the network. There are multiple methods to complete the association process.

Associate the AP to a controller using one of the following options:

Before you begin

Before associating the AP, ensure that the controller is configured with the correct country code. For more information, see Countries and Regulations chapter in *Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide*.

Procedure

- Enable the AP to discover the controller using the L2 discovery process.

Note For the discovery process, both the AP and the controller need to be in the same broadcast domain.

- Configure the AP with the controller name and IP address

  Prime the AP by using the command **capwap ap primary base** *wlc-name wlc-ip*

- Use DHCP Option 43 to initiate the discovery process.
- Use DNS A-record to let the AP discover the controller.
- Add a DNS server entry **pnpserver** in the private DNS server pointing to your Cisco Catalyst Center IP address.
- Use PnP Connect Cloud direction by using a public DNS server.

  The PnP Connect Cloud directs the AP to the Cisco Catalyst Center. From the Catalyst Center, the controller can claim and associate the AP.

Configuring Wireless Controller

Configuring 6-GHz Radio Profile

This procedure enables the 6-GHz radio DCA channels in the controller.

Note The CW9163E AP's 6-GHz radio is enabled for use in AFC approved countries only.

Procedure

Step 1 Log in to the Catalyst 9800 controller.

Step 2 Choose **Configuration** > **Tags & Profiles** > **RF/Radio**.

The **RF/Radio** page is displayed.

Step 3 In the **RF** tab, click **default-rf-profile-6ghz**.

The **Edit RF Profile** window is displayed.

Step 4 Click **RRM** > **DCA** tab.

Step 5 Ensure all the DCA Channels are enabled.

Step 6 Click **Update & Apply to Device**.

Configuring 6-GHz OFDMA

This procedure enables the 6-GHz radio OFDMA in the controller.

Procedure

Step 1 Log in to the Catalyst 9800 controller.

Step 2 Choose **Configuration** > **Radio Configurations** > **High Throughput** > **5 GHz Band** > **11ax**.

Step 3 Check **Enable 11ax** check box.

Step 4 Check the check boxes for the desired MCS/(data rate), or to select all of them, check the **Select All** check box.

Step 5 Choose **Configuration** > **Radio Configurations** > **High Throughput** > **6 GHz Band**.

Step 6 Check the check boxes for the desired MCS/(data rate), or to select all of them, check the **Select All** check box.

Step 7 Click **Update & Apply to Device**.

Configuring WPA3 Security

The Wi-Fi 6E radio protocol requires WPA3 security for the 6-GHz band. WPA3 is not backward compatible, even when the WPA3 Transition mode is enabled.

You have three options when creating a WLAN.

- All-In: You must reconfigure all the WLANs to WPA3 only.
- Multiple SSID: Reconfigure SSIDs by adding SSID/WLAN with specific security settings.

For more information, see *WPA3 Deployment Guide* at the following URL:

https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/wpa3-dep-guide-og.html

Procedure

Step 1 Log in to the Cisco Catalyst 9800 Controller.

Step 2 Choose **Configuration** > **Tags & Profiles** > **WLANs**

Perform either of the the following steps as applicable:

- To create a new WLAN for the 6-GHz radio, click **Add** and enter the profile and SSID names.
- You can choose from an existing WLAN.

  The **Edit WLAN** window is displayed

Step 3 Select the type of security protocol for the WLAN.

Enable one of the following security protocol:

- Configuring the WPA3 security protocol.
  - **a.** Choose **Security** > **Layer2** tab.
  - **b.** Select the **WPA3** tab.
  - **c.** Check one of the Auth Key Mgmt check boxes.
    - OWE
    - SAE
    - 802.1X-SHA256
  - **d.** Enable Protected Management Frame (PMF)

    Select the PMF state from **Required** or **Optional** from the drop-down list.
- Configuring WPA2 + WPA3 security protocol.
  - **a.** Choose **Security** > **Layer2** tab.
  - **b.** Select the **WPA2 + WPA3** tab.
  - **c.** Check one of the Auth Key Mgmt check boxes.

- 802.1x
- 802.1x-SHA256

Step 4 In the **Advanced** tab, to enable 802.11ax features, Check all feature check boxes under the **11ax** section.

Step 5 Save the settings.

Configuring Policy Tag

Procedure

Step 1 Log in to the Cisco Catalyst 9800 Controller.

Step 2 Choose **Configuration** > **Tags & Profiles** > **Tags**

Step 3 Click **default-policy-tag**

The **Edit Policy Tag** window is displayed.

Step 4 Select **WLAN-POLICY**, and click **Add**.

Step 5 Choose the **WLAN profile** to map with the appropriate **Policy profile** from the drop-down list and click the tick icon.

Step 6 Click **Update & Apply to Device**.

Step 7 Choose **Monitoring** > **Wireless** > **Radio Statistics** > **6 GHz Radios** *ap-name*

Verify the 6 GHz configurations on the AP after it is associated with the controller.

Configuring Client Band Steering

The client band steering feature nudges the client to join the 6-GHz band if the client supports this band instead of joining the 2.4 or 5-GHz band.

Procedure

Step 1 Log in to the Cisco Catalyst 9800 Controller.

Step 2 Choose **Configuration** > **Tags & Profiles** > **WLANs**

Step 3 Select the WLAN

When selecting an existing WLAN, the **Edit WLAN** window is displayed. Alternatively, you may create a new WLAN if required.

Step 4 Select the **Advanced** tab.

Step 5 Check the **6 GHz Client Steering** check box.

Step 6 Click **Update & Apply to Device**.

Step 7 Choose **Configuration** > **Wireless** > **Advanced** > **6 GHz Client Steering**

Step 8 Configure the threshold values.

You can set the threshold values to meet your requirements.

Step 9 Click **Apply**.

Meraki Cloud Based Deployment

You can associate the CW9163E AP to a Meraki Cloud based deployed network.

Claiming an AP in a Dashboard

In a cloud-based deployment, the access points need to be onboarded from the common pool.

Procedure

Step 1 Initiate adding the APs

You can initiate the AP add process from either of the following ways:

- **Network-wide** > **Configure** > **Add Devices**
- **Organization** > **Configure** > **Inventory**

Step 2 Filter the APs using the **Search Inventory**

You can search for the devices or group of devices with any of the following parameters:

- MAC address
- Serial number (12–digit number)
- Network name
- Model number
- Order number (09-digit Cisco Meraki order number)
- Country code

Step 3 Click **Claim**

The devices are added to the available devices list.

Configuring Firewall for Cloud Management Access

The onboarding APs need to connect with the Cloud management to ensure that the outgoing connections on specific IP addresses and ports are open for this connection to be established.

The outbound ports and IP addresses are listed under the Dashboard's **Help** > **Firewall info** section.

The Wi-Fi 6 APs use an IP address range of 209.206.48.0/20 TCP port 443 to communicate with the Dashboard.

Note Older Wi-Fi APs use TCP port 7734 and UDP port 7351 to communicate with the Dashboard.

Associating AP with Cloud Management

All gateway APs must be assigned with routable IP addresses. The AP can acquire the IP address dynamically, or you can assign a static address.

Dynamic Assignment (Recommended)

The DHCP server should be configured to assign a static IP address for every AP MAC address. Wireless network features, such as 802.1x authentication, may rely on the AP to have a static IP address.

Static Assignment

Static IPs are assigned using the local web server on each AP. Using the following procedure, you can configure the static IP address.

1. Use a PC (laptop) and connect with the AP.

   Connect with the AP over a wired connection or wirelessly on the SSID it is broadcasting.

   When using a wired connection, connect the client machine to the AP through either a PoE switch or an Injector. If using a PoE switch, plug an Ethernet cable into the AP's Ethernet jack and the other end into a PoE switch. Then, connect the client machine over the Ethernet cable to the PoE switch. If using a PoE Injector, connect the AP to the **PoE** port of the Injector and the client machine to the **LAN** port.

Access the AP Local Page

To configure the AP, you need to access and log in to the AP's local page.

1. Using a web browser on the client machine, access the AP's built-in web server by browsing to http://my.meraki.com.

   Alternatively, browse to http://10.128.128.128.

2. Click the **Uplink Configuration** tab to Log in.

   The default login is the serial number (for example: Qxxx-xxxx-xxxx), with no password.

3. Configure the static IP address, netmask, gateway IP address, and DNS servers that this AP will use on its wired connection.

   If necessary, reconnect the AP to the LAN.

Firmware Management

We recommend you run the latest stable release on the APs. When there is an upgrade in progress, the LED blinks blue and turn solid blue or green after the upgrade is complete.

License Management

All the devices are required to have a license to associate with the Dashboard.

You can claim an order, license, or device from the Dashboard.

1. Log in to the Dashboard
2. Click **Organization** > **License Info**

   Or **Organization** > **Inventory**
3. Click **Add**
4. Enter the order number, serial number, or license key.

   You can enter multiple items, one per line.
5. Click **Next**

   The list of items added is displayed.
6. You can manually assign the licenses to the devices.

   To auto-assign the licenses, select **Accept and assign**.
7. Click **Select**.

Configuring Cloud Dashboard Deployment

Procedure

Step 1 Enabling SSIDs.

You can update network name, SSID name from the Dashboard's SSID page.

a) **Wireless** > **Configure** > **SSIDs**
b) Select **Enabled** from the drop-down list.
c) Click **Save Changes**

Step 2 Configure the Access Control List.

Navigate to **Wireless** > **Configure** > **Access Control** page.

Configure the per-SSID access control settings including association security, splash page, client addressing option settings.

Step 3 Configure the security protocols.

You can custom configure each SSID security to filter the clients associated with the SSID. You can configure PSK protocols for the SSID.

The Wi-Fi 6E radio protocol requires WPA3 security for the 6-GHz band. WPA3 is not backward compatible, even when the WPA3 Transition mode is enabled.

You have three options when creating a WLAN.

- All-In: You must reconfigure all the WLANs to WPA3 only.

- Multiple SSID: Reconfigure SSIDs by adding SSID/WLAN with specific security settings.

Step 4 Configure RF Profiles

Navigate to **Wireless** > **Radio Settings** > **Overview** tab.

You can create RF profiles to apply specific radio settings that can be applied to a wireless network.

By default, two RF profiles are defined for every network. One is for indoor APs, and one is for outdoor APs. The RF profiles are automatically assigned to an AP. You can verify the RF profile assigned to a particular AP on the **Overview** page.

Step 5 Radio band selection in an RF Profile.

An RF profile can be configured to apply all bands or selective bands to all SSIDs (with or without band steering) or selective SSIDs. In per SSID configuration, 2.4GHz, 5GHz, 6GHz tri-band or tri-band with band steering options are available.

The following are the band selection options available in the Dashboard

- Check the **2.4 GHz**checkbox to set an SSID to 2.4 GHz only.
- Check the **5 GHz** checkbox to set an SSID to 5 GHz only.
- Check the **6 GHz** checkbox to set an SSID to 6 GHz only.
- Select both **2.4 GHz** and **5 GHz** checkboxes to set an SSID to dual-band operation.
- Select all three **2.4 GHz**, **5 GHz**, and **Band steering** checkboxes to set an SSID to dual-band operation with band steering.

Step 6 Band steering configuration for all radio bands.

By default, clients associate with 2.4 GHz and 5 GHz band radio. However, using the client steering feature, the 6 GHz capable clients are nudged to associate with the 6 GHz band, depending on the settings configured.

a) Choose **Wireless** > **Configure** > **Radio Settings** > **RF Profiles**.
b) Choose **Band Selection** > **All SSIDs**.

   To enable band steering for all SSIDs on APs assigned to an RF profile.

   Note Ensure both **Enable operation on 2.4 GHz band** and **Enable operation on 5 GHz band** check boxes are checked.

c) Check **Enable band steering** check box.

   Note **Enable band steering** check box is grayed out if either 2.4 GHz or 5 GHz operation check box is unchecked.

d) Choose **Band Selection** > **Per SSID** .

   To enable band steering per SSIDs on APs assigned to an RF profile.

   Note The **Band steering** check box is grayed out if either the 2.4 GHz or 5 GHz operation check box is unchecked.

e) Save the settings.