



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.

This chapter covers the following sections:

- [Onboard an On-Prem Management Center to CDO, on page 1](#)
- [Remove an On-Prem Firewall Management Center from CDO, on page 7](#)

Onboard an On-Prem Management Center to CDO

CDO provides the following methods to onboard on-prem management centers:

- (Recommended) [Auto-Onboard an On-Prem Management Center Integrated with Cisco Security Cloud](#)
- [Onboard an On-Prem Firewall Management Center to CDO with Credentials](#)

Review [Connect CDO to your Managed Devices](#) for more information.



Note CDO complements FMC by allowing you to:

- Drive consistent policy through shared object management with FMCs.

For more information, see the **Objects** section on [Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator](#).

- Enable zero-touch provisioning of Threat Defense devices.

For more information, see [Onboard a Device to On-Prem Management Center with Zero-Touch Provisioning](#).

- Get a centralised view of **Inventory**.

For more information, see [Device and Service Management](#).

- Leverage cloud CSDC and cdFMC.

For more information, see [Cisco Secure Dynamic Attributes Connector](#).

Limitations and Guidelines

These are the limitations applicable to onboarding an on-prem management center:

- Onboarding an on-prem management center also onboards all of the devices registered to the on-prem management center. Be aware that if a managed device is disabled, or unreachable, CDO may display the device in the **Inventory** page, but cannot successfully send requests or view device information.
- We recommend creating a new user on the on-prem management center specifically for CDO communication that has administrator-level permissions. If you onboard an on-prem management center and then simultaneously log into that on-prem management center with the same login credentials, onboarding fails.
- If you create a new user on the on-prem management center for CDO communication, the **Maximum Number of Failed Logins** for the user configuration must be set to "0".
- For On-Prem Management Centers running version 7.4 and older, if you experience a switchover and the FMC is no longer connected to the cloud, try disabling SecureX and then re-enabling it.

Auto-Onboard an On-Prem Management Center Integrated with Cisco Security Cloud

The auto-discovery and onboarding feature is enabled by default in CDO, so you can expect all on-prem management centers that are running Version 7.2 or later and integrated with Cisco Security Cloud are automatically discovered and onboarded to CDO. Additionally, the associated threat defense devices are onboarded to CDO.

CDO also onboards the on-prem management center high availability (HA) pair.

Before you begin

Ensure that the following prerequisites are met:

- Allow outbound traffic from port 443 on the on-prem management center.

-
- Step 1** Integrate the on-prem management center you want to onboard with Cisco Security Cloud and register it with a CDO tenant. See [Integrate On-Prem Management Center With Cisco Security Cloud, on page 2](#).
- Step 2** Log in to the CDO tenant that was registered with the on-prem management center.
- Step 3** In the left pane, choose **Tools & Services > Firewall Management Center**.
- All on-prem management centers associated with your tenant is displayed in the **FMC** tab. See [View Onboarded On-Prem Firewall Management Center](#).
-

Integrate On-Prem Management Center With Cisco Security Cloud

This procedure describes how to integrate the on-prem management center with Cisco Security Cloud. By enabling Cisco Security Cloud integration, your management center gets registered to the Cisco cloud tenancy.

Before you begin

- CDO uses Cisco security cloud sign on as its identity provider and Duo for multifactor authentication. Ensure that you have your Cisco security cloud sign on credentials and can sign in to the Cisco regional cloud where your account was created.
- A CDO tenant is required to integrate the on-prem management center with Cisco Security Cloud. If you do not already have a CDO tenant, request one. See [Create a CDO Tenant](#) for more information.

Step 1 In your on-prem management center, perform the following:

- For on-prem management center version between 7.2 and 7.4.x, go to **Integration > SecureX**.
- For on-prem management center version 7.6 or later, go to **Integration > .**

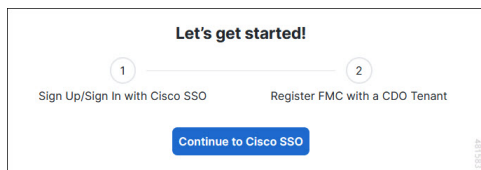
Step 2 For on-prem management center version between 7.2 and 7.4.x, click **Enable Secure X**.

For on-prem management center version 7.6 or later, click **Cisco Security Cloud**.

A separate browser tab opens to log you in to your CDO account. Make sure this page is not blocked by a pop-up blocker.

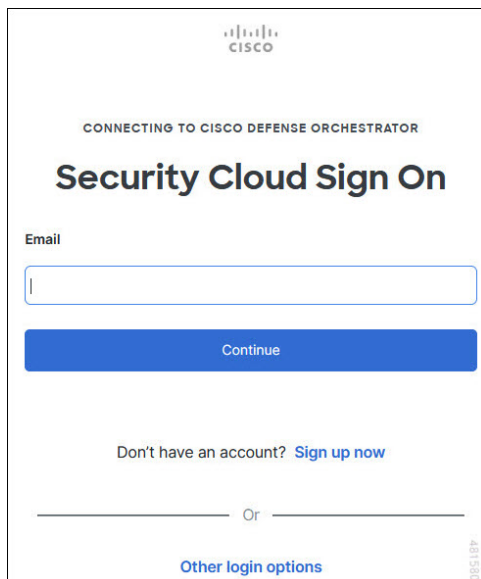
Step 3 Click **Continue to Cisco SSO**.

Figure 1: Cisco Security Cloud Welcome Page



Step 4 Log in to your CDO account.

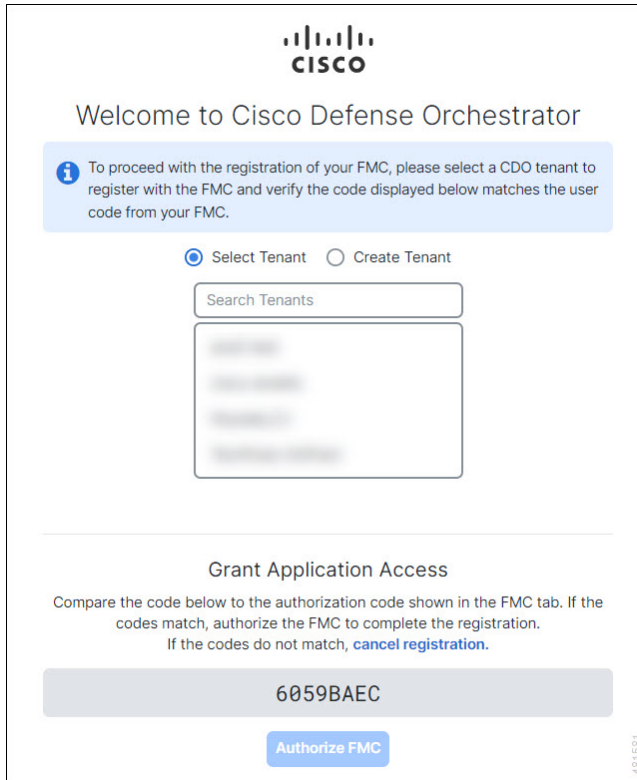
Figure 2: Cisco Security Cloud Sign On



If you do not have a security cloud sign on account to log in to CDO and you want to create one, click **Sign up now** in the **Security Cloud Sign On** page. See [Create a New Cisco Security Cloud Sign On Account](#).

- Step 5** Choose a CDO tenant that you want to use for this integration. The on-prem management center and the managed devices get onboarded to the CDO tenant that you choose here.

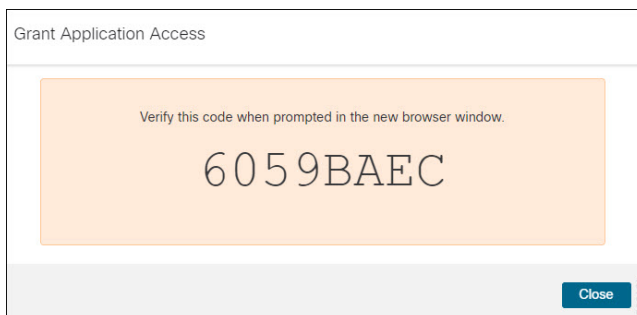
Figure 3: Choose the CDO Tenant



If you do not already have a CDO tenant or if you want to use a new tenant for this integration, create a new tenant. See [Create a CDO Tenant](#) for more information.

- Step 6** Verify that the code displayed in the CDO login page matches the code provided by the on-prem management center.

Figure 4: Verification Code in the on-prem management center



- Step 7** Click **Authorize FMC**.

- Step 8** In the on-prem management center UI, click **Save** to save the configuration.

You can view the task progress under **Notifications > Tasks**.

The registration task can take up to 90 second to complete. If you must use on-prem management center while the registration task is in progress, open the on-prem management center in a new window.

Disable Auto-Onboarding of an On-Prem Management Center

Disabling the auto-onboarding of the on-prem management centers functionality prevents auto onboarding of new on-prem management centers from your Cisco Security Cloud to this CDO tenant.

Only a Super Admin or Admin user on CDO can enable or disable this functionality.

- Step 1** In the left pane, choose **Settings > General Settings**.
- Step 2** In the **General Settings** screen, click the **Auto onboard On-Prem FMCs with Cisco Security Cloud** toggle button to disable the auto onboarding of on-prem management center functionality.
- Step 3** Click **Confirm**.

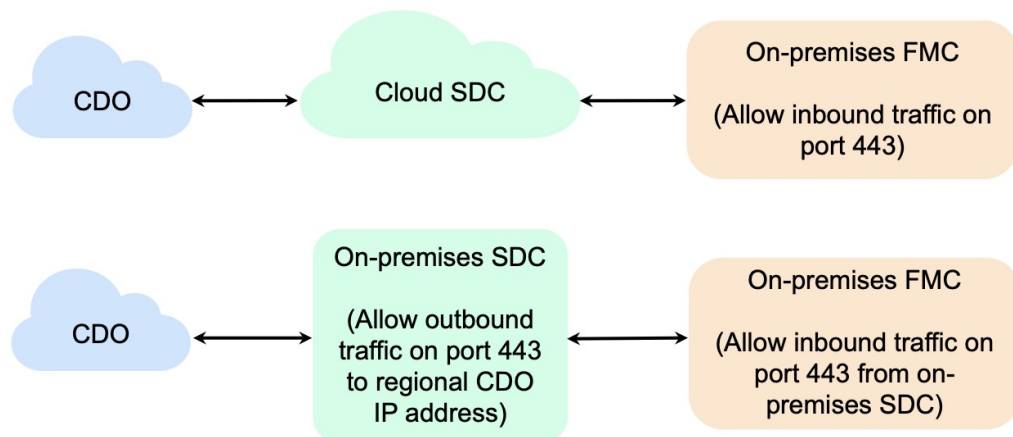
Onboard an On-Prem Firewall Management Center to CDO with Credentials

To onboard an On-Prem Firewall Management Center to CDO with credentials, follow this procedure:

Before you begin

Make sure you allow proper port access on your on-prem management center:

- Allow inbound connectivity on port 443 if you are onboarding the on-premises FMC using an on-premises Secure Device Connector.
- Allow outbound connectivity on port 443 if you are onboarding the FMC using the Cloud Connector.



- Step 1** In the left pane, click **Tools & Services > Firewall Management Center**.


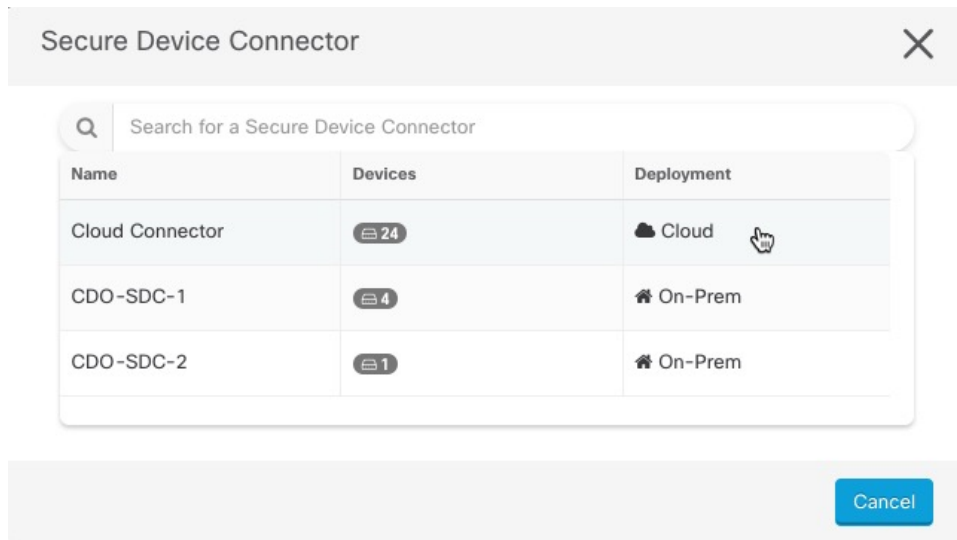
- Step 2** Click  to onboard an On-Prem Firewall Management Center.
- Step 3** Click **Firewall Management Center**.
- Step 4** Select the **Use Credentials** card.
- Step 5** Click the **Secure Device Connector** button and select an SDC installed in your network. If you would rather not use an SDC, CDO can connect to your On-Prem Management Center using the Cloud Connector. Your choice depends on how you [connect CDO to your managed devices](#).

Figure 5: Choose a Secure Device Connector



- Step 6** Enter the device name and location. Click **Next**.
- Step 7** Enter the **Username** and **Password** of the account credentials you want to use to access the On-Prem Management Center. Click **Next**.
- Step 8** The device is onboarded. From here you can opt to add labels to your On-Prem Management Center, or click **Go to Services** to view the page of onboarded devices. If healthy, the FMC is displayed with a **Synced** status.

Note Note that the devices managed by the On-Prem Management Center are automatically named as "`<fmcname>_<manageddevicename>`".

Redirect CDO to an On-Prem Firewall Management Center

After you have onboarded an On-Prem Management Center to CDO, you must update the management interface's hostname in the On-Prem Management Center UI to contain the FQDN. If you do not, you cannot cross-launch from CDO.

Use the following procedure to update the management interface hostname and redirect from CDO to the On-Prem Management Center:

- Step 1** Log into the On-Prem Management Center UI.
- Step 2** Navigate to **System > Configuration**.

- Step 3** Select the **Management Interfaces** tab.
- Step 4** Expand the **Shared Settings** header and click the edit icon.
- Step 5** Locate the **Hostname** field and enter the FMC's FQDN.
- Step 6** Save changes.

Note: You may have to log out of CDO before you can click **Manage Devices in Firepower Management Center** and cross-launch to the On-Prem Management Center UI.

Remove an On-Prem Firewall Management Center from CDO

If you choose to remove an on-prem management center from CDO, all devices by that on-prem management center will also be removed.

Before you begin

Disable the auto-onboarding option to remove one or more on-prem management centers onboarded using auto-onboarding functionality.

1. In the left pane, choose **Settings > General Settings**.
2. In the **Tenant Settings** section, disable **Auto onboard On-Prem FMCs integrated to Cisco Security Cloud**.

-
- Step 1** In the left pane, click **Tools & Services > Firewall Management Center**.
- Step 2** Ensure the **FMC** tab is selected and choose the on-prem management center you want to remove.
- Step 3** In the **Device Actions** pane located to the right, click **Remove On-Prem FMC and its managed devices**.
- Step 4** Click **OK** to confirm that you want to remove the on-prem management center and its managed devices from your tenant.
- Step 5** Refresh your browser to see an updated list of available devices.
-

