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 an On-Prem Management Center

Review Connect Cisco Defense Orchestrator to your Managed Devices for more information.

Note CDO does not support creating or modifying objects or policies associated with the On-Prem Management Center or the devices registered to the On-Prem Management Center. You must make these changes in the On-Prem Management Center UI.

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".

Network Requirements

Before you onboard a device, ensure the following ports have external access. If communication ports are blocked behind a firewall, onboarding the device may fail.

Port	Protocol/Feature	Platforms	Direction	Details
7/UDP	UDP/audit logging	FMC	Outbound	Verify connectivity with the syslog server when configuring audit logging.
25/tcp	SMTP	FMC	Outbound	Send email notices and alerts.
53/tcp 53/udp	DNS	FMC	Outbound	DNS
67/udp 68/udp	DHCP	FMC	Outbound	DHCP
80/tcp	HTTP	FMC	Outbound	Display RSS feeds in the dashboard.
80/tcp	HTTP	FMC	Outbound	Download or query URL category and reputation data (port 443 also required).
80/tcp	HTTP	FMC	Outbound	Download custom Security Intelligence feeds over HTTP.
123/udp	NTP	FMC	Outbound	Synchronize time.
162/udp	SNMP	FMC	Outbound	Send SNMP alerts to a remote trap server.
389/tcp 636/tcp	LDAP	FMC	Outbound	Communicate with an LDAP server for external authentication. Obtain metadata for detected LDAP users (FMC only). Configurable.
443/tcp	HTTPS	FMC	Inbound	Allow inbound connection to port 443 if you are onboarding the FMC with an on-premises Secure Device Connector.
443/tcp	HTPS	FMC	Outbound	Allow outbound traffic from port 443 if onboarding the FMC to CDO using the cloud connector.
443/tcp	HTPS	FMC	Outbound	Allow outbound connection for port 443 if onboarding the FMC using SecureX.

Port	Protocol/Feature	Platforms	Direction	Details
443/tcp	HTTPS	FMC	Outbound	Send and receive data from the internet.
443	HTTPS	FMC	Outbound	Communicate with the AMP cloud (public or private)
514/udp	Syslog (alerts)	FMC	Outbound	Send alerts to a remote syslog server.
1812/udp 1813/udp	RADIUS	FMC	Outbound	Communicate with a RADIUS server for external authentication and accounting. Configurable.
5222/tcp	ISE	FMC	Outbound	Communicate with an ISE identity source.
6514/tcp	Syslog (audit events)	FMC	Outbound	Send audit logs to a remote syslog server, when TLS is configured.
8305/tcp	Appliance communications	FMC	Both	Securely communicate between appliances in a deployment. Configurable. If you change this port, you must change it for *all* appliances in the deployment. We recommend you keep the default.
8989/tcp	Cisco Success Network	FMC	Outbound	Transmit usage information and statistics.

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

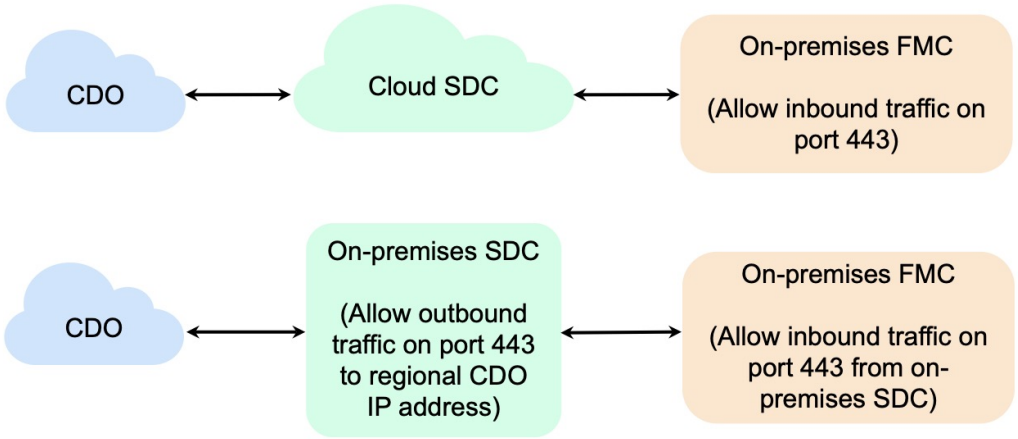
To onboard an On-Prem Firewall Management Center to CDO with credentials, follow this procedure:

Before you begin

Review Onboard an On-Prem Management Center, on page 1.

Make sure you allow proper port access on your on-premises Firewall 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 From the CDO navigation bar, click **Tools & Services** > **Firewall Management Center**.

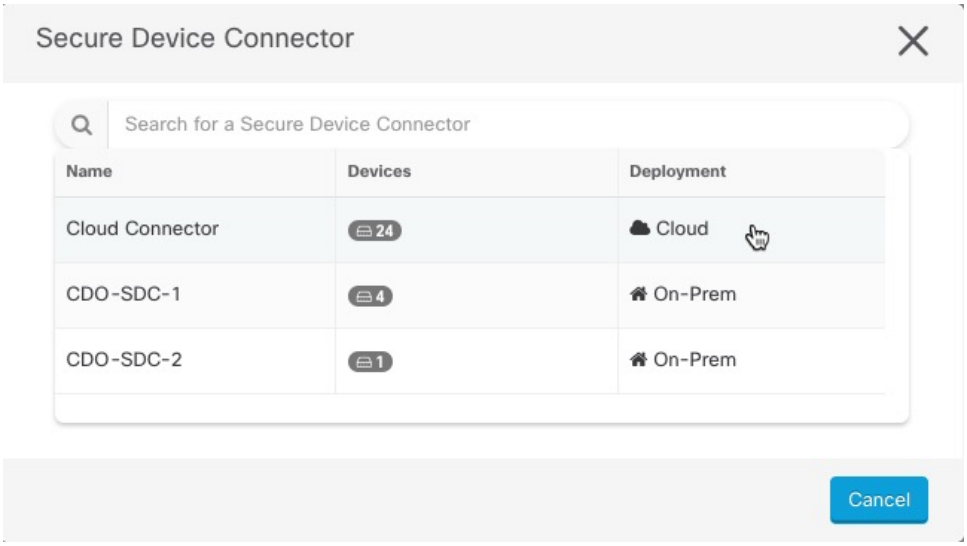
Step 2 Click + to onboard an On-Prem Firewall Management Center.

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 1: 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>*."

About Auto-Onboarding an On-Prem Firewall Management Center to CDO

As a Super Admin or Admin user on CDO, you can use the platform's auto-onboarding of on-prem management centers functionality. This feature automatically initiates the onboarding process for all on-prem management centers that are running Version 7.2 or later and are linked to your SecureX tenant or registered to the Cisco Security Cloud. Additionally, it also onboards the threat defense devices that are connected to those on-prem management centers.

This feature is enabled by default in CDO, so you can expect all on-prem management centers and threat defense devices to be automatically onboarded, which can significantly enhance efficiency. CDO polls SecureX for new on-prem management centers every hour. It onboards the active on-prem management center high availability (HA) pair.

Note that a new CDO tenant also comes with this feature enabled by default. This feature holds good for you if you have an on-prem management center running Version 7.2 and later and if you fit into one of the following categories:

- Register your on-prem management center through SecureX for the first time and you do not have a CDO tenant
- Auto-onboard an already registered on-prem management center to a new CDO tenant
- Auto-onboard an already registered on-prem management center to an existing CDO tenant

Register your on-prem management center through SecureX for the first time and you do not have a CDO tenant

If you have an on-prem management center that is not registered through SecureX, you can register it to the Cisco Security Cloud through CDO. See Cisco Secure Firewall Management Center (Version 7.2 and later) and SecureX Integration Guide for instructions on how to do this. If you do not have a CDO account already, you will be prompted to create one for yourself during the registration process, which your on-prem management center then uses to connect to the Cisco Security Cloud.

Auto-onboard an already registered on-prem management center to a new CDO tenant

If you have an on-prem management center that is already registered through SecureX and when you create a new CDO tenant, because CDO comes with the auto-onboarding of on-prem management centers feature enabled by default, you can expect your on-prem management center to get onboarded to CDO right away. See Create a CDO Tenant for more information.

Auto-onboard an already registered on-prem management center to an existing CDO tenant

If you already have a CDO tenant and an on-prem management center registered with SecureX, and you want to onboard your on-prem management center to CDO for the first time, enable the **Auto onboard On-Prem FMCs using SecureX tenant** toggle.

If you do not see your on-prem management center getting onboarded even after enabling the toggle, make sure again that your CDO and SecureX or Cisco XDR tenant accounts are merged. See Merge Accounts for

instructions. After merging, log out and log in back to your CDO tenant and try disabling and enabling the **Auto onboard On-Prem FMCs using SecureX tenant** toggle.

Auto-Onboard an On-Prem Firewall Management Center with SecureX

Before you begin

Ensure that the following requirements are met:

- The on-prem management center must be running at least Version 7.2.
- SecureX must be enabled on the on-prem management center. See Cisco Secure Firewall Management Center (Version 7.2 and later) and SecureX Integration Guide for steps and more information.
- You must allow outbound traffic from port 443 on the on-prem management center.
- The on-prem management center must have a configured module.
- Merge your CDO tenant and SecureX/CTR or Cisco XDR account prior to onboarding your device. See Merge Accounts for instructions.
- After merging your CDO tenant and SecureX/CTR or Cisco XDR, ensure that you log out of your CDO tenant and log in again.

Step 1 Click **Tools & Services** > **Firewall Management Center** > + and choose **FMC**.

Step 2 Click **Discover From SecureX Account** as the method.

The **Auto onboard On-Prem FMCs using SecureX** feature is enabled by default. You can go to **Tools & Services** > **Firewall Management Center** to see the newly onboarded on-prem management centers associated with the SecureX tenant linked to your CDO tenant.

Step 3 You can click the available link to disable this functionality.

Step 4 In the **General Settings** screen, navigate to the **Tenant Settings** section, and disable **Auto onboard On-Prem FMCs using SecureX tenant**.

Note When you disable this functionality, CDO stops further onboarding of the on-prem management center associated with the SecureX tenant. It doesn't remove the already onboarded on-prem management centers. You must manually remove them after disabling the functionality.

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 opt to remove an on-prem management center from CDO, you are also choosing to remove all of the devices managed from CDO. Note that this does **not** remove the on-prem management center from SecureX.

Use the following procedure to remove an on-prem management center and it's registered devices from CDO:

Step 1 In the navigation 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.