Managing Cisco Secure Firewall Threat Defense Devices with Cloud-delivered Firewall Management Center

The cloud-delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices and is delivered via Cisco Defense Orchestrator (CDO). The cloud-delivered Firewall Management Center offers many of the same functions as an on-premises Secure Firewall Management Center.

The cloud-delivered Firewall Management Center has the same appearance and behavior as an on-premises Secure Firewall Management Center and uses the same FMC API.

As a SaaS product, the Cisco Defense Orchestrator (CDO) operations team is responsible for deploying and maintaining cloud-delivered Firewall Management Center software. As new features are introduced, the CDO operations team updates your CDO tenant's cloud-delivered Firewall Management Center for you.

A migration wizard is available to help you migrate your Secure Firewall Threat Defense devices from your on-premises Secure Firewall Management Center to the cloud-delivered Firewall Management Center. The devices must have Threat Defense software Version 7.0.3 or a later 7.0.x release, or Version 7.2 or later installed to be migrated. Threat Defense 7.1 releases are not supported.

Onboarding Secure Firewall Threat Defense devices is carried out in CDO using familiar processes such as onboarding a device with its serial number or using a CLI command that includes a registration key. Once the device is onboarded, it is visible both in CDO and in the cloud-delivered Firewall Management Center, however, you configure the device in the cloud-delivered Firewall Management Center. In CDO, you can view device-specific information such as version, configuration status, connectivity, health status, and node status. When you click on the health status from CDO, you are taken to the respective device's health monitoring page in the cloud-delivered Firewall Management Center user interface.

CDO provides high availability support for the threat defense devices that it manages through the data interface. This feature is supported for devices running software version 7.2 or later.

You can analyze syslog events generated by your onboarded threat defense devices using Security Analytics and Logging (SaaS) or Security Analytics and Logging (On-Premises). The SaaS version stores events in the cloud and you view the events in CDO. The on-premises version stores events in an on-premises Secure Network Analytics appliance and analysis is done in the on-premises Secure Firewall Management Center. In both cases, just as with an on-premises FMC today, you can still send logs to a log collector of your choice directly from the sensors.

The license for cloud-delivered Firewall Management Center is a per-device-managed license and there is no license required for the cloud-delivered Firewall Management Center itself. Existing Secure Firewall Threat Defense devices re-use their existing smart licenses and new Secure Firewall Threat Defense devices provision new smart licenses for each feature implemented on the FTD.

Existing customers can continue to use CDO for managing other device types like, the Secure Firewall ASA, Meraki, Cisco IOS devices, Umbrella, and AWS virtual private clouds. If you use CDO to manage a Secure Firewall Threat Defense device configured for local management with Firepower Device Manager, you can continue to manage them with CDO as well.

To learn how to have a cloud-delivered Firewall Management Center provisioned on your tenant, see Enable Cloud-delivered Firewall Management Center on Your CDO Tenant, on page 3.

Learn more about the Firewall Management Center features we support in cloud-delivered Firewall Management Center

- Onboard a Secure Firewall Threat Defense device to cloud-delivered Firewall Management Center.
- Migrate Secure Firewall Threat Defense to Cloud
- Health Monitoring
- Backup/Restore
- Scheduling
- Import/Export
- Reporting and Alerting
- Transparent or Routed Firewall mode
- High Availability for Devices Managed through Management and Data Interface
- Interfaces
- Routing
- Objects and Certificates
- Network Access Control (NAT)
- Access Control policies
- Remote Access VPN and Site to Site VPN configuration
- Intrusion and Detection and Prevention policies
- Network Malware and Protection and File Policies
- Encrypted Traffic Handling
- User Identity
- Network Discovery
- FlexConfig Policies
- Advanced Network Analysis and Preprocessing

- Enable Cloud-delivered Firewall Management Center on Your CDO Tenant, on page 3

Enable Cloud-delivered Firewall Management Center on Your CDO Tenant

If you want to manage your Secure Firewall Threat Defense devices, you can enable the cloud-delivered Firewall Management Center on your tenant. You need to have an admin or a super admin user role to perform this task.

Procedure

Step 1 From the CDO menu, click **Tools & Services** > **Firewall Management Center** >  > **FMC** > **Enable Cloud-Delivered FMC**.

Step 2 CDO starts provisioning a cloud-delivered Firewall Management Center instance in the background; it typically takes 15 to 30 minutes for this to be complete. You can track the provisioning progress on the **Status** column of **Cloud-Delivered FMC**.

After the provisioning is complete, the status changes to **Active**. In addition, you get a **Cloud-delivered Firewall Management Center is Ready** notification on the CDO notifications panel and on the applications on which you have configured incoming webhooks. See Notification Settings for more information.

Note After you receive the **Cloud-delivered Firewall Management Center is Ready** notification, ensure that you log out of and log in back to your tenant once, to see the **Cloud-Delivered FMC** right pane options, such as **Actions**, **Management**, and **System**.

You can then onboard your threat defense devices to the cloud-delivered Firewall Management Center and manage them.

Hardware and Software Support

Cloud-delivered Firewall Management Center supports these Secure Firewall Threat Defense software versions when they are installed on any supported hardware or virtual device:

- Verion 7.0.3 or later 7.0.x versions.
- Version 7.2 and later versions.

Note Software Version 7.1 is _not_ supported.

See Firepower Threat Defense Support Specifics for more information.

CDO Platform Maintenance Schedule

CDO Maintenance Schedule

CDO updates its platform every week with new features and quality improvements. Updates can be made during a 3 hour period according to this schedule.

Table 1: CDO Maintenance Schedule

Day of the Week	Time of Day (24-hour time)
Thursday	09:00 UTC - 12:00 UTC

During this maintenance period, you can still access your tenant and if you have a cloud-delivered Firewall Management Center, you can access that platform as well. Additionally, the devices you have onboarded to CDO continue to enforce their security policies.

Note We advise you not to use CDO to deploy configuration changes on the devices it manages during maintenance periods.

If there is a failure that stops CDO or cloud-delivered Firewall Management Center from communicating, that failure is addressed on all affected tenants as quickly as possible even if it is outside the maintenance window.

Cloud-delivered Firewall Management Center Maintenance Schedule

Customers who have a cloud-delivered Firewall Management Center deployed on their tenant are notified approximately 1 week before CDO updates the cloud-delivered Firewall Management Center environment. Super-admin and Admin users of the tenant are notified by email. CDO also displays a banner on its home page notifying all users of upcoming updates.

The update to your tenant may take up to 1 hour and occurs within the 3 hour maintenance period on the maintenance day assigned to your tenant's region. While your tenant is being updated, you will not be able to access the cloud-delivered Firewall Management Center environment, but you will still be able to access the rest of CDO.

Table 2: Cloud-delivered Firewall Management Center Maintenance Schedule

Day of the Week	Time of Day (24-hour time)	Region
Wednesday	04:00 UTC - 07:00 UTC	Europe, the Middle East, or Africa (EMEA)
Wednesday	17:00 UTC - 20:00 UTC	Asia-Pacific-Japan (APJ)
Thursday	09:00 UTC - 12:00 UTC	Americas