



## Device Settings

---

After you add a device, you can edit device-related settings on the **Device** page.

1. Choose **Devices** > **Device Management**.
2. Next to the device you want to modify, click **Edit** (✎).
3. Click **Device**.

- [Edit General Settings, on page 1](#)
- [Edit License Settings, on page 8](#)
- [View System Information, on page 9](#)
- [View the Inspection Engine, on page 10](#)
- [Edit Health Settings, on page 10](#)
- [Edit Management Settings, on page 21](#)
- [View Inventory Details, on page 61](#)
- [Edit Applied Policies, on page 62](#)
- [Edit Advanced Settings, on page 63](#)
- [Edit Deployment Settings, on page 67](#)
- [Edit Cluster Health Monitor Settings, on page 70](#)
- [History for Device Settings, on page 75](#)

## Edit General Settings

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

Figure 1: General

General	
Name:	Thing1
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
Performance Profile:	Default
TLS Crypto Acceleration:	Disabled
Device Configuration: <span>Import</span> <span>Export</span> <span>Download</span>	

Table 1: General Section Table Fields

Field	Description
Name	The display name of the device on the Firewall Management Center.
Transfer Packets	This displays whether or not the managed device sends packet data with the events to the Firewall Management Center.
Mode	The displays the mode of the management interface for the device: <b>routed</b> or <b>transparent</b> .
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 <a href="#">Copy a Configuration to Another Device, on page 3</a> and <a href="#">Export and Import the Device Configuration, on page 4</a> .
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 Firewall 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 Firewall Threat Defense.
- Step 5** For **Device Configuration** actions, see [Copy a Configuration to Another Device, on page 3](#) and [Export and Import the Device Configuration, on page 4](#).
- Step 6** Click **Deploy**.
- 

#### What to do next

- Deploy configuration changes.

## 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 devices are the same model and are running the same version of the software.
- The source is either a standalone device or a high availability pair.
- The destination device is a standalone device.
- The source and destination devices have the same number of physical interfaces.
- The source and destination devices are in the same firewall mode: routed or transparent.
- The source and destination devices are in the same security-certifications-compliance mode.
- The source and destination devices are in the same domain.
- Configuration deployment is not in progress on either the source or the destination 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 Firewall Management Center—First unregister the device from the original Firewall Management Center, then add the device to the new Firewall 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 Firewall 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 you export a standalone configuration, you cannot import it to a high availability pair or vice versa.
- 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 <a href="#">Object Overrides</a>.</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**.

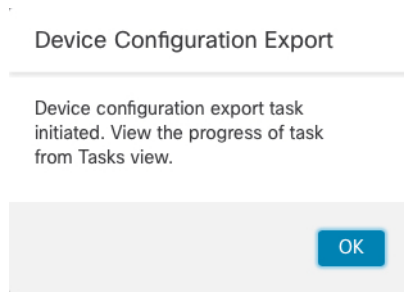
Figure 2: Export Device Configuration



General	
Name:	192.168.0.197 FTDv
Transfer Packets:	Yes
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled
Device Configuration:	<input type="button" value="Import"/> <input type="button" value="Export"/> <input type="button" value="Download"/>

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

Figure 3: Acknowledge Export



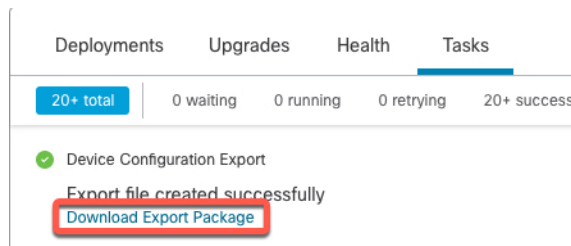
### Device Configuration Export

Device configuration export task initiated. View the progress of task from Tasks view.

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

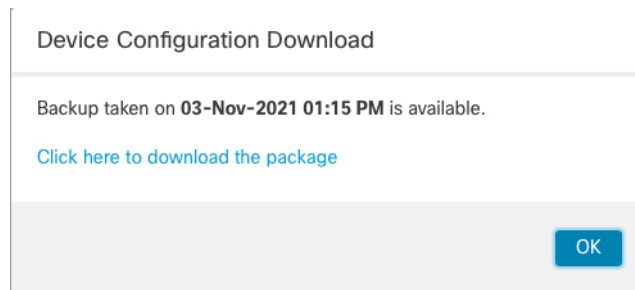
- b) On the **Notifications > Tasks** page, ensure that the export has completed; click **Download Export Package**. Alternatively, you can click the **Download** button in the **General** area.

Figure 4: Export Task



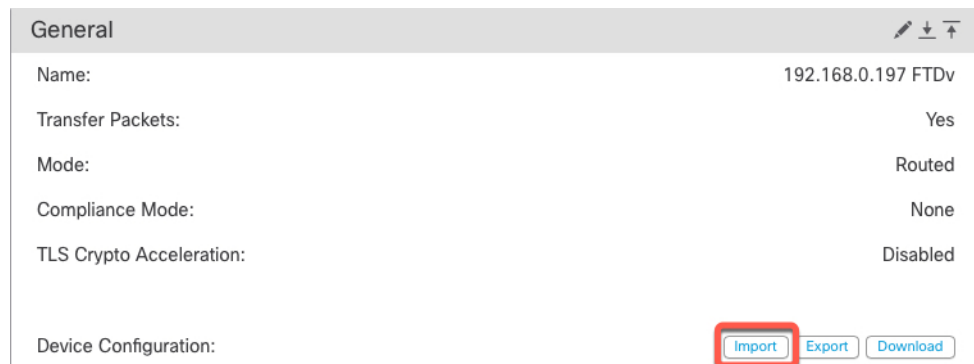
Deployments	Upgrades	Health	Tasks
20+ total	0 waiting	0 running	0 retrying 20+ success
<div> <span>✓</span> Device Configuration Export           <div>Export file created successfully</div> <div>Download Export Package</div> </div>			

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.

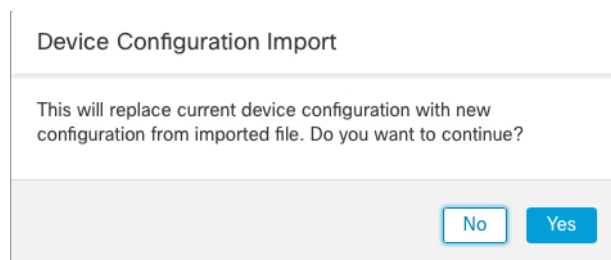
**Figure 5: Download Package**

**Step 5** Import the configuration.

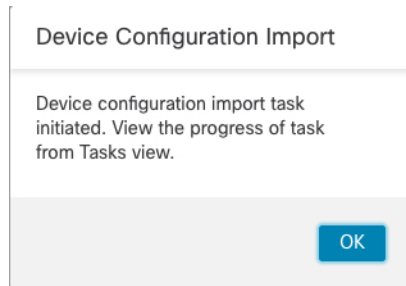
- a) In the **General** area, click **Import**.

**Figure 6: 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).

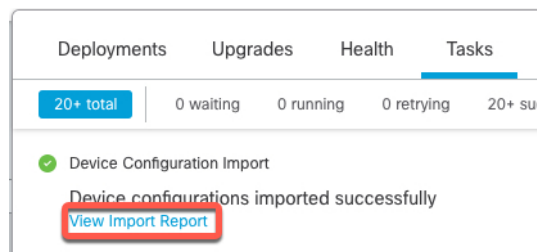
**Figure 7: Import Package****Figure 8: Navigate to Package**

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

**Figure 9: 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 10: 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-bb94-93bde3ad19d	Report does not exist	<a href="#">Device configurations import report</a>

## 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 Firewall 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 containing system information, as described in the following table.

You can also shut down or restart the device from this pane, using the icons at the top-right corner.

**Figure 11: System**

System		⏻ ⌂
Model:	Cisco Firepower 1010 Threat Defense	
Serial:	JAD253802SG	
Time:	2024-12-03 18:08:13	
Time Zone:	UTC (UTC+0:00)	
Version:	7.7.0	
Time Zone setting for Time based Rules:	UTC (UTC+0:00)	
Inventory:	<a href="#">View</a>	

**Table 3: System Section Table Fields**

Field	Description
Shut Down Device (⏻)	Shuts down the device. See <a href="#">Shut Down or Restart the Device</a> .
Restart Device (⌂)	Restarts the device. See <a href="#">Shut Down or Restart the Device</a> .
Model	Model name and number of the managed device.
Serial	Serial number of the managed device's chassis.
Time	Current system time of the device.
Time Zone	Time zone.
Version	Version of the software currently installed on the managed device.

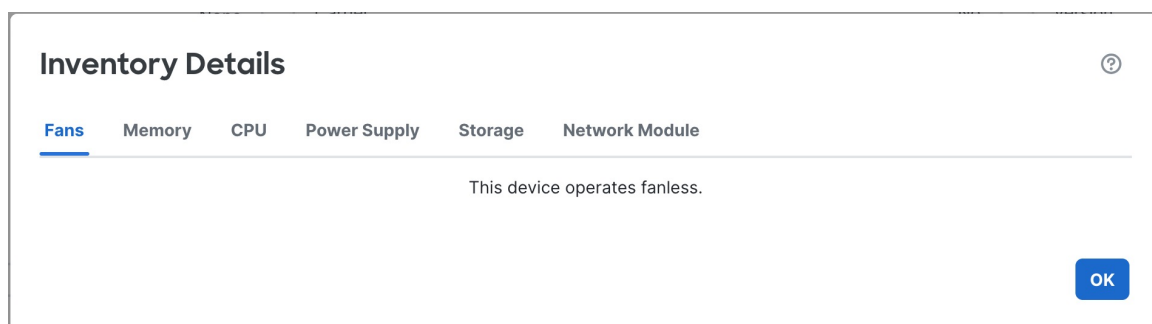
Field	Description
<b>Time Zone setting for Time based rules</b>	Current system time of the device in the time zone specified in device platform settings.
<b>Inventory</b>	Inventory details. See <a href="#">View Device Inventory</a> .

## View Device Inventory

Click **View** next to **Inventory** in the **System** section to view a table of device inventory information including Fans, Memory, CPU, Power Supply, Storage, and Network Modules.

The **Inventory Details** table displays information about all the Cisco products installed in the Firewall Threat Defense devices assigned with a product identifier (PID). The PID is the product name using which the product can be ordered.

**Figure 12: Inventory Details**



## View the Inspection Engine

The Inspection Engine section of the **Device** page shows whether your device uses Snort 2 or Snort 3. To switch the inspection engine, see *Enable Snort 3 on an Individual Device* in the [Cisco Secure Firewall Management Center Snort 3 Configuration Guide](#).

## Edit Health Settings

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

Figure 13: Health

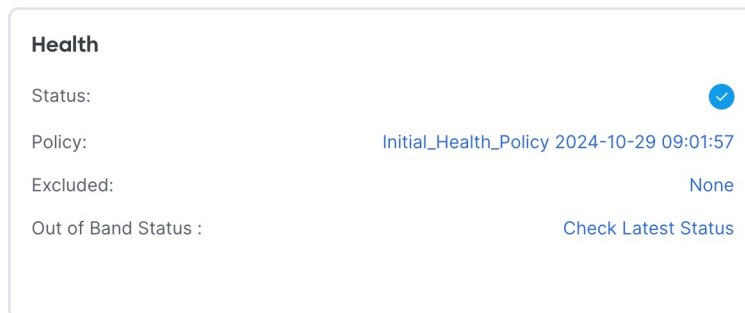


Table 4: Health Section Table Fields

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 <b>Health Exclude</b> page, where you can enable and disable health exclusion modules.
Out of Band Status	A link to the <b>Out-of-Band configuration details</b> dialog box where you can view out-of-band configuration changes made at the device CLI. You must acknowledge the configuration differences and manually match any changes you want to keep in the Firewall Management Center before the next deployment. See <a href="#">Out-of-Band Configuration Detection, on page 11</a> .

## Out-of-Band Configuration Detection

If you lose the management connection to your device, you can make select configuration changes directly at the device CLI to:

- Restore the management connection if you are using a data interface for manager access
- Make select configuration changes that can't wait until the connection is restored



### Caution

You are expected to know the commands that are required for recovery or emergency use. Do not use this feature to experiment with configuration changes. If you do not know which commands are required or are unsure about the effect of a command, we recommend that you contact Cisco TAC for guidance.

After the management connection is restored, the Firewall Management Center will detect the configuration changes on the device. It does not automatically update the device configuration in the Firewall Management Center; you must view the configuration differences, acknowledge that the device configuration is different, and then manually make the same changes in the Firewall Management Center before you deploy.

**Caution**

When you deploy after acknowledgment, any configurations not present in the Firewall Management Center configuration will be overwritten on the device.

## Guidelines for Out-of-Band Configuration

### Supported Feature Areas in Recovery-Config Mode

You can configure the following feature areas at the diagnostic CLI in recovery-config mode:

- Interfaces
- Static Routes
- Dynamic Routing: BGP and OSPF
- Prefilters
- Site-to-site VPN

Like other diagnostic CLI commands, refer to the [ASA command reference](#) for more information about each command.

### Unsupported Features

- Not supported in multi-instance mode.
- You cannot add or delete EtherChannels.
- Some platform-dependent interface commands such as speed, duplex, and shutdown are not supported.

### High Availability and Clustering

- Recovery-config mode is only available on the active/control node.
- If a failover or cluster switchover occurs before you exit the recovery-config-mode session, the Firewall Management Center will not detect the change on the new active/control node. We recommend re-entering recovery-config mode on the new active/control node and making a small change to trigger discovery of all of your previous changes. Otherwise, if you do not manually match the changes in the Firewall Management Center, they will be overwritten at deployment without any notification.
- If you make out-of-band-configuration changes on the active/control node, but then, prior to a configuration sync, the high availability/cluster ends up in "split brain" mode (where multiple nodes become active/control because of a failover/cluster-control-link failure), then when the high availability/cluster returns to a healthy state, and a different node becomes active/control, then the configuration changes will be lost.
- If you have an active recovery-config-mode session, then new nodes cannot join or rejoin the high availability/cluster until the session is exited.

### Additional Guidelines

- To modify an existing rule or route, you should delete the existing command using the **no** form of the command and then re-add the modified rule. This method avoids conflicts and errors. For example:

#### Incorrect:

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
firepower# configure recovery-config
```

CAUTION: The config CLI is for emergency use only. Use the config CLI if the management center is unreachable, and use it only under exceptional circumstances, such as loss of connectivity or to restore manager access. Do not change management center's auto-generated configurations.

After your management center is reachable, manually make the same configuration changes in the management center. The management center cannot implement them automatically. When you deploy from the management center, out-of-band configuration changes will be overwritten. Also, node join will be blocked till config CLI session is active, so make sure to exit from the config CLI after changes are made.

```
Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)# route outside 10.0.0.0 255.0.0.0 30.1.1.1
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o: y
Cryptochecksum: ccfc11a8 4e46d55e 0c99b5ae 3b18a8f1
```

```
3939 bytes copied in 0.70 secs
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
route outside 10.0.0.0 255.0.0.0 30.1.1.1 1
firepower#
```

In this case, a second route is added instead of replacing the first route.

#### Correct:

```
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 20.1.1.1 1
firepower# configure recovery-config
```

CAUTION: The config CLI is for emergency use only. Use the config CLI if the management center is unreachable, and use it only under exceptional circumstances, such as loss of connectivity or to restore manager access. Do not change management center's auto-generated configurations.

After your management center is reachable, manually make the same configuration changes in the management center. The management center cannot implement them automatically. When you deploy from the management center, out-of-band configuration changes will be overwritten. Also, node join will be blocked till config CLI session is active, so make sure to exit from the config

```

CLI after
changes are made.

Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)# no route outside 10.0.0.0 255.0.0.0 20.1.1.1
firepower(recovery-config)# route outside 10.0.0.0 255.0.0.0 30.1.1.1
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot.Save changes to memory ? [Y]es/[N]o: y
Cryptochecksum: 81bcc51d 43771bbd 15b6dde6 afeb3442

3945 bytes copied in 0.70 secs
firepower# show running-config route
route outside 10.0.0.0 255.0.0.0 30.1.1.1 1
firepower#

```

- If you have auto rollback enabled (see [Edit Deployment Settings, on page 67](#)), and you lose management connectivity because of a deployment, you should not start an out-of-band configuration. Instead, either wait 20 minutes for auto rollback to the previous deployment to occur or manually roll back at the CLI using the **configure policy rollback** command (see [Manually Roll Back the Configuration if the Firewall Management Center Loses Connectivity, on page 50](#)). Auto rollback will overwrite out-of-band configuration changes if the management connection is still down.
- For prefilter rules, we don't recommend adding completely new rules (the **access-control advanced** command); integration of prefilter rules with the intrusion policy and logging requires the Firewall Management Center, which generates the rule ID and integrates it with other policies.
- All recovery-config-mode sessions will be logged in syslog with the username "enable\_15".

## Access Recovery-Config Mode in the Diagnostic CLI

You can use the diagnostic CLI recovery-config mode to make out-of-band configuration changes when the management connection is down. Be sure to make the same changes in the Firewall Management Center; local changes will always be overwritten by the Firewall Management Center deployment.

For high availability and clustering, make your changes on the active/control node. This mode is not supported in multi-instance mode.

### Procedure

- 
- Step 1** Connect to the device CLI using either the console port or SSH.  
See [Log Into the Command-Line Interface on the Device](#).
- Step 2** Access the diagnostic CLI.  
**system support diagnostic-cli**  
**enable** (Press enter without entering a password when prompted.)

#### Example:

```

> system support diagnostic-cli
firepower> enable
Password:

```

**Step 3** Show the current running configuration for reference.

**show runing-config**

**Note**

You cannot enter **show** commands in recovery-config mode.

**Step 4** Enter recovery-config mode.

**configure recovery-config**

**Example:**

```
firepower# configure recovery-config
```

CAUTION: The config CLI is for emergency use only. Use the config CLI if the management center is unreachable, and use it only under exceptional circumstances, such as loss of connectivity or to restore manager access. Do not change management center's auto-generated configurations.

After your management center is reachable, manually make the same configuration changes in the management center. The management center cannot implement them automatically. When you deploy from the management center, out-of-band configuration changes will be overwritten. Also, node join will be blocked till config CLI session is active, so make sure to exit from the config CLI after changes are made.

```
Would you like to proceed ? [Y]es/[N]o: y
firepower(recovery-config)#
```

**Step 5** You can now enter select configuration commands.

Enter **?** to view available commands.

See [Guidelines for Out-of-Band Configuration, on page 12](#) for supported feature areas.

See the ASA [configuration guides](#) or [command reference](#) for details about the commands.

**Tip**

Keep track of all of the commands you changed. Although the Firewall Management Center will show you the differential later, it's good practice to keep a record of your command changes in case you need to make iterative changes to restore the management connection.

**Example:**

```
firepower(recovery-config)# ?
```

access-list	Configure an access control element
as-path	BGP autonomous system path filter
bfd	BFD configuration commands
bfd-template	BFD template configuration
cluster	Cluster configuration
community-list	Add a community list entry
crypto	Configure IPSec, ISAKMP, Certification authority, key
end	Exit from configure mode
exit	Exit from config mode
extcommunity-list	Add a extended community list entry

```

group-policy          Configure or remove a group policy
interface             Select an interface to configure
ip                    Configure IP address pools
ipsec                 Configure transform-set, IPSec SA lifetime and PMTU
                     Aging reset timer
ipv6                  Configure IPv6 address pools
ipv6                  Global IPv6 configuration commands
isakmp                Configure ISAKMP options
jumbo-frame           Configure jumbo-frame support
management-interface Management interface
mtu                   Specify MTU(Maximum Transmission Unit) for an interface
no                    Negate a command or set its defaults
policy-list           Define IP Policy list
prefix-list           Build a prefix list
route                 Configure a static route for an interface
route-map             Create route-map or enter route-map configuration mode
router               Enable a routing process
sla                   IP Service Level Agreement
sysopt               Set system functional options
tunnel-group          Create and manage the database of connection specific
                     records for IPSec connections
vpdn                  Configure VPDN feature
vrf                   Configure a VRF
zone                  Create or show a Zone
firepower(recovery-config)#

```

**Step 6** Exit recovery-config mode to be prompted to save your changes. Enter **exit** to exit each submode until you return to enable mode.

You can choose to save your changes to the startup configuration or keep changes only in the running configuration by not saving. Running configuration changes won't be retained after a reboot. If you make additional changes later and decide to save the configuration, all of your previous changes are also saved, since the entire running configuration is saved.

Deployment will be blocked while the recovery-config-mode session is open.

**Example:**

```

firepower(recovery-config)# interface Ethernet0/1
firepower(config-if)# ip address 10.0.0.2 255.0.0.0
firepower(config-if)# exit
firepower(recovery-config)# exit
Unsaved changes are not kept if you reboot. Save changes to memory ? [Y]es/[N]o: y

Cryptochecksum: 81a9073e f9535916 9c333d7e 9a3e5e76

3756 bytes copied in 0.70 secs
firepower#

Unsaved changes are not kept if you reboot. Save changes to memory ? [Y]es/[N]o:

Cryptochecksum: 81a9073e f9535916 9c333d7e 9a3e5e76

3756 bytes copied in 0.70 secs
firepower#

```

**Step 7** Return to the Firewall Threat Defense CLI by typing Ctrl+a, then d, or you can enter **exit** to exit each mode.

**Note**

If you type Ctrl+a, then d to return to the Firewall Threat Defense CLI without first exiting recovery-config mode, the recovery-config-mode session will remain open, and deployment will be blocked.



**Example:**

```
firepower# exit
```

```
Logoff
```

```
User enable_1 logged in to firepower
```

```
Logins over the last 1 days: 4. Last login: 20:42:51 UTC Dec 4 2024 from console
```

```
Failed logins since the last login: 0.
```

```
Type help or '?' for a list of available commands.
```

```
firepower> exit
```

```
Console connection detached.
```

```
>
```

---

## Acknowledge the Out-of-Band Configuration

When the Firewall Management Center detects an out-of-band configuration change on a device, you must acknowledge the changes and match the configuration within the Firewall Management Center that you want to keep. Until you acknowledge the changes, deployment will be blocked.

### Procedure

---

**Step 1** Open the **Out-of-Band configuration details** dialog box.

Figure 14: Out-of-Band Configuration Details

### Out-of-band configuration details (1210-1)

The configuration on the device is different from the management center. Review the differential and acknowledge. Manually make changes in the management center before deploying.

Legend: Added Removed

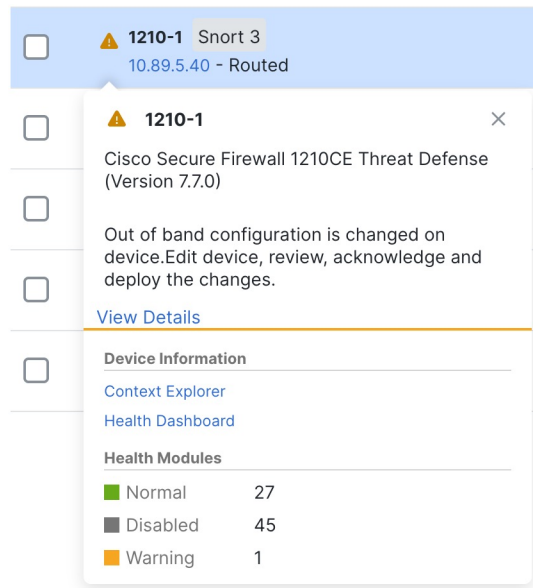
Last-deployed configuration	Configuration on device (1210-1)
1 hostname 1210-1	1 hostname 1210-1
2 enable password ***** pbkdf2	2 enable password ***** pbkdf2
3 service-module 0 keepalive-timeout 4	3 service-module 0 keepalive-timeout 4
4 service-module 0 keepalive-counter 6	4 service-module 0 keepalive-counter 6
5 names	5 names
6 no mac-address auto	6 no mac-address auto
7 interface Ethernet1/1	7 interface Ethernet1/1
8 no switchport	8 no switchport
9 shutdown	9 shutdown
10 no nameif	10 no nameif
11 no security-level	11 no security-level
12 <b>no ip address</b>	12 <b>ip address 10.89.5.30 255.255.255.192</b>
13 interface Ethernet1/2	13 interface Ethernet1/2
14 switchport	14 switchport
15 shutdown	15 shutdown
16 no security-level	16 no security-level
17 interface Ethernet1/3	17 interface Ethernet1/3
18 switchport	18 switchport
19 shutdown	19 shutdown
20 no security-level	20 no security-level
21 interface Ethernet1/4	21 interface Ethernet1/4
22 switchport	22 switchport
23 shutdown	23 shutdown
24 no security-level	24 no security-level
25 interface Ethernet1/5	25 interface Ethernet1/5

Download PDF Report Close Acknowledge

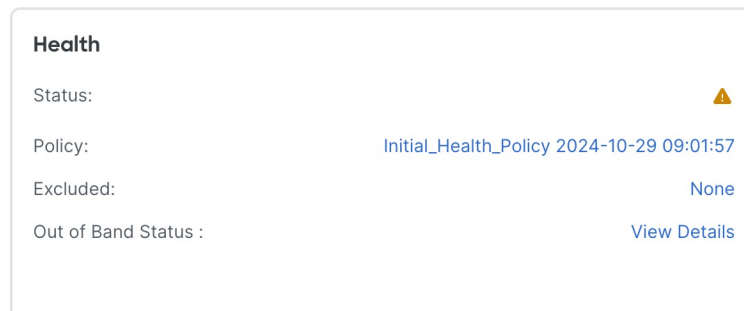
**Note**

Some commands, when set to a default setting, don't appear in the command output. However, the non-default command will show on either side as green (added) or red (removed). For example, if you add **no shutdown** to an interface in recovery-config mode, the **shutdown** command will show in red on the left **Last-deployed configuration** pane while **no shutdown** will *not* appear in the right **Configuration on device** pane. In this case, although the default setting for an interface is **shutdown**, the parser considers **no shutdown** to be the default and doesn't show it.

You can open the dialog box from multiple locations. For example, on the **Devices > Device Management** page, your device will have a warning. Click **View Details**.

**Figure 15: Device Management Warning**

Or, from the **Devices > Device Management > Device > Health** tile, you can click **View Details**.

**Figure 16: Health Out-of-Band Status****Note**

If the out-of-band notification hasn't yet reached the Firewall Management Center, you can check for changes using the **Out of Band Status > Check Latest Status** link.

**Step 2** Click **Download PDF Report** so you can refer to the configuration changes you need to make after you close the dialog box.

Or you can bring up the dialog box at any time to review the changes.

**Step 3** Click **Acknowledge**, and then **Yes**.

Figure 17: Acknowledge

## Acknowledge out-of-band configuration differential

Manually make changes in the management center before deploying. The management center configuration will overwrite the configuration on the device. To acknowledge, click Yes.

No Yes

If you want to prevent an accidental deployment until after you've made your configuration changes, you can instead make the changes and then come back and click **Acknowledge**.

**Step 4** Click **Close** on the **Out-of-Band configuration details** dialog box.

You can still revisit the dialog box to review the changes you need to make until you deploy. The status on the Device page changes to show you have acknowledged the out-of-band configuration:

Figure 18: Acknowledgement Status

⚠ Out of band configuration change is detected and acknowledged [View details...](#)

**Step 5** Make the configuration changes that you made at the CLI.

You'll need to match the configuration CLI to Firewall Management Center screens; there aren't links from the CLI changes directly to screens.

If you don't want to keep your changes, you can simply deploy and overwrite the device configuration. You should make all necessary changes to maintain the management connection as well as any other changes you want to keep. For example, if you changed the IP address at the CLI, you need to go to the **Interfaces** page, edit the interface, and set that IP address to match:

Figure 19: Match the IP Address Change

### Edit Physical Interface

General **IPv4** IPv6 Path Monitoring

IP Type:

IP Address:

eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25

There is no checking mechanism that you made the same change; you could set the IP address differently if you want.

**Step 6** Deploy configuration changes.

After you deploy, you can view the configuration differential—whether you made the changes or not—on the **System** (⚙️) > **Monitoring** > **Audit** page. Check for the subsystem called **Device** > **Device Management** > **Out of band changes**.

---

## Edit Management Settings

These settings control how the Firewall Management Center establishes the management connection with the device.

### 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.

#### 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 Firewall 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 20: 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 21: Edit Management Address

Management

Remote Host Address: 10.89.5.29

Secondary Address:

Status: ✔

Manager Access Interface: [Data Interface](#)

Manager Access Details: [Configuration](#)

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

Figure 22: Management IP Address

Management

Remote Host Address: 10.89.5.29

Secondary Address: 10.99.11.6

[Cancel](#) [Save](#)

- 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 23: Add an ECMP Zone*

The screenshot shows a window titled "Add ECMP". At the top right of the window are a help icon (?) and a close icon (X). Below the title bar is a text input field labeled "Name" containing the text "redundant-mgmt". Underneath the name field are two side-by-side containers. The left container is labeled "Available Interfaces" and is currently empty. The right container is labeled "Selected Interfaces" and contains two entries: "outside" and "redundant", each with a trash can icon to its right. A blue "Add" button is located between the two containers. At the bottom right of the window 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 24: 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

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

Selected Network  
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:

- Click **Static Route**.
- Either click **Add Route** to add a new route, or click **Edit** (✎) for an existing route.
- From the **Interface** drop-down, choose the interface.
- For the destination network, select **any-ipv4** from the **Available Networks** box and click **Add**.
- Enter the default **Gateway**.
- For **Route Tracking**, click **Add** (+) to add a new SLA monitor object.
- Enter the required parameters including the following:
  - The **Monitor Address** as the Firewall 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 25: Add SLA Monitor

**New SLA Monitor Object**

<b>Name:</b> <input type="text" value="mgmt-secondary"/>	<b>Description:</b> <input type="text"/>
<b>Frequency (seconds):</b> <input type="text" value="60"/> <small>(1-604800)</small>	<b>SLA Monitor ID*:</b> <input type="text" value="2"/>
<b>Threshold (milliseconds):</b> <input type="text"/> <small>(0-60000)</small>	<b>Timeout (milliseconds):</b> <input type="text" value="5000"/> <small>(0-604800000)</small>
<b>Data Size (bytes):</b> <input type="text" value="28"/> <small>(0-16384)</small>	<b>ToS:</b> <input type="text"/>
<b>Number of Packets:</b> <input type="text" value="1"/>	<b>Monitor Address*:</b> <input type="text" value="10.89.5.35"/>
<b>Available Zones</b> <input type="text" value="Search"/> <div> <div>mgmt</div> <div>outside</div> </div>	<b>Selected Zones/Interfaces</b> <div> <div>mgmt</div> <div></div> </div>

- 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 Firewall 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 Firewall 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 Firewall Management Center.

## Change Manager Access Interface Settings

Changing any manager interface settings on the device or on the Firewall Management Center can disrupt the management connection. See the following scenarios to change interface settings and reestablish the management connection.

### Change the Device IP Address

Change the device IP address, and then update the address in the Firewall Management Center.

#### Set the Device IP Address

Use one of the following methods to set the manager access interface IP address.

#### *Modify Firewall 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 Firewall Management Center and not at the CLI. If you need to troubleshoot a disrupted management connection, and need to make changes directly on the Firewall Threat Defense, see [Modify the Firewall Threat Defense Data Interface Used for Management at the CLI, on page 32](#).

For information about the Firewall 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 Firewall Management Center connectivity depending on how you identified the Firewall Management Center during initial device setup using the **configure manager add** command:

- **IP address—No action.** If you identified the Firewall 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 Firewall Management Center to keep the information in sync; see [Update the Hostname or IP Address in the Firewall Management Center, on page 36](#). This action can help the connection reestablish faster. **Note:** If you specified an unreachable Firewall Management Center IP address, then see the procedure for NAT ID below.
- **NAT ID only—Manually reestablish the connection.** If you identified the Firewall Management Center using only the NAT ID, then the connection cannot be automatically reestablished. In this case, change the device management IP address in Firewall Management Center according to [Update the Hostname or IP Address in the Firewall Management Center, on page 36](#).



**Note** In a High Availability Firewall Management Center configuration, when you modify the management IP address from the device CLI or from the Firewall Management Center, the secondary Firewall Management Center does not reflect the changes even after an HA synchronization. To ensure that the secondary Firewall Management Center is also updated, switch roles between the two Firewall Management Centers, making the secondary Firewall Management Center the active unit. Modify the management IP address of the registered device on the device management page of the now active Firewall 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 Firewall 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 *ip6\_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 *ip6\_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 *ip6\_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 Firewall 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 Firewall 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 27).

#### 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 farscape1.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 Firewall Management Center:

**configure network management-interface tcpport** *number*

**Example:**

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

The Firewall 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** (Firewall 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 Firewall 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 Firewall Management Center connectivity depending on how you identified the Firewall Management Center during initial device setup using the **configure manager add** command:

- **IP address—No action.** If you identified the Firewall 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 Firewall Management Center to keep the information in sync; see [Update the Hostname or IP Address in the Firewall Management Center, on page 36](#). This action can help the connection reestablish faster. **Note:** If you specified an unreachable Firewall Management Center IP address, then you must manually reestablish the connection using [Update the Hostname or IP Address in the Firewall Management Center, on page 36](#).
- **NAT ID only—Manually reestablish the connection.** If you identified the Firewall Management Center using only the NAT ID, then the connection cannot be automatically reestablished. In this case, change the device management IP address in Firewall Management Center according to [Update the Hostname or IP Address in the Firewall Management Center, on page 36](#).

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

If the management connection between the Firewall Threat Defense and the Firewall Management Center was disrupted, and you want to specify a new data interface to replace the old interface, use the Firewall Threat Defense CLI to configure the new interface.

If the management connection is active, then you should make any changes to an existing data interface using the Firewall Management Center (see [Modify the Firewall Threat Defense Data Interface Used for Management in the GUI, on page 35](#)). 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 Firewall 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 Firewall Threat Defense Management Interfaces at the CLI, on page 26](#).

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

### 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**

**Note**

If you only want to set a new IPv4 address on the same interface and not make any other changes, you can skip this step. Other changes require you to disable the interface first.

**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.

If 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 Firewall Management Center on a specific network.

**configure network management-data-interface client ip\_address netmask**

By default, all networks are allowed.

**Step 7** [Update the Hostname or IP Address in the Firewall Management Center, on page 36.](#)

The connection may be reestablished automatically, but disabling and reenabling the connection in the Firewall Management Center will help the connection reestablish faster. Or you may need to update the device IP address in the Firewall Management Center according to the linked procedure.

**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 Firewall Management Center, choose **Devices > Device Management**, and click **Edit** (✎). In the **Device > Management** area, click **Refresh** next to **Manager Access - Configuration Details**.

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

**Step 10** Choose **Interfaces**, and make the following changes.

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

**Step 11** Choose **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 Firewall Management Center configuration will overwrite any remaining conflicting settings on the Firewall Threat Defense. It is your responsibility to manually fix the configuration in the Firewall Management Center before you re-deploy.

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

### Modify the Firewall Threat Defense Data Interface Used for Management in the GUI

If the management connection is up, but you want to change the IP address of the data interface used for manager access, follow these steps. For example, if you register a device using zero-touch provisioning, then you need to change the IP address to a static address before you can enable high availability.

You can alternatively change interface settings at the CLI, but we recommend only using that method if the management connection is down. Any changes you make at the CLI will have to be replicated in the GUI anyway.

#### Procedure

- 
- Step 1** Choose **Devices > Device Management**, and click **Edit** (✎) next to the device.
- Step 2** Choose **Interfaces**.
- Step 3** If you want to change the interface used for manager access:
- Remove the IP address and name from the old data management interface and disable manager access for this interface.
  - Configure the new data management interface with the new settings and enable manager access for it.
  - If you use a static IP address, you are reminded to make sure you have a default route. Click **Yes**.
  - Click **OK** to exit the interface.
  - Click **Save** on the **Interfaces** page.
- Step 4** If you only want to change the IP address:
- Change the IP address.
  - For a static IP address, you are reminded to make sure you have a default route. Click **Yes**.
  - Click **OK** to exit the interface.
  - Click **Save** on the **Interfaces** page.
- Step 5** Choose **Routing > Static Route** and add or change the default or static route for the manager access interface.
- Step 6** Deploy configuration changes.
- The Firewall Management Center will deploy the configuration changes over the current connection. After the deployment, the data interface will have a new IP address, so the management connection will need to be reestablished.
- Step 7** [Update the Hostname or IP Address in the Firewall Management Center, on page 36.](#)
- Step 8** Ensure the management connection is reestablished.
- In the **Device > Management** area, click **Manager Access Details: Configuration** and then click **Connection Status**.
- The following status shows a successful connection for a data interface, showing the internal "tap\_nlp" interface.

Figure 26: 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 52](#).

## Update the Hostname or IP Address in the Firewall Management Center

If you edit the hostname or IP address of a device after you added it to the Firewall 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 Firewall Management Center.

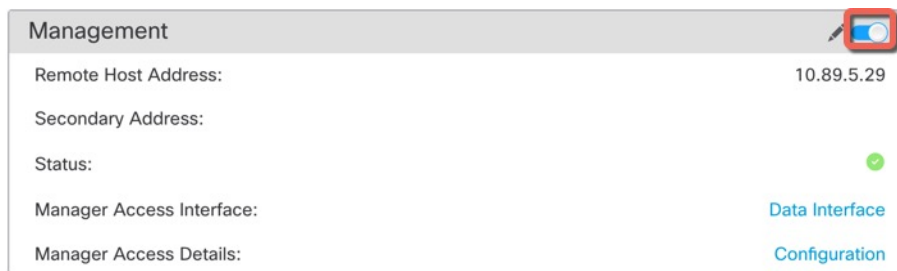
To change the device management IP address on the device, see [Modify Firewall Threat Defense Management Interfaces at the CLI, on page 26](#).

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 **Slider disabled** (🔴).

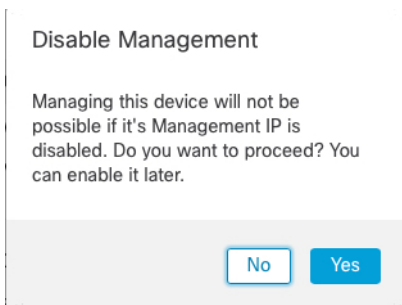
**Figure 27: Disable Management**

The Management dialog box shows the following fields:

Management	
Remote Host Address:	10.89.5.29
Secondary Address:	
Status:	
Manager Access Interface:	<a href="#">Data Interface</a>
Manager Access Details:	<a href="#">Configuration</a>

A red box highlights the 'Disable Management' button in the top right corner of the dialog.

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



**Disable Management**

Managing this device will not be possible if its Management IP is disabled. Do you want to proceed? You can enable it later.

Disabling management blocks the connection between the Firewall Management Center and the device, but does **not** unregister the device from the Firewall 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 28: Edit Management Address**

The Management dialog box shows the following fields:

Management	
Remote Host Address:	10.89.5.29
Secondary Address:	
Status:	
Manager Access Interface:	<a href="#">Data Interface</a>
Manager Access Details:	<a href="#">Configuration</a>

A red box highlights the 'Edit' button in the top right corner of the dialog.

- 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 21](#).

Figure 29: Management IP Address

Management

Remote Host Address: 10.89.5.29

Secondary Address: 10.99.11.6

Cancel Save



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

Figure 30: Enable Management Connection

Management

Remote Host Address: 10.89.5.4

Secondary Address:

Status: 

Manager Access Interface: Management Interface

## Change the Firewall Management Center IP Address

If you change the Firewall Management Center IP address or hostname, you should also change the value at the device CLI so the configurations match. Although in most cases, the management connection will be reestablished without changing the Firewall Management Center IP address or hostname on the device, in at least one case, you must perform this task for the connection to be reestablished: when you added the device to the Firewall Management Center and you specified the NAT ID only. Even in other cases, we recommend keeping the Firewall Management Center IP address or hostname up to date for extra network resiliency.

### Procedure

**Step 1** Change the Firewall Management Center IP address.

#### Caution

Be careful when making changes to the Firewall Management Center interface to which you are connected; if you cannot re-connect because of a configuration error, you need to access the Firewall 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.

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

**Step 2** At the Firewall Threat Defense CLI, view the Firewall 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
```

**Step 3** At the Firewall Threat Defense CLI, edit the Firewall Management Center IP address or hostname.

**configure manager edit identifier {hostname {ip\_address | hostname} | displayname display\_name}**

If the Firewall 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**.

The management connection will go down, and then reestablish. You can monitor the state of the connection using the **sftunnel-status** command.

**Example:**

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


## Change Both Firewall Management Center and Threat Defense IP Addresses

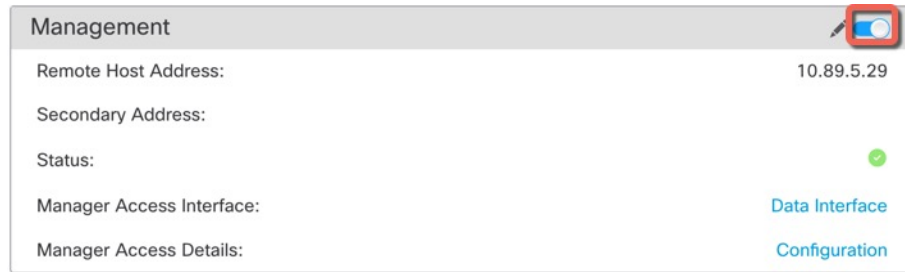
You might want to change both Firewall Management Center and Firewall Threat Defense IP addresses if you need to move them to a new network.

### Procedure

**Step 1** Disable the management connection.

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

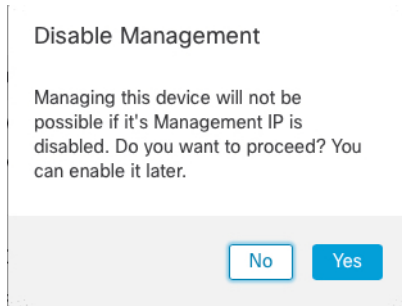
- a) Choose **Devices > Device Management**.
- b) Next to the device, click **Edit** (✎).
- c) Click **Device**, and view the **Management** area.
- d) Disable management temporarily by clicking the slider so it is disabled (.

**Figure 31: Disable Management**


The screenshot shows the 'Management' configuration page. At the top right, there is a toggle switch icon (a blue circle with a white dot) that is highlighted with a red square. Below the header, the following fields are visible:

- Remote Host Address: 10.89.5.29
- Secondary Address:
- Status: (indicated by a green checkmark)
- Manager Access Interface: Data Interface
- Manager Access Details: Configuration

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



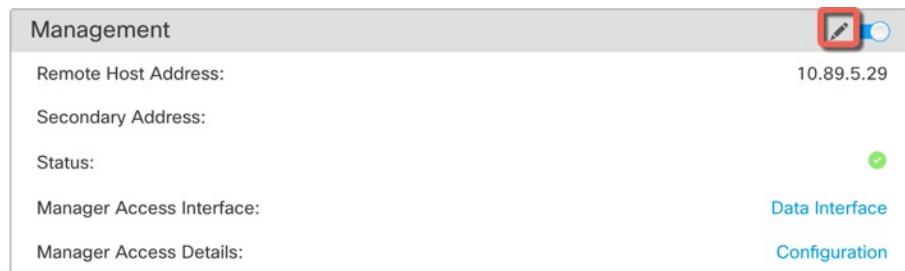
The screenshot shows a dialog box titled 'Disable Management'. The text inside reads: 'Managing this device will not be possible if it's Management IP is disabled. Do you want to proceed? You can enable it later.' At the bottom of the dialog, there are two buttons: 'No' and 'Yes'.

**Step 2** Change the device IP address in the Firewall 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.

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

**Figure 32: Edit Management Address**


The screenshot shows the 'Management' configuration page. At the top right, there is an 'Edit' icon (a pencil inside a square) that is highlighted with a red square. Below the header, the following fields are visible:

- Remote Host Address: 10.89.5.29
- Secondary Address:
- Status: (indicated by a green checkmark)
- Manager Access Interface: Data Interface
- Manager Access Details: Configuration

- 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 33: Management IP Address

**Step 3** Change the Firewall Management Center IP address.

**Caution**

Be careful when making changes to the Firewall Management Center interface to which you are connected; if you cannot re-connect because of a configuration error, you need to access the Firewall 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** > **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 Firewall Threat Defense CLI, view the Firewall 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 Firewall Management Center IP address or hostname.

**configure manager edit identifier {hostname {ip\_address | hostname} | displayname display\_name}**

If the Firewall 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:

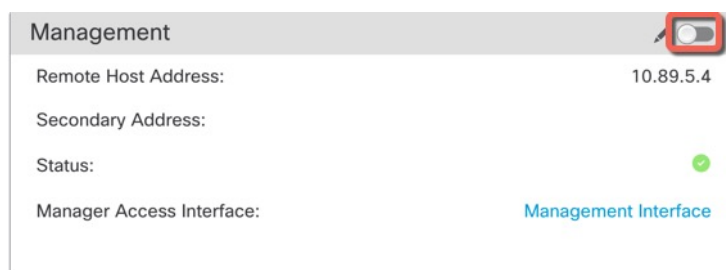
**configure network management-data-interface disable**

**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 34: Enable Management Connection*



**Step 7** (If using a data interface for manager access) Refresh the data interface settings in the Firewall Management Center.

For a high-availability pair, perform this step on both units.

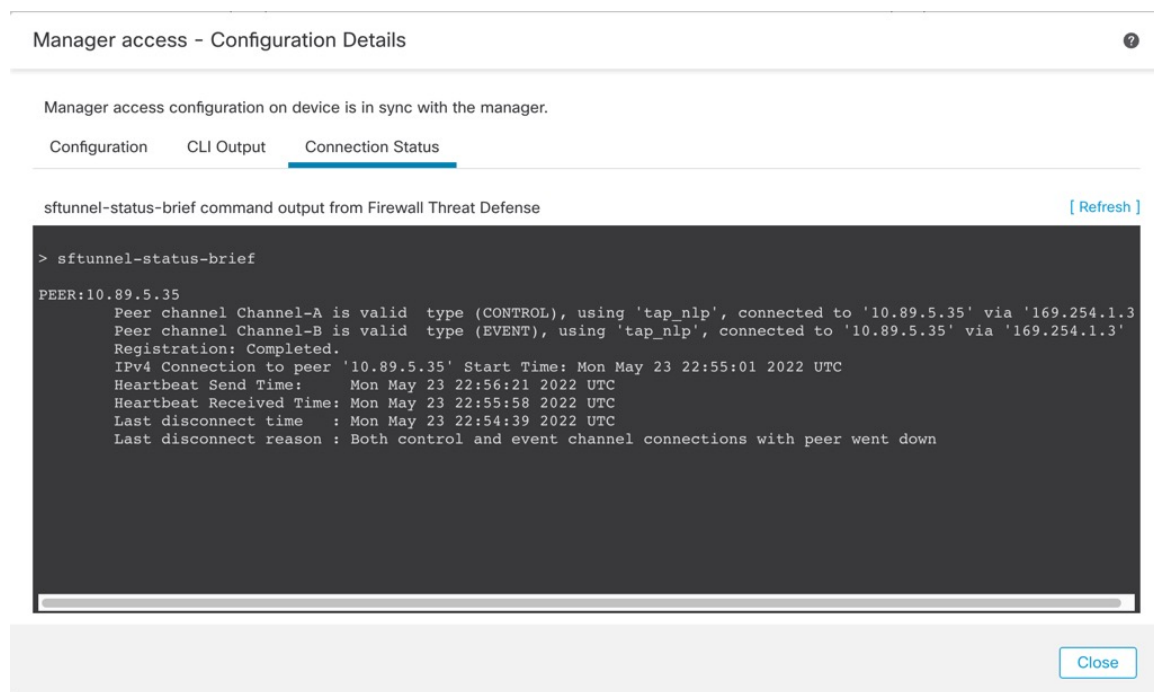
- Choose **Devices > Device Management > Device > Management > Manager Access - Configuration Details**, and click **Refresh**.
- Choose **Devices > Device Management > Interfaces**, and set the IP address to match the new address.
- Return to the **Manager Access - Configuration Details** dialog box, and click **Acknowledge** to remove the deployment block.

**Step 8** Ensure the management connection is reestablished.

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

At the Firewall 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 35: Connection Status**

**Step 9** (For a high-availability Firewall Management Center pair) Repeat configuration changes on the secondary Firewall Management Center.

- Change the secondary Firewall 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 Firewall Management Center.
- Reenable the management connection.

## Change the Manager Access Interface

After you register the device, you can change the manager access interface, between the Management interface and a data interface.

### Change the Manager Access Interface from Management to Data

You can manage the Firewall 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 Firewall 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 47](#).

Initiating the manager access migration from Management to data causes the Firewall Management Center to apply a block on deployment to the Firewall 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. Click **Device**, and in 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.

**Figure 36: 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

- b) Click **OK** and then **Close**.

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 37: 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 the data interface(s). Click **Interfaces**, click **Edit** (✎) for the interface, and then click **Manager Access**.
- Check **Enable management access** and click **OK**. By default, all networks are allowed, but you can limit access as long as the Firewall Management Center address is allowed.
- If the manager access interface uses a static IP address, you are reminded to configure routing for it.
- Click **Save** on the **Interfaces** page. See [Configure Routed Mode Interfaces](#) for more information about interface settings. 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 21](#) 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 Firewall Management Center can reach the Firewall Threat Defense at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes.
- Step 4** Make sure the Firewall Threat Defense can route to the Firewall 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 Firewall Threat Defense using SSH, you need to explicitly allow it.
- Step 7** Deploy configuration changes.
- You will see a validation error to confirm that you are changing the manager access interface. Check **Ignore warnings** and deploy again.

The Firewall 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 Firewall 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 Firewall Threat Defense so it can reach the Firewall Management Center on the data interface. For high availability, perform this step on both units.

**Step 10** In the Cloud-Delivered Firewall Management Center, disable the management connection for the Firewall Threat Defense in the **Devices > Device Management** page in the **Device > Management** area, and then reenabling the connection.

**Step 11** Ensure the management connection is reestablished.

In the **Device > Management** area, click **Manager Access Details: Configuration** and then click **Connection Status**.

Alternatively, you can check at the Firewall 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 38: 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 52](#).

## Change the Manager Access Interface from Data to Management

You can manage the Firewall 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 Firewall 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 43](#).

Initiating the manager access migration from data to Management causes the Firewall Management Center to apply a block on deployment to the Firewall 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. Click **Device**, and in 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.

**Figure 39: Manager Access Interface**

- b) Click **Save**.

Click **OK** and then **Close**.

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**.

**Figure 40: Manager Access**



- Step 2** Disable manager access on the data interface(s). Click **Interfaces**, click **Edit** (✎) for the interface, and then click **Manager Access**.
- Uncheck **Enable management access** and click **OK**. Click **Save** on the **Interfaces** page. 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 Firewall 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 Firewall Management Center.
- Step 4** Deploy configuration changes.
- The Firewall Management Center will deploy the configuration changes over the current data interface.
- Step 5** If necessary, re-cable the Firewall Threat Defense so it can reach the Firewall Management Center on the Management interface. For High Availability, perform this step on both units.
- Step 6** At the Firewall 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 Cloud-Delivered Firewall Management Center, disable the management connection for the Firewall Threat Defense in the **Devices > Device Management > Device > Management** section, and then reenables the connection.
- Step 8** Ensure the management connection is reestablished.
- In the Firewall Management Center, check the management connection status on the **Devices > Device Management > Device > Management > Status** field or view notifications in the Firewall Management Center.
- At the Firewall 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 52](#).

## Troubleshooting the Management Connection

.

## Manually Roll Back the Configuration if the Firewall Management Center Loses Connectivity

If you use a data interface on the Firewall Threat Defense for manager access, and you deploy a configuration change from the Firewall Management Center that affects the network connectivity, you can roll back the configuration on the Firewall Threat Defense to the last-deployed configuration so you can restore management connectivity. You can then adjust the configuration settings in Firewall 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 67](#).

See the following guidelines:

- Only the previous deployment is available locally on the Firewall 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 Firewall 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 Firewall Threat Defense CLI. Note that if you changed data interface settings after the last Firewall 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 Firewall 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 Firewall 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 Firewall Threat Defense notifies the Firewall Management Center that the rollback was completed successfully. In the Firewall Management Center, the deployment screen will show a banner stating that the configuration was rolled back.

#### Note

If the rollback failed and the Firewall 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 Firewall Management Center management access is restored; in this case, you can

resolve the Firewall Management Center configuration issues, and redeploy from the Firewall Management Center.

#### Example:

For the Firewall 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 Firewall Threat Defenses in a high availability pair that use a data interface for Firewall 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 Firewall Management Center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the Firewall 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 52](#).

## 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 Firewall Threat Defense in the Firewall Management Center so you do not disrupt the connection. If you change the management interface type after you add the Firewall Threat Defense to the Firewall 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 Firewall Management Center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

At the Firewall 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 Firewall Threat Defense network information

At the Firewall 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 Firewall Threat Defense registered with the Firewall Management Center**

At the Firewall Threat Defense CLI, check that the Firewall 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 Firewall Management Center

At the Firewall Threat Defense CLI, use the following command to ping the Firewall Management Center from the data interfaces:

```
ping fmc_ip
```

At the Firewall Threat Defense CLI, use the following command to ping the Firewall Management Center from the Management interface, which should route over the backplane to the data interfaces:

```
ping system fmc_ip
```

### Capture packets on the Firewall Threat Defense internal interface

At the Firewall 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 capturename trace detail
```

### Check the internal interface status, statistics, and packet count

At the Firewall 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_vtun 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 Firewall 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 Firewall 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 Firewall 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 Firewall 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 Security Cloud Control 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 Security Cloud Control 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 Security Cloud Control .

### Data Management Interface on Active unit has Connectivity Issues

1. In Security Cloud Control, manually switch the active unit to standby. See [Switch the Active Peer in the Firewall 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 Security Cloud Control.

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 Security Cloud Control 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' dialog box. At the top, there are tabs for 'General', 'IPv4', 'IPv6', 'Advanced', 'Path Monitoring', and 'Hardware Configuration'. The 'General' tab is active. Below the tabs, there is a section for 'Firewall Management Center Access'. Under this section, there is a 'Name' field with the value 'outside'. Below the 'Name' field, there is a checkbox labeled 'Enabled' which is checked. Below the 'Enabled' checkbox, there is a checkbox labeled 'Management Only' which is unchecked. At the bottom, there is a 'Description' field which is 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 Security Cloud Control 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:

Cancel OK

- 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 (enables it is available for route leak)

**outside-new (Firewall Management Center Access)**

diagnostic

IPv4-Benchmark-Tests

IPv4-Link-Local

IPv4-Multicast

IPv4-Private-10.0.0.0-8

IPv4-Private-172.16.0.0-12

Selected Network

outside-new (Firewall Management Center Access)

outside-new

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 Security Cloud Control 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 Firewall 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 Firewall 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 Security Cloud Control 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 Security Cloud Control, click **Security Devices > FTD**.
7. Select your Firewall Threat Defense and in the **Management** pane on the right, click **Device Summary**.
8. In **Management > FMC Access Details**, click **Refresh**.

The Security Cloud Control 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 Security Cloud Control manually. You can view the discrepancies between Security Cloud Control and the Firewall 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 Security Cloud Control configuration will overwrite any remaining conflicting settings on the FTD. It is your responsibility to manually fix the configuration in the Security Cloud Control 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 Security Cloud Control restores its connectivity with the active unit, Security Cloud Control 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 41: Inventory Details**

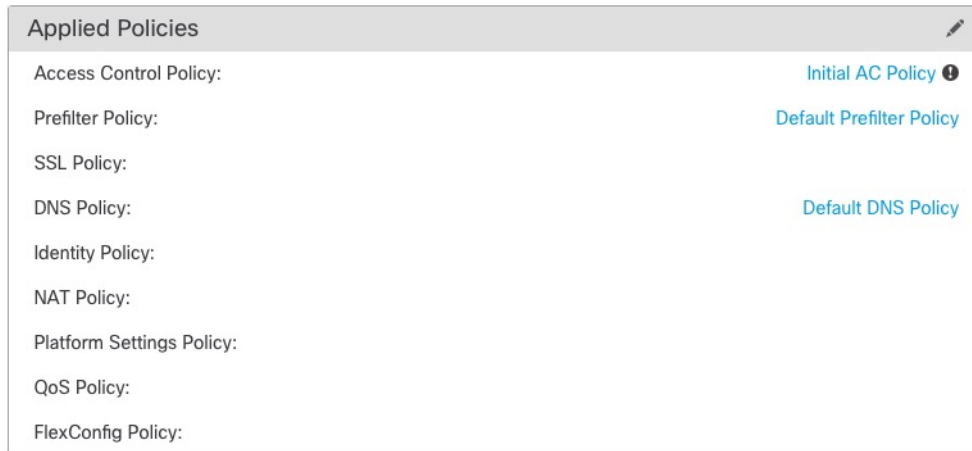
Inventory Details		
CPU Type:	CPU Xeon E5 series 2300 MHz	
CPU Cores:	1 CPU (4 cores)	
Memory:	8192 MB RAM	
Storage:	N/A	
Chassis URL:	N/A	
Chassis Serial Number:	N/A	
Chassis Module Number:	N/A	
Chassis Module Serial Number:	N/A	

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 42: Applied Policies**



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 43: Access Policy Information for Troubleshooting**

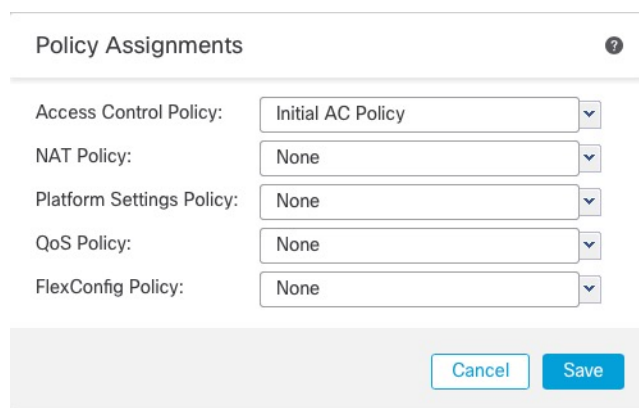


You can assign policies to an individual device from the **Device Management** page.

## 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 44: Policy Assignments*



Policy Assignments ?

Access Control Policy: Initial AC Policy

NAT Policy: None

Platform Settings Policy: None

QoS Policy: None

FlexConfig Policy: None

Cancel Save

- 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.

Field	Description
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><b>Note</b> By default, the <b>Object Group Search</b> 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 <b>Object Group Search</b> 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 1](#).

## 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 assigned device handles traffic. See [Snort Restart Traffic Behavior](#) for more information.

See the following behavior:

**Firewall 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

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

### What to do next

- Deploy configuration changes.

## Configure Object Group Search

While operating, the Firewall 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 Firewall 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 Firewall 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 Firewall 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 Firewall 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 45: 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 Firewall Management Center Loses Connectivity, on page 50](#)).

See the following guidelines:

- Only the previous deployment is available locally on the Firewall 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 Firewall 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 Firewall Threat Defense CLI. Note that if you changed data interface settings after the last Firewall 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 Firewall 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 46: 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 47: 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	<b>Routing:</b>		
Virtual Router (Global)	<b>Virtual Router: Virtual Router (Global)</b>		
Static Route IPv4	<b>Static Route IPv4:</b>		admin
Static Route IPv6	<b>Static Route IPv6:</b>		admin
	<b>IPv4 Route:</b>		
	Static Route Interface(Unchanged): outside	outside	
	Static Route Network(Unchanged): any-ipv4	any-ipv4	
	Gateway: literal:10.10.35.63	literal:10.10.35.64	
	<b>Static Route IPv6:</b>		
	<b>IPv6 Route:</b>		
	IPv6 Static Route Interface(Unchanged): inside	inside	
	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 Firewall Management Center, check the management connection status on the **Devices > Device Management > Device > Management > FMC Access Details > Connection Status** page.

At the Firewall 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 52](#).

# Edit Cluster Health Monitor Settings

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

**Figure 48: Cluster Health Monitor Settings**

Cluster Health Monitor Settings			
<b>Timeouts</b>			
Hold Time			3 s
Interface Debounce Time			9000 ms
<b>Monitored Interfaces</b>			
Service Application			Enabled
Unmonitored Interfaces			None
<b>Auto-Rejoin Settings</b>			
	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
<b>Timeouts</b>	
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.
<b>Monitored Interfaces</b>	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.

Field	Description
Unmonitored Interfaces	Shows unmonitored interfaces.
<b>Auto-Rejoin Settings</b>	
Cluster Interface	Shows the auto-rejoin settings after a cluster control link failure.
<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 49: 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 or VNet) 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 50: 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 51: 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

Add

Unmonitored Interfaces ⓘ

☒ 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 or VNet) 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.

# History for Device Settings

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Recovery-config mode for emergency on-device configuration and out-of-band configuration detection on the Firewall Management Center	20250219	7.7.0	<p>If you lose the management connection to your device, you can make select configuration changes directly at the device CLI to:</p> <ul style="list-style-type: none"> <li>• Restore the management connection if you are using a data interface for manager access</li> <li>• Make select policy changes that can't wait until the connection is restored</li> </ul> <p>After the management connection is restored, the Firewall Management Center will detect the configuration changes on the device. It does not automatically update the device configuration in the Firewall Management Center; you must view the configuration differences, acknowledge that the device configuration is different, and then manually make the same changes in the Firewall Management Center before you deploy.</p> <p>New/modified diagnostic CLI (<b>system support diagnostic-cli</b>) command: <b>configure recovery-config</b></p> <p>New/modified screens: <b>Devices &gt; Device Management &gt; Device &gt; Health &gt; Out of Band Status</b></p>
High availability is supported with redundant manager access data interfaces	20250219	7.7.0	You can now use redundant manager access data interfaces with high availability.
Cluster health monitor settings.	20221213	Any	<p>You can now edit cluster health monitor settings.</p> <p>New/modified screens: <b>Devices &gt; Device Management &gt; Cluster &gt; Cluster Health Monitor Settings</b></p> <p><b>Note</b></p> <p>If you previously configured these settings using FlexConfig, be sure to remove the FlexConfig configuration before you deploy. Otherwise the FlexConfig configuration will overwrite the management center configuration.</p>

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Redundant manager access data interface.	20221213	7.3.0	<p>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. 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.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• <b>Devices &gt; Device Management &gt; Device &gt; Management</b></li> <li>• <b>Devices &gt; Device Management &gt; Device &gt; Interfaces &gt; Manager Access</b></li> </ul>
Policy rollback support for high availability devices.	20220609	7.2.0	The <b>configure policy rollback</b> command is supported for high availability devices.
Auto rollback of a deployment that causes a loss of management connectivity.	20220609		<p>You can now enable auto rollback of the configuration if a deployment causes the management connection between the management center and the threat defense to go down. Previously, you could only manually rollback a configuration using the <b>configure policy rollback</b> command.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• <b>Devices &gt; Device Management &gt; Device &gt; Deployment Settings</b></li> <li>• <b>Deploy &gt; Advanced Deploy &gt; Preview</b></li> <li>• <b>Deploy &gt; Deployment History &gt; Preview</b></li> </ul>
Object group search is enabled by default for access control rules.	20220609	7.2.0	The <b>Object Group Search</b> setting is enabled by default for managed devices starting with Version 7.2.0. This option is in the <b>Advanced Settings</b> section when editing device settings on the Device Management page.
Import and export device configurations.	20220609	7.2.0	<p>You can export the device-specific configuration, and you can then import the saved configuration for the same device in the following use cases:</p> <ul style="list-style-type: none"> <li>• Moving the device to a different FMC.</li> <li>• Restore an old configuration.</li> <li>• Reregistering a device.</li> </ul> <p>New/modified screens: <b>Devices &gt; Device Management &gt; Device &gt; General</b></p>
Update the FMC IP address on FTD.	20220609	7.0.3	<p>If you change the FMC IP address, you can now use the FTD CLI to update the device.</p> <p>New/modified commands: <b>configure manager edit</b></p>