

Device Management Basics

The following topics describe how to manage devices in the Firepower System:

- About Device Management, on page 1
- Requirements and Prerequisites for Device Management, on page 9
- Complete the FTD Initial Configuration Using the CLI, on page 9
- Add a Device to the FMC, on page 15
- Delete a Device from the FMC, on page 18
- Add a Device Group, on page 18
- Configure Device Settings, on page 19
- Change the Manager for the Device, on page 49
- Viewing Device Information, on page 54
- History for Device Management Basics, on page 59

About Device Management

Use the Firepower Management Center to manage your devices.

About the Firepower Management Center and Device Management

When the Firepower Management Center manages a device, it sets up a two-way, SSL-encrypted communication channel between itself and the device. The Firepower Management Center uses this channel to send information to the device about how you want to analyze and manage your network traffic to the device. As the device evaluates the traffic, it generates events and sends them to the Firepower Management Center using the same channel.

By using the Firepower Management Center to manage devices, you can:

- configure policies for all your devices from a single location, making it easier to change configurations
- install various types of software updates on devices
- push health policies to your managed devices and monitor their health status from the Firepower Management Center

The Firepower Management Center aggregates and correlates intrusion events, network discovery information, and device performance data, allowing you to monitor the information that your devices are reporting in relation to one another, and to assess the overall activity occurring on your network.

You can use a Firepower Management Center to manage nearly every aspect of a device's behavior.

Note Although a Firepower Management Center can manage devices running certain previous releases as specified in the compatibility matrix available at http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html, new features are not available to these previous-release devices.

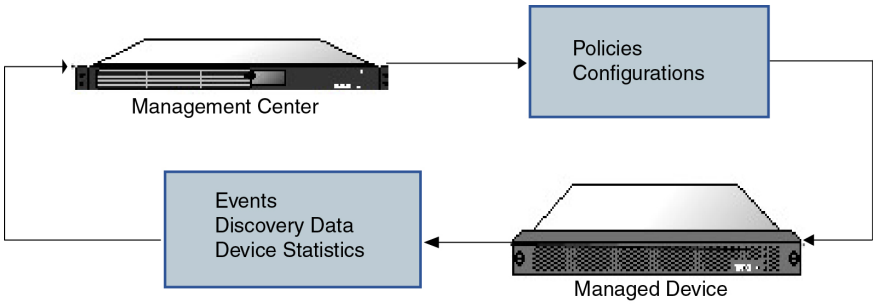
What Can Be Managed by a Firepower Management Center?

You can use the Firepower Management Center as a central management point in a Firepower System deployment to manage the following devices:

- ASA FirePOWER modules
- NGIPSv devices
- Firepower Threat Defense (physical hardware and virtual)

When you manage a device, information is transmitted between the Firepower Management Center and the device over a secure, SSL-encrypted TCP tunnel.

The following illustration lists what is transmitted between a Firepower Management Center and its managed devices. Note that the types of events and policies that are sent between the appliances are based on the device type.



Beyond Policies and Events

In addition to deploying policies to devices and receiving events from them, you can also perform other device-related tasks on the Firepower Management Center.

Backing Up a Device

You **cannot** create or restore backup files for NGIPSv devices or ASA FirePOWER modules.

When you perform a backup of a physical managed device from the device itself, you back up the device configuration **only**. To back up configuration data and, optionally, unified files, perform a backup of the device using the managing Firepower Management Center.

To back up event data, perform a backup of the managing Firepower Management Center.

Updating Devices

From time to time, Cisco releases updates to the Firepower System, including:

- intrusion rule updates, which may contain new and updated intrusion rules
- vulnerability database (VDB) updates
- geolocation updates
- software patches and updates

You can use the Firepower Management Center to install an update on the devices it manages.

About Device Management Interfaces

Each device includes a single dedicated Management interface for communicating with the FMC. You can optionally configure the device to use a data interface for management instead of the dedicated Management interface.

You can perform initial setup on the management interface, or on the console port.

Management interfaces are also used to communicate with the Smart Licensing server, to download updates, and to perform other management functions.

Management Interfaces on Managed Devices

When you set up your device, you specify the FMC IP address that you want to connect to. Both management and event traffic go to this address at initial registration. Note: In some situations, the FMC might establish the *initial* connection on a different management interface; subsequent connections should use the management interface with the specified IP address.

If the FMC has a separate event-only interface, the managed device sends subsequent event traffic is sent to the FMC event-only interface if the network allows. In addition, some managed-device models include an additional management interface that you can configure for event-only traffic. Note that if you configure a data interface for management, you cannot use separate management and event interfaces. If the event network goes down, then event traffic reverts to the regular management interfaces on the FMC and/or on the managed device.

About Using the FTD Data interface for Management

You can use either the dedicated Management interface or a regular data interface for communication with the FMC. The FMC access on a data interface is useful if you want to manage the Firepower Threat Defense remotely from the outside interface, or you do not have a separate management network.

The FMC access from a data interface has the following limitations:

- You can only enable manager access on one physical, data interface. You cannot use a subinterface or EtherChannel.
- This interface cannot be management-only.
- Routed firewall mode only, using a routed interface.
- PPPoE is not supported. If your ISP requires PPPoE, you will have to put a router with PPPoE support between the Firepower Threat Defense and the WAN modem.

- The interface must be in the global VRF only.
- You cannot use separate management and event-only interfaces.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the FMC. Because the Management interface gateway will be changed to be the data interfaces, you also cannot SSH to the Management interface from a remote network unless you add a static route for the Management interface using the **configure network static-routes** command.
- High Availability is not supported. You must use the Management interface in this case.

Management Interface Support Per Device Model

See the hardware installation guide for your model for the management interface locations.

Note For the Firepower 4100/9300 chassis, the MGMT interface is for *chassis* management, not for Firepower Threat Defense logical device management. You must configure a separate NIC interface to be of type mgmt (and/or firepower-eventing), and then assign it to the Firepower Threat Defense logical device.

Note For Firepower Threat Defense on any chassis, the physical management interface is shared between the Diagnostic logical interface, which is useful for SNMP or syslog, and is configured along with data interfaces in the FMC, and the Management logical interface for FMC communication. See Management/Diagnostic Interface for more information.

See the following table for supported management interfaces on each managed device model.

Table 1: Management Interface Support on Managed Devices

Model	Management Interface	Optional Event Interface
NGIPSv	eth0	No support
ASA FirePOWER services module on the ASA 5508-X, or 5516-X	eth0 **Note** eth0 is the internal name of the Management 1/1 interface.	No support
ASA FirePOWER services module on the ISA 3000	eth0 **Note** eth0 is the internal name of the Management 1/1 interface.	No support
Firepower Threat Defense on the Firepower 1000	management0 **Note** management0 is the internal name of the Management 1/1 interface.	No Support

Model	Management Interface	Optional Event Interface
Firepower Threat Defense on the Firepower 2100	management0 **Note** management0 is the internal name of the Management 1/1 interface.	No Support
Firepower Threat Defense on the Firepower 4100 and 9300	management0 **Note** management0 is the internal name of this interface, regardless of the physical interface ID.	management1 **Note** management1 is the internal name of this interface, regardless of the physical interface ID.
Firepower Threat Defense on the ASA 5508-X, or 5516-X	br1 **Note** br1 is the internal name of the Management 1/1 interface.	No support
Firepower Threat Defense on the ISA 3000	br1 **Note** br1 is the internal name of the Management 1/1 interface.	No support
Firepower Threat Defense Virtual	eth0	No support

Network Routes on Device Management Interfaces

Management interfaces (including event-only interfaces) support only static routes to reach remote networks. When you set up your managed device, the setup process creates a default route to the gateway IP address that you specify. You cannot delete this route; you can only modify the gateway address.

Note The routing for management interfaces is completely separate from routing that you configure for data interfaces. If you configure a data interface for management instead of using the dedicated Management interface, traffic is routed over the backplane to use the data routing table. The information in this section does not apply.

You can configure multiple management interfaces on some platforms (a management interface and an event-only interface). The default route does not include an egress interface, so the interface chosen depends on the gateway address you specify, and which interface's network the gateway belongs to. In the case of multiple interfaces on the default network, the device uses the lower-numbered interface as the egress interface.

At least one static route is recommended per management interface to access remote networks. We recommend placing each interface on a separate network to avoid potential routing problems, including routing problems from other devices to the FTD. If you do not experience problems with interfaces on the same network, then be sure to configure static routes correctly. For example, both management0 and management1 are on the same network, but the FMC management and event interfaces are on different networks. The gateway is

192.168.45.1. If you want management1 to connect to the FMC's event-only interface at 10.6.6.1/24, you can create a static route for 10.6.6.0/24 through management1 with the same gateway of 192.168.45.1. Traffic to 10.6.6.0/24 will hit this route before it hits the default route, so management1 will be used as expected.

Another example includes separate management and event-only interfaces on both the FMC and the managed device. The event-only interfaces are on a separate network from the management interfaces. In this case, add a static route through the event-only interface for traffic destined for the remote event-only network, and vice versa.

NAT Environments

Network address translation (NAT) is a method of transmitting and receiving network traffic through a router that involves reassigning the source or destination IP address. The most common use for NAT is to allow private networks to communicate with the internet. Static NAT performs a 1:1 translation, which does not pose a problem for FMC communication with devices, but port address translation (PAT) is more common. PAT lets you use a single public IP address and unique ports to access the public network; these ports are dynamically assigned as needed, so you cannot initiate a connection to a device behind a PAT router.

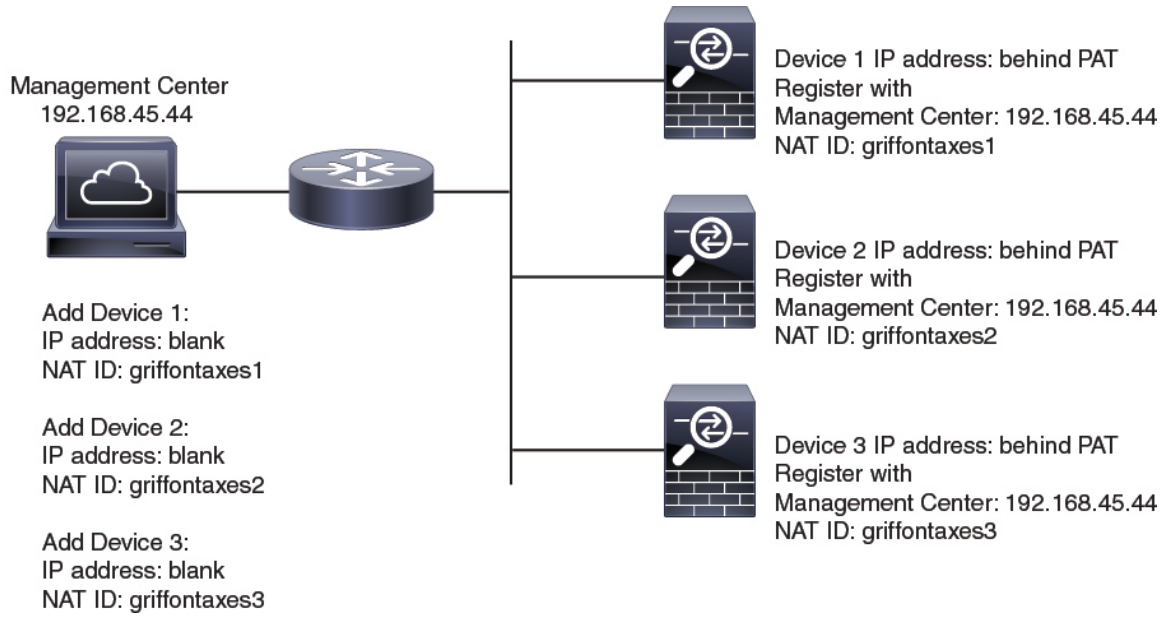
Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the FMC specifies the device IP address when you add a device, and the device specifies the FMC IP address. However, if you only know one of the IP addresses, which is the minimum requirement for routing purposes, then you must also specify a unique NAT ID on both sides of the connection to establish trust for the initial communication and to look up the correct registration key. The FMC and device use the registration key and NAT ID (instead of IP addresses) to authenticate and authorize for initial registration.

For example, you add a device to the FMC, and you do not know the device IP address (for example, the device is behind a PAT router), so you specify only the NAT ID and the registration key on the FMC; leave the IP address blank. On the device, you specify the FMC IP address, the same NAT ID, and the same registration key. The device registers to the FMC's IP address. At this point, the FMC uses the NAT ID instead of IP address to authenticate the device.

Although the use of a NAT ID is most common for NAT environments, you might choose to use the NAT ID to simplify adding many devices to the FMC. On the FMC, specify a unique NAT ID for each device you want to add while leaving the IP address blank, and then on each device, specify both the FMC IP address and the NAT ID. Note: The NAT ID must be unique per device.

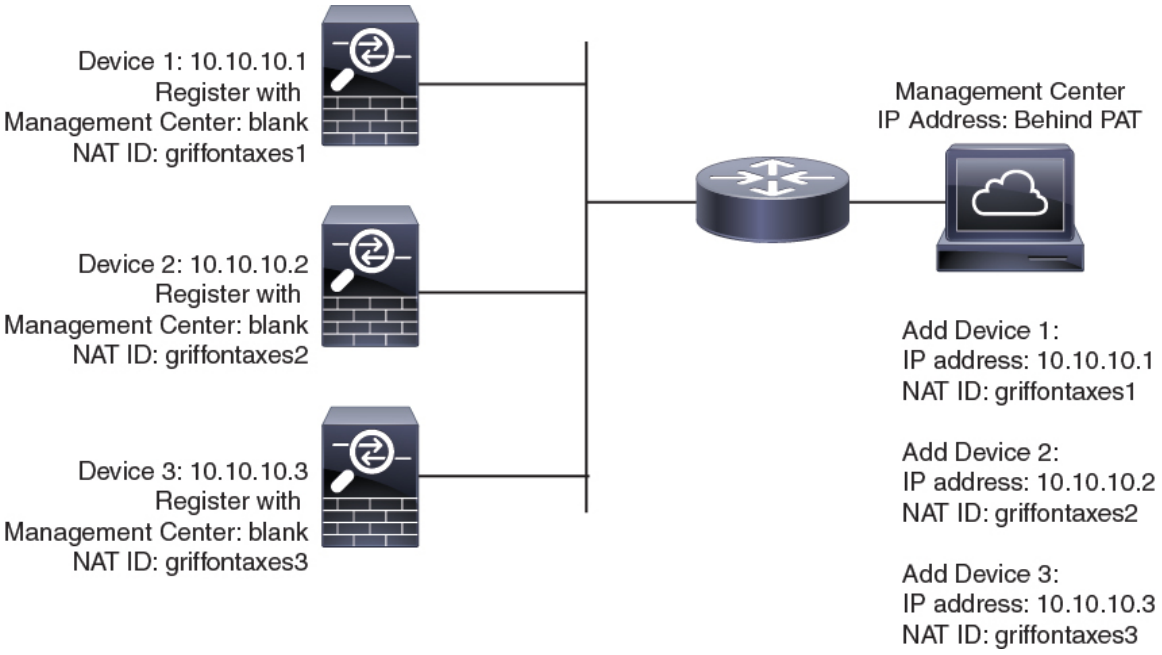
The following example shows three devices behind a PAT IP address. In this case, specify a unique NAT ID per device on both the FMC and the devices, and specify the FMC IP address on the devices.

Figure 1: NAT ID for Managed Devices Behind PAT



The following example shows the FMC behind a PAT IP address. In this case, specify a unique NAT ID per device on both the FMC and the devices, and specify the device IP addresses on the FMC.

Figure 2: NAT ID for FMC Behind PAT

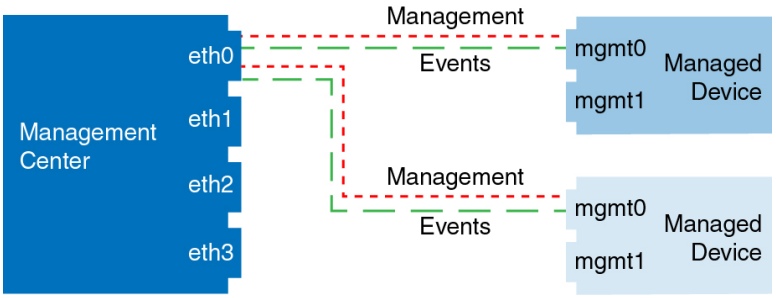


Management and Event Traffic Channel Examples

Note If you use a data interface for management on an FTD, you cannot use separate management and event interfaces for that device.

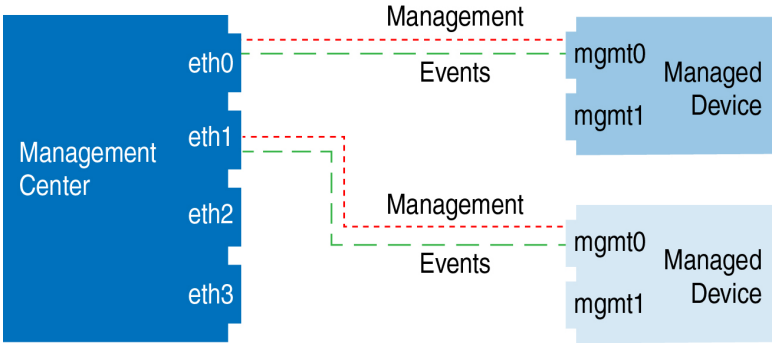
The following example shows the Firepower Management Center and managed devices using only the default management interfaces.

Figure 3: Single Management Interface on the Firepower Management Center



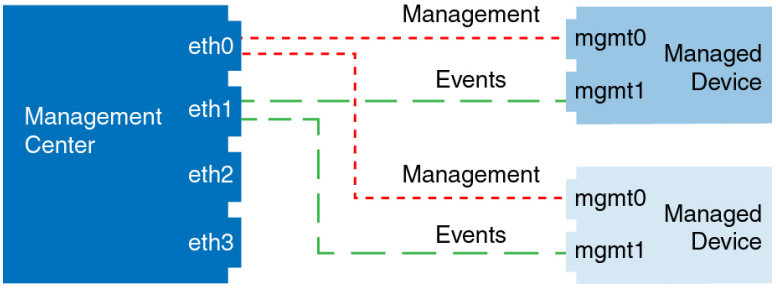
The following example shows the Firepower Management Center using separate management interfaces for devices; and each managed device using 1 management interface.

Figure 4: Mutliple Management Interfaces on the Firepower Management Center



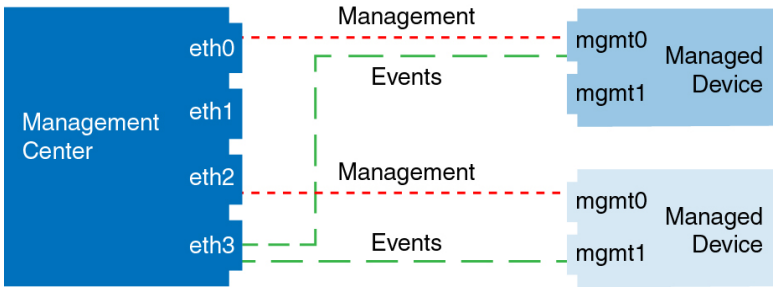
The following example shows the Firepower Management Center and managed devices using a separate event interface.

Figure 5: Separate Event Interface on the Firepower Management Center and Managed Devices



The following example shows a mix of multiple management interfaces and a separate event interface on the Firepower Management Center and a mix of managed devices using a separate event interface, or using a single management interface.

Figure 6: Mixed Management and Event Interface Usage



Requirements and Prerequisites for Device Management

Model Support

Any managed device; unless noted in the procedure.

Supported Domains

The domain in which the device resides.

User Roles

- Admin
- Network Admin

Complete the FTD Initial Configuration Using the CLI

Connect to the FTD CLI to perform initial setup, including setting the Management IP address, gateway, and other basic networking settings using the setup wizard. The dedicated Management interface is a special interface with its own network settings. If you do not want to use the Management interface for FMC access, you can use the CLI to configure a data interface instead. You will also configure FMC communication settings.

Before you begin

This procedure applies to all FTD devices except for the Firepower 4100/9300.

Procedure

Step 1 Connect to the FTD CLI, either from the console port or using SSH to the Management interface, which obtains an IP address from a DHCP server by default. If you intend to change the network settings, we recommend using the console port so you do not get disconnected.

(Firepower 1000/2100) The console port connects to the FXOS CLI. The SSH session connects directly to the FTD CLI.

Step 2 Log in with the username **admin** and the password **Admin123**.

(Firepower 1000/2100) At the console port, you connect to the FXOS CLI. The first time you log in to FXOS, you are prompted to change the password. This password is also used for the FTD login for SSH.

Note If the password was already changed, and you do not know it, you must reimage the device to reset the password to the default. See the FXOS troubleshooting guide for the reimage procedure.

Example:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Step 3 (Firepower 1000/2100) If you connected to FXOS on the console port, connect to the FTD CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4 The first time you log in to FTD, you are prompted to accept the End User License Agreement (EULA) and, if using an SSH connection, to change the admin password. You are then presented with the CLI setup script.

Note You cannot repeat the CLI setup wizard unless you clear the configuration; for example, by reimaging. However, all of these settings can be changed later at the CLI using **configure network** commands. See the FTD command reference.

Defaults or previously entered values appear in brackets. To accept previously entered values, press **Enter**.

Note The Management interface settings are used even when you enable FMC access on a data interface. For example, the management traffic that is routed over the backplane through the data interface will resolve FQDNs using the Management interface DNS servers, and not the data interface DNS servers.

See the following guidelines:

- **Configure IPv4 via DHCP or manually?**—If you want to use a data interface for FMC access instead of the management interface, choose **manual**. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address. You cannot configure a data interface for management if the management interface is set to DHCP, because the default route, which must be **data-interfaces** (see the next bullet), might be overwritten with one received from the DHCP server.
- **Enter the IPv4 default gateway for the management interface**—If you want to use a data interface for FMC access instead of the management interface, set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the FMC access data interface. If you want to use the Management interface for FMC access, you should set a gateway IP address on the Management 1/1 network.
- **If your networking information has changed, you will need to reconnect**—If you are connected with SSH but you change the IP address at initial setup, you will be disconnected. Reconnect with the new IP address and password. Console connections are not affected.
- **Manage the device locally?**—Enter **no** to use FMC. A **yes** answer means you will use Firepower Device Manager instead.
- **Configure firewall mode?**—We recommend that you set the firewall mode at initial configuration. Changing the firewall mode after initial setup erases your running configuration.Note that data interface FMC access is only supported in routed firewall mode.

Example:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy
```

```
You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Step 5 Identify the FMC that will manage this FTD.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**} *reg_key* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the FMC. If the FMC is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id*. At least one of the devices, either the FMC or the FTD, must have a reachable IP address to establish the two-way, SSL-encrypted communication channel between the two devices. If you specify **DONTRESOLVE** in this command, then the FTD must have a reachable IP address or hostname.
- *reg_key*—Specifies a one-time registration key of your choice that you will also specify on the FMC when you register the FTD. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the FMC when you register the FTD when one side does not specify a reachable IP address or hostname. It is required if you set the FMC to **DONTRESOLVE**. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the FMC.

  Note If you use a data interface for management, then you must specify the NAT ID on both the FTD and FMC for registration.

Example:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

If the FMC is behind a NAT device, enter a unique NAT ID along with the registration key, and specify DONTRESOLVE instead of the hostname, for example:

Example:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

If the FTD is behind a NAT device, enter a unique NAT ID along with the FMC IP address or hostname, for example:

Example:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

Step 6 (Optional) Configure a data interface for FMC access.

configure network management-data-interface

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

Note You should use the console port when using this command. If you use SSH to the Management interface, you might get disconnected and have to reconnect to the console port. See below for more information about SSH usage.

See the following details for using this command. See also About Using the FTD Data interface for Management, on page 3.

- The original Management interface cannot use DHCP if you want to use a data interface for management. If you did not set the IP address manually during initial setup, you can set it now using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- When you add the FTD to the FMC, the FMC discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For more information about the DNS server configuration, see below. In FMC, you can later make changes to the FMC access interface configuration, but make sure you don't make changes that can prevent the FTD or FMC from re-establishing the management connection. If the management connection is disrupted, the FTD includes the **configure policy rollback** command to restore the previous deployment.
- If you configure a DDNS server update URL, the FTD automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the FTD can validate the DDNS server certificate for the HTTPS connection. The FTD supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).
- This command sets the *data* interface DNS server. The Management DNS server that you set with the setup script (or using the **configure network dns servers** command) is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface.

  On the FMC, the data interface DNS servers are configured in the Platform Settings policy that you assign to this FTD. When you add the FTD to the FMC, the local setting is maintained, and the DNS servers are *not* added to a Platform Settings policy. However, if you later assign a Platform Settings policy to the FTD that includes a DNS configuration, then that configuration will overwrite the local setting. We suggest that you actively configure the DNS Platform Settings to match this setting to bring the FMC and the FTD into sync.

  Also, local DNS servers are only retained by FMC if the DNS servers were discovered at initial registration. For example, if you registered the device using the Management interface, but then later configure a data interface using the **configure network management-data-interface** command, then you must manually configure all of these settings in FMC, including the DNS servers, to match the FTD configuration.
- You can change the management interface after you register the FTD to the FMC, to either the Management interface or another data interface.

- The FQDN that you set in the setup wizard will be used for this interface.
- You can clear the entire device configuration as part of the command; you might use this option in a recovery scenario, but we do not suggest you use it for initial setup or normal operation.
- To disable data managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://jcrichton:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

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

Setting IPv4 network configuration.
Network settings changed.

>
```

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
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]:

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

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 7 (Optional) Limit data interface access to an FMC on a specific network.

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

By default, all networks are allowed.

What to do next

Register your device to a FMC.

Add a Device to the FMC

Use this procedure to add a single device to the FMC. If you plan to link devices for redundancy or performance, you must still use this procedure, keeping in mind the following points:

- Firepower Threat Defense high availability—Use this procedure to add each device to the Firepower Management Center, then establish high availability; see Add a Firepower Threat Defense High Availability Pair.
- Firepower Threat Defense clusters—For detailed information about adding clusters, see FMC: Add a Cluster.



Note If you have established or will establish FMC high availability, add devices *only* to the active (or intended active) FMC. When you establish high availability, devices registered to the active FMC are automatically registered to the standby.

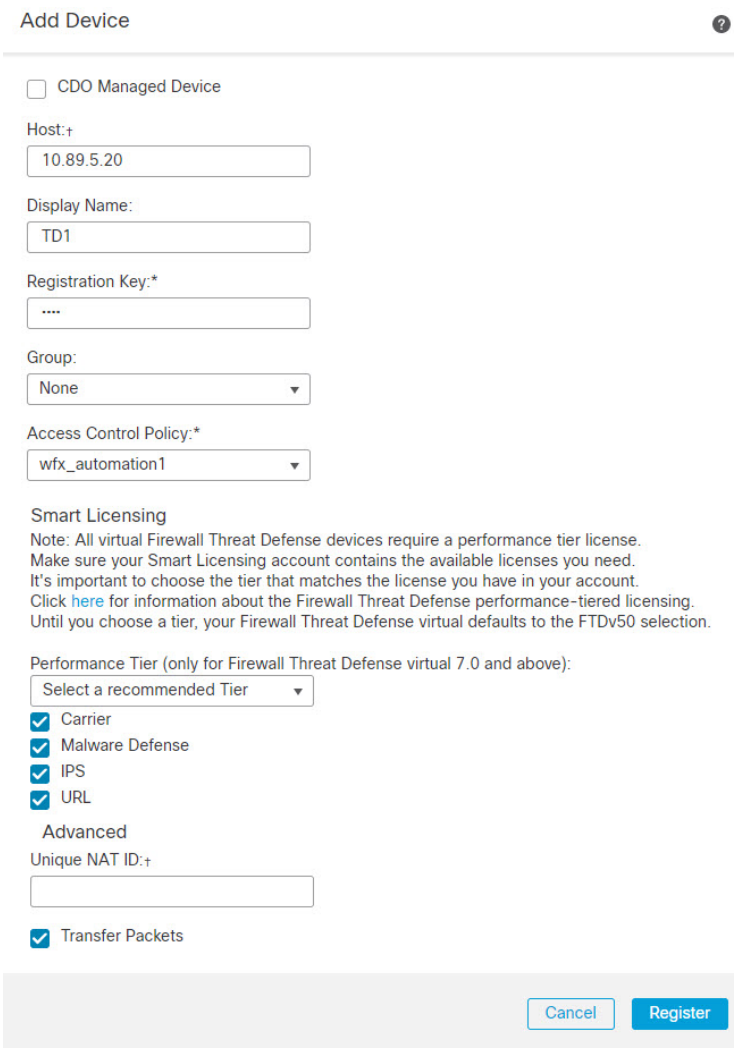
Before you begin

- Set up the device to be managed by the FMC. See:
  - Firepower Threat Defense devices: Complete the FTD Initial Configuration Using the CLI, on page 9
  - Other device types: The getting started guide for your model
- If you are adding an FTD device, the FMC must be registered for Smart Licensing. A valid evaluation license is sufficient, but if it expires, you will not be able to add new devices until you successfully register.
- If you registered a FMC and a device using IPv4 and want to convert them to IPv6, you must delete and reregister the device.

Procedure

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

Step 2 From the **Add** drop-down menu, choose **Device**.



Step 3 In the **Host** field, enter the IP address or the hostname of the device you want to add.

The hostname of the device is the fully qualified domain name or the name that resolves through the local DNS to a valid IP address. Use a hostname rather than an IP address if your network uses DHCP to assign IP addresses.

In a NAT environment, you may not need to specify the IP address or hostname of the device, if you already specified the IP address or hostname of the FMC when you configured the device to be managed by the FMC. For more information, see NAT Environments, on page 6.

Step 4 In the **Display Name** field, enter a name for the device as you want it to display in the FMC.

Step 5 In the **Registration Key** field, enter the same registration key that you used when you configured the device to be managed by the FMC. The registration key is a one-time-use shared secret. The key can include alphanumeric characters and hyphens (-).

Step 6 In a multidomain deployment, regardless of your current domain, assign the device to a leaf **Domain**.

If your current domain is a leaf domain, the device is automatically added to the current domain. If your current domain is not a leaf domain, post-registration, you must switch to the leaf domain to configure the device.

Step 7 (Optional) Add the device to a device **Group**.

Step 8 Choose an initial **Access Control Policy** to deploy to the device upon registration, or create a new policy.

If the device is incompatible with the policy you choose, deploying will fail. This incompatibility could occur for multiple reasons, including licensing mismatches, model restrictions, passive vs inline issues, and other misconfigurations. After you resolve the issue that caused the failure, manually deploy configurations to the device.

Step 9 Choose licenses to apply to the device.

If you registered the FMC to use Smart Licensing, then this dialog box only shows available Smart Licenses.

Smart Licensing

Assign the Smart Licenses you need for the features you want to deploy:

- **Malware** (if you intend to use AMP malware inspection)
- **Threat** (if you intend to use intrusion prevention)
- **URL** (if you intend to implement category-based URL filtering)

Note You can apply an AnyConnect remote access VPN license after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.

Classic Licensing

If you registered the FMC to use Smart Licensing, then this dialog box only shows available Smart Licenses. For classic licenses, go to the **Devices** > **Device Management** > **Device** > **License** area to assign licenses.

- Control, Malware, and URL Filtering licenses require a Protection license.

Step 10 If you used a NAT ID during device setup, expand in the **Advanced** section and enter the same NAT ID in the **Unique NAT ID** field. The NAT ID can include alphanumeric characters and hyphens (-).

Step 11 Check the **Transfer Packets** check box to allow the device to transfer packets to the Firepower Management Center.

This option is enabled by default. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the FMC for inspection. If you disable it, only event information will be sent to the FMC but packet data is not sent.

Step 12 Click **Register**.

It may take up to two minutes for the FMC to verify the device's heartbeat and establish communication. If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the device fails to register, check the following items:

- Ping—Access the device CLI, and ping the FMC IP address using the following command:

  ping system *ip_address*

  If the ping is not successful, check your network settings using the **show network** command. If you need to change the device IP address, use the **configure network** {**ipv4** | **ipv6**} **manual** command.

- Registration key, NAT ID, and FMC IP address—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the device using the **configure manager add** command.

For more troubleshooting information, see https://cisco.com/go/fmc-reg-error.

Delete a Device from the FMC

If you no longer want to manage a device, you can delete it from the FMC. Deleting a device:

- Severs all communication between the FMC and the device.
- Removes the device from the Device Management page.
- Returns the device to local time management if the device is configured using the platform settings policy to receive time from the FMC using NTP.

After deleting the device from the FMC:

- The FTD continues to process the traffic after you delete it from the FMC.
  - Policies, such as NAT and VPN, ACLs, and the interface configurations remain intact.
- Registering the FTD again to the same or a different FMC, the FTD configuration is removed from the FTD.
  - The ACLs that are selected during registration replace the earlier ACLs and the interface configuration remains intact.
- To manage the device later, re-add it to the FMC.

Note When a device is deleted and then re-added, the FMC web interface prompts you to re-apply your access control policies. However, there is no option to re-apply the NAT and VPN policies during registration. Any previously applied NAT or VPN configuration will be removed during registration and must be re-applied after registration is complete.

Procedure

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

Step 2 Next to the device you want to delete, click **Delete** ( ).

Step 3 Confirm that you want to delete the device.

Add a Device Group

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

In a multidomain deployment, you can create device groups within a leaf domain only. When you configure a Firepower Management Center for multitenancy, existing device groups are removed; you can re-add them at the leaf domain level.

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

Procedure

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

Step 2 From the **Add** drop-down menu, choose **Add Group**.

To edit an existing group, click **Edit** ( ) for the group you want to edit.

Step 3 Enter a **Name**.

Step 4 Under **Available Devices**, choose one or more devices to add to the device group. Use Ctrl or Shift while clicking to choose multiple devices.

Step 5 Click **Add** to include the devices you chose in the device group.

Step 6 Optionally, to remove a device from the device group, click **Delete** ( ) next to the device you want to remove.

Step 7 Click **OK** to add the device group.

Configure Device Settings

After you add a device, you can configure some settings on the device's **Device** page.

Managing System Shut Down

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any except ASA FirePOWER	Leaf only	Admin/Network Admin

Note You cannot shut down or restart the ASA FirePOWER with the Firepower System user interface. See the ASA documentation for more information on how to shut down the respective devices.

Procedure

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

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

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

Step 3 Click **Device**.

Step 4 To shut down the device, click **Shut Down Device** ( ) in the **System** section.

Step 5 When prompted, confirm that you want to shut down the device.

Step 6 To restart the device, click **Restart Device** ( ).

Step 7 When prompted, confirm that you want to restart the device.

Edit Management Settings

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

Update the Hostname or IP Address in FMC

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

To change the device management IP address on the device, see Modify Device Management Interfaces at the CLI, on page 30.

Procedure

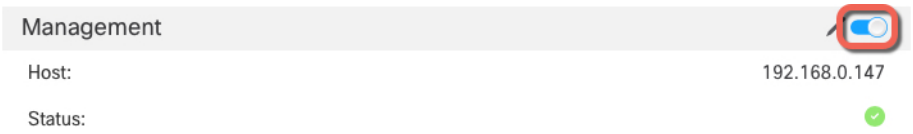
Step 1 Choose **Devices** > **Device Management**.

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

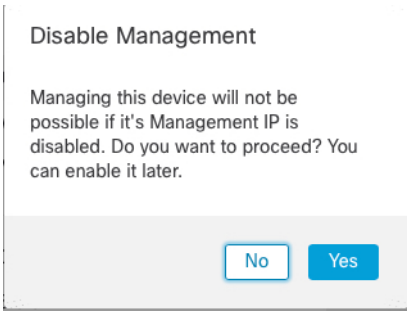
In a multidomain deployment, if you are not in a leaf domain, the system prompts you to switch.

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

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

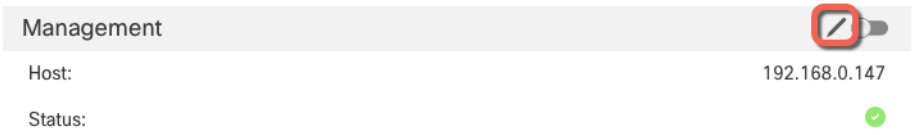


You are prompted to proceed with disabling management; click **Yes**.



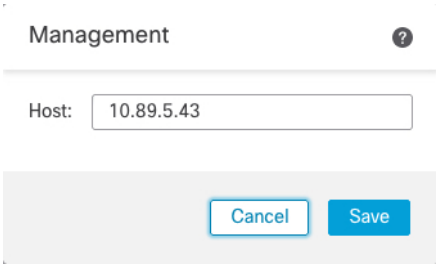
Disabling management blocks the connection between the Firepower Management Center and the device, but does **not** delete the device from the Firepower Management Center.

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



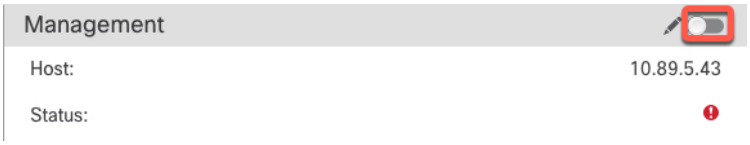
Step 6 In the **Management** dialog box, modify the name or IP address in the **Host** field, and click **Save**.

Figure 7: Management IP Address



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

Figure 8: Enable Management Connection



Change the FMC Access Interface from Management to Data

You can manage the FTD from either the dedicated Management interface, or from a data interface. If you want to change the FMC access interface after you added the device to FMC, follow these steps to migrate from the Management interface to a data interface. To migrate the other direction, see Change the FMC Access Interface from Data to Management, on page 24.

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

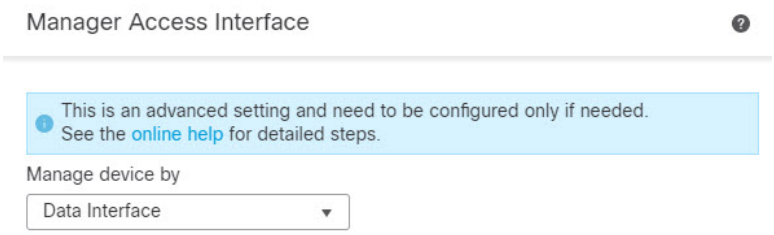
See the following steps to enable FMC access on a data interface, and also configure other required settings.

Procedure

Step 1 Initiate the interface migration.

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

The **FMC 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.



c) Click **Save**.

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

Figure 9: FMC Access



If you click **Configuration**, the **FMC Access Details** dialog box opens. The **FMC Access Mode** shows a Deploy Pending state.

Configuration		
Version	7.1.0	7.1.0 (Build 1760)
Configuration Cleared		No
FMC Access Mode	Data Interface (Deploy pending)	Management Interface
Connectivity Status	Connected	Connected

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

See Configure Routed Mode Interfaces. You can enable FMC 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 **Devices** > **Device Management** > **DHCP** > **DDNS** page. The standard type is not supported.

See Configure Dynamic DNS. DDNS ensures the FMC can reach the FTD at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes.

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

See Add a Static Route.

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

See Configure DNS. DNS is required if you use DDNS. You may also use DNS for FQDNs in your security policies.

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

See Configure Secure Shell. SSH is not enabled by default on the data interfaces, so if you want to manage the FTD using SSH, you need to explicitly allow it.

Step 7 Deploy configuration changes; see Deploy Configuration Changes.

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

Step 8 At the FTD CLI (preferably from the console port), set the Management interface to use a static IP address and set the gateway to use the data interfaces.

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

- *ip_address netmask*—Although you do not plan to use the Management interface, you must set a static IP address, for example, a private address so that you can set the gateway to **data-interfaces** (see the next bullet). 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 FMC access data interface.

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

Step 9 If necessary, re-cable the FTD so it can reach the FMC on the data interface.

Step 10 In FMC, disable the management connection, update the **Host** IP address for the FTD in the **Devices** > **Device Management** > **Device** > **Management** section, and reenable the connection.

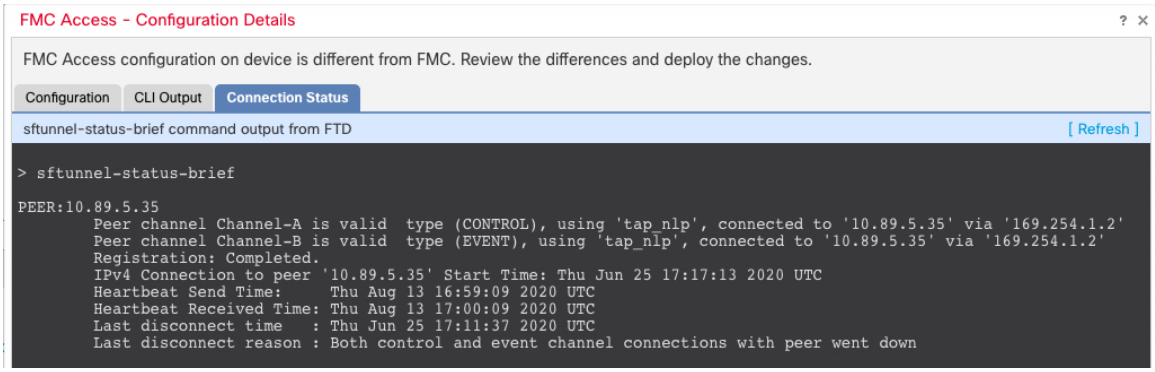
See Update the Hostname or IP Address in FMC, on page 20. If you used the FTD hostname or just the NAT ID when you added the FTD to the FMC, you do not need to update the value; however, you need to disable and reenable the management connection to restart the connection.

Step 11 Ensure the management connection is reestablished.

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

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

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



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 FMC Access Interface from Data to Management

You can manage the FTD from either the dedicated Management interface, or from a data interface. If you want to change the FMC access interface after you added the device to FMC, follow these steps to migrate from a Data interface to the Management interface. To migrate the other direction, see Change the FMC Access Interface from Management to Data, on page 21.

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

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

Before you begin

Model Support—FTD

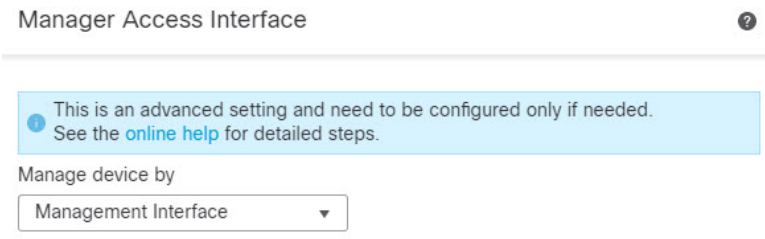
Procedure

Step 1 Initiate the interface migration.

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

b) Go to the **Device** > **Management** section, and click the link for **FMC Access Interface**.

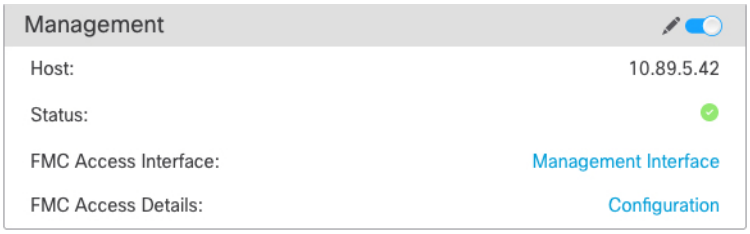
The **FMC Access Interface** field shows the current management interface. When you click the link, choose the new interface type, **Management Interface**, in the **Manage device by** drop-down list.



c) Click **Save**.

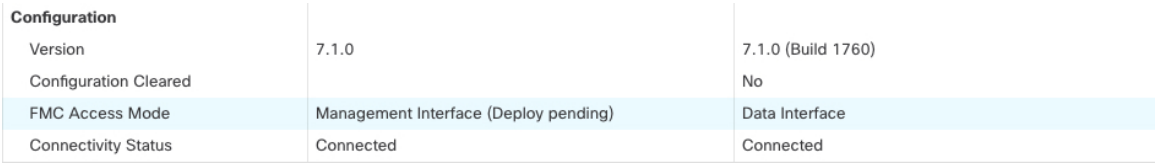
You must now complete the remaining steps in this procedure to enable FMC access on the data interface. The **Management** area now shows the **FMC Access Interface: Data Interface**, and **FMC Access Type: Configuration**.

Figure 10: FMC Access



If you click **Configuration**, the **FMC Access Details** dialog box opens. The **FMC Access Mode** shows a Deploy Pending state.

Figure 11: FMC Access Mode



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

See Configure Routed Mode Interfaces. This step removes the block on deployment.

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

See Configure DNS. The FMC deployment that disables FMC 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 FMC.

Step 4 Deploy configuration changes; see Deploy Configuration Changes.

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

Step 5 If necessary, re-cable the FTD so it can reach the FMC on the Management interface.

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

When you originally configured the data interface for FMC access, the Management gateway was set to data-interfaces, which forwarded management traffic over the backplane so it could be routed through the FMC 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 FMC, disable the management connection, update the **Host** IP address for the FTD in the **Devices** > **Device Management** > **Device** > **Management** section, and reenable the connection.

See Update the Hostname or IP Address in FMC, on page 20. If you used the FTD hostname or just the NAT ID when you added the FTD to the FMC, 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 FMC, check the management connection status on the **Devices** > **Device Management** > **Device** > **Management** > **Status** field or view notifications in FMC.

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

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See Troubleshoot Management Connectivity on a Data Interface, on page 39.

View FMC Access Details for Data Interface Management

Model Support—FTD

When you use a data interface for FMC management instead of using the dedicated Management interface, you must be careful about changing the interface and network settings for the device in FMC so you do not disrupt the connection. You can also change the data interface settings locally on the device, which requires you to reconcile those changes in FMC manually. The **Devices** > **Device Management** > **Device** > **Management** > **FMC Access Details** dialog box helps you resolve any discrepancies between the FMC and the FTD local configuration.

Normally, you configure the FMC access data interface as part of initial FTD setup before you add the FTD to the FMC. When you add the FTD to the FMC, the FMC discovers and maintains the interface configuration, including the following settings: interface name and IP address, static route to the gateway, DNS servers, and DDNS server. For the DNS server, the configuration is maintained locally if it is discovered during registration, but it is not added to the Platform Settings policy in FMC.

After you add the FTD to the FMC, if you change the data interface settings on the FTD locally using the **configure network management-data-interface** command, then the FMC detects the configuration changes, and blocks deployment to the FTD. The FMC detects the configuration changes using one of the following methods:

- Deploy to the FTD. Before the FMC deploys, it will detect the configuration differences and stop the deployment.
- The **Sync** button in the **Interfaces** page.
- The **Refresh** button on the **FMC Access Details** dialog box.

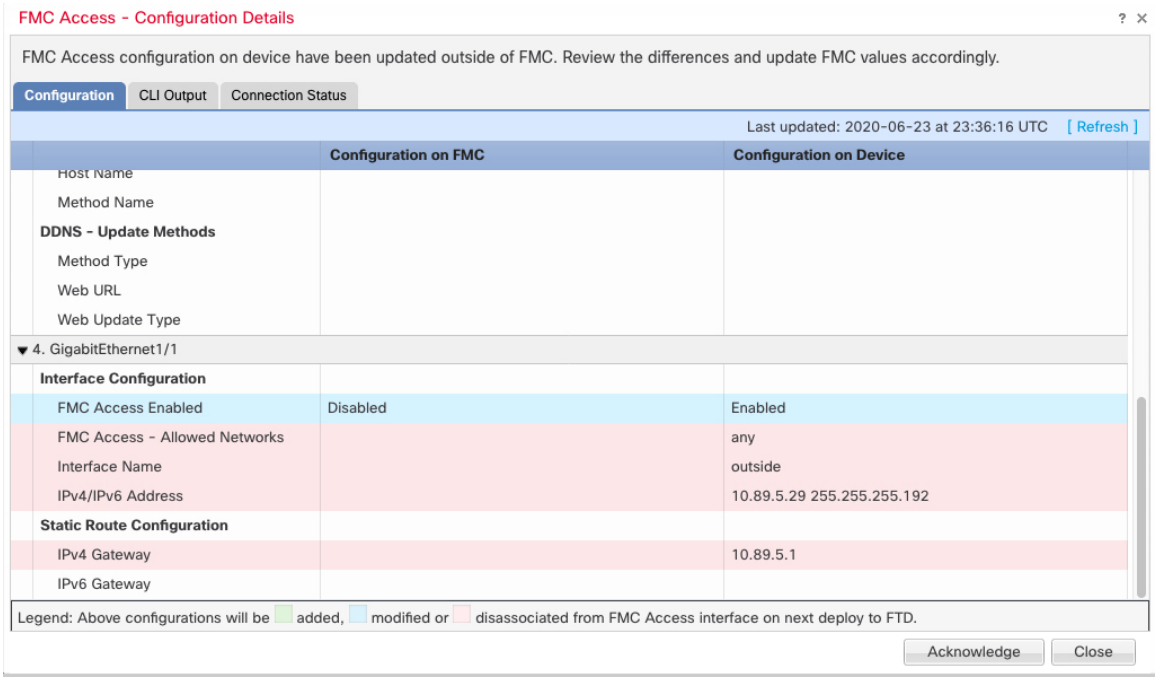
To remove the block, you must go to the **FMC Access Details** dialog box and click **Acknowledge**. The next time you deploy, the FMC configuration will overwrite any remaining conflicting settings on the FTD. It is your responsibility to manually fix the configuration in the FMC before you re-deploy.

See the following pages on this dialog box.

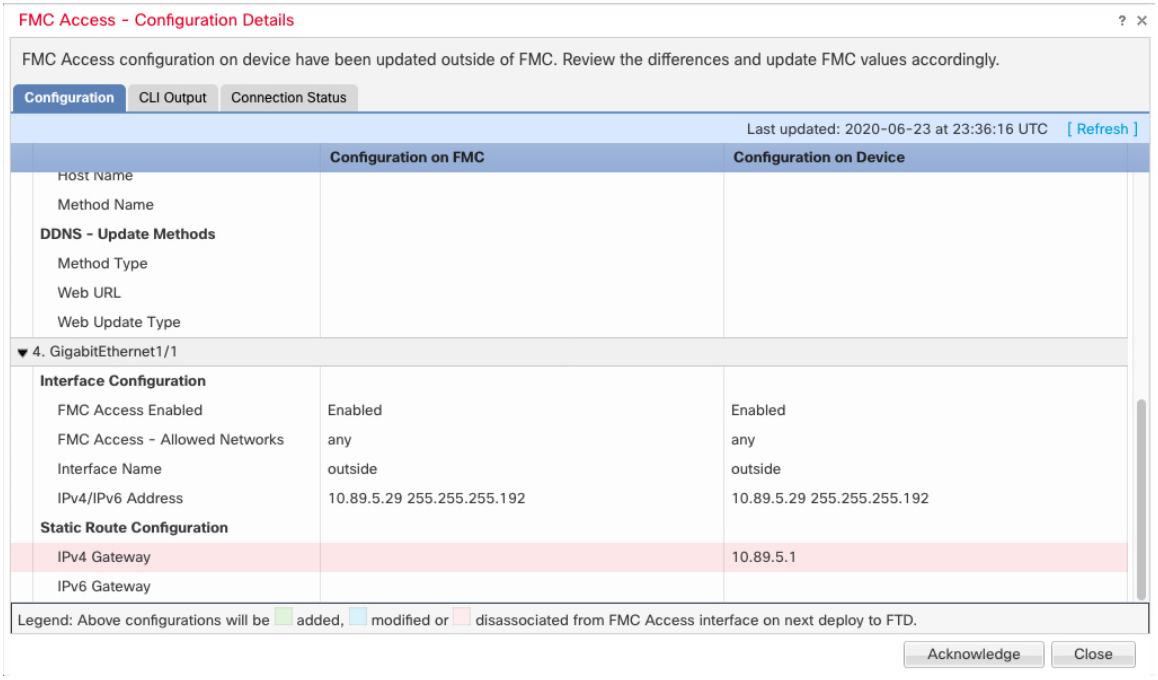
Configuration

View the configuration comparison of the FMC access data interface on the FMC and the FTD.

The following example shows the configuration details of an FTD where the **configure network management-data-interface** command was entered on the FTD. The pink highlights show that if you **Acknowledge** the differences but do not match the configuration in FMC, then the FTD configuration will be removed. The blue highlights show configurations that will be modified on the FTD. The green highlights show configurations that will be added to the FTD.

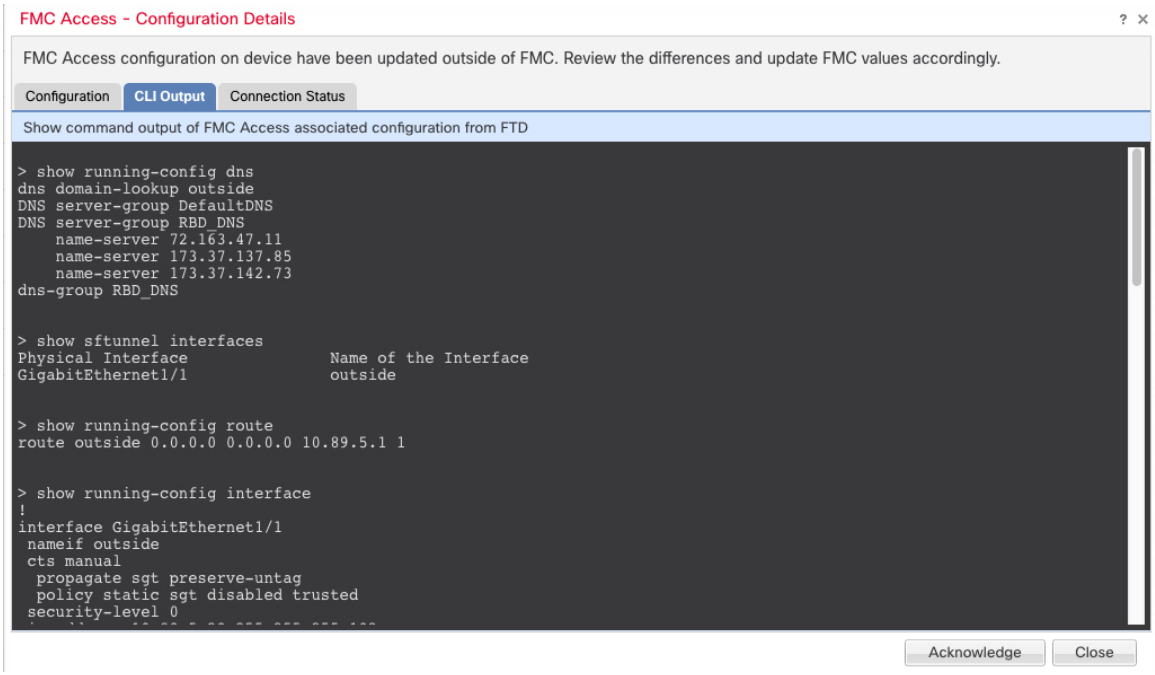


The following example shows this page after configuring the interface in FMC; the interface settings match, and the pink highlight was removed.



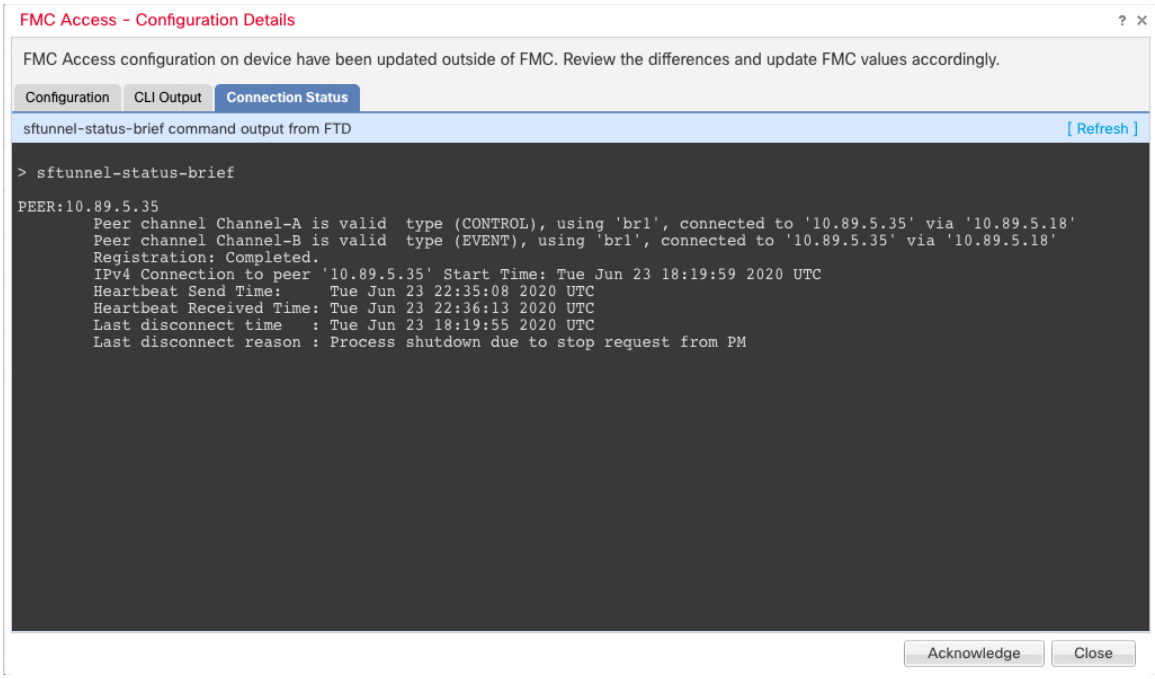
CLI Output

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

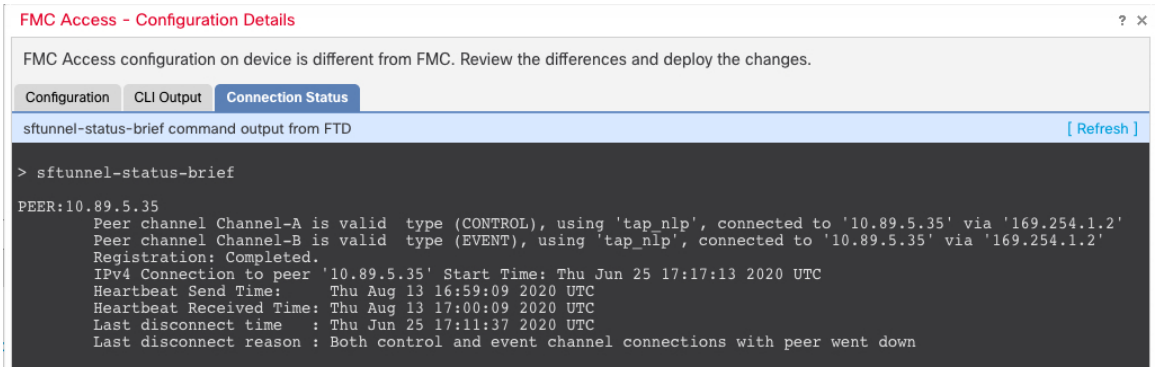


Connection Status

View management connection status. The following example shows that the management connection is still using the Management "br1" interface.



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



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

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

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

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
```

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

Modify Device Management Interfaces at the CLI

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

Note This topic applies to the dedicated Management interface. You can alternatively configure a data interface for management. If you want to change network settings for that interface, you should do so within FMC and not at the CLI. If you need to troubleshoot a disrupted management connection, and need to make changes directly on the FTD, see Modify the FTD Data Interface Used for Management at the CLI, on page 36.

For information about the Firepower Threat Defense CLI, see the FTD command reference.

For information about the classic device CLI, see Classic Device Command Line Reference in this guide.

The Firepower Threat Defense and classic devices use the same commands for management interface configuration. Other commands may differ between the platforms.

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

Note If you change the device management IP address, then see the following tasks for FMC connectivity depending on how you identified the FMC during initial device setup using the **configure manager add** command (see Identify a New FMC, on page 51):

- **IP address—No action.** If you identified the FMC 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 FMC to keep the information in sync; see Update the Hostname or IP Address in FMC, on page 20. This action can help the connection reestablish faster. **Note**: If you specified an unreachable FMC IP address, then see the procedure for NAT ID below.
- **NAT ID only—Manually reestablish the connection.** If you identified the FMC using only the NAT ID, then the connection cannot be automatically reestablished. In this case, change the device management IP address in FMC according to Update the Hostname or IP Address in FMC, on page 20.

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

Before you begin

- For Firepower Threat Defense devices, 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 for SSH.

Procedure

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

See Logging Into the Command Line Interface on Firepower Threat Defense Devices or Logging Into the CLI on ASA FirePOWER and NGIPSv Devices.

Step 2 Log in with the Admin username and password.

Step 3 (Firepower 4100/9300 only) Enable an event-only interface.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

Example:

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

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

>
```

The Firepower Management Center event-only interface cannot accept management channel traffic, so you should simply disable the management channel on the device event interface.

You can optionally disable events for the 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.

Step 4 Configure the network settings of the management interface and/or event interface:

If you do not specify the *management_interface* argument, then you change the network settings for the default management interface. When configuring an event interface, be sure to specify the *management_interface* argument. The event interface can be on a separate network from the management interface, or on the same

network. If you are connected to the interface you are configuring, you will be disconnected. You can re-connect to the new IP address.

a) Configure the IPv4 address:

- Manual configuration:

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

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

  Example:

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

  >
  ```

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

  configure network ipv4 dhcp

b) Configure the IPv6 address:

- Stateless autoconfiguration:

  configure network ipv6 router [*management_interface*]

  Example:

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

  >
  ```

- Manual configuration:

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

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

  Example:

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

>
```

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

  configure network ipv6 dhcp

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

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

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

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

Example:

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

Step 6 (Firepower Threat Defense only) 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 Firepower Threat Defense Virtual. To display the status of the DHCP server, enter **show network-dhcp-server**:

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

Step 7 Add a static route for the event-only interface if the Firepower 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).

For information about routing, see Network Routes on Device Management Interfaces, on page 5.

Example:

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

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

>
```

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

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

Step 8 Set the hostname:

configure network hostname *name*

Example:

```
> configure network hostname farscape1.cisco.com
```

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

Step 9 Set the search domains:

configure network dns searchdomains *domain_list*

Example:

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

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

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

configure network dns servers *dns_ip_list*

Example:

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

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

configure network management-interface tcpport *number*

Example:

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

The FMC and managed devices communicate using a two-way, SSL-encrypted communication channel, which by default is on port 8305.

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

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

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

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

Example:

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

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

Step 13 Configure an HTTP proxy. The device is configured to directly-connect to the internet on ports TCP/443 (HTTPS) and TCP/80 (HTTP). You can use a proxy server, to which you can authenticate via HTTP Digest. After issuing the command, you are prompted for the HTTP proxy address and port, whether proxy authentication is required, and if it is required, the proxy username, proxy password, and confirmation of the proxy password.

Note For proxy password on Cisco Firepower Threat Defense, you can use A-Z, a-z, and 0-9 characters only.

configure network http-proxy

Example:

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

Step 14 If you change the device management IP address, then see the following tasks for FMC connectivity depending on how you identified the FMC during initial device setup using the **configure manager add** command (see Identify a New FMC, on page 51):

- **IP address—No action.** If you identified the FMC 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 FMC to keep the information in sync; see Update the Hostname or IP Address in FMC, on page 20. This action can help the connection reestablish faster. **Note**: If you specified an unreachable FMC IP address, then you must manually reestablish the connection using Update the Hostname or IP Address in FMC, on page 20.
- **NAT ID only—Manually reestablish the connection.** If you identified the FMC using only the NAT ID, then the connection cannot be automatically reestablished. In this case, change the device management IP address in FMC according to Update the Hostname or IP Address in FMC, on page 20.

Modify the FTD Data Interface Used for Management at the CLI

If the management connection between the FTD and the FMC was disrupted, and you want to specify a new data interface to replace the old interface, use the FTD CLI to configure the new interface. This procedure assumes you want to use replace the old interface with a new interface on the same network. If the management connection is active, then you should make any changes to an existing data interface using FMC. For initial setup of the data management interface, see the **configure network management-data-interface** command in Complete the FTD Initial Configuration Using the CLI, on page 9.

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 Device Management Interfaces at the CLI, on page 30.

For information about the Firepower Threat Defense CLI, see the FTD 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 for SSH.

Procedure

Step 1 If you are changing the data management interface to a new interface, move the current interface cable to the new interface.

Step 2 Connect to the device CLI.

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

See Logging Into the Command Line Interface on Firepower Threat Defense Devices.

Step 3 Log in with the Admin username and password.

Step 4 Configure a data interface for FMC access.

configure network management-data-interface

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

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

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

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

Setting IPv4 network configuration.
Network settings changed.

>
```

Step 5 (Optional) Limit data interface access to an FMC on a specific network.

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

By default, all networks are allowed.

Step 6 The connection will be reestablished automatically, but disabling and reenabling the connection in FMC will help the connection reestablish faster. See Update the Hostname or IP Address in FMC, on page 20.

Step 7 Check that the management connection was reestablished.

sftunnel-status-brief

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

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

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

Step 8 In FMC, choose **Devices** > **Device Management** > **Device** > **Management** > **FMC Access Details**, and click **Refresh**.

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

Step 9 Choose **Devices** > **Device Management** > **Interfaces**, and make the following changes.

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

b) Configure the new data management interface with the settings of the old interface (the ones you used at the CLI), and enable FMC Access for it.

Step 10 Choose **Devices** > **Device Management** > **Routing** > **Static Route** and change the default route from the old data management interface to the new one.

Step 11 Return to the **FMC Access Details** dialog box, and click **Acknowledge** to remove the deployment block.

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

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

Roll Back the Configuration if the FMC Loses Connectivity

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

See the following guidelines:

- Only the previous deployment is available locally on the Firepower Threat Defense; you cannot roll back to any earlier deployments.
- Rollback is not supported for High Availability or Clustering deployments.
- The rollback only affects configurations that you can set in the FMC. For example, the rollback does not affect any local configuration related to the dedicated Management interface, which you can only configure at the Firepower Threat Defense CLI. Note that if you changed data interface settings after the last FMC deployment using the **configure network management-data-interface** command, and then you use the rollback command, those settings will not be preserved; they will roll back to the last-deployed FMC 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.

Before you begin

Model Support—FTD

Procedure

Step 1 At the Firepower Threat Defense CLI, roll back to the previous configuration.

configure policy rollback

After the rollback, the Firepower Threat Defense notifies the FMC that the rollback was completed successfully. In the FMC, the deployment screen will show a banner stating that the configuration was rolled back.

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

Example:

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

At the Firepower 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

Model Support—FTD

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

This topic helps you troubleshoot the loss of management connectivity.

View management connection status

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

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

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

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

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

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

View the FTD network information

At the Firepower Threat Defense CLI, view the Management and the FMC access data interface network settings:

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]=======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
```

```
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

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

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.29
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

Check that the FTD registered with the FMC

At the Firepower Threat Defense CLI, check that the FMC registration was completed. Note that this command will not show the *current* status of the management connection.

show managers

```
> show managers
Type                      : Manager
Host                      : 10.89.5.35
Registration              : Completed

>
```

Ping the FMC

At the Firepower Threat Defense CLI, use the following command to ping the FMC from the data interfaces:

ping *fmc_ip*

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

ping system *fmc_ip*

Capture packets on the FTD internal interface

At the Firepower Threat Defense CLI, capture packets on the internal backplane interface (nlp_int_tap) to see if management packets are being sent:

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

show capture*name* **trace detail**

Check the internal interface status, statistics, and packet count

At the Firepower Threat Defense CLI, see information about the internal backplane interface, nlp_int_tap:

show interace detail

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

Check routing and NAT

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

show route

```
> show route

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

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

>
```

show nat

```
> show nat

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

Check other settings

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

show running-config sftunnel

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

show running-config ip-client

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

show conn address *fmc_ip*

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

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

Check for a successful DDNS update

At the Firepower Threat Defense CLI, check for a successful DDNS update:

debug ddns

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

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

show crypto ca certificates *trustpoint_name*

To check the DDNS operation:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

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

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

Check FMC log files

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

Edit General Settings

Procedure

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

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

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

Step 3 Click **Device**.

Step 4 In the **General** section, click **Edit** ( ).

Step 5 Enter a **Name** for the managed device.

Step 6 Change the **Transfer Packets** setting:

- Check the check box to allow packet data to be stored with events on the Firepower Management Center.
- Clear the check box to prevent the managed device from sending packet data with the events.

Step 7 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 FTD.

Step 8 Click **Deploy**.

What to do next

- Deploy configuration changes; see Deploy Configuration Changes.

Copy a Configuration to Another Device

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

Before you begin

Confirm that:

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

Model Support—FTD

Procedure

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

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

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

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 the destination to which configuration is to be copied in the **Target Device** drop-down list.

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

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

Step 6 Click **OK**.

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

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

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

Edit License Settings

You can enable licenses on your device if you have available licenses on your Firepower 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** ( ).

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

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.

Edit Advanced Settings

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

Note For information about the Transfer Packets setting, see Edit General Settings, on page 44.

Configure Automatic Application Bypass

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

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

See the following behavior:

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

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

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

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

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

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

Procedure

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

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

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

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

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.

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.

Object group search is disabled by default. You can enable it on one device at a time; you cannot enable it globally. We recommend that you enable it on any device to which you deploy access rules that use network or interface objects.

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

Before you begin

- Model Support—FTD
- 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.

Procedure

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

Step 2 Next to the FTD 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

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

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



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

Before you begin

Model Support—FTD

Procedure

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

Step 2 Next to the FTD device where you want to configure the rule, click the **Edit** ( ).

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

Step 4 Check **Interface Object Optimization**.

Step 5 Click **Save**.

Change the Manager for the Device

You might need to change the manager on a device in the following circumstances:

- Edit the FMC IP Address or Hostname on the Device, on page 50—If you change the FMC IP address or hostname, we recommend that you match the new IP address or hostname on the device.
- Identify a New FMC, on page 51—After you delete the device from the old FMC, if present, you can configure the device for the new FMC, and then add it to the FMC.

- Switch from Firepower Device Manager to FMC, on page 52—You cannot use both FDM and FMC at the same time for the same device. If you change from FDM to FMC, the FTD configuration will be erased, and you will need to start over.
- Switch from FMC to Firepower Device Manager, on page 53—You cannot use both FDM and FMC at the same time for the same device. If you change from FMC to FDM, the FTD configuration will be erased, and you will need to start over.

Edit the FMC IP Address or Hostname on the Device

If you change the FMC 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 FMC 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 FMC and you specified the NAT ID only. Even in other cases, we recommend keeping the FMC IP address or hostname up to date for extra network resiliency.

Before you begin

Model Support—FTD

Procedure

Step 1 At the FMC CLI, view the unique UUID for the FMC so you can specify it in the FTD command. For information about the FMC CLI, see Firepower Management Center Command Line Reference.

show version

The FMC UUID definitively identifies the FMC; for example, in the case of FMC High Availability, you need to specify the active FMC on the FTD.

Example:

```
> show version
-------------------[ firepower ]--------------------
Model                     : Cisco Firepower Management Center for VMWare (66) Version 6.7.0
 (Build 1222)
UUID                       : f2a06484-9f7f-11ea-b9f4-541a108ebbb5
Rules update version       : 2020-05-26-001-vrt
VDB version                : 334
----------------------------------------------------
```

Step 2 At the FTD CLI, edit the FMC IP address or hostname.

configure manager edit *fmc_uuid* {*ip_address* | *hostname*}

If the FMC 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 f2a06484-9f7f-11ea-b9f4-541a108ebbb5 10.10.5.1
```

Identify a New FMC

This procedure shows how to identify a new FMC for the managed device. You should perform these steps even if the new FMC uses the old FMC's IP address.

Procedure

Step 1 On the old FMC, if present, delete the managed device. See Delete a Device from the FMC, on page 18.

You cannot change the FMC IP address if you have an active connection with an FMC.

Step 2 Connect to the device CLI, for example using SSH.

Step 3 Configure the new FMC.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address*}—Sets the FMC hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE**—If the FMC is not directly addressable, use **DONTRESOLVE** instead of a hostname or IP address. If you use **DONTRESOLVE** , then a *nat_id* is required. When you add this device to the FMC, make sure that you specify both the device IP address and the *nat_id*; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.
- *regkey*—Make up a registration key to be shared between the FMC and the device during registration. You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD.
- *nat_id*—Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the FMC and the device when one side does not specify an IP address. This NAT ID is a one-time password used only during registration. Make sure the NAT ID is unique, and not used by any other devices awaiting registration. Specify the same NAT ID on the FMC when you add the FTD.

Example:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

Step 4 Add the device to the FMC. See Add a Device to the FMC, on page 15.

Switch from Firepower Device Manager to FMC

This procedure describes how to change your manager from Firepower Device Manager (FDM), a local device manager, to FMC. You can switch between FDM and FMC without reinstalling the software. You cannot use both FDM and FMC at the same time for the same device. If you change from FDM to FMC, the FTD configuration will be erased, and you will need to start over.



Caution Changing the manager resets the Firepower Threat Defense configuration to the factory default. However, the management bootstrap configuration is maintained.

Before you begin

Model Support—FTD

Procedure

Step 1 In FDM, for High Availability, break the high availability configuration. Ideally, break HA from the active unit.

Step 2 In FDM, unregister the device from the Smart Licensing server.

Step 3 Connect to the device CLI, for example using SSH.

Step 4 Remove the current management setting.

configure manager delete

Caution Deleting the local manager resets the Firepower Threat Defense configuration to the factory default. However, the management bootstrap configuration is maintained.

Example:

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

Step 5 Configure the new FMC.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address*}—Sets the FMC hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE**—If the FMC is not directly addressable, use **DONTRESOLVE** instead of a hostname or IP address. If you use **DONTRESOLVE** , then a *nat_id* is required. When you add this device to the FMC, make sure that you specify both the device IP address and the *nat_id*; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.

- *regkey*—Make up a registration key to be shared between the FMC and the device during registration. You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD.
- *nat_id*—Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the FMC and the device when one side does not specify an IP address. This NAT ID is a one-time password used only during registration. Make sure the NAT ID is unique, and not used by any other devices awaiting registration. Specify the same NAT ID on the FMC when you add the FTD.

Example:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

Step 6 Add the device to the FMC. See Add a Device to the FMC, on page 15.

Switch from FMC to Firepower Device Manager

This procedure describes how to change your manager from FMC to Firepower Device Manager (FDM), a local device manager. You can switch between FDM and FMC without reinstalling the software. You cannot use both FDM and FMC at the same time for the same device. If you change from FMC to FDM, the FTD configuration will be erased, and you will need to start over.

Caution Changing the manager resets the Firepower Threat Defense configuration to the factory default. However, the management bootstrap configuration is maintained.

Before you begin

Model Support—FTD

Procedure

Step 1 In FMC, for High Availability, break the high availability configuration. Ideally, break HA from the active unit. See Separate Units in a High Availability Pair.

Step 2 In FMC, delete the managed device. See Delete a Device from the FMC, on page 18.

You cannot change the manager if you have an active connection with an FMC.

Step 3 Connect to the device CLI, for example using SSH.

Step 4 Remove the current management setting.

configure manager delete

Caution Deleting the local manager resets the Firepower Threat Defense configuration to the factory default. However, the management bootstrap configuration is maintained.

Example:

```
> configure manager delete

If you enabled any feature licenses, you must disable them in
Firepower Device Manager before deleting the local manager.
Otherwise, those licenses remain assigned to the device in
Cisco Smart Software Manager.
Do you want to continue[yes/no]:yes

DHCP Server Disabled
>
```

Step 5 Configure the new FMC.

configure manager add {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE** } *regkey* [*nat_id*]

- {*hostname* | *IPv4_address* | *IPv6_address*}—Sets the FMC hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE**—If the FMC is not directly addressable, use **DONTRESOLVE** instead of a hostname or IP address. If you use **DONTRESOLVE** , then a *nat_id* is required. When you add this device to the FMC, make sure that you specify both the device IP address and the *nat_id*; one side of the connection needs to specify an IP address, and both sides need to specify the same, unique NAT ID.
- *regkey*—Make up a registration key to be shared between the FMC and the device during registration. You can choose any text string for this key between 1 and 37 characters; you will enter the same key on the FMC when you add the FTD.
- *nat_id*—Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the FMC and the device when one side does not specify an IP address. This NAT ID is a one-time password used only during registration. Make sure the NAT ID is unique, and not used by any other devices awaiting registration. Specify the same NAT ID on the FMC when you add the FTD.

Example:

```
> configure manager add DONTRESOLVE abc123 efg456
Manager successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.

>
```

Step 6 Add the device to the FMC. See Add a Device to the FMC, on page 15.

Viewing Device Information

In a multidomain deployment, ancestor domains can view information about all devices in descendant domains. You must be in a leaf domain to edit a device.

Procedure

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

Step 2 Click **Edit** ( ) next to the device you want to view.

In a multidomain deployment, if you are in an ancestor domain, you can click **View** ( ) to view a device from a descendant domain in read-only mode.

Step 3 Click **Device**.

Step 4 You can view the following information:

- General — Displays general settings for the device; see General Information, on page 56.
- License — Displays license information for the device; see License Information, on page 56.
- System — Displays system information about the device; see System Information, on page 56.
- Health — Displays information about the current health status of the device; see Health Information, on page 57.
- Management — Displays information about the communication channel between the Firepower Management Center and the device; see Management Information, on page 57.
- Advanced — Displays information about advanced feature configuration; see Advanced Settings, on page 58.

Device Management Page Information

The Device Management page provides you with range of information and options to manage Firepower devices:

- View By—Use this option to view the devices based on group, licenses, model, or access control policy.
- Device State—You can also view the devices based on its state. You can click on a state icon to view the devices belonging to it. The number of devices belonging to the states are provided within brackets.
- Search—You can search for a configured device by providing the device name, host name, or the IP address.
- Add options—You can use the add options to configure device, high availability, FTD cluster, stack, and group.
- Edit and other actions—Against each configured device, use the **Edit** ( ) icon to edit the device parameters and attributes. Click the **More** ( ) icon and execute other actions:
  - Delete—To delete the device.
  - Packet Tracer—To navigate to the packet tracer page for examining policy configuration on the device by injecting a model packet into the system.
  - Packet Capture—To navigate to the packet capture page, where, you can view the verdicts and actions the system takes while processing a packet.
  - Revert Upgrade—To revert the upgrade and configuration changes that were made after the last upgrade. This action results in restoring the device to the version that was before the upgrade.
  - For Firepower 4100/9300 series devices, a link to the Firepower Chassis Manager web interface.

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

General Information

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

Table 2: General Section Table Fields

Field	Description
Name	The display name of the device on the Firepower Management Center.
Transfer Packets	This displays whether or not the managed device sends packet data with the events to the Firepower Management Center.
Mode	The displays the mode of the management interface for the device: **routed** or **transparent**. **Note** The **Mode** field is displayed only for Firepower Threat Defense devices.
Compliance Mode	This displays the security certifications compliance for a device. Valid values are CC, UCAPL and None.

License Information

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

System Information

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

Table 3: System Section Table Fields

Field	Description
Model	The model name and number for the managed device.
Serial	The serial number of the chassis of the managed device.
Time	The current system time of the device. This is always in UTC. See also the Time Zone setting for time-based rules, below.
Version	The version of the software currently installed on the managed device.
Time Zone setting for time-based rules	The current system time of the device, in the time zone specified in device platform settings.
Policy	A link to the platform settings policy currently deployed to the managed device.

Field	Description
Inventory	A link to the inventory details for the associated device. This field only appears for some platforms, for example, the Firepower 2100 or a Firepower 4100/9300 container instance. To update information for a container instance, click **Update**. For example, if you change the resource profile, you can force an update of the inventory to avoid problems with mismatching High Availability pairs. Otherwise, this information is updated when you deploy policy changes.

You can also shut down or restart the device.

Health Information

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

Table 4: Health Section Table Fields

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

Management Information

The **Management** section of the **Device** page displays the fields described in the table below.

Table 5: Management Section Table Fields

Field	Description
Host	The IP address or hostname of the device. To change the hostname or IP Address of the device, see Edit Management Settings, on page 20.
Status	An icon indicating the status of the communication channel between the Firepower Management Center and the managed device. You can hover over the status icon to view the last time the Firepower Management Center contacted the device.
FMC Access Interface	Shows the type of interface used for FMC management: a data interface or the management interface. To change the interface, click the value. See Edit Management Settings, on page 20.
FMC Access Details	Click the **Configuration** link to view the data interface configuration on the FMC compared to the values on the device, as well as connection status. For more information, see View FMC Access Details for Data Interface Management, on page 26.

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 6: Advanced Section Table Fields

Field	Description	Supported Devices
Application Bypass	The state of Automatic Application Bypass on the device.	NGIPSv ASA FirePOWER Firepower Threat Defense
Bypass Threshold	The Automatic Application Bypass threshold, in milliseconds.	
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.	Firepower Threat Defense
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.	Firepower Threat Defense

History for Device Management Basics

Feature	Version	Details
Filter devices by upgrade status.	6.7.0	The Device Management page now provides upgrade information about your managed devices, including whether a device is upgrading (and what its upgrade path is), and whether its last upgrade succeeded or failed. New/modified screens: **Devices** > **Device Management**
One-click access to Firepower Chassis Manager.	6.4.0	For Firepower 4100/9300 series devices, the Device Management page provides a link to the Firepower Chassis Manager web interface. New/modified screens: **Devices** > **Device Management**
Filter devices by health and deployment status; view version information.	6.2.3	The Device Management page now provides version information for managed devices, as well as the ability to filter devices by health and deployment status. New/modified screens: **Devices** > **Device Management**