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 a Cisco IOS Device

You can onboard a live Cisco device running Cisco IOS (Internetwork Operating System).

Onboard a Cisco IOS Device

Before you begin

Before you begin, make sure you have met these prerequisites:

- Ensure that the ciphers your Cisco IOS server supports are supported by CDO. At this time, CDO supports a limited set of ciphers for onboarding Cisco IOS devices. The supported ciphers are: `aes128-ctr`, `aes192-ctr, aes256-ctr, aes128-gcm, aes128-gcm@openssh.com, aes256-gcm, aes256-gcm@openssh.com`. To determine the ciphers your server supports, log in to your SDC and run this command: `ssh -vv <ip_address>`.

- You must have an active on-premises Secure Device Connector (SDC) in your network to onboard a Cisco IOS device. See Secure Device Connector for a discussionof SDCs and links to deployment scenarios.

Step 1 From the CDO Navigation Bar, click **Inventory**.

Step 2 Click the blue plus button to begin onboarding the device.

Step 3   Click the **Integrations** tile. If it is grayed-out, it means you do not have an active Secure Device Connector deployed in your network and used by your CDO tenant.

Step 4   Click the Secure Device Connector button and select the SDC in your network that this device will communicate with. The default SDC is displayed but you can change it by clicking the SDC name.

Step 5   Give the device a name.

Step 6   In the Integrations drop-down menu, select **IOS**.

Step 7   Enter the location (IP address, fully qualified domain name, or hostname) of the device. The default connection port is 22.

Step 8   Click **Go**.

Step 9   (Optional) At the Create Integration page, you have an opportunity to download and review the SSH fingerprint.

Step 10   Enter the device's administrator name and password.

         Note   CDO does not support connections using public key authentication at this time.

Step 11   If you have set an enable password on the device, enter that in the **EnablePassword** field.

Step 12   Click **Connect**.

Step 13   (Optional) Enter a label for the device. See Labels and Label Groups for more information.

Step 14   Click **Continue**.

Step 15   Onboard another IOS device or click **Finish**.

Step 16   Return to the **Inventory** page. After the device has been successfully onboarded, you will see that the Configuration Status is "Synced" and the Connectivity state is "Online."

Step 17   (Optional) If you want you can write a note about the device by typing it in the device's Notes pate. See Device Notes for more information.

Create and Import an ASR or ISR Model

A Cisco IOS model is a copy of the running configuration file of a Cisco IOS device that you have onboarded to CDO. You can download the Cisco IOS device configuration to a text file and import it as an IOS model to another tenant that you manage.

Download ASR or ISR Configuration

Step 1   In the navigation bar, click **Inventory**.

Step 2   Click the **Devices** tab.

Step 3   Click the **IOS** tab and select a device.

Step 4   In the **Management** on the left pane, click **Configuration**.

Step 5   Click **Download** to download the device configuration to your local computer.

Import ASR or ISR Configuration

Step 1   Navigate to the **Inventory** page.

Step 2   Click the blue plus ( ) button to import the configuration.

Step 3 Click on **Import a config file without a device**.

Step 4 Select the **Device Type** as **ASR** or **ISR**.

Step 5 Click **Browse** and select the configuration file (text format) to upload.

Step 6 Once the configuration is verified, you're prompted to label the device or service. See Labels and Label Groups for more information.

Step 7 After labeling your model device, you can view it in the **Inventory** list.

> **Note** Depending on the size of the configuration and the number of other devices or services, it may take some time for the configuration to be analyzed.

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.

Import Configuration for Offline Device Management

Importing a device's configuration for offline management allows you to review and optimize a device's configuration without having to work on a live device in your network. CDO also refers to these uploaded configuration files as "models."

You can import the configurations of these devices to CDO:

- Cisco IOS devices like the Aggregation Services Routers (ASR) and Integrated Services Routers (ISRs). See Create and Import an ASR or ISR Model.

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.