



Get started with Security Cloud Control Firewall Management

This chapter explains the steps for provisioning the firewall management within Security Cloud Control Firewall Management and explains how to access it. Additionally, it presents an overview of the firewall dashboard.

- [Overview of Security Cloud Control Firewall Management, on page 1](#)
- [Overview of Cloud-Delivered Firewall Management Center, on page 4](#)

Overview of Security Cloud Control Firewall Management

Security Cloud Control Firewall Management (formerly Cisco Defense Orchestrator or CDO) is a cloud-based security policy manager that helps simplify and unify security policies across your Cisco firewalls and other devices such as Cisco IOS and SSH. The firewalls and devices can be managed from **Firewall**, which is listed under **Products** in the Security Cloud Control dashboard.

Security Cloud Control Firewall Management helps you optimize your security policies by identifying inconsistencies within them and by providing with the tools to fix them. It provides you with ways to share objects and policies, as well as create configuration templates, to promote policy consistency across devices.

Because Security Cloud Control Firewall Management coexists with Adaptive Security Device Manager (ASDM), it keeps track of configuration changes made by ASDM and reconciles the differences.

You can manage a wide range of devices in one place. Advanced users will also find their traditional CLI interface with some new enhancements to make management even more efficient for them.

Security Cloud Control Firewall Management also provides a guided "Day 0" experience, helping you to quickly onboard Threat Defense devices to your on-premises or Cloud-Delivered Firewall Management Center. It also presents you with other key features that you may benefit from and helps you enable and configure them.

Device onboarding requirements

Before you onboard a device, complete these prerequisites:

- Complete the installation wizard.
- License the device.

After you complete those prerequisites, use the Security Cloud Control Firewall Management onboarding wizard to onboard the device.

Keep these restrictions in mind:

- After you onboard devices to a Security Cloud Control Firewall Management associated with an organization, you cannot migrate those devices to another organization.
- To move devices to a new organization, you must re-onboard them to the new organization.

Cisco Online Privacy Statement

Cisco Systems, Inc. and its subsidiaries (collectively referred to as "Cisco") are committed to protecting your privacy and providing you with a positive experience on Cisco websites and while using Cisco products and services ("Solutions"). Read the [Cisco Online Privacy Statement](#) carefully to get a clear understanding of how Cisco collects, uses, shares, and protects your personal information.

Security Cloud Control Firewall Management Platform Maintenance Schedule

Security Cloud Control Firewall Management updates its platform every week with new features and quality improvements. Updates are made during a 3-hour period according to this schedule:

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

During the Security Cloud Control Firewall Management upgrade period, you can still access your organization and the Cloud-Delivered Firewall Management Center. Additionally, the devices that you have onboarded to Security Cloud Control Firewall Management continue to enforce their security policies.



Note

- During the maintenance period of the Security Cloud Control Firewall Management, refrain from creating or deploying configurations to the devices it manages.
- If there is any issue that stops Security Cloud Control Firewall Management from communicating, Cisco addresses that issue in all the affected tenants as quickly as possible, even if it is outside the maintenance window.

Security Cloud Control Firewall Management licenses

Security Cloud Control Firewall Management requires a base subscription for organization entitlement and device licenses for managing devices. You can buy one or more Security Cloud Control Firewall Management base subscriptions based on the number of tenants you require and device licenses based on the device model number and the quantity. In other words, purchasing the base subscription provides you with a Security Cloud Control Firewall Management organization. For every device you choose to manage using Security Cloud Control Firewall Management, you need separate device licenses.

For the purposes of planning your deployment, note that each Security Cloud Control Firewall Management tenant can manage approximately 500 devices through the Secure Device Connector (SDC) and any number of devices using the cloud connector. See [Secure Device Connector \(SDC\)](#) for more information.

To onboard and manage devices from Security Cloud Control Firewall Management, you must purchase a base subscription and device-specific, term-based subscriptions based on the devices you want to manage.

Subscriptions

Security Cloud Control Firewall Management subscriptions are term-based:

- **Base:** Offers subscriptions for one, three, and five years, and provides entitlement to access the Security Cloud Control Firewall Management organization and onboard adequately licensed devices.
- **Device License:** Offers subscriptions for one, three, and five years for any supported device you choose to manage. For example, you can choose to manage a Cisco Firepower 1010 device using Security Cloud Control Firewall Management for three years if you purchase a three-year software subscription for the Cisco Firepower 1010 device.

See [Software and Hardware Supported by Security Cloud Control Firewall Management](#) for more information on Cisco security devices that Security Cloud Control Firewall Management supports.



Important

You do not require two separate device licenses to manage a high-availability device pair in Security Cloud Control Firewall Management. If you have a high-availability pair, purchasing one device license is sufficient because Security Cloud Control Firewall Management considers the pair of high-availability devices as one single device.



Note

- Catalyst SD-WAN does not require an additional license for integration with Security Cloud Control Firewall Management. Customers with Cisco Digital Network Architecture (DNA) or WAN Essentials licenses can use these existing licenses for integration without needing any other license.
-



Note

You cannot manage Security Cloud Control Firewall Management licensing through the Cisco Smart Licensing portal.

Software Subscription Support

The Security Cloud Control Firewall Management base subscription includes software subscription support that is valid for the term of the subscription and provides access to software updates, major upgrades, and Cisco Technical Assistance Center (TAC) at no extra cost. While software support is selected by default, you can also leverage Security Cloud Control Firewall Management solution support based on your requirement.

More Supported Devices and Licenses

In addition to supporting Secure Firewall Threat Defense devices through the Cloud-Delivered Firewall Management Center, Security Cloud Control also manages these devices:

- Cisco Secure Firewall ASA
- On-premises Cisco Secure Firewall Management Center
- Cisco Meraki Security Appliance
- Cisco IOS devices
- Devices accessible using SSH
- Amazon Web Services (AWS) virtual private cloud (VPC)
- Umbrella Organization

You will need a Security Cloud Control base entitlement license and a license specific to the device you want to manage.

Overview of Cloud-Delivered Firewall Management Center

Cloud-Delivered Firewall Management Center is a software-as-a-service product that manages Secure Firewall Threat Defense devices through Security Cloud Control Firewall Management. It provides many of the same functions as an On-Premises Firewall Management Center.

Cloud-Delivered Firewall Management Center has the same appearance and behavior as an On-Premises Firewall Management Center and uses the same FMC API.

Because it is a SaaS product, the Security Cloud Control Firewall Management operations team deploys and maintains the Cloud-Delivered Firewall Management Center software. As new features are introduced, the operations team updates the Cloud-Delivered Firewall Management Center in your Security Cloud Control Firewall Management organization.

Migration and onboarding details

A migration wizard is available to help you migrate Threat Defense devices from an On-Premises Firewall Management Center to Cloud-Delivered Firewall Management Center.

Devices must run one of these Threat Defense software releases before you migrate them:

- Minimum On-Premises Firewall Management Center: 7.2
- Minimum Threat Defense: 7.2.x (not supported for Version 7.1)

Threat Defense 7.1 releases are not supported for migration.

You onboard Threat Defense devices in Security Cloud Control Firewall Management by using familiar methods, such as entering the serial number or using a CLI command that includes a registration key.

After onboarding:

- The device appears in both Security Cloud Control Firewall Management and Cloud-Delivered Firewall Management Center.

- You configure the device in Cloud-Delivered Firewall Management Center.
- In Security Cloud Control Firewall Management, you can review device information such as version, configuration status, connectivity, health status, and node status.
- When you click the health status in Security Cloud Control Firewall Management, the platform opens the device health monitoring page in the Cloud-Delivered Firewall Management Center user interface.

Availability and Security Analytics

Security Cloud Control Firewall Management supports high availability for the Threat Defense devices that it manages through the data interface. This feature is supported for devices that run software version 7.2 or later.

You can analyze security events from onboarded threat defense devices by using either Security Analytics and Logging (SaaS) or Security Analytics and Logging (On-Premises):

- Security Analytics and Logging (SaaS) stores events in the cloud, and you view those events in Security Cloud Control Firewall Management.
- Security Analytics and Logging (On-Premises) stores events on an on-premises Secure Network Analytics appliance, and analysis occurs in the On-Premises Firewall Management Center.

In both cases, you can still send logs directly from firewalls to a log collector of your choice.

Licenses

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 Secure Firewall Threat Defense. For more information, see [Cloud-Delivered Firewall Management Center license](#).

Existing customers can continue to use Security Cloud Control for managing other device types like, the Secure Firewall ASA, Meraki, Cisco IOS devices, Umbrella, and AWS virtual private clouds. If you use Security Cloud Control to manage a Secure Firewall Threat Defense device configured for local management with Firepower Device Manager, you can continue to manage them with Security Cloud Control 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 Security Cloud Control Tenant](#).

See [Managing Cisco Secure Firewall Threat Defense with Cloud-delivered Firewall Management Center](#) for the complete administrator guide to the Cloud-Delivered Firewall Management Center.

Enable Cloud-Delivered Firewall Management Center

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

From the Security Cloud Control menu, click **Administration > Integrations > Firewall Management Center** and click **Enable Cloud-Delivered FMC**.

Security Cloud Control 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 Security Cloud Control 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**.

What to do next

1. Register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager (CSSM) to activate smart license. For detailed steps, refer to [Register the Cloud-Delivered Firewall Management Center with the Smart Software Manager](#).
2. Onboard your Firewall Threat Defense devices to the Cloud-Delivered Firewall Management Center and manage them.

Determine the Cloud-Delivered Firewall Management Center Version in Security Cloud Control Firewall Management

Information about the Cloud-Delivered Firewall Management Center version is required primarily for migration planning, feature support verification, troubleshooting, licensing, and operational management.

Use this procedure to determine the current version of your Cloud-Delivered Firewall Management Center in Security Cloud Control Firewall Management.

Before you begin

Enable [Enable Cloud-Delivered Firewall Management Center](#) in your organization.

Procedure

-
- Step 1** In the left pane, click **Administration > Integrations > Firewall Management Center**.
- Step 2** Under the **FMC** tab, the version is displayed under the **Version** column.

☐	Name	Version	Devices	Type	Status	Last heartbeat
☐	Cloud-Delivered FMC	20250825	2	Cloud-Delivered FMC	Active	10/10/2025, 19:22:48
☐	OnPrem_FMC_1	7.6.0-build 1526	1	On-Prem FMC	Synced	10/10/2025, 19:22:39
☐	OnPrem_FMC_2	7.7.0-build 91	1	On-Prem FMC	Synced	10/10/2025, 19:22:39

For more information about Cloud-Delivered Firewall Management Center versions, see [Release Notes for Cloud-Delivered Firewall Management Center](#).

Cloud-Delivered Firewall Management Center licensing and registration

Register Cloud-Delivered Firewall Management Center with Cisco Smart Licensing the same way you would for On-Premises Firewall Management Center.

Overview

Cloud-Delivered Firewall Management Center is included with the base subscription and trial for Security Cloud Control Firewall Management. You do not need to purchase a separate license for Cloud-Delivered Firewall Management Center. The base subscription or trial covers Cloud-Delivered Firewall Management Center, enabling you to manage Firewall Threat Defense devices through the cloud.

Cloud-Delivered Firewall Management Center is provisioned with a 90-day evaluation license upon deployment.



Important

We strongly recommend registering Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager immediately after deployment to access all features, including those requiring export encryption such as RAVPN and SSL VPN. Early registration prevents feature limitations and deployment interruptions.

Evaluation license

- Features requiring export encryption, such as Remote Access VPN, SSL VPN, and other encryption-dependent options, remain disabled until you register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager (CSSM).
- After the 90-day evaluation period ends, you can continue onboarding Firewall Threat Defense devices, but manually triggered or scheduled deployments are blocked until registration with CSSM is completed.
- Security Cloud Control Firewall Management sends alert notifications as the evaluation license nears expiration.



Note The **Smart license** field displays a warning when the evaluation license is expiration.

Cloud-Delivered FMC	
Hostname	amallio.app.staging.cdo.cisco.com
Version	20260213
Smart license	Evaluation period (expires in 89 days)

When the evaluation period ends, Cloud-Delivered Firewall Management Center is unregistered. Registering Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager converts from evaluation mode to a fully licensed state.

Click the evaluation warning link to open the smart licensing registration page and register Cloud-Delivered Firewall Management Center with Cisco Smart Software Manager.

Registration with Cisco Smart Software Manager (CSSM)

- Connect Cloud-Delivered Firewall Management Center to your smart licensing account, following the same process as On-Premises Firewall Management Center. The high-level procedure is provided in this section.
- No separate license purchase is needed for Cloud-Delivered Firewall Management Center; the license is automatically applied upon registration.
- Registering with smart licensing enables encryption export features.
- Registration ensures compliance and prevents deployment issues.

To learn how to get a Cloud-Delivered Firewall Management Center provisioned on your Security Cloud Control tenant, see [Request a Cloud-Delivered Firewall Management Center for your Security Cloud Control Tenant](#).

Licensing for Firewall Threat Defense devices

- No separate license purchase is needed for Cloud-Delivered Firewall Management Center.
- Each Firewall Threat Defense device managed by Cloud-Delivered Firewall Management Center requires an individual license.
- After registering Cloud-Delivered Firewall Management Center with CSSM, an administrator may apply feature licenses to security devices.

Step-by-step registration

A high-level procedure is provided here. For detailed steps, see [Register the Management Center with the Smart Software Manager](#).

1. Create or Access Your Smart Account:

Ensure you have a Cisco Smart Software Manager account. If you do not have one, create it at [Smart Software Manager](#).

2. Generate a Registration Token or Use a Registration Token:

In the Smart Software Manager, use an existing valid registration token or generate a registration token for the virtual account to which you want to register the Cloud-Delivered Firewall Management Center.

- a. Navigate to **Inventory > New Token**.
- b. Enter a description and set an expiration (Cisco recommends 30 days).
- c. Create and copy the token.

3. Register Cloud-Delivered Firewall Management Center with the Token:

- a. Log in to the Cloud-Delivered Firewall Management Center interface.
- b. Navigate to **System > Licenses > Smart Licenses**.
- c. Click **Register** and paste the registration token into the **Product Instance Registration Token** field.
- d. Ensure there are no extra spaces or blank lines before or after the token.
- e. Click **Apply Changes**.

4. Verify Registration:

After registration, verify the license status under **System > Licenses > Smart Licenses** to confirm successful registration, license application, and that “Export-Controlled Features” are enabled.

Cloud-Delivered Firewall Management Center Maintenance Schedule

Customers who have a Cloud-Delivered Firewall Management Center deployed on their organization are notified approximately 1 week before Security Cloud Control updates the Cloud-Delivered Firewall Management Center environment.

Super Admin and Admin users of the tenant are notified by email. Security Cloud Control also displays a banner on its home page notifying all users of upcoming updates.



Note

- During the maintenance period of the Cloud-Delivered Firewall Management Center, refrain from creating or deploying configurations to the devices it manages.
 - If there is any issue that stops Security Cloud Control 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.
-

