



Migrate Secure Firewall Threat Defense to Cloud

- [Migrate Secure Firewall Threat Defense from Secure Firewall Management Center to Cloud](#), on page 1
- [Before You Begin Migration](#), on page 8
- [Migrate Threat Defense to Cloud-delivered Firewall Management Center](#), on page 10
- [View Threat Defense Migration Jobs](#), on page 12
- [Troubleshoot FTD Migration to Cloud](#), on page 17

Migrate Secure Firewall Threat Defense from Secure Firewall Management Center to Cloud

Cisco Defense Orchestrator allows a user with CDO Admin rights to migrate the threat defense devices from the management center to the cloud.

Before initiating the migration process on the threat defense devices, the management center associated with those devices must already be onboarded to CDO.

On migrating the threat defense to the cloud, CDO onboards the devices and imports all shared policies and associated objects, device-specific policies, and device configuration from the management center to CDO.



Note CDO handles all duplicate policy and object names that are identified during the management center migration process. This behavior is explained in detail later in this document.

The events and analytics management can be transferred to CDO or retained with the management center.

Once you perform the migration, you have 14 days to evaluate your changes. The evaluation period allows you to modify or change specific actions or change the management of these devices back to the management center. After the evaluation period, you cannot revert any changes.

User Roles

The user roles of the on-prem management center are no longer applicable in CDO after migration. Your authorization to perform tasks on the migrated device is based on your user role in CDO. See the [Users](#) topic to understand the on-prem management center and cloud-delivered Firewall Management Center user role mapping.

Supported Software

This section describes the minimum software requirements for migration:

- Management Center: 7.2
- Secure Firewall Threat Defense:
 - 7.0.3 or above
 - 7.2 or above



Note This support is not provided for threat defense running on software version 7.1.

Licensing

- When the threat defense is migrated to the cloud, all feature licenses associated with the device are transferred to CDO and released from the management center to the Smart License pool. The device reclaims the device-specific licenses during its registration with CDO. You need not apply license on the device again.
- The device-specific licenses are not required if you want to keep devices in the management center for analytics.
- Ensure you have registered the cloud-delivered Firewall Management Center with a smart license.

Supported Features

Handling Shared Policies and Objects

When the migration process begins, the shared policies and associated objects that are associated with the threat defense devices are imported first and then followed by the device configuration.

The following shared policies are imported to CDO after changing the manager on threat defense devices:

- Access control
- IPS
- SSL
- Prefilter
- NAT
- QoS
- Identity
- Platform settings
- Flex config

- Network analysis
- DNS
- Malware & file
- Health
- Remote Access VPN

If a policy or object in CDO has the same name as the policy or object that is imported from the Secure Firewall Management Center, CDO takes the following actions after changing the management successfully.

Policies, Objects	Condition	Action
Access control, SSL, IPS, Prefilter, NAT, QoS, Identity, Platform settings, Network analysis, DNS, Malware & File policies.	Name of the cloud-delivered Firewall Management Center policy matches the management center policy.	The cloud-delivered Firewall Management Center policy is used instead of the imported policy from the management center.
RA VPN Default group policy DfltGrpPolicy	The default group policy DfltGrpPolicy from the management center is ignored.	The existing cloud-delivered Firewall Management Center default group policy DfltGrpPolicy is used instead.
Network, Port objects	Name and content of network and port objects in the cloud-delivered Firewall Management Center match the ones in the management center.	The existing cloud-delivered Firewall Management Center network and port objects with the same name and content are used instead of imported objects from the management center. If the object has the same name but different content, an object override is created.
All other objects		The existing cloud-delivered Firewall Management Center object is used instead of the imported object from the management center.

Any Syslog alert object that is associated with the access control policy is imported into Cisco Defense Orchestrator.

Migration Support for Threat Defense in a High Availability Pair

You can migrate a device in a high availability pair. The device management of both active and standby devices is changed and imported into CDO.



Important We strongly recommend committing the manager changes before performing any advanced operations, such as creating HA configuration or breaking HA on the devices that are being migrated.

Performing such operations during the evaluation period is not supported and may result in unintended behavior.

Migration Support for Management Center in a High Availability Pair

You can migrate the threat defense devices from a high availability configured management center to the cloud.

The management center can be onboarded using SecureX or credentials with the SDC method. Always onboard the active management center and not the standby.



Note If you have already onboarded a standalone management center and later configured it as a standby, delete the standby management center and onboard the active one.

Points to Remember:

- **SecureX Onboarding Method**

- High availability break is not supported during the 14 days evaluation period. You can break high availability after committing the changes manually or automatically after the evaluation period.
- High availability switchover is supported during the 14 days evaluation period.

- **Credentials Onboarding Method Using SDC**

- High availability break or high availability switchover is not supported during the 14 days evaluation period. You can perform these operations after committing the changes manually or automatically after the evaluation period.
- After a switchover, onboard the new active unit, which was previously in standby mode, and then start a migration job on the devices.

Unsupported Features

The Migrate FTD to cdFMC screen doesn't allow migration of the device to the cloud in the following conditions:

- A device with a Site-to-Site VPN policy.
- A device part of a cluster.
- A device registered only for analytics-only with the management center.

The following configuration are not imported from the management center to CDO as part of migration:

- Custom Widgets, Application Detectors, Correlation, SNMP and Email Alerts, Scanners, Groups, Dynamic Access Policy, Custom AMP Configuration, Users, Domains, Scheduled Deployment Tasks, ISE configuration, Scheduled GeoDB Updates, Threat Intelligence Director configuration, Dynamic Analysis Connections.
- ISE internal certificate object is not imported as part of the migration. You must export a new system certificate or a certificate and its associated private key from ISE and import it into CDO.

Secure Firewall Recommended Rules

Migrating threat defense to the cloud mirrors the rule recommendations that are already associated with any of the intrusion policies. However, the cloud-delivered Firewall Management Center does not allow the generation of new rule recommendations or auto-update the already migrated recommendations post migration. This is because the cloud-delivered Firewall Management Center does not support rule recommendations. See [Auto Cisco Recommended Rules](#).

Custom Network Analysis

If the device is associated with a custom network analysis policy, you must remove all references to this policy from the on premise before migration.

1. Log on to the on premise management center.
2. Choose **Policies > Access Control**.
3. Click the edit icon on the access control policy you want to disassociate the custom NAP and then click the **Advanced** tab.
4. In the **Network Analysis and Intrusion Policies** area, click the edit icon.
5. In the **Default Network Analysis Policy** list, select a system-provided policy.
6. Click **OK**.
7. Click **Save** to save the changes and then click **Deploy** to download the changes to the device.

After migration, you can manually create the Network Analysis Policy in CDO.

Migration Guidelines and Limitations for VPN Configuration

Keep the following in mind when you migrate a device with VPN configuration:

Migration Support for Remote Access VPN Policy

CDO imports all the settings of a remote access VPN policy as part of the migration.

As part of the migration process, CDO imports all the settings of a remote access VPN policy except for the following:

- Object overrides are not imported.

If overrides are used in the address pool object, you must manually add them to the imported object using CDO after migration.

- Local users are not imported.

If the authentication server is configured to a local database for user authentication, the associated local realm object will be imported into CDO. However, you must manually add the local users to the imported local realm object using CDO after migration. See [Create a Realm and Realm Directory](#).

- VPN load balancing configuration is not migrated.
- RA VPN certificate enrollment with domain configuration is not imported.

You can perform the following after migration:

1. In CDO, click **Inventory > FTD**.

2. Select the migrated FTD and in the **Device Management** on the right, click **Device Overview**.
3. Choose **Devices > Certificates**.

Perform one of the following:

- If the certificates are imported in an error state, click the **Refresh certificate status** icon to synchronize the certificate status with the device. The certificate status turns green.
- If the certificates are not imported, you must manually add the certificates defined in the RA VPN policy configured in the management center.

Managing Threat Defense Events and Analytics

The events and analytics management can be retained in the management center or transferred to Cisco Defense Orchestrator, where the devices must be configured to send events to Cisco Defense Orchestrator. While initiating the migration process, you are allowed to choose the manager to which the device events must be sent for analytics.

If you select the management center for analytics, Cisco Defense Orchestrator becomes the manager for selected devices but retains a copy of those devices on the management center in analytics-only mode. The devices continue to send events to the management center, and Cisco Defense Orchestrator manages the configuration changes.

If you select Cisco Defense Orchestrator for analytics, Cisco Defense Orchestrator becomes the manager for the selected devices and deletes these devices from the management center. Cisco Defense Orchestrator manages both configuration changes and events and analytics management. You must configure threat defense devices to send events to the Cisco cloud. You can use either Security Services Exchange or the Secure Event Connector (SEC) to send events from the devices to the Cisco Secure Analytics and Logging (SAL) in the cloud.

Enable Notification Settings

You can subscribe to get email notifications from CDO whenever a device associated with your tenant experiences a specific action when migrating threat defense devices to CDO.

CDO sends an email if you enable to receive a notification for the following state during the Migrate FTD to cdFMC job:

- **Failed:** When a migration job fails.
- **Started:** When a migration job is initiated.
- **Succeeded:** When a migration job is completed successfully.
- **Commit Pending:** When the manager changes are to be committed.

To enable notification settings, see [Notification Settings](#).

Verify Threat Defense Connectivity with Cloud-delivered Firewall Management Center

This section provides the commands to determine the threat defense connectivity with the cloud-delivered Firewall Management Center.

Check internet connectivity on the device

Execute the **ping system** *<any OpenDNS server address>* command to check whether the device can reach the internet.

1. Connect to the CLI of the device, either from the console port or using SSH.
2. Log in with the Admin username and password.
3. Enter **ping system** *<OpenDNS IPAddress>*.

```
ping system 208.67.222.222
PING 208.67.222.222 (208.67.222.222) 56(84) bytes of data.
64 bytes from 208.67.222.222: icmp_seq=1 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=2 ttl=48 time=22.10 ms
64 bytes from 208.67.222.222: icmp_seq=3 ttl=48 time=22.8 ms
64 bytes from 208.67.222.222: icmp_seq=4 ttl=48 time=22.6 ms
^C
--- 208.67.222.222 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 22.588/22.841/22.995/0.223 ms
```

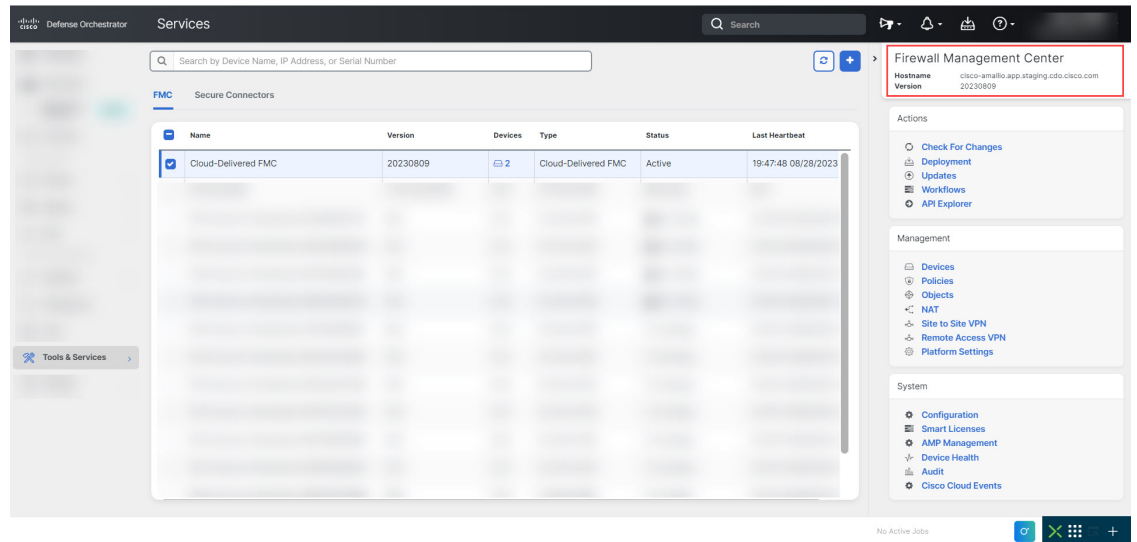
The above example shows that the device can connect to the internet using the OpenDNS Server IP address. Also, the number of packets transmitted is the same as received, indicating that internet connectivity is available on the device. This shows that the device can reach the internet.



Note If your results don't match, check the internet connection manually.

Check device connectivity with Cloud-delivered Firewall Management Center

1. Obtain the host name of the cloud-delivered Firewall Management Center.
 - a. In the CDO navigation pane, click **Tools & Services > Firewall Management Center**.
 - b. Choose **Cloud-Delivered FMC** to see the cloud-delivered Firewall Management Center details on the right pane.
 - c. In the **Hostname** field, copy only the hostname shown in the following example image.



In the above figure, the highlighted text is the hostname (*cdo-acc10.app.us.cdo.cisco.com*) of the FMC to be copied.

2. Connect to the CLI of the device, either from the console port or using SSH.
3. Enter **ping system** *<hostname of the FMC>*.

```
ping system cdo-acc10.app.us.cdo.cisco.com
PING cdo-acc10.app.us.cdo.cisco.com (54.187.125.161) 56(84) bytes of data.
^C
--- cdo-acc10.app.us.cdo.cisco.com ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 64ms
```

In the above example, the hostname is resolved with the IP address, indicating your connection is successful. Ignore the "100% packet loss" message shown in the response.



Note If you can't connect to the host, you can rectify the DNS configuration in the CLI using **configure network dns** *<address>*.

Before You Begin Migration

Before you begin the process, ensure that the following prerequisites are met:

- A provisioned CDO tenant.
- CDO is registered with Smart License.
- The on-prem management center is onboarded to CDO. Onboarding the on-prem management center also onboards all the threat defense devices registered to that on-prem management center. See [Onboard an FMC](#).



Note Create a new user in the on-prem management center with Administrator role or a custom user role with "Devices" and "System" permissions for onboarding purposes.



Caution If you onboard an on-prem management center to CDO and simultaneously sign in to that on-prem management center with the same user name, the onboarding fails.

- The threat defense devices must be synchronized and have no pending changes on them. The migration job fails on a device if CDO identifies pending changes on that device.
- On-Prem Management Center should allow outbound HTTP/HTTPS to upload configurations to Amazon S3.
- CDO imports Syslog alert object used in the access control policy from the on-prem management center. If CDO already contains an alert object with the same name but a different type (SNMP, Email), it is reused during configuration import.

The user must check whether the Syslog object name matches the existing SNMP or Email alert object in CDO. If the name matches, you must rename the Syslog object in the on-prem management center before starting the migration process.


- If you attempt to migrate firewalls with modified system defined FlexConfig text objects from an on-prem management center to the cloud-delivered Firewall Management Center, the values of the modified system defined FlexConfig text objects are not migrated to the cloud-delivered Firewall Management Center, and the deployment will fail.


To avoid this, perform these tasks before you start the migration:

- Copy the modified system defined FlexConfig text object values from the on-prem management center to cloud-delivered Firewall Management Center before migration.
- Initiate migration from on-prem management center to cloud-delivered Firewall Management Center after verifying the predefined FlexConfig text objects.

High Availability Failover Link Must Be Up

The high availability failover link should be up for a successful migration. Before initiating the migration process on CDO, determine the health status of the failover link on the on-prem management center.

1. Identify the failover interfaces of all HA pairs you want to migrate to cloud-delivered Firewall Management Center.
 - a. Choose **Devices > Device Management**.
 - b. Next to the device high-availability pair you want to edit, click **Edit** ()
 - c. Click the **High Availability** tab.
 - d. In the **High Availability Link** area, the **Interface** field shows the failover interface used in the pair.

- e. Identify the interfaces used for failover communication if there are multiple HA pairs for migration.
2. Check the health status of the failover interfaces.
 - a. Choose **Devices > Device Management**.
 - b. Next to the device high-availability pair you want, click **Health Monitor**.
 - c. In the left pane, expand the high availability pair to see the threat defense devices.
 - d. Click the device indicated in the exclamation mark ().
 - e. Click the **Critical** button at the top.
The **Interface Status** shows the errors associated with interfaces.
 - f. If the failover interface is down, the **Interface 'failover_interfacename' has no link** message is displayed.




Note However, you can migrate the HA pair to cloud-delivered Firewall Management Center if you see any other data interface issues except for the failover interface.

- g. Rectify the issue and click **Sync from onprem fmc now** to obtain the latest changes on the device.

Migrate Threat Defense to Cloud-delivered Firewall Management Center

Procedure

Step 1 In the navigation bar on the left, click **Tools & Services > Migrations > Migrate FTD to cdFMC**.

Step 2 Click  icon to initiate the threat defense migration process.

Note You can initiate only one migration job at one time.

Step 3 In the **Select OnPrem FMC** step, perform the following:

- a. You can click the **Onboard an FMC** link to onboard the on-premise management center if you have not done already. See [Onboard an FMC](#).
- b. Select the management center from the available list and click **Next**.

In the **Select Devices** step, you will see the threat defense devices that the selected management center manages. If a high-availability pair is set up on the on-premise management center, the high availability node will be shown instead of the active and standby devices.

The **Last Synced time** field indicates the time elapsed since the device configuration synchronized into the management center. You can click **Sync from OnPrem FMC Now** to fetch the latest device changes.

Step 4 In the **Select Devices** step, perform the following:

- a) Select the devices you want to migrate. In case of a high availability pair, select the high availability node.

Migrate FTD to Cloud
Migrate FTD Manager from Firewall Management Center to CDO

1 Select OnPrem FMC **OnPrem FMC: FMC_OnPrem**

2 Select Devices Select FTD devices to migrate to cloud from OnPrem FMC to CDO and specify an action in bulk or per device.

1 device(s) selected Multi-Device Action: Retain on OnPrem FMC for Analytics

	Name	Domain	Action
<input type="checkbox"/>	FMC_OnPrem_192.168.0.31	Global	Retain on OnPrem FMC for Analytics
<input checked="" type="checkbox"/>	FMC_OnPrem_192.168.0.32	Global	Retain on OnPrem FMC for Analytics

Displaying 2 of 2 results

Migrate FTD to Cloud

- Note**
- The devices running on unsupported versions are not available for selection.
 - The devices that are registered for analytics only with the management center or have pending changes to be deployed are not eligible for migration.

b) In the **Multi-Device Action** list, you can choose a common action to apply on all devices.

c) In the **Commit Action** column, you can choose one of the following actions for the selected device:

- **Retain on OnPrem FMC for Analytics:** After the migration process is completed, the analytics management for selected threat defense devices is retained on the management center.
- **Delete FTD from OnPrem FMC:** After the migration process is completed, the selected devices are removed from the management center and are available for CDO to handle the analytics. You must configure the devices to send events to CDO for managing analytics. Once the devices are deleted from the management center, they cannot be revoked.

Note The device is not deleted from the management center unless the changes are committed, either automatic or manual.

- Note**
- Revert Manager to OnPrem FMC, or
 - Retain on On-Prem Firewall Management Center for Analytics or Delete threat defense from On-Prem Firewall Management Center

Note The actions specified here are committed automatically after 14 days evaluation period or after the changes are committed manually.

Step 5 Click **Migrate FTD to cdFMC**.


Step 6 Click **View Migration to Cloud Progress** to see the progress of your job.

What to do next

You can view the overall and individual status of migration jobs and generate a report when a job is completed successfully. See [View Threat Defense Migration Jobs, on page 12](#).

View Threat Defense Migration Jobs

You can see the status of all migration jobs that are initiated from CDO. You can expand a job to see the status of individual devices associated with the management center.

If you have [Enable Notification Settings](#) alerts for device workflows, click the notifications icon  to view the alerts that have occurred during migration. You will also receive an email notification if you have subscribed to get email notifications from CDO.

Once a migration job is successful, you have 14 days to evaluate your devices using CDO. During this period, you can modify or change specific actions or change the management of these devices back to the management center.

We recommend committing the devices manually if you are convinced with the migration changes. CDO auto-commits the changes after the evaluation period expires without requiring further action from you. The commit action applies the changes to devices. See [Commit Manager Changes Manually, on page 15](#).

Once the changes are committed, you can't revoke the actions that are specified in the window.

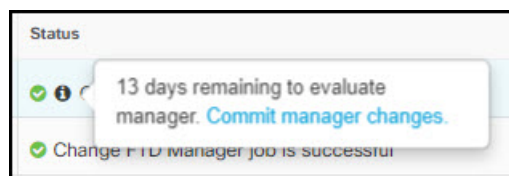


Important

Changes can be made and deployed to the device using CDO in the evaluation period. If you choose to revert the device management back to the management center, the CDO-specific changes that are made during the evaluation period will not be retained on the device after reverting its manager. You must deploy the changes from the on premise management center to the device after reverting its manager.

- **Name:** Represents the job name which shows the management center name and the date and time when the job was initiated.
- **Number of FTDs:** This shows the total number of devices that are being migrated to the cloud.
- **Status:** Displays the status of the job. Expand the job to see the status of individual devices.

When a job is completed successfully, the **FTD Migration job is successful** message appears in the **Status** column. You can click the tooltip to see the number of days remaining for evaluating the manager.



You can click [Commit Manager Changes Manually](#) to commit the changes manually before the 14 days evaluation period ends.

- **Last Update:** The date and time are updated only when a change is made to the device.
- **Actions:**
 - **Workflows:** Provides a link that directs you to the workflows page for monitoring the job.
 - **Download Report:** Allows you to generate and download a report of every job that is completed successfully. See [Generate Threat Defense Migration Report, on page 14](#).
 - **Commit Manager Changes:** Allows you to apply the changes manually to devices before the evaluation period ends. See [Commit Manager Changes Manually, on page 15](#).
 - **Remove Migration Job:** Allows you to remove a completed job. The link is available only for completed jobs.

After a successful migration, CDO deploys the configuration to the device. If the system identifies errors or warnings in the changes to be deployed, it displays them in the **Validation Messages** window. To view complete details, click the arrow icon before the warnings or errors. If the deployment fails, see the *Best Practices for Deploying Configuration Changes* section of [Firepower Management Center Device Configuration Guide X.Y](#).

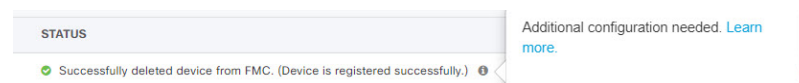


-
- Important** During the 14-day evaluation period, you cannot delete a device or an OnPrem FMC from CDO. Do one of the following and then delete the device or OnPrem FMC:
- Perform [Remove Migration Job](#) associated with the OnPrem FMC or device you want to delete.
 - Select **Revert Manager to OnPrem FMC** and [Commit Manager Changes Manually](#).
-

Configure Relam Sequence for Identity Policy

If the device contains an identity policy with a Realm or ISE configuration, configure your device as a proxy for CDO to communicate with the identity source. The identity policies don't function if CDO fails to connect to the Identity Realms.

A tooltip appears in the **Status** column for a device that requires additional configuration.




1. Click the tooltip icon and then click **Learn more**.
2. In the **Configure Proxy** window, click **Configure my realms**.

To add a proxy sequence, see the *Create a Proxy Sequence* section in the [Firepower Management Center Device Configuration Guide, 7.2](#).

Generate Threat Defense Migration Report

When a migration job is successful, you can generate and download a report in a PDF format to analyze the value of every parameter imported from the management center to CDO. The report provides details of each device associated with the job. The details include information about devices, values of shared policies, objects, routing details, interfaces, network settings, and many more.

On the migration jobs page, click the  under the **Actions** column of a completed job and then click **Download Report**. You must download the report within a year of the job triggered.

View Migrated Devices

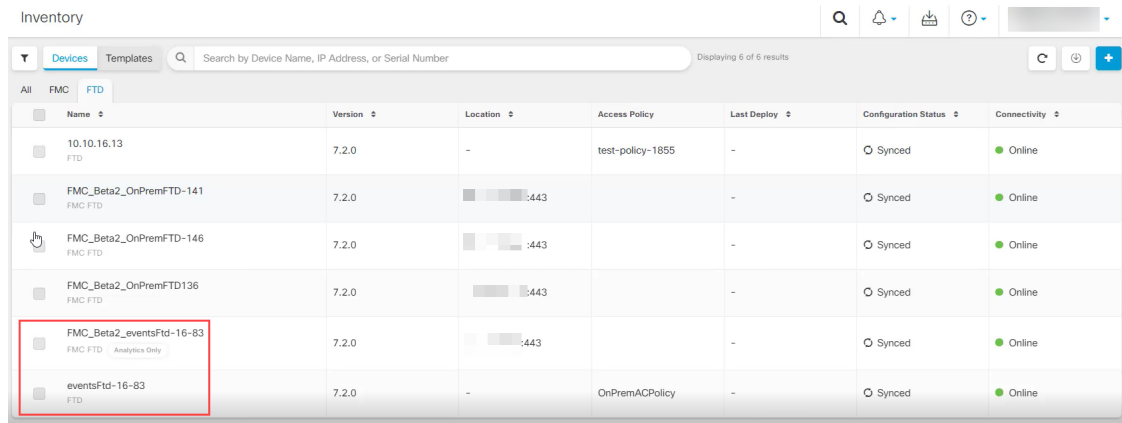
The migrated devices appear on the **Inventory** page in CDO. You can cross-launch and configure the required feature on the cloud-delivered Firewall Management Center.



Note The devices on the cloud-delivered Firewall Management Center device listing page may show `NO-IP` instead of the device's management IP address. Because the device registration uses the NAT ID, the device initiates the process, and therefore, the management IPs aren't discovered or used for the connection. Note that this applies to newly onboarded devices and devices migrated from the on-prem management center.

Analytics Only Threat Defense Device Example

CDO creates two instances of the same device that is configured to retain on the management center for analytics.



Name	Version	Location	Access Policy	Last Deploy	Configuration Status	Connectivity
10.10.16.13 FTD	7.2.0	-	test-policy-1855	-	Synced	Online
FMC_Beta2_OnPremFTD-141 FMC FTD	7.2.0	:-:443		-	Synced	Online
FMC_Beta2_OnPremFTD-146 FMC FTD	7.2.0	:-:443		-	Synced	Online
FMC_Beta2_OnPremFTD136 FMC FTD	7.2.0	:-:443		-	Synced	Online
FMC_Beta2_eventsFtd-16-83 FMC FTD Analytics Only	7.2.0	:-:443		-	Synced	Online
eventsFtd-16-83 FTD	7.2.0	-	OnPremACPolicy	-	Synced	Online

The device instance with **FMC FTD** and **Analytics Only** labels shows that the management center handles the analytics. The device instance with the **FTD** label indicates that CDO manages its configuration.

You can manage the configuration of the device using CDO. To see the device in the cloud-delivered Firewall Management Center, do the following:

Select the device having **FTD** label and in the **Management** pane on the right, click **Device Summary**.

Defense Orchestrator
Devices / Device Management

Monitoring Policies Devices Objects Integration

Return to Inventory Deploy

View By: Group

All (1) Error (0) Warning (0) Offline (0) Normal (1) Deployment Pending (0) Upgrade (0) Snort 3 (1)

Search Device Add

Collapse All

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
eventsFtd-16-83 N/A - Routed	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	OnPremACPolicy	

You can view the events from the device in the management center. To see the events, do the following:

1. Select the device having **FMC FTD** and **Analytics Only** labels and on the right, click the **Manage Devices** link.
2. Log on to the on premise management center.
3. Click **Device > Device Management**.

Firewall Management Center
Devices / Device Management

Overview Analysis Policies Devices Objects Integration

Deploy

View By: Group

All (4) Error (0) Warning (0) Offline (0) Normal (4) Deployment Pending (1) Upgrade (0) Snort 3 (4) CDO (1)

Search Device Add

Collapse All

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
eventsFtd-16-83 10.10.16.83 - Routed	FTDv for VMware	7.2.0	N/A	CDO Managed	CDO Managed	
OnPremFTD-141 10.10.14.141 - Routed	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...)	OnPremACPolicy	

You can't select this device as CDO manages the configuration. The management center shows the **CDO Managed** label for this device.

To see the live events in the management center, click **Analysis > Events**.

Commit Manager Changes Manually

We recommend committing manager changes manually if you are convinced with your changes and not waiting for Cisco Defense Orchestrator to auto-commit changes. The window shows the number of days remaining to revert to the management center as your device manager or change your actions and commit the changes to Cisco Defense Orchestrator. During the evaluation period, you have an opportunity to change specified actions for selected threat defense devices before committing the changes.


Once the changes are committed, you can't revoke the actions specified in the window.



Note The commit manager changes actions are disabled in the following conditions:

- The 14 days evaluation period has passed.
- The threat defense devices have been reverted or deleted, in which case, no further actions can be taken.

Procedure


- Step 1** On the migration jobs page, click the  under the **Actions** column of a completed job.
- Step 2** Click **Commit Manager Changes**. This link is available only when the job is completed successfully.
- Step 3** If you want to change the actions specified for a device, select the device, and in the **Actions** list, select an action:
- **Retain on OnPrem FMC for Analytics:** After committing the changes, analytics management for selected threat defense devices is retained on the management center.
 - **Delete Threat Defense from OnPrem FMC:** After committing the changes, the selected devices are removed from the management center and are available for Cisco Defense Orchestrator to handle the analytics. You must configure the threat defense to send events to Cisco Defense Orchestrator for managing analytics. Once the threat defense devices are deleted from the management center, they cannot be revoked.
 - **Revert Manager to OnPrem FMC:** After committing the changes, the device management is returned to the management center from Cisco Defense Orchestrator.
- Note**
- After committing this action, you can't change the management of the device to Cisco Defense Orchestrator again.
- Workaround:** You must remove the device from the management center and onboard it. Then, you can change the management of the device in Cisco Defense Orchestrator.
- After committing this action, the device does not show an "Out-of-Date" status in the management center.
- Workaround:** On the on premises management center, deploy the changes to the device.
- Step 4** Click **Commit** executes your specified actions immediately without further confirmation.
- Step 5** On the migration jobs screen, you can expand the job to check the progress of the actions specified.
-

Remove Migration Job

You can delete a migration job, and the outcome is dependent on when it was deleted

- During the 14-day evaluation period: Stops the migration, and the configuration of the devices associated with the migration job is reverted to their original state.
- After committing migration changes: The record is deleted from the migration job list.

Procedure

- Step 1** On the migration jobs page, click the  under the **Actions** column and then click **Remove Migration Job**.

Step 2 Click **Delete** to confirm your action.

Troubleshoot FTD Migration to Cloud

This section provides information to troubleshoot specific errors that may occur when migrating FTD to the cloud.

HTTP Status Code 201 (Created) Found in FMC Response

CDO shows this error at the device level.

Issue:

The Secure Device Connector (SDC) version is not compatible.

Number of FTDs	Status
1 devices	⚠️ Change FTD Manager job failed
IP ADDRESS	STATUS
10.10.90.32	⚠️ Device Connectivity with CDO failed. (HTTP status code 201 (Created) found in FMC response.)

Resolution:

Ensure that the SDC is upgraded to version "202205191350" or later.

1. Navigate to **Admin > Secure Connectors**.
2. Click the SDC to see the existing SDC version in the **Details** pane on the right.
3. [Update your Secure Device Connector](#).

Device Connectivity to CDO Failed

Name	Number of FTDs	Status	Last Updated	Actions
1771Fmc_change-management_2022-02-28-104213	2 devices	⚠️ Change FTD Manager job failed	Feb 28, 2022, 4:14:12 PM	⋮
DEVICE NAME	IP ADDRESS	STATUS	LAST UPDATED	
1771Fmc_10.10.16.84	10.10.16.84	⚠️ Device Connectivity with CDO failed	Feb 28, 2022, 4:12:53 PM	

The device is unable to reach CDO for one of the following reasons:

- The device is cabled incorrectly.
- Your network may require a static IP address for the device.
- Your network uses custom DNS, or there is external DNS blocking on the customer network.
- PPPoE authentication is needed.
- The device is behind a proxy.

Resolution:

- Check the cabling and network connectivity.

- Ensure that your firewall is not blocking any traffic.
- [Verify Threat Defense Connectivity with Cloud-delivered Firewall Management Center.](#)

Failed to Configure CDO as Configuration Manager

When CDO cannot communicate with the device due to network loss, it fails to execute the configure manager command with the cloud-delivered Firewall Management Center.

Name	Number of FTDs	Status	Last Updated	Actions
1771Fmc_change-management_2022-03-04-055700	2 devices	Change FTD Manager job is in progress	Mar 4, 2022, 11:33:07 AM	...
DEVICE NAME	IP ADDRESS	STATUS	LAST UPDATED	
1771Fmc_10.10.16.86	10.10.16.86	Syncing	Mar 4, 2022, 11:29:03 AM	
1771Fmc_10.10.16.84	10.10.16.84	Failed to configure CDO as Configuration Manager	Mar 4, 2022, 11:28:16 AM	

Resolution:

1. Check the cabling and network connectivity.
2. Ensure that your firewall is not blocking any traffic.
3. Ensure that FTD has internet connectivity and the DNS address is resolved to an IP address. See [Verify Threat Defense Connectivity with Cloud-delivered Firewall Management Center, on page 7.](#)
4. Retry migration for this FTD from CDO in a new change manager job.

Change Manager Already Exists or in Progress for Source Manager

You can create an FTD migration job for a on-prem management center only when the previous job is completed.

This error occurs when you create a new job when the previous job is in progress.

Migrate FTD to Cloud
Change FTD Manager from Firewall Management Center to CDO

1 Select OnPrem FMC **OnPrem FMC: fmc-beta2-18-3**

2 Select Devices **change ftd management already exists or in progress for source manager fmc-beta2-18-3**

Select FTD devices to migrate to cloud from OnPrem FMC to CDO and specify an action in bulk or per device.

1 device(s) selected Multi-Device Action Retain on OnPrem FMC for Analytics

Name	Domain	Action
<input type="checkbox"/> fmc-beta2-18-3_10.10.16.20	Global	Retain on OnPrem FMC for Analytics
<input checked="" type="checkbox"/> fmc-beta2-18-3_10.10.16.25	Global	Retain on OnPrem FMC for Analytics
<input type="checkbox"/> fmc-beta2-18-3_10.10.16.9	Global	Retain on OnPrem FMC for Analytics

Displaying 3 of 3 results

Migrate FTD to Cloud

3 Finish

Resolution:

1. Navigate to the migration table to see if another job is in progress for a particular source on premise management center.
2. Wait for the current migration job to complete.
3. Initiate the next migration job.

