Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator

Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator

About On-Prem Firewall Management Center

On-Prem Management Center support is limited to onboarding, viewing its managed devices, viewing, managing network objects and cross-launching to On-Prem Management Center UI to manage associated devices and objects. Additional features will be supported soon. For functionality that may not be supported by CDO at this time, you must use the On-Prem Management Center console. See the Cisco Secure Firewall Management Center Configuration Guide of the version your system is running, to know more about the features provided by On-Prem Management Center.

The On-Prem Management Center is a centralized management console with graphical user interface that you can use to perform administrative, management, analysis, and reporting tasks. It is a management console that is comparable, but not identical, to ASDM and FDM. For a list of On-Prem Management Center devices and software versions that CDO supports, see Software and Hardware support by CDO.

Version Support

CDO supports version 6.4 and later. An On-Prem Management Center can manage older devices, usually a few major versions back. For example, devices running version 6.6.0 can manage a Version 6.4.0 device. If an On-Prem Management Center manages a device that is running a version earlier than 6.4, the device may be displayed in the **Inventory** page, but cannot be deployed to or its policies modified from CDO. You must make changes and deploy from the On-Prem Management Center UI.

Note 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.

Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator

How does CDO Communicate with an FMC

CDO acts as a REST API client to send requests to the On-Prem Management Center, and the On-Prem Management Center then uses its designated client to channel the requests to its managed devices. Because the device does not allow multiple logins with the same login credentials, we recommend creating a new user on the On-Prem Management Center specifically for CDO communication that has administrator-level permissions. This new user will have to be replicated on CDO, as either a CDO-provided Administrator or a custom user role with **system** and **devices** permission. Without an admin login, CDO will not be able to successfully use REST API commands to modify or create policy, rules, or objects.

Onboard or Remove an On-Prem Management Center

You can onboard or remove an On-Prem Management Center at any time. The On-Prem Management Center and its registered device must be running at least Version 6.4 to be read by CDO. To onboard an On-Prem Management Center and its registered devices, see Onboard an FMC.

Once an On-Prem Management Center is onboarded, selecting the On-Prem Management Center from the **Services** page, clicking **Devices** under **Management** or any actions on the right pane opens up the **Verify FMC Cross Launch URL** wizard, which lets you enter the public IP address or the FQDN and the port number of your management center. Clicking **Continue** cross-launches to the selected On-Prem Management Center web UI in a new tab using the IP address you entered. You can also add external links manually in the **Add External Links** option under **External Links** on the right pane.

Removing an On-Prem Management Center from your CDO tenant also removes the devices registered to that On-Prem Management Center. See Remove an FMC from CDO for more information. If an On-Prem Management Center experiences an "Invalid Credentials" status after onboarding, you can **reconnect** the appliance. See Troubleshoot Invalid Credentials for more information.

Note Devices running Firepower 6.6 do not support the **reconnect** feature. If you have to reconnect the appliance, we recommend removing the On-Prem Management Center and re-onboarding the appliance.

On-Prem Management Center High Availability Pairs

CDO does not support high availability (HA) functionality for On-Prem Management Center appliances. If a pair of On-Prem Management Center appliances are configured for HA, the pair is listed as individual appliances in the **Services** page.

Devices Managed by an On-Prem Management Center

Once you onboard an On-Prem Management Center to CDO, all of the devices registered to that On-Prem Management Center are also read into CDO. From the **Inventory** page, you can see device information such as name, IP address, type of device, software version, and the state. Note that your On-Prem Management Center is displayed on the **Services** page and the devices it manages are listed on the **Inventory** page. In the **Services** page, you can see information such as version, devices managed, type of device, and status. Clicking the devices icon on the **Services** page, which displays the number of devices your FMC manages, takes you to the **Inventory** page, with the device filter applied, so all the devices managed by the On-Prem Management Center you selected are displayed.

You can perform actions using relevant options in the **Device Actions**, **Monitoring**, **Device Management**, and **Policies** panels on the right pane in the **Inventory**. If you select a device that is currently managed by an FMC and click these options, CDO automatically launches the On-Prem Management Center console that manages the devices using the cross-launch URL you had entered. Use the filter icon to further organize the

Inventory page. From here you can opt to view all the devices managed by the onboarded On-Prem Management Center, as well as the other supported device types. In addition, you can expand or collapse devices in a cluster and select them indivdually or as a group to perform actions.

Device Health Status

CDO displays the health status of threat defense devices in the **Inventory** page, such as **Normal**, **Error**, **Warning**, and **Disabled**; you can click the status of a device to navigate to the **Health Monitoring** page that corresponds to the device in the On-Prem Management Center user interface.

Note CDO keeps automatically updating the device health status every 10 minutes; however, you can do this manually by selecting the device and clicking **Check for Changes**.

Manage Security Policies in CDO

Security policies examine network traffic with the ultimate goal of allowing the traffic to its intended destination or dropping it if a security threat is identified. You can use CDO to configure security policies on many different types of devices.

Objects

After you onboard an On-Prem Management Center to CDO, you can choose to discover objects from the On-Prem Management Center and manage them in CDO. You can do this by navigating to **Tools & Services** > **Firewall Management Center**, selecting the desired On-Prem Management Center, and clicking **Settings**. You can turn the **Discover & Manage Network Objects** toggle button on; when this option is enabled, CDO automatically reads all the objects from the On-Prem Management Center-managed devices into CDO. Once imported, the objects can be managed from CDO. Note that you need to have the super admin or admin user role to be able to use the **Settings** button.

When making a configuration change to an object from CDO, the change gets staged in CDO and you can manually push the change to the On-Prem Management Center after reviewing it from **Pending Changes**. In addition, when you make a configuration change to an object from the On-Prem Management Center user interface, CDO detects those changes as out-of-band changes that can be synchronized later. If you want your changes to be automatically synchronized with on-prem management center and not staged for review, turn the **Enable automatic sync of network objects** toggle on.

If you have existing objects in CDO that you want to assign to your On-Prem Management Center, select the On-Prem Management Center from the **Services** page and choose **Assign Objects** on the right pane. CDO displays all the existing objects and lets you select ones that you want to associate with the On-Prem Management Center that you selected. This heps promote consistency in network object definitions across platforms managed by CDO. Note that you can use the **Assign Objects** button only if **Discover & Manage Network Objects** is enabled for the selected on-prem management center.

Note

- You cannot turn the **Discover & Manage Network Objects** toggle on if the on-prem management center that you have selected has one or more child domains or has the Chanage Management workflow enabled on it..
- You cannot turn the **Enable automatic sync of network objects** toggle on if the **Discover & Manage Network Objects** toggle is turned off.

Managing On-Prem Firewall Management Center with Cisco Defense Orchestrator

On-Prem Management Center supports the following object types:

- Network Objects
- Network-Group Objects

Object Issues

CDO identifies the duplicate, inconsistent, or ununsed objects. You can filter the issues based on their issue states. However, CDO cannot resolve object issues.

Eventing

Searching and filtering the Historical and Live event tables for specific events, works the same way as it does when searching and filtering for other information in CDO. For more information, see Firepower Management Center and Cisco Security Analytics and Logging (SaaS) Integration Guide.

Cisco Security Analytics and Logging

Cisco Security Analytics and Logging allows you to capture connection, intrusion, file, malware, and Security Intelligence events from all of your devices and view them in one place in CDO.

The events are stored in the Cisco cloud and viewable from the Event Logging page in CDO where you can filter and review them to gain a clear understanding of what security rules are triggering in your network. The **Logging and Troubleshooting** package gives you these capabilities.

With the **Firewall Analytics and Monitoring** package, the system can apply Secure Cloud Analytics dynamic entity modeling to your events, and use behavioral modeling analytics to generate Secure Cloud Analytics observations and alerts. If you obtain a **Total Network Analytics and Monitoring** package, the system applies dynamic entity modeling to both your device events and your network traffic, and generates observations and alerts. You can cross-launch from CDO to a Secure Cloud Analytics portal provisioned for you, using Cisco Single Sign-On.