



Device Management

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

This chapter describes how to add and manage devices in the Secure Firewall Management Center.

- [About Device Management, on page 1](#)
- [Requirements and Prerequisites for Device Management, on page 10](#)
- [Log Into the Command Line Interface on the Device, on page 10](#)
- [Complete the Threat Defense Initial Configuration, on page 12](#)
- [Add a Device to the Management Center, on page 26](#)
- [Delete \(Unregister\) a Device from the Management Center, on page 29](#)
- [Add a Device Group, on page 31](#)
- [Shut Down or Restart the Device, on page 31](#)
- [Configure Device Settings, on page 32](#)
- [Change the Management Settings for the Device, on page 76](#)
- [Hot Swap an SSD on the Secure Firewall 3100, on page 83](#)
- [History for Device Management Basics, on page 85](#)

About Device Management

Use the management center to manage your devices.

About the Management Center and Device Management

When the management center manages a device, it sets up a two-way, SSL-encrypted communication channel between itself and the device. The 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 management center using the same channel.

By using the 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 management center



Note If you have a CDO-managed device and are using the on-prem management center for analytics only, then the on-prem management center does not support policy configuration or upgrading. Chapters and procedures in this guide related to device configuration and other unsupported features do not apply to devices whose primary manager is CDO.

The 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 the management center to manage nearly every aspect of a device's behavior.



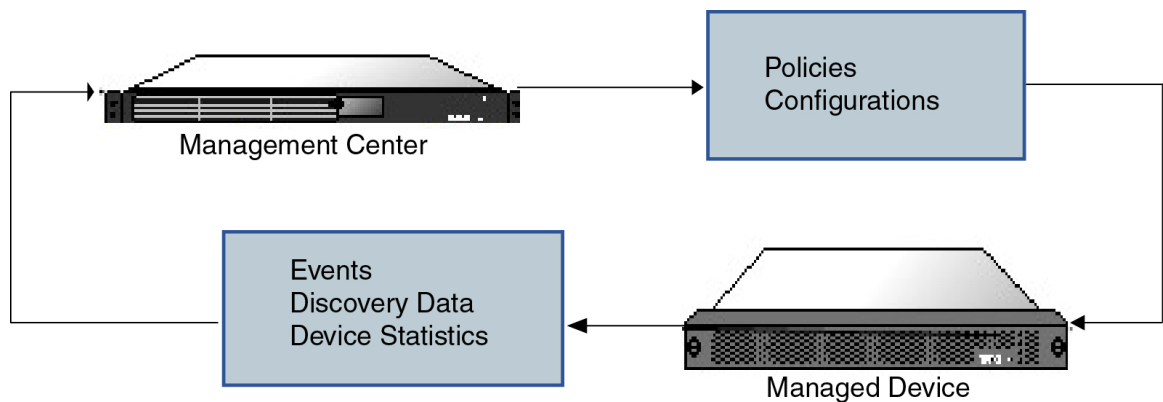
Note Although the management center can manage devices running certain previous releases as specified in the compatibility matrix available at <http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html>, new features that require the latest version of threat defense software are not available to these previous-release devices. Some management center features may be available for earlier versions.

What Can Be Managed by a Secure Firewall Management Center?

You can use the Secure Firewall Management Center as a central management point to manage threat defense devices.

When you manage a device, information is transmitted between the management center and the device over a secure, TLS-1.3-encrypted communication channel. You do not need to run this traffic over an additional encrypted tunnel such as Site-to-Site VPN for security purposes. If the VPN goes down, for example, you will lose your management connection, so we recommend a simple management path.

The following illustration lists what is transmitted between the 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.



About the Management Connection

After you configure the device with the management center information and after you add the device to the management center, either the device or the management center can establish the management connection. Depending on initial setup:

- Either the device or the management center can initiate.
- Only the device can initiate.
- Only the management center can initiate.

Initiation always originates with eth0 on the management center or with the lowest-numbered management interface on the device. Additional management interfaces are tried if the connection is not established. Multiple management interfaces on the management center let you connect to discrete networks or to segregate management and event traffic. However, the initiator does not choose the best interface based on the routing table.

Make sure the management connection is stable, without excessive packet loss, with at least 5Mbps throughput.



Note The management connection is a secure, TLS-1.3-encrypted communication channel between itself and the device. You do not need to run this traffic over an additional encrypted tunnel such as Site-to-Site VPN for security purposes. If the VPN goes down, for example, you will lose your management connection, so we recommend a simple management path.

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 management center.

Backing Up a Device

You cannot backup a physical managed device from the FTD CLI. To back up configuration data, and, optionally, unified files, perform a backup of the device using the management center that is managing the device.

To back up event data, perform a backup of the management center that is managing the device.

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 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 management center. 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 and Event Interfaces on the Threat Defense

When you set up your device, you specify the management center IP address or hostname that you want to connect to, if known. In this case, the device initiates the connection, and both management and event traffic go to this address at initial registration. If the management center is not known, then the management center establishes the initial connection. In this case, it might initially connect from a different management center management interface than specified on the threat defense. Subsequent connections should use the management center management interface with the specified IP address.

If the management center has a separate event-only interface, the managed device sends subsequent event traffic to the management center 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 management center and/or on the managed device.

Using the Threat Defense Data Interface for Management

You can use either the dedicated Management interface or a regular data interface for communication with the management center. Manager access on a data interface is useful if you want to manage the threat defense remotely from the outside interface, or you do not have a separate management network.

Manager Access Requirements

Manager access from a data interface has the following requirements.

- 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 threat defense and the WAN modem.
- The interface must be in the global VRF only.
- SSH is not enabled by default for data interfaces, so you will have to enable SSH later using the management center. 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. For threat defense virtual on Amazon Web Services, a console port is not available, so you should maintain your SSH access to the Management interface: add a static route for Management before you continue with your

configuration. Alternatively, be sure to finish all CLI configuration (including the **configure manager add** command) before you configure the data interface for manager access and you are disconnected.

- You cannot use separate management and event-only interfaces.
- Clustering is not supported. You must use the Management interface in this case.
- 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, the MGMT interface is for *chassis* management, not for threat defense logical device management. You must configure a separate interface to be of type mgmt (and/or firepower-eventing), and then assign it to the threat defense logical device.



Note For the 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 management center, and the Management logical interface for the management center 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
Firepower 1000	management0 Note management0 is the internal name of the Management 1/1 interface.	No Support
Firepower 2100	management0 Note management0 is the internal name of the Management 1/1 interface.	No Support
Secure Firewall 3100	management0 Note management0 is the internal name of the Management 1/1 interface.	No Support

Model	Management Interface	Optional Event Interface
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.
ISA 3000	br1 Note br1 is the internal name of the Management 1/1 interface.	No support
Secure Firewall 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 threat defense.



Note The interface used for management connections is not determined by the routing table. Connections are always tried using the lowest-numbered interface first.

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 management center 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.

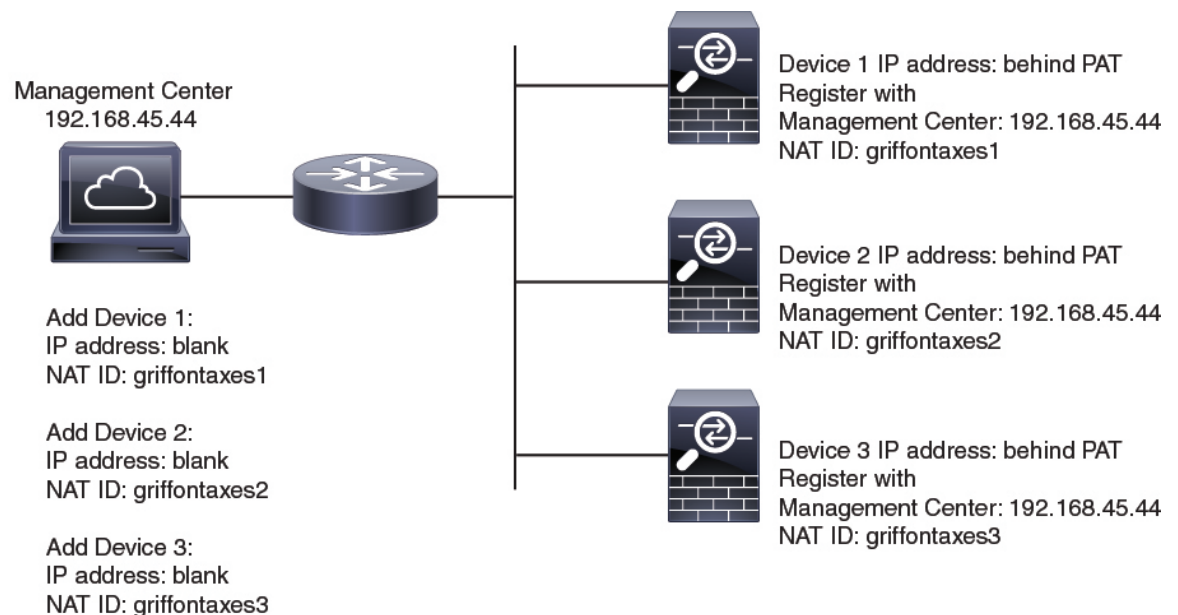
Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the management center specifies the device IP address when you add a device, and the device specifies the management center IP address. However, if you only know one of the IP addresses, 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 management center 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 management center, 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 management center; leave the IP address blank. On the device, you specify the management center IP address, the same NAT ID, and the same registration key. The device registers to the management center's IP address. At this point, the management center 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 management center. On the management center, 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 management center IP address and the NAT ID. Note: The NAT ID must be unique per device.

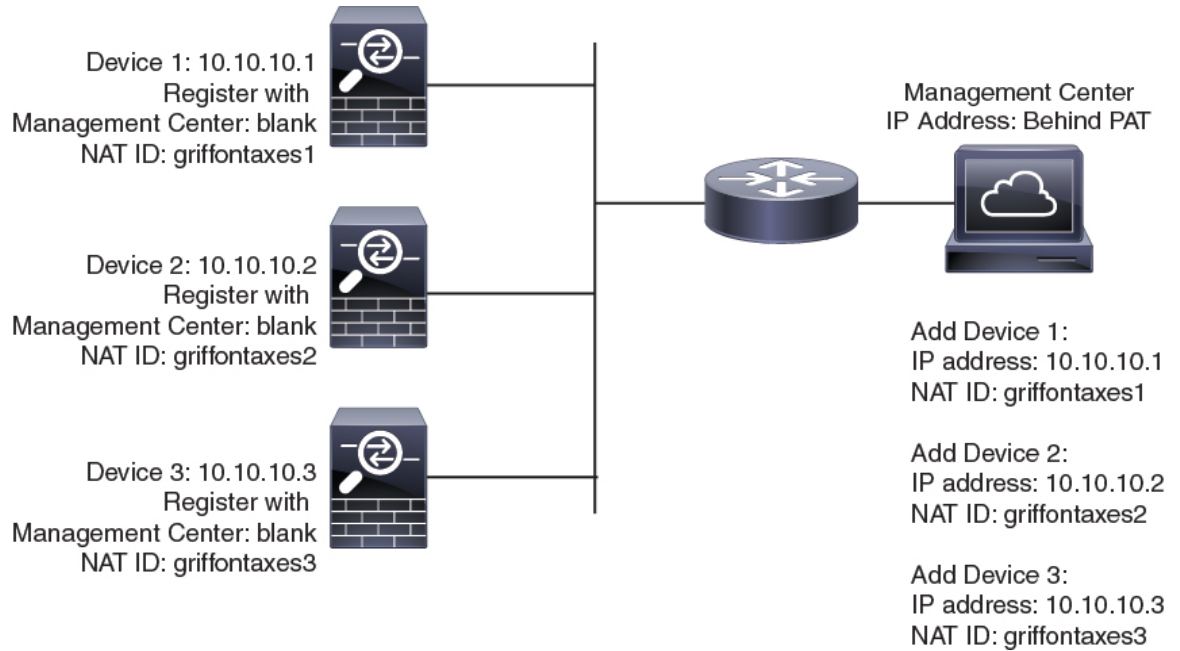
The following example shows three devices behind a PAT IP address. In this case, specify a unique NAT ID per device on both the management center and the devices, and specify the management center IP address on the devices.

Figure 1: NAT ID for Managed Devices Behind PAT



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

Figure 2: NAT ID for Management Center Behind PAT



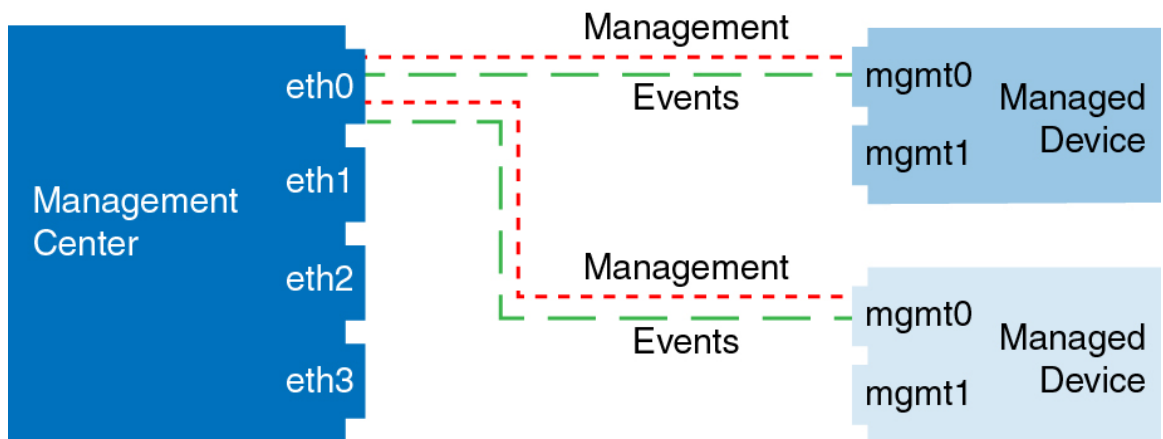
Management and Event Traffic Channel Examples



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

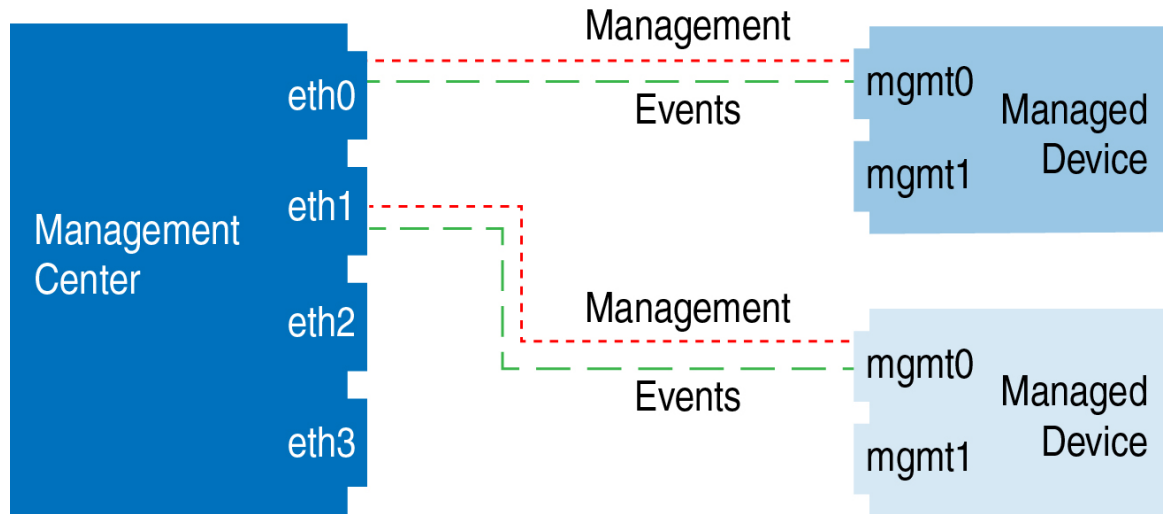
The following example shows the management center and managed devices using only the default management interfaces.

Figure 3: Single Management Interface on the Secure Firewall Management Center



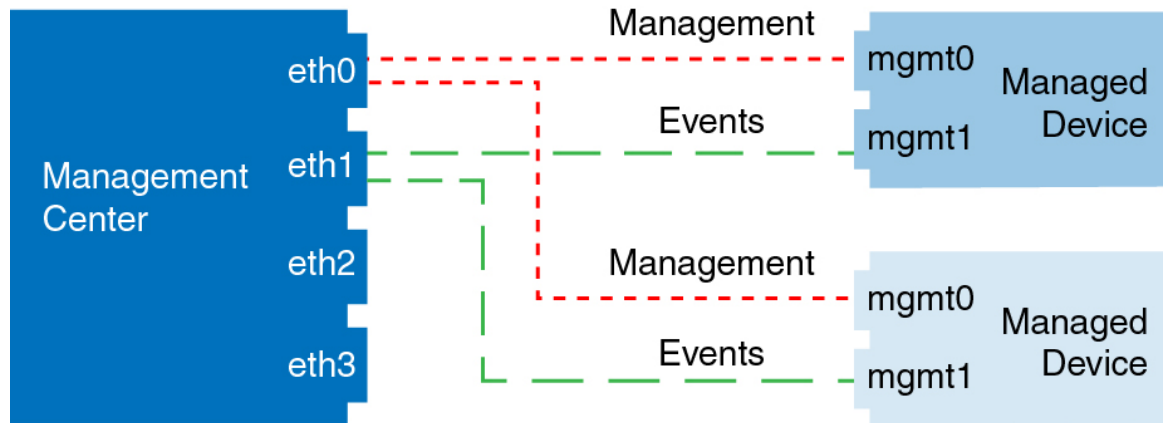
The following example shows the management center using separate management interfaces for devices; and each managed device using 1 management interface.

Figure 4: Multiple Management Interfaces on the Secure Firewall Management Center



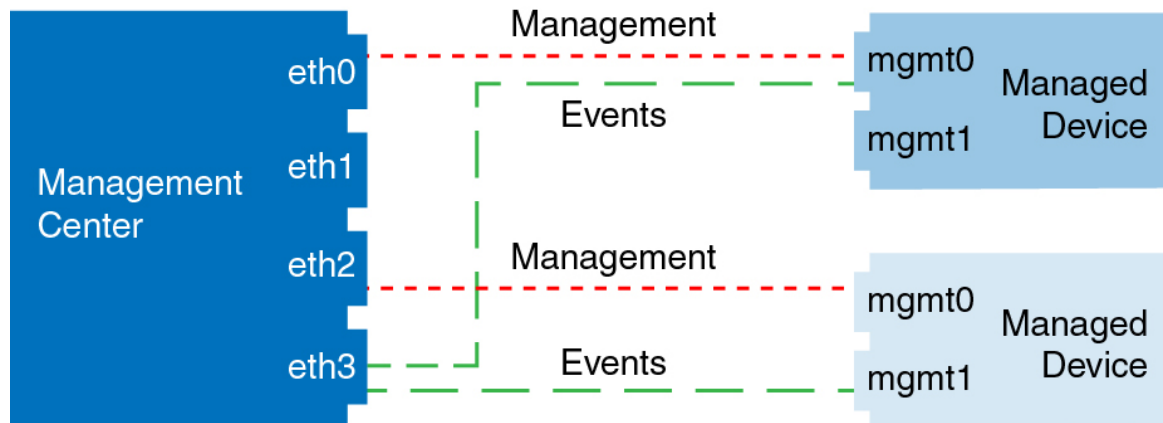
The following example shows the management center and managed devices using a separate event interface.

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



The following example shows a mix of multiple management interfaces and a separate event interface on the 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

Supported Domains

The domain in which the device resides.

User Roles

- Admin
- Network Admin

Management Connection

Make sure the management connection is stable, without excessive packet loss, with at least 5Mbps throughput.

Log Into the Command Line Interface on the Device

You can log directly into the command line interface on threat defense devices. If this is your first time logging in, complete the initial setup process using the default **admin** user; see [Complete the Threat Defense Initial Configuration Using the CLI, on page 18](#).



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

Before you begin

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

Procedure

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

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

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

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

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

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

Example:

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

firepower#
```

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

connect ftd

Note This step does not apply to the ISA 3000.

Example:

```
firepower# connect ftd
>
```

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

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

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

connect fxos

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

Step 6 (Optional) Access the diagnostic CLI:

system support diagnostic-cli

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

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

Example:

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

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

Complete the Threat Defense Initial Configuration

You can complete the threat defense initial configuration using the CLI or the device manager for all models except for the Firepower 4100/9300. For the Firepower 4100/9300, you complete initial configuration when you deploy the logical device. See [Logical Devices on the Firepower 4100/9300](#).

Complete the Threat Defense Initial Configuration Using the Device Manager

Connect to the device manager to perform initial setup of the threat defense. When you perform initial setup using the device manager, *all* interface configuration completed in the device manager is retained when you switch to the management center for management, in addition to the Management interface and manager access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the CLI, only the Management interface and manager access settings are retained (for example, the default inside interface configuration is not retained).

- This procedure does not apply for CDO-managed devices for which you want to use an on-prem management center *for analytics only*. The device manager configuration is meant to configure the primary manager. See [Complete the Threat Defense Initial Configuration Using the CLI, on page 18](#) for more information about configuring the device for analytics.
- This procedure applies to all other devices except for the Firepower 4100/9300 and the ISA 3000. You can use the device manager to onboard these devices to the management center, but because they have different default configurations than other platforms, the details in this procedure may not apply to these platforms.

Procedure

Step 1

Log into the device manager.

- a) Enter the following URL in your browser.
 - Inside—<https://192.168.95.1>.

- **Management**—https://management_ip. The Management interface is a DHCP client, so the IP address depends on your DHCP server. You will have to set the Management IP address to a static address as part of this procedure, so we recommend that you use the inside interface so you do not become disconnected.

- b) Log in with the username **admin**, and the default password **Admin123**.
- c) You are prompted to read and accept the End User License Agreement and change the admin password.

Step 2

Use the setup wizard when you first log into the device manager to complete the initial configuration. You can optionally skip the setup wizard by clicking **Skip device setup** at the bottom of the page.

After you complete the setup wizard, in addition to the default configuration for the inside interface, you will have configuration for an outside (Ethernet1/1) interface that will be maintained when you switch to the management center management.

- a) Configure the following options for the outside and management interfaces, and click **Next**.
 1. **Outside Interface Address**—This interface is typically the internet gateway, and might be used as your manager access interface. You cannot select an alternative outside interface during initial device setup. The first data interface is the default outside interface.

If you want to use a different interface from outside (or inside) for manager access, you will have to configure it manually after completing the setup wizard.

Configure IPv4—The IPv4 address for the outside interface. You can use DHCP or manually enter a static IP address, subnet mask, and gateway. You can also select **Off** to not configure an IPv4 address. You cannot configure PPPoE using the setup wizard. PPPoE may be required if the interface is connected to a DSL modem, cable modem, or other connection to your ISP, and your ISP uses PPPoE to provide your IP address. You can configure PPPoE after you complete the wizard.

Configure IPv6—The IPv6 address for the outside interface. You can use DHCP or manually enter a static IP address, prefix, and gateway. You can also select **Off** to not configure an IPv6 address.

2. Management Interface

You will not see Management Interface settings if you performed initial setup at the CLI.

The Management interface settings are used even if you enable manager 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.

DNS Servers—The DNS server for the system's management address. Enter one or more addresses of DNS servers for name resolution. The default is the OpenDNS public DNS servers. If you edit the fields and want to return to the default, click **Use OpenDNS** to reload the appropriate IP addresses into the fields.

Firewall Hostname—The hostname for the system's management address.

- b) Configure the **Time Setting (NTP)** and click **Next**.
 1. **Time Zone**—Select the time zone for the system.
 2. **NTP Time Server**—Select whether to use the default NTP servers or to manually enter the addresses of your NTP servers. You can add multiple servers to provide backups.
- c) Select **Start 90 day evaluation period without registration**.

Do not register the threat defense with the Smart Software Manager; all licensing is performed on the management center.

- d) Click **Finish**.
- e) You are prompted to choose **Cloud Management** or **Standalone**. For management center management, choose **Standalone**, and then **Got It**.

Step 3 (Might be required) Configure the Management interface.

You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the device manager if you were using the Management interface for the device manager connection.

- Data interface for manager access—The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.
- Management interface for manager access—If you want to configure a static IP address, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, then you do not need to configure anything assuming you successfully get the gateway from DHCP.

Step 4 If you want to configure additional interfaces, including an interface other than outside or inside that you want to use for manager access, choose **Device**, and then click the link in the **Interfaces** summary.

Other device manager configuration will not be retained when you register the device to management center.

Step 5 Choose **Device > System Settings > Central Management**, and click **Proceed** to set up the management center management.

Step 6 Configure the **Management Center/CDO Details**.

Figure 7: Management Center/CDO Details

Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes No

Threat Defense

10.89.5.16
fe80::6a87:c6ff:fea6:4c00/64

→

Management Center/CDO

10.89.5.35

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

••••

NAT ID

Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.

11203

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup

Management Center/CDO Access Interface

Data Interface

Please select an interface

Management Interface [View details](#)

CANCEL CONNECT

- a) For **Do you know the Management Center/CDO hostname or IP address**, click **Yes** if you can reach the management center using an IP address or hostname, or **No** if the management center is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the management center or the threat defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

- b) If you chose **Yes**, then enter the **Management Center/CDO Hostname/IP Address**.
- c) Specify the **Management Center/CDO Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the management center when you register the threat defense device. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the management center.

- d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the management center. This field is required if you only specify the IP address on one of the devices; but we recommend that you specify the NAT ID even if you know the IP addresses of both devices. 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 management center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked.

Step 7 Configure the **Connectivity Configuration**.

- a) Specify the **FTD Hostname**.

If you use a data interface for the **Management Center/CDO Access Interface** access, then this FQDN will be used for this interface.

- b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

If you intend to choose a data interface for the **Management Center/CDO Access Interface**, then this setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likely to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense device. When you add the threat defense device to the management center, 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 threat defense device 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 management center and the threat defense device into sync.

Also, local DNS servers are only retained by the management center if the DNS servers were discovered at initial registration.

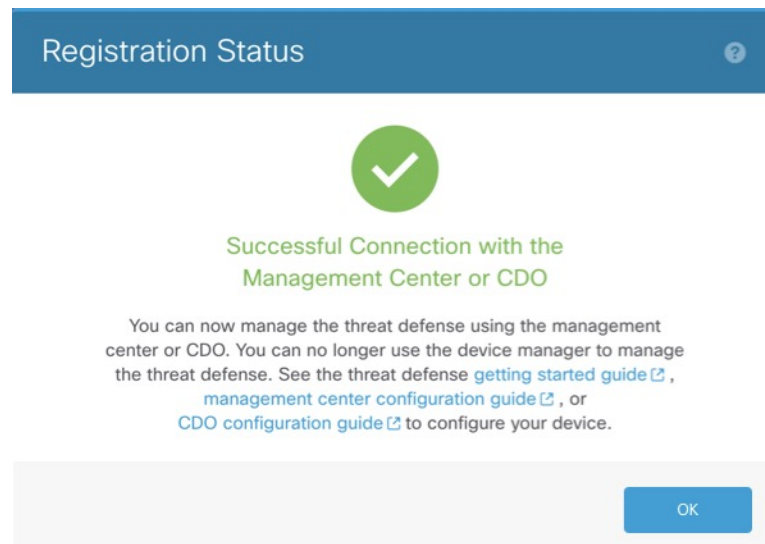
If you intend to choose the Management interface for the **FMC Access Interface**, then this setting configures the Management DNS server.

- c) For the **Management Center/CDO Access Interface**, choose any configured interface.

You can change the manager interface after you register the threat defense device to the management center, to either the Management interface or another data interface.

- Step 8** (Optional) If you chose a data interface, and it was not the outside interface, then add a default route. You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the management center. If you chose the Management interface, then you need to configure the gateway to be a unique gateway before you can proceed on this screen.
- Step 9** (Optional) If you chose a data interface, click **Add a Dynamic DNS (DDNS) method**. DDNS ensures the management center can reach the threat defense device at its Fully-Qualified Domain Name (FQDN) if the IP address changes. See **Device > System Settings > DDNS Service** to configure DDNS. If you configure DDNS before you add the threat defense device to the management center, the threat defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense device can validate the DDNS server certificate for the HTTPS connection. Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (<https://help.dyn.com/remote-access-api/>). DDNS is not supported when using the Management interface for manager access.
- Step 10** Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the management center. After the **Saving Management Center/CDO Registration Settings** step, go to the management center, and add the firewall. If you want to cancel the switch to the management center, click **Cancel Registration**. Otherwise, do not close the device manager browser window until after the **Saving Management Center/CDO Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the device manager. If you remain connected to the device manager after the **Saving Management Center/CDO Registration Settings** step, you will eventually see the **Successful Connection with Management Center or CDO** dialog box, after which you will be disconnected from the device manager.

Figure 8: Successful Connection



Complete the Threat Defense Initial Configuration Using the CLI

Connect to the threat defense 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 manager access, you can use the CLI to configure a data interface instead. You will also configure management center communication settings. When you perform initial setup using the device manager, *all* interface configuration completed in the device manager is retained when you switch to the management center for management, in addition to the Management interface and manager access interface settings. Note that other default configuration settings, such as the access control policy, are not retained.

This procedure applies to all models except for the Firepower 4100/9300. To deploy a logical device and complete initial configuration on the Firepower 4100/9300, see [Logical Devices on the Firepower 4100/9300](#).

Procedure

Step 1 Connect to the threat defense 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 and Secure Firewall hardware models) The console port connects to the FXOS CLI. The SSH session connects directly to the threat defense CLI.

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

(Firepower and Secure Firewall hardware models) 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 threat defense 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.

For Firepower and Secure Firewall hardware, see the [Reimage Procedures](#) in the [Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Threat Defense](#).

For the ISA 3000, see the [Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#).

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 and Secure Firewall hardware models) If you connected to FXOS on the console port, connect to the threat defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4 The first time you log in to the threat defense, 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 [threat defense 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 manager 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:

- **Do you want to configure IPv4?** and/or **Do you want to configure IPv6?**—Enter **y** for at least one of these types of addresses.
- **Enter the IPv4 default gateway for the management interface** and/or **Enter the IPv6 gateway for the management interface**—If you want to use a data interface for manager 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** and/or **Configure IPv6 via DHCP, router, or manually?**—If you want to use a data interface for manager 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 manager access data interface. If you want to use the Management interface for manager 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 the management center. 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 manager 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 configure the network to continue.
 Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
 Do you want to configure IPv4? (y/n) [y]:
 Do you want to configure IPv6? (y/n) [y]: **n**
 Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
 Enter an IPv4 address for the management interface [192.168.45.61]: **10.89.5.17**
 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]: **10.89.5.1**
 Enter a fully qualified hostname for this system [firepower]: **1010-3**
 Enter a comma-separated list of DNS servers or 'none'
 [208.67.222.222,208.67.220.220,2620:119:35::35]:
 Enter a comma-separated list of search domains or 'none' []: **cisco.com**
 If your networking information has changed, you will need to reconnect.
 Disabling IPv6 configuration: management0
 Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
 Setting DNS domains:cisco.com
 Setting hostname as 1010-3
 Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: 10.89.5.1 on management0
 Updating routing tables, please wait...
 All configurations applied to the system. Took 3 Seconds.
 Saving a copy of running network configuration to local disk.
 For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: **no**
 DHCP server is already disabled
 DHCP Server Disabled
 Configure firewall mode? (routed/transparent) [routed]:
 Configuring firewall mode ...

Device is in OffBox mode - disabling/removing port 443 from iptables.
 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 management center that will manage this threat defense.

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

Note If you are using CDO for management, use the CDO-generated **configure manager add** command for this step.

- {hostname | IPv4_address | IPv6_address | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the management center. If the management center is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id*. At least one of the devices, either the management center or the threat defense, must have a reachable IP address to establish the two-way, TLS-1.3-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 management center when you register the threat defense. The registration key must not exceed 37 characters. Valid characters include alphanumeric 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 management center when you register the threat defense when one side does not specify a reachable IP address or hostname. For example, it is required if you set the management center to **DONTRESOLVE**. It is also required if you use the data interface for management, even if you specify IP addresses. The NAT ID must not exceed 37 characters. Valid characters include alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the management center.
- Note** If you use a data interface for management, then you must specify the NAT ID on both the threat defense and management center, even if you specify both IP addresses.
- *display_name*—Provide a display name for showing this manager with the **show managers** command. This option is useful if you are identifying CDO as the primary manager and an on-prem management center for analytics only. If you don't specify this argument, the firewall auto-generates a display name using one of the following methods:
 - *hostname* | *IP_address* (if you don't use the **DONTRESOLVE** keyword)
 - **manager-timestamp**

Example:

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

Example:

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

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

Example:

If the threat defense is behind a NAT device, enter a unique NAT ID along with the management center IP address or hostname, for example:

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

Step 6 If you are using CDO as your primary manager and want to use an on-prem management center for analytics only, identify the on-prem management center.

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

Example:

The following example uses the generated command for CDO with a CDO-generated display name and then specifies an on-prem management center for analytics only with the "analytics-FMC" display name.

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzml1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
> configure manager add 10.70.45.5 regk3y78 natid56 analytics-FMC
Manager successfully configured.
```

Step 7 (Optional) Configure a data interface for manager 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 [Using the Threat Defense Data Interface for Management, on page 4](#).

- 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 threat defense to the management center, the management center 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 the management center, you can later make changes to the manager access interface configuration, but make sure you don't make changes that can prevent the threat defense or management center from re-establishing the management connection. If the management connection is disrupted, the threat defense includes the **configure policy rollback** command to restore the previous deployment.
- If you configure a DDNS server update URL, the threat defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense can validate the DDNS server certificate for the HTTPS connection. The threat defense 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 management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense. When you add the threat defense to the management center, 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 threat defense 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 management center and the threat defense into sync.

Also, local DNS servers are only retained by the management center 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 the management center, including the DNS servers, to match the FTD configuration.

- You can change the management interface after you register the threat defense to the management center, 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 management, 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://dwinchester: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 manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

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

Setting IPv4 network configuration.
Network settings changed.

>

Step 8 (Optional) Limit data interface access to a manager 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 management center.

Configure an Event Interface

You always need a management interface for management traffic. If your device has a second management interface, for example, the Firepower 4100/9300, you can enable it for event-only traffic.

Before you begin

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

Procedure

Step 1 Enable the second management interface as an event-only interface.

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

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

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

Example:

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

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

>

Step 2 Configure the IP address of the event interface.

The event interface can be on a separate network from the management interface, or on the same network.

a) Configure the IPv4 address:

```
configure network ipv4 manual ip_address netmask gateway_ip management1
```

Note that the *gateway_ip* in this command is used to create the default route for the device, so you should enter the value you already set for the management0 interface. It 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 create a static route separately for the event-only interface.

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.
```

```
>
```

b) Configure the IPv6 address:

- Stateless autoconfiguration:

```
configure network ipv6 router management1
```

Example:

```
> configure network ipv6 router management1  
Setting IPv6 network configuration.  
Network settings changed.
```

```
>
```

- Manual configuration:

```
configure network ipv6 manual ip6_address ip6_prefix_length management1
```

Example:

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

```
>
```

Step 3 Add a static route for the event-only interface if the management center is on a remote network; otherwise, all traffic will match the default route through the management interface.

```
configure network static-routes {ipv4 | ipv6} add management1 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 2, on page 25](#)).

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
[...]
```

Add a Device to the Management Center

Use this procedure to add a single device to the management center. If you plan to link devices for high availability, you must still use this procedure; see [Add a High Availability Pair](#). For clustering, see the clustering chapter for your model.

You can also add a cloud-managed device for which you want to use the on-prem management center for event logging and analytics purposes.

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

Before you begin

- Set up the device to be managed by the management center. See:
 - [Complete the Threat Defense Initial Configuration, on page 12](#)
 - The getting started guide for your model
- The management center must be registered to the Smart Software Manager. 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 device using IPv4 and want to convert it 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**.

Figure 9: Add Device

Add Device ?

CDO Managed Device

Host:†

Display Name:

Registration Key:†

Group:

Access Control Policy:†

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Malware
 Threat
 URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

Step 3 If you want to add a cloud-managed device to your on-prem management center for analytics only, check **CDO Managed Device**.

The system hides licensing and packet transfer settings because they are managed by CDO. You can skip those steps.

Figure 10: Add Device for CDO

Step 4 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 management center when you configured the device to be managed by the management center. For more information, see [NAT Environments, on page 6](#).

Note In a management center high availability environment, when both the management centers are behind NAT, to register the device on the secondary management center, you must specify a value in the **Host** field.

Step 5 In the **Display Name** field, enter a name for the device as you want it to display in the management center.

Step 6 In the **Registration Key** field, enter the same registration key that you used when you configured the device to be managed by the management center. The registration key is a one-time-use shared secret. The key can include alphanumeric characters and hyphens (-).

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.

You can also apply licenses after you add the device, from the **System > Licenses > Smart Licenses** page.

For threat defense virtual, you must also select the **Performance Tier**. It's important to choose the tier that matches the license you have in your account. Until you choose a tier, your device defaults to the FTDv50 selection. For more information about the performance-tiered license entitlements available for threat defense virtual, see *FTDv Licenses* in the [Cisco Secure Firewall Management Center Administration Guide](#).

Note If you are upgrading your threat defense virtual to Version 7.0+, you can choose **FTDv - Variable** to maintain your current license compliance.

Step 10 If you used a NAT ID during device setup, in the **Advanced** section enter the same NAT ID in the **Unique NAT ID** field.

The **Unique NAT ID** specifies a unique, one-time string of your choice that you will also specify on the device during initial setup when one side does not specify a reachable IP address or hostname. For example, it is required if you left the **Host** field blank. It is also required if you use the device's data interface for management, even if you specify IP addresses. 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 management center.

Note If you use a data interface on the device for management, then you must specify the NAT ID on both the device and management center, even if you specify both IP addresses.

Step 11 Check the **Transfer Packets** check box to allow the device to transfer packets to the 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 management center for inspection. If you disable it, only event information will be sent to the management center but packet data is not sent.

Step 12 Click **Register**.

It may take up to two minutes for the management center 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 management center 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 management center 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 (Unregister) a Device from the Management Center

If you no longer want to manage a device, you can unregister it from the management center.

To unregister a cluster, cluster node, or high availability pair, see the chapters for those deployments.

Unregistering a device:

- Severs all communication between the management center and the device.
- Removes the device from the **Device Management** page.
- Returns the device to local time management if the device's platform settings policy is configured to receive time from the management center using NTP.
- Leaves the configuration intact, so the device continues to process traffic.

Policies, such as NAT and VPN, ACLs, and the interface configurations remain intact.

Registering the device again to the same or a different management center causes the configuration to be removed, so the device will stop processing traffic at that point.

Before you delete the device, be sure to export the configuration so you can re-apply the device-level configuration (interfaces, routing, and so on) when you re-register it. If you do not have a saved configuration, you will have to re-configure device settings.

After you re-add the device and either import a saved configuration or re-configure your settings, you need to deploy the configuration before it starts passing traffic again.

Before you begin

To re-apply the device-level configuration if you re-add it to the management center:

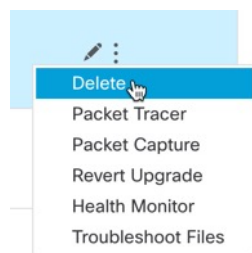
- Export the device configuration. See [Export and Import the Device Configuration, on page 35](#).

Procedure

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

Step 2 Next to the device you want to unregister, click **More** (⋮), and then click **Delete**.

Figure 11: Delete



Step 3 Confirm that you want to unregister the device.

Step 4 You can now change your manager.

- Re-register the device to this management center—If you know the registration key and NAT ID, you can [Add a Device to the Management Center, on page 26](#). If you need to reset them, you can reconfigure the manager as though it's new. See [Identify a New Management Center, on page 76](#).
- Register to a new management center—[Identify a New Management Center, on page 76](#).

- Change to the device manager—[Switch from Management Center to Device Manager, on page 82](#).
- Delete the manager without specifying a new one—To sever the management connection on the threat defense without identifying a new manager (no manager mode), from the threat defense CLI use the **configure manager delete** command.

Add a Device Group

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

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

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** From the **Add** drop-down menu, choose **Add Group**.
- To edit an existing group, click **Edit** (✎) for the group you want to edit.
- Step 3** Enter a **Name**.
- Step 4** Under **Available Devices**, choose one or more devices to add to the device group. Use Ctrl or Shift while clicking to choose multiple devices.
- Step 5** Click **Add** to include the devices you chose in the device group.
- Step 6** Optionally, to remove a device from the device group, click **Delete** (🗑) next to the device you want to remove.
- Step 7** Click **OK** to add the device group.
-

Shut Down or Restart the Device

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

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



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

Procedure

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device that you want to restart, click **Edit** (✎).
- Step 3** Click **Device**.
- Step 4** To restart the device:
- Click **Restart Device** (↺).
 - When prompted, confirm that you want to restart the device.
- Step 5** To shut down the device:
- Click **Shut Down Device** (⊗) in the **System** section.
 - When prompted, confirm that you want to shut down the device.
 - If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. You will see the following prompt:

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

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

Configure Device Settings

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

- **View By**—Use this option to view the devices based on group, licenses, model, or access control policy.
- **Device State**—You can also view the devices based on its state. You can click on a state icon to view the devices belonging to it. The number of devices belonging to the states are provided within brackets.
- **Search**—You can search for a configured device by providing the device name, host name, or the IP address.
- **Add options**—You can add devices, high availability pairs, clusters and groups.
- **Edit and other actions**—Against each configured device, use the **Edit** (✎) icon to edit the device parameters and attributes. Click the **More** (⋮) icon and execute other actions:
 - **Access Control Policy**—Click on the link in the Access Control Policy column to view the policy that is deployed to the device.
 - **Delete**—To unregister the device.
 - **Packet Tracer**—To navigate to the packet tracer page for examining policy configuration on the device by injecting a model packet into the system.

- **Packet Capture**—To navigate to the packet capture page, where, you can view the verdicts and actions the system takes while processing a packet.
- **Revert Upgrade**—To revert the upgrade and configuration changes that were made after the last upgrade. This action results in restoring the device to the version that was before the upgrade.
- **Health Monitor**—To navigate to the device's health monitoring page.
- **Troubleshooting Files**—Generate troubleshooting files, where you can choose the type of data to be included in the report.
- For Firepower 4100/9300 series devices, a link to the chassis manager web interface.

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

Edit General Settings

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

Table 2: General Section Table Fields

Field	Description
Name	The display name of the device on the management center.
Transfer Packets	This displays whether or not the managed device sends packet data with the events to the management center.
Mode	This displays the mode of the management interface for the device: routed or transparent .
Compliance Mode	This displays the security certifications compliance for a device. Valid values are CC, UCAPL and None.
TLS Crypto Acceleration:	Shows whether TLS crypto acceleration is enabled or disabled.
Device Configuration	Lets you copy, export, or import a configuration. See Copy a Configuration to Another Device, on page 34 and Export and Import the Device Configuration, on page 35 .

You can edit some of these settings from this section.

Procedure

-
- Step 1** Choose **Devices > Device Management**.
 - Step 2** Next to the device you want to modify, click **Edit** (✎).
 - Step 3** Click **Device**.
 - Step 4** In the **General** section, click **Edit** (✎).
 - a) Enter a **Name** for the managed device.

- b) Check **Transfer Packets** to allow packet data to be stored with events on the management center.
- c) Click **Force Deploy** to force deployment of current policies and device configuration to the device.

Note Force-deploy consumes more time than the regular deployment since it involves the complete generation of the policy rules to be deployed on the threat defense.

Step 5 For **Device Configuration** actions, see [Copy a Configuration to Another Device, on page 34](#) and [Export and Import the Device Configuration, on page 35](#).

Step 6 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 threat defense devices are the same model and are running the same version of the software.
- The source is either a standalone Secure Firewall Threat Defense device or a Secure Firewall Threat Defense high availability pair.
- The destination device is a standalone threat defense device.
- The source and destination threat defense devices have the same number of physical interfaces.
- The source and destination threat defense devices are in the same firewall mode - routed or transparent.
- The source and destination threat defense devices are in the same security certifications compliance mode.
- The source and destination threat defense devices are in the same domain.
- Configuration deployment is not in progress on either the source or the destination threat defense devices.

Procedure

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

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

Step 3 Click **Device**.

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

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

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

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

Step 6 Click **OK**.

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

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



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

Export and Import the Device Configuration

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

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

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

- Moving the device to a different management center—First delete the device from the original management center, then add the device to the new management center. Then you can import the saved configuration.
- Moving the device between domains—When you move a device between domains, some device-specific configuration is not retained because supporting objects (such as interface groups for security zones) do not exist in the new domain. By importing the configuration after the domain move, any necessary objects are created for that domain, and the device configuration is restored.
- Restore an old configuration—If you deployed changes that negatively impacted the operation of the device, you can import a backup copy of a known working configuration to restore a previous operational state.

- Reregistering a device—If you delete a device from the management center, but then want to add it back, you can import the saved configuration.

See the following guidelines:

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

Table 3: Object Import Action

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

Procedure

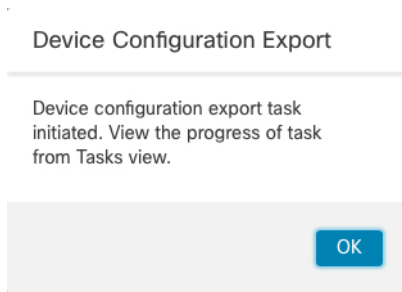
-
- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the device you want to edit, click **Edit** (✎).
- Step 3** Click **Device**.
- Step 4** Export the configuration.
- a) In the **General** area, click **Export**.

Figure 12: Export Device Configuration



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

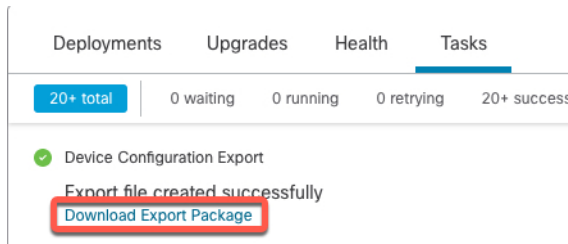
Figure 13: Acknowledge Export



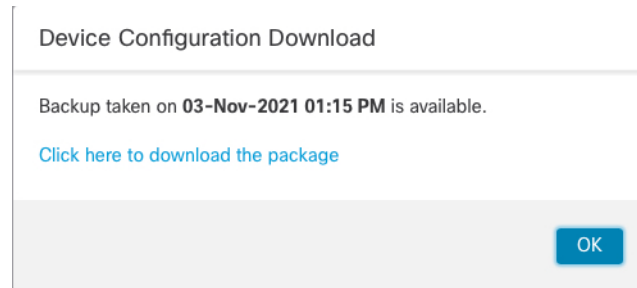
You can view the export progress in the **Tasks** page.

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

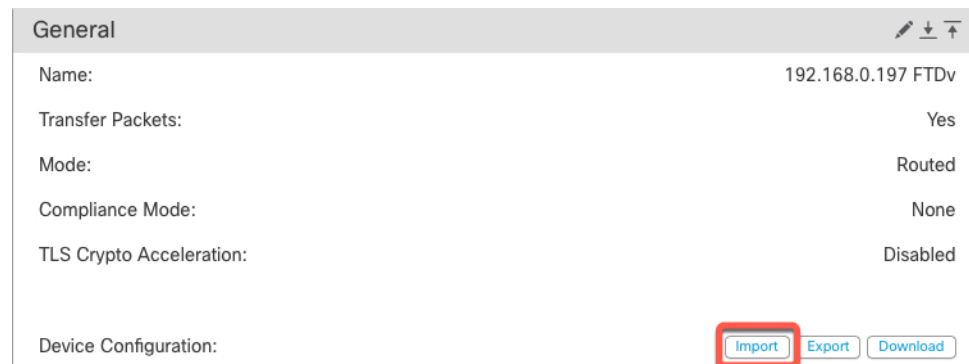
Figure 14: Export Task



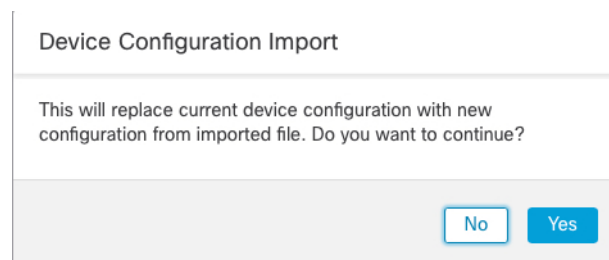
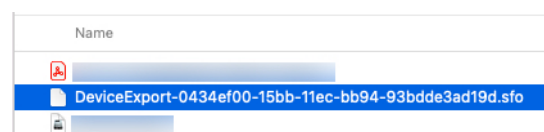
You are prompted to download the package; click **Click here to download the package** to save the file locally, and then click **OK** to exit the dialog box.

Figure 15: Download Package**Step 5** Import the configuration.

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

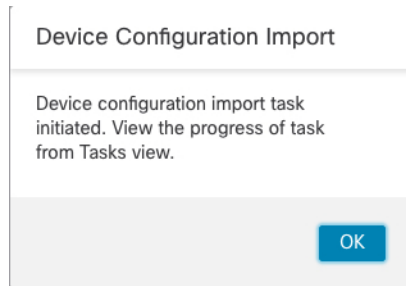
Figure 16: Import Device Configuration

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

Figure 17: Import Package**Figure 18: Navigate to Package**

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

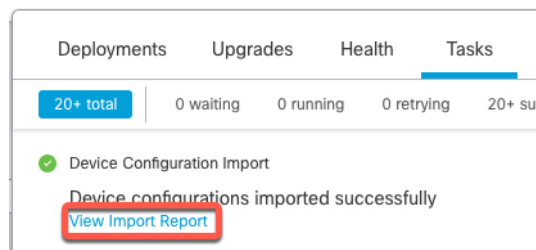
Figure 19: Acknowledge Import



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

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

Figure 20: View Import Report



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

Cisco Firepower Management Center

Device Configuration Import Reports

Device	Shared Policies	Device Configurations
0434ef00-15bb-11ec-bb94-93bde3ad19d	Report does not exist	Device configurations import report

Edit License Settings

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

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

Procedure

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

View System Information

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

You can also shut down or restart the device.

Table 4: System Section Table Fields

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

View the Inspection Engine

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

View Health Information

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

Table 5: 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.

Field	Description
Policy	A link to a read-only version of the health policy currently deployed at the device.
Excluded	A link to the Health Exclude page, where you can enable and disable health exclusion modules.

Edit Management Settings

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

Update the Hostname or IP Address in Management Center

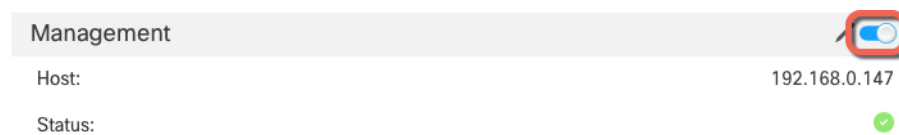
If you edit the hostname or IP address of a device after you added it to the management center (using the device's CLI, for example), you need to use the procedure below to manually update the hostname or IP address on the managing management center.

To change the device management IP address on the device, see [Modify Threat Defense Management Interfaces at the CLI, on page 52](#).

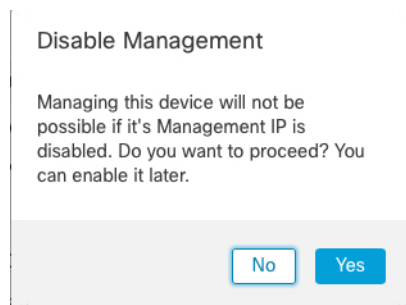
If you used only the NAT ID when registering the device, then the IP shows as **NO-IP** on this page, and you do not need to update the IP address/hostname.

Procedure

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

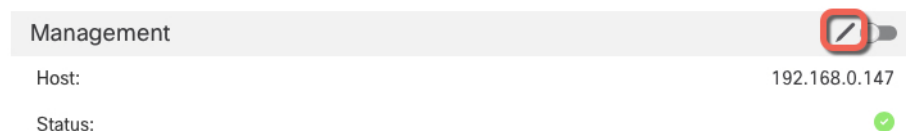


You are prompted to proceed with disabling management; click **Yes**.



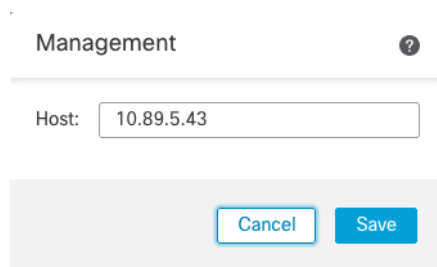
Disabling management blocks the connection between the management center and the device, but does **not** delete the device from the management center.

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 21: Management IP Address



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

Figure 22: Enable Management Connection



Change the Manager Access Interface from Management to Data

You can manage the threat defense from either the dedicated Management interface, or from a data interface. If you want to change the manager access interface after you added the device to the management center, follow these steps to migrate from the Management interface to a data interface. To migrate the other direction, see [Change the Manager Access Interface from Data to Management, on page 45](#).

Initiating the manager access migration from Management to data causes the management center to apply a block on deployment to the threat defense. To remove the block, enable manager access on the data interface.

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

Procedure

Step 1 Initiate the interface migration.

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

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

Figure 23: Manager Access Interface

Manager Access Interface

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

Manage device by
Data Interface

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

Close Save

- c) Click **Save**.

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

Figure 24: Manager Access

Management	
Remote Host Address:	10.10.1.12
Secondary Address:	
Status:	
Manager Access Interface:	Data Interface
Manager Access Details:	Configuration

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

Step 2

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

See [Configure Routed Mode Interfaces](#). You can enable manager access on one routed data interface. 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.
- See [Configure Dynamic DNS](#). DDNS ensures the management center can reach the threat defense at its Fully-Qualified Domain Name (FQDN) if the FTD's IP address changes.
- Step 4** Make sure the threat defense can route to the management center through the data interface; add a static route if necessary on **Devices > Device Management > Routing > Static Route**.
- See [Add a Static Route](#).
- Step 5** (Optional) Configure DNS in a Platform Settings policy, and apply it to this device at **Devices > Platform Settings > DNS**.
- See [DNS](#). DNS is required if you use DDNS. You may also use DNS for FQDNs in your security policies.
- Step 6** (Optional) Enable SSH for the data interface in a Platform Settings policy, and apply it to this device at **Devices > Platform Settings > Secure Shell**.
- See [Secure Shell](#). SSH is not enabled by default on the data interfaces, so if you want to manage the threat defense using SSH, you need to explicitly allow it.
- Step 7** Deploy configuration changes; see [Deploy Configuration Changes](#).
- The management center will deploy the configuration changes over the current Management interface. After the deployment, the data interface is now ready for use, but the original management connection to Management is still active.
- Step 8** At the threat defense CLI (preferably from the console port), set the Management interface to use a static IP address and set the gateway to use the data interfaces.
- ```
configure network {ipv4 | ipv6} manual ip_address netmask data-interfaces
```
- *ip\_address netmask*—Although you do not plan to use the Management interface, you must set a static IP address, for example, a private address so that you can set the gateway to **data-interfaces** (see the next bullet). You cannot use DHCP because the default route, which must be **data-interfaces**, might be overwritten with one received from the DHCP server.
  - **data-interfaces**—This setting forwards management traffic over the backplane so it can be routed through the manager access data interface.
- We recommend that you use the console port instead of an SSH connection because when you change the Management interface network settings, your SSH session will be disconnected.
- Step 9** If necessary, re-cable the threat defense so it can reach the management center on the data interface.
- Step 10** In the management center, disable the management connection, update the **Host** IP address for the threat defense in the **Devices > Device Management > Device > Management** section, and reenabling the connection.
- See [Update the Hostname or IP Address in Management Center, on page 41](#). If you used the threat defense hostname or just the NAT ID when you added the threat defense to the management center, you do not need to update the value; however, you need to disable and reenabling the management connection to restart the connection.
- Step 11** Ensure the management connection is reestablished.
- In the management center, check the management connection status on the **Devices > Device Management > Device > Management > Manager Access - Configuration Details > Connection Status** page.

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

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

**Figure 25: Connection Status**

Manager access - Configuration Details

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

Configuration CLI Output **Connection Status**

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

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

[Close](#)

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 62](#).

## Change the Manager Access Interface from Data to Management

You can manage the threat defense from either the dedicated Management interface, or from a data interface. If you want to change the manager access interface after you added the device to the management center, follow these steps to migrate from a data interface to the Management interface. To migrate the other direction, see [Change the Manager Access Interface from Management to Data, on page 42](#).

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

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

### Procedure

#### Step 1

Initiate the interface migration.

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

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

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

**Figure 26: Manager Access Interface**

- c) Click **Save**.

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

**Figure 27: Manager Access**

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

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

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

- Step 3** If you have not already done so, configure DNS settings for the data interface in a Platform Setting policy, and apply it to this device at **Devices > Platform Settings > DNS**.
- See [DNS](#). The management center deployment that disables manager access on the data interface will remove any local DNS configuration. If that DNS server is used in any security policy, such as an FQDN in an Access Rule, then you must re-apply the DNS configuration using the management center.
- Step 4** Deploy configuration changes; see [Deploy Configuration Changes](#).
- The management center will deploy the configuration changes over the current data interface.
- Step 5** If necessary, re-cable the threat defense so it can reach the management center on the Management interface.
- Step 6** At the threat defense CLI, configure the Management interface IP address and gateway using a static IP address or DHCP.
- When you originally configured the data interface for manager access, the Management gateway was set to data-interfaces, which forwarded management traffic over the backplane so it could be routed through the manager access data interface. You now need to set an IP address for the gateway on the management network.
- Static IP address:**
- ```
configure network {ipv4 | ipv6} manual ip_address netmask gateway_ip
```
- DHCP:**
- ```
configure network {ipv4 | ipv6} dhcp
```
- Step 7** In the management center, disable the management connection, update the **Host** IP address for the threat defense in the **Devices > Device Management > Device > Management** section, and reenables the connection.
- See [Update the Hostname or IP Address in Management Center, on page 41](#). If you used the threat defense hostname or just the NAT ID when you added the threat defense to the management center, you do not need to update the value; however, you need to disable and re-enable the management connection to restart the connection.
- Step 8** Ensure the management connection is reestablished.
- In the management center, check the management connection status on the **Devices > Device Management > Device > Management > Status** field or view notifications in the management center.
- At the threat defense CLI, enter the **sftunnel-status-brief** command to view the management connection status.
- If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 62](#).

---

## View Manager Access Details for Data Interface Management

Model Support—Threat Defense

When you use a data interface for management center management instead of using the dedicated Management interface, you must be careful about changing the interface and network settings for the device in the management center 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 the management center manually. The **Devices > Device Management > Device > Management > Manager Access - Configuration Details** dialog

box helps you resolve any discrepancies between the management center and the threat defense local configuration.

Normally, you configure the manager access data interface as part of initial threat defense setup before you add the threat defense to the management center. When you add the threat defense to the management center, the management center 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 management center.

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

- Deploy to the threat defense. Before the management center deploys, it will detect the configuration differences and stop the deployment.
- The **Sync** button in the **Interfaces** page.
- The **Refresh** button on the **Manager Access - Configuration Details** dialog box.

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

See the following pages on this dialog box.

### Configuration

View the configuration comparison of the manager access data interface on the management center and the threat defense.

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



Manager access - Configuration Details

Manager access configuration on device have been updated outside of Manager. Review the differences and update Manager values accordingly.

[Configuration](#) [CLI Output](#) [Connection Status](#)

Last updated: 2022-09-02 at 20:35:58 UTC [\[ Refresh \]](#)

|                                   | Configuration on Manager | Configuration on Device |
|-----------------------------------|--------------------------|-------------------------|
| 4. Ethernet1/1                    |                          |                         |
| <b>Interface Configuration</b>    |                          |                         |
| FMC Access Enabled                | Disabled                 | Enabled                 |
| FMC Access - Allowed Networks     |                          | any                     |
| Interface Name                    |                          | outside                 |
| IPv4/IPv6 Address                 |                          | 10.89.5.29/26           |
| <b>Static Route Configuration</b> |                          |                         |
| IPv4 Gateway                      |                          | 10.89.5.1               |
| IPv6 Gateway                      |                          |                         |
| 5. Ethernet1/8                    |                          |                         |

Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from manager access interface on next deploy to device.

[Close](#) [Acknowledge](#)

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

Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

[Configuration](#) [CLI Output](#) [Connection Status](#)

Last updated: 2022-09-09 at 07:10:54 UTC [\[ Refresh \]](#)

|                                   | Configuration on Manager   | Configuration on Device    |
|-----------------------------------|----------------------------|----------------------------|
| Web Update Type                   |                            |                            |
| 4. GigabitEthernet0/0             |                            |                            |
| <b>Interface Configuration</b>    |                            |                            |
| FMC Access Enabled                | Enabled                    | Enabled                    |
| FMC Access - Allowed Networks     | any                        | any                        |
| Interface Name                    | outside                    | outside                    |
| IPv4/IPv6 Address                 | 10.89.5.29 255.255.255.192 | 10.89.5.29 255.255.255.192 |
| <b>Static Route Configuration</b> |                            |                            |
| IPv4 Gateway                      |                            | 10.89.5.1                  |
| IPv6 Gateway                      |                            |                            |

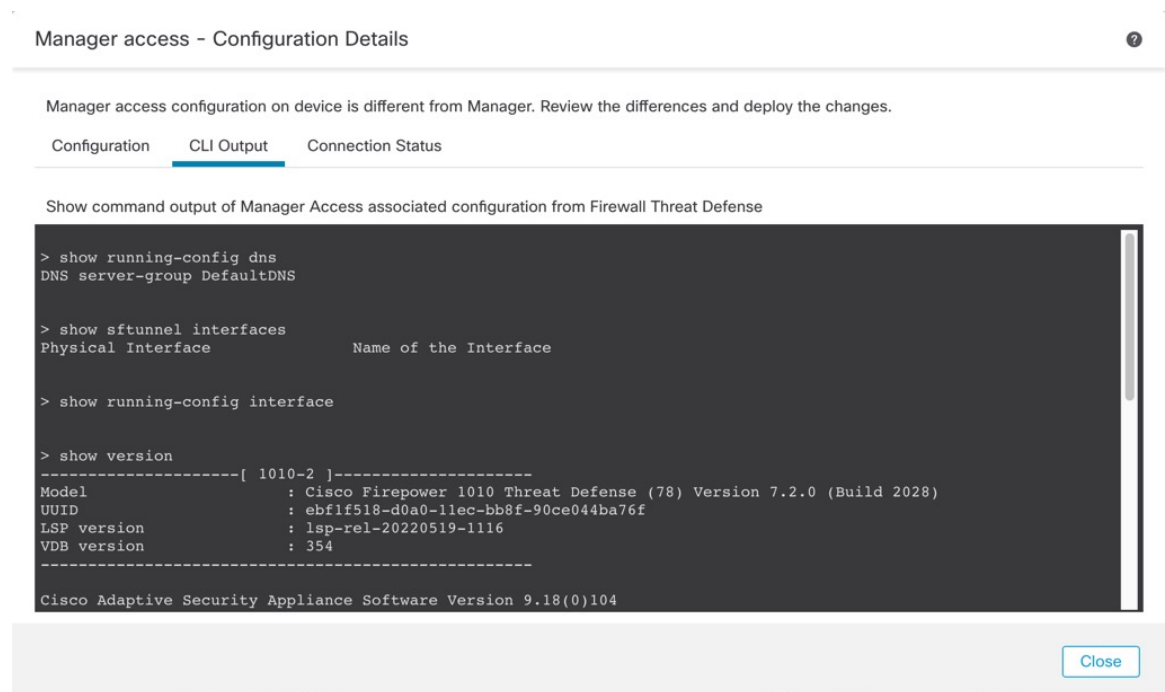
Legend: Above configurations will be ■ added, ■ modified or ■ disassociated from manager access interface on next deploy to device.

[Close](#)

**CLI Output**

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

Figure 28: CLI Output



Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

Configuration **CLI Output** Connection Status

Show command output of Manager Access associated configuration from Firewall Threat Defense

```
> show running-config dns
DNS server-group DefaultDNS

> show sftunnel interfaces
Physical Interface Name of the Interface

> show running-config interface

> show version
-----[1010-2]-----
Model : Cisco Firepower 1010 Threat Defense (78) Version 7.2.0 (Build 2028)
UUID : eb1f518-d0a0-11ec-bb8f-90ce044ba76f
LSP version : lsp-rel-20220519-1116
VDB version : 354

Cisco Adaptive Security Appliance Software Version 9.18(0)104
```

Close

### Connection Status

View management connection status. The following example shows that the management connection is still using the Management "management0" interface.

Figure 29: Connection Status

Manager access - Configuration Details

Manager access configuration on device is different from Manager. Review the differences and deploy the changes.

Configuration CLI Output **Connection Status**

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

```

> sftunnel-status-brief
PEER:10.89.5.35
Peer channel Channel-A is valid type (CONTROL), using 'managemen', connected to '10.89.5.35' via '10.89.5.1'
Peer channel Channel-B is valid type (EVENT), using 'managemen', connected to '10.89.5.35' via '10.89.5.18'
Registration: Completed.
IPv4 Connection to peer '10.89.5.35' Start Time: Tue May 10 21:39:06 2022 UTC
Heartbeat Send Time: Mon May 23 22:46:51 2022 UTC
Heartbeat Received Time: Mon May 23 22:47:53 2022 UTC

```

[Close](#)

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

Figure 30: Connection Status

Manager access - Configuration Details

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

Configuration CLI Output **Connection Status**

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

```

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

```

[Close](#)

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 Threat Defense Management Interfaces at the CLI

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




---

**Note** This topic applies to the dedicated Management interface. You can alternatively configure a data interface for management. If you want to change network settings for that interface, you should do so within management center and not at the CLI. If you need to troubleshoot a disrupted management connection, and need to make changes directly on the threat defense, see [Modify the Threat Defense Data Interface Used for Management at the CLI, on page 58](#).

---

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




---

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

---



**Note** If you change the device management IP address, then see the following tasks for management center connectivity depending on how you identified the management center during initial device setup using the **configure manager add** command (see [Identify a New Management Center, on page 76](#)):

- **IP address—No action.** If you identified the management center using a reachable IP address, then the management connection will be reestablished automatically after several minutes. We recommend that you also change the device IP address shown in management center to keep the information in sync; see [Update the Hostname or IP Address in Management Center, on page 41](#). This action can help the connection reestablish faster. **Note:** If you specified an unreachable management center IP address, then see the procedure for NAT ID below.
- **NAT ID only—Manually reestablish the connection.** If you identified the management center using only the NAT ID, then the connection cannot be automatically reestablished. In this case, change the device management IP address in management center according to [Update the Hostname or IP Address in Management Center, on page 41](#).



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

### Before you begin

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

### Procedure

- Step 1** Connect to the device CLI, either from the console port or using SSH.  
See [Log Into the Command Line Interface on the Device, on page 10](#).
- Step 2** Log in with the Admin username and password.
- Step 3** (Firepower 4100/9300 only) Enable the second management interface as an event-only interface.

```
configure network management-interface enable management1
```

```
configure network management-interface disable-management-channel management1
```

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

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

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

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

**Example:**

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

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

>
```

**Step 4**

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

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

a) Configure the IPv4 address:

- Manual configuration:

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

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

**Example:**

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

```
>
```

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

```
configure network ipv4 dhcp
```

b) Configure the IPv6 address:

- Stateless autoconfiguration:

```
configure network ipv6 router [management_interface]
```

**Example:**

```
> configure network ipv6 router management0
```

```
Setting IPv6 network configuration.
Network settings changed.
```

```
>
```

- Manual configuration:

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

Note that the *ipv6\_gateway\_ip* in this command is used to create the default route for the device. If you configure an event-only interface, then you must enter the *ipv6\_gateway\_ip* as part of the command; however, this entry just configures the default route to the value you specify and does not create a separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you set the *ipv6\_gateway\_ip* for use with the management interface, and then create a static route separately for the event-only interface using the **configure network static-routes** command.

**Example:**

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

```
>
```

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

```
configure network ipv6 dhcp
```

**Step 5**

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

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

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

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

**Example:**

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

**Step 6**

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

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

**Example:**

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

```
>
```

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

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

**Step 7**

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

**configure network static-routes {ipv4 | ipv6} add management\_interface destination\_ip netmask\_or\_prefix gateway\_ip**

For the *default* route, do not use this command; you can only change the default route gateway IP address when you use the **configure network ipv4** or **ipv6** commands (see [Step 4, on page 54](#)).

**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 management center:

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

**Example:**

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

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

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

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

**configure network mtu [*bytes*] [*interface\_id*]**

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

**Example:**

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

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

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

authentication is required, and if it is required, the proxy username, proxy password, and confirmation of the proxy password.

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

### configure network http-proxy

#### Example:

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

#### Step 14

If you change the device management IP address, then see the following tasks for management center connectivity depending on how you identified the management center during initial device setup using the **configure manager add** command (see [Identify a New Management Center, on page 76](#)):

- **IP address—No action.** If you identified the management center using a reachable IP address, then the management connection will be reestablished automatically after several minutes. We recommend that you also change the device IP address shown in management center to keep the information in sync; see [Update the Hostname or IP Address in Management Center, on page 41](#). This action can help the connection reestablish faster. **Note:** If you specified an unreachable management center IP address, then you must manually reestablish the connection using [Update the Hostname or IP Address in Management Center, on page 41](#).
- **NAT ID only—Manually reestablish the connection.** If you identified the management center using only the NAT ID, then the connection cannot be automatically reestablished. In this case, change the device management IP address in management center according to [Update the Hostname or IP Address in Management Center, on page 41](#).

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

If the management connection between the threat defense and the management center was disrupted, and you want to specify a new data interface to replace the old interface, use the threat defense CLI to configure the new interface. This procedure assumes you want to replace the old interface with a new interface on the same network. If the management connection is active, then you should make any changes to an existing data interface using the management center. For initial setup of the data management interface, see the **configure network management-data-interface** command in [Complete the Threat Defense Initial Configuration Using the CLI, on page 18](#).



**Note** This topic applies to the data interface that you configured for Management, not the dedicated Management interface. If you want to change network settings for the Management interface, see [Modify Threat Defense Management Interfaces at the CLI, on page 52](#).

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

### Before you begin

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

### Procedure

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

**Step 2** Connect to the device CLI.

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

See [Log Into the Command Line Interface on the Device, on page 10](#).

**Step 3** Log in with the Admin username and password.

**Step 4** Disable the interface so you can reconfigure its settings.

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

#### Example:

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

Configuration updated successfully..!!
```

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

**Step 5** Configure the new data interface for manager access.

**configure network management-data-interface**

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

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

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

```
Do you wish to clear all the device configuration before applying ? (y/n) [n]: y
```

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

```
Setting IPv4 network configuration.
Network settings changed.
```

```
>
```

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

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

By default, all networks are allowed.

**Step 7** The connection will be reestablished automatically, but disabling and reenabling the connection in the management center will help the connection reestablish faster. See [Update the Hostname or IP Address in Management Center, on page 41](#).

**Step 8** Check that the management connection was reestablished.

```
sftunnel-status-brief
```

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

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

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

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

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

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

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

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

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

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

---

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

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

Alternatively, you can enable auto rollback of the configuration if you lose connectivity after a deployment; see [Edit Deployment Settings, on page 73](#).

See the following guidelines:

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

### Procedure

---

**Step 1** At the threat defense CLI, roll back to the previous configuration.

#### **configure policy rollback**

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

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

**Example:**

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

```
> configure policy rollback

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

Y

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

**Step 2** Check that the management connection was reestablished.

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

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

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 62](#).

## Troubleshoot Management Connectivity on a Data Interface

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

This topic helps you troubleshoot the loss of management connectivity.

### View management connection status

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

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

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

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

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

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

### View the threat defense network information

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

#### show network

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

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

===== [Proxy Information] =====
```

```

State : Disabled
Authentication : Disabled

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

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

```

### Check that the threat defense registered with the management center

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

#### show managers

```

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

```

### Ping the management center

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

#### ping *fmc\_ip*

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

#### ping system *fmc\_ip*

### Capture packets on the threat defense internal interface

At the threat defense CLI, capture packets on the internal backplane interface (nlp\_int\_tap) to see if management packets are being sent:

#### capture *name* interface nlp\_int\_tap trace detail match ip any any

#### show capture*name* trace detail

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

At the threat defense CLI, see information about the internal backplane interface, nlp\_int\_tap:

#### show interface detail



```

> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
 Hardware is en_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 threat defense CLI, check that the default route (S\*) was added and that internal NAT rules exist for the Management interface (nlp\_int\_tap).

### show route

```

> show route

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

Gateway of last resort is 10.89.5.1 to network 0.0.0.0

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

>

```

**show nat**

```
> show nat

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

**Check other settings**

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

**show running-config sftunnel**

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

**show running-config ip-client**

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

**show conn address *fmc\_ip***

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

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

**Check for a successful DDNS update**

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

**debug ddns**

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

```
DDNS: IDB SB total = 0
```

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

```
show crypto ca certificates trustpoint_name
```

To check the DDNS operation:

```
show ddns update interface fmc_access_ifc_name
```

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

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

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


### Check management center log files


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

## View Inventory Details

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

**Figure 31: Inventory Details**

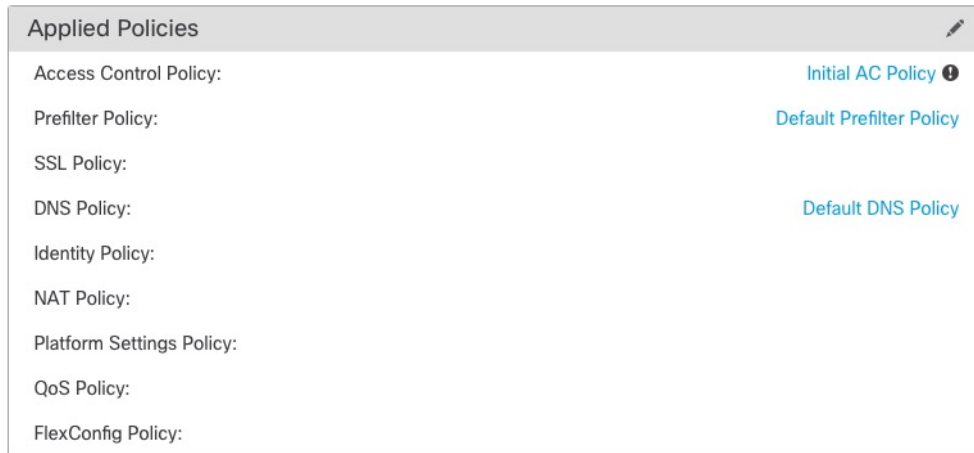
| Inventory Details  |                             |
|---------------------------------------------------------------------------------------------------------|-----------------------------|
| CPU Type:                                                                                               | CPU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

To update information, click **Refresh** .

## Edit Applied Policies

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

Figure 32: Applied Policies



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

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

Figure 33: Access Policy Information for Troubleshooting



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

### Procedure

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

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

**Step 3** Click **Device**.

**Step 4** In the **Applied Policies** section, click **Edit** (✎).

*Figure 34: Policy Assignments*

Policy Assignments

Access Control Policy: Initial AC Policy

NAT Policy: None

Platform Settings Policy: None

QoS Policy: None

FlexConfig Policy: None

Cancel Save

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

**Step 6** Click **Save**.

### What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

## Edit Advanced Settings

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

*Table 6: Advanced Section Table Fields*

| Field              | Description                                                  |
|--------------------|--------------------------------------------------------------|
| Application Bypass | The state of Automatic Application Bypass on the device.     |
| Bypass Threshold   | The Automatic Application Bypass threshold, in milliseconds. |

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

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



**Note** For information about the Transfer Packets setting, see [Edit General Settings, on page 33](#).

## Configure Automatic Application Bypass

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



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

See the following behavior:

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

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

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

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

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

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

### Procedure

---

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

### What to do next

- Deploy configuration changes; see [Deploy Configuration Changes](#).

## Configure Object Group Search

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

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

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



---

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

---

### Before you begin

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

### Procedure

---

- Step 1** Choose **Devices > Device Management**.
- Step 2** Next to the threat defense device where you want to configure the rule, click the **Edit** (✎).
- Step 3** Click the **Device** tab, then click the **Edit** (✎) in the **Advanced Settings** section.
- Step 4** Check **Object Group Search**.
- Step 5** To have object group search work on interface objects in addition to network objects, check **Interface Object Optimization**.
- If you do not select **Interface Object Optimization**, the system deploys separate rules for each source/interface pair, rather than use the security zones and interface groups used in the rules. This means the interface groups are not available for object group search processing.
- Step 6** Click **Save**.
- 

## Configure Interface Object Optimization

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



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



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

**Before you begin**

Model Support—Threat Defense

**Procedure**

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

## Edit Deployment Settings

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

*Figure 35: Deployment Settings*

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

*Table 7: Deployment Settings*

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

You can set deployment settings from the **Device Management** page. Deployment settings include enabling auto rollback of the deployment if the management connection fails as a result of the deployment; specifically if you use data for management center access, and then you misconfigure the data interface. You can alternatively manually roll back the configuration using the **configure policy rollback** command (see [Manually Roll Back the Configuration if the Management Center Loses Connectivity, on page 61](#)).

See the following guidelines:

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

## Procedure

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

*Figure 36: Deployment Settings*

Deployment Settings

Auto Rollback Deployment if Connectivity Fails:

Connectivity Monitor Interval (in Minutes): 20

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

Cancel Save

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

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

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

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

**Figure 37: Rollback Changes**

Change Log: 10.10.35.97

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

Preview Changes | Rollback Changes

Legend: ■ Added ■ Edited ■ Removed

| Changed Policies                                                                                                                                                                                                                                                     | Deployed Version                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | Version on FMC | Modified By |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------|-------------|
| <ul style="list-style-type: none"> <li>Routing               <ul style="list-style-type: none"> <li>Virtual Router (Global)                   <ul style="list-style-type: none"> <li>Static Route IPv4</li> <li>Static Route IPv6</li> </ul> </li> </ul> </li> </ul> | <b>Routing:</b><br><b>Virtual Router: Virtual Router (Global)</b><br><b>Static Route IPv4:</b><br><b>IPv4 Route:</b> admin<br>Static Route Interface(Unchanged): outside outside<br>Static Route Network(Unchanged): any-ipv4 any-ipv4<br>Gateway: literal:10.10.35.63 literal:10.10.35.64<br><b>Static Route IPv6:</b><br><b>IPv6 Route:</b> admin<br>IPv6 Static Route Interface(Unchanged): inside inside<br>IPv6 Static Route Network(Unchanged): any-ipv6 any-ipv6<br>IPv6 Static Route gateway: literal:20::20 literal:20::23 |                |             |

Download as PDF OK

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

**Step 8** Check that the management connection was reestablished.

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

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

If it takes more than 10 minutes to reestablish the connection, you should troubleshoot the connection. See [Troubleshoot Management Connectivity on a Data Interface, on page 62](#).

# Change the Management Settings for the Device

You might need to change the manager, change the manager IP address, or perform other management tasks.

## Edit the Management Center IP Address or Hostname on the Device

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

### Procedure

---

**Step 1** At the threat defense CLI, view the management center identifier.

**show managers**

**Example:**

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

**Step 2** At the threat defense CLI, edit the management center IP address or hostname.

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

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

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

**Example:**

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

---

## Identify a New Management Center

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

## Procedure

---

**Step 1** On the old management center, if present, delete the managed device. See [Delete \(Unregister\) a Device from the Management Center, on page 29](#).

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

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

**Step 3** Configure the new management center.

**configure manager add** {*hostname* | *IPv4\_address* | *IPv6\_address* | **DONTRESOLVE** } *regkey* [*nat\_id*] [*display\_name*]

- {*hostname* | *IPv4\_address* | *IPv6\_address*}—Sets the management center hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE**—If the management center 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 management center, 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 management center 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 management center when you add the threat defense.
- *nat\_id*—Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the management center 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 management center when you add the threat defense.
- *display\_name*—Provide a display name for showing this manager with the **show managers** command. This option is useful if you are identifying CDO as the primary manager and an on-prem management center for analytics only. If you don't specify this argument, the firewall auto-generates a display name using one of the following methods:
  - *hostname* | *IP\_address* (if you don't use the **DONTRESOLVE** keyword)
  - **manager-timestamp**

### 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 management center. See [Add a Device to the Management Center, on page 26](#).

---

## Switch from the Device Manager to the Management Center

When you switch from the device manager to the management center, all interface configuration is retained, in addition to the Management interface and the manager access settings. Note that other configuration settings, such as the access control policy or security zones, are not retained.

After you switch to the management center, you can no longer use the device manager to manage the threat defense device.

### Before you begin

If the firewall is configured for high availability, you must first break the high availability configuration using the device manager (if possible) or the **configure high-availability disable** command. Ideally, break high availability from the active unit.

### Procedure

---

**Step 1** In the device manager, unregister the device from the Cisco Smart Software Manager.

**Step 2** (Might be required) Configure the Management interface.

You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the device manager if you were using the Management interface for the device manager connection.

- Data interface for manager access—The Management interface must have the gateway set to data interfaces. By default, the Management interface receives an IP address and gateway from DHCP. If you do not receive a gateway from DHCP (for example, you did not connect this interface to a network), then the gateway will default to data interfaces, and you do not need to configure anything. If you did receive a gateway from DHCP, then you need to instead configure this interface with a static IP address and set the gateway to data interfaces.
- Management interface for manager access—If you want to configure a static IP address, be sure to also set the default gateway to be a unique gateway instead of the data interfaces. If you use DHCP, then you do not need to configure anything assuming you successfully get the gateway from DHCP.

**Step 3** Choose **Device > System Settings > Central Management**, and click **Proceed** to set up the management center management.

**Step 4** Configure the **Management Center/CDO Details**.

Figure 38: Management Center/CDO Details

### Configure Connection to Management Center or CDO

Provide details to register to the management center/CDO.

Management Center/CDO Details

Do you know the Management Center/CDO hostname or IP address?

Yes  No

**Threat Defense**
**Management Center/CDO**

Management Center/CDO Hostname or IP Address

10.89.5.35

Management Center/CDO Registration Key

••••

NAT ID

*Required when the management center/CDO hostname or IP address is not provided. We recommend always setting the NAT ID even when you specify the management center/CDO hostname or IP address.*

11203

---

Connectivity Configuration

Threat Defense Hostname

1120-3

DNS Server Group

CustomDNSServerGroup

Management Center/CDO Access Interface

Data Interface

Please select an interface

Management Interface [View details](#)

CANCEL
CONNECT

- a) For **Do you know the Management Center/CDO hostname or IP address**, click **Yes** if you can reach the management center using an IP address or hostname, or **No** if the management center is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the management center or the threat defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

- b) If you chose **Yes**, then enter the **Management Center/CDO Hostname/IP Address**.
- c) Specify the **Management Center/CDO Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the management center when you register the threat defense device. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the management center.

- d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the management center. This field is required if you only specify the IP address on one of the devices; but we recommend that you specify the NAT ID even if you know the IP addresses of both devices. 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 management center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked.

#### Step 5 Configure the **Connectivity Configuration**.

- a) Specify the **FTD Hostname**.

If you use a data interface for the **Management Center/CDO Access Interface** access, then this FQDN will be used for this interface.

- b) Specify the **DNS Server Group**.

Choose an existing group, or create a new one. The default DNS group is called **CiscoUmbrellaDNSServerGroup**, which includes the OpenDNS servers.

If you intend to choose a data interface for the **Management Center/CDO Access Interface**, then this setting sets the *data* interface DNS server. The Management DNS server that you set with the setup wizard is used for management traffic. The data DNS server is used for DDNS (if configured) or for security policies applied to this interface. You are likely to choose the same DNS server group that you used for Management, because both management and data traffic reach the DNS server through the outside interface.

On the management center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this threat defense device. When you add the threat defense device to the management center, 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 threat defense device 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 management center and the threat defense device into sync.

Also, local DNS servers are only retained by the management center if the DNS servers were discovered at initial registration.

If you intend to choose the Management interface for the **FMC Access Interface**, then this setting configures the Management DNS server.

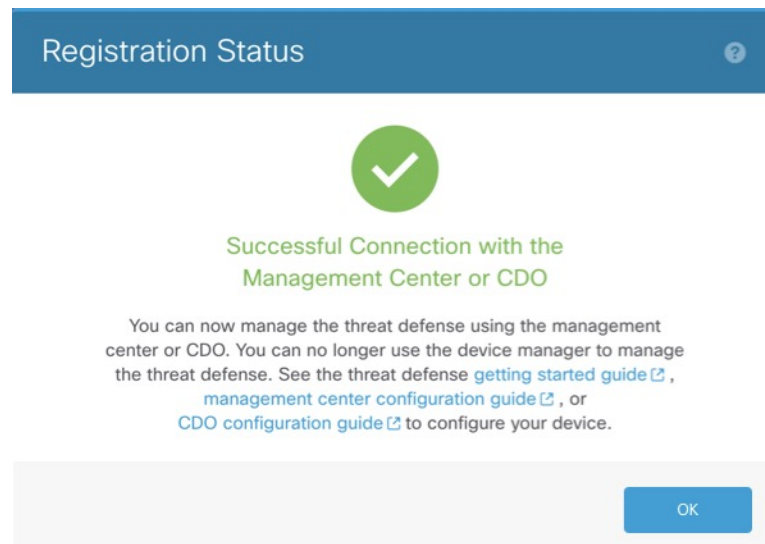
- c) For the **Management Center/CDO Access Interface**, choose any configured interface.

You can change the manager interface after you register the threat defense device to the management center, to either the Management interface or another data interface.



- Step 6** (Optional) If you chose a data interface, and it was not the outside interface, then add a default route. You will see a message telling you to check that you have a default route through the interface. If you chose outside, you already configured this route as part of the setup wizard. If you chose a different interface, then you need to manually configure a default route before you connect to the management center. If you chose the Management interface, then you need to configure the gateway to be a unique gateway before you can proceed on this screen.
- Step 7** (Optional) If you chose a data interface, click **Add a Dynamic DNS (DDNS) method**. DDNS ensures the management center can reach the threat defense device at its Fully-Qualified Domain Name (FQDN) if the IP address changes. See **Device > System Settings > DDNS Service** to configure DDNS. If you configure DDNS before you add the threat defense device to the management center, the threat defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the threat defense device can validate the DDNS server certificate for the HTTPS connection. Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (<https://help.dyn.com/remote-access-api/>). DDNS is not supported when using the Management interface for manager access.
- Step 8** Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the management center. After the **Saving Management Center/CDO Registration Settings** step, go to the management center, and add the firewall. If you want to cancel the switch to the management center, click **Cancel Registration**. Otherwise, do not close the device manager browser window until after the **Saving Management Center/CDO Registration Settings** step. If you do, the process will be paused, and will only resume when you reconnect to the device manager. If you remain connected to the device manager after the **Saving Management Center/CDO Registration Settings** step, you will eventually see the **Successful Connection with Management Center or CDO** dialog box, after which you will be disconnected from the device manager.

*Figure 39: Successful Connection*



## Switch from Management Center to Device Manager

You can configure the threat defense device currently being managed by the on-premises or cloud-delivered management center to use the device manager instead.

You can switch from the management center to the device manager without reinstalling the software. Before switching from the management center to the device manager, verify that the device manager meets all of your configuration requirements. If you want to switch from the device manager to the management center, see [Switch from the Device Manager to the Management Center, on page 78](#).




---

**Caution** Switching to the device manager erases the device configuration and returns the system to the default configuration. However, the Management IP address and hostname are preserved.

---

### Procedure

---

**Step 1** In the management center, delete the firewall from the **Devices > Device Management** page.

**Step 2** Connect to the threat defense CLI using SSH or the console port. For SSH, open a connection to the **management IP address**, and log into the threat defense CLI with the **admin** username (or any other user with admin privileges).

The console port defaults to the FXOS CLI. Connect to the threat defense CLI using the **connect ftd** command. The SSH session connects directly to the threat defense CLI.

If you cannot connect to the management IP address, do one of the following:

- Ensure that the Management physical port is wired to a functioning network.
- Ensure that the management IP address and gateway are configured for the management network. Use the **configure network ipv4/ipv6 manual** command.

**Step 3** Verify you are currently in remote management mode.

**show managers**

**Example:**

```
> show managers
Type : Manager
Host : 10.89.5.35
Display name : 10.89.5.35
Identifier : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration : Completed
```

**Step 4** Delete the remote manager and go into no manager mode.

**configure manager delete uuid**

You cannot go directly from remote management to local management. If you have more than one manager defined, you need to specify the identifier (also known as the UUID; see the **show managers** command). Delete each manager entry separately.

**Example:**

```
> configure manager delete
Deleting task list
Manager successfully deleted.

>
> show managers
No managers configured.
```

**Step 5** Configure the local manager.

#### **configure manager local**

You can now use a web browser to open the local manager at <https://management-IP-address>.

#### **Example:**

```
> configure manager local
Deleting task list

> show managers
Managed locally.
```

---

## Hot Swap an SSD on the Secure Firewall 3100

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

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



---

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

---

### **Procedure**

---

**Step 1** Remove one of the SSDs.

- a) Remove the SSD from the RAID.

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

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

**Example:**

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

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

**show raid**

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

**Example:**

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

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

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

> show raid
Virtual Drive
ID: 1
Size (MB): 858306
Operability: degraded
Presence: equipped
Lifecycle: available
Drive State: degraded
Type: raid
Level: raid1
Max Disks: 2
Meta Version: 1.0
Array State: active
Sync Action: idle
```

```

Sync Completed: unknown
Degraded: 1
Sync Speed: none

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

```

- c) Physically remove the SSD from the chassis.

### Step 2 Add an SSD.

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

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

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

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

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

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

## History for Device Management Basics

| Feature                                                | Minimum Management Center | Minimum Threat Defense | Details                                                                                  |
|--------------------------------------------------------|---------------------------|------------------------|------------------------------------------------------------------------------------------|
| Policy rollback support for high availability devices. | 7.2.0                     | 7.2.0                  | The <b>configure policy rollback</b> command is supported for high availability devices. |

| Feature                                                                      | Minimum Management Center | Minimum Threat Defense | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------|---------------------------|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Multi-manager support.                                                       | 7.2.0                     | 7.2.0                  | <p>We introduced the cloud-delivered management center. The cloud-delivered management center uses the Cisco Defense Orchestrator (CDO) platform and unites management across multiple Cisco security solutions. We take care of manager updates.</p> <p>Hardware or virtual management centers running Version 7.2+ can "co-manage" cloud-managed devices, but for event logging and analytics purposes only. You cannot deploy policy to these devices from the hardware or virtual management center.</p> <p>New/modified commands: <b>configure manager add</b>, <b>configure manager delete</b>, <b>configure manager edit</b>, <b>show managers</b></p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• When you add a cloud-managed device to a hardware or virtual management center, use the new <b>CDO Managed Device</b> check box to specify that it is analytics-only.</li> <li>• View which devices are analytics-only on <b>Devices &gt; Device Management</b>.</li> </ul> <p>For more information, see CDO documentation.</p> |
| Object group search is enabled by default for access control rules.          | 7.2.0                     | 7.2.0                  | <p>The <b>Object Group Search</b> setting is enabled by default for managed devices starting with Version 7.2.0. This option is in the <b>Advanced Settings</b> section when editing device settings on the Device Management page.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Auto rollback of a deployment that causes a loss of management connectivity. | 7.2.0                     | 7.2.0                  | <p>You can now enable auto rollback of the configuration if a deployment causes the management connection between the management center and the threat defense to go down. Previously, you could only manually rollback a configuration using the <b>configure policy rollback</b> command.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• <b>Devices &gt; Device Management &gt; Device &gt; Deployment Settings</b></li> <li>• <b>Deploy &gt; Advanced Deploy &gt; Preview</b></li> <li>• <b>Deploy &gt; Deployment History &gt; Preview</b></li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| RAID support for SSDs on the Secure Firewall 3100.                           | 7.1.0                     | 7.1.0                  | <p>The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID.</p> <p>New/modified commands: <b>configure raid</b>, <b>show raid</b>, <b>show ssd</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Support for TLS 1.3 for the management connection.                           | 7.1.0                     | 7.1.0                  | <p>The FMC-device management connection now uses TLS 1.3. Previously, TLS 1.2 was supported.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Feature                                                                   | Minimum Management Center | Minimum Threat Defense | Details                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---------------------------------------------------------------------------|---------------------------|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Import and export device configurations.                                  | 7.1.0                     | 7.1.0                  | <p>You can export the device-specific configuration, and you can then import the saved configuration for the same device in the following use cases:</p> <ul style="list-style-type: none"> <li>• Moving the device to a different FMC.</li> <li>• Restore an old configuration.</li> <li>• Reregistering a device.</li> </ul> <p>New/modified screens: <b>Devices &gt; Device Management &gt; Device &gt; General</b></p>                                                                                                                                                                                                                                   |
| Use FDM to configure FTD for management by the FMC.                       | 7.1.0                     | 7.1.0                  | <p>When you perform initial setup using FDM, all interface configuration completed in FDM is retained when you switch to FMC for management, in addition to the Management and manager access settings. Note that other default configuration settings, such as the access control policy or security zones, are not retained. When you use the FMC CLI, only the Management and manager access settings are retained (for example, the default inside interface configuration is not retained).</p> <p>After you switch to FMC, you can no longer use FDM to manage FTD.</p> <p>New/modified FDM screens: <b>System Settings &gt; Management Center</b></p> |
| Filter devices by upgrade status.                                         | 6.7.0                     | 6.7.0                  | <p>The <b>Device Management</b> 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.</p> <p>New/modified screens: <b>Devices &gt; Device Management</b></p>                                                                                                                                                                                                                                                                                                                                                           |
| Update the FMC IP address on FTD.                                         | 6.7.0                     | 6.7.0                  | <p>If you change the FMC IP address, you can now use the FTD CLI to update the device.</p> <p>New/modified commands: <b>configure manager edit</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| One-click access to the Firepower Chassis Manager.                        | 6.4.0                     | 6.4.0                  | <p>For Firepower 4100/9300 series devices, the Device Management page provides a link to the Firepower Chassis Manager web interface.</p> <p>New/modified screens: <b>Devices &gt; Device Management</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Filter devices by health and deployment status; view version information. | 6.2.3                     | 6.2.3                  | <p>The Device Management page now provides version information for managed devices, as well as the ability to filter devices by health and deployment status.</p> <p>New/modified screens: <b>Devices &gt; Device Management</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                         |

