

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 11
- View inventory details, on page 40
- Edit applied policies, on page 40
- Edit advanced settings, on page 42
- Edit deployment settings, on page 46
- Hot swap an SSD, on page 49
- Configure SNMP for FXOS, on page 52
- Configure alarms for the ISA 3000, on page 55
- History for Device Settings, on page 67

Edit general settings

Edit general device settings to customize the device name, packet transfer options, and force deployment settings for managed devices.

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

Table 1: General section table fields

Field	Description
Name	The display name of the device on the Firewall Management Center.

Field	Description
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: **routed** or **transparent**.
Compliance Mode	This displays the security certifications compliance for a device. Valid values are CC, UCAPL and None.
TLS Crypto Acceleration:	Shows whether TLS crypto acceleration is enabled or disabled.
Device Configuration	Lets you copy, export, or import a configuration. See Copy a configuration to another device, on page 2 and Export and import the device configuration, on page 4.

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** ( ).

a) Enter a **Name** for the managed device.

b) Check **Transfer Packets** to allow packet data to be stored with events on the Firewall Management Center.

c) 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 2 and Export and import the device configuration, on page 4.

Step 6 Click **Deploy**.

What to do next

- Deploy configuration changes; see Deploy configuration changes.

Copy a configuration to another device

Copy configurations and policies from a pre-configured device to a new device, instead of manually reconfiguring the new device.

When a new device is deployed in the network, you can 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.
- No configuration deployment is in progress on the source or the destination devices.

Follow these steps to copy a configuration to another device:

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 such as 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

Export device-specific configuration to create a backup that can be imported for the same device in various scenarios including moving the device to a different Firewall Management Center, restoring old configurations, or reregistering a device.

You can export all device-specific configurations available 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 these use cases:

- Moving the device to a different Firewall Management Center—First delete 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.
- Moving the device between domains—When you move a device between domains, some device-specific configuration is not retained because supporting objects (such as interface groups for security zones) do not exist in the new domain. By importing the configuration after the domain move, any necessary objects are created for that domain, and the device configuration is restored.
- 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 delete a device from the Firewall Management Center, but then want to add it back, you can import the saved configuration.

Before you begin

Review these 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 make inventory changes after your export (such as adding or deleting network modules or configuring or joining breakout ports), the device inventory will not match the Firewall Management Center. In this case, the device inventory will be maintained, and you will be prompted to sync the

interfaces (see Sync Interface Changes with the Firewall Management Center) and discard incompatible configuration in the Firewall Management Center when you try to deploy. You will have to repeat the inventory changes and related configuration in the Firewall Management Center.

- If you export a standalone configuration, you cannot import it to a high availability pair or vice versa.
- When moving the device to a different Firewall Management Center, the target Firewall Management Center version must be the same as the source version.
- If an object doesn't exist, it will be created. If an object exists, but the value is different, refer to this table:

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.	Network and Port objects: Create object overrides for this device. See Object overrides. 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. All other objects: Reuse existing objects even though the values are different.
Object doesn't exist.	Create new objects.

Follow these steps to export and import the device configuration:

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.

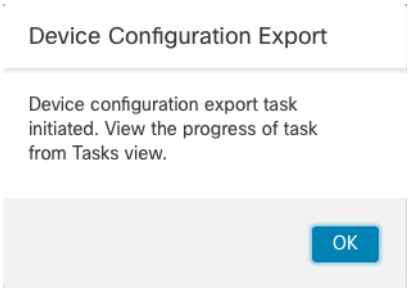
a) In the **General** area, click **Export**.

Figure 1: Export device configuration



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

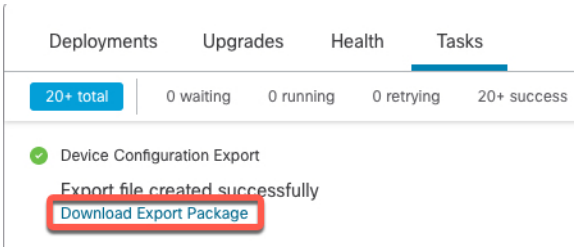
Figure 2: Acknowledge export



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

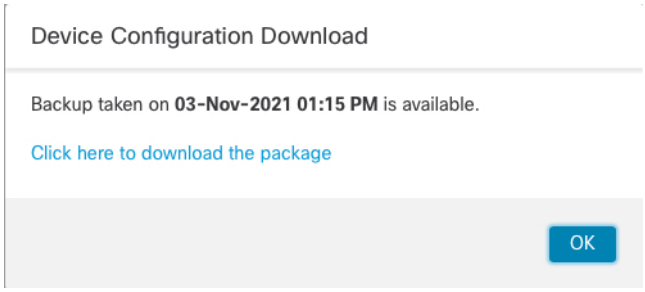
b) Click **Notifications**, and then click the **Tasks** tab. Verify if the export has completed, and then click **Download Export Package**. Alternatively, you can click the **Download** button in the **General** area.

Figure 3: Export task



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

Figure 4: Download package



Step 5 Import the configuration.

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

Figure 5: 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 6: Import package

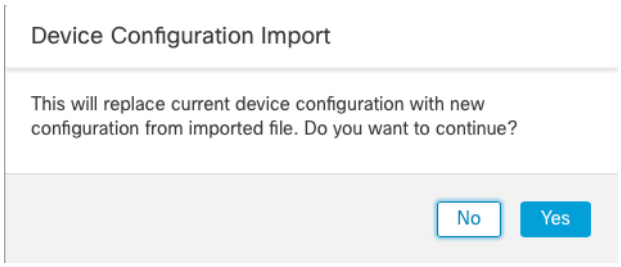
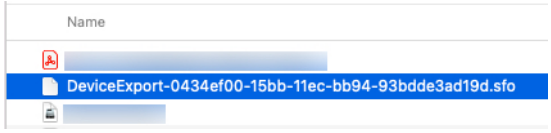
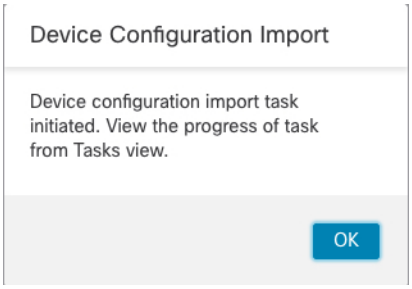


Figure 7: Navigate to package



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

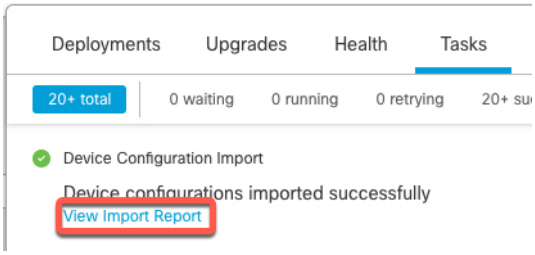
Figure 8: Acknowledge import



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

b) To view the import reports, click **Notifications**, and then click the **Tasks** tab. Click **View Import Report**.

Figure 9: View import report



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

Cisco Firepower Management Center

Device Configuration Import Reports

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

c) Deploy configuration changes; see Deploy configuration changes.

Edit license settings

Enable or disable specific licenses on your managed device to control which features are available for use.

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; see Deploy configuration changes.

View system information

The **System** section of the **Device** page displays a read-only table containing system information. You can also shut down or restart the device from this pane, using the icons at the top-right corner.

Figure 10: System

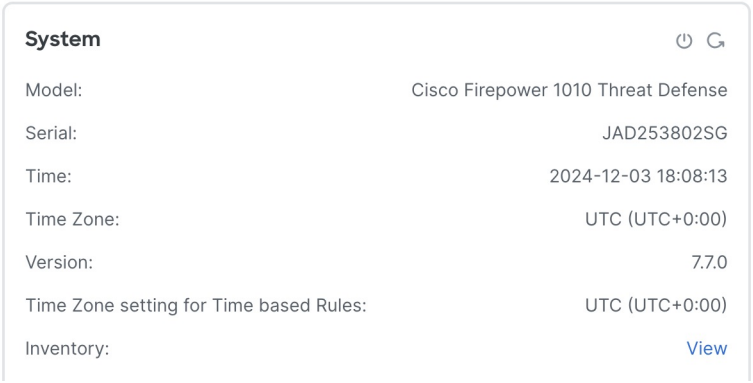


Table 3: System section table fields

Field	Description
Shut Down Device ( )	Shuts down the device. See Shut down or restart the device.
Restart Device ( )	Restarts the device. See Shut down or restart the device.
Model	Model name and number.
Serial	PCB (circuit board) serial number. The firewall includes two serial numbers: the chassis serial number and the PCB serial number. The chassis serial number is shown in the Inventory section.
Time	Current system time of the device.
Time Zone	Time zone.

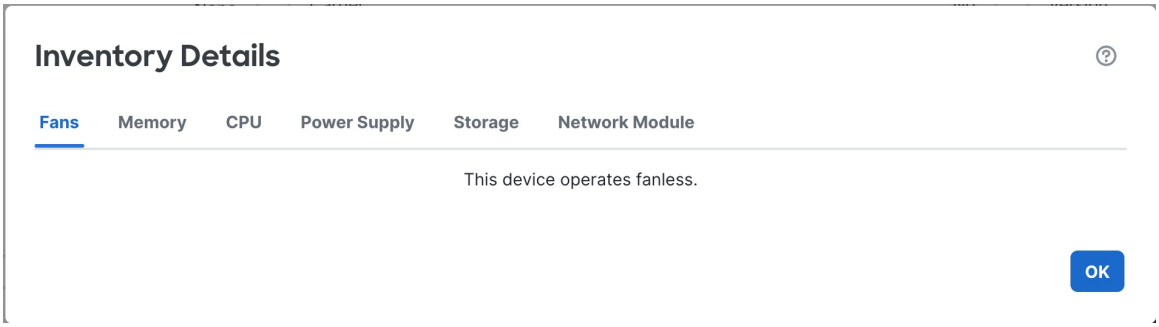
Field	Description
Version	Version of the software currently installed on the managed device.
Time Zone setting for Time based rules	Current system time of the device in the time zone specified in device platform settings.
Inventory	Inventory details. See View Device Inventory.

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 11: 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 *Custom Snort 3 Intrusion Policies for Access Control*.

Note Snort3 is default for Secure Firewall 1200. It does not support Snort2.

Edit health settings

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

Table 4: Health section table fields

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

Edit management settings

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

Change manager access interface settings

Changing manager interface settings on the device or on the Firewall Management Center can disrupt the management connection. Review these scenarios that 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 these methods to set the manager access interface IP address.

Modify Firewall Threat Defense management interface settings at the CLI

Many management interface settings are set during device initial setup; this task allows you to update them, add event-only interfaces (if supported), or configure static routes, DNS domains, and other advanced settings. Use the CLI when you need direct device access or troubleshooting. If you wish to configure network settings for a data interface used for management, use the device management center interface instead.

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 16 .

For information about the Firewall Threat Defense CLI, see the *Cisco Secure Firewall Threat Defense Command Reference* .

Before you begin

- You can create user accounts that can log into the CLI using the **configure user add** command ; see Add an internal user at the CLI . You can also configure AAA users according to Configure external authentication .
- Be cautious when making changes to the management interface using SSH. If you cannot re-connect because of a configuration error, access the device console port.
- In high-availability configurations, when you modify the management IP address of a registered device from the device CLI or from the Firewall Management Center , the standby Firewall Management Center does not reflect the changes even after a high-availability synchronization. To ensure that the standby Firewall Management Center is also updated, switch roles between the two Firewall Management Center s, making the secondary Firewall Management Center as the active unit. Modify the management IP address of the registered device on the **Device Management** page of the standby Firewall Management Center .

Procedure

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

See Log into the Command-Line Interface on the device .

Step 2 Log in with the Admin username and password.

Step 3 (Firepower 4100/9300 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.

(Optional) 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 must enable an event-only interface on the Firewall Management Center that is dedicated exclusively to event traffic. See the *Cisco Secure Firewall Management Center Administration Guide* .

Example:

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

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

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

a) Configure the IPv4 address:

- Manual configuration:

  configure network ipv4 manual *ip_address netmask gateway_ip* [*management_interface*]

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

  Example:

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

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

  configure network ipv4 dhcp

b) Configure the IPv6 address:

- Stateless autoconfiguration:

  configure network ipv6 router [*management_interface*]

  Example:

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

- Manual configuration:

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

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

  Example:

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

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

  configure network ipv6 dhcp

c) 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 5 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 6 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 12).

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 7 Do these settings:

a) 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.

b) 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.

c) 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
```

d) 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
We recommend 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.

e) (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
>
```

f) 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 8 If you change the device management IP address, then see the following tasks for Firewall Management Center connectivity. Perform these tasks depending on how you identified the Firewall Management Center during initial device setup using the **configure manager add** command (see Register with a new management center) :

- **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 20. This action can help reestablish the connection faster. 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 20
- **NAT ID only — Manually reestablish the connection.** If you identified the Firewall Management Center using only the NAT ID, then the connection does not automatically reestablish. 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 20 .

Modify the Firewall Threat Defense data interface used for management at the CLI

This task allows you to specify a new data interface to replace the old interface when the management connection has been disrupted and you need to restore connectivity between the Firewall Threat Defense and the Firewall Management Center.

If the management connection is active, make 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 19). For initial setup of the data management interface, see the **configure network management-data-interface** command in Complete the Firewall Threat Defense Initial Configuration Using the CLI.

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 interface settings at the CLI , on page 11.

For information about the Firewall Threat Defense CLI, see the *Cisco Secure Firewall Threat Defense Command Reference*.

Before you begin

If you are changing the data management interface to a new interface, move the current interface cable to the new interface.

Procedure

Step 1 Connect to the device CLI.

Use the console port when executing 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 have SSH access to the dedicated management interface, you can use the SSH connection.

See Log into the Command-Line Interface on the device.

a) Log in with the **admin** username and password.

Step 2 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 3 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.

>
```

a) 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 4 Update the Hostname or IP Address in the Firewall Management Center, on page 20.

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 5 Check that the management connection was reestablished.

sftunnel-status-brief

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

```
> 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 6 In the Firewall Management Center, choose **Devices** > **Device Management**, and click **Edit** (). In the **Device** area, against the **Management** field, 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 7 Choose **Interfaces**, and make the changes.

a) Remove the IP address and name from the old data management interface and disable manager access for this interface.

b) Configure the new data management interface with the new settings (the ones you used at the CLI) and enable manager access for it.

Step 8 Under the **Routing** tab, click **Static Route**, and change the default route from the old data management interface to the new one.

Step 9 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

Configure the data interface IP address settings to change the management connection or update the interface used for manager access.

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 using that method only if the management connection is down. Any changes you make at the CLI should be replicated in the GUI.

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:

a) Remove the IP address and name from the old data management interface and disable manager access for this interface.

b) Configure the new data management interface with the new settings and enable manager access for it.

c) If you use a static IP address, you are reminded to make sure you have a default route. Click **Yes**.

d) Click **OK** to exit the interface.

e) Click **Save** on the **Interfaces** page.

Step 4 If you only want to change the IP address:

a) Change the IP address.

b) For a static IP address, you are reminded to make sure you have a default route. Click **Yes**.

c) Click **OK** to exit the interface.

d) Click **Save** on the **Interfaces** page.

Step 5 Click the **Routing** tab, click **Static Route**, and then add or change the default or static route for the manager access interface.

Step 6 Deploy configuration changes; see 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.

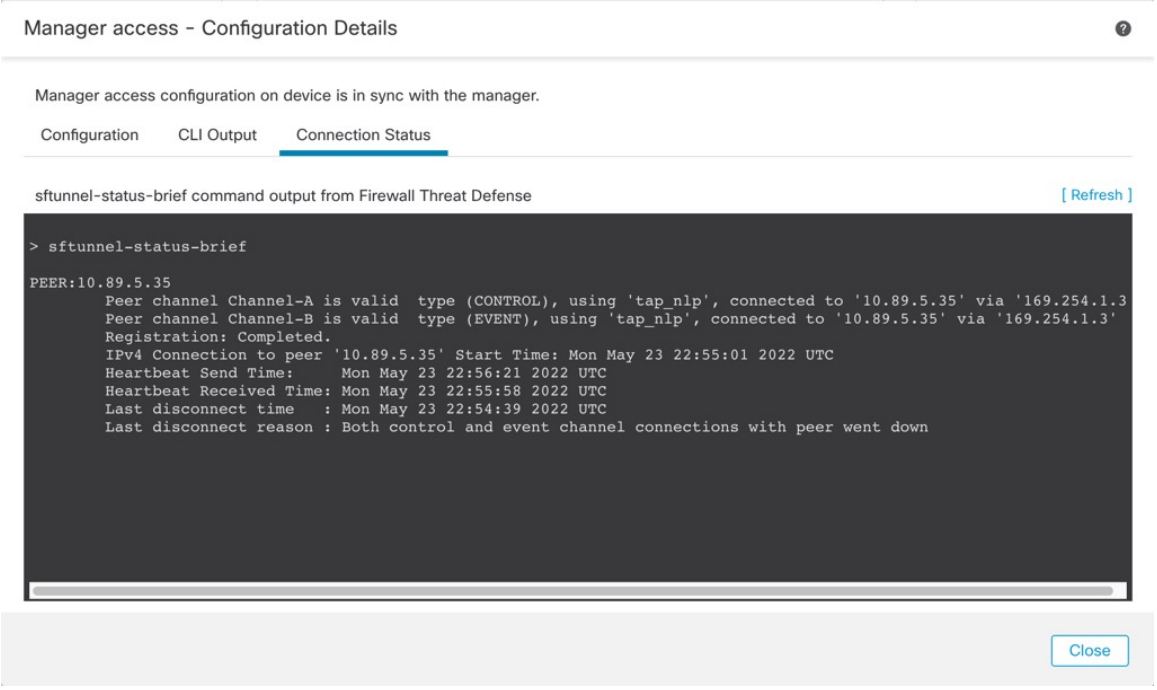
Step 7 Update the Hostname or IP Address in the Firewall Management Center, on page 20.

Step 8 Ensure the management connection is reestablished.

In the **Device** area, against the **Management** field, 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 12: 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 39.

Update the Hostname or IP Address in the Firewall Management Center

This task allows you to manually update the hostname or IP address on the managing Firewall Management Center when device network settings have been modified outside of the management interface.

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 this procedure 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 interface settings at the CLI , on page 11.

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.

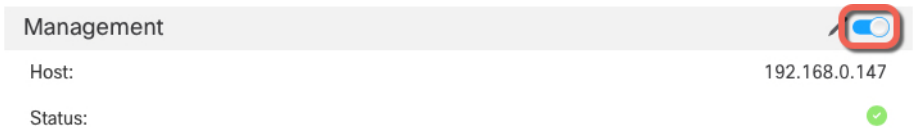
Procedure

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

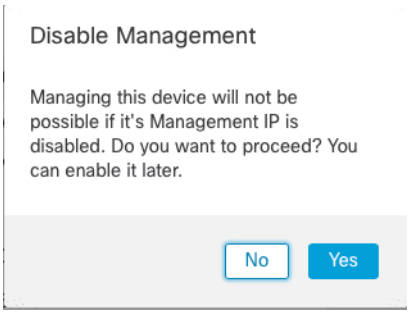
Step 2 Next to the device where you want to modify management options, click **Edit** ( ).

Step 3 Click **Device** and view the **Management** area.

Step 4 Disable management temporarily by clicking the slider so it is disabled **Slider disabled** ( ).

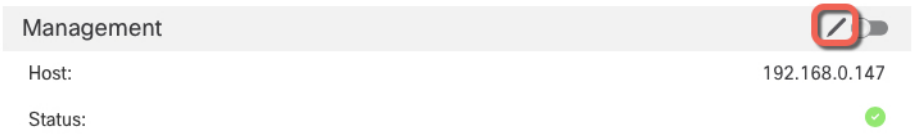


You are prompted to proceed with disabling management; click **Yes**.



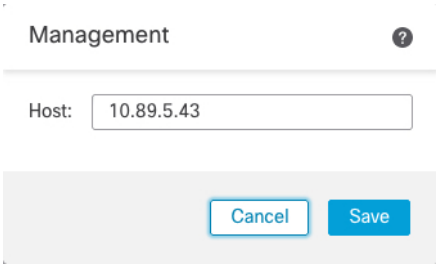
Disabling management blocks the connection between the Firewall Management Center and the device, but does **not** delete the device from the Firewall Management Center.

Step 5 Edit the **Host** IP address or hostname by clicking **Edit** ( ).



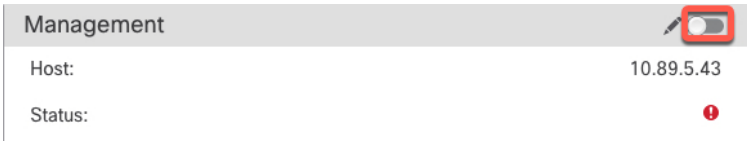
Step 6 In the **Management** dialog box, modify the name or IP address in the **Host** field. Click **Save**.

Figure 13: Management IP address



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

Figure 14: Enable management connection



Change the Firewall Management Center IP Address

This task ensures the Firewall Management Center IP address or hostname matches between the management center and device CLI, maintaining consistent configurations and network resiliency.

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.

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 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.

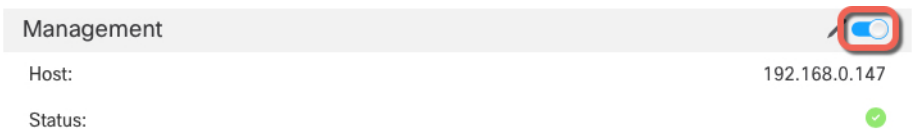
For a high-availability pair or cluster, perform these steps on all units.

a) Choose **Devices** > **Device Management**.

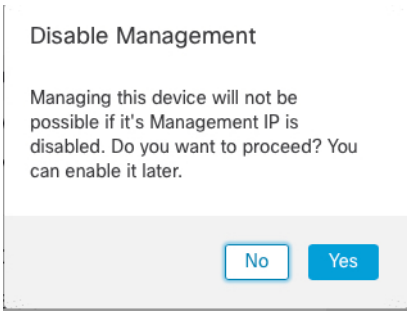
b) Next to the device, click **Edit** ( ).

c) Click **Device**, and view the **Management** area.

d) Disable management temporarily by clicking the slider so it is disabled ( ).



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

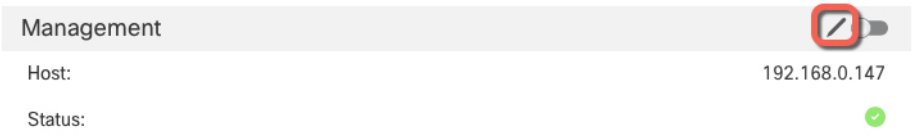


Step 2 Change the device IP address in the Firewall Management Center to the new device IP address.

You will change the IP address on the device later.

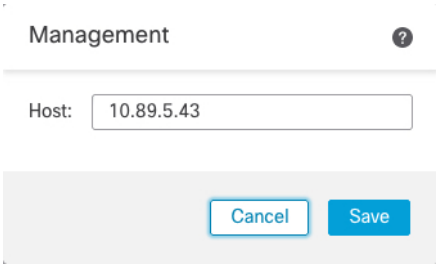
For a high-availability pair or cluster, perform these steps on all units.

a) Edit the **Host** IP address or hostname by clicking **Edit** ( ).



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

Figure 15: 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:

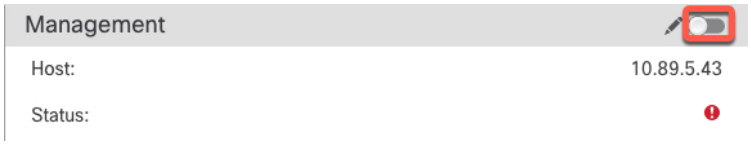
configure network management-data-interface disable

configure network management-data-interface

Step 6 Re-enable management by clicking the slider ( ).

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

Figure 16: Enable Management Connection



Step 7 (If you use 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.

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

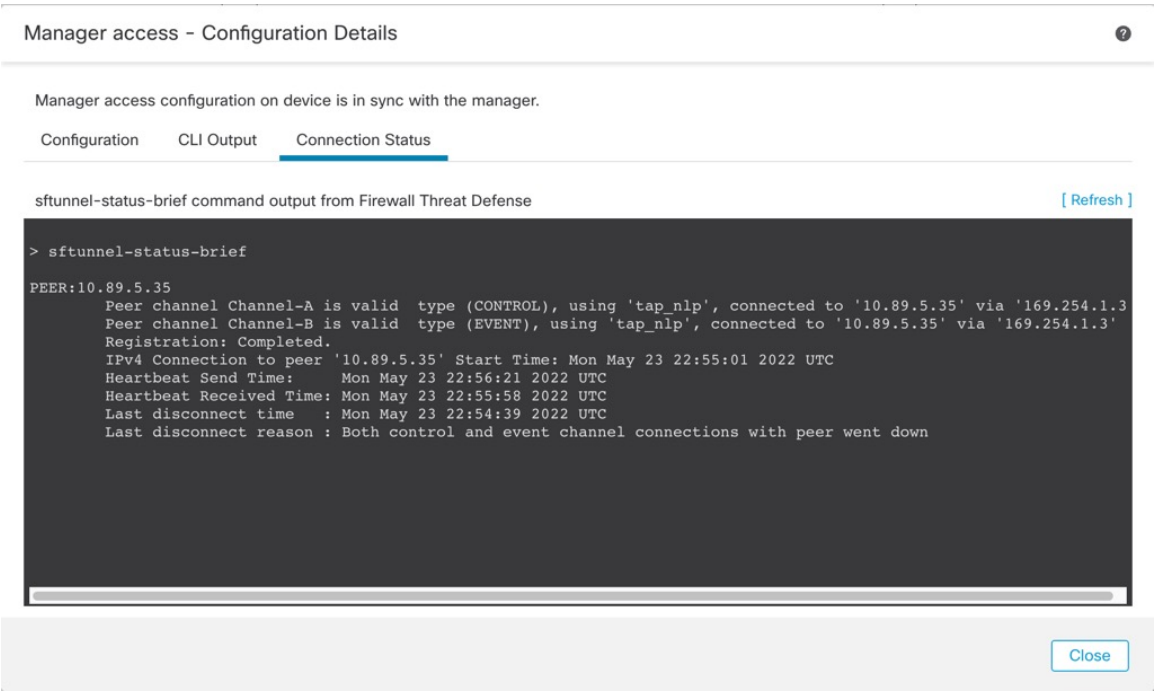
Step 8 Ensure the management connection is reestablished.

In the Firewall Management Center, check the management connection status. Navigate to the **Devices** > **Device Management**, and click **Management** section under the **Device** tab. Then, click **Manager Access - Configuration Details** to view the **Connection Status** page.

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

This status indicates a successful connection for a data interface and displays the internal "tap_nlp" interface.

Figure 17: Connection Status



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

a) Change the secondary Firewall Management Center IP address.
b) Specify the new peer addresses on both units.
c) Make the secondary unit the active unit.
d) Disable the device management connection.
e) Change the device IP address in the Firewall Management Center.
f) Re-enable 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, refer to Change the manager access interface from data to management, on page 30 .

When you initiate the manager access migration from management to data, the Firewall Management Center applies a block on deployment to the Firewall Threat Defense. To remove the block, enable manager access on the data interface.

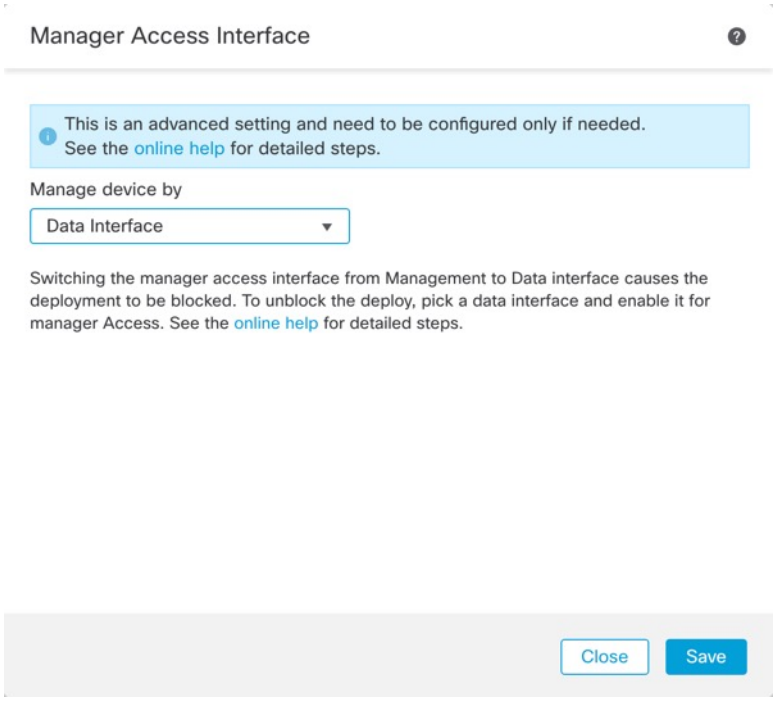
Procedure

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 **Manager Access Interface** link.

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 18: Manager Access Interface



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 19: Manager Access



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

Step 2 Enable manager access on the data interface . 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 . Make sure this interface is fully configured with a name and IP address and that it is enabled.

Step 3 (Optional) If you use DHCP for the interface, enable the web type DDNS method on the DDNS page. Navigate to **Devices** > **Device Management** , and then click **DDNS** under the **DHCP** tab.

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 the Static Route page. Navigate to **Devices** > **Device Management** and then click **Static Route** under the **Routing** tab.

See Add a static route .

Step 5 (Optional) Configure DNS in a Platform Settings policy: choose **Devices** > **Platform Settings** , and click **DNS** . Apply the policy to this device.

See Configure DNS server settings . 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** > **Device Management** page. Click **Edit** ( ) for the device and then click **SSH Access** .

See Configure Secure Shell (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; see 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 After deployment, perform these actions.

a) 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.

```
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.

b) If necessary, re-cable the Firewall Threat Defense so it can reach the Firewall Management Center on the data interface.

c) In the Firewall Management Center , disable the management connection, update the **Host** IP address for the Firewall Threat Defense in the **Devices** > **Device Management** page in the **Management** area under the **Device** tab, and reenable the connection.

Refer to Update the Hostname or IP Address in the Firewall Management Center, on page 20 . If you used the Firewall Threat Defense hostname or just the NAT ID when you added the Firewall Threat Defense to the Firewall Management Center , you don't have to update the value. To restart the connection, you must disable and re-enable the management connection.

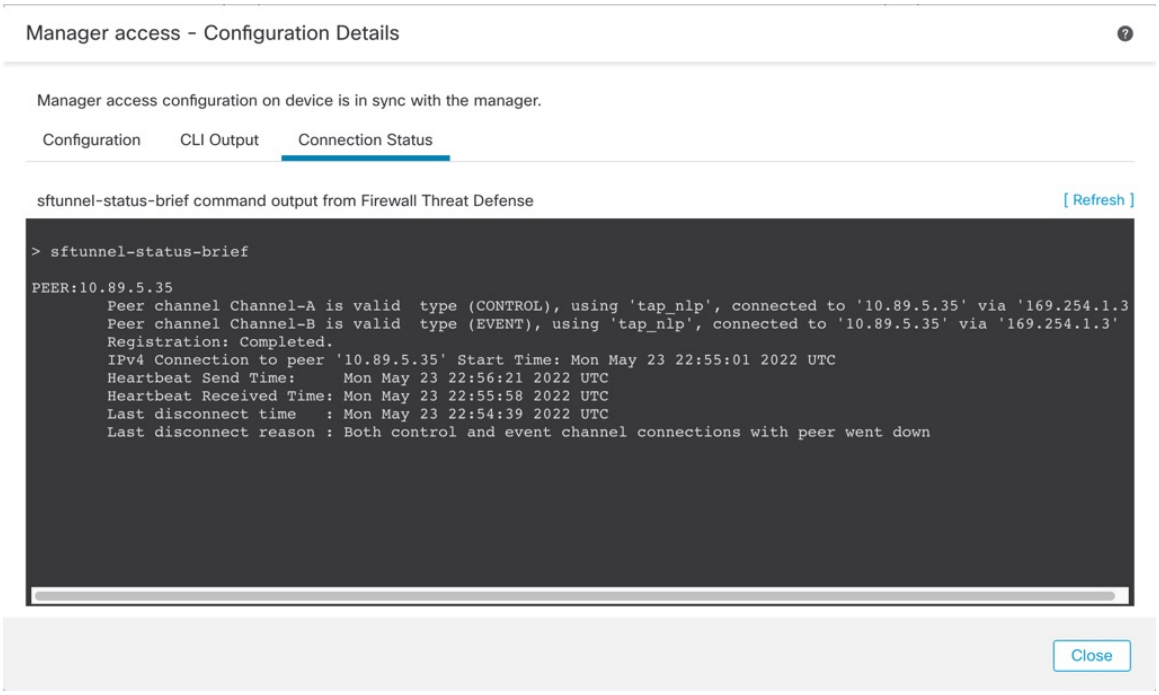
Step 9 Ensure the management connection is reestablished.

In the **Devices** > **Device Management** page, 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.

This status indicates a successful connection for a data interface, showing the internal "tap_nlp" interface.

Figure 20: 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 39 .

Change the manager access interface from data to management

This task enables you to migrate manager access from a data interface to the dedicated management interface, allowing you to manage the Firewall Threat Defense through the Management interface instead of a data interface.

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 27.

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.

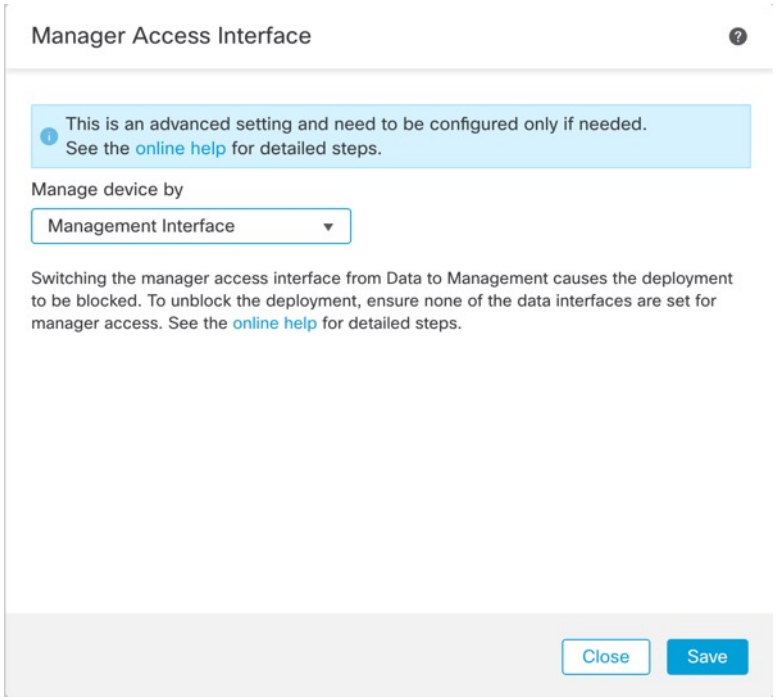
Procedure

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 21: 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 22: Manager access



Step 2 Disable manager access on the data interface. 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** > **Device Management** page. Click **Edit** (✎) for the device and then click **DNS**.

See Configure DNS server settings. 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; see 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.

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

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 Firewall Management Center, disable the management connection, update the **Host** IP address for the Firewall Threat Defense in the **Devices** > **Device Management**, **Management** section under **Device** tab, and reenable the connection.

See Update the Hostname or IP Address in the Firewall Management Center, on page 20. If you used the Firewall Threat Defense hostname or just the NAT ID when you added the Firewall Threat Defense to the Firewall Management Center, you do not need to update the value; however, you need to disable and reenable the management connection to restart 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**, **Management** section under **Device** tab, **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 39.

View manager access details for data interface management

If you use a data interface for Firewall Management Center management instead of the dedicated management interface, you must be careful about changing the interface and network settings for the device in the Firewall

Management Center to prevent disruption of the connection. When you change data interface settings locally on the device, you must reconcile them manually in the Firewall Management Center.

Use the **Devices** > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** dialog box to resolve any discrepancies between the Firewall Management Center and the Firewall Threat Defense local configuration.

Typically, you configure the manager access data interface as part of initial Firewall Threat Defense setup before you add the Firewall Threat Defense to the Firewall Management Center. When you add the Firewall Threat Defense to the Firewall Management Center, the Firewall Management Center discovers and maintains the interface configuration, which includes interface name and IP address, static route to the gateway, DNS servers, and DDNS server. The DNS server configuration is maintained locally if discovered during registration, but it is not added to the Platform Settings policy in Firewall Management Center.

After you add the Firewall Threat Defense to the Firewall Management Center, if you change the data interface settings on the Firewall Threat Defense locally using the **configure network management-data-interface** command, the Firewall Management Center detects the configuration changes and blocks deployment to the Firewall Threat Defense. The Firewall Management Center detects the configuration changes using one of these methods:

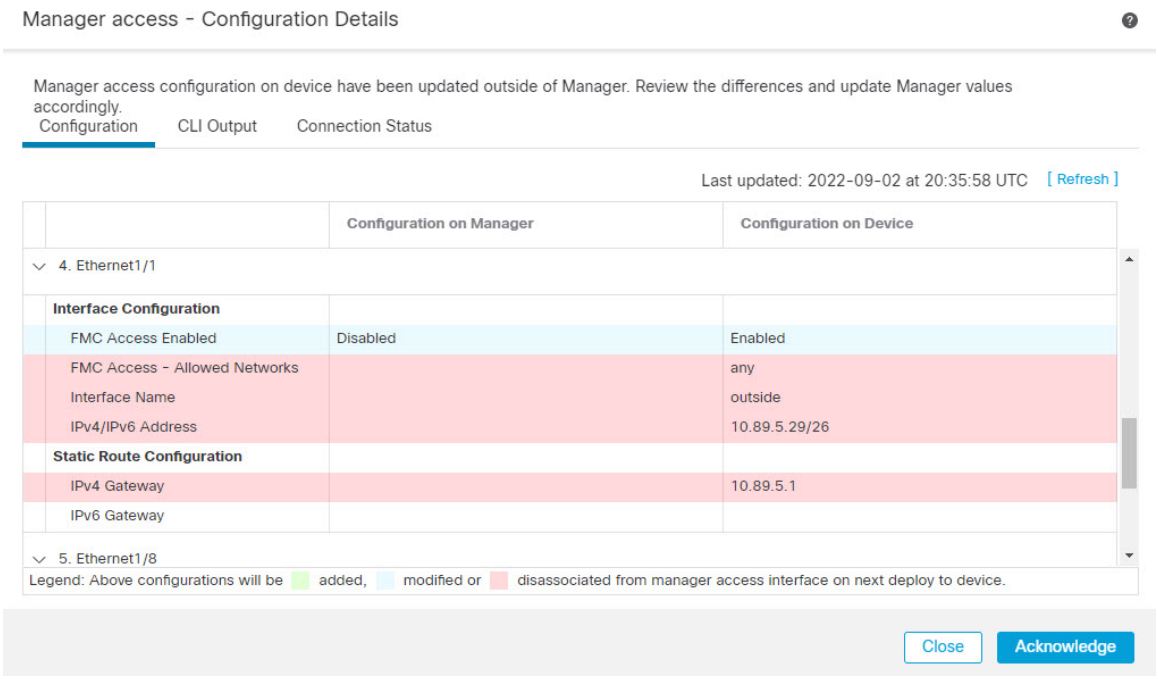
- Deploy to the Firewall Threat Defense. Before the Firewall Management Center deploys, it will detect the configuration differences and stop the deployment.
- The **Sync** button in the **Interfaces** page.
- The **Refresh** button on the **Manager Access - Configuration Details** dialog box.

To remove the block, you must go to the **Manager Access - Configuration Details** dialog box and click **Acknowledge**. 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.

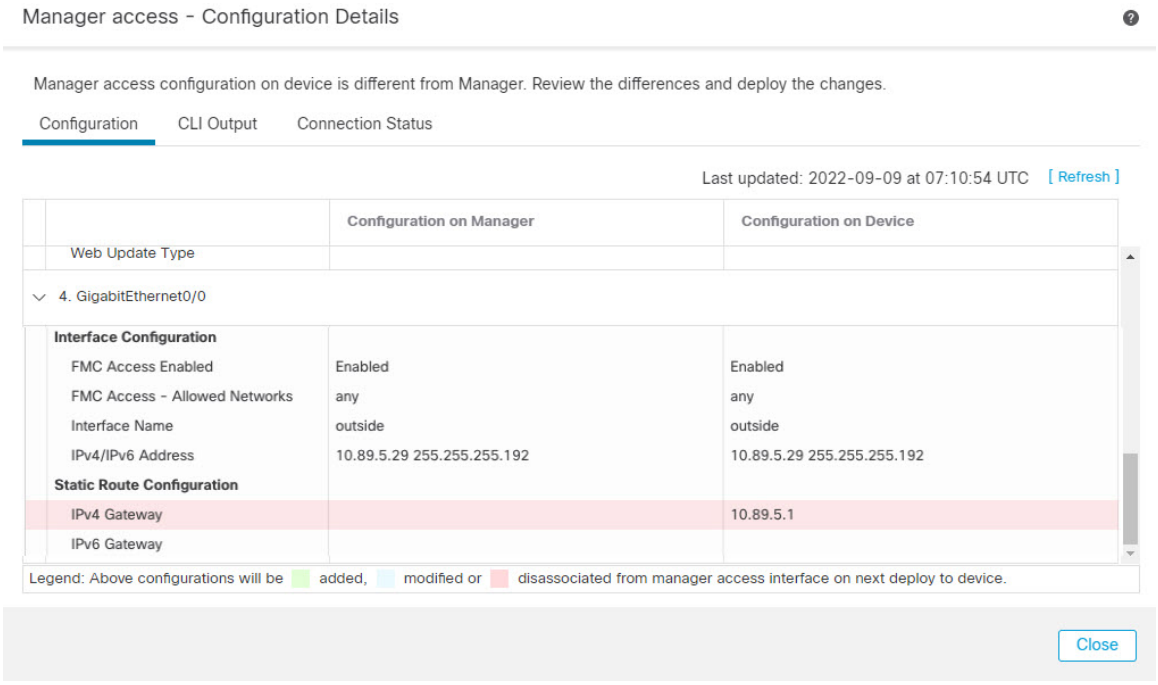
Configuration

View the configuration comparison of the manager access data interface on the Firewall Management Center and the Firewall Threat Defense.

This example shows the configuration details of the Firewall Threat Defense where the **configure network management-data-interface** command was entered on the Firewall Threat Defense. Pink highlights indicate that, if you **Acknowledge** the differences but do not match the configuration in the Firewall Management Center, then the Firewall Threat Defense configuration will be removed. Blue highlights mark configurations that will be modified on the Firewall Threat Defense. Green highlights mark configurations that will be added to the Firewall Threat Defense.



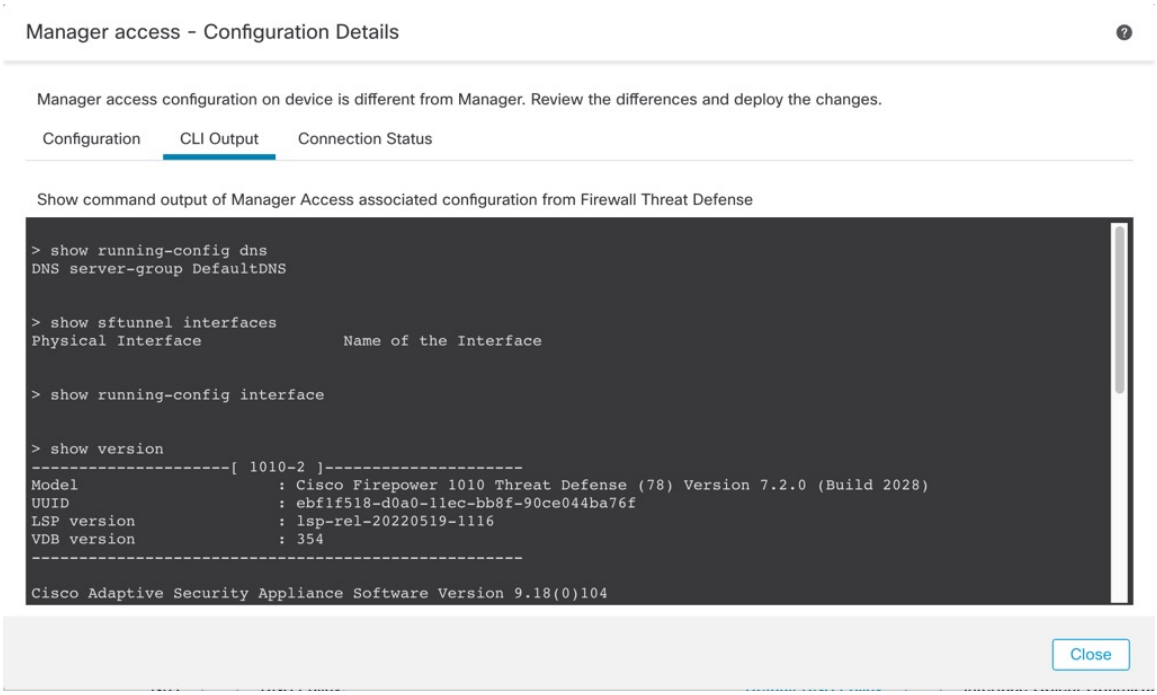
This example shows the page after configuring the interface in the Firewall Management Center. The interface settings match, and the pink highlight was removed.

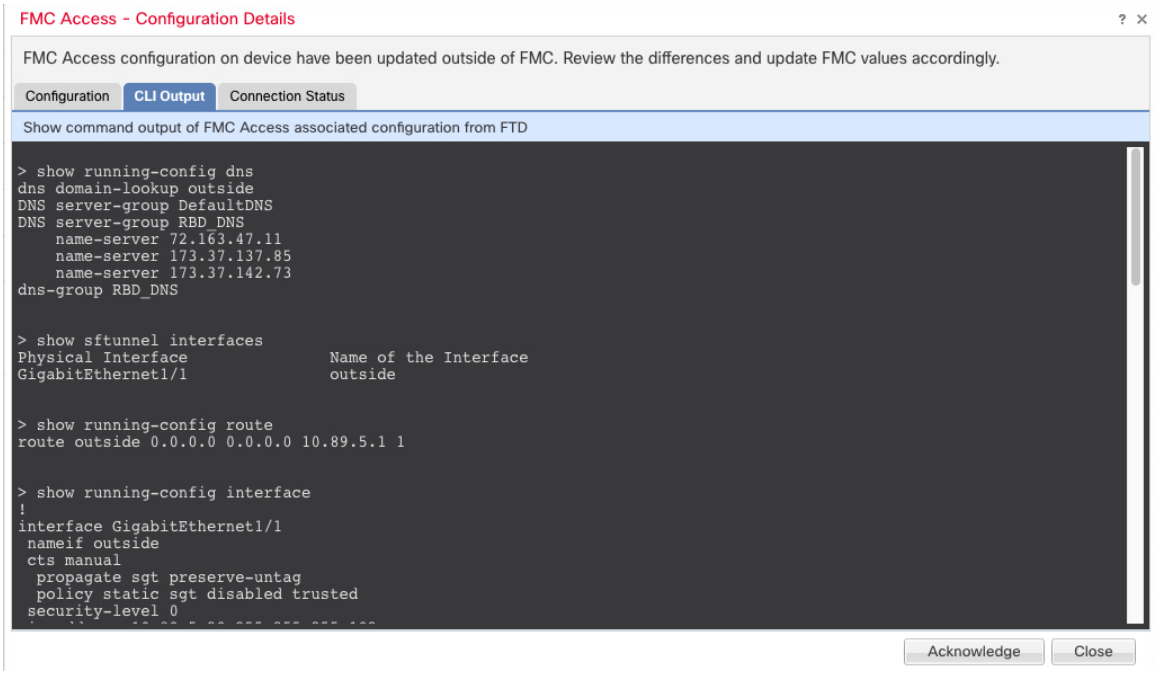


CLI output

View the CLI configuration of the manager access data interface, which is useful if you are familiar with the underlying CLI.

Figure 23: CLI output

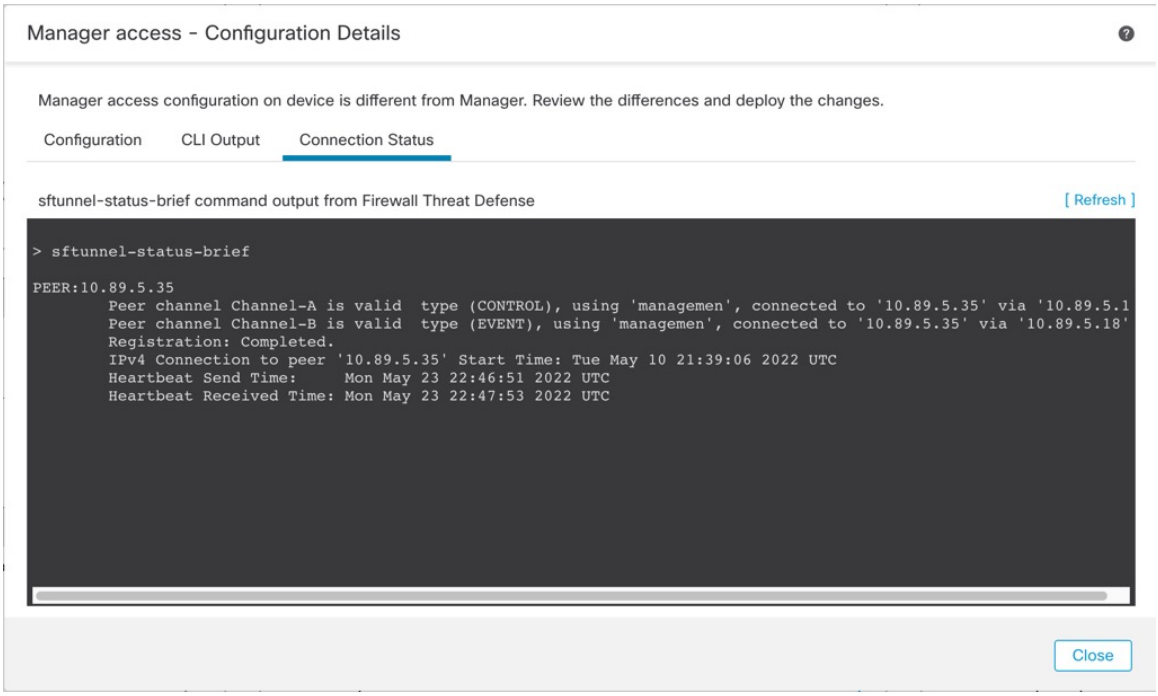




Connection status

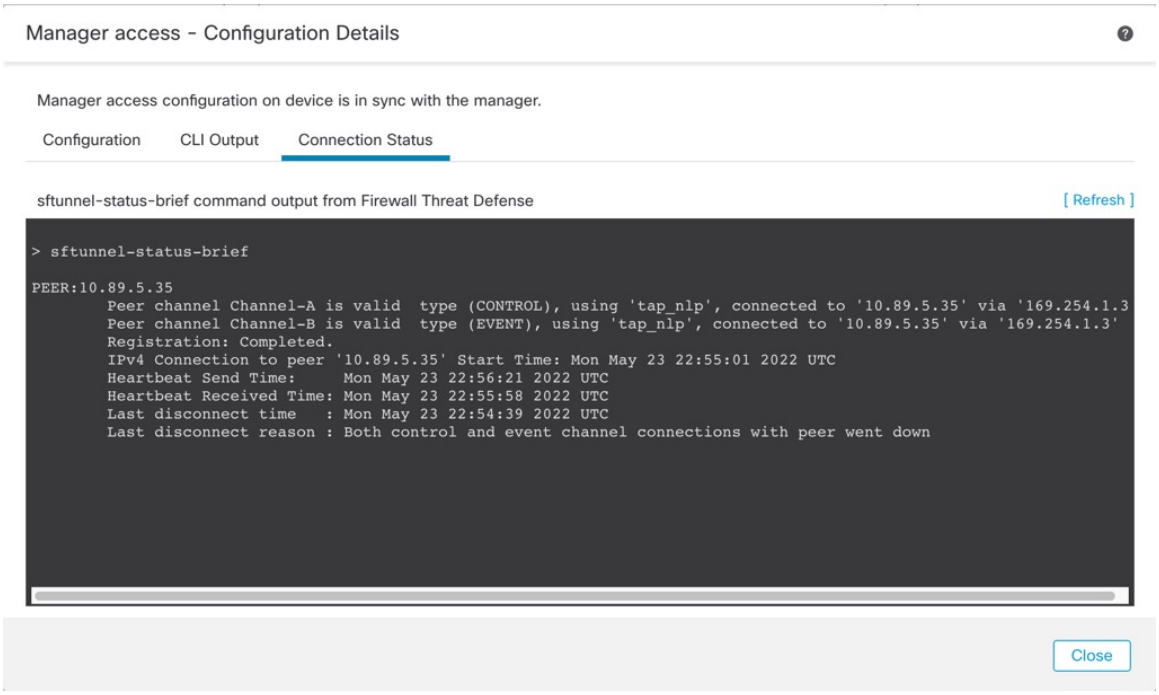
View the management connection status. In this example, the management connection still uses the Management "management0" interface.

Figure 24: Connection status



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

Figure 25: Connection status



This sample output shows a connection that is down. No peer channel "connected to" information or heartbeat information appears:

```
> 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
```

This sample output shows a connection that is up, with peer channel and heartbeat information displayed:

```
> 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
```

Troubleshoot the management connection

This reference provides information to help diagnose and resolve management connection issues.

Manually Roll Back the configuration if the Firewall Management Center loses Connectivity

Use this task to restore management connectivity when a configuration change deployed from the Firewall Management Center affects network connectivity and you need to roll back to the last-deployed configuration.

If you use a data interface on the Firewall Threat Defense for manager access and deploy a configuration change from the Firewall Management Center that affects network connectivity, you can roll back the configuration on the Firewall Threat Defense to the last-deployed configuration to restore management connectivity. Afterward, update the configuration settings in Firewall Management Center to maintain network connectivity, 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 46.

See these 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.
- 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. If you change 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 are not be preserved. They 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

After the rollback, the Firewall Threat Defense notifies the Firewall Management Center about the successful completion. The deployment screen In the Firewall Management Center displays a banner indicating that the configuration was rolled back.

Note
If the rollback fails 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 may fail after the Firewall Management Center management access is restored. Resolve any 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:
.....................
.....................
>
```

Step 2 Check that the management connection was reestablished.

In Firewall Management Center, check the management connection status on the Connection Status page. Navigate to **Devices** > **Device Management** and then navigate to **Management** area under the **Devices** tab. Then in the **Manager Access - Configuration Details** screen, click **Connection Status**.

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 39.

Troubleshoot Management Connectivity on a Data Interface

This topic helps you troubleshoot the loss of management connectivity when using a data interface for manager access instead of the dedicated Management interface.

If you use a data interface for manager access instead of the dedicated Management interface, exercise caution when changing the interface and network settings for the Firewall Threat Defense in the Firewall Management Center to avoid disrupting the connection. If you change the management interface type after adding the Firewall Threat Defense to the Firewall Management Center (switching between data and Management interfaces), misconfiguration of interfaces and network settings can result in loss of management connectivity.

Use the following methods to troubleshoot management connectivity:

- View management connection status: Check the status in the **Devices** > **Device Management** page or use **sftunnel-status-brief** at the CLI.
- View network information: Use **show network** to verify Management and manager access data interface settings.
- Check registration: Use **show managers** to confirm registration completion.
- Ping the manager: Use **ping** or **ping system** to test connectivity.
- Capture packets: Use **capture** on the `nlp_int_tap` interface to trace management traffic.
- Check interface status: Use **show interface detail** for the `nlp_int_tap` interface.
- Check routing and NAT: Use **show route** and **show nat** to verify routing and internal NAT rules.
- Check DDNS: Use **debug ddns** and related commands to verify DDNS updates.

```
> 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
```

```
> 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
...
```

Note 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.

Refer to https://cisco.com/go/fmc-reg-error for Firewall Management Center log file information.

View inventory details

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

Figure 26: Inventory details



This section shows the chassis serial number. The firewall includes two serial numbers: the chassis serial number and the PCB (circuit board) serial number. The PCB serial number is shown in the System section. The Firewall Threat Defense Virtual does not have a chassis serial number.

Note For physical Firewall Threat Defense devices, the Memory field in **Inventory Details** shows only the data plane memory, not the total system memory.

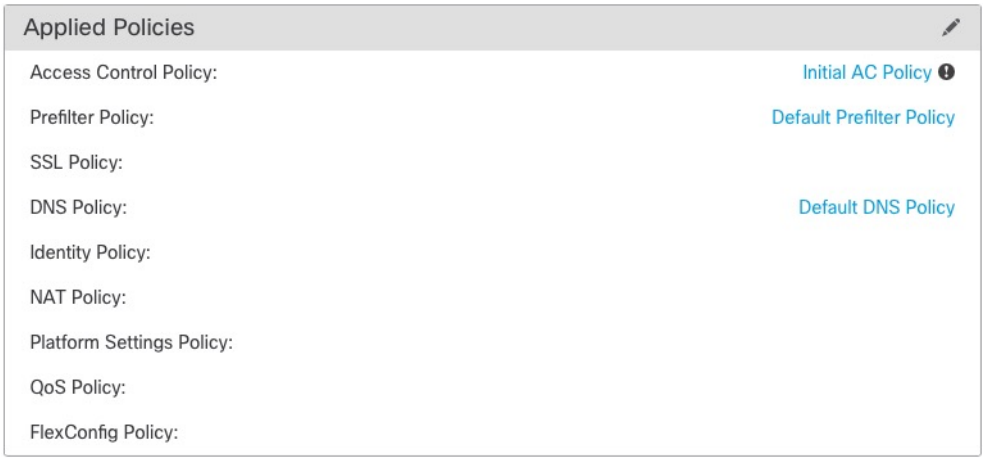
To update information, click **Refresh** ( ).

Edit applied policies

This task allows you to assign or modify policies for an individual firewall device, including access control policies and other security policies that govern device behavior.

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

Figure 27: 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 28: Access policy information for troubleshooting



Procedure

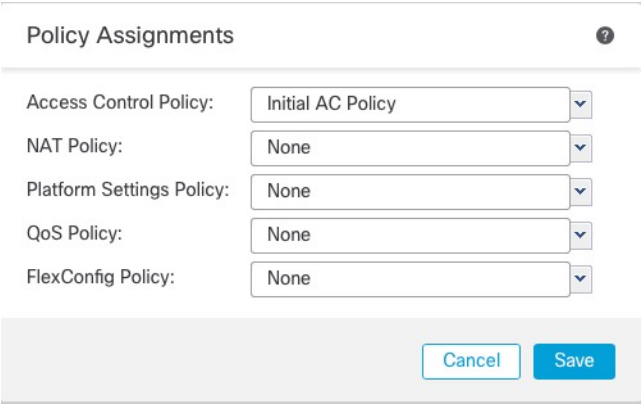
Step 1 Choose **Devices** > **Device Management**.

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 29: Policy assignments



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

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see 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 settings 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	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. **Note** By default, the **Object Group Search** is enabled when you add threat defense for the first time in the management center.
Interface Object Optimization	The state of interface object optimization on the device. During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source/destination interface pair. If you enable interface object optimization, the system will instead deploy a single rule per access control/prefilter rule, which can simplify the device configuration and improve deployment performance. If you select this option, also select the **Object Group Search** option to reduce memory usage on the device.

These 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) enables packet processing to continue when Snort detection becomes unavailable or exceeds processing time limits. This feature ensures network traffic flow continuity while providing diagnostic information for troubleshooting detection engine failures.

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. Refer to Snort restart traffic behavior.

Note 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 these steps:

Procedure

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

Step 2 Next to the device where you want to edit advanced device settings, click **Edit** ( ).

Step 3 Click **Device**, then click **Edit** ( ) in the **Advanced Settings** section.

Step 4 Check **Automatic Application Bypass**.

Step 5 Enter a **Bypass Threshold** from 250 ms to 60,000 ms. The default setting is 3000 milliseconds (ms).

Step 6 Click **Save**.

What to do next

- Deploy configuration changes; see Deploy configuration changes.

Configure object group search

This task enables object group search on a Firewall Threat Defense device to reduce memory requirements for access control policies that include network or interface objects.

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 a 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, do not disable the object group search after you have enabled it.

Before you begin

- Model support—Firewall 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.

Follow these steps to configure object group search:

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 that 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

Interface object optimization enables the system to deploy a single rule per access control/prefilter rule instead of generating separate rules for each source/destination interface pair, simplifying device configuration and improving deployment performance.

During deployment, interface groups and security zones used in the access control and prefilter policies generate separate rules for each source and destination interface pair. Enabling interface object optimization deploys a single rule per access control or prefilter rule. This approach simplifies device configuration and can improve deployment performance. If you select this option, also select the **Object Group Search** option to reduce evice memory usage.

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, the system deploys existing access control rules without using interface objects. This process might take longer. If object group search is enabled, its benefits do not apply to interface objects, and the device's running configuration might show expanded access control rules. If this expansion requires more memory than is available, the device can become inconsistent, which may affect performance

Before you begin

Model support—Firewall 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 Under the **Device** tab, click **Edit** ( ) in the **Advanced Settings** section.

Step 4 Check **Interface Object Optimization**.

Step 5 Click **Save**.

Edit deployment settings

Configure the deployment settings to enable auto rollback of the deployment if the management connection fails as a result of the deployment. For example, if you use data for management center access and then you misconfigure the data interface.

The **Deployment Settings** section of the **Device** page displays information for managing automatic rollback configuration. As an alternative, you can 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 37).

Figure 30: Deployment settings



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.

Consider 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.
- 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. If you change 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 are not be preserved. They 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

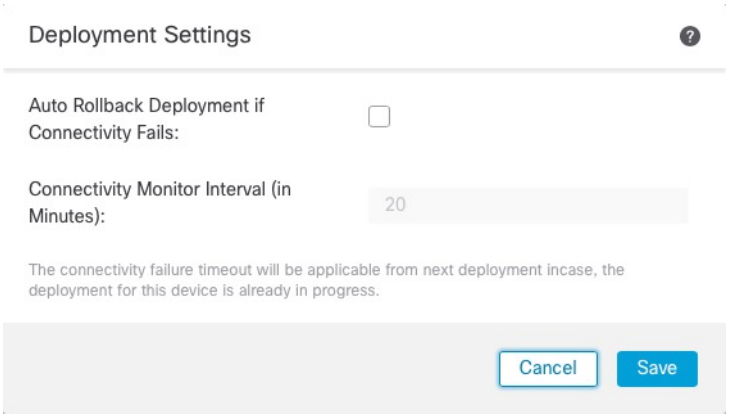
Step 1 Choose **Devices** > **Device Management**.

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 31: Deployment settings



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

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

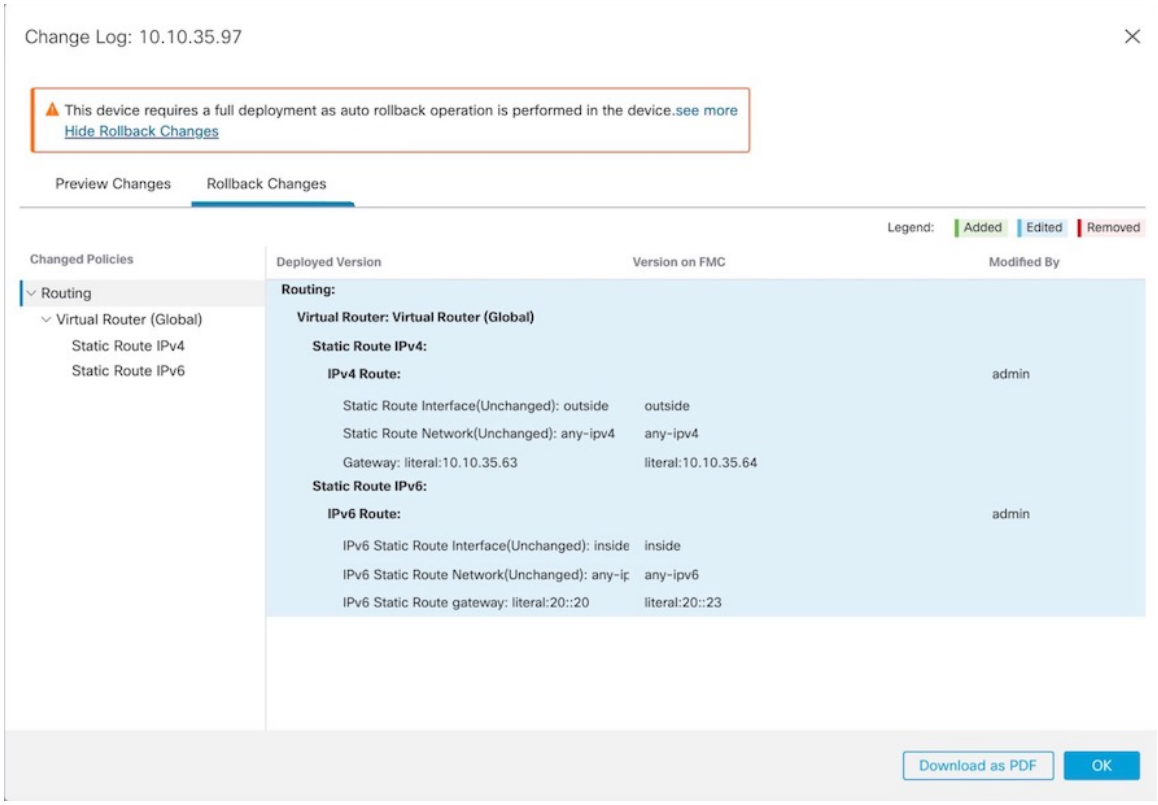
Step 7 If a rollback occurs, consider these next steps.

- If the auto rollback was successful, you see a success message instructing you to do a full deployment.
- Go to **Deploy** > **Advanced Deploy** page and click the **Preview** ( ) icon to view the parts of the configuration that were rolled back (see Deploy configuration changes).

  To view the changes, click **Show Rollback Changes**.

  To hide the changes, click **Hide Rollback Changes**.

Figure 32: Rollback changes



- In the Deployment History Preview, you can view the rollback changes. See View deployment history.

Step 8 Verify that the management connection was reestablished.

a. In Firewall Management Center, check the management connection status on the connection status page.

b. Navigate to **Devices** > **Device Management** and then in **Management** area under the **Devices** tab, click **Connection Status** to view the **Connection Status** page.

c. 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, troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 39.

Hot swap an SSD

Hot swapping SSDs allows you to maintain system operation while replacing faulty drives, removing drives, or adding drives to form a RAID configuration.

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

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

  When you use only one SSD in Secure Firewall devices, the **Drive State** will show as **degraded**.



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

Procedure

Step 1 Remove one of the SSDs.

a) Remove the SSD from the RAID.

configure RAID remove-secure local-disk {**1** | **2**}

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

Example:

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

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

show RAID

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

Example:

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

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

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

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

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

c) Physically remove the SSD from the chassis.

Step 2 Add an SSD.

a) Physically add the SSD to the empty slot.

b) Add the SSD to the RAID.

configure RAID add local-disk {**1** | **2**}

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

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

configure RAID add local-disk {**1** | **2**} *psid*

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

Configure SNMP for FXOS

You can configure the Simple Network Management Protocol (SNMP) for the underlying FXOS operating system that controls low-level chassis functions. For SNMP for the Firewall Threat Defense, see Configure SNMP for a security device.

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. SNMP provides a standardized framework and a common language used for the monitoring and management of devices in a network.

The SNMP framework consists of three parts:

- An SNMP manager—The system used to control and monitor the activities of network devices using SNMP.
- An SNMP agent—The software component within the chassis that maintains the data for the chassis and reports the data, as needed, to the SNMP manager. The chassis includes the agent and a collection of MIBs. To enable the SNMP agent and create the relationship between the manager and agent, enable and configure SNMP in the Firewall Management Center.
- A managed information base (MIB)—The collection of managed objects on the SNMP agent.

The chassis supports SNMPv1, SNMPv2c and SNMPv3. Both SNMPv1 and SNMPv2c use a community-based form of security. SNMPv3 uses username and password for security.

Enable SNMP for FXOS

Enable SNMP and configure settings.

Procedure

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

Step 2 Click **SNMP**.

Step 3 Complete the following fields:

Name	Description
Admin State check box	Whether SNMP is enabled or disabled. Enable this service only if your system includes integration with an SNMP server.
Port field	The port on which the Firepower chassis communicates with the SNMP host. You cannot change the default port.

Name	Description
Community field	The default SNMPv1 or v2 community name or SNMP v3 username and password that the Firepower chassis includes on any trap messages it sends to the SNMP host. Enter a valid community string for SNMPv1 and SNMPv2: • Alphanumeric string between 1 and 32 characters and special characters ! (exclamation), - (hyphen), ~ (tilde), && (double ampersand), [ ] (square brackets), ^ (carat), ' (single quote), " (double quotes), and < > (angle brackets). • Do not use @ (at sign), \ (backslash), ? (question mark) or an empty space. • The string can also be in ASCII characters ranging 0x21 to 0x7E inclusive, excluding HTML interjection vectors, namely single quote ('), double quotes ("), and angle brackets (< >). Enter a valid username and password for SNMPv3: • Username can be alphanumeric string and can include @ (at sign), \ (backslash), . (period), _ (underscore), and - (hyphen). • The password restrictions are same as the community string restrictions. Note that if the **Community** field is already set, the text to the right of the empty field reads **Set: Yes**. If the **Community** field is not yet populated with a value, the text to the right of the empty field reads **Set: No**.
System Admin Name field	The contact person responsible for the SNMP implementation. Enter a string of up to 255 characters, such as an email address or a name and telephone number.
Location field	The location of the host on which the SNMP agent (server) runs. Enter an alphanumeric string up to 510 characters.

Step 4 Click **Save**.

What to do next

Create SNMP traps and users.

Create an SNMP Trap for FXOS

Create traps for SNMP.

Procedure

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

Step 2 Click **SNMP**.

Step 3 In the **SNMP Traps Configuration** area, click **Add**.

Step 4 In the **SNMP Trap Configuration** dialog box, complete the following fields:

Name	Description
Host Name field	The hostname or IP address of the SNMP host to which the Firepower chassis should send the trap.
Community field	The SNMP v1 or v2 community name or the SNMP v3 username the Firepower chassis includes when it sends the trap to the SNMP host. This must be the same as the community or username that is configured for the SNMP service. Enter an alphanumeric string between 1 and 32 characters. Do not use @ (at sign), \ (backslash), " (double quote), ? (question mark) or an empty space.
Port field	The port on which the Firepower chassis communicates with the SNMP host for the trap. Enter an integer between 1 and 65535.
Version field	The SNMP version and model used for the trap. This can be one of the following: • **V1** • **V2** • **V3**
Type field	If you select **V2** or **V3** for the version, the type of trap to send. This can be one of the following: • **Traps** • **Informs**
Privilege field	If you select **V3** for the version, the privilege associated with the trap. This can be one of the following: • **Auth**—Authentication but no encryption • **Noauth**—No authentication or encryption • **Priv**—Authentication and encryption

Step 5 Click **OK** to close the **SNMP Trap Configuration** dialog box.

Step 6 Click **Save**.

Create an SNMP user for FXOS

Create SNMP users.

Procedure

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

Step 2 Click **SNMP**.

Step 3 In the **SNMP Users Configuration** area, click **Add**.

Step 4 In the **SNMP User Configuration** dialog box, complete the following fields:

Name	Description
Username field	The username assigned to the SNMP user. Enter up to 32 letters or numbers. The name must begin with a letter and you can also specify _ (underscore), . (period), @ (at sign), and - (hyphen).
Auth Algorithm Type field	The authorization type: **SHA**.
Use AES-128 checkbox	If checked, this user uses AES-128 encryption. **Note** SNMPv3 does not support DES. If you leave the AES-128 box unchecked, no privacy encryption will be done and any configured privacy password will have no effect.
Authentication Password field	The password for the user.
Confirm field	The password again for confirmation purposes.
Encryption Password field	The privacy password for the user.
Confirm field	The privacy password again for confirmation purposes.

Step 5 Click **OK** to close the **SNMP User Configuration** dialog box.

Step 6 Click **Save**.

Configure alarms for the ISA 3000

You can configure the alarm system on a Cisco ISA 3000 device to alert you when undesirable conditions occur.

About alarms

You can configure the ISA 3000 to issue alarms for a variety of conditions. If any conditions do not match the configured settings, the system triggers an alarm, which is reported by way of LEDs, syslog messages, SNMP traps, and through external devices connected to the alarm output interface. By default, triggered alarms issue syslog messages only.

You can configure the alarm system to monitor the following:

- Power supply.
- Primary and secondary temperature sensors.
- Alarm input interfaces.

The ISA 3000 has internal sensors plus two alarm input interfaces and one alarm output interface. You can connect external sensors, such as door sensors, to the alarm inputs. You can connect external alarm devices, such as buzzers or lights, to the alarm output interface.

The alarm output interface is a relay mechanism. Depending on the alarm conditions, the relay is either energized or de-energized. When it is energized, any device connected to the interface is activated. A de-energized relay results in the inactive state of any connected devices. The relay remains in an energized state as long as alarms are triggered.

For information about connecting external sensors and the alarm relay, Refer to Alarms for the Cisco ISA 3000 chapter in Cisco ASA Series General Operations CLI Configuration Guide. see Cisco ISA 3000 Industrial Security Appliance Hardware Installation Guide.

Alarm input interfaces

You can connect the alarm input interfaces (or contacts) to external sensors, such as one that detects if a door is open.

Each alarm input interface has a corresponding LED. These LEDs convey the alarm status of each alarm input. You can configure the trigger and severity for each alarm input. In addition to the LED, you can configure the contact to trigger the output relay (to activate an external alarm), to send syslog messages, and to send SNMP traps.

The following table explains the statuses of the LEDs in response to alarm conditions for the alarm inputs. It also explains the behavior for the output relay, syslog messages, and SNMP traps, if you enable these responses to the alarm input.

Alarm Status	LED	Output Relay	Syslog	SNMP Trap
Alarm not configured	Off	—	—	—
No alarms triggered	Solid green	—	—	—
Alarm activated	Minor alarm—solid red Major alarm—flashing red	Relay energized	Syslog generated	SNMP trap sent
Alarm end	Solid green	Relay de-energized	Syslog generated	—

Alarm output interface

You can connect an external alarm, such as a buzzer or light, to the alarm output interface.

The alarm output interface functions as a relay and also has a corresponding LED, which conveys the alarm status of an external sensor connected to the input interface, and internal sensors such as the dual power supply and temperature sensors. You configure which alarms should activate the output relay, if any.

The following table explains the statuses of the LEDs and output relay in response to alarm conditions. It also explains the behavior for syslog messages, and SNMP traps, if you enable these responses to the alarm.

Alarm Status	LED	Output Relay	Syslog	SNMP Trap
Alarm not configured	Off	—	—	—
No alarms triggered	Solid green	—	—	—
Alarm activated	Solid red	Relay energized	Syslog generated	SNMP trap sent
Alarm end	Solid green	Relay de-energized	Syslog generated	—

Syslog alarms

By default, the system sends syslog messages when any alarm is triggered. You can disable syslog messaging if you do not want the messages.

For syslog alarms to work, you must also enable diagnostic logging. Choose **Devices** > **Platform Settings**, add or edit a Threat Defense platform settings policy that is assigned to the device, and configure destinations and settings on the **Syslog** page. For example, you can configure a syslog server, console logging, or internal buffer logging.

Without enabling a destination for diagnostic logging, the alarm system has nowhere to send syslog messages.

SNMP Alarms

You can optionally configure the alarms to send SNMP traps to your SNMP server. For SNMP trap alarms to work, you must also configure SNMP settings.

Choose **Devices** > **Platform Settings**, add or edit a Threat Defense platform settings policy that is assigned to the device, and enable SNMP and configure settings on the **SNMP** page.

Defaults for alarms

The following table specifies the defaults for alarm input interfaces (contacts), redundant power supply, and temperature.

	Alarm	Trigger	Severity	SNMP Trap	Output Relay	Syslog Message
Alarm Contact 1	Enabled	Closed State	Minor	Disabled	Disabled	Enabled
Alarm Contact 2	Enabled	Closed State	Minor	Disabled	Disabled	Enabled

	Alarm	Trigger	Severity	SNMP Trap	Output Relay	Syslog Message
Redundant Power Supply (when enabled)	Enabled	—	—	Disabled	Disabled	Enabled
Temperature	Enabled for the primary temperature alarm (default values of 92°C and -40°C for the high and low thresholds respectively) Disabled for the secondary alarm.	—	—	Enabled for primary temperature alarm	Enabled for primary temperature alarm	Enabled for primary temperature alarm

Prerequisites for alarms

Model support

Firewall Threat Defense on the ISA 3000.

Configure alarms for the ISA 3000

You use FlexConfig to configure alarms for the ISA 3000. The following topics explain how to configure the different types of alarms.

Configure alarm input contacts

If you connect the alarm input contacts (interfaces) to external sensors, you can configure the contacts to issue alarms based on the input from the sensor. In fact, the contacts are enabled by default to send syslog messages if the contact is closed, that is, if the electrical current stops flowing through the contact. You need to configure the contact only if the defaults do not meet your requirements.

The alarm contacts are numbered 1 and 2, so you need to understand how you have wired the physical pins to configure the correct settings. You configure the contacts separately.

Procedure

Step 1 Create the FlexConfig object to configure the alarm input contacts.

a) Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

b) Click **Add FlexConfig Object**, configure the following properties, and click **Save**.

- **Name**—The object name. For example, Configure_Alarm_Contacts.

- **Deployment**—Select **Everytime**. You want this configuration to be sent in every deployment to ensure it remains configured.
- **Type**—Keep the default, **Append**. The commands are sent to the device after the commands for directly-supported features.
- **Object body**—In the object body, type the commands needed to configure the alarm contacts. The following steps explain the commands.

c) Configure a description for the alarm contact.

alarm contact {**1** | **2**} **description** *string*

For example, to set the description of contact 1 to "Door Open," enter the following:

```
alarm contact 1 description Door Open
```

d) Configure the severity for the alarm contact.

alarm contact {**1** | **2** | **any**} **severity** {**major** | **minor** | **none**}

Instead of configuring one contact, you can specify **any** to change the severity for all contacts. The severity controls the behavior of the LED associated with the contact.

- **major**—The LED blinks red.
- **minor**—The LED is solid red. This is the default.
- **none**—The LED is off.

For example, to set the severity of contact 1 to Major, enter the following:

```
alarm contact 1 severity major
```

e) Configure the trigger for the alarm contact.

alarm contact {**1** | **2** | **any**} **trigger** {**open** | **closed**}

Instead of configuring one contact, you can specify **any** to change the trigger for all contacts. The trigger determines the electrical condition that signals an alert.

- **open**—The normal condition for the contact is closed, that is, the electrical current is running through the contact. An alert is triggered if the contact becomes open, that is, the electrical current stops flowing.
- **closed**—The normal condition for the contact is open, that is, the electrical current does not run through the contact. An alert is triggered if the contact becomes closed, that is, the electrical current starts running through the contact. This is the default.

For example, you connect a door sensor to alarm input contact 1, and its normal state has no electrical current flowing through the alarm contact (it is open). If the door is opened, the contact is closed and electrical current flows through the alarm contact. You would set the alarm trigger to closed so that the alarm goes off when the electrical current starts flowing.

```
alarm contact 1 trigger closed
```

f) Configure the actions to take when the alarm contact is triggered.

alarm facility input-alarm {**1** | **2**} {**relay** | **syslog** | **notifies**}

You can configure more than one action. For example, you can configure the device to activate the external alarm, send syslog messages, and also send SNMP traps.

- **relay**—Energize the alarm output relay, which activates the external alarm that you attached to it, such as a buzzer or a flashing light. The output LED also goes red.
- **syslog**—Send a syslog message. This option is enabled by default.
- **notifies**—Send an SNMP trap.

For example, to enable all actions for the alarm input contact 1, enter the following:

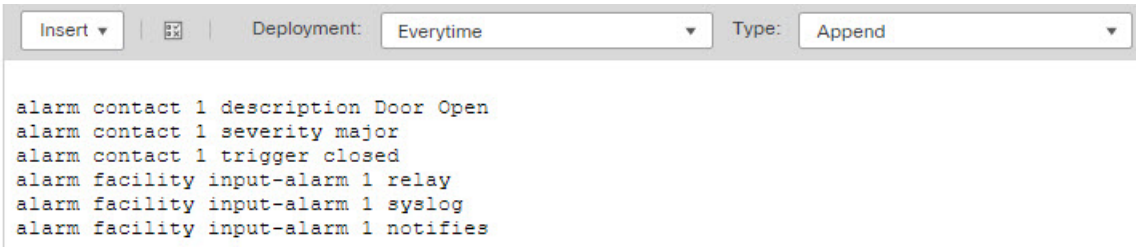
```
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

g) Verify that the object body contains the commands you want.

For example, if your template includes all of the command examples shown in this procedure, the object body would have the following commands:

```
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

The object body should look similar to the following:



h) Click **Save**.

Step 2 Create the FlexConfig policy and assign it to the devices.

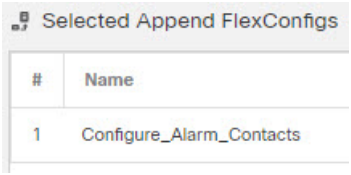
a) Choose **Devices** > **FlexConfig**.

b) Either click **New Policy**, or if an existing FlexConfig policy should be assigned to (or is already assigned to) the target devices, simply edit that policy.

When creating a new policy, assign the target devices to the policy in the dialog box where you name the policy.

c) Select the alarm contact FlexConfig object in the **User Defined** folder in the table of contents and click > to add it to the policy.

The object should be added to the **Selected Appended FlexConfigs** list.



d) Click **Save**.

e) If you have not yet assigned all the targeted devices to the policy, click the **Policy Assignments** link below Save and make the assignments now.

f) Click **Preview Config**, and in the Preview dialog box, select one of the assigned devices.

The system generates a preview of the configuration CLI that will be sent to the device. Verify that the commands generated from the FlexConfig object look correct. These will be shown at the end of the preview. Note that you will also see commands generated from other changes you have made to managed features. For the alarm contact commands, you should see something similar to the following:

```
###Flex-config Appended CLI ###
alarm contact 1 description Door Open
alarm contact 1 severity major
alarm contact 1 trigger closed
alarm facility input-alarm 1 relay
alarm facility input-alarm 1 syslog
alarm facility input-alarm 1 notifies
```

Step 3 Deploy your changes.

Because you assigned a FlexConfig policy to the devices, you will always get a deployment warning, which is meant to caution you about the use of FlexConfig. Click **Proceed** to continue with the deployment.

After the deployment completes, you can check the deployment history and view the transcript for the deployment. This is especially valuable if the deployment fails. See Verify the deployed configuration.

Configure power supply alarms

The ISA 3000 has two power supplies. By default, the system operates in single-power mode. However, you can configure the system to operate in dual mode, where the second power supply automatically provides power if the primary power supply fails. When you enable dual-mode, the power supply alarm is automatically enabled to send syslog alerts, but you can disable the alert altogether, or also enable SNMP traps or the alarm hardware relay.

The following procedure explains how to enable dual mode, and how to configure the power supply alarms.

Procedure

Step 1 Create the FlexConfig object to configure the power supply alarm.

a) Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

b) Click **Add FlexConfig Object**, configure the following properties, and click **Save**.

- **Name**—The object name. For example, Power_Supply_Alarms.

- **Deployment**—Select **Everytime**. You want this configuration to be sent in every deployment to ensure it remains configured.
- **Type**—Keep the default, **Append**. The commands are sent to the device after the commands for directly-supported features.
- **Object body**—In the object body, type the commands needed to configure the power supply alarms. The following steps explain the commands.

c) Enable dual power supply mode.

power-supply dual

For example:

```
power-supply dual
```

d) Configure the actions to take when the power supply alarm is triggered.

alarm facility power-supply rps {**relay** | **syslog** | **notifies** | **disable**}

You can configure more than one action. For example, you can configure the device to activate the external alarm, send syslog messages, and also send SNMP traps.

- **relay**—Energize the alarm output relay, which activates the external alarm that you attached to it, such as a buzzer or a flashing light. The output LED also goes red.
- **syslog**—Send a syslog message. This option is enabled by default.
- **notifies**—Send an SNMP trap.
- **disable**—Disable the power supply alarm. Any other actions configured for the power supply alarm are inoperable.

For example, to enable all actions for the power supply alarm, enter the following:

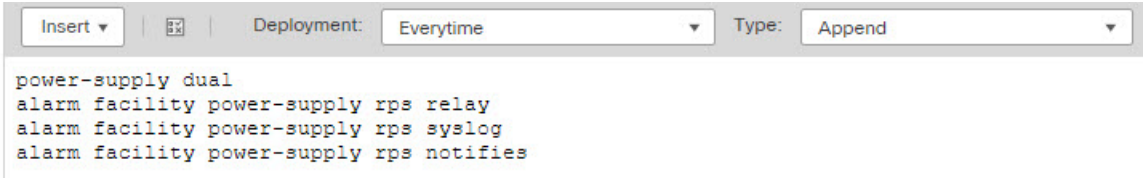
```
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

e) Verify that the object body contains the commands you want.

For example, if your template includes all of the command examples shown in this procedure, the object body would have the following commands:

```
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

The object body should look similar to the following:



f) Click **Save**.

Step 2 Create the FlexConfig policy and assign it to the devices.

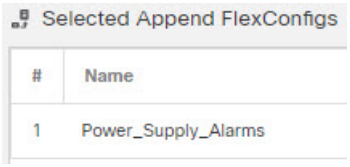
a) Choose **Devices** > **FlexConfig**.

b) Either click **New Policy**, or if an existing FlexConfig policy should be assigned to (or is already assigned to) the target devices, simply edit that policy.

When creating a new policy, assign the target devices to the policy in the dialog box where you name the policy.

c) Select the power supply alarm FlexConfig object in the **User Defined** folder in the table of contents and click > to add it to the policy.

The object should be added to the **Selected Appended FlexConfigs** list.



d) Click **Save**.

e) If you have not yet assigned all the targeted devices to the policy, click the **Policy Assignments** link below Save and make the assignments now.

f) Click **Preview Config**, and in the Preview dialog box, select one of the assigned devices.

The system generates a preview of the configuration CLI that will be sent to the device. Verify that the commands generated from the FlexConfig object look correct. These will be shown at the end of the preview. Note that you will also see commands generated from other changes you have made to managed features. For the power supply alarm commands, you should see something similar to the following:

```
###Flex-config Appended CLI ###
power-supply dual
alarm facility power-supply rps relay
alarm facility power-supply rps syslog
alarm facility power-supply rps notifies
```

Step 3 Deploy your changes.

Because you assigned a FlexConfig policy to the devices, you will always get a deployment warning, which is meant to caution you about the use of FlexConfig. Click **Proceed** to continue with the deployment.

After the deployment completes, you can check the deployment history and view the transcript for the deployment. This is especially valuable if the deployment fails. See Verify the deployed configuration.

Configure temperature alarms

You can configure alarms based on the temperature of the CPU card in the device.

You can set a primary and secondary temperature range. If the temperature drops below the low threshold, or exceeds the high threshold, the alarm is triggered.

The primary temperature alarm is enabled by default for all alarm actions: output relay, syslog, and SNMP. The default settings for the primary temperature range is -40°C to 92°C.

The secondary temperature alarm is disabled by default. You can set the secondary temperature within the range -35°C to 85°C.

Because the secondary temperature range is more restrictive than the primary range, if you set either the secondary low or high temperature, that setting disables the corresponding primary setting, even if you configure non-default values for the primary setting. You cannot enable two separate high and two separate low temperature alarms.

Thus, in practice, you should configure the primary only, or the secondary only, setting for high and low.

Procedure

Step 1 Create the FlexConfig object to configure the temperature alarms.

a) Choose **Objects** > **Object Management** > **FlexConfig** > **FlexConfig Object**.

b) Click **Add FlexConfig Object**, configure the following properties, and click **Save**.

- **Name**—The object name. For example, Configure_Temperature_Alarms.
- **Deployment**—Select **Everytime**. You want this configuration to be sent in every deployment to ensure it remains configured.
- **Type**—Keep the default, **Append**. The commands are sent to the device after the commands for directly-supported features.
- **Object body**—In the object body, type the commands needed to configure the temperature alarms. The following steps explain the commands.

c) Configure the acceptable temperature range.

alarm facility temperature {**primary** | **secondary**} {**low** | **high**} *temperature*

The temperature is in Celsius. The allowed range for the primary alarm is -40 to 92, which is also the default range. The allowed range for the secondary alarm is -35 to 85. The low value must be lower than the high value.

For example, to set a more restrictive temperature range of -20 to 80, which falls within the allowed range for the secondary alarm, configure the secondary alarm as follows:

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
```

d) Configure the actions to take when the temperature alarm is triggered.

alarm facility temperature {**primary** | **secondary**} {**relay** | **syslog** | **notifies**}

You can configure more than one action. For example, you can configure the device to activate the external alarm, send syslog messages, and also send SNMP traps.

- **relay**—Energize the alarm output relay, which activates the external alarm that you attached to it, such as a buzzer or a flashing light. The output LED also goes red.
- **syslog**—Send a syslog message.
- **notifies**—Send an SNMP trap.

For example, to enable all actions for the secondary temperature alarm, enter the following:

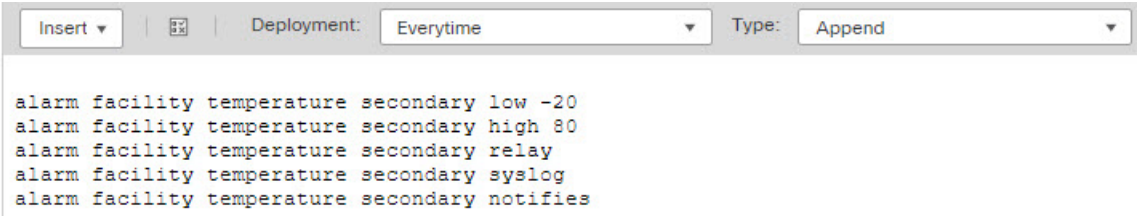
```
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

e) Verify that the object body contains the commands you want.

For example, if your template includes all of the command examples shown in this procedure, the object body would have the following commands:

```
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

The object body should look similar to the following:



f) Click **Save**.

Step 2 Create the FlexConfig policy and assign it to the devices.

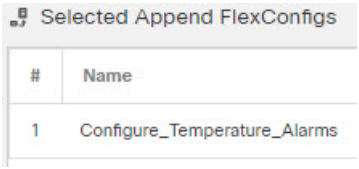
a) Choose **Devices** > **FlexConfig**.

b) Either click **New Policy**, or if an existing FlexConfig policy should be assigned to (or is already assigned to) the target devices, simply edit that policy.

When creating a new policy, assign the target devices to the policy in the dialog box where you name the policy.

c) Select the temperature alarms FlexConfig object in the **User Defined** folder in the table of contents and click > to add it to the policy.

The object should be added to the **Selected Appended FlexConfigs** list.



d) Click **Save**.

e) If you have not yet assigned all the targeted devices to the policy, click the **Policy Assignments** link below Save and make the assignments now.

f) Click **Preview Config**, and in the Preview dialog box, select one of the assigned devices.

The system generates a preview of the configuration CLI that will be sent to the device. Verify that the commands generated from the FlexConfig object look correct. These will be shown at the end of the preview. Note that you will also see commands generated from other changes you have made to managed features. For the temperature alarms commands, you should see something similar to the following:

```
###Flex-config Appended CLI ###
alarm facility temperature secondary low -20
alarm facility temperature secondary high 80
alarm facility temperature secondary relay
alarm facility temperature secondary syslog
alarm facility temperature secondary notifies
```

Step 3 Deploy your changes.

Because you assigned a FlexConfig policy to the devices, you will always get a deployment warning, which is meant to caution you about the use of FlexConfig. Click **Proceed** to continue with the deployment.

After the deployment completes, you can check the deployment history and view the transcript for the deployment. This is especially valuable if the deployment fails. See Verify the deployed configuration.

Turn off the external alarm

If you are using an external alarm that is attached to the alarm output, and the alarm is triggered, you can turn off the external alarm from the device CLI using the **clear facility-alarm output** command. This command de-energizes the output pin and also turns off the output LED.

Monitoring alarms

The following topics explain how to monitor and manage alarms.

Monitoring alarm status

You can use the following commands in the CLI to monitor alarms.

- **show alarm settings**

  Shows the current configuration for each possible alarm.

- **show environment alarm-contact**

  Shows information about the physical status of the input alarm contacts.

- **show facility-alarm relay**

  Shows information about the alarms that have triggered the output relay.

- **show facility-alarm status** [**info** | **major** | **minor**]

  Shows information on all alarms that have been triggered. You can limit the view by filtering on **major** or **minor** status. The **info** keyword provides the same output as using no keyword.

Monitoring syslog messages for alarms

Depending on the type of alarms you configure, you might see the following syslog messages.

Dual Power Supply Alarms

- %FTD-1-735005: Power Supply Unit Redundancy OK
- %FTD-1-735006: Power Supply Unit Redundancy Lost

Temperature Alarms

In these alarms, *Celsius* is replaced by the temperature detected on the device, in Celsius.

- %FTD-6-806001: Primary alarm CPU temperature is High *Celsius*
- %FTD-6-806002: Primary alarm for CPU high temperature is cleared
- %FTD-6-806003: Primary alarm CPU temperature is Low *Celsius*
- %FTD-6-806004: Primary alarm for CPU Low temperature is cleared
- %FTD-6-806005: Secondary alarm CPU temperature is High *Celsius*
- %FTD-6-806006: Secondary alarm for CPU high temperature is cleared
- %FTD-6-806007: Secondary alarm CPU temperature is Low *Celsius*
- %FTD-6-806008: Secondary alarm for CPU Low temperature is cleared

Alarm Input Contact Alarms

In these alarms, *description* is the description for the contact that you configured.

- %FTD-6-806009: Alarm asserted for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806010: Alarm cleared for ALARM_IN_1 *alarm_1_description*
- %FTD-6-806011: Alarm asserted for ALARM_IN_2 *alarm_2_description*
- %FTD-6-806012: Alarm cleared for ALARM_IN_2 *alarm_2_description*

History for Device Settings

Provides a comprehensive reference of feature introductions, command modifications, and interface updates related to device settings and management.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Policy rollback support for high availability devices.	7.2.0	7.2.0	The **configure policy rollback** command is supported for high availability devices.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Auto rollback of a deployment that causes a loss of management connectivity.	7.2.0	7.2.0	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 **configure policy rollback** command. New/modified screens: • **Devices** > **Device Management** > **Device** > **Deployment Settings** • **Deploy** > **Advanced Deploy** > **Preview** • **Deploy** > **Deployment History** > **Preview**
Object group search is enabled by default for access control rules.	7.2.0	7.2.0	The **Object Group Search** setting is enabled by default for managed devices starting with Version 7.2.0. This option is in the **Advanced Settings** section when editing device settings on the Device Management page.
Import and export device configurations.	7.1.0	7.1.0	You can export the device-specific configuration, and you can then import the saved configuration for the same device in the following use cases: • Moving the device to a different FMC. • Restore an old configuration. • Reregistering a device. New/modified screens: **Devices** > **Device Management** > **Device** > **General**
Update the FMC IP address on FTD.	6.7.0	6.7.0	If you change the FMC IP address, you can now use the FTD CLI to update the device. New/modified commands: **configure manager edit**
Alarms for the Cisco ISA 3000 series.	6.7	Any	Configuring alarms for the Cisco ISA 3000 series was validated using FlexConfig. You should be able to configure the alarms in older releases that support FlexConfig, except for the dual power supply alarms. Supported platforms: Secure Firewall Threat Defense