



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 a Threat Defense Device, on page 1](#)
- [Delete a Device from CDO, on page 45](#)
- [Import Configuration for Offline Device Management, on page 45](#)
- [Backing Up FDM-Managed Devices, on page 45](#)
- [FDM Software Upgrade Paths, on page 52](#)
- [FDM-Managed Device Upgrade Prerequisites, on page 54](#)
- [Upgrade a Single FDM-Managed Device, on page 55](#)
- [Bulk FDM-Managed Devices Upgrade, on page 57](#)
- [Upgrade an FDM-Managed High Availability Pair, on page 59](#)
- [Upgrade to Snort 3.0, on page 62](#)
- [Revert From Snort 3.0 for FDM-Managed Device, on page 65](#)
- [Schedule a Security Database Update, on page 66](#)

Onboard a Threat Defense Device



Attention Secure Firewall device manager (FDM) support and functionality is only available upon request. If you do not already have Firewall device manager support enabled on your tenant you cannot manage or deploy to FDM-managed devices. [Send a request to the support team](#) to enable this platform.

There are different methods of onboarding a threat defense device. We recommend using the registration key method.

If you experience issues while onboarding a device, see [Troubleshoot FDM-Managed Device Onboarding Using Serial Number](#) or [Failed Because of Insufficient License](#) for more information.

Onboard a Threat Defense Device to Cloud-delivered Firewall Management Center

You can onboard threat defense devices running version 7.2 and later to the Cloud-delivered Firewall Management Center. See [Onboard an FTD to the Cloud-Delivered Firewall Management Center](#) for more information.

Onboard a Threat Defense Device with a Serial Number

This procedure is a simplified method of onboarding the Firepower 1000, Firepower 2100, or Secure Firewall 3100 series physical devices running supported versions of software. To onboard the device, you need the chassis serial number or PCA serial number of the device and ensure that the device is added to a network that can reach the internet.

You can onboard new factory-shipped devices or already configured devices to CDO.

See [Onboard an FDM-Managed Device using the Device's Serial Number, on page 19](#) for more information.

Onboard a Threat Defense Device with a Registration Key

We recommend onboarding threat defense devices with a registration key. This is beneficial if your device is assigned an IP address using DHCP. If that IP address changes for some reason, your threat defense device remains connected to CDO if you have onboarded it with a registration key.

- [Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 11](#)
- [Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key, on page 15](#)

Onboard an Threat Defense Device Using Credentials

You can onboard a threat defense device using the device credentials and the IP address of the device's outside, inside, or management interface depending on how the device is configured in your network. To onboard a device with credentials, see [Onboard an FDM-Managed Device Using Username, Password, and IP Address, on page 9](#). To onboard with an interface address, see [Onboard a Threat Defense Device](#) later in this article.

CDO needs HTTPS access to the device in order to manage it. How you allow HTTPS access to the device depends on how your device is configured in your network and whether you onboard the device using a [Secure Device Connector](#) or a Cloud Connector.



Note If you connect to <https://www.defenseorchestrator.eu> and you are using software version 6.4, you must onboard the threat defense device with this method. You cannot use the registration key method.

When using device credentials to connect CDO to a device, it is a best practice to download and deploy a Secure Device Connector (SDC) in your network to manage the communication between CDO and the device. Typically, these devices are non-perimeter based, do not have a public IP address, or have an open port to the outside interface. The threat defense device, when onboarded with credentials, can be onboarded to CDO using an SDC.

Note that customers also using the threat defense device as the head-end for VPN connections will not be able to use the outside interface to manage their device.

Onboard a Threat Defense Cluster

You can onboard a threat defense device that is clustered prior to onboarding to CDO. Clustering lets you group multiple firewall threat defense units together as a single logical device that provides the convenience of a single device (management, integration into a network) while achieving the increased throughput and redundancy of multiple devices.

See [Onboard a Clustered Secure Firewall Threat Defense Device, on page 34](#).

FDM-Managed Device Configuration Prerequisites for Onboarding

FDM-Managed Device Management

You can only onboard threat defense devices that are being managed by Secure Firewall device manager (FDM). threat defense devices being managed by Secure Firewall Management Center cannot be managed by the cloud-delivered Firewall Management Center.

If the device is not configured for local management, you must switch to local management before onboarding the device. See the **Switching Between Local and Remote Management** chapter of the [Secure Firewall Threat Defense Configuration Guide for Firepower Device Manager](#).

Licensing

The device **must** have at least an license installed before it can be onboarded to CDO although you can have a Smart License applied in some circumstances.

Onboarding Method	Secure Firewall device manager Software Version	90-day Evaluation licensed allowed?	Can the device already be smart-licensed before onboarding?	Can the device already be registered with Cisco Cloud Services before you onboarding?
Credentials (user name and password)	6.4 or later	Yes	Yes	Yes
Registration Key	6.4 or 6.5	Yes	No. Unregister the smart license and then onboard the device.	N/A
Registration Key	6.6 or later	Yes	Yes	No. Unregister the device from Cisco Cloud Services and then onboard the device.
Low Touch Provisioning	6.7 or later	Yes	Yes	Yes
Onboarding a device with a Serial Number	6.7 or later	Yes	Yes	Yes

See [Cisco Firepower System Feature Licenses](#) for more information.

Device Addressing

It is a best practice that the address you use to onboard the FDM-managed device is a static address. If the device's IP address is assigned by DHCP, it would be optimal to use a DDNS (dynamic domain name system) to automatically update your device's domain name entry with the new IP address of the device if it changes.



Note FDM-managed devices do not natively support DDNS; you must configure your own DDNS.

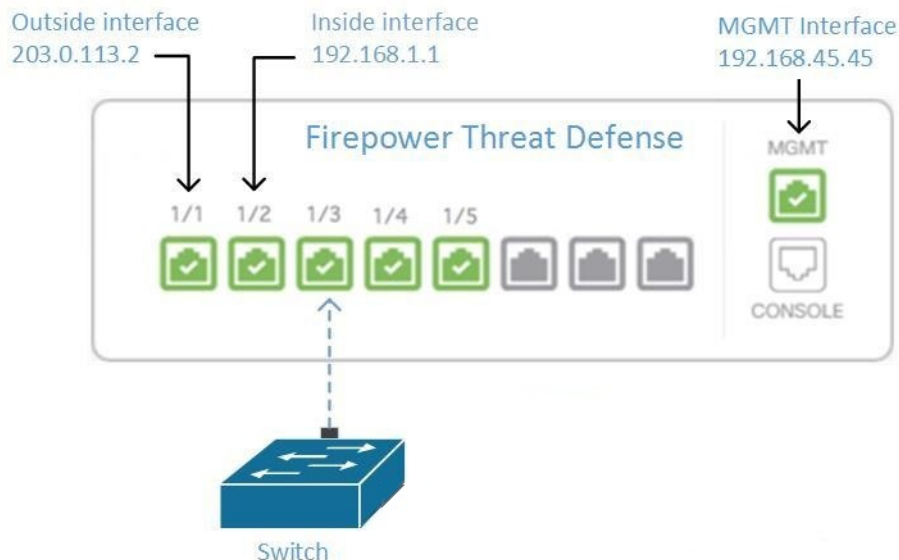


Important If your device gets an IP address from a DHCP server, and you *do not* have a DDNS server updating the FDM-managed device's domain name entry with any new IP addresses, or your device receives a new address, you can [change the IP address CDO maintains for the device](#) and then [reconnect the device](#). Better still, onboard the device with a registration key.

Managing an FDM-Managed Device from the Inside Interface

Managing an FDM-managed device using the inside interface may be desirable if the dedicated MGMT interface is assigned an address that is not routable within your organization; for example, it might only be reachable from within your data center or lab.

Figure 1: Interface Addresses



Remote Access VPN Requirement

If the FDM-managed device you manage with CDO will be managing Remote Access VPN (RA VPN) connections, CDO must manage the device using the inside interface.

What to do next:

Continue to [Manage an FDM-Managed Device from the Inside Interface](#) for the procedure for configuring the FDM-managed device.

Manage an FDM-Managed Device from the Inside Interface

This configuration method:

- Assumes that the FDM-managed device has not been on-boarded to CDO.
- Configures a data interface as the inside interface.
- Configures the inside interface to receive MGMT traffic (HTTPS).
- Allows the address of the cloud connector to reach the inside interface of the device.

Before you begin

Review the prerequisites for this configuration in these topics:

- [Managing an FDM-Managed Device from the Inside Interface](#)
- [Connect Cisco Defense Orchestrator to your Managed Devices](#)

Procedure

-
- Step 1** Log in to the Secure Firewall device manager.
- Step 2** In the **System Settings** menu, click **Management Access**.
- Step 3** Click the **Data Interfaces** tab and click **Create Data Interface**.
- In the **Interface** field, select the pre-named "**inside**" interface from the list of interfaces.
 - In the **Protocols** field, select **HTTPS** if it is not already.
 - In the **Allowed Networks** field, select the network objects that represent the networks inside your organization that will be allowed to access the inside address of the FDM-managed device. The IP address of the SDC or cloud connector should be among the addresses allowed to access the inside address of the device.

In the [Interface Addresses](#) diagram, the SDC's IP address, 192.168.1.10 should be able to reach 192.168.1.1.
- Step 4** **Deploy the change.** You can now manage the device using the inside interface.
-

What to do next**What if you are using a Cloud Connector?**

Use the procedure above and add these steps:

- Add a step to "NAT" the outside interface to (203.0.113.2) to the inside interface (192.168.1.1).
- In step 3c of the procedure above, your "Allowed Network" is a network group object containing the the public IP addresses of the cloud connector.

- Add a step that creates an Access Control rule allowing access to the outside interface (203.0.113.2) from the public IP addresses of the cloud connector.

If you are a customer in **Europe, the Middle East, or Africa (EMEA)**, and you connect to CDO at <https://defenseorchestrator.eu/>, these are the public IP addresses of the cloud connector:

- 35.157.12.126
- 35.157.12.15

If you are a customer in the **United States**, and you connect to CDO at <https://defenseorchestrator.com/>, these public IP addresses of the cloud connector:

- 52.34.234.2
- 52.36.70.147

If you are a customer in the **Asia-Pacific-Japan-China (AJPC)** region, and you connect to CDO at <https://www.apj.cdo.cisco.com/>, allow inbound access from the following IP addresses:

- 54.199.195.111
- 52.199.243.0

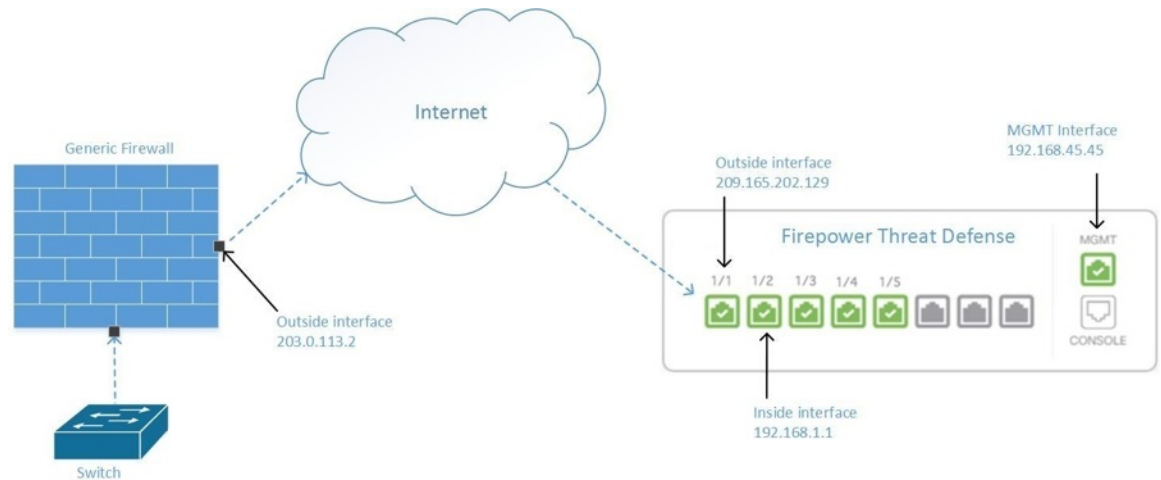
Onboard the FDM-Managed Device

The recommended way of onboarding the FDM-managed device to CDO is to use the registration token onboarding approach. After you configure the inside interface to allow management access from the Cloud Connector to the FDM-managed device, onboard the FDM-managed device with the user name and password.

Managing an FDM-Managed Device from the Outside Interface

Managing an cloud-delivered Firewall Management Center device from the outside interface may be desirable if you have one public IP address assigned to a branch office and Cisco Defense Orchestrator is managed using a Cloud Connector at another location.

Figure 2: Device Management on Outside Interface



This configuration doesn't mean that the physical MGMT interface is no longer the device's management interface. If you were in the office where the cloud-delivered Firewall Management Center device was located, you would be able to connect to the address of the MGMT interface and manage the device directly.

Remote Access VPN Requirement

If the device you manage with cloud-delivered Firewall Management Center will be managing Remote Access VPN (RA VPN) connections, cloud-delivered Firewall Management Center will not be able to manage the cloud-delivered Firewall Management Center device using the outside interface. See [Managing an FDM-Managed Device from the Inside Interface](#) instead.

What to do next:

Continue to [Manage the FDM-Managed Device's Outside Interface](#) for the procedure for configuring the cloud-delivered Firewall Management Center device.

Manage the FDM-Managed Device's Outside Interface

This configuration method:

1. Assumes that the FDM-managed device has not been on-boarded to CDO.
2. Configures a data interface as the outside interface.
3. Configures management access on the outside interface.
4. Allows the public IP address of the cloud connector (after it has been NAT'd through the firewall) to reach the outside interface.

Before you begin

Review the prerequisites for this configuration in these topics:

- [Manage the FDM-Managed Device's Outside Interface](#)

- [Connect Cisco Defense Orchestrator to your Managed Devices](#)

Procedure

- Step 1** Log in to the Secure Firewall device manager.
- Step 2** In the **System Settings** menu, click **Management Access**.
- Step 3** Click the **Data Interfaces** tab and click **Create Data Interface**.
- In the **Interface** field, select the pre-named "**outside**" interface from the list of interfaces.
 - In the **Protocols** field, select **HTTPS** if it is not already. CDO only needs HTTPS access.
 - In the **Allowed Networks** field, create a host network object containing the public-facing IP address of the cloud connector after it gets NAT'd through the firewall.

In the [Device Management from Outside Interface](#) network diagram, the cloud connector's IP address, 10.10.10.55, would be NAT'd to 203.0.113.2. For the Allowed Network, you would create a host network object with the value 203.0.113.2.
- Step 4** Create an Access Control policy in Secure Firewall device manager that allows management traffic (HTTPS) from the public IP address of the SDC or cloud connector, to the outside interface of your FDM-managed device. In this scenario, the source address would be 203.0.113.2 and the source protocol would be HTTPS; the destination address would be 209.165.202.129 and the protocol would be HTTPS.
- Step 5** **Deploy the change.** You can now manage the device using the outside interface.
-

What to do next

What if you are using a cloud connector?

The process is very similar, except for two things:

- In step 3c of the procedure above, your "Allowed Network" is a network group object containing the the public IP addresses of the cloud connector.
 - If you are a customer in **Europe, the Middle East, or Africa (EMEA)**, and you connect to CDO at <https://defenseorchestrator.eu/>, these are the public IP addresses of the cloud connector:
 - 35.157.12.126
 - 35.157.12.15
 - If you are a customer in the **United States**, and you connect to CDO at <https://defenseorchestrator.com/>, these are the public IP addresses of the cloud connector:
 - 52.34.234.2
 - 52.36.70.147
 - If you are a customer in the **Asia-Pacific-Japan-China (AJPC)** region, and you connect to CDO at <https://www.apj.cdo.cisco.com/>, allow inbound access from the following IP addresses:
 - 54.199.195.111

- 52.199.243.0

- In step 4 of the procedure above, you create an Access Control rule that allows access to the outside interface from the public IP addresses of the cloud connector.

The [Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key](#) approach is the recommended way of onboarding the FDM-managed device to CDO. After you configure the outside interface to allow management access from the cloud connector, onboard the FDM-managed device. You will connect using the IP address of the outside interface. In our scenario, that address is 209.165.202.129.

Onboard an FDM-Managed Device to CDO

Use the following procedures to onboard an FDM-managed to CDO with the following methods.

Onboard an FDM-Managed Device Using Username, Password, and IP Address

Use this procedure to onboard an FDM-managed device using only the device credentials and the device's Management IP address. This is the simplest method of onboarding an FDM-managed device. However, the recommended way of onboarding an FDM-managed device to CDO is by using a [Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key](#).

Before you begin



Important

Before you onboard an FDM-managed device to Cisco Defense Orchestrator, read [Onboard a Threat Defense Device](#) and [Connect Cisco Defense Orchestrator to your Managed Devices](#). They provide the general device requirements and onboarding prerequisites needed to onboard a device.

- You need the following information to onboard an FDM-managed device using the credentials method:
 - The device credentials CDO will use to connect to the device.
 - The device's IP address of the interface you are using to manage the device. This may be the Management interface, an inside interface, or the outside interface depending on how you have configured your network.
 - The device must be managed by Secure Firewall device manager and configured for local management in order for you to onboard it to CDO. It cannot be managed by Secure Firewall Management Center.




Note

If you connect to <https://www.defenseorchestrator.eu> and your FDM-managed device is running software version 6.4, you must use this method. You can only onboard an FDM-managed device running software version 6.5+.

Procedure

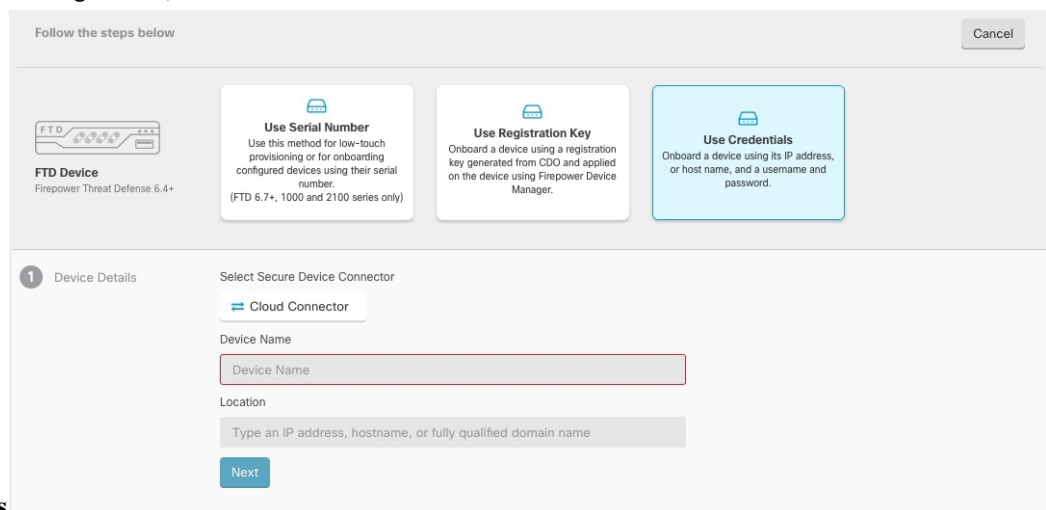
Step 1 Log in to CDO.

Step 2 In the navigation pane, click **Inventory** and click the blue plus button  to **Onboard** a device.

Step 3 Click **FTD**.

Important When you attempt to onboard an FDM-managed device, CDO prompts you to read and accept the Secure Firewall Threat Defense End User License Agreement (EULA), which is a one-time activity for your tenant. Once you accept the EULA, CDO won't prompt you again to accept it unless the EULA changes.

Step 4 In the onboarding wizard, click **Use**



Follow the steps below Cancel

FTD Device
Firepower Threat Defense 6.4+

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000 and 2100 series only)

Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

Use Credentials
Onboard a device using its IP address, or host name, and a username and password.

1 Device Details

Select Secure Device Connector
 Cloud Connector

Device Name

Location

Next

Credentials

Step 5 In the Device Details step:

- Click the **Secure Device Connector** button and select a Secure Device Connector (SDC) installed in your network. If you would rather not use an SDC, CDO can connect to your FDM-managed device using the Cloud Connector. Your choice depends on how you [connect CDO to your managed devices](#).
- Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.
- In the **Location** field, enter the IP address of the interface you are using to manage the device, hostname, or fully qualified domain name of the device. The default port is 443.

Important If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO tenant and SecureX/CTR account in order for your devices to be registered with SecureX. Your accounts can be merged through the SecureX portal. See [Merge Your CDO and SecureX Accounts](#) for instructions. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features.

Step 6 In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** is enabled by default. This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See [Update FTD Security Databases](#) and [Schedule a Security Database Update](#).

Disabling this option does not affect any previously scheduled updates you may have configured through FDM.

Click **Next**.

- Step 7** Enter the device administrator's username and password and click **Next**.
- Step 8** If there are pending changes on the device's Secure Firewall device manager, you will be notified and you can revert the changes or log in to the manager and deploy the pending changes. If there are no pending changes on Secure Firewall device manager, you will not see a prompt.
- Step 9** (Optional) Add a label the device. See [Labels and Label Groups](#) for more information.

Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key

This procedure describes how to onboard an FDM-managed device using a registration key. This method is the recommended way of onboarding the FDM-managed device to Cisco Defense Orchestrator and is beneficial if your FDM-managed device is assigned an IP address using DHCP. If that IP address changes for some reason, your FDM-managed device remains connected to CDO. Additionally, your FDM-managed device can have an address on your local area network, and as long as it can access the outside network, it can be onboarded to CDO using this method.



Warning If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO tenant and SecureX/CTR account in order for your devices to be registered with SecureX. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features. We **strongly** recommend merging your accounts before you create a CDO module in SecureX. Your accounts can be merged through the SecureX portal. See [Merge Accounts](#) for instructions.

Before Onboarding

- For customers running version 6.4, this method of onboarding is only supported for the US region (defenseorchestrator.com).
- For customers running version 6.4, and connecting to the EU region (defenseorchestrator.eu), they must onboard their device using its [Onboard an FDM-Managed Device Using Username, Password, and IP Address](#).
- Customers running version 6.5 or later, and connecting either to the US, EU, or APJC region (apj.cdo.cisco.com) regions can use this method of onboarding.
- Review [Connect Cisco Defense Orchestrator to your Managed Devices](#) for the networking requirements needed to connect CDO to your FDM-managed device.
- Make sure your device is managed by Secure Firewall device manager, not Secure Firewall Management Center.
- Devices running version 6.4 and 6.5 must not be registered with Cisco Smart Software Manager before onboarding them with a registration key. You will need to unregister the smart licenses of those FDM-managed devices before onboarding them to CDO. See "Unregistering a Smart-licensed Firewall device manager" below.
- The device may be using a 90-day evaluation license.

- Log in to the FDM-managed device and make sure that there are no pending changes waiting on the device.
- Make sure DNS is configured properly on your FDM-managed device.
- Make sure the time services are configured properly on the FDM-managed device.
- Make sure the FDM-managed device shows the correct date and time otherwise the onboarding will fail.

What to do next

Do one of these two things:

- Unregister your FDM-managed device from Cisco Smart Software Manager if it is already smart-licensed. **You must unregister the device from Cisco Smart Software Manager before you onboard it to CDO with a registration Key.** Continue to [Unregister a Smart-licensed FDM-Managed Device, on page 12](#).
- If your device is not already smart-licensed, continue to [Procedure to Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 13](#).

Unregister a Smart-licensed FDM-Managed Device

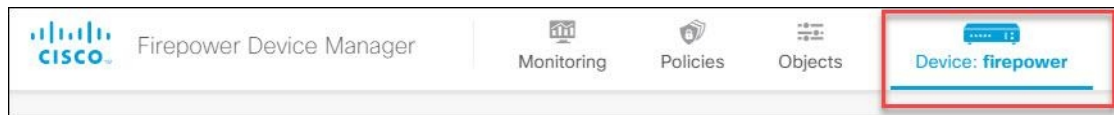
If the device you want to onboard is running version 6.4 or 6.5, and is already smart-licensed, the device is likely to be registered with Cisco Smart Software Manager. **You must unregister the device from Cisco Smart Software Manager before you onboard it to CDO with a registration Key.** When you unregister, the base license and all optional licenses associated with the device, are freed in your virtual account.

After unregistering the device, the current configuration and policies on the device continue to work as-is, but you cannot make or deploy any changes.

Procedure

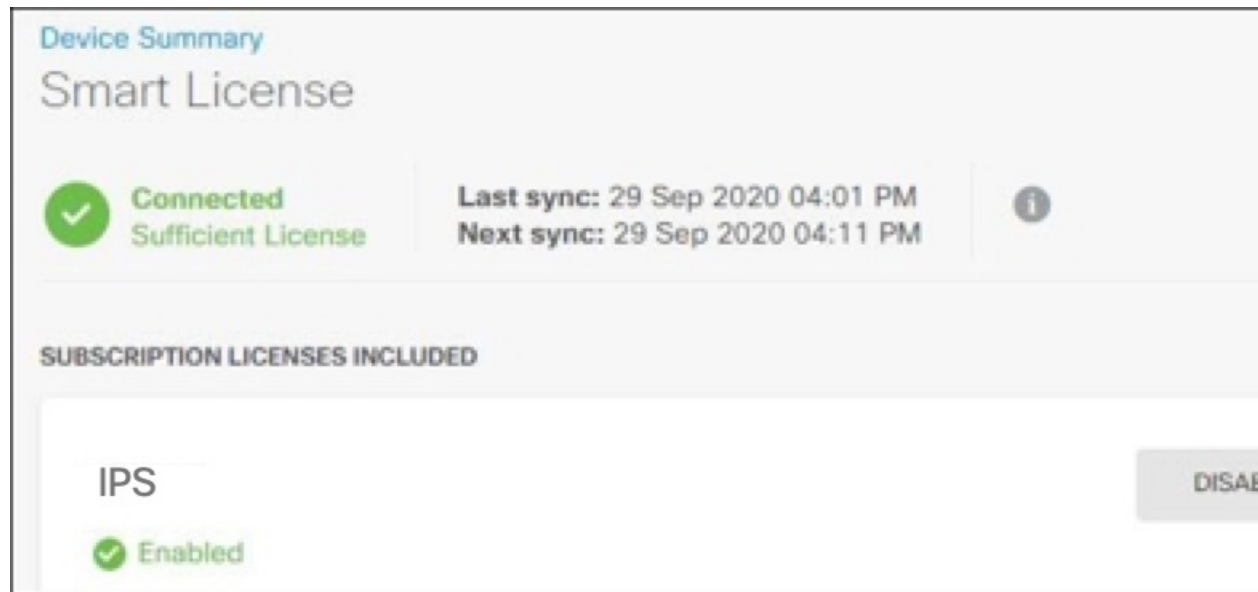
Step 1 Log on to the device using the Secure Firewall device manager.

Step 2 Click the device icon in the upper tab.



Step 3 In the **Smart License** area, click **View Configuration**.

Step 4 Click the **Go to Cloud Services** gear menu and select **Unregister Device**.



Step 5 Read the warning and click **Unregister** to unregister the device.

What to do next

If you unregistered your in order to onboard it to CDO, continue to [Procedure to Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 13](#)

Procedure to Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key


To onboard an FDM-managed using a registration key, follow this procedure:

Before you begin

Review the prerequisites discussed in [Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key, on page 11](#).

Procedure

Step 1 Log in to CDO.

Step 2 In the navigation pane, click **Inventory** and click the blue plus button  to **Onboard** a device.

Step 3 Click **FTD**.

Important When you attempt to onboard an FDM-managed device, Cisco Defense Orchestrator prompts you to read and accept the Firepower Threat Defense End User License Agreement (EULA), which is a one-time activity in your tenant. Once you accept this agreement, CDO doesn't prompt it again in subsequent FDM-managed onboarding. If the EULA agreement changes in the future, you must accept it again when prompted.

Step 4 On the **Onboard FTD Device** screen, click **Use Registration Key**.


Step 5 Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.

Step 6 In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** option is enabled by default. This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See [Update FTD Security Databases](#) and [Schedule a Security Database Update](#) for more information.

Note Disabling this option does not affect any previously scheduled updates you may have configured through Secure Firewall device manager.

Step 7 In the **Create Registration Key** area, CDO generates a registration key.

Note If you move away from the onboarding screen after the key is generated and before the device is fully onboarded, you will not be able to return to the onboarding screen; however, CDO creates a placeholder for that device on the **Inventory** page. When you select the device's placeholder, you will be able to see the key for that device in an action pane located to the right.

Step 8 Click the Copy icon  to copy the registration key.

Note You can skip copying the registration key and click **Next** to complete the place holder entry for the device and later, register the device. This option is useful when you're attempting to create the device first and later register it or if you're a Cisco partner installing a Proof of Value (POV) device in a customer network.

On the **Inventory** page, you will see that the device is now in the connectivity state, "Unprovisioned". Copy the registration key appearing under **Unprovisioned** to Firewall device manager to complete the onboarding process.

Step 9 Log into the Secure Firewall device manager of the device you want to onboard to CDO.

Step 10 In **System Settings**, click **Cloud Services**.

Step 11 In the CDO tile, click **Get Started**.

Step 12 In the **Region** field, select the Cisco cloud region that your tenant is assigned to:

- If you log in to defenseorchestrator.com, choose US.
- If you log in to defenseorchestrator.eu, choose EU.
- If you log in to apj.cdo.cisco.com, choose APJ.

Note This step is not applicable FDM-managed devices running version 6.4.

Step 13 In the **Registration Key** field, paste the registration key that you generated in CDO.

Cisco Defense Orchestrator

You can manage the device using Cisco Defense Orchestrator. With Cisco Defense Orchestrator, you can configure multiple devices of different types from a cloud-based configuration portal, simplifying policy consistency and deployment across your network.

- If you already have a Cisco Defense Orchestrator account, log in and obtain a registration key for the device, which you can enter below. [Log into Defense Orchestrator](#).
- If you do not have an account, learn more about what Cisco Defense Orchestrator can do for you, and how to open an account and register this device. [Learn more about Defense Orchestrator and how to register.](#)

How cloud management works

CUSTOMER → POLICIES → CLOUD → DEVICE

GET STARTED

Registration Key

Region

Please select

REGISTER

Step 14 Click **Register** and then **Accept** the Cisco Disclosure.

Step 15 Return to CDO. Select all the licenses you want to apply to the device.

For more information, see [Applying or Updating a Smart License](#). You can also click **Skip** to continue the onboarding with a 90-day evaluation license.

Step 16 Return to CDO, open the **Inventory** page and see that the device status progresses from "Unprovisioned" to "Locating" to "Syncing" to "Synced."

Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key

This procedure describes how to onboard an FDM-managed device running Version 6.6+ using a registration key. This method is the recommended way of onboarding the FDM-managed device to Cisco Defense Orchestrator and is beneficial if your FDM-managed device is assigned an IP address using DHCP. If that IP address changes for some reason, your FDM-managed device remains connected to CDO. Additionally, your FDM-managed device can have an address on your local area network, and as long as it can access the outside network, it can be onboarded to CDO using this method.



Warning If you already have a SecureX or Cisco Threat Response (CTR) account, you will need to merge your CDO tenant and SecureX/CTR account in order for your devices to be registered with SecureX. Until your accounts are merged, you will not be able to see your device's events in SecureX or benefit from other SecureX features. We **strongly** recommend merging your accounts before you create a CDO module in SecureX. Your accounts can be merged through the SecureX portal. See [Merge Accounts](#) for instructions.

If you want to onboard an FDM-managed device running version 6.4 or 6.5, see [Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key](#).

Before Onboarding

- This method of onboarding is currently available for version 6.6+ and to customers connecting to defenseorchestrator.com, defenseorchestrator.eu, and apj.cdo.cisco.com.
- **Review** [Connect Cisco Defense Orchestrator to your Managed Devices](#) for the networking requirements needed to connect CDO to your FDM-managed device.
- Make sure your device is managed by Secure Firewall device manager, not Secure Firewall Management Center.
- The device can be using a 90-day evaluation license or it can be smart-licensed. Devices running version 6.6+ can be onboarded to CDO using a registration key without unregistering any installed smart licenses.
- The device cannot already be registered with Cisco Cloud Services. See "Unregistering an FDM-Managed Device from Cisco Cloud Services" below before onboarding.
- Log in to the device's Secure Firewall device manager UI and make sure that there are no pending changes waiting on the device.
- Make sure DNS is configured properly on your FDM-managed device.
- Make sure the time services are configured on the FDM-managed device.
- Make sure the FDM-managed device shows the correct date and time otherwise the onboarding will fail.

What to do next:

Do one of these things:

- If your FDM-managed device running version 6.6+ is already registered with Cisco Cloud Services, you need to unregister the device before onboarding it. Continue to [Unregistering an FDM-Managed Device from Cisco Cloud Services, on page 16](#).
- If your device is not registered to Cisco Cloud Services, continue to [Procedure to Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key, on page 17](#).

Unregistering an FDM-Managed Device from Cisco Cloud Services

The following procedure is how to unregister the device from Cisco Cloud Services. Use this method before you onboard and FDM-managed device to CDO with a registration key.



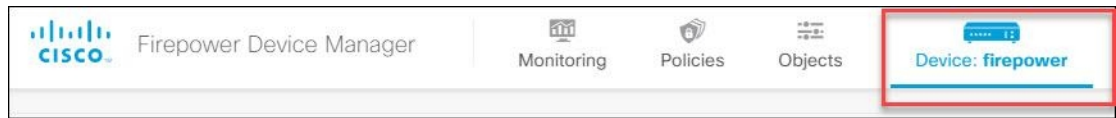
Note If you onboard a virtual FDM-managed device running version 7.0 or later, registering the virtual FDM-managed device to CDO automatically resets the performance-tiered Smart Licensing selection to **Variable**, which is the default tier. You **must** manually re-select the tier that matches the license associated with the device through the Secure Firewall device manager UI after onboarding.

Use this procedure to check and make sure it is not registered to Cisco Cloud Services:

Procedure

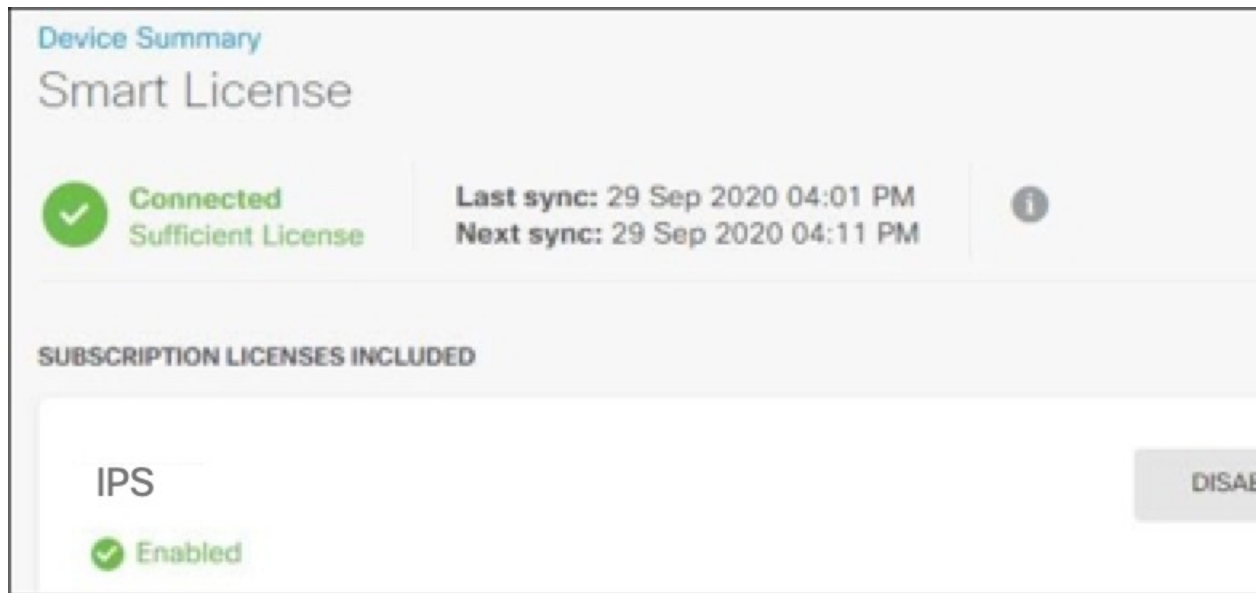
Step 1 Log on to the device using Secure Firewall device manager.

Step 2 Click the device icon in the upper tab.



Step 3 Expand the **System Settings** menu and then click **Cloud Services**.

Step 4 In the **Cloud Services** page, click the gear menu and select **Unregister Cloud Services**.



Step 5 Read the warning and click **Unregister** to unregister the device.

What to do next


If you are trying to onboard a FDM-managed device running version 6.6 or later, continue to [Procedure to Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key](#), on page 17.

Procedure to Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key

To onboard an FDM-managed device using a registration key, follow this procedure:


Procedure

Step 1 Log in to CDO.

Step 2 In the navigation pane, click **Inventory** and click the blue plus button  to **Onboard** a device.

Step 3 Click **FTD**.

Important When you attempt to onboard the FDM-managed device, Cisco Defense Orchestrator prompts you to read and accept the End User License Agreement (EULA), which is a one-time activity in your tenant. Once you accept this agreement, CDO doesn't prompt it again in subsequent onboarding. If the EULA agreement changes in the future, you must accept it again when prompted.

- Step 4** On the **Onboard FTD Device** screen, click **Use Registration Key**.
- Step 5** Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.
- Step 6** In the **Database Updates** area, the **Immediately perform security updates, and enable recurring updates** is enabled by default. This option immediately triggers a security update as well as automatically schedules the device to check for additional updates every Monday at 2AM. See [Update FTD Security Databases](#) and [Schedule a Security Database Update](#) for more information.
- Note** Disabling this option does not affect any previously scheduled updates you may have configured through Secure Firewall device manager.
- Step 7** In the **Create Registration Key** step, CDO generates a registration key.
- Note** If you move away from the onboarding screen after the key is generated and before the device is fully onboarded, you will not be able to return to the onboarding screen; however, CDO creates a placeholder for that device on the **Inventory** page. When you select the device's placeholder, you will be able to see the key for that device, on that page.
- Step 8** Click the Copy icon  to copy the registration key.
- Note** You can skip copying the registration key and click **Next** to complete the place holder entry for the device and later, register the device. This option is useful when you're attempting to create the device first and register it later, or if you're a Cisco partner installing a Proof of Value (POV) device in a customer network.
- On the **Inventory** page, you will see that the device is now in the connectivity state, "Unprovisioned". Copy the registration key appearing under **Unprovisioned** to Firewall device manager to complete the onboarding process.
- Step 9** Log into the Secure Firewall device manager of the device you are onboarding.
- Step 10** Under **System Settings**, click **Cloud Services**.
- Step 11** In the **Region** field, select the Cisco cloud region that your tenant is assigned to:
- If you log in to defenseorchestrator.com, choose US.
 - If you log in to defenseorchestrator.eu, choose EU.
 - If you log in to apj.cdo.cisco.com, choose APJ.
- Step 12** In the **Enrollment Type** area, click **Security Account** .
- Note** For devices running version 6.6, note that the Tenancy tab for CDO is titled **Security Account** and you must manually enable CDO in Secure Firewall device manager.

The screenshot shows a registration form with the following sections:

- Enrollment Type:** Two buttons, "Security/CDO Account" (highlighted with a blue border) and "Smart Licensing".
- Region:** A dropdown menu currently set to "US Region" with a help icon to its right.
- Registration Key:** A text input field with the placeholder text "Enter Registration Key".
- Service Enrollment:** A section with a blue arrow icon and the title "Service Enrollment".
 - Cisco Defense Orchestrator:** A paragraph explaining it's a cloud-based management tool. Below it is a checked checkbox labeled "Enable Cisco Defense Orchestrator".
 - Cisco Success Network:** A paragraph explaining it provides usage information. Below it is a checked checkbox labeled "Enroll Cisco Success Network".
 - A link: "Check out the [Sample Data](#) that will be sent to Cisco. [See more](#) ▾"
- Buttons:** A blue "REGISTER" button and a "Need help?" link with a question mark icon.

- Step 13** In the **Registration Key** field, paste the registration key that you generated in CDO.
- Step 14** For devices running version 6.7 or later in the Service Enrollment area, check **Enable Cisco Defense Orchestrator**.
- Step 15** Review the information about the Cisco Success Network Enrollment. If you do not want to participate, uncheck the **Enroll Cisco Success Network** checkbox.
- Step 16** Click **Register** and then **Accept** the Cisco Disclosure. Secure Firewall device manager sends the registration request to CDO.
- Step 17** Return to CDO, in the **Create Registration Key** area, click **Next**.
- Step 18** Select all licenses you want to apply to the device. Click **Next**.
- Step 19** Return to CDO, open the **Inventory** page and see that the device status progresses from "Unprovisioned" to "Locating" to "Syncing" to "Synced."

Onboard an FDM-Managed Device using the Device's Serial Number

This procedure is a simplified method of setting up and onboarding the FDM-managed devices to Cisco Defense Orchestrator. All you need is the chassis serial number or PCA serial number of the device. You can apply a smart license or use a 90-day evaluation license when onboarding the device.

Ensure that you read through the use cases to understand the concepts before you perform the [Workflow and Prerequisites to Onboard the FDM-Managed Device Using Low-Touch Provisioning](#).



Important These methods of onboarding FDM-managed devices are only available for devices running version 6.7 or higher.

Use Cases

- [Onboard an FDM-Managed Device using the Device's Serial Number, on page 19](#): Onboarding a new factory-shipped FDM-managed device that is added to a network and reached from the Internet. The initial device setup wizard is not complete on the device.
- [Onboard a Configured FDM-Managed Device using the Device's Serial Number, on page 27](#): Onboarding an already configured FDM-managed device or an upgraded device that is already added to a network and reached from the Internet. The initial device setup wizard is complete on the device.



Important If you want to use this method to onboard a device running on an older software version that is supported for your device, you need to perform a fresh installation (reimage) of the software on that device instead of an upgrade.

Related Information:

- [Terminologies and Definitions](#)
- [Troubleshoot FDM-Managed Device Onboarding using Serial Number](#)

Workflow and Prerequisites to Onboard the FDM-Managed Device Using Low-Touch Provisioning

Low-touch provisioning is a feature that allows a new factory-shipped Firepower 1000, Firepower 2100, or Secure Firewall 3100 series device to be provisioned and configured automatically, eliminating most of the manual tasks involved with onboarding the device to CDO. The low-touch provisioning is intended for remote offices or other locations where your employees are less experienced working with networking devices.

To use the low-touch provisioning process, you must onboard the device to CDO, connect it to a network that can reach the internet, and power on the device. See [Onboard a Configured FDM-Managed Device using the Device's Serial Number, on page 27](#) for more information.



Note You can power-on the device before or after onboarding it to CDO. **We recommend that you onboard the device to CDO first and power-on the device and connect it to your branch network second.** When you onboard the device in CDO, the device is associated with your CDO tenant in the Cisco cloud and CDO automatically syncs the device configuration.

You can also use this procedure to onboard a device purchased from an external vendor or onboard a device already managed by another cloud tenant in a different region. However, if the device is already registered to the external vendor's cloud tenant or a cloud tenant in a different region, CDO doesn't onboard the device but displays the "*Device serial number already claimed*" error message. In such cases, the CDO admin must unregister the device's serial number from its previous cloud tenant and then claim the CDO device in their own tenant. See [Device Serial Number Already Claimed](#) in the troubleshooting chapter.

The device **Connectivity** status changes to "Online" and the **Configuration** status changes to "Synced". The FDM-managed device is onboarded to CDO.

You can see the Status LED (Firepower 1010), SYS LED (Firepower 2100), or S LED Secure Firewall 3100 flashing green on the rear panel of the hardware. The device LED continues to flash in green when it's connected to the cloud. If the device can't connect to the Cisco cloud or loses its connectivity after being connected, you

can see the Status LED (Firepower 1010), SYS LED (Firepower 2100), or M LED (Secure Firewall 3100) flashing alternate green and amber.

See this video: [Installing Your Cisco Firepower Firewall Using Low-touch Provisioning](#) video to understand the LED indicators.



Important

If you have logged into the FDM-managed device console, SSH, or Secure Firewall Threat Defense, you would have changed the device's password during your first login. You can still use the low-touch provisioning process for onboarding the device using CDO. After you log into Secure Firewall Threat Defense, ensure that you do not complete the device setup wizard step that configures the outside interface. If you complete this step, the device is unregistered from the cloud, and you cannot use the low-touch provisioning process.

When you log into Secure Firewall Threat Defense, you will see the following screen on the dashboard.

Without proceeding further on the Secure Firewall Threat Defense UI, go to the serial number onboarding wizard and onboard the device. Here, you must select **Default Password Changed** because the device password has already been changed.

Prerequisites

Software and Hardware Requirements

The FDM-managed devices must be running software that supports serial-number-onboarding. Use the following table as a guide:

Table 1: Hardware and Software Support

Firewall Model Numbers that Support Low-Touch Provisioning	Supported Firewall Software Version	Software Package
Firepower 1000 series device models: 1010, 1120, 1140, 1150	6.7 or later	SF-F1K-TDx.x-K9
Firepower 2100 series device models: 2110, 2120, 2130, 2140	6.7 or later	SF-F2K-TDx.x-K9
Secure Firewall 3100 series device models: 3110, 3120, 3130, 3140	7.1 or later	SF-F3K-TDx.x-K9

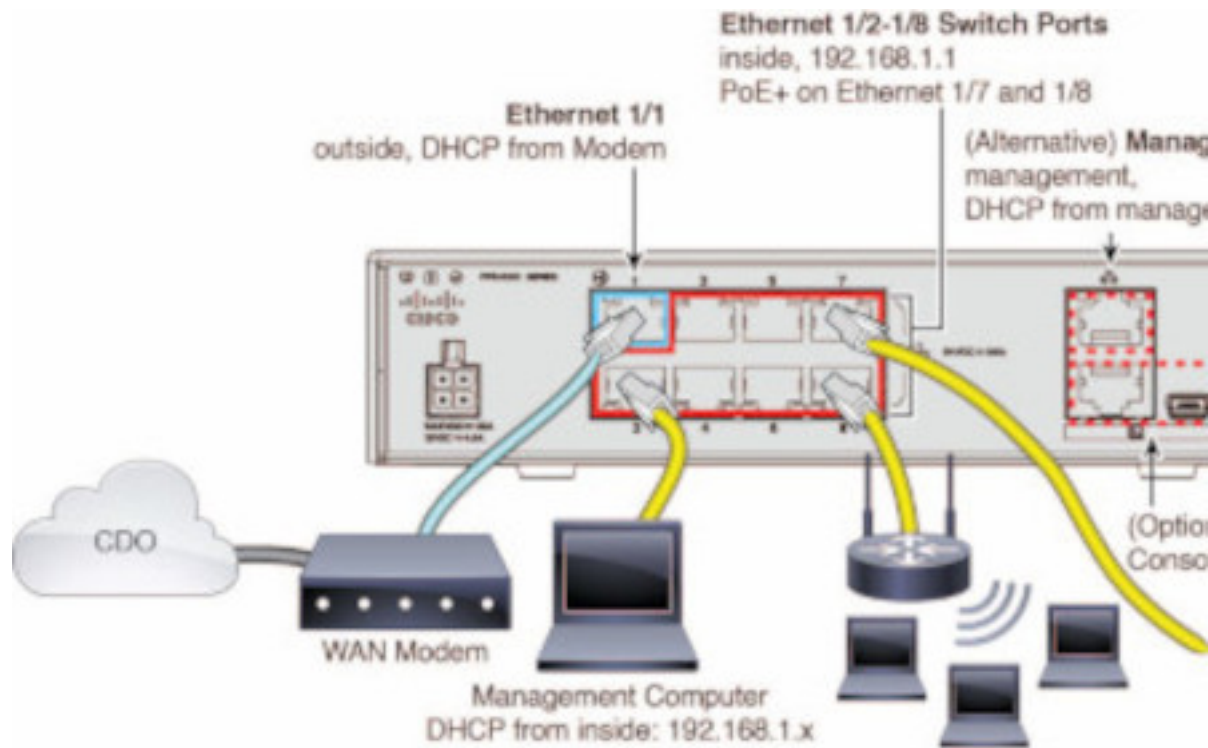
Confirm the management platforms are running the correct version.

Table 2: Support FTD Manager Versions

Manager	Supported Version
Secure Firewall Device Manager	7.0 or later
On-Prem Firewall Management Center	7.2 or later
Cloud-delivered Firewall Management Center	Not applicable

Configuration Prerequisites for Hardware Installation

- **The network at the branch office cannot use the 192.168.1.0/24 address space.** The network on Ethernet 1/1 (outside) cannot use the 192.168.1.0/24 address space. The default IP address of the Ethernet 1/2 "inside" interface on the 1000 and 2100 series devices running FDM 6.7 is 192.168.1.1 may conflict with the DHCP address allocated by your WAN modem if it's on that subnet.
 - **inside** - Ethernet 1/2, IP address 192.168.1.1
 - **outside** - Ethernet 1/1, IP address from DHCP or an address you specify during setup



If you are unable to change the outside interface settings, use Secure Firewall device manager to change the subnet on the Ethernet 1/2 "inside" interface settings to avoid conflict. For example, you could change to the following subnet settings:

- IP Address: 192.168.95.1
- DHCP server range: 192.168.95.5-192.168.95.254

To learn about the steps for configuring the physical interface, see the "[Secure Firewall Device Manager Configuration Guide](#)". In the "Interfaces" chapter, see the "Configure a Physical Interface" section.

- The threat defense device must be installed and connected to the Cisco Cloud.
- The outside or management interface of the device must be connected to a network providing DHCP addressing. Typically, the device has a default DHCP client on the outside or management interface.



Note If the management interface is connected to a network having a DHCP server, it takes precedence over the outside interface for Linux stack initiated traffic.

- Your outside or management interface needs to access to be able to access the following Security Services Exchange domains for the serial onboarding method.
 - US Region
 - api-sse.cisco.com
 - est.sco.cisco.com (common across geographies)
 - mx*.sse.itd.cisco.com (currently only mx01.sse.itd.cisco.com)

- dex.sse.itd.cisco.com (for customer success)
- eventing-ingest.sse.itd.cisco.com (for CTR and CDO)
- registration.us.sse.itd.cisco.com (allows for device registration to the regional Cisco cloud)
- EU Region
 - api.eu.sse.itd.cisco.com
 - est.sco.cisco.com (common across geographies)
 - mx*.eu.sse.itd.cisco.com (currently only mx01.eu.sse.itd.cisco.com)
 - dex.eu.sse.itd.cisco.com (for customer success)
 - eventing-ingest.eu.sse.itd.cisco.com (for CTR and CDO)
 - registration.eu.sse.itd.cisco.com (allows for device registration to the regional Cisco cloud)
- APJ Region
 - api.apj.sse.itd.cisco.com
 - est.sco.cisco.com (common across geographies)
 - mx*.apj.sse.itd.cisco.com (currently only mx01.apj.sse.itd.cisco.com)
 - dex.apj.sse.itd.cisco.com (for customer success)
 - eventing-ingest.apj.sse.itd.cisco.com (for CTR and CDO)
 - <http://registration.apj.sse.itd.cisco.com> (allows for device registration to the regional Cisco cloud)
- The outside interface of the device must have DNS access to Cisco Umbrella DNS.

Before Claiming the Device in CDO

Before claiming the device in CDO, make sure that you have the following information:

- Chassis serial number or PCA number of the threat defense device. You can find this information on the bottom of the hardware chassis or on the carton box in which your device is delivered. In the following example picture, you can see the serial number "*****X0R9" on the bottom of the Firepower 1010 chassis.



- The default password of the device.
- A smart license generated from [Cisco Smart Software Manager](#) for using the additional capabilities. However, you can complete the device onboarding using a 90-day evaluation license and later apply the smart license.

Onboard a Secure Firewall Threat Defense Device With Low-Touch Provisioning




Caution

When the device is being onboarded in CDO, we recommend that you not perform the device easy setup using the Secure Firewall device manager. This causes provisional error in CDO.

Before you begin

- The threat defense device must not be previously or currently managed by Firewall Device Manager or Management Center. If the device is currently managed by a platform, see [Onboard a Configured FDM-Managed Device using the Device's Serial Number, on page 27](#).
- If you onboard a device with the intention of managing it with an on-prem management center, the on-prem management center **must** be running version 7.4 and later.

Procedure

- Step 1** If you are onboarding a device purchased from an external vendor, you must reimage the device first. For more information, see the "Reimage Procedures" chapter of the [Cisco FXOS Troubleshooting Guide](#).
- Step 2** Log in to CDO.
- Step 3** In the navigation pane, click **Inventory** and click the blue plus button  to **Onboard** a device.

- Step 4** Click the **FTD** tile.
- Important** When you attempt to onboard a device, CDO prompts you to read and accept the End User License Agreement (EULA), which is a one-time activity in your tenant. Once you accept this agreement, CDO doesn't prompt it again in subsequent onboarding. If the EULA agreement changes in the future, you must accept it again when prompted.
- Step 5** On the **Onboard FTD Device** screen, click **Use Serial Number**.
- Step 6** In the **Select FMC** step, use the drop-down menu to select an on-prem management center that has already been onboarded to CDO. Click **Next**.
- The on-prem management center must be running version 7.4 or higher. If you do not have an on-prem management center onboarded, click +Onboard On-Prem FMC for the onboarding wizard.
- Step 7** In the **Connection** step, enter the device's serial number and device name. Click **Next**.
- Step 8** For low-touch provisioning, the device must be brand new, or has been reimaged. For the **Password Reset**, be sure to select **Yes, this new device has never been logged into or configured for a manager**. Enter a new password and confirm the new password for the device, then click **Next**.
- Step 9** For **Policy Assignment**, use the drop-down menu to select a access control policy to be deployed once the device is onboarded. If you do not have a customized policy, CDO auto-selects the default access control policy. Click **Next**.
- Step 10** Select all licenses you want to apply to the device. Click **Next**.
- Step 11** (Optional) Add labels to the device. CDO applies these labels once the device successfully onboards.

What to do next

CDO starts claiming the device, and you will see the **Claiming** message on the right. CDO continuously polls for an hour to determine if the device is online and registered to the cloud. Once it's registered to the cloud, CDO starts the initial provisioning and onboards the device successfully. The device registration can be confirmed when the LED status flashes green on the device. If the device can't connect to the Cisco cloud or lose its connectivity after being connected, you can see the Status LED (Firepower 1000) or SYS LED (Firepower 2100) flashing alternate green and amber.

If the device is still not registered to the cloud within the first one hour, a time-out occurs, and now CDO polls periodically for every 10 minutes to determine the device status and remain in **Claiming** state. When the device is turned on and connected to the cloud, you don't have to wait for 10 minutes to know its onboarding status. You can click the **Check Status** link anytime to see the status. CDO starts the initial provisioning and onboards the device successfully.



-
- Important** Suppose you have already completed the device setup wizard (see [Onboard a Configured FDM-Managed Device using the Device's Serial Number](#)), the device is unregistered from the cloud, and in this case, CDO remains in **Claiming** state. You need to complete manual registration from Secure Firewall device manager to add it to CDO. (In Secure Firewall device manager, go to **System Settings > Cloud Services** and select the **Auto-enroll with Tenancy from Cisco Defense Orchestrator** option and click **Register**). Then, click **Check Status**.
-

Onboard a Configured FDM-Managed Device using the Device's Serial Number

This procedure is for devices that have already been configured for local management. Because the device setup wizard is completed on an already configured FDM-managed device, the device is unregistered from the cloud, and you can't onboard such devices to CDO using the low-touch provisioning process.

If your device is brand new and has never been managed or configured, you can onboard the device with low-touch provisioning. See [Onboard a Secure Firewall Threat Defense Device With Low-Touch Provisioning, on page 25](#) for more information.



Note When the device is not connected to the Cisco cloud, you can see the Status LED (Firepower 1000), SYS LED (Firepower 2100), or M LED (Secure Firewall 3100) flashing alternate green and amber.

You may have completed the device setup wizard to perform the following tasks:


- The device must be running version 6.7 or later.
- Configure a static IP address on the management interface of the device. If the interfaces cannot obtain the necessary dynamic IP address, or the DHCP server does not provide the gateway route, you need to configure a static IP address.
- Obtain an address using PPPoE and configure the outside interface.
- Manage the device running version 6.7 or later device using Secure Firewall device manager or Secure Firewall Management Center.
- You have an active SecureX account. If you do not have a SecureX account, see [SecureX and CDO](#) for more information.
- Your CDO and SecureX account are merged. See [Link Your Cisco Defense Orchestrator and SecureX or Cisco XDR Tenant Accounts](#) for more information.



Important You can switch the manager of a Secure Firewall Threat Defense device from Secure Firewall device manager to Secure Firewall Management Center, or the other way. Perform the steps explained in the **Switching Between Local and Remote Management** section of the "System Management" chapter of the [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#) for the version the device runs.

If you want to onboard devices, perform the following:

Procedure

- Step 1** Review the prerequisites for onboarding here [Workflow and Prerequisites to Onboard the FDM-Managed Device Using Low-Touch Provisioning](#).
- Step 2** In the Secure Firewall device manager UI, navigate to **System Settings > Cloud Services** and select the **Auto-enroll with Tenancy from Cisco Defense Orchestrator** option and click **Register**.
- Step 3** Log in to CDO.
- Step 4** In the navigation pane, click **Inventory** and click the blue plus button  to **Onboard** a device.

- Step 5** Click the **FTD tile**.
- Step 6** On the **Onboard FTD Device** screen, click **Use Serial Number**.
- Step 7** In the **Select FMC** step, use the drop-down menu to select an on-prem management center that has already been onboarded to CDO. Click **Next**.
- The on-prem management center must be running version 7.4 or higher. If you do not have an on-prem management center onboarded, click +Onboard On-Prem FMC for the onboarding wizard.
- Step 8** In the **Connection** step, enter the device's serial number and device name. Click **Next**.
- Step 9** If the device is **not** brand new and has already been configured for management, select **Yes, this new device has never been logged into or configured for a manager** for the **Password Reset**. Click **Next**.
- Step 10** For **Policy Assignment**, use the drop-down menu to select a access control policy to be deployed once the device is onboarded. If you do not have a customized policy, CDO auto-selects the default access control policy. Click **Next**.
- Step 11** Select all licenses you want to apply to the device. Click **Next**.

CDO changes the device **Connectivity** status changes to "Online" and the **Configuration** status changes to the "Synced" state. The FDM-managed device is onboarded to CDO. You can see the Status LED (Firepower 1000), SYS LED (Firepower 2100), or M LED flashing green on the rear panel of the hardware. The device LED continues to flash in green when it's connected to Cisco Cloud. If the device can't connect to the Cisco cloud or loses its connectivity after being connected, you can see the same status LED flash alternate green and amber.

Related Information:

- [Terminologies and Definitions](#)

Onboard an FDM-Managed High Availability Pair

To onboard an Secure Firewall Threat Defense HA pair to CDO, you must onboard each device of the pair individually. Once both peers of the pair are onboarded CDO automatically combines them as a single entry in the **Inventory** page. Onboard the devices using either the device login credentials or a registration key. We recommend onboarding **both** devices with the same method. Also be aware that if you onboard a device that is in standby mode first, CDO disables the ability to deploy or read from that device. You can only read or deploy to the active device within an HA pair.



Note CDO strongly recommends onboarding devices with a registration key. Onboarding with a registration key is slightly different for Threat Defense devices running specific versions. See [Onboard an FDM-Managed HA Pair Running Version 6.4 or Version 6.5, on page 29](#) and [Onboard an FDM-Managed HA Pair Running Version 6.6 or Version 6.7 and later, on page 30](#) for more information.

Before you onboard an Threat Defense HA pair to CDO, review the following:

- Your HA pair is already formed prior to onboarding to CDO.
- Both devices are in a healthy state. The pair could be either primary/active and secondary/standby **or** primary/standby and secondary/active modes. Unhealthy devices will not successfully sync to CDO.
- Your HA pair is managed by Secure Firewall device manager, not Secure Firewall Management Center.

- Your cloud connector connects to CDO at <https://www.defenseorchestrator.com>.

Onboard an FDM-Managed High Availability Pair with a Registration Key

Be aware of the following prerequisites before you onboard an FDM-managed High Availability (HA) pair with a registration key:

- Onboarding devices that are running version 6.4 with a registration key is only supported for the US region ([defenseorchestrator.com](https://www.defenseorchestrator.com)). To connect to the EU region ([defenseorchestrator.eu](https://www.defenseorchestrator.eu)), they must onboard their HA pair with username, password, and IP address.
- Customers running version 6.5 or later, and connecting either to the US, EU, or APJC regions can use this method of onboarding.
- Devices running version 6.4 and 6.5 must not be registered with Cisco Smart Software Manager before onboarding them with a registration key. You will need to unregister the smart licenses of those FDM-managed devices before onboarding them to CDO. See [Unregister a Smart-licensed FDM-Managed Device, on page 12](#) for more information.

Onboard an FDM-Managed HA Pair Running Version 6.4 or Version 6.5


To onboard an FDM-managed HA pair running software version 6.4 or 6.5, you must onboard the devices one at a time. It does not matter if you onboard the active or standby, the primary or secondary device.



Note If you onboard either device of an HA pair with a registration key, you must onboard the other peer device in the same method.

Use the following steps for onboard an HA pair running Version 6.4 or 6.5:

Procedure

- Step 1** Onboard a peer device. See [Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key](#) to onboard the first device within the pair.
- Step 2** In the navigation pane, click **Inventory**.
- Step 3** Click the **Devices** tab to locate your device.
- Step 4** Click the **FTD** tab. Once the device is synced, select the device so it is highlighted. In the action pane located directly below **Device Details**, click **Onboard Device**.
- Step 5** Enter the **HA Peer Device Name** for the peer device that has already been onboarded. Click **Next**.
- Step 6** If you provided a smart license for the first device, CDO repopulates that license so you can use it for onboarding this current device. Click **Next**.
 - Note** If you unregistered your device's Smart License to onboard your FDM-managed device, this is where you re-apply the smart license.
- Step 7** CDO automatically generates that registration key for the device you are preparing to onboarding. Click the **Copy** icon  to copy the registration key.
- Step 8** Log into the Secure Firewall device manager UI of the device you are onboarding.
- Step 9** In **System Settings**, click **Cloud Services**.

Step 10 In the CDO tile, click **Get Started**.

Step 11 In the **Registration Key** field, paste the registration key that you generated in CDO.

Step 12 In the **Region** field, select the Cisco cloud region that your tenant is assigned to:

- If you log in to defenseorchestrator.com, choose US.
- If you log in to defenseorchestrator.eu, choose EU.
- If you log in to apj.cdo.cisco.com, Choose APJ.

Note This step is not applicable to the FDM-managed device running on version 6.4.

Step 13 Click **Register** and then **Accept** the Cisco Disclosure.

Step 14 Return to CDO and, in the **Create Registration Key** area, click **Next**.

Step 15 Click **Go to Inventory**. CDO automatically onboards the device and combines them as a single entry. Similar to the first peer device you onboard, the device status changes from "Unprovisioned" to "Locating" to "Syncing" to "Synced."

Onboard an FDM-Managed HA Pair Running Version 6.6 or Version 6.7 and later


To onboard an FDM-managed HA pair running version 6.6 or 6.7, you must onboard the device one at a time. It does not matter if you onboard the active or standby, the primary or secondary device.



Note If you onboard either device of an HA pair with a registration key, you must onboard the other peer device in the same method.

Use the following steps for onboard an HA pair running version 6.6 or 6.7:

Procedure

- Step 1** Onboard a peer device. See [Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key](#) for more information.
- Step 2** In the navigation pane, click **Inventory**.
- Step 3** Click the **Devices** tab to locate your device.
- Step 4** Click the **FTD** tab. Once the device is synced, select the device so it is highlighted. In the action pane located directly below **Device Details**, click **Onboard Device**.
- Step 5** Enter the HA Peer Device Name for the peer device that has already been onboarded. Click **Next**.
- Step 6** If you provided a smart license for the first device, CDO repopulates that license so you can use it for onboarding this current device. Click **Next**.
- Step 7** CDO automatically generates that registration key for the device you are preparing to onboarding. Click the Copy icon  to copy the registration key.
- Step 8** Log into the Secure Firewall device manager UI of the device you want to onboard to CDO.
- Step 9** Under **System Settings**, click **Cloud Services**.
- Step 10** In the **Enrollment Type** area, click **Security/CDO Account**.

Note For devices running version 6.6, note that the Tenancy tab for CDO is titled **Security Account** and you must manually enable CDO in the Secure Firewall device manager UI.

The screenshot displays the 'Service Enrollment' configuration page. At the top, there are two tabs: 'Security/CDO Account' (selected) and 'Smart Licensing'. Below this is a 'Region' dropdown menu set to 'US Region'. A 'Registration Key' field is present with the placeholder text 'Enter Registration Key'. The main section is titled 'Service Enrollment' and contains two items:

- Cisco Defense Orchestrator**: A description states it is a cloud-based management tool. A checkbox labeled 'Enable Cisco Defense Orchestrator' is checked.
- Cisco Success Network**: A description explains that enablement provides usage information and statistics to Cisco. A checkbox labeled 'Enroll Cisco Success Network' is checked.

At the bottom, there is a blue 'REGISTER' button and a link for 'Need help?'.

Step 11 In the **Region** field, select the Cisco cloud region that your tenant is assigned to:

- If you log in to defenseorchestrator.com, choose US.
- If you log in to defenseorchestrator.eu, choose EU.
- If you log in to apj.cdo.cisco.com, choose APJ.

Step 12 In the **Registration Key** field, paste the registration key that you generated in CDO.

Step 13 For devices running version 6.7 or later in the Service Enrollment area, check **Enable Cisco Defense Orchestrator**.

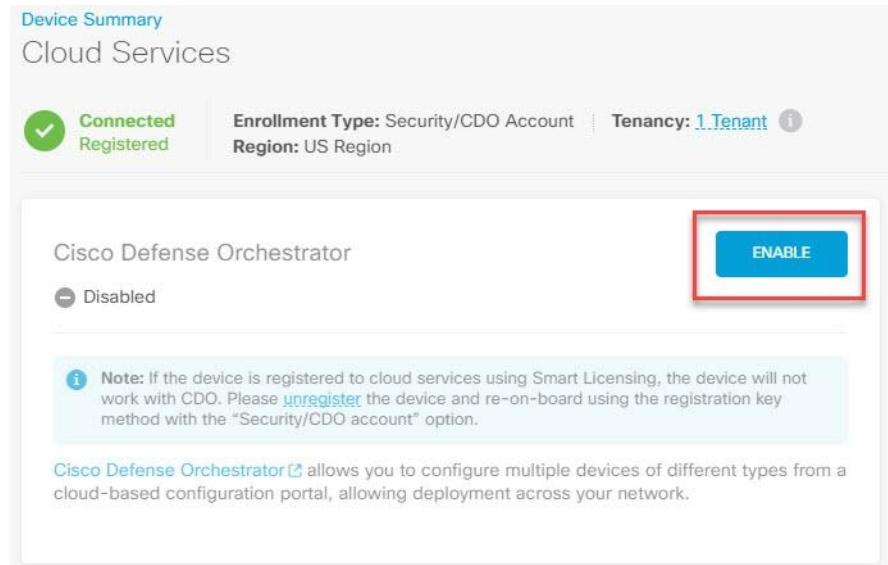
Step 14 Review the information about the Cisco Success Network Enrollment. If you do not want to participate, uncheck the **Enroll Cisco Success Network** checkbox.

Step 15 Click **Register** and then **Accept** the Cisco Disclosure. FDM sends the registration request to CDO.

Step 16 Return to CDO, in the **Create Registration Key** area, click **Next**.

Step 17 In the **Smart License** area, you can apply a smart license to the FDM-managed device and click **Next** or you can click **Skip** to continue the onboarding with a 90-day evaluation license or if the device is already smart-licensed. For more information, see [Updating an Existing Smart License of an FDM-Managed Device](#).

Note If your device is running version 6.6, you need to manually enable communication to CDO. From the device's FDM-managed UI, navigate to **System Settings > Cloud Services** and, in the **Cisco Defense Orchestrator** tile, click **Enable**.



Step 18 Return to CDO, click **Go to Inventory**. CDO automatically onboards the device and combines them as a single entry. Similar to the first peer device you onboard, the device status changes from "Unprovisioned" to "Locating" to "Syncing" to "Synced."

Onboard an FDM-Managed High Availability Pair



Note Whichever method you onboard the first device of an HA pair with, you must onboard the other peer device in the same method.

To onboard an FDM-managed HA pair that has been created outside of CDO, follow this procedure:

Procedure

- Step 1** Onboard one of the peer devices within the HA pair. Onboard the device with its [Onboard an FDM-Managed Device Using Username, Password, and IP Address, Procedure to Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key](#), or [Onboard a Configured FDM-Managed Device using the Device's Serial Number](#).
- Step 2** Once the device is synced, in the **Inventory** page, click the **Devicestab**.
- Step 3** Click the **FTD** tab.
- Step 4** Select the device. In the action pane located directly below **Device Details**, click **Onboard Device**.
- Step 5** In the pop-up window, enter the HA peer's device name and location.

- Step 6** Click **Onboard Device**. Once both devices are successfully synced to CDO, the HA pair is displayed as a single entity in the **Inventory** page.
-

Onboard an FTD Cluster

.

Onboard a Clustered Secure Firewall Threat Defense Device

Onboard a threat defense device that has already been clustered with the following procedure:

Before you begin


The following devices support clustering:

- Secure Firewall 3100 devices
- Firepower 4100 devices
- Firepower 9300 devices
- Threat Defense Virtual device (AWS, Azure, VMware, KVM, GCP)

Note the following limitations for clustered devices:

- Devices must be running at least version 6.4.
- Devices must be managed by a physical or virtual Secure Firewall Management Center.
- Firepower 4100 and Firepower 9300 devices must be clustered through the device's chassis manager.
- Secure Firewall 3100 devices, KVM, and VMware environments must be clustered through the Secure Firewall Management Center UI.
- Azure, AWS, and GCP environment clusters must be created through their own environment and onboarded to Secure Firewall Management Center.

Procedure

- Step 1** Log in to CDO.
- Step 2** In the navigation pane, click **Inventory** and click the blue plus button  to **Onboard** a device.
- Step 3** Click **FTD**.
- Step 4** Under **Management Mode**, be sure **FTD** is selected.
- By selecting **FTD**, you are retaining Secure Firewall Management Center as the managing platform. If you select **FDM**, this switches the manager from Secure Firewall Management Center to a local manager such as the Firewall Device Manager or cloud-delivered Firewall Management Center. Note that Switching managers resets all existing policy configurations except for interface configurations and you must re-configure policies after you onboard the device.
- Step 5** On the **Onboard FTD Device** screen, click **Use CLI Registration Key**.

- Step 6** Enter the device name in the **Device Name** field. This could be the hostname of the device or any other name you choose.
- Step 7** In the Policy Assignment step, use the drop-down menu to select an access control policy to deploy once the device is onboarded. If you have no policies configured, select the **Default Access Control Policy**.
- Step 8** Specify whether the device you are onboarding is a physical or virtual device. If you are onboarding a virtual device, you must select the device's performance tier from the drop-down menu.
- Step 9** Select the essentials licenses you want applied to the device. Click **Next**.
- Step 10** CDO generates a command with the registration key. Paste the entire registration key as is into the device's CLI.
- Step 11** The device starts to onboard. As an optional step, you can add labels to your device to help sort and filter the Inventory page. Enter a label and select the blue plus button. .

What to do next

Once the device is synchronized, CDO automatically detects that the device is clustered. From here, select the device you just onboarded from the Inventory page and select any of the options listed under the Management pane located to the right. We strongly recommend the following actions:

- If you did not already, create a custom access control policy to customize the security for your environment. See [FDM-Managed Access Control Policy](#) for more information.
- Enable Cisco Security Analytics and Logging (SAL) to view events in the CDO dashboard **or** register the device to an Secure Firewall Management Center for security analytics.

Applying or Updating a Smart License

Applying a New Smart License to an FDM-Managed Device

Perform one of the following procedures to Smart License the FDM-managed device:

- Smart license an FDM-managed device when onboarding using a registration key.
- Smart license an FDM-managed device after onboarding the device using a registration key or the administrator's credentials.

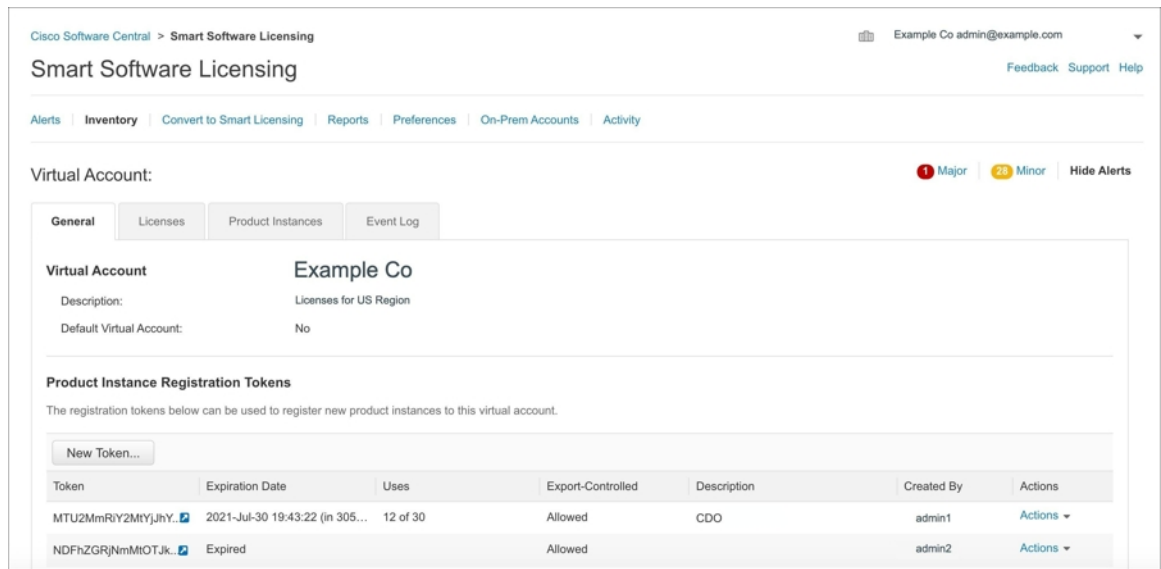


Note The FDM-managed device may be using a 90-day evaluation license, or the license could be unregistered.

Smart-License an FDM-Managed Device When Onboarding Using a Registration Key

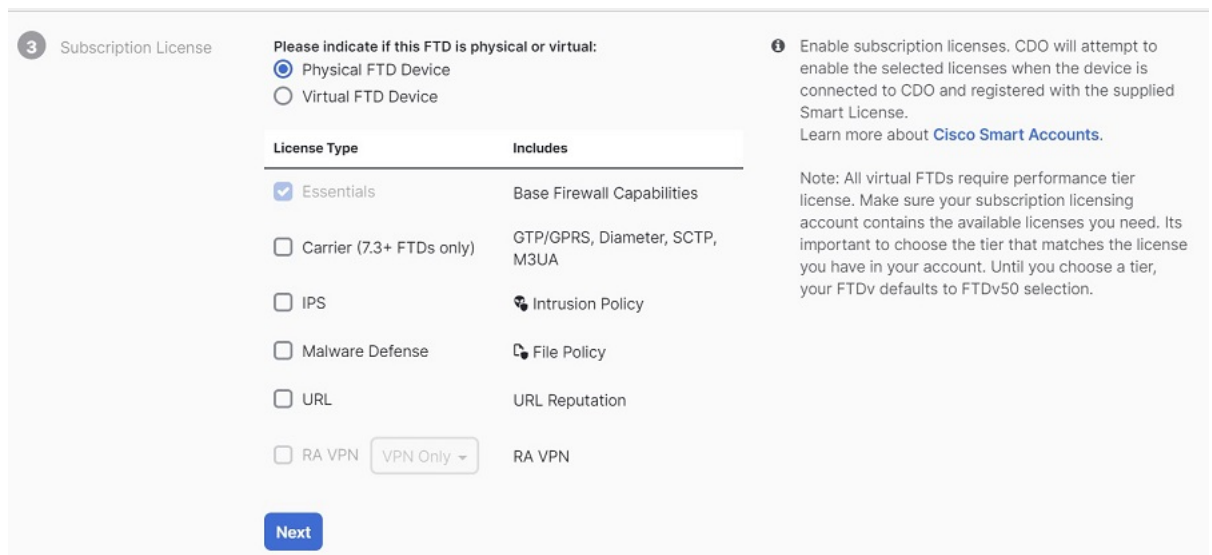
Procedure

- Step 1** Log on to the [Cisco Smart Software Manager](#) and generate a new Smart License key. Copy the newly generated key. You can watch the [Generate Smart Licensing](#) video for more information.



Step 2 Begin onboarding an FDM-managed device using a registration key. For more information, see [Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key](#) or [Onboard an FDM-Managed Device Running Software Version 6.4 or 6.5 Using a Registration Key](#).

Step 3 In step 4 of the onboarding wizard, in the **Smart License here** box, paste the Smart License in the **Activate** field and click **Next**.

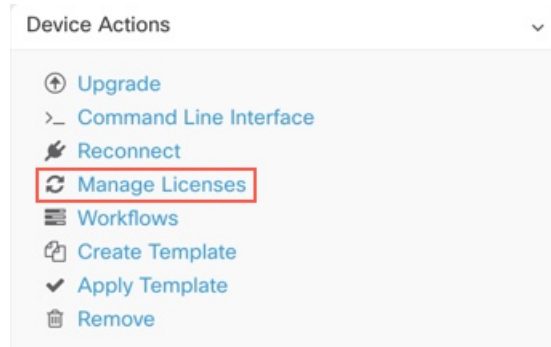


Step 4 Click **Go to Inventory page**.

Step 5 Click the **FTD** tab and see the progress of the onboarding process. The device starts synchronizing and applies the Smart License.

You should see that the device is now in the **Online** connectivity state. If the device is not in the online connectivity state, look in the Device Actions pane on the right and click **Manage Licenses > Refresh Licenses** to update the connectivity state.

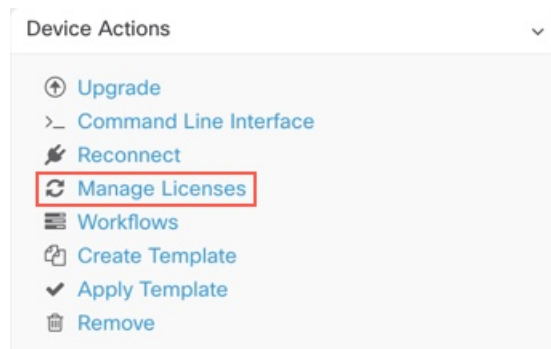
- Step 6** After applying the Smart License successfully to the FDM-managed device, click the **Manage Licenses**. The device status shows "**Connected, Sufficient License**." You can enable or disable the optional licenses. For more information, see [FDM-Managed Device Licensing Types](#).



Smart-License an FDM-Managed Device After Onboarding the Device Using a Registration Key or its Credentials

Procedure

- Step 1** In the navigation pane, click **Inventory**.
- Step 2** Click the **Devices** tab to locate the device.
- Step 3** Click the **FTD** tab and select the device that you want to license.
- Step 4** In the **Device Actions** pane on the right, click **Manage Licenses**.



- Step 5** Follow the on-screen instructions and enter the Smart License generated from Cisco Smart Software Manager.
- Step 6** Paste the new license key in the box and click **Register Device**. After synchronizing with the device, the connectivity state changes to 'Online'. After applying the Smart License successfully to the FDM-managed device, the device status shows "**Connected, Sufficient License**." You can enable or disable the optional licenses. For more information, see [FDM-Managed Device Licensing Types](#).

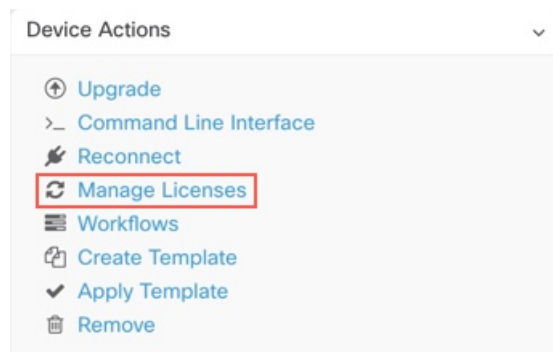
Updating an Existing Smart License of an FDM-Managed Device

You can apply a new Smart License to an FDM-managed device which is Smart Licensed. Based on the method you have selected for onboarding your device, select the appropriate procedure:

Change the Smart License Applied to an FDM-Managed Device Onboarded Using a Registration Key

Procedure

-
- Step 1** Remove the corresponding FDM-managed device from Cisco Defense Orchestrator.
 - Step 2** Log into the Secure Firewall device manager for that device and unregister the Smart License. For more information, see [Unregister a Smart-licensed FDM-Managed Device](#).
 - Step 3** In CDO, onboard the FDM-managed device again using a registration key. For more information, see [Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key](#).
 - Step 4** Click the **Devices** tab to locate the device.
 - Step 5** Click the tab.
 - Step 6** Apply the new Smart License during the onboarding process or by looking in the **Device Actions** pane on the right and clicking **Manage Licenses**.



Change the Smart License Applied to an FDM-Managed Device Onboarded Using its Credentials

Procedure

-
- Step 1** Log into the Secure Firewall device manager for that device and unregister the Smart License. For more information, see [Onboard an FDM-Managed Device Running Software Version 6.6+ Using a Registration Key](#).
 - Step 2** Apply the new Smart License to the FDM-managed device in Secure Firewall device manager.
 - a. In the **Smart License** area, click **View Configuration**.
 - b. Click **Register Now** and follow the onscreen instructions.

- Step 3** On the **Inventory** page in CDO, click the **Devices** tab.
- Step 4** Click the **FTD** device. Check the FDM-managed device configuration for changes so that CDO can make a copy of the FDM-managed device's deployed configuration and save it to the CDO database. For more information, see [Reading, Discarding, Checking for, and Deploying Configuration Changes](#).
-

CDO Support for DHCP Addressing of FDM-Managed Devices

What happens if the IP address used by my FDM-managed device changes?

Cisco Defense Orchestrator (CDO) has many Adaptive Security Appliance (ASA) and FDM-managed device customers who have onboarded devices using the IP address provided by their service provider using DHCP.

If the IP address of the device for any reason, whether that is a change in the static IP address or a change in the IP address due to DHCP, you can [change the IP address that CDO uses to connect to the device](#) and then reconnect the device.

The field, expressed concerns regarding the case of branch deployed FDM-managed devices managed by CDO, a static IP is required on the outside interface of the FDM-managed device, which, in the view of some SE's, precludes using CDO as a management solution when the FDM-managed device has a DHCP address configured for the outside interface.

However, this situation does not impact customers that have VPN tunnels to remote branch firewalls, and we know that a vast majority of customers have Site to Site tunnels from their Branch Offices back to their datacenters. In the case that Site-to -Site VPN is used to connect to the central site from devices, DHCP on the outside interface is not a concern since CDO (and any management platform) can connect to the FW via its inside, statically addressed, interface (if so configured). This is a recommended practice and we have CDO customers with many (+1000) devices using this deployment mode.

Also, the fact that an interface IP address is being issued via DHCP does not preclude the customer from managing the device using that IP. Again, this is not optimal, but the experience of periodically having to potentially change the IP address in CDO has not been seen as a hurdle to customers. This situation is not exclusive to CDO and happens with any manager using the outside interface including ASDM, FDM or SSH.

FDM-Managed Device Licensing Types

Smart License Types

The following table explains the licenses available for FDM-managed devices.

Your purchase of an FDM-managed device automatically includes a base license. All additional licenses are optional.

License	Duration	Granted Capabilities
License (automatically included)	Perpetual	<p>All features not covered by the subscription term licenses.</p> <p>You must also specify whether to Allow export-controlled functionality on the products registered with this token. You can select this option only if your country meets export-control standards. This option controls your use of advanced encryption and the features that require advanced encryption.</p>
	Term-based	<p>Intrusion detection and prevention-Intrusion policies analyze network traffic for intrusions and exploits and, optionally, drop offending packets.</p> <p>File control-File policies detect and, optionally, block users from uploading (sending) or downloading (receiving) files of specific types. AMP for Firepower, which requires a Malware license, allows you to inspect and block files that contain malware. You must have the license to use any type of File policy.</p> <p>Security Intelligence filtering-Drop selected traffic before the traffic is subjected to analysis by access control rules. Dynamic feeds allow you to drop connections based on the latest intelligence immediately.</p>
Malware	Term-based	<p>File policies that check for malware, which use Cisco Advanced Malware Protection (AMP) with AMP for Firepower (network-based Advanced Malware Protection) and Cisco Threat Grid.</p> <p>File policies can detect and block malware in files transmitted over your network.</p>

License	Duration	Granted Capabilities
URL License	Term-based	Category and reputation-based URL filtering. You can perform URL filtering on individual URLs without this license.
	Term-based or perpetual based on the license type	Remote access VPN configuration. Your essentials license must allow export-controlled functionality to configure RA VPN. You select whether you meet export requirements when you register the device. Firepower Device Manager can use any valid AnyConnect license. The available features do not differ based on the license type. If you have not already purchased one, see Licensing Requirements for Remote Access VPN. Also, see the Cisco AnyConnect Ordering Guide, http://www.cisco.com/.../orderingguide/anyconnect/

Virtual FDM-Managed Device Tiered Licenses

Version 7.0 introduces support for performance-tiered Smart Licensing for virtual FDM-Managed devices based on throughput requirements and RA VPN session limits. When the virtual FDM-Managed device is licensed with one of the available performance licenses, two things occur: session limits for RA VPNs are determined by the installed virtual FDM-Managed device platform entitlement tier, and enforced via a rate limiter.

CDO **does not** fully support tiered smart licensing at this time; see the following limitations:

- You cannot modify the tiered license through CDO. You must make the changes in the Secure Firewall device manager UI.
- If you register a virtual FDM-Managed device to be managed by the cloud-delivered Firewall Management Center, the tiered license selection automatically resets to **Variable**, which is the default tier.
- If you onboard a virtual FDM-Managed device running version 7.0 or later, and select a license that is **not** a default license during the onboarding process, the tiered license selection automatically resets to **Variable**, which is the default tier.

We strongly recommend selecting a tier for your virtual FDM-Managed device license after onboarding your device to avoid the issues listed above. See [Managing Smart Licenses](#) for more information.

Viewing Smart-Licenses for a Device

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab to locate your device.
- Step 3** Click the **FTD** tab.
- Step 4** Select an FDM-managed device to view its current license status.
- Step 5** In the **Device Actions** pane on the right, click **Manage Licenses**. The **Manage Licenses** screen provides the following information:
- **Smart License Agent status:** Shows whether you're using a 90-day evaluation license, or if you have registered with the Cisco Smart Software Manager. The Smart License Agent status can be the following:
 - **"Connected," "Sufficient Licenses"** - The device has contacted and registered successfully with the License Authority, which has authorized the license entitlements for the appliance. The device is now In-Compliance.
 - **Out-of-Compliance** - There's no available license entitlement for the device. Licensed features continue to work. However, you can either purchase or free up extra entitlements to become In-Compliance.
 - **Authorization Expired** - The device hasn't communicated with the Licensing Authority in 90 or more days. Licensed features continue to work. In this state, the Smart License Agent retries its authorization requests. If a retry succeeds, the agent enters either an Out-of-Compliance or Authorized state and begins a new Authorization Period. Try manually synchronizing the device.
 - **License Registration:** Allows you to apply smart-license to an already onboarded FDM-managed device. Once registered, you can see the status of the connection to the Cisco Smart Software Manager and the status for each type of license.
 - **License Status:** Shows the status of the optional licenses available for your FDM-managed device. You can enable a license to use the features controlled by the license.
-

Enabling or Disabling Optional Licenses

You can enable (register) optional licenses on FDM-managed devices that are using a 90-day evaluation license or a full license. You must enable a license to use the features controlled by the license.

If you no longer want to use the features covered by an optional term license, you can disable (release) the license. Disabling the license releases it in your Cisco Smart Software Manager account so that you can apply it to another device.

In evaluation mode, you can also enable evaluation versions of the optional licenses and perform all operations. In this mode, the licenses aren't registered with Cisco Smart Software Manager until you register the device.



Note You can't enable the license in evaluation mode.

Before you begin

Before disabling a license, ensure that you are not using it. Rewrite or delete any policies that require the license.

For units operating in a high availability configuration, you enable or disable licenses on the active unit only. The change is reflected in the standby unit the next time you deploy the configuration when the standby unit requests (or frees) the necessary licenses. When enabling licenses, you must ensure that your Cisco Smart Software Manager account has sufficient licenses available, or you could have one unit compliant while the other unit is non-compliant.

To enable or disable optional licenses, follow this procedure:

Procedure

-
- Step 1** In the **Inventory** page, select the FDM-managed device that you want and click **Manage Licenses** in **Device Actions pane**. The **Manage Licenses** screen appears.
- Step 2** Click the slider control for each optional license to enable or disable the license. The status of the license shows OK when enabled.
- **Enabled:** Registers the license with your Cisco Smart Software Manager account and enable the controlled features. You can now configure and deploy policies controlled by the license.
 - **Disabled:** Unregisters the license with your Cisco Smart Software Manager account and disables the controlled features. You cannot configure the features in new policies, nor can you deploy policies that use the feature.
- Step 3** Click **Save** to save the changes.
-

Impact of Expired or Disabled Optional Licenses

If an optional license expires, you can continue using features that require the license. However, the license is marked out of compliance, and you need to purchase the license and add it to your account to bring the license back into compliance.

If you disable an optional license, the system reacts as follows:

- **Malware license:** The system stops querying the AMP cloud and also stops acknowledging retrospective events sent from the AMP cloud. You cannot re-deploy existing access control policies if they include file policies that apply malware inspection. Note that for a very brief time after a Malware license is disabled, the system can use existing cached file dispositions. After the time window expires, the system assigns a disposition of Unavailable to those files.
- : The system no longer applies intrusion or file-control policies. For Security Intelligence policies, the system no longer applies the policy and stops downloading feed updates. You cannot re-deploy existing policies that require the license.
- **URL:** Access control rules with URL category conditions immediately stop filtering URLs, and the system no longer downloads updates to URL data. You cannot re-deploy existing access control policies if they include rules with category and reputation-based URL conditions.
- : You cannot edit the remote access VPN configuration, but you can remove it. Users can still connect using the RA VPN configuration. However, if you change the device registration so that the system is

no longer export compliant, the remote access VPN configuration stops immediately, and no remote users can connect through the VPN.

Create and Import an Firewall Device Manager Model

Cisco Defense Orchestrator provides the ability to export the complete configuration of an FDM-managed device on a CDO tenant to a JSON file format. You can then import this file to another tenant as an Firewall device manager model and apply it to a new device on that tenant. The feature is beneficial when you want to use an FDM-managed device's configuration on different tenants that you manage.



Note If the FDM-managed device contains rulesets, the shared rules associated with the rulesets are modified as local rules when exporting the configuration. Later, when the model is imported to another tenant and applied to an FDM-managed device, you'll see the local rules in the device.

Export FDM-Managed Device Configuration

The export configuration functionality is unavailable if your FDM-managed device has the following configuration:


- High Availability
- Snort 3 enabled

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab to locate the device or the **Templates** tab to locate the model device.
- Step 3** Click the **FTD** tab.
- Step 4** Select an FDM-managed device and in the **Device Actions** on the right pane, click **Export Configuration**.
-

Import FDM-Managed Device Configuration

Procedure

- Step 1** In the **Inventory** page, click the blue plus () button to import the configuration.
- Step 2** Click **Import** to import configuration for offline management.
- Step 3** Select the **Device Type** as **FTD**.
- Step 4** Click **Browse** and select the configuration file (JSON format) to upload.
- Step 5** Once the configuration is verified, you're prompted to label the device or service. See [Labels and Label Groups](#) for more information.
- Step 6** After labeling your model device, you can view it in the **Inventory** list.

Note Depending on the size of the configuration and the number of other devices or services, it may take some time for the configuration to be analyzed.

Delete a Device from CDO

Use the following procedure to delete a device from CDO:

Procedure

- Step 1** Log into CDO.
- Step 2** Navigate to the **Inventory** page.
- Step 3** Locate the device you want to delete and check the device in the device row to select it.
- Step 4** In the Device Actions panel located to the right, select **Remove**.
- Step 5** When prompted, select **OK** to confirm the removal of the selected device. Select **Cancel** to keep the device onboarded.

Note that both devices in an FDM-managed HA pair must be deleted simultaneously. Click the FDM-managed HA pair name and not the individual peers.

Import Configuration for Offline Device Management

Importing a device's configuration for offline management allows you to review and optimize a device's configuration without having to work on a live device in your network. CDO also refers to these uploaded configuration files as "models."

You can import the configurations of these devices to CDO:

- FDM-Managed Device. See [Create and Import an Firewall Device Manager Model](#).
- Cisco IOS devices like the Aggregation Services Routers (ASR) and Integrated Services Routers (ISRs).

Backing Up FDM-Managed Devices

You can use Cisco Defense Orchestrator to back up an FDM-managed device's system configuration so that you can restore the device to a previous state. Backups include the configuration only, and not the system software. If you need to completely reimage the device, you need to reinstall the software, then you can upload a backup and recover the configuration. CDO saves the last 5 backups made for a device. When a new backup occurs, the oldest backup is deleted in order to store the newest backup.



Note The backup does not include the management IP address configuration. Thus, when you recover a backup file, the management address is not replaced from the backup copy. This ensures that any changes you made to the address are preserved, and also makes it possible to restore the configuration on a different device on a different network segment.

The configuration database is locked during backup. You cannot make configuration changes during a backup, although you can view policies, dashboards, and so forth. During a restore, the system is completely unavailable.

To make backup schedules across your devices consistent, you can configure your own default backup schedule. When you schedule a backup for a particular device, you can use your own default settings or change them. You can schedule recurring backups with cadences from daily to once a month and you can perform an on-demand backup. You can also download backups and then use the Threat Defense device manager to restore them.

Requirements and best practice for backing up and restoring an FDM-managed device using CDO

- CDO can backup FDM-managed devices running software version 6.5 and later.
- The FDM-managed device must be onboarded to CDO using a registration key.
- You can restore a backup onto a replacement device only if the two devices are the same model and are running the same version of the software, including the build number, not just the same point release. For example, a backup of an FDM-managed device running software version 6.6.0-90 can only be restored to an FDM-managed device running 6.6.0-90. Do not use the backup and restore process to copy configurations between appliances. A backup file contains information that uniquely identifies an appliance, so that it cannot be shared in this manner.
- For the Secure Firewall Threat Defense backup functionality to work in CDO, threat defense needs to access one of these CDO URLs based on your tenant region.
 - edge.us.cdo.cisco.com
 - edge.eu.cdo.cisco.com
 - edge.apj.cdo.cisco.com
- Ensure that port 443 has external and outbound access for the HTTPS protocol. If the port is blocked behind a firewall, the backup and restore process may fail.

Best Practice

The device you are going to backup should be in the Synced state in CDO. CDO backs up the configuration of the device *from the device* not from CDO. So, if the device is in a Not Synced state, changes on CDO will not be backed up. If the device is in a Conflict Detected state, those changes will be backed up.

Related Information:

- [Configure a Default Recurring Backup Schedule for all FDM-Managed Devices](#)
- [Configure a Recurring Backup Schedule for a Single FDM-Managed Device](#)
- [Back up an FDM-Managed Device On-Demand](#)
- [Download the Device Backup](#)
- [Edit a Backup](#)

- [Restore a Backup to an FDM-Managed Device, on page 50](#)

Back up an FDM-Managed Device On-Demand

This procedure describes how to backup an FDM-managed device so that it can be restored if need be.

Before you Begin

Review these [Backing Up FDM-Managed Devices](#) before you backup up an FDM-managed device.

Procedure

Procedure

- Step 1** (Optional) Create a [change request](#) for the backup.
- Step 2** In the navigation bar, click **Inventory**.
- Step 3** Click the **Devices** tab.
- Step 4** Click the **FTD** tab and select the device you want to backup.
- Step 5** In the **Device Actions** pane on the right, click **Manage Backups**.
- Step 6** Click **Backup Now**. The Device enters the Backing Up configuration state.
- When the backup is done, the Cisco Defense Orchestrator displays the device's configuration state it was in before the backup started. You can also open the change log page to look for a recent change log record with the description, "Backup completed successfully."
- If you created a change request in step 1, you can also filter by that value to find the change log entry.
- Step 7** if you created a change request in step 1, clear the change request value so you do not inadvertently associated more changes with the change request.
-

Configure a Recurring Backup Schedule for a Single FDM-Managed Device

Before you Begin

Review these [Backing Up FDM-Managed Devices](#) before you backup up an FDM-managed device.

Procedure

Procedure


- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and select the device you want to backup.
- Step 4** In the **Device Actions** pane on the right, click **Manage Backups**.

- Step 5** In the **Device Backups** page, click **Set Recurring Backup** or click the schedule in the Recurring Backup field. CDO presents the default backup schedule for all FDM-managed devices on your tenant. See [Configure a Default Recurring Backup Schedule for all FDM-Managed Devices](#) for more information.
- Step 6** Select the time of day, in 24-hour time, you want the backup to occur. Note that you schedule the time in Coordinated Universal Time (UTC) time.
- Step 7** In the Frequency field, select daily, weekly, or monthly backup.
- Daily backups: Give the scheduled backup a name and a description.
 - Weekly backups: Check the days of the week on which you want the backup to occur. Give the scheduled backup time a name and a description.
 - Monthly backups: Click in the Days of Month field and add whichever days of the month you want to the schedule the backup. Note: If you enter day 31 but a month doesn't have 31 days in it, the backup will not take place. Give the scheduled backup time a name and a description.
- Step 8** Click **Save**. Notice that on the Device Backup page, the Recurring Backup field is replaced by the backup schedule you set and reflects your local time.
-

Download the Device Backup

This procedure describes how to download a .tar file containing a backup of an FDM-managed device.

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and the device whose backup you want to download.
- Step 4** In the Actions pane on the right, click **Manage Backups**.
- Step 5** Select the backup you want to download and, in its row, click the **Generate Download Link** button . The button changes to read, "Download Backup Image."
- Step 6** The button now reads **Download Backup Image**. Do one of these things:
- If you are on a device that can also reach the Firewall device manager of the device you want to restore, click the **Download Backup Image** button and save the downloaded file. Save it with a name that you will remember.
 - If you are not on a device that can also reach the FDM of the device you want to restore:
 - a. Right-click the **Download Backup Image** button and copy the link address.

Important The link address expires 15 minutes after you click the Generate Download Link button.
 - b. Open a browser on a device that will also reach the Firewall device manager of the Secure Firewall Threat Defense you want to restore the image to.

- c. Enter the download link into the browser address bar and download the backup file to that device. Save it with a name that you will remember.
-

Edit a Backup

This procedure allows you to edit the name or description of a successful FDM-managed device download.


Procedure

- Step 1** In the navigation bar, click **Inventory**.
 - Step 2** Click the **Devices** tab.
 - Step 3** Click the **FTD** tab and select the device you want to edit.
 - Step 4** In the Actions pane on the right, click **Manage Backups**.
 - Step 5** Select the backup you want to edit and its row, click the edit icon .
 - Step 6** Change the name or description of the backup. You can see the new information in the Device Backups page.
-

Delete a Backup

CDO saves the last 5 backups made for a device. When a new backup occurs, the oldest backup is deleted in order to store the newest backup. Deleting existing backups may help you manage which backups are kept and which are deleted.

Procedure

- Step 1** In the navigation bar, click **Inventory**.
 - Step 2** Click the **Devices** tab.
 - Step 3** Click the **FTD** tab and select the device you want to delete.
 - Step 4** In the Actions pane on the right, click **Manage Backups**.
 - Step 5** Select the backup you want to delete and its row, click the trash icon .
 - Step 6** Click **OK** to confirm.
-

Managing Device Backup

Backups of FDM-managed devices you produce using Cisco Defense Orchestrator can be seen in the Device Backups page:

Procedure

- Step 1** In the navigation bar, click **Inventory**.
 - Step 2** Click the **Devices** tab.
 - Step 3** Click the **FTD** tab.
 - Step 4** Click the filter icon and check FDM under Devices/Services to see only FDM-managed devices in the device table.
 - Step 5** Select the device you want.
 - Step 6** In the **Device Actions** pane, click **Manage Backups**. You will see up to 5 of the latest backups made of that device.
-

What to do next

See [Restore a Backup to an FDM-Managed Device, on page 50](#) if you want to restore a backup.

Restore a Backup to an FDM-Managed Device

Review this information before you restore a backup of an FDM-managed managed threat defense device.

- Review these [Backing Up FDM-Managed Devices](#) before you restore a backup to an FDM-managed threat defense device.
- If the backup copy you want to restore is not already on the device, you must **upload** the backup first before restoring it.
- During a restore, the system is completely unavailable. After the backup is restored, the device reboots.
- This procedure assumes that you have an existing backup of the device ready to be restored to the device.
- You cannot restore a backup if the device is part of a high availability pair. You must first break HA from the Device > High Availability page, then you can restore the backup. If the backup includes the HA configuration, the device will rejoin the HA group. Do not restore the same backup on both units, because they would then both go active. Instead, restore the backup on the unit you want to go active first, then restore the equivalent backup on the other unit.




Note The backup does not include the management IP address configuration. Thus, when you recover a backup file, the management address is not replaced from the backup copy. This ensures that any changes you made to the address are preserved, and also makes it possible to restore the configuration on a different device on a different network segment.

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab.

Step 3 Click the **FTD** tab and select the device you want to restore.

Step 4 In the **Device Actions** pane on the right, click **Manage Backups**.

Step 5 Select the backup you want to restore. In its row, click the **Generate Download Link** button .

Note The link address expires 15 minutes after you click the Generate Download Link button.

Step 6 The button now reads **Download Backup Image**. Do one of these things:

- If you are on a device that can also reach the Firewall device manager of the device you want to restore, click the **Download Backup Image** button and save the downloaded file. *Save it with a name that you will remember.*
- If you are not on a device that can also reach the firewall device manager of the device you want to restore:
 - a. Right-click the **Download Backup Image** button and copy the link address.
 - b. Open a browser on a device that will also reach the firewall device manager you want to restore the image to.
 - c. Enter the download link into the browser address bar and download the backup file to that device. *Save it with a name that you will remember.*

Step 7 Log on to Firewall device manager for the device you want to restore.

Step 8 Open version 6.5 or higher of the [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#). Navigate to the System Management chapter, and search for **Restoring a Backup**. Follow those instructions to restore the image you just downloaded to your FDM-managed device.

Tip You will need to upload your image to firewall device manager in order to restore it.

Step 9 Follow the prompts in firewall device manager. When the restore starts, your browser is disconnected from firewall device manager. After the restore has finished, the device reboots.

Related Information:

- [Backing Up FDM-Managed Devices](#)
- [Back up an FDM-Managed Device On-Demand](#)
- [Configure a Recurring Backup Schedule for a Single FDM-Managed Device](#)
- [Download the Device Backup](#)
- [Edit a Backup](#)

FDM Software Upgrade Paths

Upgrading FDM Versions

If you use CDO to upgrade your FDM-managed firewalls, CDO determines which version you can upgrade to and you will not need this topic. If you maintain your own repository of FDM images and upgrade your FDM-managed devices using your own images, this topic explains what upgrade paths are available to you.

You can upgrade an FDM-managed device directly from one major or maintenance version to another; for example, Version 6.4.0 > 6.5.0, or Version 6.4.0 > 7.0.1. You do not need to be running any specific patch level.

If direct upgrade is not possible, your upgrade path must include intermediate versions, such as Version 6.4.0 > 7.0.0 > 7.1.0.

Table 3: Upgrade Paths for Major Releases

Target Version	Oldest Release you can Upgrade to the Target Version
7.3.x	7.0.0
7.2.x	6.6.0
7.1.x	6.5.0
7.0.x	6.4.0
6.7.x	6.4.0
6.6.x	6.4.0
6.5.0	6.4.0

Patching FDM-Managed Devices

You cannot upgrade directly from a patch of one version to a patch of another version, such as from Version 6.4.0.1 > 6.5.0.1. You must upgrade to the major release first, and then patch that release. For example you must upgrade from Version 6.4.0.1 > 6.5.0 > 6.5.0.1.

Firepower Hotfixes

CDO does not support hotfix updates or installations. If there is a hotfix available for your device model or software version, we strongly recommend using the configured manager's dashboard or UI. After a hotfix is installed on the device, CDO detects out of band configuration changes.

Removing FDM Upgrades

You cannot use CDO to remove or downgrade any release type, whether major, maintenance, or patch.

Starting with Secure Firewall Threat Defense defense Version 6.7.0, you can use Firepower Device Manager or the FTD CLI to revert a successfully upgraded device to its state just before the last major or maintenance upgrade (also called a snapshot). Reverting after patching necessarily removes patches as well. After reverting,

you must reapply any configuration changes you made between **upgrading** and reverting. **Note that to revert a major or maintenance upgrade to FDM Version 6.5.0 through 6.6.x, you must reimage.** See the "System Management" section of a [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#) for more information.

Removing FDM Patches

You cannot remove an FDM patch with either CDO or FDM. To remove a patch, you must reimage to a major or maintenance release.

Snort Upgrade

Snort is the main inspection engine for the product and is packaged into the Secure Firewall Threat Defense software for your convenience. Version 6.7 introduces an update to the package that you can upgrade to, or revert from, at any time. Although you can switch Snort versions freely, some intrusion rules in Snort 2.0 might not exist in Snort 3.0, and vice versa. We strongly recommend reading about the differences in the Firepower Device Manager Configuration Guide for Version 6.7.0 for more information.

To proceed with upgrading your FDM-managed device to use Snort 3 or to revert from Snort 3 back to Snort 2 from the CDO UI, see [Upgrade to Snort 3.0](#) and [Revert From Snort 3.0 for FDM-Managed Device](#) respectively.

Other Upgrade Limitations

2100 Series Devices

CDO can upgrade Firepower 2100 series devices only if they are running appliance mode.

- Firepower Threat Defense devices are always in appliance mode.

What to do next

See the "[Cisco Firepower 2100 Getting Started Guide](#)" for a more detailed discussion of these commands.

4100 and 9300 Series Devices

CDO does not support the upgrade for the 4100 or 9300 series devices. You must upgrade these devices outside of CDO.

Related Information:

- [FDM-Managed Device Upgrade Prerequisites](#)
- [Upgrade a Single FDM-Managed Device](#)
- [Bulk FDM-Managed Devices Upgrade](#)
- [Upgrade an FDM-Managed High Availability Pair](#)

FDM-Managed Device Upgrade Prerequisites

Cisco Defense Orchestrator (CDO) provides a wizard that helps you upgrade the Firewall device manager (FDM) images installed on an individual device or an HA pair.

The wizard guides you through the process of choosing compatible images, installs them, and reboots the device to complete the upgrade. We secure the upgrade process by validating that the images you chose on CDO are the ones copied to, and installed on, your FDM-managed device. We strongly recommend the FDM-managed devices you are upgrading have outbound access to the internet.

If your FDM-managed device does not have outbound access to the internet, you can download the image you want from Cisco.com, store them in your own repository, provide the upgrade wizard with a custom URL to those images, and CDO performs upgrades using those images. In this case, however, you determine what images you want to upgrade to. CDO does not perform the image integrity check or disk-space check.

Configuration Prerequisites

- DNS needs to be enabled on the FDM-managed device. See the "Configuring DNS" section of the **System Administration** chapter of the [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#) for the version your device is running for more information.
- The FDM-managed device should be able to reach the internet if you use upgrade images from CDO's image repository.
- The FDM-managed device has been successfully onboarded to CDO.
- The FDM-managed device is reachable.
- The FDM-managed device is synced.
 - If you update a device that has pending changes in CDO and you do not accept changes, pending changes are lost after the upgrade completes. Best practice is to deploy any pending changes before you upgrade..
 - If you have staged changes in firewall device manager and the device is not synced, the upgrade in CDO will fail at an eligibility check.

4100 and 9300 Series Running FTD

CDO does not support the upgrade for the 4100 or 9300 series devices. You must upgrade these devices outside of CDO.

Software and Hardware Requirements

CDO is a cloud management platform. Software updates are released over time and are generally not dependent on hardware. See [Software and Hardware Supported by CDO](#) for information about supported hardware types.

Devices running firewall device manager software have a recommended upgrade path for optimal performance. See [FDM Software Upgrade Paths](#) for more information.

Upgrade Notes

You cannot deploy changes to a device while it is upgrading.

Related Information:

- [FDM Software Upgrade Paths](#)
- [Upgrade a Single FDM-Managed Device](#)
- [Bulk FDM-Managed Devices Upgrade](#)
- [Upgrade an FDM-Managed High Availability Pair](#)

Upgrade a Single FDM-Managed Device

Before You Begin

Be sure to read through the [FDM-Managed Device Upgrade Prerequisites](#), [FDM Software Upgrade Paths](#), and the [Software and Hardware Supported by CDO](#) before you upgrade. This document covers any requirements and warnings you should know prior to upgrading to your desired version of Firepower software.

Upgrade A Single FDM-Managed Device with Images from Cisco Defense Orchestrator's Repository

Use the following procedure to upgrade a standalone FDM-managed device using a software image that is stored in CDO's repository:

Procedure

-
- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab to locate your device..
- Step 3** Click the **FTD** tab.
- Step 4** Select the device you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.
- Step 6** In step 1, click **Use CDO Image Repository** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 7** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 8** Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning** If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, CDO does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.
- Step 9** Alternatively, if you want CDO to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.

- Step 10** Look at the [notifications tab](#) for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the [Jobs page](#).
- Step 11** Upgrade the system databases. You must do this step in Firewall device manager. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4in for more information.

Upgrade a Single FDM-Managed Device with Images from your own Repository

Use the following procedure to upgrade a standalone FDM-managed device using a URL protocol to locate a software image:

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab to locate your device..
- Step 3** Click the **FTD** tab.
- Step 4** Select the device you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.
- Step 6** In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 7** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 8** Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning** If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Cisco Defense Orchestrator does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.
- Step 9** Alternatively, if you want CDO to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.
- Step 10** Look at the [notifications tab](#) for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the [Jobs page](#).
- Step 11** Upgrade the system databases. You must do this step in Firewall device manager. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4in for more information.

Monitor the Upgrade Process

You can view the progress of your single device by selecting that device on the **Inventory** page and clicking the upgrade button. CDO takes you to the Device Upgrade page for that device.

If the upgrade fails at any point, CDO displays a message. CDO does not automatically restart the upgrade process.



Warning Upgrading devices that have self-signed certificates may experience issues; see [New Certificate Detected](#) for more information

Bulk FDM-Managed Devices Upgrade

Before You Begin

Be sure to read through the [FDM-Managed Device Upgrade Prerequisites](#), [FDM Software Upgrade Paths](#), and the [Software and Hardware Supported by CDO](#) before you upgrade. This document covers any requirements and warnings you should know prior to upgrading to your desired version of Firepower software.



Note You can only bulk upgrade FDM-managed devices if they are all upgrading to the same software version.

Upgrade Bulk FDM-Managed Devices with Images from Cisco Defense Orchestrator's Repository

Use the following procedure to upgrade multiple FDM-managed devices using a software image that is stored in CDO's repository:

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab to locate your devices.
- Step 3** Click the **FTD** tab.
- Step 4** Use the [filter](#) to narrow down the list of devices you may want to include in your bulk upgrade.
- Step 5** From the filtered list of devices, select the devices you want to upgrade.
- Step 6** In the **Device Actions** pane, click **Upgrade**.
- Step 7** On the Bulk Device Upgrade page, the devices that can be upgraded are presented to you. If any of the devices you chose are not upgradable, CDO gives you a link to view the not upgradable devices.
- Step 8** Alternatively, if you want CDO to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.
- Step 9** In step 1, click **Use CDO Image Repository** to select the software image you want to upgrade to. You are only presented with choices that are compatible with the devices you can upgrade. Click **Continue**.

- Step 10** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 11** Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning** If you decide to cancel the upgrades while in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrades after it has started, CDO does not deploy or poll for changes from the devices. Devices do not roll back to the previous configuration after a canceled upgrade, either. This may cause the devices to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.
- Step 12** Look at the [notifications tab](#) for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the [Jobs page](#).
- Step 13** Upgrade the system databases. You must do this step in Firewall device manager. See **Updating System Databases** in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), for the version your device is running.

Upgrade Bulk FDM-Managed Devices with Images from your own Repository

Use the following procedure to upgrade multiple FDM-managed devices using a URL protocol to locate a software image:

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab to locate your devices.
- Step 3** Click the **FTD** tab.
- Step 4** Use the [filter](#) to narrow down the list of devices you may want to include in your bulk upgrade.
- Step 5** From the filtered list of devices, select the devices you want to upgrade.
- Step 6** In the **Device Actions** pane, click **Upgrade**.
- Step 7** On the Bulk Device Upgrade page, the devices that can be upgraded are presented to you. If any of the devices you chose are not upgradable, Cisco Defense Orchestrator gives you a link to view the not upgradable devices.
- Step 8** Alternatively, if you want CDO to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.
- Step 9** In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**.
- Step 10** In step 2, confirm your choices and decide whether you only want to download the images to your devices or copy the images, install them, and reboot the device.
- Step 11** Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Warning If you decide to cancel the upgrades while in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrades after it has started, CDO does not deploy or poll for changes from the devices and the devices do not roll back to the previous configuration. This may cause the devices to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Step 12 Look at the [notifications tab](#) for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the [Jobs page](#).

Step 13 Upgrade the system databases. You must do this step in Firewall device manager. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4 in for more information.

Monitor the Bulk Upgrade Process

You can view the progress of a single device that was included in the bulk upgrade by selecting that device on the **Inventory** page and clicking the upgrade button. You can also view the progress details by clicking **Jobs** in the navigation pane and expanding the bulk operation.

If the upgrade fails at any point, CDO displays a message. CDO does not automatically restart the upgrade process.

Upgrade an FDM-Managed High Availability Pair

Upgrade your HA pair without disrupting traffic; the standby device continues to handle traffic detection while the secondary device is upgraded.

When you upgrade an HA pair, CDO executes an eligibility check and copies or identifies the image location before starting the upgrade. The secondary device in a high availability pair upgrades first, even if it is currently the active device; if the secondary device is the active device, the paired devices automatically switch roles for the upgrade process. Once the secondary devices successfully upgrade, the devices switch roles, then the new standby device upgrades. When the upgrade completes, the devices are automatically configured so the primary device is active and the secondary device is standby.

We do not recommend deploying to the HA pair during the upgrade process.

Before You Begin

- Deploy all pending changes to the active device before upgrading.
- Ensure there are no tasks running during the upgrade.
- Both devices in the HA pair are healthy.
- Confirm you are ready to upgrade; you cannot rollback to a previous version in CDO.
- Read through the [FDM-Managed Device Upgrade Prerequisites](#), [FDM Software Upgrade Paths](#), and the [Software and Hardware Supported by CDO](#) to review any requirements and warnings that may incur during the upgrade process.

Upgrade an FDM-Managed HA Pair with Images from Cisco Defense Orchestrator's Repository

Use the following procedure to upgrade an FDM-managed HA pair using a software image that is stored in CDO's repository:

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab to locate your device.
- Step 3** Click the **FTD** tab.
- Step 4** Select the HA pair you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.
- Step 6** In step 1, click **Use CDO Image Repository** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 7** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 8** Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning** If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, CDO does not deploy or poll changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.
- Step 9** Alternatively, if you want CDO to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.
- Step 10** Look at the [notifications tab](#) for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the [Jobs page](#).
- Step 11** Upgrade the system databases. You must do this step in FDM. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4 in for more information.
-

Upgrade an FDM-Managed HA Pair with Images from your own Repository

Use the following procedure to upgrade an FDM-managed HA pair using a URL protocol to locate a software image:

Procedure

- Step 1** In the navigation bar, click **Inventory**.

- Step 2** Click the **Devices** tab to locate your device.
- Step 3** Click the **FTD** tab.
- Step 4** Select the HA pair you want to upgrade.
- Step 5** In the **Device Actions** pane, click **Upgrade**.
- Step 6** In step 1, click **Specify Image URL** to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 7** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 8** Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning** If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, Cisco Defense Orchestrator does not deploy or poll changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.
- Step 9** Alternatively, if you want CDO to perform the upgrade later, select the Schedule Upgrade check box. Click the field to select a date and time in the future. When you are done, click the Schedule Upgrade button.
- Step 10** Look at the [notifications tab](#) for the progress of the bulk upgrade action. If you want more information about how the actions in the bulk upgrade job succeeded or failed, click the blue Review link and you will be directed to the [Jobs page](#).
- Step 11** Upgrade the system databases. You must do this step in Firewall device manager. See "Updating System Databases" in [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#), Version 6.4 for more information.

Monitor the Upgrade Process

You can view the progress of your single device by selecting that device on the **Inventory** page and clicking the upgrade button. Cisco Defense Orchestrator takes you to the **Device Upgrade** page for that device.

During the upgrade, the system suspends HA while updating system libraries, which includes an automatic deployment, and may not be in a healthy state for the entirety of the upgrade process. This is expected. The device is available for SSH connections during the last part of this process, so if you log in shortly after applying an upgrade, you might see HA in suspended status. If the system experiences issues during the upgrade process and the HA pair appears to be suspended, manually resume HA from the Firewall device manager console of the active device.



Note If the upgrade fails at any point, CDO displays a message. CDO does not automatically restart the upgrade process.



Warning Upgrading devices that have self-signed certificates may experience issues; see [New Certificate Detected](#) for more information.

Upgrade to Snort 3.0

Snort 3 is the latest snort engine, or a powerful preprocessor that uses Open Source Intrusion Prevention System (IPS), available for Firepower Version 6.7 and later. The snort engine uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users and is ideally used as a packet sniffer, a packet logger, or, more traditionally, as a standalone network IPS.

With Snort 3, you can now create custom intrusion policies; every FDM-managed device running Snort 3 has a set of intrusion policies that are pre-defined from Cisco's Talos Intelligence Group (Talos). Snort 3 makes it possible to change these default policies, although we strongly recommend building on top of the base for a more robust policy.

You cannot create custom policies with Snort 2.

Switching from Snort 2 to Snort 3

You can switch Snort versions freely, though some intrusion rules in Snort 2.0 might not exist in Snort 3.0, and vice versa. If you changed the rule action for an existing rule, that change is not preserved if you switch to Snort 3 and then back to Snort 2, or back again to Snort 3. Your changes to rule actions for rules that exist in both versions are preserved. Note that the mapping between rules in Snort 3 and Snort 2 can be one-to-one or one-to-many, so preservation of changes is done on a best-effort basis.

If you choose to upgrade from Snort 2 to Snort 3, please note that upgrading the snort engines is comparable to a system upgrade. We strongly recommend upgrading during a maintenance window to minimize the interruption in traffic monitoring for your network. See [Managing Intrusion Policies \(Snort3\)](#) in the *Firepower Device Manager Configuration Guide* as to how switching snort versions will affect how rules process traffic.



Tip You can filter by Snort version on the **Inventory** page, and the Details window of a selected device displays the current version running on the device.

Snort 3 Limitations

License Requirements

To allow the snort engine to process traffic for intrusion and malware analysis, you must have the **license** enabled for the FDM-managed device. To enable this license through Firewall device manager, log into the Firewall device manager UI and navigate to **Device > View Configuration > Enable/Disable** and enable the license.

Hardware Support

The following devices support Snort 3:

- FTD 1000 series
- FTD 2100 series
- FTD 4100 series
- FTD virtual with AWS
- FTD virtual with Azure

- ASA 5500-X Series with FTD

Software Support

Devices **must** be running at least Firewall device manager Version 6.7. Cisco Defense Orchestrator supports Snort 3 functionality for devices running Version 6.7 and later.

For FTD 1000 and 2000 series, see [FXOS bundled support](#) for more information on FXOS patch support.

Configuration Limitations

CDO does not support upgrading to Snort 3 if your device has the following configurations:

- Device is not running at least Version 6.7.
- If a device has pending changes. Deploy any changes prior to upgrading.
- If a device is currently upgrading. Do not attempt to upgrade or deploy to the device until the device is synced.
- If a device is configured with a virtual router.



Note If you upgrade or revert the Snort version, the system automatically deploys to implement the changes between Snort 2 intrusion policies and Snort 3 intrusion policies.

Rulesets and Snort 3

Note that Snort 3 does not have full feature support at this time. CDO rulesets are not supported on Snort 3 devices. If you simultaneously upgrade a device to Firewall device manager 6.7 or higher, and from Snort 2 to Snort 3, any rulesets configured prior to the upgrade are broken up and the rules in them are saved as individual rules.

For a full list of ruleset support in regards to devices configured for Snort 3, see [Rulesets](#).

Upgrade the Device and the Intrusion Prevention Engine Simultaneously

CDO allows you to upgrade the device to Version 6.7 and the Snort 3. Use the following procedure to upgrade the FDM-managed device:

Procedure

-
- Step 1** In the navigation bar, click **Inventory**.
 - Step 2** Click the **Devices** tab.
 - Step 3** Click the **FTD** tab and select the device or devices you want to upgrade.
 - Step 4** In the **Devices Actions** pane located to the right, click **Upgrade**.
 - Step 5** Set the upgrade toggle to **FTD System Upgrade**.

FTD System Upgrade Intrusion Prevention Engine

- Step 6** (Optional) If you want CDO to perform the upgrade later, check the **Schedule Upgrade** check box. Click in the field to select a date and time in the future.

- Step 7** In step 1, select your upgrade method. Either use the CDO Image Repository and an image from your own repository:
- **Use CDO Image Repository** - Click this option to select the software image you want to upgrade to, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
 - **Specify Image URL** - Click this option to select the software image that is currently stored in your own repository, and click **Continue**. You are only presented with choices that are compatible with the device you can upgrade.
- Step 8** In step 2, confirm your choices and decide whether you only want to download the images to your device or copy the images, install them, and reboot the device.
- Step 9** Check **Upgrade to Snort 3 Engine**.
- Step 10** Click **Perform Upgrade** when you are ready. From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.
- Warning** If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, CDO does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

Upgrade the Intrusion Prevention Engine

For devices that are already running Version 6.7 with Snort 2, use the following procedure to update just the Snort engine to version 3:

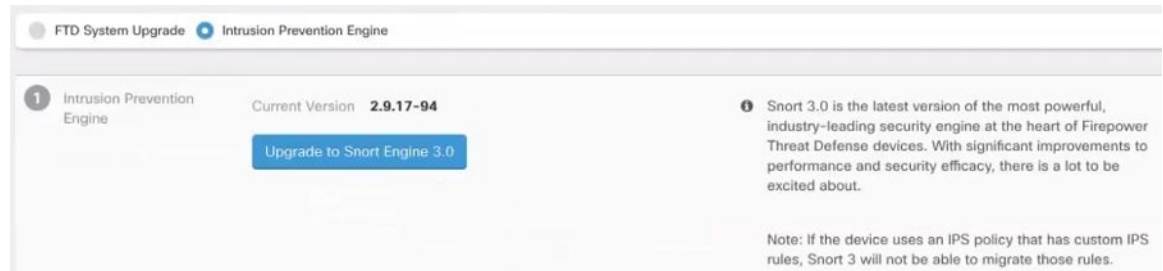
Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and select the device or devices you want to upgrade.
- Step 4** In the **Device Actions** pane located to the right, click **Upgrade**.
- Step 5** Set the upgrade toggle to **Intrusion Prevention Engine**.



The screenshot shows a horizontal bar with two radio button options. The first option is 'FTD System Upgrade' with an unselected radio button. The second option is 'Intrusion Prevention Engine' with a selected radio button.

- Step 6** Click **Upgrade to Snort Engine 3.0**.



Step 7 From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Monitor the Upgrade Process



Warning If you decide to cancel the upgrade while it is in progress, click **Abort Upgrade** from the Upgrade page. If you cancel the upgrade after it has started, CDO does not deploy or check for changes from the device and the device does not roll back to the previous configuration. This may cause the device to enter an unhealthy state. If you experience any issues during the upgrade process, contact Cisco TAC.

You can view the progress of your single device by selecting that device on the **Inventory** page and clicking the upgrade button. CDO takes you to the **Device Upgrade** page for that device.

If the upgrade fails at any point, CDO displays a message. CDO does not automatically restart the upgrade process.



Warning Upgrading devices that have self-signed certificates may experience issues; see [New Certificate Detected](#) for more information

Revert From Snort 3.0 for FDM-Managed Device

Some intrusion rules in Snort 2.0 might not exist in Snort 3.0. If you downgrade to 2.0, any custom intrusion policies that you created are converted to the base policy used in the custom policy. As far as possible, rule action overrides are retained. If more than one custom policy uses the same base policy, the overrides of the custom policy that is used in the most access control policies are retained, and the overrides for the other custom policies are lost. Access control rules that used these "duplicate" policies will now use the base policy created from your most-used custom policy. All custom policies are deleted.

Before you opt to revert from Snort 3.0, read [Managing Intrusion Policies \(Snort2\)](#) of the *Firepower Device Manager Configuration Guide* and find out how switching snort engine versions will affect your current rules and policies.



Note Reverting to version 2 does not uninstall the Firepower software version.

Revert From Snort 3.0

If you change the Snort version, the system will perform an automatic deployment to implement the change. Note that you can only revert individual devices from Snort 3.0 to version 2.

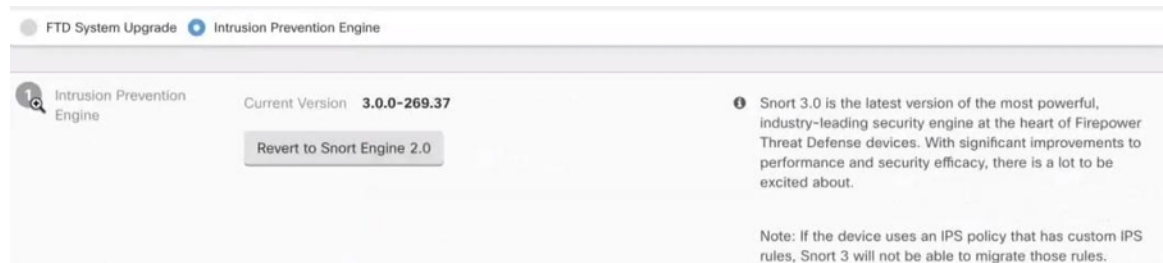
Use the following procedure to revert the intrusion prevention engine:

Procedure

- Step 1** In the navigation pane, click **Inventory**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and click the device you want to revert.
- Step 4** In the **Device Actions** pane located to the right, click **Upgrade**.
- Step 5** Set the upgrade toggle to **Intrusion Prevention Engine**.



- Step 6** In Step 1, confirm you want to revert from Snort version 3, and click **Revert to Snort Engine 2**.



- Step 7** From the **Inventory** page, devices that are upgrading have a "Upgrade in Progress" configuration status.

Schedule a Security Database Update

Use the following procedure to create a scheduled task to check and update the security databases for an FDM-managed device:

Procedure

- Step 1** In the navigation pane, click **Inventory**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and select the desired FDM-managed device.
- Step 4** In the Actions pane, locate the **Security Database Updates** section and click the add + button.

Note If there is an existing scheduled task for the selected device, click the edit icon to create a new task. Creating a new task will overwrite the existing one.

- Step 5** Configure the scheduled task with the following:
- **Frequency** - Choose for the update to occur daily, weekly, or monthly.
 - **Time** - Choose the time of day. Note that the time displayed is UTC.
 - **Select Days** - Choose which day(s) of the week you want the update to occur.
- Step 6** Click **Save**.
- Step 7** The device's Configuration Status will change to "Updating Databases".
-

Edit a Scheduled Security Database Update

Use the following procedure to edit an existing scheduled task to check and update the security databases for an FDM-managed device

Procedure

- Step 1** In the navigation bar, click **Inventory**.
- Step 2** Click the **Devices** tab.
- Step 3** Click the **FTD** tab and select the desired FDM-managed device.
- Step 4** In the Actions pane, locate the **Database Updates** section and click the edit icon.
- Step 5** Edit the scheduled task with the following:
- **Frequency** - Choose for the update to occur daily, weekly, or monthly.
 - **Time** - Choose the time of day. Note that the time displayed is UTC.
 - **Select Days** - Choose which day(s) of the week you want the update to occur.
- Step 6** Click **Save**.
- Step 7** The device's Configuration Status will change to "Updating Databases".
-

