



Onboard Devices and Services

You can onboard both live devices and model devices to CDO. Model devices are uploaded configuration files that you can view and edit using CDO.

Most live devices and services require an open HTTPS connection so that the Secure Device Connector can connect CDO to the device or service.

See [Secure Device Connector](#) for more information on the SDC and its state.

This chapter covers the following sections:

- [Onboard Meraki MX to Defense Orchestrator, on page 1](#)
- [Onboard Meraki Templates to Defense Orchestrator, on page 3](#)
- [Update Meraki MX Connection Credentials, on page 5](#)
- [Delete a Device from CDO, on page 5](#)

Onboard Meraki MX to Defense Orchestrator

MX devices can be managed by both Cisco Defense Orchestrator (CDO) and the Meraki dashboard. CDO deploys configuration changes to the Meraki dashboard, which in turn deploys the configuration securely to the device.

Before you begin

- Review [Connect Cisco Defense Orchestrator to your Managed Devices](#)
- Review [How Does CDO Communicate With Meraki](#)
- You must first register the Meraki MX in the Meraki dashboard. Without having access to the Meraki dashboard, your organization will not be recognized by the Meraki cloud and you will not be able to generate an API token to onboard your device.
- CDO silently converts invalid CIDR prefix notation IP addresses and IP address ranges to valid form by zeroing all bits associated with the host.
- Onboarding Meraki MX devices or templates no longer requires a connection through a Secure Device Connector (SDC). If you have some Meraki MX devices that have already been onboarded and connect to CDO using an SDC, that connection will continue to work unless you remove and re-onboard the device or [Update Meraki MX Connection Credentials](#).

- MX devices do not have to be connected to the Meraki Cloud in order to be managed by CDO. If a MX device has *never* connected to the cloud, the device connectivity is listed as **unreachable**. This is normal, and does not affect your ability to manage or deploy policies to this device.

Procedure

| | Command or Action | Purpose |
|---------------|--|---------|
| Step 1 | When you onboard a Meraki MX device, you must generate a Meraki API key. The key authenticates the dashboard and allows you to securely onboard a device. See Generate and Retrieve Meraki API Key . | |
| Step 2 | Onboard a Meraki Device to CDO using the API key. | |

Generate and Retrieve Meraki API Key

Use this procedure to enable CDO access to the Meraki dashboard with API access:

Before you begin

Review the notes and prerequisites on [Onboard Meraki MX to Defense Orchestrator, on page 1](#)

-
- Step 1** Log into the Meraki dashboard.
- Step 2** In the navigation panel, click **Organization > Settings**.
- Step 3** Under **Dashboard API Access**, check **Enable access to the Cisco Meraki Dashboard API**. Without this option, you cannot generate API keys to onboard MX devices to CDO.
- Step 4** Click **Save changes**.
- Step 5** On the Meraki dashboard, click on your **username** in the upper right corner of the screen and then click **My Profile**.
- Step 6** Locate the API access header and click **Generate new API key**. Copy this API key. We recommend temporarily pasting it into a note until you are ready to use it. If you close the copy source before you paste the API key, you lose the copied API key.

Note You only need one API key per device. You can re-onboard a Meraki device without generating a new key.

What to do next


Continue to [Onboard an MX Device to CDO](#).

Onboard an MX Device to CDO

Use this procedure to onboard a Cisco Meraki device:

Before you begin

[Generate and Retrieve Meraki API Key, on page 2](#).

-
- Step 1** In the navigation pane, click **Inventory**
- Step 2** Click the blue plus button  and click the **Meraki** tile.
- Step 3** Select the [Secure Device Connector](#) that this device will communicate with. The default SDC is displayed but you can change it by clicking the blue **Change** link.
- Step 4** Paste the API access key you copied. If the key is incomplete or incorrect, you will not be able to onboard the device. Click **Connect**.
- Step 5** Use the drop-down menu to select the correct Organization. The generated list of organizations are retrieved from the Meraki dashboard and includes devices and templates. Select the desired device and click **Select**.
- Step 6** Use the drop-down menu to select the correct Network. The generated list of networks are retrieved from the Meraki network. Click **Select**.
- Step 7** Optionally, you can add unique Labels for the device. You can later filter your list of devices by this label.
- Step 8** Click **Continue**. The device begins the onboarding process. Once completed, CDO redirects you to **Inventory**.
-

Related Information

- [Meraki MX Templates](#)
- [Onboard an Meraki Template to CDO, on page 4](#)
- [How Does CDO Communicate With Meraki](#)
- [Manage the Meraki Access Control Policy](#)
- [Create or Edit a Meraki Network Object or Network Group](#)
- [Create or Edit a Meraki Service Object or Service Group](#)

Onboard Meraki Templates to Defense Orchestrator

Meraki Templates are an excellent way to manage multiple locations or networks with a single policy. Meraki templates can be managed by both Cisco Defense Orchestrator (CDO) and the Meraki dashboard. Note that CDO deploys configuration changes to the Meraki dashboard, which in turn deploys the configuration securely to the template. See [How Does CDO Communicate With Meraki](#) for more information.



Note To onboard a template to CDO, you must first create a template in the Meraki dashboard. Without having access to the Meraki dashboard, your organization will not be recognized by the Meraki cloud and you will not be able to generate an API token to onboard your device. In the Meraki dashboard, click **Organization** > **Configuration templates** and read [Managing Multiple Networks with Configuration Templates](#) for more information.

Onboarding a Meraki template requires three steps:

-
- Step 1** Create a template network in the Meraki dashboard. See [Meraki Templates Best Practices](#) for more information.

- Step 2** [Generate and Retrieve Meraki API Key](#). When you onboard a Meraki template, you must generate a Meraki API key. The key authenticates the dashboard and allows you to securely onboard a device.
- Step 3** [Onboard an Meraki Template to CDO](#).
-

Generate and Retrieve Meraki API Key


Use this procedure to enable CDO access to the Meraki dashboard with API access:

- Step 1** Log into the Meraki dashboard.
- Step 2** In the navigation panel click **Organization > Settings**.
- Step 3** Under **Dashboard API Access**, check **Enable access to the Cisco Meraki Dashboard API**. Without this option, you cannot generate API keys to onboard MX devices to CDO.
- Step 4** Click **Save changes**.
- Step 5** On the Meraki dashboard, click on your **username** in the upper right corner of the screen and then click **My Profile**.
- Step 6** Locate the API access header and click **Generate new API key**. Copy this API key. We recommend temporarily pasting it into a note until you are ready to use it. If you close the copy source before you paste the API key, you lose the copied API key.

Note You only need one API key per template. You can re-onboard a template without generating a new key.

Onboard an Meraki Template to CDO

Use the following procedure to onboard a Meraki template:

- Step 1** In the navigation pane, click **Inventory** and click the blue plus button  and click **Connect to Cisco Meraki**.
- Step 2** Paste the API access key you copied. If the key is incomplete or incorrect, you will not be able to onboard the device. Click **Connect**.
- Step 3** Use the drop-down menu to select the template name as ab **Organization**. The generated list of organizations are retrieved from the Meraki dashboard and includes devices and templates. Select the desired template and click **Select**.
- Step 4** Optionally, you can add unique Labels for the device. You can later filter your list of devices by this label.
- Step 5** Click **Continue**. The device beings the onboarding process. Once completed, CDO redirects you to **Inventory**. Once the template is synched to CDO, the **Inventory** page displays the names of the devices associated with the template and the **Device Details** window of displays the number of networks bound to the template.
-

Related Information

- [How Does CDO Communicate With Meraki](#)
- [Manage the Meraki Access Control Policy](#)
- [Objects Associated with Meraki Devices](#)

- [Create or Edit a Meraki Network Object or Network Group](#)
- [Create or Edit a Meraki Service Object or Service Group](#)
- [Onboard Meraki MX to Defense Orchestrator](#)

Update Meraki MX Connection Credentials

If you generate a new API key from the Meraki dashboard, you must update the connection credentials in CDO. To generate a new key, see [Generate and Retrieve Meraki API Key, on page 2](#) for more information. CDO does not allow you to update the connection credentials for the device itself; if necessary, you can manually refresh the API key in the Meraki dashboard. You must manually update the API key in the CDO UI to update the credentials and re-establish communication.



Note If CDO fails to sync the device, the connectivity status in CDO may show "Invalid Credentials." If that's the case, you may have tried to use an API key. Confirm the API key for the selected Meraki MX is correct.

Use the following procedure to update the credentials for a Meraki MX device:

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab and then click the **Meraki** tab.
- Step 3** Select the Meraki MX whose connection credentials you want to update.
- Step 4** In the **Device Actions** pane, click **Update Credentials**.
- Step 5** Enter the **API key** CDO uses to log into the device and click **Update**. Unless it was changed, this API key is the same credential you used to onboard the Meraki MX. You do not have to deploy these changes to the device.

Delete a Device from CDO

Use the following procedure to delete a device from CDO:

- Step 1** Log into CDO.
- Step 2** Navigate to the **Inventory** page.
- Step 3** Locate the device you want to delete and check the device in the device row to select it.
- Step 4** In the Device Actions panel located to the right, select **Remove**.
- Step 5** When prompted, select **OK** to confirm the removal of the selected device. Select **Cancel** to keep the device onboarded.

