



Device Management

This guide applies to an *on-premises* Secure Firewall Management Center, either as your primary manager or as an analytics-only manager. When using the Cisco Defense Orchestrator (CDO) cloud-delivered Firewall Management Center as your primary manager, you can use an on-prem management center for analytics. Do not use this guide for cloud-delivered Firewall Management Center management; see [Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Defense Orchestrator](#).

You can manage devices in the Secure Firewall Management Center.

- [Log Into the Command Line Interface on the Device, on page 1](#)
- [Add a Device Group, on page 3](#)
- [Shut Down or Restart the Device, on page 3](#)
- [Download the Managed Device List, on page 4](#)
- [Configure Device Settings, on page 5](#)
- [Hot Swap an SSD on the Secure Firewall 3100/4200, on page 74](#)
- [Disable the USB Port, on page 77](#)
- [Migrate the Configuration to a New Model, on page 79](#)

Log Into the Command Line Interface on the Device

You can log directly into the command line interface on threat defense devices. If this is your first time logging in, complete the initial setup process using the default **admin** user; see [Complete the Initial Configuration of a Secure Firewall Threat Defense Device Using the CLI](#).



Note If a user makes three consecutive failed attempts to log into the CLI via SSH, the system terminates the SSH connection.

Before you begin

Create additional user accounts that can log into the CLI using the **configure user add** command.

Procedure

Step 1 Connect to the threat defense CLI, either from the console port or using SSH.

You can SSH to the management interface of the threat defense device. You can also connect to the address on a data interface if you open the interface for SSH connections. SSH access to data interfaces is disabled by default. See [SSH Access](#) to allow SSH connections to specific data interfaces.

For physical devices, you can directly connect to the console port on the device. See the hardware guide for your device for more information about the console cable. Use the following serial settings:

- 9600 baud
- 8 data bits
- No parity
- 1 stop bit

The CLI on the console port is FXOS (with the exception of the ISA 3000, where it is the regular threat defense CLI). Use the threat defense CLI for basic configuration, monitoring, and normal system troubleshooting. See the FXOS documentation for information on FXOS commands.

For a chassis in multi-instance mode, you can connect to FXOS on the console port, or you can enable SSH for the Management interface according to [Configure SSH and SSH Access List](#). SSH is disabled by default.

Step 2 Log in with the **admin** username and password.

Example:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Step 3 If you used the console port, access the threat defense CLI.

connect ftd

Multi-instance mode:

connect ftd *name*

To view the instance names, enter the command without a name.

Note This step does not apply to the ISA 3000.

Example:

```
firepower# connect ftd
>
```

Step 4 At the CLI prompt (>), use any of the commands allowed by your level of command line access.

To return to FXOS on the console port, enter **exit**.

Step 5 (Optional) If you used SSH, you can connect to FXOS.

connect fxos

To return to the threat defense CLI, enter **exit**.

Step 6 (Optional) Access the diagnostic CLI:

system support diagnostic-cli

Use this CLI for advanced troubleshooting. This CLI includes additional **show** and other commands.

This CLI has two sub-modes: user EXEC and privileged EXEC mode. More commands are available in privileged EXEC mode. To enter privileged EXEC mode, enter the **enable** command; press enter without entering a password when prompted.

Example:

```
> system support diagnostic-cli
firepower> enable
Password:
firepower#
```

To return to the regular CLI, type **Ctrl-a, d**.

Add a Device Group

The management center allows you to group devices so you can easily deploy policies and install updates on multiple devices. You can expand and collapse the list of devices in the group.

If you add the primary device in a high-availability pair to a group, both devices are added to the group. If you break the high-availability pair, both devices remain in that group.

Procedure

- Step 1** Choose **Devices > Device Management**.
 - Step 2** From the **Add** drop-down menu, choose **Add Group**.

To edit an existing group, click **Edit** (✎) for the group you want to edit.
 - Step 3** Enter a **Name**.
 - Step 4** Under **Available Devices**, choose one or more devices to add to the device group. Use Ctrl or Shift while clicking to choose multiple devices.
 - Step 5** Click **Add** to include the devices you chose in the device group.
 - Step 6** Optionally, to remove a device from the device group, click **Delete** (🗑) next to the device you want to remove.
 - Step 7** Click **OK** to add the device group.
-

Shut Down or Restart the Device

It's important that you shut down your system properly. Simply unplugging the power or pressing the power switch can cause serious file system damage. Remember that there are many processes running in the background all the time, and unplugging or shutting off the power does not allow the graceful shutdown of your firewall.

See the following task to shut down or restart your system properly.



Note After restarting your device, you may see an error that the management connection could not be reestablished. In some cases, the connection is attempted before the Management interface on the device is ready. The connection will be retried automatically and should come up within 15 minutes.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device that you want to restart, click **Edit** (✎).

Step 3 Click **Device**.

Step 4 To restart the device:

- a) Click **Restart Device** (↻).
- b) When prompted, confirm that you want to restart the device.

Step 5 To shut down the device:

- a) Click **Shut Down Device** (⊗) in the **System** section.
- b) When prompted, confirm that you want to shut down the device.
- c) If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

```
System is stopped.  
It is safe to power off now.  
Do you want to reboot instead? [y/N]
```

If you do not have a console connection, wait approximately 3 minutes to ensure the system has shut down.

For the ISA 3000, when shutdown is complete, the System LED will turn off. Wait at least 10 seconds before you remove the power.

Download the Managed Device List

You can download a report of all the managed devices.

Before you begin

To perform the following task, you must be an Admin user.

Procedure

Step 1 Choose **Devices > Device Management**.

- Step 2** Click the **Download Device List Report** link.
- Step 3** You can download the device list in CSV or PDF format. Choose **Download CSV** or **Download PDF** to download the report.
-

Configure Device Settings

The **Devices > Device Management** page provides you with range of information and options:

- **View By**—Use this option to view the devices based on group, licenses, model, version, or access control policy.
- **Device State**—You can also view the devices based on its state. You can click on a state icon to view the devices belonging to it. The number of devices belonging to the states are provided within brackets.
- **Search**—You can search for a configured device by providing the device name, host name, or the IP address.
- **Add options**—You can add devices, high availability pairs, clusters and groups.
- **Edit and other actions**—Against each configured device, use the **Edit** (✎) icon to edit the device parameters and attributes. Click the **More** (⋮) icon and execute other actions:
 - **Access Control Policy**—Click on the link in the Access Control Policy column to view the policy that is deployed to the device.
 - **Delete**—To unregister the device.
 - **Packet Tracer**—To navigate to the packet tracer page for examining policy configuration on the device by injecting a model packet into the system.
 - **Packet Capture**—To navigate to the packet capture page, where, you can view the verdicts and actions the system takes while processing a packet.
 - **Revert Upgrade**—To revert the upgrade and configuration changes that were made after the last upgrade. This action results in restoring the device to the version that was before the upgrade.
 - **Health Monitor**—To navigate to the device's health monitoring page.
 - **Troubleshooting Files**—Generate troubleshooting files, where you can choose the type of data to be included in the report.
 - For Firepower 4100/9300 series devices, a link to the chassis manager web interface.

When you click on the device, the device properties page appears with several tabs. You can use the tabs to view the device information, and configure routing, interfaces, inline sets, and DHCP.

Edit General Settings

The **General** section of the **Device** page displays the settings described in the table below.

Figure 1: General

Table 1: General Section Table Fields

Field	Description
Name	The display name of the device on the management center.
Transfer Packets	This displays whether or not the managed device sends packet data with the events to the management center.
Troubleshoot	Lets you generate and download troubleshooting files and also see CLI command output. See Generate Troubleshooting Files, on page 7 and View CLI Output, on page 9 .
Mode	The displays the mode of the management interface for the device: routed or transparent .
Compliance Mode	This displays the security certifications compliance for a device. Valid values are CC, UCAPL and None.
Performance Profile	This displays the core allocation performance profile for the device, as configured in the platform settings policy.
TLS Crypto Acceleration:	Shows whether TLS crypto acceleration is enabled or disabled.
Device Configuration	Lets you copy, export, or import a configuration. See Copy a Configuration to Another Device, on page 11 and Export and Import the Device Configuration, on page 12 .
OnBoarding Method	Shows whether the device was registered using a registration key or using the serial number (zero-touch provisioning).

You can edit some of these settings from this section.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to modify, click **Edit** (✎).
- Step 3** Click **Device**.
- Step 4** In the **General** section, click **Edit** (✎).
- Enter a **Name** for the managed device.
 - Check **Transfer Packets** to allow packet data to be stored with events on the management center.
 - Click **Force Deploy** to force deployment of current policies and device configuration to the device.
- Note** Force-deploy consumes more time than the regular deployment since it involves the complete generation of the policy rules to be deployed on the threat defense.
- Step 5** For **Troubleshoot** actions, see [Generate Troubleshooting Files, on page 7](#) and [View CLI Output, on page 9](#).
- Step 6** For **Device Configuration** actions, see [Copy a Configuration to Another Device, on page 11](#) and [Export and Import the Device Configuration, on page 12](#).
- Step 7** Click **Deploy**.
-

What to do next

- Deploy configuration changes.

Generate Troubleshooting Files

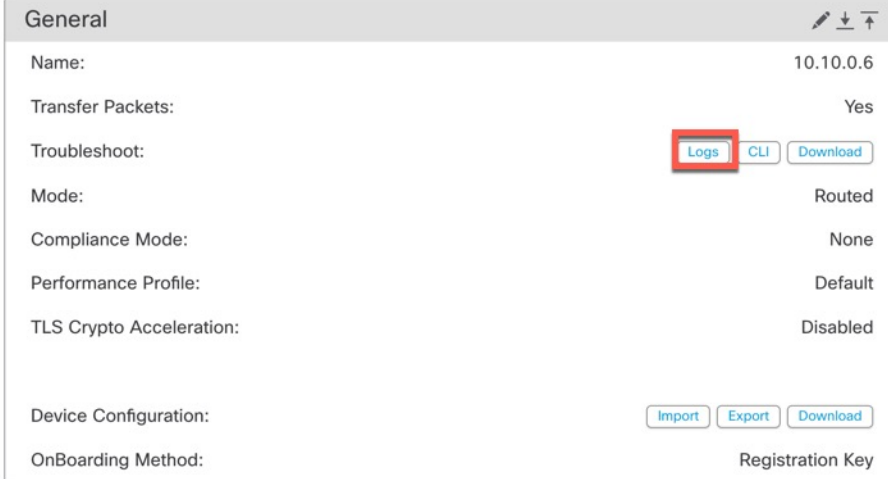
You can generate and download troubleshooting files for each device and also for all cluster nodes. For a cluster, you can download all files as a single compressed file. You can also include cluster logs for the cluster for cluster nodes.

You can alternatively trigger file generation from the **Devices > Device Management > More** (☰) > **Troubleshoot Files** menu.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device or cluster you want to view, click **Edit** (✎).
- In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.
- Step 3** Click **Device** or **Cluster**.
- Step 4** Generate logs for the device or for all cluster nodes.
- On the **General > Troubleshoot** section, click **Logs**.

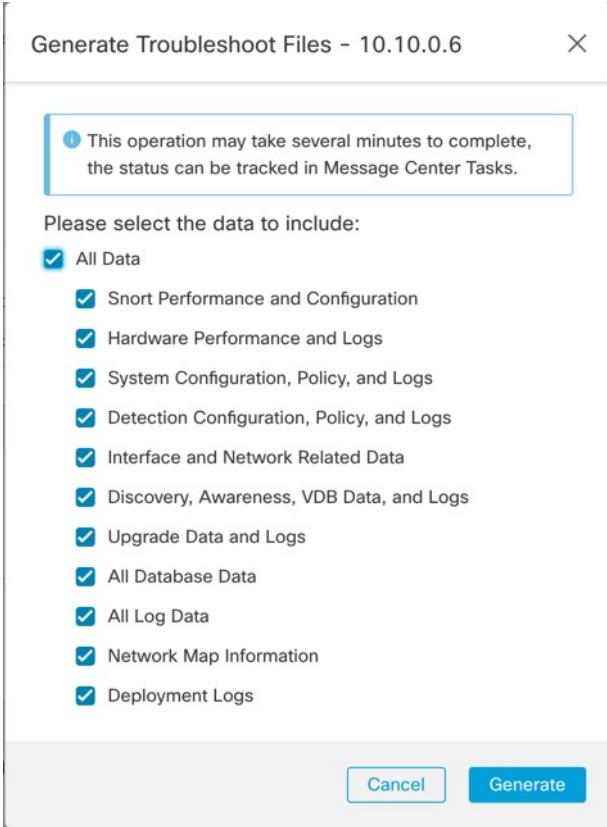
Figure 2: Logs



General	
Name:	10.10.0.6
Transfer Packets:	Yes
Troubleshoot:	Logs CLI Download
Mode:	Routed
Compliance Mode:	None
Performance Profile:	Default
TLS Crypto Acceleration:	Disabled
Device Configuration:	Import Export Download
OnBoarding Method:	Registration Key

- b) You are prompted to choose the logs you want to include. For a cluster, under **Device**, you can choose **All Devices** or an individual node. A cluster also has the **Cluster Logs** available.

Figure 3: Generate Troubleshoot Files



Generate Troubleshoot Files - 10.10.0.6

This operation may take several minutes to complete, the status can be tracked in Message Center Tasks.

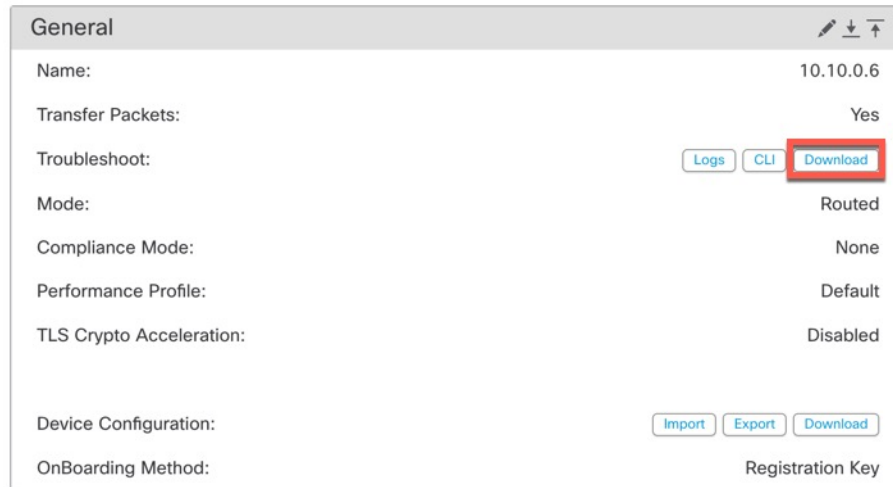
Please select the data to include:

- All Data
 - Snort Performance and Configuration
 - Hardware Performance and Logs
 - System Configuration, Policy, and Logs
 - Detection Configuration, Policy, and Logs
 - Interface and Network Related Data
 - Discovery, Awareness, VDB Data, and Logs
 - Upgrade Data and Logs
 - All Database Data
 - All Log Data
 - Network Map Information
 - Deployment Logs

Cancel Generate

- c) Click **Generate**.

Step 5 To download the generated logs, on the **General > Troubleshoot** section, click **Download**.

Figure 4: Download

The screenshot shows a configuration page titled 'General'. It contains several fields and buttons. The 'Name' field is set to '10.10.0.6'. The 'Transfer Packets' field is set to 'Yes'. The 'Troubleshoot' section has three buttons: 'Logs', 'CLI', and 'Download', with the 'Download' button highlighted by a red box. The 'Mode' field is set to 'Routed'. The 'Compliance Mode' field is set to 'None'. The 'Performance Profile' field is set to 'Default'. The 'TLS Crypto Acceleration' field is set to 'Disabled'. At the bottom, there are three buttons: 'Import', 'Export', and 'Download'. The 'OnBoarding Method' field is set to 'Registration Key'.

The logs are downloaded to your computer.

View CLI Output

You can view a set of pre-defined CLI outputs that can help you troubleshoot the device or cluster. You can also enter any **show** command and see the output.

For a device, the following commands are executed:

- **show version**
- **show asp drop**
- **show counters**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**

For a cluster or cluster node:

- **show running-config cluster**
- **show cluster info**
- **show cluster info health**
- **show cluster info transport cp**
- **show version**
- **show asp drop**
- **show counters**

- **show arp**
- **show int ip brief**
- **show blocks**
- **show cpu detailed**
- **show interface *ccl_interface***
- **ping *ccl_ip* size *ccl_mtu* repeat 2**

Procedure

Step 1 Choose **Devices > Device Management**.

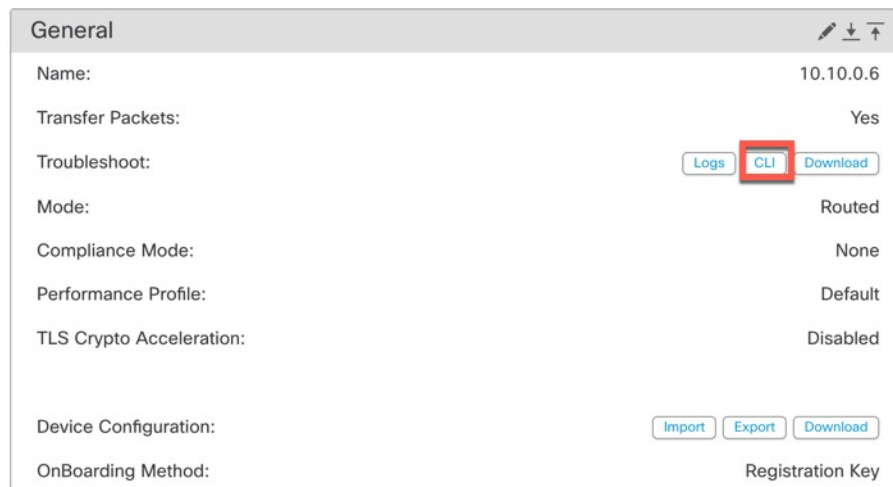
Step 2 Next to the device or cluster you want to view, click **Edit** (✎).

In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

Step 3 Click **Device** or **Cluster**.

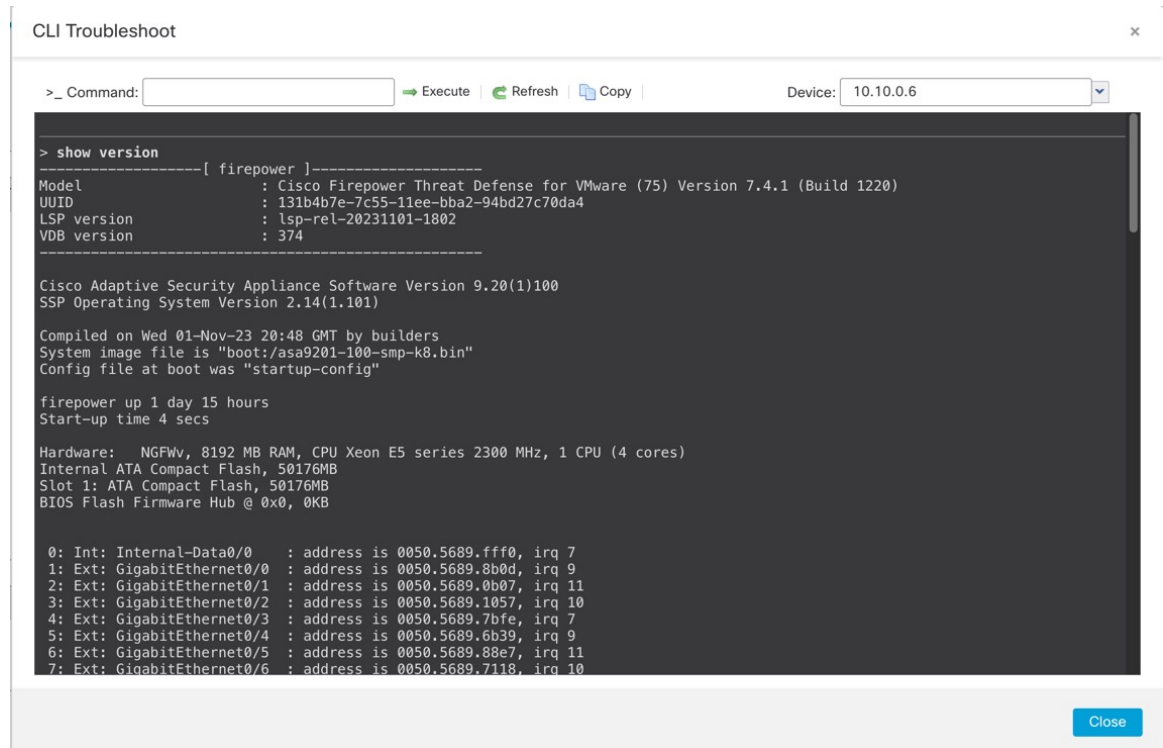
Step 4 In the **General > Troubleshoot** section, click **CLI**.

Figure 5: CLI



The **CLI Troubleshoot** dialog box appears with the pre-defined CLIs executed.

Figure 6: CLI Troubleshoot



- Step 5** On the **CLI Troubleshoot** dialog box, you can perform the following tasks.
- Enter a **show** command in the **Command** field, and click **Execute**. The new command output will be added to the window.
 - Click **Refresh** to re-run the predefined CLIs.
 - Click **Copy** to copy the output to your clipboard.
 - For a cluster, choose a different node from the **Device** drop down list.
- Step 6** Click **Close**.

Copy a Configuration to Another Device

When a new device is deployed in the network you can easily copy configurations and policies from a pre-configured device, instead of manually reconfiguring the new device.

Before you begin

Confirm that:

- The source and destination threat defense devices are the same model and are running the same version of the software.

- The source is either a standalone Secure Firewall Threat Defense device or a Secure Firewall Threat Defense high availability pair.
- The destination device is a standalone threat defense device.
- The source and destination threat defense devices have the same number of physical interfaces.
- The source and destination threat defense devices are in the same firewall mode - routed or transparent.
- The source and destination threat defense devices are in the same security certifications compliance mode.
- The source and destination threat defense devices are in the same domain.
- Configuration deployment is not in progress on either the source or the destination threat defense devices.

Procedure

Step 1 Choose **Devices > Device Management**.

Step 2 Next to the device you want to modify, click **Edit** (✎).

Step 3 Click **Device**.

Step 4 In the **General** section, do one of the following:

- Click **Get Device Configuration** (⇩) to copy device configuration from another device to the new device. On the **Get Device Configuration** page, select the source device in the **Select Device** drop-down list.
- Click **Push Device Configuration** (⇧) to copy device configuration from the current device to the new device. On the **Push Device Configuration** page, select the destination to which configuration is to be copied in the **Target Device** drop-down list.

Step 5 (Optional) Check **Include shared policies configuration** check box to copy policies.

Shared policies like AC policy, NAT, Platform Settings and FlexConfig policies can be shared across multiple devices.

Step 6 Click **OK**.

You can monitor the status of the copy device configuration task on **Tasks** in the Message Center.

When the copy device configuration task is initiated, it erases the configuration on the target device and copies the configuration of the source device to the destination device.



Warning When you have completed the copy device configuration task, you cannot revert the target device to its original configuration.

Export and Import the Device Configuration

You can export all of the the device-specific configuration configurable on the Device pages, including:

- Interfaces
- Inline Sets
- Routing
- DHCP
- VTEP
- Associated objects

You can then import the saved configuration for the same device in the following use cases:

- Moving the device to a different management center—First unregister the device from the original management center, then add the device to the new management center. Then you can import the saved configuration.
- Restore an old configuration—If you deployed changes that negatively impacted the operation of the device, you can import a backup copy of a known working configuration to restore a previous operational state.
- Reregistering a device—If you unregister a device from the management center, but then want to add it back, you can import the saved configuration.

See the following guidelines:

- You can only import the configuration to the same device (the UUID must match). You cannot import a configuration to a different device, even if it is the same model.
- Do not change the version running on the device between exporting and importing; the version must match.
- If an object doesn't exist, it will be created. If an object exists, but the value is different, see below:

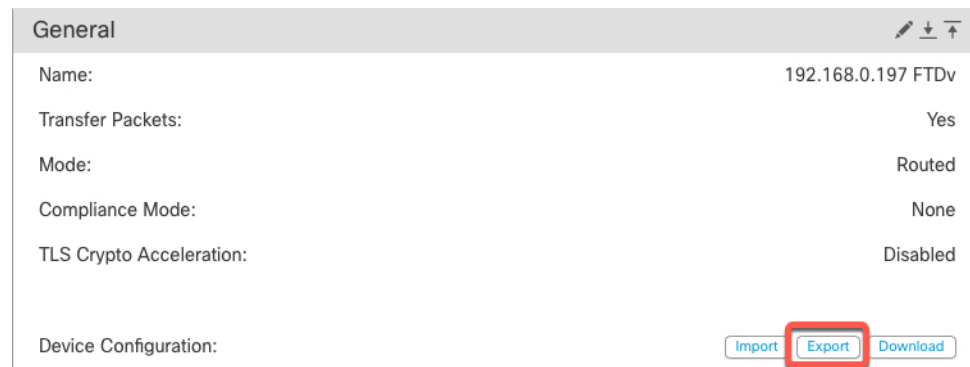
Table 2: Object Import Action

Scenario	Import Action
Object exists with the same name and value.	Reuse existing objects.
Object exists with the same name but different value.	<p>Network and Port objects: Create object overrides for this device. See Object Overrides.</p> <p>Interface objects: Create new objects. For example, if both the type (security zone or interface group) and the interface type (routed or switched, for example) do not match, then a new object is created.</p> <p>All other objects: Reuse existing objects even though the values are different.</p>
Object doesn't exist.	Create new object.s

Procedure

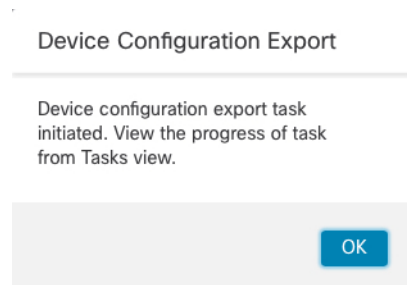
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to edit, click **Edit** (✎).
- Step 3** Click **Device**.
- Step 4** Export the configuration.
- a) In the **General** area, click **Export**.

Figure 7: Export Device Configuration



You are prompted to acknowledge the export; click **OK**.

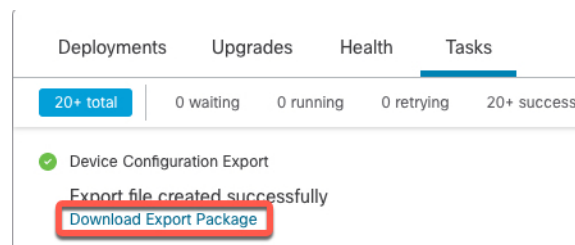
Figure 8: Acknowledge Export



You can view the export progress in the **Tasks** page.

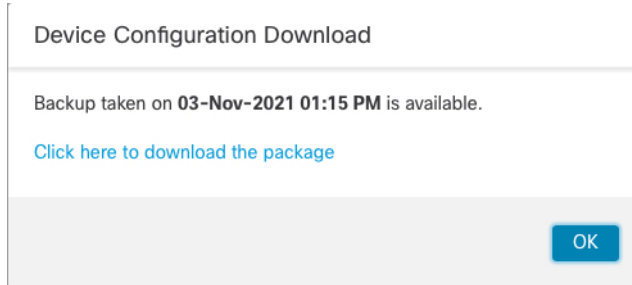
- b) On the **Notifications > Tasks** page, ensure that the export has completed; click **Download Export Package**. Alternatively, you can click the **Download** button in the **General** area.

Figure 9: Export Task



You are prompted to download the package; click **Click here to download the package** to save the file locally, and then click **OK** to exit the dialog box.

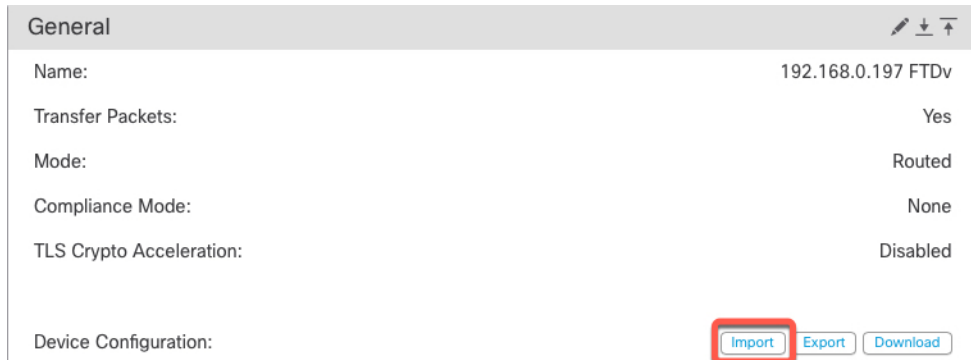
Figure 10: Download Package



Step 5 Import the configuration.

- a) In the **General** area, click **Import**.

Figure 11: Import Device Configuration



You are prompted to acknowledge that the current configuration will be replaced. Click **Yes**, and then navigate to the configuration package (with the suffix `.sfo`; note that this file is different from the Backup/Restore files).

Figure 12: Import Package

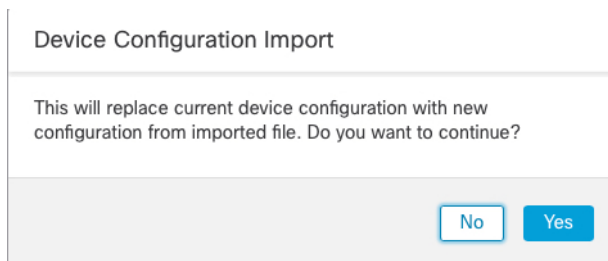
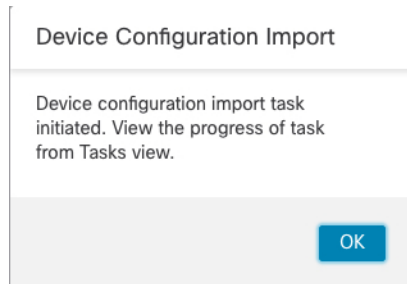


Figure 13: Navigate to Package



You are prompted to acknowledge the import; click **OK**.

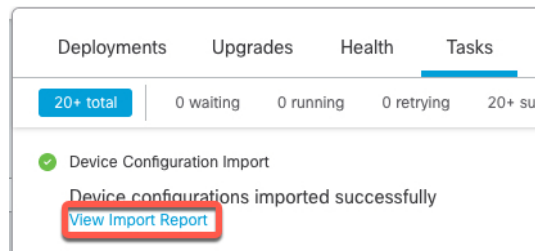
Figure 14: Acknowledge Import



You can view the import progress in the **Tasks** page.

- b) View the import reports so you can see what was imported. On the **Notifications > Tasks** page for the import task, click **View Import Report**.

Figure 15: View Import Report



The **Device Configuration Import Reports** page provides links to available reports.

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bdde3ad19d	Report does not exist	Device configurations import report

Edit License Settings

The **License** section of the **Device** page displays the licenses enabled for the device.

You can enable licenses on your device if you have available licenses on your management center.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device where you want to enable or disable licenses, click **Edit** (✎).

- Step 3** Click **Device**.
- Step 4** In the **License** section, click **Edit** (✎).
- Step 5** Check or clear the check box next to the license you want to enable or disable for the managed device.
- Step 6** Click **Save**.

What to do next

- Deploy configuration changes.

View System Information

The System section of the **Device** page displays a read-only table of system information, as described in the following table.

You can also shut down or restart the device.

Table 3: System Section Table Fields

Field	Description
Model	The model name and number for the managed device.
Serial	The serial number of the chassis of the managed device.
Time	The current system time of the device.
Time Zone	Shows the time zone.
Version	The version of the software currently installed on the managed device.
Time Zone setting for time-based rules	The current system time of the device, in the time zone specified in device platform settings.

View the Inspection Engine

The Inspection Engine section of the **Device** page shows whether your device uses Snort2 or Snort3. To switch the inspection engine, see *Enable Snort 3 on an Individual Device* in the [Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#).

View Health Information

The **Health** section of the **Device** page displays the information described in the table below.

Table 4: Health Section Table Fields

Field	Description
Status	An icon that represents the current health status of the device. Clicking the icon displays the Health Monitor for the appliance.
Policy	A link to a read-only version of the health policy currently deployed at the device.
Excluded	A link to the Health Exclude page, where you can enable and disable health exclusion modules.

Edit Management Settings

You can edit management settings in the **Management** area.

Update the Hostname or IP Address in the Management Center

If you edit the hostname or IP address of a device after you added it to the management center (using the device’s CLI, for example), you need to use the procedure below to manually update the hostname or IP address on the managing management center.

To change the device management IP address on the device, see [Modify Threat Defense Management Interfaces at the CLI, on page 41](#).

If you used only the NAT ID when registering the device, then the IP shows as **NO-IP** on this page, and you do not need to update the IP address/hostname.

If you used zero-touch provisioning to register the device on the outside interface, the hostname is automatically generated along with a matching DDNS configuration; you cannot edit the hostname in this case.

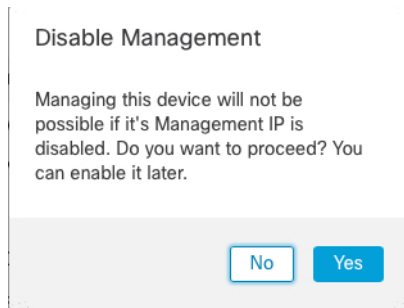
Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device where you want to modify management options, click **Edit** (✎).
- Step 3** Click **Device**, and view the **Management** area.
- Step 4** Disable management temporarily by clicking the slider so it is disabled (🔴).

Figure 16: Disable Management



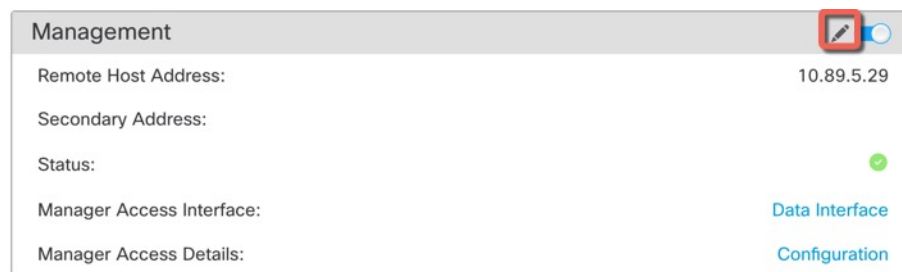
You are prompted to proceed with disabling management; click **Yes**.



Disabling management blocks the connection between the management center and the device, but does **not** unregister the device from the management center.

Step 5 Edit the **Remote Host Address** IP address and optional **Secondary Address** (when using a redundant data interface) or hostname by clicking **Edit** (✎).

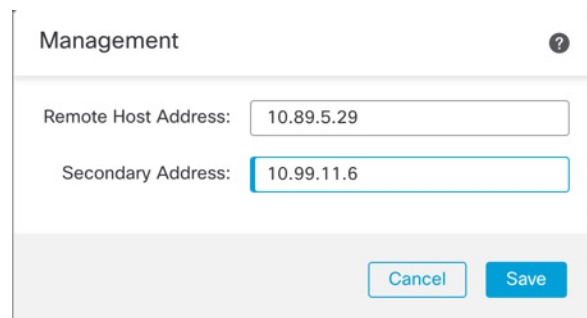
Figure 17: Edit Management Address



Step 6 In the **Management** dialog box, modify the name or IP address in the **Remote Host Address** field and the optional **Secondary Address** field, and click **Save**.

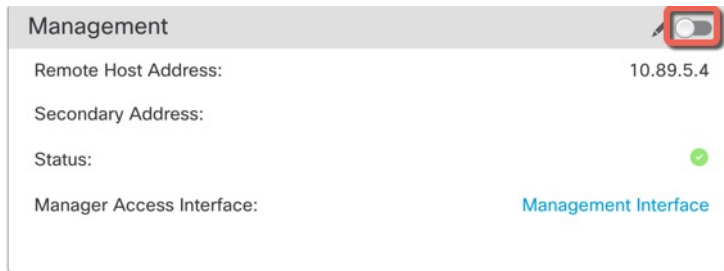
For information about using a secondary manager access data interface, see [Configure a Redundant Manager Access Data Interface, on page 36](#).

Figure 18: Management IP Address



Step 7 Reenable management by clicking the slider so it is enabled (🔘).

Figure 19: Enable Management Connection



Change Both Management Center and Threat Defense IP Addresses

You might want to change both management center and threat defense IP addresses if you need to move them to a new network.

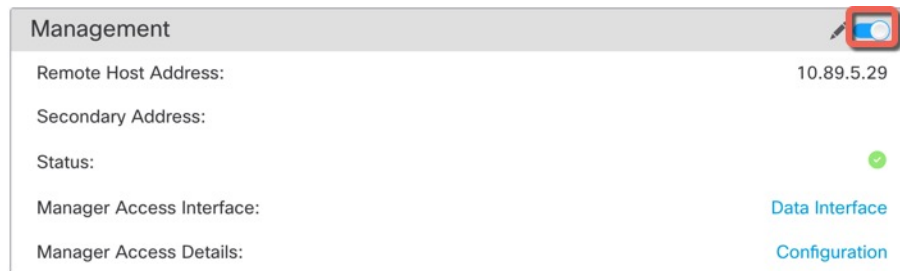
Procedure

Step 1 Disable the management connection.

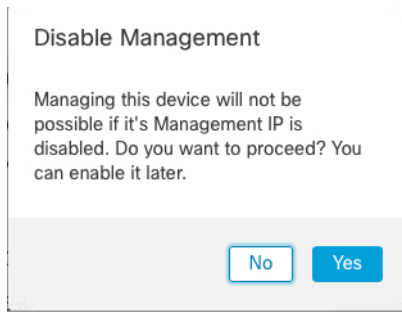
For a high-availability pair or cluster, perform these steps on all units.

- a) Choose **Devices > Device Management**.
- b) Next to the device, click **Edit** (✎).
- c) Click **Device**, and view the **Management** area.
- d) Disable management temporarily by clicking the slider so it is disabled (☐).

Figure 20: Disable Management



You are prompted to proceed with disabling management; click **Yes**.



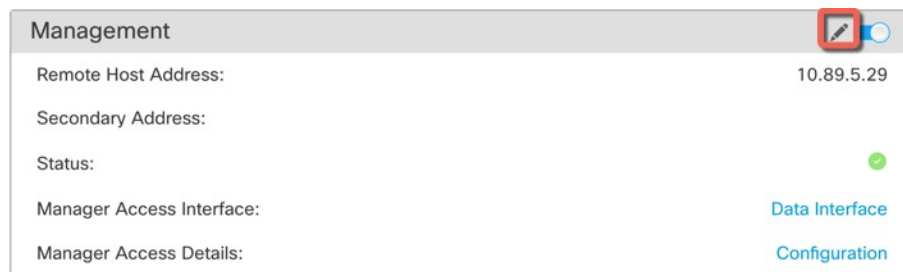
Step 2 Change the device IP address in the management center to the new device IP address.

You will change the IP address on the device later.

For a high-availability pair or cluster, perform these steps on all units.

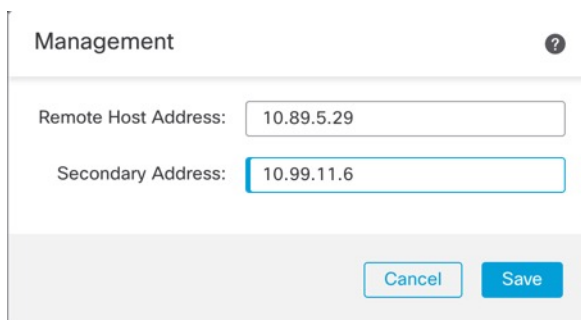
- a) Edit the **Remote Host Address** IP address and optional **Secondary Address** (when using a redundant data interface) or hostname by clicking **Edit** (✎).

Figure 21: Edit Management Address



- b) In the **Management** dialog box, modify the name or IP address in the **Remote Host Address** field and the optional **Secondary Address** field, and click **Save**.

Figure 22: Management IP Address



Step 3 Change the management center IP address.

Caution Be careful when making changes to the management center interface to which you are connected; if you cannot re-connect because of a configuration error, you need to access the management center console port to re-configure the network settings in the Linux shell. You must contact Cisco TAC to guide you in this operation.

- a) Choose **System** (⚙️) > **Configuration**, and then choose **Management Interfaces**.
- b) In the **Interfaces** area, click **Edit** next to the interface that you want to configure.
- c) Change the IP address, and click **Save**.

Step 4 Change the manager IP address on the device.

For a high-availability pair or cluster, perform these steps on all units.

- a) At the threat defense CLI, view the management center identifier.

show managers

Example:

```
> show managers
Type                : Manager
Host                : 10.10.1.4
Display name       : 10.10.1.4
Identifier          : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration        : Completed
Management type    : Configuration
```

- b) Edit the management center IP address or hostname.

configure manager edit identifier {hostname {ip_address | hostname} | displayname display_name}

If the management center was originally identified by **DONTRESOLVE** and a NAT ID, you can change the value to a hostname or IP address using this command. You cannot change an IP address or hostname to **DONTRESOLVE**.

Example:

```
> configure manager edit f7ffad78-bf16-11ec-a737-baa2f76ef602 hostname 10.10.5.1
```

Step 5 Change the IP address of the manager access interface at the console port.

For a high-availability pair or cluster, perform these steps on all units.

If you use the dedicated Management interface:


configure network ipv4

configure network ipv6

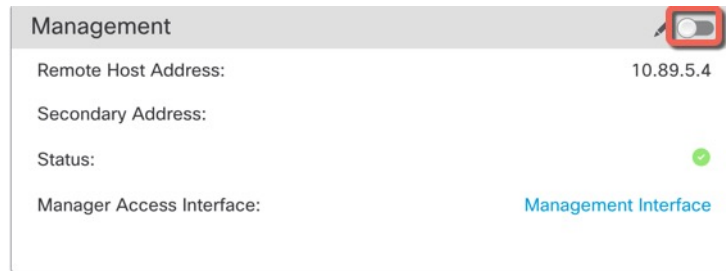
If you use the dedicated Management interface:

configure network management-data-interface disable

configure network management-data-interface

Step 6 Reenable management by clicking the slider so it is enabled ()

For a high-availability pair or cluster, perform these steps on all units.

Figure 23: Enable Management Connection

- Step 7** (If using a data interface for manager access) Refresh the data interface settings in the management center. For a high-availability pair, perform this step on both units.
- Choose **Devices > Device Management > Device > Management > Manager Access - Configuration Details**, and click **Refresh**.
 - Choose **Devices > Device Management > Interfaces**, and set the IP address to match the new address.
 - Return to the **Manager Access - Configuration Details** dialog box, and click **Acknowledge** to remove the deployment block.
- Step 8** Ensure the management connection is reestablished.

In the management center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

The following status shows a successful connection for a data interface, showing the internal "tap_nlp" interface.

Figure 24: Connection Status

Manager access - Configuration Details

Manager access configuration on device is in sync with the manager.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [\[Refresh \]](#)

```

> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down

```

[Close](#)

- Step 9** (For a high-availability management center pair) Repeat configuration changes on the secondary management center.
- Change the secondary management center IP address.
 - Specify the new peer addresses on both units.
 - Make the secondary unit the active unit.
 - Disable the device management connection.
 - Change the device IP address in the management center.
 - Reenable the management connection.

Change the Manager Access Interface from Management to Data

You can manage the threat defense from either the dedicated Management interface, or from a data interface. If you want to change the manager access interface after you added the device to the management center, follow these steps to migrate from the Management interface to a data interface. To migrate the other direction, see [Change the Manager Access Interface from Data to Management, on page 28](#).

Initiating the manager access migration from Management to data causes the management center to apply a block on deployment to the threat defense. To remove the block, enable manager access on the data interface. See the following steps to enable manager access on a data interface, and also configure other required settings.

Before you begin

For high-availability pairs, unless stated otherwise, perform all steps only on the active unit. Once the configuration changes are deployed, the standby unit synchronizes configuration and other state information from the active unit.

Procedure

Step 1

Initiate the interface migration.

- a) On the **Devices > Device Management** page, click **Edit** (✎) for the device.
- b) Go to the **Device > Management** section, and click the link for **Manager Access Interface**.

The **Manager Access Interface** field shows the current Management interface. When you click the link, choose the new interface type, **Data Interface**, in the **Manage device by** drop-down list.

Figure 25: Manager Access Interface

Manager Access Interface

This is an advanced setting and need to be configured only if needed. See the [online help](#) for detailed steps.

Manage device by

Data Interface

Switching the manager access interface from Management to Data interface causes the deployment to be blocked. To unblock the deploy, pick a data interface and enable it for manager Access. See the [online help](#) for detailed steps.

Close Save

- c) Click **Save**.

You must now complete the remaining steps in this procedure to enable manager access on the data interface. The **Management** area now shows **Manager Access Interface: Data Interface**, and **Manager Access Details: Configuration**.

Figure 26: Manager Access

Management

Remote Host Address: 10.10.1.12

Secondary Address:

Status: ✓

Manager Access Interface: Data Interface

Manager Access Details: Configuration

If you click **Configuration**, the **Manager Access - Configuration Details** dialog box opens. The **Manager Access Mode** shows a Deploy pending state.

Step 2 Enable manager access on a data interface on the **Devices > Device Management > Interfaces > Edit Physical Interface > Manager Access** page.

See [Configure Routed Mode Interfaces](#). You can enable manager access on one routed data interface, plus an optional secondary interface. Make sure these interfaces are fully configured with a name and IP address and that they are enabled.

If you use a secondary interface for redundancy, see [Configure a Redundant Manager Access Data Interface, on page 36](#) for additional required configuration.

Step 3 (Optional) If you use DHCP for the interface, enable the web type DDNS method on the **Devices > Device Management > DHCP > DDNS** page.

See [Configure Dynamic DNS](#). DDNS ensures the management center can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes.

Step 4 Make sure the threat defense can route to the management center through the data interface; add a static route if necessary on **Devices > Device Management > Routing > Static Route**.

See [Add a Static Route](#).

Step 5 (Optional) Configure DNS in a Platform Settings policy, and apply it to this device at **Devices > Platform Settings > DNS**.

See [DNS](#). DNS is required if you use DDNS. You may also use DNS for FQDNs in your security policies.

Step 6 (Optional) Enable SSH for the data interface in a Platform Settings policy, and apply it to this device at **Devices > Platform Settings > Secure Shell**.

See [SSH Access](#). SSH is not enabled by default on the data interfaces, so if you want to manage the threat defense using SSH, you need to explicitly allow it.

Step 7 Deploy configuration changes.

The management center will deploy the configuration changes over the current Management interface. After the deployment, the data interface is now ready for use, but the original management connection to Management is still active.

Step 8 At the threat defense CLI (preferably from the console port), set the Management interface to use a static IP address and set the gateway to use the data interfaces. For high availability, perform this step on both units.

configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

- *ip_address netmask*—Although you do not plan to use the Management interface, you must set a static IP address, for example, a private address so that you can set the gateway to **data-interfaces** (see the next bullet). You cannot use DHCP because the default route, which must be **data-interfaces**, might be overwritten with one received from the DHCP server.
- **data-interfaces**—This setting forwards management traffic over the backplane so it can be routed through the manager access data interface.

We recommend that you use the console port instead of an SSH connection because when you change the Management interface network settings, your SSH session will be disconnected.

Step 9 If necessary, re-cable the threat defense so it can reach the management center on the data interface. For high availability, perform this step on both units.

Step 10 In the management center, disable the management connection, update the **Remote Host Address** IP address and optional **Secondary Address** for the threat defense in the **Devices > Device Management > Device > Management** section, and reenble the connection.

See [Update the Hostname or IP Address in the Management Center, on page 18](#). If you used the threat defense hostname or just the NAT ID when you added the threat defense to the management center, you do not need to update the value; however, you need to disable and reenble the management connection to restart the connection.

Step 11 Ensure the management connection is reestablished.

In the management center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

The following status shows a successful connection for a data interface, showing the internal "tap_nlp" interface.

Figure 27: Connection Status

Manager access - Configuration Details

Manager access configuration on device is in sync with the manager.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [\[Refresh \]](#)

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

[Close](#)

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 51](#).

Change the Manager Access Interface from Data to Management

You can manage the threat defense from either the dedicated Management interface, or from a data interface. If you want to change the manager access interface after you added the device to the management center, follow these steps to migrate from a data interface to the Management interface. To migrate the other direction, see [Change the Manager Access Interface from Management to Data, on page 24](#).

Initiating the manager access migration from data to Management causes the management center to apply a block on deployment to the threat defense. You must disable manager access on the data interface to remove the block.

See the following steps to disable manager access on a data interface, and also configure other required settings.

Before you begin

For high-availability pairs, unless stated otherwise, perform all steps only on the active unit. Once the configuration changes are deployed, the standby unit synchronizes configuration and other state information from the active unit.

Procedure

Step 1

Initiate the interface migration.

- a) On the **Devices > Device Management** page, click **Edit** (✎) for the device.
- b) Go to the **Device > Management** section, and click the link for **Manager Access Interface**.

The **Manager Access Interface** field shows the current management interface as data. When you click the link, choose the new interface type, **Management Interface**, in the **Manage device by** drop-down list.

Figure 28: Manager Access Interface

Manager Access Interface

This is an advanced setting and need to be configured only if needed. See the [online help](#) for detailed steps.

Manage device by
Management Interface

Switching the manager access interface from Data to Management causes the deployment to be blocked. To unblock the deployment, ensure none of the data interfaces are set for manager access. See the [online help](#) for detailed steps.

Close Save

c) Click **Save**.

You must now complete the remaining steps in this procedure to enable manager access on the Management interface. The **Management** area now shows the **Manager Access Interface: Management Interface**, and **Manager Access Details: Configuration**.

Figure 29: Manager Access

Management

Remote Host Address: 10.10.1.12

Secondary Address:

Status: ✔

Manager Access Interface: Management Interface

If you click **Configuration**, the **Manager Access - Configuration Details** dialog box opens. The **Manager Access Mode** shows a Deploy pending state.

Step 2 Disable manager access on the data interface(s) on the **Devices > Device Management > Interfaces > Edit Physical Interface > Manager Access** page.

See [Configure Routed Mode Interfaces](#). This step removes the block on deployment.

Step 3 If you have not already done so, configure DNS settings for the data interface in a Platform Setting policy, and apply it to this device at **Devices > Platform Settings > DNS**.

See [DNS](#). The management center deployment that disables manager access on the data interface will remove any local DNS configuration. If that DNS server is used in any security policy, such as an FQDN in an Access Rule, then you must re-apply the DNS configuration using the management center.

Step 4 Deploy configuration changes.

The management center will deploy the configuration changes over the current data interface.

Step 5 If necessary, re-cable the threat defense so it can reach the management center on the Management interface. For High Availability, perform this step on both units.

Step 6 At the threat defense CLI, configure the Management interface IP address and gateway using a static IP address or DHCP. For high availability, perform this step on both units.

When you originally configured the data interface for manager access, the Management gateway was set to data-interfaces, which forwarded management traffic over the backplane so it could be routed through the manager access data interface. You now need to set an IP address for the gateway on the management network.

Static IP address:

```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```

DHCP:

```
configure network {ipv4 | ipv6} dhcp
```

Step 7 In the management center, disable the management connection, update the **Remote Host Address** IP address and remove the optional **Secondary Address** for the threat defense in the **Devices > Device Management > Device > Management** section, and reenable the connection.

See [Update the Hostname or IP Address in the Management Center, on page 18](#). If you used the threat defense hostname or just the NAT ID when you added the threat defense to the management center, you do not need to update the value; however, you need to disable and re-enable the management connection to restart the connection.

Step 8 Ensure the management connection is reestablished.

In the management center, check the management connection status on the **Devices > Device Management > Device > Management > Status** field or view notifications in the management center.

At the threat defense CLI, enter the `sftunnel-status-brief` command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 51](#).

Change the Manager Access Interface from Management to Data in a High Availability Pair

You can manage the FTD from either the dedicated Management interface, or from a data interface. If you want to change the Cisco Defense Orchestrator access interface after you added the device to CDO, follow these steps to migrate from the Management interface to a data interface. To migrate the other direction, see [Change the Manager Access Interface from Data to Management in a High Availability Pair, on page 34](#).

Initiating the CDO access migration from Management to data causes the CDO to apply a block on deployment to the FTD. To remove the block, enable CDO access on the data interface.



Note Unless stated otherwise, perform all steps mentioned in this section only on the active unit. Once the configuration changes are deployed, the standby unit synchronizes configuration and other state information from the active unit.

See the following steps to enable CDO access on a data interface, and also configure other required settings.

Before you begin

Model Support—Threat Defense

Procedure

Step 1 Initiate the interface migration.

- a) In the navigation bar, click **Inventory**.
- b) Click the **FTD** tab.
- c) Select the active device and in the **Management** pane on the right, click **Device Summary**.
- d) Under the **Management** area, click the link for **Manager Access Interface**.

The **Manager Access Interface** field shows the current management interface. When you click the link, choose the new interface type, **Data Interface**, in the **Manage device by** drop-down list.

Manager Access Interface

This is an advanced setting and need to be configured only if needed.
See the [online help](#) for detailed steps.

Manage device by

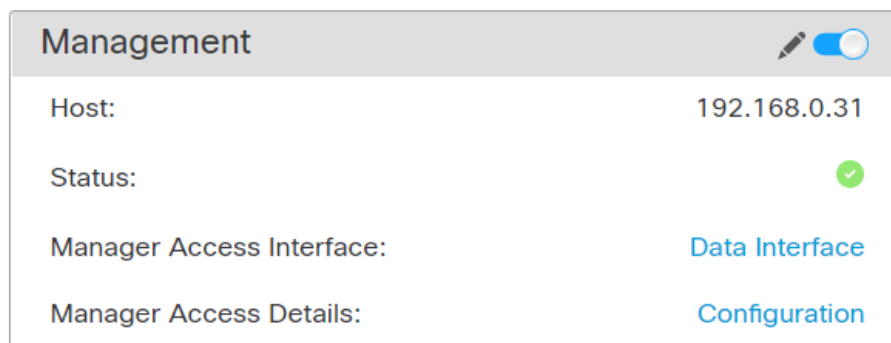
Data Interface

Note The link is unavailable for the standby unit as the access interface can be changed on the active unit.

- e) Click **Save**.

You must now complete the remaining steps in this procedure to enable CDO access on the data interface. The **Management** area now shows **Manager Access Interface: Data Interface**, and **Manager Access Details: Configuration**.

Figure 30: Manager Access



If you click **Configuration**, the **Manager Access - Configuration Details** dialog box opens. The **Manager Access Mode** shows a Deploy pending state.

Step 2 Enable CDO access on a data interface on the **Devices > Device Management > Interfaces > Edit Physical Interface > Manager Access** page.

See [Configure Routed Mode Interfaces](#). You can enable CDO access on one routed data interface. Make sure this interface is fully configured with a name and IP address and that it is enabled.

Step 3 Make sure the FTD can route to the CDO through the data interface; add a static route if necessary on **Devices > Device Management > Routing > Static Route**.

See [Add a Static Route](#).

Step 4 (Optional) Configure DNS in a Platform Settings policy, and apply it to this device at **Devices > Platform Settings > DNS**.

[DNS](#). DNS is required if you use DDNS. You may also use DNS for FQDNs in your security policies.

Step 5 (Optional) Enable SSH for the data interface in a Platform Settings policy, and apply it to this device at **Devices > Platform Settings > Secure Shell**.

See [SSH Access](#). SSH is not enabled by default on the data interfaces, so if you want to manage the FTD using SSH, you need to explicitly allow it.

Step 6 Deploy configuration changes.

The CDO will deploy the configuration changes over the current Management interface. After the deployment, the data interface is now ready for use, but the original management connection to Management is still active.

Step 7 At the FTD CLI (preferably from the console port), set the Management interface to use a static IP address and set the gateway to use the data interfaces.

configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces

- *ip_address netmask*—Although you do not plan to use the Management interface, you must set a static IP address, for example, a private address so that you can set the gateway to **data-interfaces** (see the next bullet).
- **data-interfaces**—This setting forwards management traffic over the backplane so it can be routed through the CDO access data interface.

We recommend that you use the console port instead of an SSH connection because when you change the Management interface network settings, your SSH session will be disconnected.

Note Repeat this step on the standby unit.

Step 8 When the deployment completes around 90 percent, the new management interface takes effect. At this stage, you must re-cable the FTD so that the CDO reaches FTD on the data interface and completes the deployment successfully.

After you re-cable, the deployment may fail if it timed out before re-establishing the management connection to the new interface. In that case, you must reinitiate the deployment after re-cabling for a successful deployment.

Note Repeat this step on the standby unit.

Step 9 Ensure the management connection is reestablished.

In CDO, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the FTD CLI, enter the **sftunnel-status-brief** command to view the management connection status.

The following status shows a successful connection for a data interface, showing the internal "tap_nlp" interface.

Figure 31: Connection Status

Manager access - Configuration Details

Manager access configuration on device is in sync with the manager.

Configuration CLI Output **Connection Status**

sftunnel-status-brief command output from Firewall Threat Defense [Refresh]

```
> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Peer channel Channel-B is valid type (EVENT), using 'tap_nlp', connected to '10.89.5.35' via '169.254.1.3'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Mon May 23 22:55:01 2022 UTC
Heartbeat Send Time: Mon May 23 22:56:21 2022 UTC
Heartbeat Received Time: Mon May 23 22:55:58 2022 UTC
Last disconnect time : Mon May 23 22:54:39 2022 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Close

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 51](#).

Change the Manager Access Interface from Data to Management in a High Availability Pair

You can manage the FTD from either the dedicated Management interface, or from a data interface. If you want to change the Cisco Defense Orchestrator access interface after you added the device to CDO, follow these steps to migrate from a Data interface to the Management interface. To migrate the other direction, see [Change the Manager Access Interface from Management to Data in a High Availability Pair, on page 30](#).

Initiating the CDO access migration from data to Management causes the CDO to apply a block on deployment to the FTD. You must disable CDO access on the data interface to remove the block.



Note Unless stated otherwise, perform all steps mentioned in this section only on the active unit. Once the configuration changes are deployed, the standby unit synchronizes configuration and other state information from the active unit.

See the following steps to disable CDO access on a data interface, and also configure other required settings.

Procedure

Step 1 Initiate the interface migration.

- a) In the navigation bar, click **Inventory**.
- b) Click the **FTD** tab.
- c) Select the active device and in the **Management** pane on the right, click **Device Summary**.
- d) Under the **Management** area, click the link for **Manager Access Interface**.

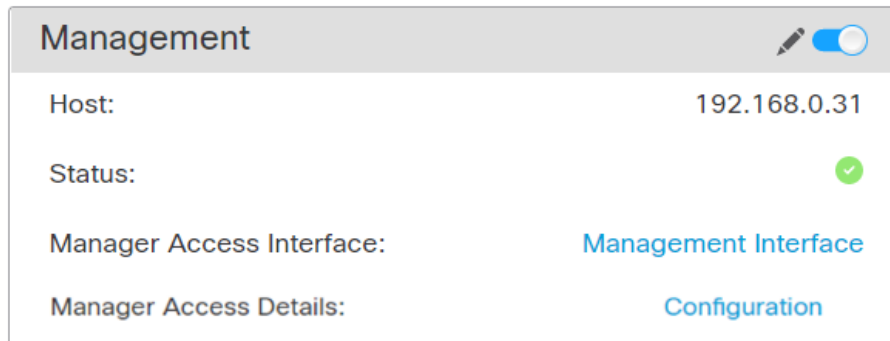
The **Manager Access Interface** field shows the current management interface as data. When you click the link, choose the new interface type, **Management Interface**, in the **Manage device by** drop-down list.

Note The link is unavailable for the standby unit as the access interface can be changed on the active unit.

- e) Click **Save**.

You must now complete the remaining steps in this procedure to enable CDO access on the data interface. The **Management** area now shows the **Manager Access Interface: Management Interface**, and **Manager Access Details: Configuration**.

Figure 32: Manager Access



If you click **Configuration**, the **Manager Access - Configuration Details** dialog box opens. The **Manager Access Mode** shows a Deploy pending state.

Step 2 Disable CDO access on a data interface on the **Devices > Device Management > Interfaces > Edit Physical Interface > FMC Access** page.

See [Configure Routed Mode Interfaces](#). This step removes the block on deployment.

Step 3 If you have not already done so, configure DNS settings for the data interface in a Platform Setting policy, and apply it to this device at **Devices > Platform Settings > DNS**.

See [DNS](#). The CDO deployment that disables CDO access on the data interface will remove any local DNS configuration. If that DNS server is used in any security policy, such as an FQDN in an Access Rule, then you must re-apply the DNS configuration using CDO.

Step 4 Deploy configuration changes.

The CDO will deploy the configuration changes over the current data interface.

Step 5 When the deployment completes around 90 percent, the new management interface takes effect. At this stage, you must re-cable the FTD so that the CDO reaches FTD on the Management interface and completes the deployment successfully.

After you re-cable, the deployment may fail if it timed out before re-establishing the management connection to the new interface. In that case, you must reinitiate the deployment after re-cabling for a successful deployment.

Note Repeat this step on the standby unit.

Step 6 At the FTD CLI, configure the Management interface IP address and gateway using a static IP address or DHCP.

When you originally configured the data interface for CDO access, the Management gateway was set to data-interfaces, which forwarded management traffic over the backplane so it could be routed through the CDO access data interface. You now need to set an IP address for the gateway on the management network.

Static IP address:

```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```

DHCP:

```
configure network {ipv4 | ipv6} dhcp
```

Note Repeat this step on the standby unit.

Step 7 Ensure the management connection is reestablished.

In CDO, check the management connection status on the **Devices > Device Management > Device > Management > Status** field or view notifications in CDO.

At the FTD CLI, enter the **sftunnel-status-brief** command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 51](#).

Configure a Redundant Manager Access Data Interface

When you use a data interface for manager access, you can configure a secondary data interface to take over management functions if the primary interface goes down. You can configure only one secondary interface. The device uses SLA monitoring to track the viability of the static routes and an ECMP zone that contains both interfaces so management traffic can use both interfaces.

High availability is not supported.

Before you begin

- The secondary interface needs to be in a separate security zone from the primary interface.
- All of the same requirements apply to the secondary interface as apply to the primary interface. See [Using the Threat Defense Data Interface for Management](#).

Procedure

Step 1 On the **Devices > Device Management** page, click **Edit** (✎) for the device.

Step 2 Enable manager access for the secondary interface.

This setting is in addition to standard interface settings such as enabling the interface, setting the name, setting the security zone, and setting a static IPv4 address.

- a) Choose **Interfaces > Edit Physical Interface > Manager Access**.
- b) Check **Enable management on this interface for the Manager**.
- c) Click **OK**.

Both interfaces show (**Manager Access**) in the interface listing.

Figure 33: Interface Listing

Interface	Logical Name	Type	Security Zones
Diagnostic1/1	diagnostic	Physical	
Ethernet1/1 (Manager Access)	outside	Physical	outside
Ethernet1/2		Physical	
Ethernet1/3		Physical	
Ethernet1/4		Physical	
Ethernet1/5		Physical	
Ethernet1/6		Physical	
Ethernet1/7		Physical	
Ethernet1/8 (Manager Access)	redundant	Physical	mgmt

Step 3 Add the secondary address to the **Management** settings.

- Click **Device**, and view the **Management** area.
- Click **Edit** ().

Figure 34: Edit Management Address

- In the **Management** dialog box, modify the name or IP address in the **Secondary Address** field

Figure 35: Management IP Address

- Click **Save**.

Step 4 Create an ECMP zone with both interfaces.

- a) Click **Routing**.
- b) From the virtual router drop-down, choose the virtual router in which the primary and secondary interfaces reside.
- c) Click **ECMP**, and then click **Add**.
- d) Enter a **Name** for the ECMP zone.
- e) Select the primary and secondary interfaces under the **Available Interfaces** box, and then click **Add**.

Figure 36: Add an ECMP Zone

The screenshot shows a dialog box titled "Add ECMP". At the top right of the dialog are a help icon (question mark) and a close icon (X). Below the title bar is a text input field labeled "Name" with the text "redundant-mgmt" entered. Below the name field are two columns: "Available Interfaces" and "Selected Interfaces". The "Available Interfaces" column is currently empty. The "Selected Interfaces" column contains two entries: "outside" and "redundant", each with a trash icon to its right. An "Add" button is located between the two columns. At the bottom right of the dialog are two buttons: "Cancel" and "OK".

- f) Click **OK**, and then **Save**.

Step 5

Add equal-cost default static routes for both interfaces and enable SLA tracking on both.

The routes should be identical except for the gateway and should both have metric 1. The primary interface should already have a default route that you can edit.

Figure 37: Add/Edit Static Route

Edit Static Route Configuration

Type: IPv4 IPv6

Interface*
outside

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Selected Network

Q Search

10.99.11.1
any-ipv4
IPv4-Benchmark-Tests
IPv4-Link-Local
IPv4-Multicast
IPv4-Private-10.0.0.0-8

any-ipv4

Ensure that egress virtualrouter has route to that destination

Gateway
10.89.5.1 +

Metric:
1
(1 - 254)

Tunneled: (Used only for default Route)

Route Tracking:
 +

- a) Click **Static Route**.
- b) Either click **Add Route** to add a new route, or click **Edit** () for an existing route.
- c) From the **Interface** drop-down, choose the interface.
- d) For the destination network, select **any-ipv4** from the **Available Networks** box and click **Add**.
- e) Enter the default **Gateway**.
- f) For **Route Tracking**, click **Add** () to add a new SLA monitor object.
- g) Enter the required parameters including the following:
 - The **Monitor Address** as the management center IP address.
 - The zone for the primary or secondary management interface in **Available Zones**; for example, choose the outside zone for the primary interface object, and the mgmt zone for the secondary interface object.

See [SLA Monitor](#) for more information.

Figure 38: Add SLA Monitor

New SLA Monitor Object ?

Name:

Description:

Frequency (seconds):
(1-604800)

SLA Monitor ID*:

Threshold (milliseconds):
(0-60000)

Timeout (milliseconds):
(0-604800000)

Data Size (bytes):
(0-16384)

ToS:

Number of Packets:

Monitor Address*:

Available Zones

- mgmt
- outside

Add

Selected Zones/Interfaces

- mgmt

Cancel Save

- h) Click **Save**, then choose the SLA object you just created in the **Route Tracking** drop-down list.
- i) Click **OK**, and then **Save**.
- j) Repeat for the default route for the other management interface.

Step 6 Deploy configuration changes.

As part of the deployment for this feature, the management center enables the secondary interface for management traffic, including auto-generated policy-based routing configuration for management traffic to get to the right data interface. The management center also deploys a second instance of the **configure network management-data-interface** command. Note that if you edit the secondary interface at the CLI, you cannot configure the gateway or otherwise alter the default route, because the static route for this interface can only be edited in the management center.

Modify Threat Defense Management Interfaces at the CLI

Modify the management interface settings on the managed device using the CLI. Many of these settings are ones that you set when you performed the initial setup; this procedure lets you change those settings, and set additional settings such as enabling an event interface if your model supports it, or adding static routes.



Note This topic applies to the dedicated Management interface. You can alternatively configure a data interface for management. If you want to change network settings for that interface, you should do so within management center and not at the CLI. If you need to troubleshoot a disrupted management connection, and need to make changes directly on the threat defense, see [Modify the Threat Defense Data Interface Used for Management at the CLI, on page 47](#).

For information about the threat defense CLI, see the [Cisco Secure Firewall Threat Defense Command Reference](#).



Note When using SSH, be careful when making changes to the management interface; if you cannot re-connect because of a configuration error, you will need to access the device console port.



Note If you change the device management IP address, then see the following tasks for management center connectivity depending on how you identified the management center during initial device setup using the **configure manager add** command:

- **IP address—No action.** If you identified the management center using a reachable IP address, then the management connection will be reestablished automatically after several minutes. We recommend that you also change the device IP address shown in management center to keep the information in sync; see [Update the Hostname or IP Address in the Management Center, on page 18](#). This action can help the connection reestablish faster. **Note:** If you specified an unreachable management center IP address, then see the procedure for NAT ID below.
- **NAT ID only—Manually reestablish the connection.** If you identified the management center using only the NAT ID, then the connection cannot be automatically reestablished. In this case, change the device management IP address in management center according to [Update the Hostname or IP Address in the Management Center, on page 18](#).



Note In a High Availability management center configuration, when you modify the management IP address from the device CLI or from the management center, the secondary management center does not reflect the changes even after an HA synchronization. To ensure that the secondary management center is also updated, switch roles between the two management centers, making the secondary management center the active unit. Modify the management IP address of the registered device on the device management page of the now active management center.

Before you begin

- You can create user accounts that can log into the CLI using the **configure user add** command; see [Add an Internal User at the CLI](#). You can also configure AAA users according to [External Authentication](#).

Procedure

-
- Step 1** Connect to the device CLI, either from the console port or using SSH.
- Step 2** Log in with the Admin username and password.
- Step 3** (Firepower 4100/9300/Secure Firewall 4200 only) Enable the second management interface as an event-only interface.

configure network management-interface enable management1**configure network management-interface disable-management-channel management1**

You always need a management interface for management traffic. If your device has a second management interface, you can enable it for event-only traffic.

You can optionally disable events for the main management interface using the **configure network management-interface disable-events-channel** command. In either case, the device will try to send events on the event-only interface, and if that interface is down, it will send events on the management interface even if you disable the event channel.

You cannot disable both event and management channels on an interface.

To use a separate event interface, you also need to enable an event interface on the management center. See the [Cisco Secure Firewall Management Center Administration Guide](#).

Example:

```
> configure network management-interface enable management1
Configuration updated successfully

> configure network management-interface disable-management-channel management1
Configuration updated successfully

>
```

- Step 4** Configure the IP address of the management interface and/or event interface:

If you do not specify the *management_interface* argument, then you change the network settings for the default management interface. When configuring an event interface, be sure to specify the *management_interface* argument. The event interface can be on a separate network from the management interface, or on the same network. If you are connected to the interface you are configuring, you will be disconnected. You can re-connect to the new IP address.

- a) Configure the IPv4 address:

- Manual configuration:

configure network ipv4 manual ip_address netmask gateway_ip [management_interface]

Note that the *gateway_ip* in this command is used to create the default route for the device. If you configure an event-only interface, then you must enter the *gateway_ip* as part of the command; however, this entry just configures the default route to the value you specify and does not create a

separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you set the *gateway_ip* for use with the management interface, and then create a static route separately for the event-only interface using the **configure network static-routes** command.

Example:

```
> configure network ipv4 manual 10.10.10.45 255.255.255.0 10.10.10.1 management1
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

- DHCP (supported on the default management interface only):

configure network ipv4 dhcp

- b) Configure the IPv6 address:

- Stateless autoconfiguration:

configure network ipv6 router [*management_interface*]

Example:

```
> configure network ipv6 router management0
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- Manual configuration:

configure network ipv6 manual *ip6_address ip6_prefix_length* [*ip6_gateway_ip*]
[*management_interface*]

Note that the *ipv6_gateway_ip* in this command is used to create the default route for the device. If you configure an event-only interface, then you must enter the *ipv6_gateway_ip* as part of the command; however, this entry just configures the default route to the value you specify and does not create a separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you set the *ipv6_gateway_ip* for use with the management interface, and then create a static route separately for the event-only interface using the **configure network static-routes** command.

Example:

```
> configure network ipv6 manual 2001:0DB8:BA98::3210 64 management1
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- DHCPv6 (supported on the default management interface only):

configure network ipv6 dhcp

Step 5 For IPv6, enable or disable ICMPv6 Echo Replies and Destination Unreachable messages. These messages are enabled by default.

```
configure network ipv6 destination-unreachable {enable | disable}
```

```
configure network ipv6 echo-reply {enable | disable}
```

You might want to disable these packets to guard against potential denial of service attacks. Disabling Echo Reply packets means you cannot use IPv6 ping to the device management interfaces for testing purposes.

Example:

```
> configure network ipv6 destination-unreachable disable
> configure network ipv6 echo-reply disable
```

Step 6 Enable a DHCP server on the default management interface to provide IP addresses to connected hosts:

```
configure network ipv4 dhcp-server-enable start_ip_address end_ip_address
```

Example:

```
> configure network ipv4 dhcp-server-enable 10.10.10.200 10.10.10.254
DHCP Server Enabled
>
```

You can only configure a DHCP server when you set the management interface IP address manually. This command is not supported on the management center virtual. To display the status of the DHCP server, enter **show network-dhcp-server**:

```
> show network-dhcp-server
DHCP Server Enabled
10.10.10.200-10.10.10.254
```

Step 7 Add a static route for the event-only interface if the management center is on a remote network; otherwise, all traffic will match the default route through the management interface.

```
configure network static-routes {ipv4 | ipv6} add management_interface destination_ip netmask_or_prefix gateway_ip
```

For the *default* route, do not use this command; you can only change the default route gateway IP address when you use the **configure network ipv4** or **ipv6** commands (see [Step 4, on page 42](#)).

Example:

```
> configure network static-routes ipv4 add management1 192.168.6.0 255.255.255.0 10.10.10.1
Configuration updated successfully

> configure network static-routes ipv6 add management1 2001:0DB8:AA89::5110 64
2001:0DB8:BA98::3211
Configuration updated successfully

>
```

To display static routes, enter **show network-static-routes** (the default route is not shown):

```
> show network-static-routes
-----[ IPv4 Static Routes ]-----
Interface           : management1
Destination         : 192.168.6.0
Gateway             : 10.10.10.1
Netmask             : 255.255.255.0
[...]
```

Step 8 Set the hostname:

configure network hostname *name*

Example:

```
> configure network hostname farscapel.cisco.com
```

Syslog messages do not reflect a new hostname until after a reboot.

Step 9 Set the search domains:

configure network dns searchdomains *domain_list*

Example:

```
> configure network dns searchdomains example.com,cisco.com
```

Set the search domain(s) for the device, separated by commas. These domains are added to hostnames when you do not specify a fully-qualified domain name in a command, for example, **ping system**. The domains are used only on the management interface, or for commands that go through the management interface.

Step 10 Set up to 3 DNS servers, separated by commas:

configure network dns servers *dns_ip_list*

Example:

```
> configure network dns servers 10.10.6.5,10.20.89.2,10.80.54.3
```

Step 11 Set the remote management port for communication with the management center:

configure network management-interface tcpport *number*

Example:

```
> configure network management-interface tcpport 8555
```

The management center and managed devices communicate using a two-way, TLS-1.3-encrypted communication channel, which by default is on port 8305.

Note Cisco **strongly** recommends that you keep the default settings for the remote management port, but if the management port conflicts with other communications on your network, you can choose a different port. If you change the management port, you must change it for **all** devices in your deployment that need to communicate with each other.

Step 12 (Threat Defense only) Set the management or eventing interface MTU. The MTU is 1500 bytes by default.

configure network mtu [*bytes*] [*interface_id*]

- *bytes*—Sets the MTU in bytes. For the management interface, the value can be between 64 and 1500 if you enable IPv4, and 1280 to 1500 if you enable IPv6. For the eventing interface, the value can be between 64 and 9000 if you enable IPv4, and 1280 to 9000 if you enable IPv6. If you enable both IPv4 and IPv6, then the minimum is 1280. If you do not enter the *bytes*, you are prompted for a value.
- *interface_id*—Specifies the interface ID on which to set the MTU. Use the **show network** command to see available interface IDs, for example management0, management1, br1, and eth0, depending on the platform. If you do not specify an interface, then the management interface is used.

Example:

```
> configure network mtu 8192 management1
MTU set successfully to 1500 from 8192 for management1
Refreshing Network Config...
NetworkSettings::refreshNetworkConfig MTU value at start 8192

Interface management1 speed is set to '10000baseT/Full'
NetworkSettings::refreshNetworkConfig MTU value at end 8192
>
```

Step 13

Configure an HTTP proxy. The device is configured to directly-connect to the internet on ports TCP/443 (HTTPS) and TCP/80 (HTTP). You can use a proxy server, to which you can authenticate via HTTP Digest. After issuing the command, you are prompted for the HTTP proxy address and port, whether proxy authentication is required, and if it is required, the proxy username, proxy password, and confirmation of the proxy password.

Note For proxy password on threat defense, you can use A-Z, a-z, and 0-9 characters only.

configure network http-proxy**Example:**

```
> configure network http-proxy
Manual proxy configuration
Enter HTTP Proxy address: 10.100.10.10
Enter HTTP Proxy Port: 80
Use Proxy Authentication? (y/n) [n]: Y
Enter Proxy Username: proxyuser
Enter Proxy Password: proxypassword
Confirm Proxy Password: proxypassword
```

Step 14

If you change the device management IP address, then see the following tasks for management center connectivity depending on how you identified the management center during initial device setup using the **configure manager add** command:

- **IP address—No action.** If you identified the management center using a reachable IP address, then the management connection will be reestablished automatically after several minutes. We recommend that you also change the device IP address shown in management center to keep the information in sync; see [Update the Hostname or IP Address in the Management Center, on page 18](#). This action can help the connection reestablish faster. **Note:** If you specified an unreachable management center IP address, then you must manually reestablish the connection using [Update the Hostname or IP Address in the Management Center, on page 18](#).
- **NAT ID only—Manually reestablish the connection.** If you identified the management center using only the NAT ID, then the connection cannot be automatically reestablished. In this case, change the

device management IP address in management center according to [Update the Hostname or IP Address in the Management Center, on page 18](#).

Modify the Threat Defense Data Interface Used for Management at the CLI

If the management connection between the threat defense and the management center was disrupted, and you want to specify a new data interface to replace the old interface, use the threat defense CLI to configure the new interface. This procedure assumes you want to replace the old interface with a new interface on the same network. If the management connection is active, then you should make any changes to an existing data interface using the management center. For initial setup of the data management interface, see the **configure network management-data-interface** command.

For high-availability pairs, perform all CLI steps on both units. Within the management center, perform steps only on the active unit. Once the configuration changes are deployed, the standby unit synchronizes configuration and other state information from the active unit.



Note This topic applies to the data interface that you configured for Management, not the dedicated Management interface. If you want to change network settings for the Management interface, see [Modify Threat Defense Management Interfaces at the CLI, on page 41](#).

For information about the threat defense CLI, see the [Cisco Secure Firewall Threat Defense Command Reference](#).

Before you begin

You can create user accounts that can log into the CLI using the **configure user add** command. You can also configure AAA users according to [External Authentication](#).

Procedure

- Step 1** If you are changing the data management interface to a new interface, move the current interface cable to the new interface.
- Step 2** Connect to the device CLI.
- You should use the console port when using these commands. If you are performing initial setup, then you may be disconnected from the Management interface. If you are editing the configuration due to a disrupted management connection, and you have SSH access to the dedicated Management interface, then you can use that SSH connection.
- Step 3** Log in with the Admin username and password.
- Step 4** Disable the interface so you can reconfigure its settings.

configure network management-data-interface disable

Example:

```
> configure network management-data-interface disable

Configuration updated successfully..!!
```

Configuration disable was successful, please update the default route to point to a gateway on management interface using the command 'configure network'

Step 5 Configure the new data interface for manager access.

configure network management-data-interface

You are then prompted to configure basic network settings for the data interface.

When you change the data management interface to a new interface on the same network, use the same settings as for the previous interface except the interface ID. In addition, for the **Do you wish to clear all the device configuration before applying ? (y/n) [n]**: option, choose **y**. This choice will clear the old data management interface configuration, so that you can successfully reuse the IP address and interface name on the new interface.

```
> configure network management-data-interface
Data interface to use for management: ethernet1/4
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y
```

Configuration done with option to allow manager access from any network, if you wish to change the manager access network use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>

Step 6 (Optional) Limit data interface access to the management center on a specific network.

configure network management-data-interface client ip_address netmask

By default, all networks are allowed.

Step 7 The connection will be reestablished automatically, but disabling and reenabling the connection in the management center will help the connection reestablish faster. See [Update the Hostname or IP Address in the Management Center, on page 18](#).

Step 8 Check that the management connection was reestablished.

sftunnel-status-brief

See the following sample output for a connection that is up, with peer channel and heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202' via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202' via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
```



```
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Step 9 In the management center, choose **Devices > Device Management > Device > Management > Manager Access - Configuration Details**, and click **Refresh**.

The management center detects the interface and default route configuration changes, and blocks deployment to the threat defense. When you change the data interface settings locally on the device, you must reconcile those changes in the management center manually. You can view the discrepancies between the management center and the threat defense on the **Configuration** tab.

Step 10 Choose **Devices > Device Management > Interfaces**, and make the following changes.

- a) Remove the IP address and name from the old data management interface, and disable manager access for this interface.
- b) Configure the new data management interface with the settings of the old interface (the ones you used at the CLI), and enable manager access for it.

Step 11 Choose **Devices > Device Management > Routing > Static Route** and change the default route from the old data management interface to the new one.

Step 12 Return to the **Manager Access - Configuration Details** dialog box, and click **Acknowledge** to remove the deployment block.

The next time you deploy, the management center configuration will overwrite any remaining conflicting settings on the threat defense. It is your responsibility to manually fix the configuration in the management center before you re-deploy.

You will see expected messages of "Config was cleared" and "Manager access changed and acknowledged."

Manually Roll Back the Configuration if the Management Center Loses Connectivity

If you use a data interface on the threat defense for manager access, and you deploy a configuration change from the management center that affects the network connectivity, you can roll back the configuration on the threat defense to the last-deployed configuration so you can restore management connectivity. You can then adjust the configuration settings in management center so that the network connectivity is maintained, and re-deploy. You can use the rollback feature even if you do not lose connectivity; it is not limited to this troubleshooting situation.

Alternatively, you can enable auto rollback of the configuration if you lose connectivity after a deployment; see [Edit Deployment Settings, on page 66](#).

See the following guidelines:

- Only the previous deployment is available locally on the threat defense; you cannot roll back to any earlier deployments.
- Rollback is supported for high availability but not supported for clustering deployments.
- Rollback is not supported immediately after high availability creation.
- The rollback only affects configurations that you can set in the management center. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the threat defense CLI. Note that if you changed data interface settings after the last management center deployment using the **configure network management-data-interface**

command, and then you use the rollback command, those settings will not be preserved; they will roll back to the last-deployed management center settings.

- UCAPL/CC mode cannot be rolled back.
- Out-of-band SCEP certificate data that was updated during the previous deployment cannot be rolled back.
- During the rollback, connections will drop because the current configuration will be cleared.

Procedure

Step 1

At the threat defense CLI, roll back to the previous configuration.

configure policy rollback

Note For a high availability pair, this command is allowed only on the active unit.

After the rollback, the threat defense notifies the management center that the rollback was completed successfully. In the management center, the deployment screen will show a banner stating that the configuration was rolled back.

Note If the rollback failed and the management center management is restored, refer to <https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html> for common deployment problems. In some cases, the rollback can fail after the management center management access is restored; in this case, you can resolve the management center configuration issues, and redeploy from the management center.

Example:

For the threat defense that uses a data interface for manager access:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
.....
.....
>
```

Example:

For threat defenses in a high availability pair that use a data interface for management center access:

```
> configure policy rollback

Checking Eligibility ....
===== DEVICE DETAILS =====
```

```

Device Version: 7.2.0
Device Type: FTD
Device Mode: Offbox
Device in HA: true
Is HA disabled: false
HA state: active - standby ready
=====
Device is eligible for policy rollback
Do you want to continue [YES/NO]?

YES

Starting rollback...
  Preparing policy configuration on the device.           Status: success
  Applying updated policy configuration on the device.    Status: success
  Applying Lina File Configuration on the device.        Status: success
  Applying Lina Configuration on the device.             Status: success
  Commit Lina Configuration.                             Status: success
  Commit Lina File Configuration.                       Status: success
  Commit Lina File Configuration.                       Status: success
=====
POLICY ROLLBACK STATUS: SUCCESS
=====
>

```

Step 2 Check that the management connection was reestablished.

In management center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 51](#).

Troubleshoot Management Connectivity on a Data Interface

When you use a data interface for manager access instead of using the dedicated Management interface, you must be careful about changing the interface and network settings for the threat defense in the management center so you do not disrupt the connection. If you change the management interface type after you add the threat defense to the management center (from data to Management, or from Management to data), if the interfaces and network settings are not configured correctly, you can lose management connectivity.

This topic helps you troubleshoot the loss of management connectivity.

View management connection status

In the management center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status. You can also use **sftunnel-status** to view more complete information.

See the following sample output for a connection that is down; there is no peer channel "connected to" information, nor heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

See the following sample output for a connection that is up, with peer channel and heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
  via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
  via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

View the threat defense network information

At the threat defense CLI, view the Management and manager access data interface network settings:

show network

```
> show network
===== [ System Information ] =====
Hostname                : FTD-4
Domains                 : cisco.com
DNS Servers             : 72.163.47.11
DNS from router        : enabled
Management port        : 8305
IPv4 Default route
  Gateway               : data-interfaces

===== [ management0 ] =====
Admin State             : enabled
Admin Speed             : 1gbps
Operation Speed        : 1gbps
Link                   : up
Channels                : Management & Events
Mode                   : Non-Autonegotiation
MDI/MDIX               : Auto/MDIX
MTU                    : 1500
MAC Address            : 68:87:C6:A6:54:80
----- [ IPv4 ] -----
Configuration          : Manual
Address                : 10.89.5.4
Netmask                : 255.255.255.192
Gateway                : 169.254.1.1
----- [ IPv6 ] -----
Configuration          : Disabled

===== [ Proxy Information ] =====
State                  : Disabled
Authentication         : Disabled
```

```

===== [ System Information - Data Interfaces ] =====
DNS Servers           : 72.163.47.11
Interfaces            : Ethernet1/1

===== [ Ethernet1/1 ] =====
State                 : Enabled
Link                  : Up
Name                  : outside
MTU                   : 1500
MAC Address           : 68:87:C6:A6:54:A4
----- [ IPv4 ] -----
Configuration         : Manual
Address               : 10.89.5.6
Netmask               : 255.255.255.192
Gateway               : 10.89.5.1
----- [ IPv6 ] -----
Configuration         : Disabled

```

Check that the threat defense registered with the management center

At the threat defense CLI, check that the management center registration was completed. Note that this command will not show the *current* status of the management connection.

show managers

```

> show managers
Type                : Manager
Host                 : 16a3893c-caa7-11ee-8436-0925c06e7608DONTRESOLVE
Display name        : manager-1707852946.80444
Version             : 7.6.0 (Build 1385)
Identifier           : a904b8b2-ca9a-11ee-a583-5e804c16b2fd
Registration        : Completed
Management type     : Configuration

```

Ping the management center

At the threat defense CLI, use the following command to ping the management center from the data interfaces:

ping *fmc_ip*

At the threat defense CLI, use the following command to ping the management center from the Management interface, which should route over the backplane to the data interfaces:

ping system *fmc_ip*

Capture packets on the threat defense internal interface

At the threat defense CLI, capture packets on the internal backplane interface (*nlp_int_tap*) to see if management packets are being sent:

capture *name* interface *nlp_int_tap* trace detail match ip any any

show capture *name* trace detail

Check the internal interface status, statistics, and packet count

At the threat defense CLI, see information about the internal backplane interface, *nlp_int_tap*:

show interface detail

```

> show interface detail
[...]
```

```

Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_ymtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
  (Full-duplex), (1000 Mbps)
  Input flow control is unsupported, output flow control is unsupported
  MAC address 0000.0100.0001, MTU 1500
  IP address 169.254.1.1, subnet mask 255.255.255.248
  37 packets input, 2822 bytes, 0 no buffer
  Received 0 broadcasts, 0 runts, 0 giants
  0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
  0 pause input, 0 resume input
  0 L2 decode drops
  5 packets output, 370 bytes, 0 underruns
  0 pause output, 0 resume output
  0 output errors, 0 collisions, 0 interface resets
  0 late collisions, 0 deferred
  0 input reset drops, 0 output reset drops
  input queue (blocks free curr/low): hardware (0/0)
  output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
  37 packets input, 2304 bytes
  5 packets output, 300 bytes
  37 packets dropped
    1 minute input rate 0 pkts/sec,  0 bytes/sec
    1 minute output rate 0 pkts/sec,  0 bytes/sec
    1 minute drop rate, 0 pkts/sec
    5 minute input rate 0 pkts/sec,  0 bytes/sec
    5 minute output rate 0 pkts/sec,  0 bytes/sec
    5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
  Interface number is 14
  Interface config status is active
  Interface state is active

```

Check routing and NAT

At the threat defense CLI, check that the default route (S*) was added and that internal NAT rules exist for the Management interface (nlp_int_tap).

show route

```

> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*    0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C     10.89.5.0 255.255.255.192 is directly connected, outside
L     10.89.5.29 255.255.255.255 is directly connected, outside

>

```

show nat

```

> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface service
  tcp 8305 8305
  translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface service
  tcp ssh ssh
  translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
  ipv6 service tcp 8305 8305
  translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
  translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
  translate_hits = 0, untranslate_hits = 0
>

```

Check other settings

See the following commands to check that all other settings are present. You can also see many of these commands on the management center's **Devices > Device Management > Device > Management > Manager Access - Configuration Details > CLI Output** page.

show running-config sftunnel

```

> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305

```

show running-config ip-client

```

> show running-config ip-client
ip-client outside

```

show conn address *fmc_ip*

```

> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
  preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap 10.89.5.29(169.254.1.2):51231 outside 10.89.5.35:8305, idle 0:00:04,
  bytes 86684, flags UxIO
TCP nlp_int_tap 10.89.5.29(169.254.1.2):8305 outside 10.89.5.35:52019, idle 0:00:02,
  bytes 1630834, flags UIO
>

```

Check for a successful DDNS update

At the threat defense CLI, check for a successful DDNS update:

debug ddns

```

> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfully updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0

```

If the update failed, use the **debug http** and **debug ssl** commands. For certificate validation failures, check that the root certificates are installed on the device:

show crypto ca certificates *trustpoint_name*

To check the DDNS operation:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside
```

```
Dynamic DNS Update on outside:
  Update Method Name Update Destination
  RBD_DDNS not available
```

```
Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Check management center log files

See <https://cisco.com/go/fmc-reg-error>.

Troubleshoot Management Connectivity on a Data Interface in a High Availability Pair

This topic helps you troubleshoot the loss of management connectivity on a data interface in High Availability.

Model Support—Threat Defense

The management connection between the active peer and the CDO can be disrupted due to the following reasons:

- Data interface used for management on the Active unit has connectivity issues.
You should manually fail over to the standby unit and then configure a new data interface for CDO access.
- Internet Service Provider has changed.
You should manually update the new network details on the active unit using the CLI commands to restore the device connectivity with CDO .

Data Management Interface on Active unit has Connectivity Issues

1. In CDO, manually switch the active unit to standby. See [Switch the Active Peer in the Threat Defense High Availability Pair](#).
Alternatively, you can run the **no failover active** command on the active unit.
The standby device becomes the new active device in the high availability pair and establishes communication with CDO.
2. Next to the device high-availability pair you want to edit, click **Edit** (✎).
3. Choose **Routing > Static Route** and delete the static route defined for the old data management interface.
4. Click the **Interfaces** tab, and make the following changes.

- a. Remove the IP address and name from the old data management interface, and disable CDO Access for this interface.



Note Before removing the old data management interface information, remember the details if you want to use the same information.

1. Click the **Edit** (✎) next to the interface you want to remove.

The screenshot shows the 'Edit Physical Interface' configuration window. At the top, there are tabs for 'General', 'IPv4', 'IPv6', 'Advanced', 'Path Monitoring', and 'Hardware Configuration'. Below the tabs is the 'Firewall Management Center Access' section. The 'Name' field is set to 'outside'. There are two checkboxes: 'Enabled' (checked) and 'Management Only' (unchecked). Below these is a 'Description' field which is currently empty.

2. Clear the content in the **Name** field.
 3. Uncheck the **Enabled** checkbox.
 4. In the **IPv4** or **IPv6** tab, remove the active address.
 5. In the **Firewall Management Center Access** tab, uncheck **Enable management on this interface for the Firepower Management Center**.
 6. Click **OK**.
 7. Click **Yes** to confirm the changes.
- b. Configure the new data management interface with the settings of the old interface (the ones you used at the CLI), and enable CDO Access for it.
 1. Click **Edit** (✎) next to the data interface you want for handling management traffic.
 2. In the **Name** field, specify a name for the interface.
 3. Check the **Enabled** checkbox.
 4. In the **IPv4** or **IPv6** tab, specify the active address.
 5. In the **Firewall Management Center Access** tab, check **Enable management on this interface for the Firepower Management Center**.
 6. Click **OK**.
 7. Click **Yes** to confirm the changes.
5. Click the **High Availability** tab, and make the following changes.

- a. In the **Monitored Interfaces** area, click the **Edit** (✎) next to the new data management interface.

Monitored Interfaces						
Interface Name	Active IPv4	Standby IPv4	Active IPv6 - Standby IPv6	Active Link-Local IPv6	Standby Link-Local IPv6	Monitor
outside-new	192.168.0.11					
diagnostic						

The **Active IP Address** shows the active device's IP address.

- b. On the **IPv4** tab, enter the **Standby IP Address** and **Gateway** address.

Edit outside-new ?

Monitor this interface for failures

IPv4 **IPv6**

Interface Name:
outside-new

Active IP Address:
192.168.0.11

Mask:
255.255.255.0

Standby IP Address:

- c. If you configured the IPv6 address manually, on the IPv6 tab, click **Edit** (✎) next to the active IP address, enter the **Standby IP Address**, and click **OK**.
- d. Click **OK**.

- 6. Click **Save** at the top-right corner to save the changes.
- 7. Choose **Routing > Static Route** and add the static route defined for the new data management interface. The new data interface appears in the **Interface** list.

Add Static Route Configuration ?

Type: IPv4 IPv6

Interface*

Null0 (Nullifies it is available for route leak)

outside-new (Firewall Management Center Access) Selected Network

diagnostic

outside-new (Firewall Management Center Access)

outside-new

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Gateway* +

8. Click **Save** at the top-right corner to save the changes.
9. Deploy configuration changes..
10. When the deployment completes around 90 percent, the new management interface takes effect. At this stage, you must re-cable the FTD so that the CDO reaches FTD on the new interface and completes the deployment successfully.



Note After you re-cable, the deployment may fail if it timed out before re-establishing the management connection to the new interface. In that case, you must reinitiate the deployment after re-cabling for a successful deployment.

11. Ensure the management connection is reestablished.

In Management Center, check the management connection status on the **Devices > Device Management > Device > Management > FMC Access Details > Connection Status** page.

Alternatively, at the FTD CLI, enter the **sftunnel-status-brief** command to view the management connection status.

Internet Service Provider has Changed

If you have changed your ISP, you can lose management connectivity, even though High Availability health is normal. Configure the new network details of the management interface using the CLI commands.



Note These commands are available only on the active unit and not on standby.

For information about the threat defense CLI, see the [FTD command reference](#).

1. Connect to the device CLI.

You should use the console port when using these commands. If you are editing the configuration due to a disrupted management connection, and you have SSH access to the dedicated Management interface, then you can use that SSH connection.

See [Log Into the Command Line Interface on the Device](#).

2. Log in with the Admin username and password.
3. Use one of the following commands depending on the network value you want to update:

- **configure network management-data-interface ipv4 manual *ip_address ip_netmask* interface *interface_id***
- **configure network management-data-interface ipv4 *gateway_ip* interface *interface_id***
- **configure network management-data-interface ipv4 manual *ip_address ipv4_netmask* gateway_ip interface *interface_id***

Example:

```
Configure network management-data-interface ipv4 manual 10.10.6.7 255.255.255.0 interface
gig0/0
Configuration updated successfully..!!
```



Note All other CLI commands of **configure network management-data-interface** are not supported on devices in a High Availability pair.

The configuration is automatically pushed to the standby device.

- 4. Optional:**Limit data interface access to CDO on a specific network.

```
configure network management-data-interface client ip_address netmask
```

By default, all networks are allowed.

- 5.** Check that the management connection was reestablished.

sftunnel-status-brief

See the following sample output for a connection that is up, with peer channel and heartbeat information shown:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

- 6.** In CDO, click **Inventory > FTD**.
- 7.** Select your threat defense and in the **Management** pane on the right, click **Device Summary**.
- 8.** In **Management > FMC Access Details**, click **Refresh**.

The CDO detects the interface and default route configuration changes, and blocks deployment to the FTD. When you change the data interface settings locally on the device, you must reconcile those changes in CDO manually. You can view the discrepancies between CDO and the threat defense on the **Configuration** tab.

- 9.** Return to the **FMC Access Details** dialog box, and click **Acknowledge** to remove the deployment block.

The next time you deploy, the CDO configuration will overwrite any remaining conflicting settings on the FTD. It is your responsibility to manually fix the configuration in the CDO before you re-deploy.


You will see expected messages of "Config was cleared" and "FMC Access changed and acknowledged."


The configuration change made on the active unit is automatically pushed to standby. Once the CDO restores its connectivity with the active unit, CDO updates the standby IP address.

View Inventory Details

The **Inventory Details** section of the **Device** page shows chassis details such as the CPU and memory.

Figure 39: Inventory Details



Inventory Details 	
CPU Type:	CPU Xeon E5 series 2300 MHz
CPU Cores:	1 CPU (4 cores)
Memory:	8192 MB RAM
Storage:	N/A
Chassis URL:	N/A
Chassis Serial Number:	N/A
Chassis Module Number:	N/A
Chassis Module Serial Number:	N/A

To update information, click **Refresh** .

Edit Applied Policies

The **Applied Policies** section of the **Device** page displays the following policies applied to your firewall:

Figure 40: Applied Policies

Applied Policies 	
Access Control Policy:	Initial AC Policy 
Prefilter Policy:	Default Prefilter Policy
SSL Policy:	
DNS Policy:	Default DNS Policy
Identity Policy:	
NAT Policy:	
Platform Settings Policy:	
QoS Policy:	
FlexConfig Policy:	

For policies with links, you can click the link to view the policy.


For the Access Control Policy, view the **Access Policy Information for Troubleshooting** dialog box by clicking the **Exclamation**  icon. This dialog box shows how access rules are expanded into access control entries (ACEs).

Figure 41: Access Policy Information for Troubleshooting

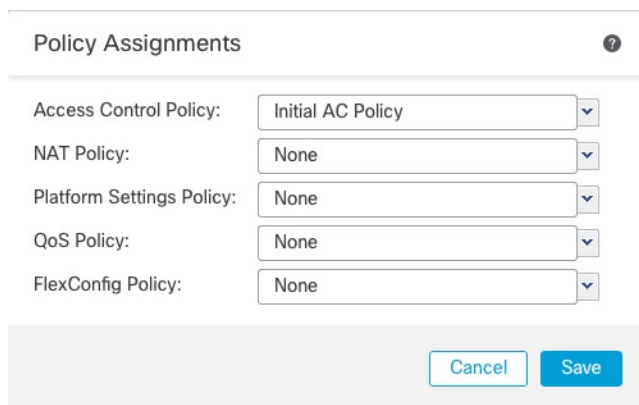


You can assign policies to an individual device from the **Device Management** page.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device where you want to assign policies, click **Edit** (✎).
- Step 3** Click **Device**.
- Step 4** In the **Applied Policies** section, click **Edit** (✎).

Figure 42: Policy Assignments



- Step 5** For each policy type, choose a policy from the drop-down menu. Only existing policies are listed.

Step 6 Click **Save**.

What to do next

- Deploy configuration changes.

Edit Advanced Settings

The **Advanced Settings** section of the **Device** page displays a table of advanced configuration settings, as described below. You can edit any of these settings.

Table 5: Advanced Section Table Fields

Field	Description
Application Bypass	The state of Automatic Application Bypass on the device.
Bypass Threshold	The Automatic Application Bypass threshold, in milliseconds.
Object Group Search	<p>The state of object group search on the device. While operating, the FTD device expands access control rules into multiple access control list entries based on the contents of any network or interface objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network or interface objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your access rules are defined or how they appear in Firepower Management Center. It impacts only how the device interprets and processes them while matching connections to access control rules.</p> <p>Note By default, the Object Group Search is enabled when you add threat defense for the first time in the management center.</p>
Interface Object Optimization	<p>The state of interface object optimization on the device. During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source/destination interface pair. If you enable interface object optimization, the system will instead deploy a single rule per access control/prefilter rule, which can simplify the device configuration and improve deployment performance. If you select this option, also select the Object Group Search option to reduce memory usage on the device.</p>

The following topics explain how to edit the advanced device settings.



Note For information about the Transfer Packets setting, see [Edit General Settings, on page 5](#).

Configure Automatic Application Bypass

Automatic Application Bypass (AAB) allows packets to bypass detection if Snort is down or, for a Classic device, if a packet takes too long to process. AAB causes Snort to restart within ten minutes of the failure, and generates troubleshooting data that can be analyzed to investigate the cause of the Snort failure.



Caution AAB activation partially restarts the Snort process, which temporarily interrupts the inspection of a few packets. Whether traffic drops during this interruption or passes without further inspection depends on how the target device handles traffic. See [Snort Restart Traffic Behavior](#) for more information.

See the following behavior:

Threat Defense Behavior: If Snort is down, then AAB is triggered after the specified timer duration. If Snort is up, then AAB is never triggered, even if packet processing exceeds the configured timer.

Classic Device Behavior: AAB limits the time allowed to process packets through an interface. You balance packet processing delays with your network's tolerance for packet latency.

The feature functions with any deployment; however, it is most valuable in inline deployments.

Typically, you use Rule Latency Thresholding in the intrusion policy to fast-path packets after the latency threshold value is exceeded. Rule Latency Thresholding does not shut down the engine or generate troubleshooting data.

If detection is bypassed, the device generates a health monitoring alert.

By default the AAB is disabled; to enable AAB follow the steps described.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
 - Step 2** Next to the device where you want to edit advanced device settings, click **Edit** (✎).
 - Step 3** Click **Device**, then click **Edit** (✎) in the **Advanced Settings** section.
 - Step 4** Check **Automatic Application Bypass**.
 - Step 5** Enter a **Bypass Threshold** from 250 ms to 60,000 ms. The default setting is 3000 milliseconds (ms).
 - Step 6** Click **Save**.
-

What to do next

- Deploy configuration changes.

Configure Object Group Search

While operating, the threat defense device expands access control rules into multiple access control list entries based on the contents of any network or interface objects used in the access rule. You can reduce the memory required to search access control rules by enabling object group search. With object group search enabled, the system does not expand network or interface objects, but instead searches access rules for matches based on those group definitions. Object group search does not impact how your access rules are defined or how

they appear in management center. It impacts only how the device interprets and processes them while matching connections to access control rules.

Enabling object group search reduces memory requirements for access control policies that include network or interface objects. However, it is important to note that object group search might also decrease rule lookup performance and thus increase CPU utilization. You should balance the CPU impact against the reduced memory requirements for your specific access control policy. In most cases, enabling object group search provides a net operational improvement.

By default, the object group search is enabled for the threat defense devices that are added for the first time in the management center. In the case of upgraded devices, if the device is configured with disabled object group search, then you need to manually enable it. You can enable it on one device at a time; you cannot enable it globally. We recommend that you enable it on any device to which you deploy access rules that use network or interface objects.



Note If you enable object group search and then configure and operate the device for a while, be aware that subsequently disabling the feature might lead to undesirable results. When you disable object group search, your existing access control rules will be expanded in the device's running configuration. If the expansion requires more memory than is available on the device, your device can be left in an inconsistent state and you might see a performance impact. If your device is operating normally, you should not disable object group search once you have enabled it.

Before you begin

- Model Support—Threat Defense
- We recommend that you also enable transactional commit on each device. From the device CLI, enter the **asp rule-engine transactional-commit access-group** command.
- Changing this setting can be disruptive to system operation while the device recompiles the ACLs. We recommend that you change this setting during a maintenance window.
- You can use FlexConfig to configure the **object-group-search threshold** command to enable a threshold to help prevent performance degradation. When operating with a threshold, for each connection, both the source and destination IP addresses are matched against network objects. If the number of objects matched by the source address times the number matched by the destination address exceeds 10,000, the connection is dropped. Configure your rules to prevent an excessive number of matches.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the threat defense device where you want to configure the rule, click the **Edit** (✎).
- Step 3** Click the **Device** tab, then click the **Edit** (✎) in the **Advanced Settings** section.
- Step 4** Check **Object Group Search**.
- Step 5** To have object group search work on interface objects in addition to network objects, check **Interface Object Optimization**.

If you do not select **Interface Object Optimization**, the system deploys separate rules for each source/interface pair, rather than use the security zones and interface groups used in the rules. This means the interface groups are not available for object group search processing.

Step 6 Click **Save**.

Configure Interface Object Optimization

During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source/destination interface pair. If you enable interface object optimization, the system will instead deploy a single rule per access control/prefilter rule, which can simplify the device configuration and improve deployment performance. If you select this option, also select the **Object Group Search** option to reduce memory usage on the device.

Interface object optimization is disabled by default. You can enable it on one device at a time; you cannot enable it globally.



Note If you disable interface object optimization, your existing access control rules will be deployed without using interface objects, which might make deployment take longer. In addition, if object group search is enabled, its benefits will not apply to interface objects, and you might see expansion in the access control rules in the device's running configuration. If the expansion requires more memory than is available on the device, your device can be left in an inconsistent state and you might see a performance impact.

Before you begin

Model Support—Threat Defense

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the threat defense device where you want to configure the rule, click the **Edit** (✎).
- Step 3** Click the **Device** tab, then click **Edit** (✎) in the **Advanced Settings** section.
- Step 4** Check **Interface Object Optimization**.
- Step 5** Click **Save**.

Edit Deployment Settings

The **Deployment Settings** section of the **Device** page displays the information described in the table below.

Figure 43: Deployment Settings


Deployment Settings 	
Auto Rollback Deployment if Connectivity fails	Disabled
Connectivity Monitor Interval (in Minutes) 	20 Mins.

Table 6: Deployment Settings


Field	Description
Auto Rollback Deployment if Connectivity Fails	Enabled or Disabled. You can enable auto rollback if the management connection fails as a result of the deployment; specifically if you use data for management center access, and then you misconfigure the data interface.
Connectivity Monitor Interval (in Minutes)	Shows the amount of time to wait before rolling back the configuration.

You can set deployment settings from the **Device Management** page. Deployment settings include enabling auto rollback of the deployment if the management connection fails as a result of the deployment; specifically if you use data for management center access, and then you misconfigure the data interface. You can alternatively manually roll back the configuration using the **configure policy rollback** command (see [Manually Roll Back the Configuration if the Management Center Loses Connectivity, on page 49](#)).

See the following guidelines:

- Only the previous deployment is available locally on the threat defense; you cannot roll back to any earlier deployments.
- Rollback is supported for high availability but not supported for clustering deployments.
- Rollback is not supported immediately after high availability creation.
- The rollback only affects configurations that you can set in the management center. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the threat defense CLI. Note that if you changed data interface settings after the last management center deployment using the **configure network management-data-interface** command, and then you use the rollback command, those settings will not be preserved; they will roll back to the last-deployed management center settings.
- UCAPL/CC mode cannot be rolled back.
- Out-of-band SCEP certificate data that was updated during the previous deployment cannot be rolled back.
- During the rollback, connections will drop because the current configuration will be cleared.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device where you want to assign policies, click **Edit** .

Step 3 Click **Device**.

Step 4 In the **Deployment Settings** section, click **Edit** (✎).

Figure 44: Deployment Settings

Deployment Settings

Auto Rollback Deployment if Connectivity Fails:

Connectivity Monitor Interval (in Minutes):

The connectivity failure timeout will be applicable from next deployment incase, the deployment for this device is already in progress.

Cancel Save

Step 5 Check **Auto Rollback Deployment if Connectivity Fails** to enable auto rollback.

Step 6 Set the **Connectivity Monitor Interval (in Minutes)** to set the amount of time to wait before rolling back the configuration. The default is 20 minutes.

Step 7 If a rollback occurs, see the following for next steps.

- If the auto rollback was successful, you see a success message instructing you to do a full deployment.
- You can also go to the **Deploy > Advanced Deploy** screen and click the **Preview** (📄) icon to view the parts of the configuration that were rolled back (see [Deploy Configuration Changes](#)). Click **Show Rollback Changes** to view the changes, and **Hide Rollback Changes** to hide the changes.

Figure 45: Rollback Changes

Change Log: 10.10.35.97

⚠ This device requires a full deployment as auto rollback operation is performed in the device. see more [Hide Rollback Changes](#)

Preview Changes Rollback Changes

Legend: Added Edited Removed

Changed Policies	Deployed Version	Version on FMC	Modified By
Routing	Routing:		
Virtual Router (Global)	Virtual Router: Virtual Router (Global)		
Static Route IPv4	Static Route IPv4:		
Static Route IPv6	IPv4 Route:		
	Static Route Interface(Unchanged): outside	outside	admin
	Static Route Network(Unchanged): any-ipv4	any-ipv4	
	Gateway: literal:10.10.35.63	literal:10.10.35.64	
	Static Route IPv6:		
	IPv6 Route:		
	IPv6 Static Route Interface(Unchanged): inside	inside	admin
	IPv6 Static Route Network(Unchanged): any-ipv6	any-ipv6	
	IPv6 Static Route gateway: literal:20::20	literal:20::23	

Download as PDF OK

- In the Deployment History Preview, you can view the rollback changes. See [View Deployment History](#).

Step 8 Check that the management connection was reestablished.

In management center, check the management connection status on the **Devices > Device Management > Device > Management > FMC Access Details > Connection Status** page.

At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 51](#).

Edit Cluster Health Monitor Settings

The **Cluster Health Monitor Settings** section of the **Cluster** page displays the settings described in the table below.

Figure 46: Cluster Health Monitor Settings

Cluster Health Monitor Settings			
Timeouts			
Hold Time			3 s
Interface Debounce Time			9000 ms
Monitored Interfaces			
Service Application			Enabled
Unmonitored Interfaces			None
Auto-Rejoin Settings			
	Attempts	Interval Between Attempts	Interval Variation
Cluster Interface	-1	5	1
Data Interface	3	5	2
System	3	5	2

Table 7: Cluster Health Monitor Settings Section Table Fields

Field	Description
Timeouts	
Hold Time	Between .3 and 45 seconds; The default is 3 seconds. To determine node system health, the cluster nodes send heartbeat messages on the cluster control link to other nodes. If a node does not receive any heartbeat messages from a peer node within the hold time period, the peer node is considered unresponsive or dead.
Interface Debounce Time	Between 300 and 9000 ms. The default is 500 ms. The interface debounce time is the amount of time before the node considers an interface to be failed, and the node is removed from the cluster.
Monitored Interfaces	The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular node, but there are active ports under the same logical interface on other nodes, then the node is removed from the cluster. The amount of time before the node removes a member from the cluster depends on the type of interface and whether the node is an established node or is joining the cluster.
Service Application	Shows whether the Snort and disk-full processes are monitored.
Unmonitored Interfaces	Shows unmonitored interfaces.
Auto-Rejoin Settings	
Cluster Interface	Shows the auto-rejoin settings after a cluster control link failure.

Field	Description
<i>Attempts</i>	Between -1 and 65535. The default is -1 (unlimited). Sets the number of rejoin attempts.
<i>Interval Between Attempts</i>	Between 2 and 60. The default is 5 minutes. Defines the interval duration in minutes between rejoin attempts.
<i>Interval Variation</i>	Between 1 and 3. The default is 1x the interval duration. Defines if the interval duration increases at each attempt.
Data Interfaces	Shows the auto-rejoin settings after a data interface failure.
<i>Attempts</i>	Between -1 and 65535. The default is 3. Sets the number of rejoin attempts.
<i>Interval Between Attempts</i>	Between 2 and 60. The default is 5 minutes. Defines the interval duration in minutes between rejoin attempts.
<i>Interval Variation</i>	Between 1 and 3. The default is 2x the interval duration. Defines if the interval duration increases at each attempt.
System	Shows the auto-rejoin settings after internal errors. Internal failures include: application sync timeout; inconsistent application statuses; and so on.
<i>Attempts</i>	Between -1 and 65535. The default is 3. Sets the number of rejoin attempts.
<i>Interval Between Attempts</i>	Between 2 and 60. The default is 5 minutes. Defines the interval duration in minutes between rejoin attempts.
<i>Interval Variation</i>	Between 1 and 3. The default is 2x the interval duration. Defines if the interval duration increases at each attempt.



Note If you disable the system health check, fields that do not apply when the system health check is disabled will not show.

You can change these settings from this section.

You can monitor any port-channel ID, single physical interface ID, as well as the Snort and disk-full processes. Health monitoring is not performed on VLAN subinterfaces or virtual interfaces such as VNIs or BVIs. You cannot configure monitoring for the cluster control link; it is always monitored.

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the cluster you want to modify, click **Edit** (✎).
- Step 3** Click **Cluster**.
- Step 4** In the **Cluster Health Monitor Settings** section, click **Edit** (✎).
- Step 5** Disable the system health check by clicking the **Health Check** slider .

Figure 47: Disable the System Health Check

Edit Cluster Health Monitor Settings

Health Check ⓘ

▼ Timeouts

Hold Time Range: 0.3 to 45 seconds

Interface Debounce Time Range: 300 to 9000 milliseconds

> Auto-Rejoin Settings

> Monitored Interfaces

Reset to Defaults Cancel Save

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 6 Configure the hold time and interface debounce time.

- **Hold Time**—Set the hold time to determine the amount of time between node heartbeat status messages, between .3 and 45 seconds; The default is 3 seconds.
- **Interface Debounce Time**—Set the debounce time between 300 and 9000 ms. The default is 500 ms. Lower values allow for faster detection of interface failures. Note that configuring a lower debounce time increases the chances of false-positives. When an interface status update occurs, the node waits the number of milliseconds specified before marking the interface as failed, and the node is removed from the cluster. In the case of an EtherChannel that transitions from a down state to an up state (for example, the switch reloaded, or the switch enabled an EtherChannel), a longer debounce time can prevent the interface from appearing to be failed on a cluster node just because another cluster node was faster at bundling the ports.

Step 7 Customize the auto-rejoin cluster settings after a health check failure.

Figure 48: Configure Auto-Rejoin Settings

▼ Auto-Rejoin Settings

Cluster Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Data Interface

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

System

Attempts Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts Range: 2-60 minutes between rejoin attempts

Interval Variation Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Set the following values for the **Cluster Interface**, **Data Interface**, and **System** (internal failures include: application sync timeout; inconsistent application statuses; and so on):

- **Attempts**—Sets the number of rejoin attempts, between -1 and 65535. **0** disables auto-rejoining. The default for the **Cluster Interface** is -1 (unlimited). The default for the **Data Interface** and **System** is 3.
- **Interval Between Attempts**—Defines the interval duration in minutes between rejoin attempts, between 2 and 60. The default value is 5 minutes. The maximum total time that the node attempts to rejoin the cluster is limited to 14400 minutes (10 days) from the time of last failure.
- **Interval Variation**—Defines if the interval duration increases. Set the value between 1 and 3: **1** (no change); **2** (2 x the previous duration), or **3** (3 x the previous duration). For example, if you set the interval duration to 5 minutes, and set the variation to 2, then the first attempt is after 5 minutes; the 2nd attempt is 10 minutes (2 x 5); the 3rd attempt 20 minutes (2 x 10), and so on. The default value is **1** for the **Cluster Interface** and **2** for the **Data Interface** and **System**.

Step 8

Configure monitored interfaces by moving interfaces in the **Monitored Interfaces** or **Unmonitored Interfaces** window. You can also check or uncheck **Enable Service Application Monitoring** to enable or disable monitoring of the Snort and disk-full processes.

Figure 49: Configure Monitored Interfaces

▼ Monitored Interfaces

Monitored Interfaces

- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2
- GigabitEthernet0/3
- GigabitEthernet0/4
- GigabitEthernet0/5
- GigabitEthernet0/6
- GigabitEthernet0/7
- Diagnostic0/0

Unmonitored Interfaces 1

Add

Enable Service Application Monitoring

The interface health check monitors for link failures. If all physical ports for a given logical interface fail on a particular node, but there are active ports under the same logical interface on other nodes, then the node is removed from the cluster. The amount of time before the node removes a member from the cluster depends on the type of interface and whether the node is an established node or is joining the cluster. Health check is enabled by default for all interfaces and for the Snort and disk-full processes.

You might want to disable health monitoring of non-essential interfaces.

When any topology changes occur (such as adding or removing a data interface, enabling or disabling an interface on the node or the switch, or adding an additional switch to form a VSS or vPC) you should disable the system health check feature and also disable interface monitoring for the disabled interfaces. When the topology change is complete, and the configuration change is synced to all nodes, you can re-enable the system health check feature and monitored interfaces.

Step 9 Click **Save**.

Step 10 Deploy configuration changes.

Hot Swap an SSD on the Secure Firewall 3100/4200

If you have two SSDs, they form a RAID when you boot up. You can perform the following tasks at the threat defense CLI while the firewall is powered up:

- Hot swap one of the SSDs—If an SSD is faulty, you can replace it. Note that if you only have one SSD, you cannot remove it while the firewall is powered on.
- Remove one of the SSDs—If you have two SSDs, you can remove one.
- Add a second SSD—If you have one SSD, you can add a second SSD and form a RAID.



Caution Do not remove an SSD without first removing it from the RAID using this procedure. You can cause data loss.

Procedure

Step 1 Remove one of the SSDs.

a) Remove the SSD from the RAID.

configure raid remove-secure local-disk {1 | 2}

The **remove-secure** keyword removes the SSD from the RAID, disables the self-encrypting disk feature, and performs a secure erase of the SSD. If you only want to remove the SSD from the RAID and want to keep the data intact, you can use the **remove** keyword.

Example:

```
> configure raid remove-secure local-disk 2
```

b) Monitor the RAID status until the SSD no longer shows in the inventory.

show raid

After the SSD is removed from the RAID, the **Operability** and **Drive State** will show as **degraded**. The second drive will no longer be listed as a member disk.

Example:

```
> show raid
Virtual Drive
ID: 1
Size (MB): 858306
Operability: operable
Presence: equipped
Lifecycle: available
Drive State: optimal
Type: raid
Level: raid1
Max Disks: 2
Meta Version: 1.0
Array State: active
Sync Action: idle
Sync Completed: unknown
Degraded: 0
Sync Speed: none

RAID member Disk:
Device Name: nvme0n1
Disk State: in-sync
Disk Slot: 1
Read Errors: 0
Recovery Start: none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name: nvme1n1
Disk State: in-sync
```

```

Disk Slot:                2
Read Errors:              0
Recovery Start:          none
Bad Blocks:
Unacknowledged Bad Blocks:

> show raid
Virtual Drive
ID:                      1
Size (MB):               858306
Operability:             degraded
Presence:                equipped
Lifecycle:               available
Drive State:             degraded
Type:                    raid
Level:                   raid1
Max Disks:               2
Meta Version:            1.0
Array State:             active
Sync Action:             idle
Sync Completed:          unknown
Degraded:                1
Sync Speed:              none

RAID member Disk:
Device Name:             nvme0n1
Disk State:              in-sync
Disk Slot:               1
Read Errors:             0
Recovery Start:          none
Bad Blocks:
Unacknowledged Bad Blocks:

```

- c) Physically remove the SSD from the chassis.

Step 2

Add an SSD.

- a) Physically add the SSD to the empty slot.
- b) Add the SSD to the RAID.

```
configure raid add local-disk {1 | 2}
```

It can take several hours to complete syncing the new SSD to the RAID, during which the firewall is completely operational. You can even reboot, and the sync will continue after it powers up. Use the **show raid** command to show the status.

If you install an SSD that was previously used on another system, and is still locked, enter the following command:

```
configure raid add local-disk {1 | 2} psid
```

The *psid* is printed on the label attached to the back of the SSD. Alternatively, you can reboot the system, and the SSD will be reformatted and added to the RAID.

Disable the USB Port

By default, the type-A USB port is enabled. You might want to disable USB port access for security purposes. Disabling USB is supported on the following models:

- Firepower 1000 Series
- Secure Firewall 3100
- Secure Firewall 4200

Guidelines

- Enabling or disabling the USB port requires a reboot.
- If the USB port is disabled and you downgrade to a version that does not support this feature, the port will remain disabled, and you cannot re-enable it without erasing the NVRAM (the FXOS local-mgmt **erase secure all** command).
- If you perform a ROMMON **factory-reset** or FXOS local-mgmt **erase secure**, the USB port will be re-enabled.
- For high availability or clustering, you must disable or re-enable the port individually on each unit.



Note This feature does not affect the USB console port, if present.

Disable the USB Port on a Device

To disable the USB port on a device, you can do so at the threat defense CLI.

Procedure

Step 1 Disable the USB port.

```
system support usb configure disable
```

```
reboot
```

To re-enable the USB port, enter **system support usb configure enable**.

Example:

```
>system support usb configure disable
USB Port Admin State set to 'disabled'.
Please reboot the system to apply any control state changes.
```

```
>reboot
This command will reboot the system. Continue?
Please enter 'YES' or 'NO': YES
```

Step 2 View the port status.

system support usb show

The Admin State shows the USB port configuration. The Oper State shows the current operation. For example, if you disable the USB port but do not reload, the Admin State will show disabled while the Oper State would be enabled.

Example:

```
>system support usb show
USB Port Info
-----
Admin State: disabled
Oper State: disabled
```

Disable the USB Port in Multi-Instance Mode

To disable the USB port in multi-instance mode, you can do so at the FXOS CLI.

Procedure**Step 1**

Disable the USB port and reboot for the change to take effect.

- a) Disable the USB port.

```
scope fabric-interconnect
```

```
disable usb-port
```

```
commit buffer
```

- b) Reboot the chassis.

```
connect local-mgmt
```

```
reboot
```

Example:

```
firepower-4245 /fabric-interconnect # disable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

Step 2

Enable the USB port and reboot for the change to take effect.

- a) Enable the USB port.

```
scope fabric-interconnect
```

```
enable usb-port
```

```
commit buffer
```

b) Reboot the chassis.

```
connect local-mgmt
```

```
reboot
```

Example:

```
firepower-4245 /fabric-interconnect # enable usb-port
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:
device /fabric-interconnect* # commit buffer
Note: USB enablement or disablement changes are effected only after FXOS reboot.
Confirm change? (yes/no) [yes]:yes
firepower-4245 /fabric-interconnect # connect local-mgmt
firepower-4245(local-mgmt)# reboot
Before rebooting, please take a configuration backup.
Do you still want to reboot? (yes/no):yes
Broadcast message from admin@firepower-4245 (Wed Feb 21 05:59:55 2024):
All shells being terminated due to system /sbin/reboot
```

Step 3 View the USB port status.

```
scope fabric-interconnect
```

```
show usb-port
```

The Admin State shows the USB port configuration. The Oper State shows the current operation. For example, if you disable the USB port but do not reload, the Admin State will show Disabled while the Oper State would will Enabled.

Example:

```
firepower-4245# scope fabric-interconnect
firepower-4245 /fabric-interconnect # show usb-port
Usb Port:
Equipment      Admin State Oper State
-----
A               Disabled   Disabled
```

Migrate the Configuration to a New Model

The Firewall Threat Defense model migration wizard enables you to migrate configurations from an old threat defense model to a new model. You can map source device interfaces to target device interfaces. Before the migration, the source and target devices are locked.

Supported Devices for Migration

Supported Source Devices

- Cisco Firepower 1120
- Cisco Firepower 1140
- Cisco Firepower 1150
- Cisco Firepower 2110
- Cisco Firepower 2120
- Cisco Firepower 2130
- Cisco Firepower 2140



Note The source devices must be version 7.0 or later.

Supported Target Devices

- Cisco Secure Firewall 3105
- Cisco Secure Firewall 3110
- Cisco Secure Firewall 3120
- Cisco Secure Firewall 3130
- Cisco Secure Firewall 3140



Note The Cisco Secure Firewall 3110, 3120, 3130, and 3140 devices must be version 7.1 or later. Cisco Secure Firewall 3105 must be version 7.3 or later.

License for Migration

You must register and enroll the device with the smart licensing account. The migration copies the source device licenses to the target device.

Prerequisites for Migration

- You must register the source and the target devices to the management center.
- Your Smart Licensing account must have the license entitlements for the target device.
- We recommend that the target device is a freshly registered device without any configurations.
- Source and target devices must be in the same:

- Domain
- Firewall mode: Routed or Transparent
- Compliance mode
- The target device must not be:
 - In a multi-instance mode
 - Part of a cluster
- The user must have modify permissions on the device.
- The configurations on the source device must be valid and have no errors.
- The source device can have pending deployments. However, deployment, import, or export tasks must not run on either of the devices during the migration.
- If the source device is part of an HA pair, the target device need not be part of an HA pair and vice versa. The migration does not form or break the HA pair.

What Configurations Does the Wizard Migrate?

The migration wizard copies the following configurations from the source device to the target device:

- Licenses
- Interface configurations
- Inline sets configurations
- Routing configurations
- DHCP and DDNS configurations
- Virtual router configurations
- Policies
- Associated objects and object overrides
- Platform settings
- Remote branch deployment configurations

The migration wizard copies the following policy configurations from the source device to the target device:

- Health policies
- NAT policies
- QoS policies
- Remote access VPN policies
- FlexConfig policies
- Access control policies

- Prefilter policies
- IPS policies
- DNS policies
- SSL policies
- Malware and File policies
- Identity policies

The migration wizard copies the following routing configurations from the source device to the target device:

- ECMP
- BFD
- OSPFv2/v3
- EIGRP
- RIP
- BGP
- Policy Based Routing
- Static Route
- Multicast Routing
- Virtual Router

The migration wizard copies the following interfaces from the source device to the target device:

- Physical interfaces
- Sub-interfaces
- Etherchannel interfaces
- Bridge group interfaces
- VTI interfaces
- VNI interfaces
- Loopback interfaces

Limitations for Migration

- The wizard does not migrate:
 - Site-to-site VPN policies
 - SNMP configurations

After the migration, you can configure SNMP using the platform settings for the device.

- You can perform only one migration at a time.
- If the speed, auto-negotiation, and duplex settings of the source interface are valid for the mapped interface of the target device, the values are copied. If not, these parameters are set to the default values.
- Remote access VPN trustpoint certificates are not enrolled. You must manually enroll these certificates before the deployment.
- After migration, by default, the target device uses Snort 3 and not Snort 2, even if the source device uses Snort 2.
- For HA devices:
 - Target Device: You cannot map the interfaces that are part of the failover configuration. These interfaces are disabled in the wizard.
 - Source and Target Devices: The wizard does not migrate HA configurations such as monitored interfaces, failover trigger criteria, and interface MAC addresses. You must manually configure these parameters after the migration if required.

Migrate the Secure Firewall Threat Defense

Before you begin

Review the prerequisites and limitations for the migration.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Click **Migrate** on the top-right of the page.
- Step 3** Click **Start** on the welcome screen.
- Step 4** From the **Source Device** drop-down list, choose a device.
If the device is part of an HA pair, only the container name of the HA pair appears.
- Step 5** Click **Next**.
- Step 6** From the **Target Device** drop-down list, choose a device.
If the device is part of an HA pair, only the container name of the HA pair appears.
- Step 7** Click **Next**.
- Step 8** In the **Configure Interfaces** step, map the physical interfaces of the source device with those of the target device.
Mapping of all interfaces is not mandatory. You must map all named interfaces and interfaces that are part of other interfaces. You cannot map interfaces that are part of an HA failover configuration. These interfaces are disabled in the wizard. The wizard creates the logical interfaces according to the interface mapping provided by the user.
- Click **Map Default** to configure default interface mappings.
For example, Ethernet1/1 in the source device will be mapped to Ethernet1/1 in the target device.

- Click **Clear All** to clear all the mappings.

- Step 9** Click **Next**.
- Step 10** Click **View Mappings** to verify the interface mappings.
- Step 11** Click **Submit** to start the migration.
- Step 12** View the migration status in the **Notifications > Tasks** page.
-

What to do next

After a successful migration, you can deploy the device.

Deployment is not mandatory, you can validate the configurations and deploy as required. However, before the deployment ensure that you perform the actions mentioned in [Best Practices for Migration, on page 84](#).

Best Practices for Migration

After a successful migration, we recommend that you perform the following actions before the deployment:

- Change the IP addresses of the interfaces if the source device is live, as they are copied to the target device from the source device.
- Ensure that you update your NAT policies with the modified IP addresses.
- Configure the interface speeds if they are set to default values after migration.
- Re-enroll the device certificates, if any, on the target device.
- If you have a HA setup, configure HA parameters such as monitored interfaces, failover trigger criteria, and interface MAC addresses.
- Configure the diagnostic interface as it gets reset after migration.
- (Optional) Configure SNMP using the platform settings for the device.
- (Optional) Configure remote branch deployment configurations.

If the source or target device had manager access through a data interface, after the migration, the manager access will be lost. Update the manager access configuration on the target device. For more information, see the *Change the Manager Access Interface from Management to Data* topic in the Cisco Secure Firewall Management Center Device Configuration Guide or the Online Help.

- (Optional) Configure site-to-site VPN if required. These configurations are not migrated from the source device.
- View the deployment preview before the deployment. Choose **Deploy > Advanced Deploy** and click the **Preview** (📄) icon for the device.