Device Registration

You can add and manage devices in the Secure Firewall Management Center.

- About device registration, on page 1
- Prerequisites for device registration, on page 10
- Log Into the Command-Line Interface on the Device, on page 11
- Complete the Firewall Threat Defense Initial Configuration, on page 13
- Manage device registration, on page 28
- Switch Managers, on page 37
- History for device registration, on page 43

About device registration

Register your devices to the Firewall Management Center.

Firewall Management Center overview

This guide applies to an *on-premises* Firewall Management Center, either as your primary manager or as an analytics-only manager. When using the Security Cloud Control Cloud-Delivered Firewall Management Center as your primary manager, you can use an on-prem Firewall Management Center for analytics. Do not use this guide for the Cloud-Delivered Firewall Management Center; see *Cisco Security Cloud Control: Cloud-Delivered Firewall Management Center for Firewall Threat Defense*.

The Firewall Management Center is a powerful, web-based, multi-device manager that runs on its own server hardware, or as a virtual device on a hypervisor. You should use the Firewall Management Center if you want a multi-device manager, and you require all features on the Firewall Threat Defense. The Firewall Management Center also provides powerful analysis and monitoring of traffic and events.

Note If you have a Security Cloud Control-managed device and are using the on-prem Firewall Management Center for analytics only, then the on-prem Firewall Management Center does not support policy configuration or upgrading. Some chapters and procedures in this guide related might not apply to devices whose primary manager is Security Cloud Control.

For the Firewall Management Center used as the primary manager: The Firewall Management Center is not compatible with other managers because the Firewall Management Center owns the Firewall Threat Defense

configuration, and you are not allowed to configure the Firewall Threat Defense directly, bypassing the Firewall Management Center.

About the Firewall Management Center and Device Management

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

By using the Firewall 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 Firewall Management Center

Note If you have a Security Cloud Control-managed device and are using the on-prem Firewall Management Center for analytics only, then the on-prem Firewall 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 Security Cloud Control.

The Firewall 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 Firewall Management Center to manage nearly every aspect of a device's behavior.

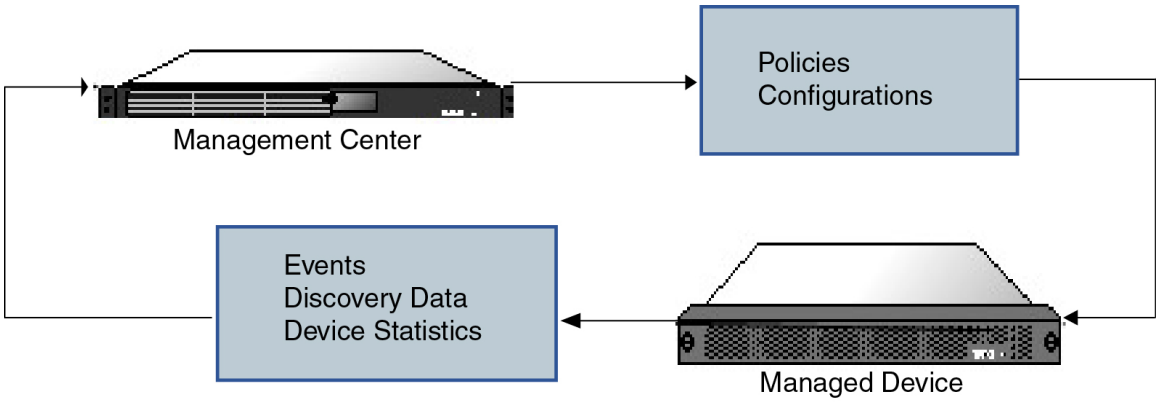
Note Although the Firewall Management Center can manage devices running certain previous releases as specified in the compatibility matrix available at http://www.cisco.com/c/en/us/support/security/defense-center/products-device-support-tables-list.html, new features that require the latest version of Firewall Threat Defense software are not available to these previous-release devices. Some Firewall 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 Firewall Threat Defense devices.

When you manage a device, information is transmitted between the Firewall 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 Firewall 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 Firewall Management Center information and after you add the device to the Firewall Management Center, either the device or the Firewall Management Center can establish the management connection. Depending on initial setup:

- Either the device or the Firewall Management Center can initiate.
- Only the device can initiate.
- Only the Firewall Management Center can initiate.

Initiation always originates with eth0 on the Firewall 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 Firewall 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 5 Mbps throughput. By default, the management connection uses TCP port 8305 (this port is configurable). If you place another Firewall Threat Defense between devices and the Firewall Management Center, to prevent potential management disruption, be sure to exempt management traffic from deep inspection by applying a prefilter policy for it.

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 Firewall 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 Firewall Management Center that is managing the device.

To back up event data, perform a backup of the Firewall 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 Firewall 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 Firewall 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 Firewall Threat Defense

When you set up your device, you specify the Firewall 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 Firewall Management Center is not known, then the Firewall Management Center establishes the initial connection. In this case, it might initially connect from a different Firewall Management Center management interface than specified on the Firewall Threat Defense. Subsequent connections should use the Firewall Management Center management interface with the specified IP address.

If the Firewall Management Center has a separate event-only interface, the managed device sends subsequent event traffic to the Firewall 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 Firewall Management Center and/or on the managed device. If the device management interface is down, the eventing interface will be used to establish the management connection, even if you disable management traffic for it.

Using the Firewall Threat Defense Data Interface for Management

You can use either the dedicated Management interface or a regular data interface for communication with the Firewall Management Center. Manager access on a data interface is useful if you want to manage the Firewall 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, nor can you create a subinterface on the manager access interface.
- 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 Firewall 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 Firewall 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 Firewall 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 Firewall 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 Firewall Threat Defense logical device.

Note For the Firewall 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 Firewall Management Center, and the Management logical interface for the Firewall Management Center communication. See Management/Diagnostic Interface for more information.

For devices with Management and Eventing interfaces, if one interface is down, the other interface will be used as backup for management or eventing even if you disable that function for the interface.

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
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 Firewall 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 Firewall 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.

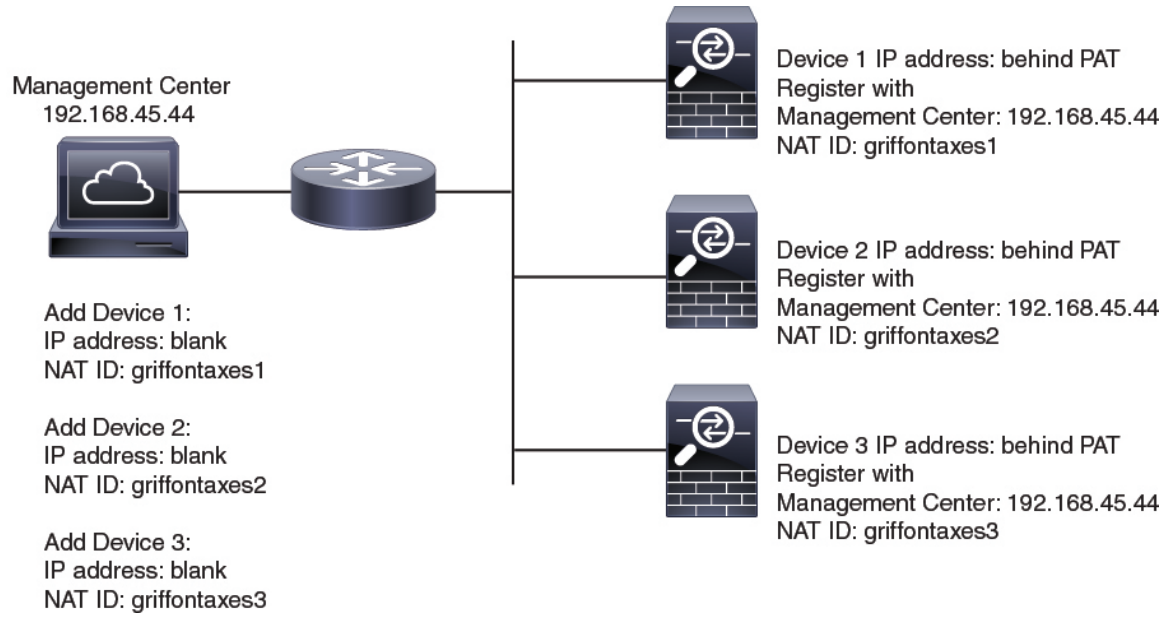
Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the Firewall Management Center specifies the device IP address when you add a device, and the device specifies the Firewall Management Center IP address. However, if you only know one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

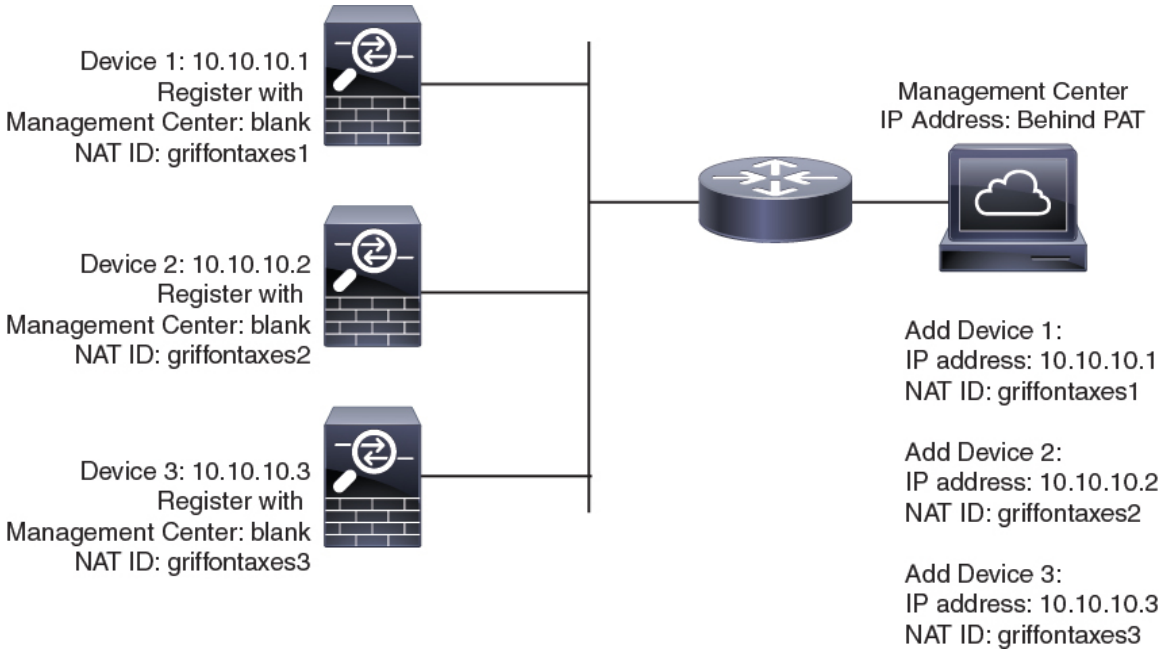
The following example shows three devices behind a PAT IP address. In this case, specify a unique NAT ID per device on both the Firewall Management Center and the devices, and specify the Firewall Management Center IP address on the devices.

Figure 1: NAT ID for Managed Devices Behind PAT



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

Figure 2: NAT ID for Firewall Management Center Behind PAT

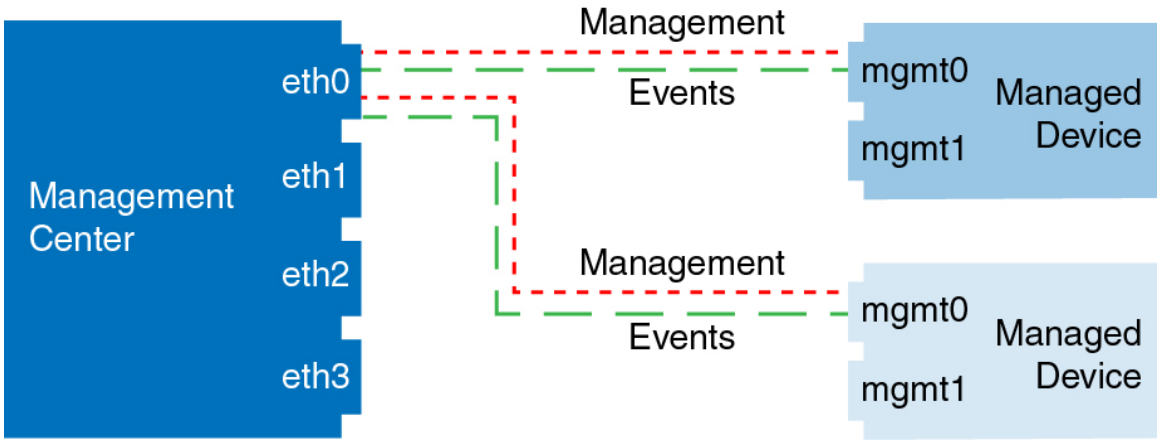


Management and Event Traffic Channel Examples

Note If you use a data interface for management on a Firewall Threat Defense, you cannot use separate management and event interfaces for that device.

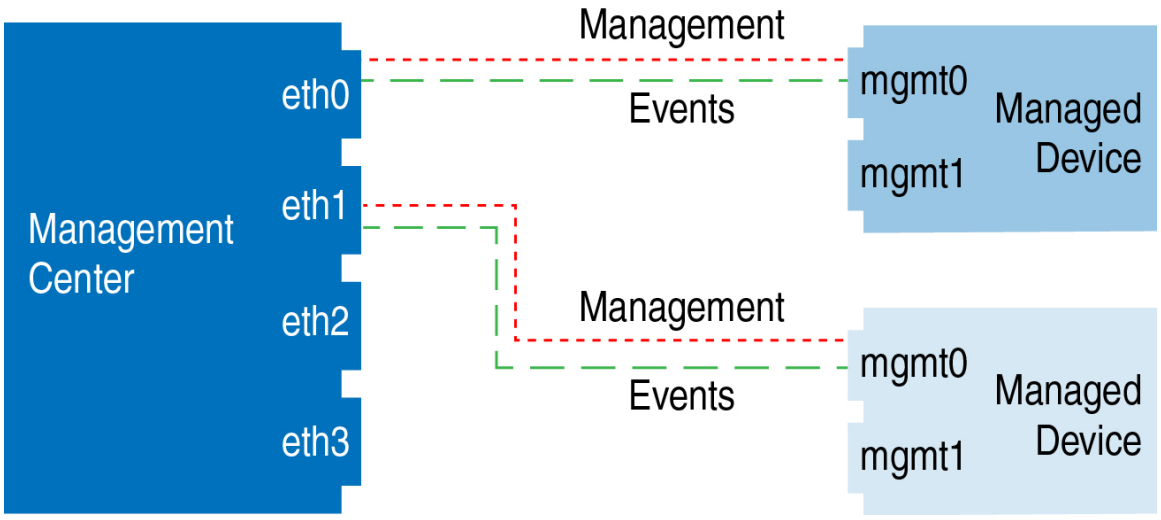
The following example shows the Firewall Management Center and managed devices using only the default management interfaces.

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



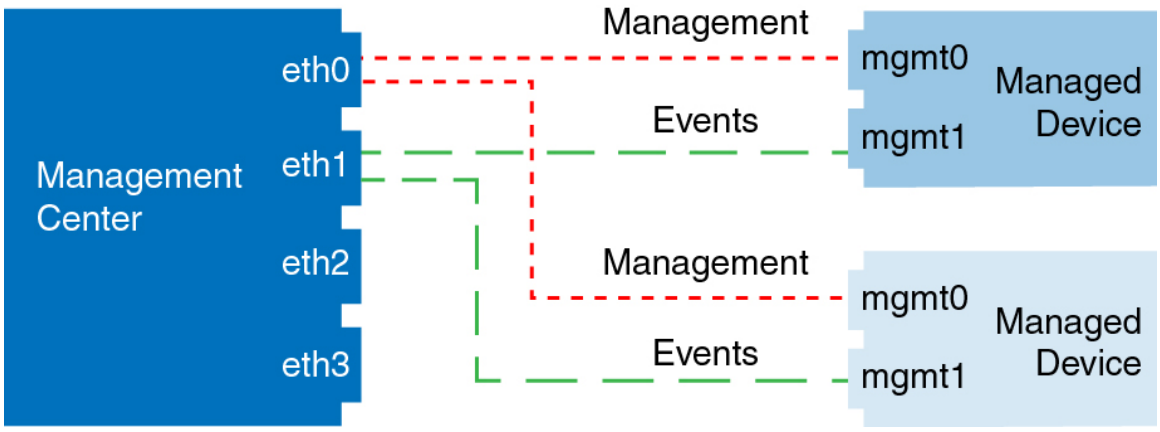
The following example shows the Firewall Management Center using separate management interfaces for devices; and each managed device using 1 management interface.

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



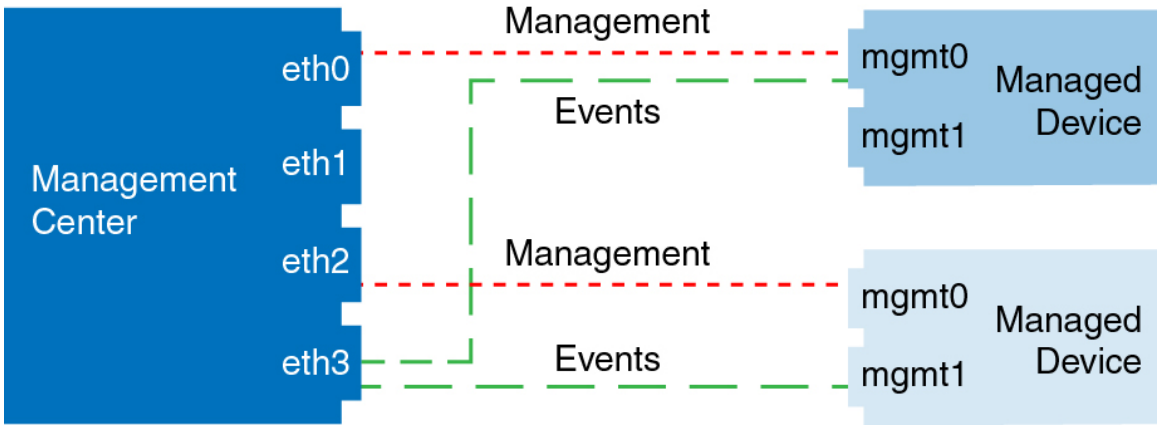
The following example shows the Firewall Management Center and managed devices using a separate event interface.

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 Firewall 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



Prerequisites for device registration

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.

Zero-Touch Provisioning requirements

Zero-Touch Provisioning is not supported with clustering or multi-instance mode.

High availability is only supported when you use the Management interface because zero-touch provisioning uses DHCP, which is not supported for data interfaces and high availability.

Zero-Touch Provisioning is supported on the following models using 7.4 or later:

- Firepower 1010
- Firepower 1100
- Secure Firewall 1200
- Firepower 2100 (on supported device versions)
- Secure Firewall 3100

Log Into the Command-Line Interface on the Device

You can log directly into the command-line interface on Firewall Threat Defense devices. If this is your first time logging in, complete the initial setup process using the default **admin** user; see Complete the Firewall Threat Defense Initial Configuration Using the CLI, on page 19.

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.
- If you get unreadable characters when connecting to the console port, verify the port settings. If they are correct, try the cable with another device using the same settings. If the cable is good, you might need to replace the hardware for the console port. Also consider trying a different workstation to make the connection.

Procedure

Step 1 Connect to the Firewall Threat Defense CLI, either from the console port or using SSH.

You can SSH to the management interface of the Firewall 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 Firewall Threat Defense CLI). Use the Firewall 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 Firewall 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 Firewall 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 submodes: user EXEC mode, privileged EXEC mode. More commands are available in privileged EXEC mode than user 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 Firewall Threat Defense Initial Configuration

You can complete the Firewall Threat Defense initial configuration using the CLI or the Firewall 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 Firewall Threat Defense Initial Configuration Using the Firewall Device Manager

When you use the Firewall Device Manager for initial setup, the following interfaces are preconfigured in addition to the Management interface and manager access settings:

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration
- Ethernet 1/2 (or for the 1010), the VLAN1 interface)— "inside", 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

If you perform additional interface-specific configuration within Firewall Device Manager before registering with the Firewall Management Center, then that configuration is preserved.

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 Security Cloud Control-managed devices for which you want to use an on-prem Firewall Management Center *for analytics only*. The Firewall Device Manager configuration is meant to configure the primary manager. See Complete the Firewall Threat Defense Initial Configuration Using the CLI, on page 19 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 Firewall Device Manager to onboard these devices to the Firewall 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 Firewall 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 Firewall 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 Firewall 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 Firewall Threat Defense with the Smart Software Manager; all licensing is performed on the Firewall Management Center.

d) Click **Finish**.

e) You are prompted to choose **Cloud Management** or **Standalone**. For Firewall 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 Firewall Device Manager if you were using the Management interface for the Firewall 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.

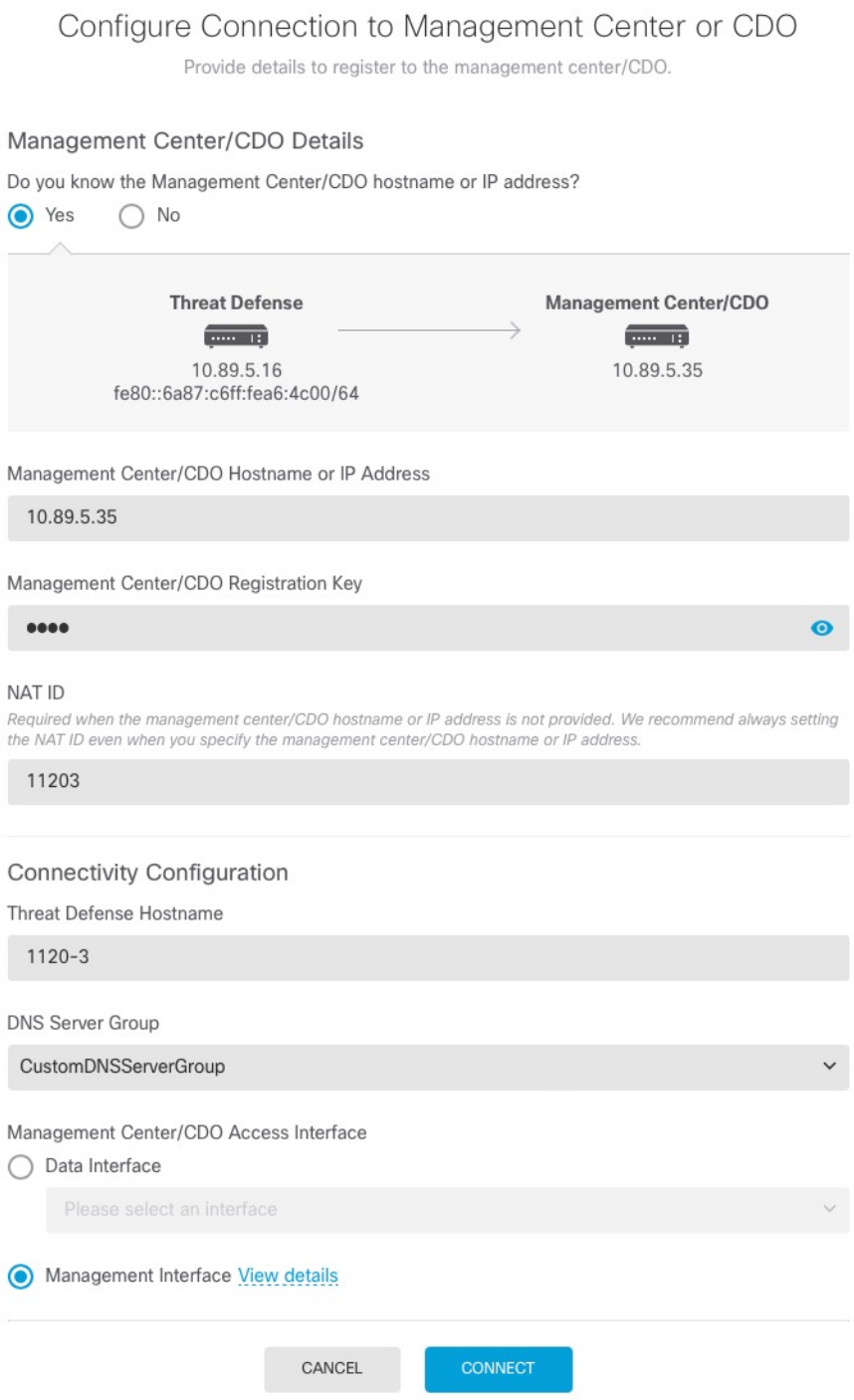
Step 4 If you want to configure additional interfaces, including an interface other than outside or inside that you want to use for manager access, choose **Device**, and then click the link in the **Interfaces** summary.

Other Firewall Device Manager configuration will not be retained when you register the device to Firewall Management Center.

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

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

Figure 7: Management Center/Security Cloud Control Details



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

At least one of the devices, either the Firewall Management Center or the Firewall 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 or 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 Firewall Management Center when you register the Firewall Threat Defense device. The registration key must be between 2 and 36 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 Firewall Management Center.

a) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the Firewall Management Center. The NAT ID must be between 2 and 36 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 Firewall 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. We recommended that you always use the NAT ID even when it is optional, but it is required if:

- You set the Firewall Management Center IP address to **DONTRESOLVE**.
- When adding the device on the Firewall Management Center, you do not specify a reachable device IP address or hostname.
- You use the data interface for management, even if you specify IP addresses on both sides.
- The Firewall Management Center uses multiple management interfaces.

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 Firewall Management Center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense device. When you add the Firewall Threat Defense device to the Firewall 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 Firewall 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 Firewall Management Center and the Firewall Threat Defense device into sync.

Also, local DNS servers are only retained by the Firewall Management Center if the DNS servers were discovered at initial registration.

If you intend to choose the Management interface for the **Management Center/CDO Access InterfaceFMC 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 Firewall Threat Defense device to the Firewall 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 Firewall 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 Firewall Management Center can reach the Firewall 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 Firewall Threat Defense device to the Firewall Management Center, the Firewall Threat Defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense device can validate the DDNS server certificate for the HTTPS connection. Firewall Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

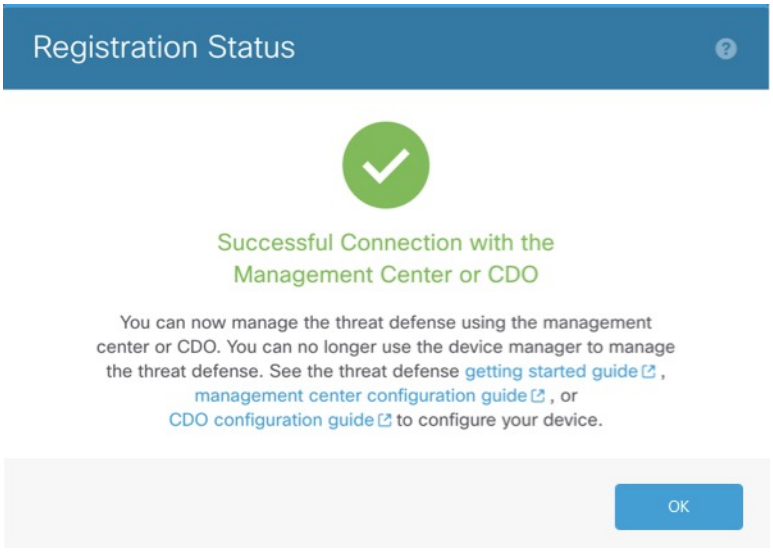
DDNS is not supported when using the Management interface for manager access.

Step 10 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the Firewall Management Center. After the **Saving Management Center/CDO Registration Settings** step, go to the Firewall Management Center, and add the firewall.

If you want to cancel the switch to the Firewall Management Center, click **Cancel Registration**. Otherwise, do not close the Firewall 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 Firewall Device Manager.

If you remain connected to the Firewall Device Manager after the **Saving Management Center/CDO Registration Settings** step, you will eventually see the **Successful Connection with Management Center/CDO** dialog box, after which you will be disconnected from the Firewall Device Manager.

Figure 8: Successful Connection



Complete the Firewall Threat Defense Initial Configuration Using the CLI

Connect to the Firewall 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 Firewall Management Center communication settings. When you perform initial setup using the Firewall Device Manager, *all* interface configuration completed in the Firewall Device Manager is retained when you switch to the Firewall 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 Firewall 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.

The console port connects to the FXOS CLI. The SSH session connects directly to the Firewall Threat Defense CLI. The exception is for the ISA 3000, where the console connection connects to the Firewall Threat Defense CLI.

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

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 Firewall 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 Firewall Threat Defense .

For the ISA 3000, see the Cisco Secure Firewall ASA and 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 If you connected to FXOS on the console port, connect to the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 4 The first time you log in to the Firewall 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. Make sure this interface is on a different subnet from the manager access interface to prevent routing issues. 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 Firewall Management Center. A **yes** answer means you will use Secure Firewall 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:
Cisco General Terms
[...]

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 Firewall Management Center that will manage this Firewall Threat Defense.

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

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

- {*hostname* | *IPv4_address* | *IPv6_address* | **DONTRESOLVE**}—Specifies either the FQDN or IP address of the Firewall Management Center. If the Firewall Management Center is not directly addressable, use **DONTRESOLVE** and also specify the *nat_id*. At least one of the devices, either the Firewall Management Center or the Firewall 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 Firewall Threat Defense 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 Firewall Management Center when you register the Firewall Threat Defense. The registration key must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense. The NAT ID must be between 2 and 36 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 Firewall 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. We recommended that you always use the NAT ID even when it is optional, but it is required if:

- You set the Firewall Management Center IP address to **DONTRESOLVE**.
- When adding the device on the Firewall Management Center, you do not specify a reachable device IP address or hostname.
- You use the data interface for management, even if you specify IP addresses on both sides.
- The Firewall Management Center uses multiple management interfaces.

- *display_name*—Provide a display name for showing this manager with the **show managers** command. This option is useful if you are identifying Security Cloud Control as the primary manager and an on-prem Firewall 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 Firewall 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 Firewall Threat Defense is behind a NAT device, enter a unique NAT ID along with the Firewall 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 Security Cloud Control as your primary manager and want to use an on-prem Firewall Management Center for analytics only, identify the on-prem Firewall 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 Security Cloud Control with a Security Cloud Control-generated display name and then specifies an on-prem Firewall Management Center for analytics only with the "analytics-FMC" display name.

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb 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

After pressing **Enter**, 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 Firewall Threat Defense Data Interface for Management, on page 5.

- 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. Make sure this interface is on a different subnet from the manager access interface to prevent routing issues. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- When you add the Firewall Threat Defense to the Firewall Management Center, the Firewall 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 Firewall 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 Firewall Threat Defense or Firewall Management Center from re-establishing the management connection. If the management connection is disrupted, the Firewall Threat Defense includes the **configure policy rollback** command to restore the previous deployment.
- DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense at its Fully-Qualified Domain Name (FQDN) if the IP address changes. If you configure a DDNS server update URL, the Firewall Threat Defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense can validate the DDNS server certificate for the HTTPS connection. The Firewall 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 Firewall Management Center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense. When you add the Firewall Threat Defense to the Firewall 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 Firewall 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 Firewall Management Center and the Firewall Threat Defense into sync.

  Also, local DNS servers are only retained by the Firewall 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 Firewall Management Center, including the DNS servers, to match the FTD configuration.
- You can change the management interface after you register the Firewall Threat Defense to the Firewall 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 Firewall 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 Firewall 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. Similarly, if the management interface is down, the event-only interface will be used for management as a backup.

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 Firewall Management Center is on a remote network; otherwise, all traffic will match the default route through the management interface.

configure network static-routes {**ipv4** | **ipv6**} **add 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 26).

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
```

[...]

Manage device registration

Register and unregister devices to the Firewall Management Center.

About the Device Management Page

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

- **View By**—View devices based on group, licenses, model, or access control policy.
- **Device State**—View devices based on state (**Error**, **Warning**, etc.). 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 Device**—Search for a device by device name, host name, or IP address.
- **Add**—Add devices and other manageable components.
- Columns—Click the column head to sort by that column.
  - **Name**
  - **Model**
  - **Version**
  - **Chassis**—For supported models, click **Manage** to bring up the integrated Chassis Manager. For the Firepower 4100/9300, the link cross-launches the Firewall Chassis Manager.
  - **Licenses**
  - **Access Control Policy**—Click on the link in the Access Control Policy column to view the policy that is deployed to the device.
  - **Auto-Rollback**—Shows whether auto-rollback of the configuration is enabled ( ) or disabled) if the deployment causes the management connection to go down. See Edit Deployment Settings.
- **Edit**—For each device, use the **Edit** ( ) icon to edit the device settings.

  You can also just click on the device name or IP address.
- **More**—For each device, click the **More** ( ) icon to execute other actions:
  - **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.
- **Troubleshoot Files**—Generate troubleshooting files, where you can choose the type of data to be included in the report.

Add a Device Group

The Firewall 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.

Groups are not supported in a multidomain environment.

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.

Register With the Management Center

The Firewall Management Center offers multiple methods to register your devices.

Add a Device

Use this procedure to add a single device to the Firewall 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 use this procedure to add a device that is managed by a Cloud-Delivered Firewall Management Center, and you want to use the on-prem Firewall Management Center for event logging and analytics purposes only.

If you use Firewall Management Center high availability, add devices *only* to the active Firewall Management Center. Devices registered to the active Firewall Management Center are automatically registered to the standby.

Before you begin

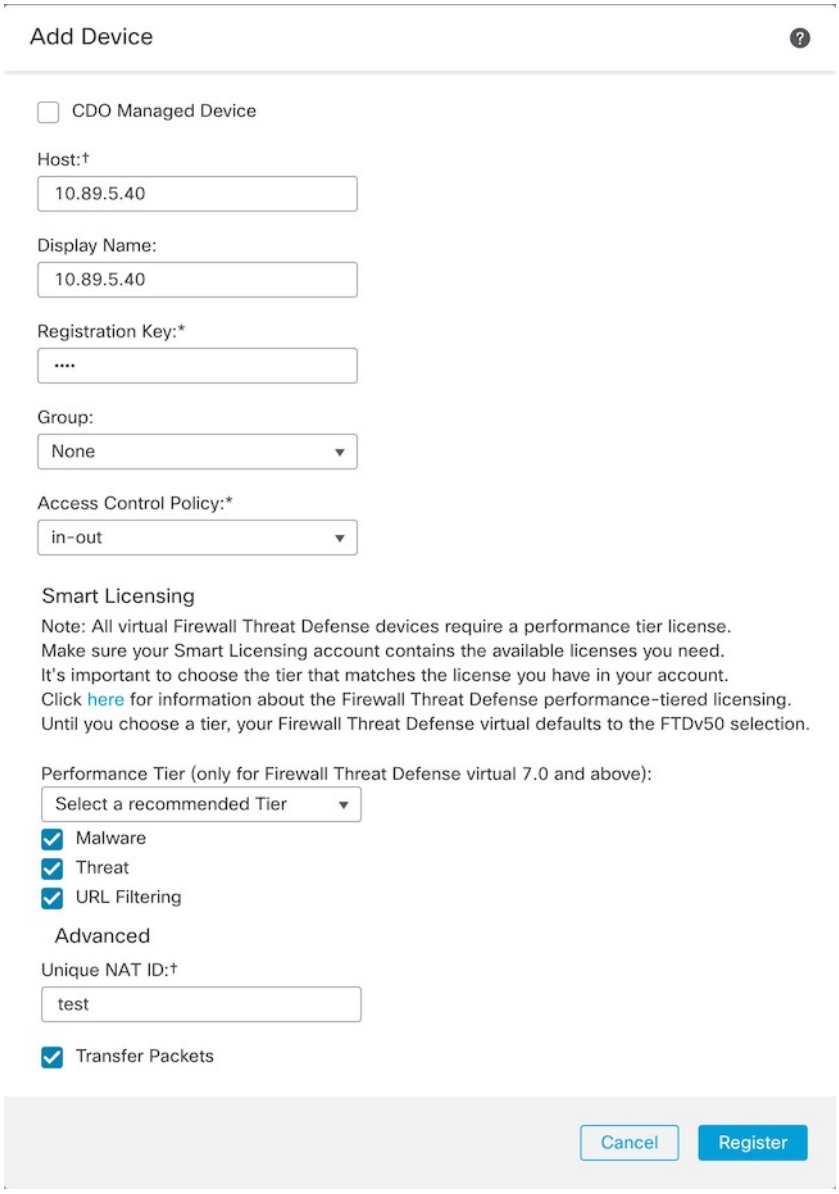
- Set up the device to be managed by the Firewall Management Center. See:
  - Complete the Firewall Threat Defense Initial Configuration, on page 13
  - The getting started guide for your model
- The Firewall Management Center must be registered to the Smart Software Manager. A valid evaluation license 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**.

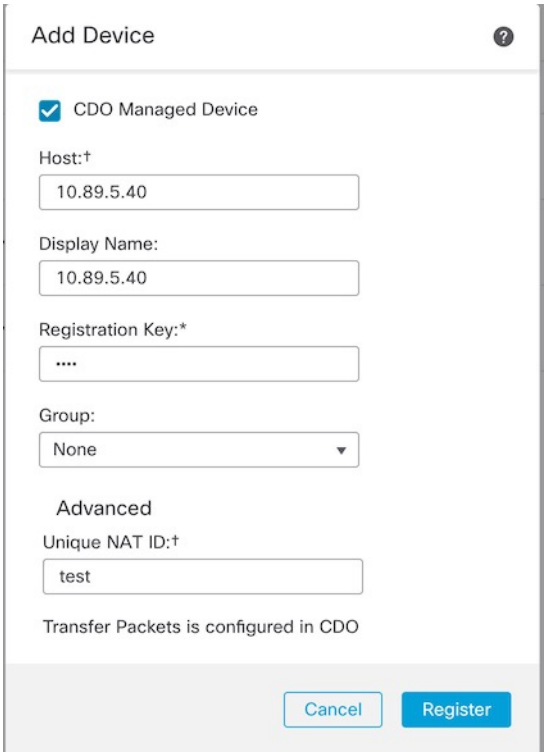
Figure 9: Add Device



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

The system hides licensing and packet transfer settings because they are managed by Security Cloud Control (formerly CDO). You can skip those steps.

Figure 10: Add Device for Security Cloud Control



Step 4 For the **Host**, enter the IP address or the hostname of the device you want to add. Leave this field blank if you don't know the device IP address (for example, it's behind NAT).

If you leave this field blank, the initial configuration on the device needs to include a reachable Firewall Management Center IP address or hostname plus the NAT ID. For more information, see NAT Environments, on page 7.

Step 5 For the **Display Name**, enter a name for the device as you want it to display in the Firewall Management Center. You cannot change this name later.

Step 6 For the **Registration Key**, enter the same registration key in your initial configuration. The registration key is a one-time-use shared secret. The key can be up to 37-characters in length and include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). The registration key does not need to be unique per device.

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

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

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

Step 9 Choose licenses to apply to the device.

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

For Firewall 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 Firewall Threat Defense Virtual, see *FTDv Licenses* in the *Cisco Secure Firewall Management Center Administration Guide*.

Note
If you are upgrading your Firewall Threat Defense Virtual to Version 7.0+, you can choose **FTDv - Variable** to maintain your current license compliance.

Step 10 If you specified a NAT ID during initial configuration, in the **Advanced** section enter the same NAT ID for the **Unique NAT ID**.

The **Unique NAT ID** specifies a unique, one-time string of your choice that you will also specify on the device during initial configuration. It is required when one side does not specify a reachable IP address or hostname, for example if you left the **Host** field blank. Although technically optional, we recommend always specifying the NAT ID even when you know the IP addresses of both sides because it is required in certain situations. The ID can be up to 37-characters in length and include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the Firewall Management Center.

Step 11 Check **Transfer Packets** so that for each intrusion event, the device transfers the packet to the Firewall Management Center for inspection.

This option is enabled by default. For each intrusion event, the device sends event information and the packet that triggered the event to the Firewall Management Center for inspection. If you disable it, only event information will be sent to the Firewall Management Center; the packet will not be sent.

Step 12 Click **Register**.

It may take up to two minutes for the Firewall 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 Firewall 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 Firewall 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.

Register With a New Management Center

This procedure shows how to register with a new Firewall Management Center. You should perform these steps even if the new Firewall Management Center uses the old Firewall Management Center's IP address.

Procedure

Step 1 On the old Firewall Management Center, if present, delete the managed device. See Delete (Unregister) a Device from the Firewall Management Center, on page 35.

You cannot change the Firewall Management Center IP address if you have an active connection with the Firewall Management Center.

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

Step 3 Configure the new Firewall Management Center.

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

- {*hostname* | *IPv4_address* | *IPv6_address*}—Sets the Firewall Management Center hostname, IPv4 address, or IPv6 address.
- **DONTRESOLVE**—If the Firewall 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 Firewall 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 Firewall 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 Firewall Management Center when you add the Firewall Threat Defense.
- *nat_id*—Make up an alphanumeric string from 1 to 37 characters used only during the registration process between the Firewall 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 Firewall Management Center when you add the Firewall 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 Security Cloud Control as the primary manager and an on-prem Firewall 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 Firewall Management Center.

Delete (Unregister) a Device from the Firewall Management Center

If you no longer want to manage a device, you can unregister it from the Firewall 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 Firewall 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 Firewall 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 Firewall 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 Firewall Management Center:

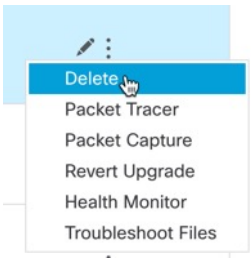
- Export the device configuration. See Export and Import the Device Configuration.

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 Firewall Management Center—If you know the registration key and NAT ID, refer to Add a Device, on page 29. If you need to reset them, you can reconfigure the manager as though it's new. See Register With a New Management Center, on page 33.
- Register to a new Firewall Management Center—Register With a New Management Center, on page 33.
- Change to the Firewall Device Manager—Switch from Firewall Management Center to Firewall Device Manager, on page 41.
- Delete the manager without specifying a new one—To sever the management connection on the Firewall Threat Defense without identifying a new manager (no manager mode), from the Firewall Threat Defense CLI use the **configure manager delete** command.

Shut Down or Restart the Device

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

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

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

Procedure

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

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

Step 3 Click **Device**.

Step 4 To restart the device:

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

Step 5 To shut down the device:

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

```
System is stopped.
```

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

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

Switch Managers

You can change between managers if needed.

Switch from the Firewall Device Manager to the Firewall Management Center

When you switch from the Firewall Device Manager to the Firewall 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 Firewall Management Center, you can no longer use the Firewall Device Manager to manage the Firewall Threat Defense device.

Before you begin

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

Procedure

Step 1 In the Firewall Device Manager, unregister the device from the Cisco Smart Software Manager.

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

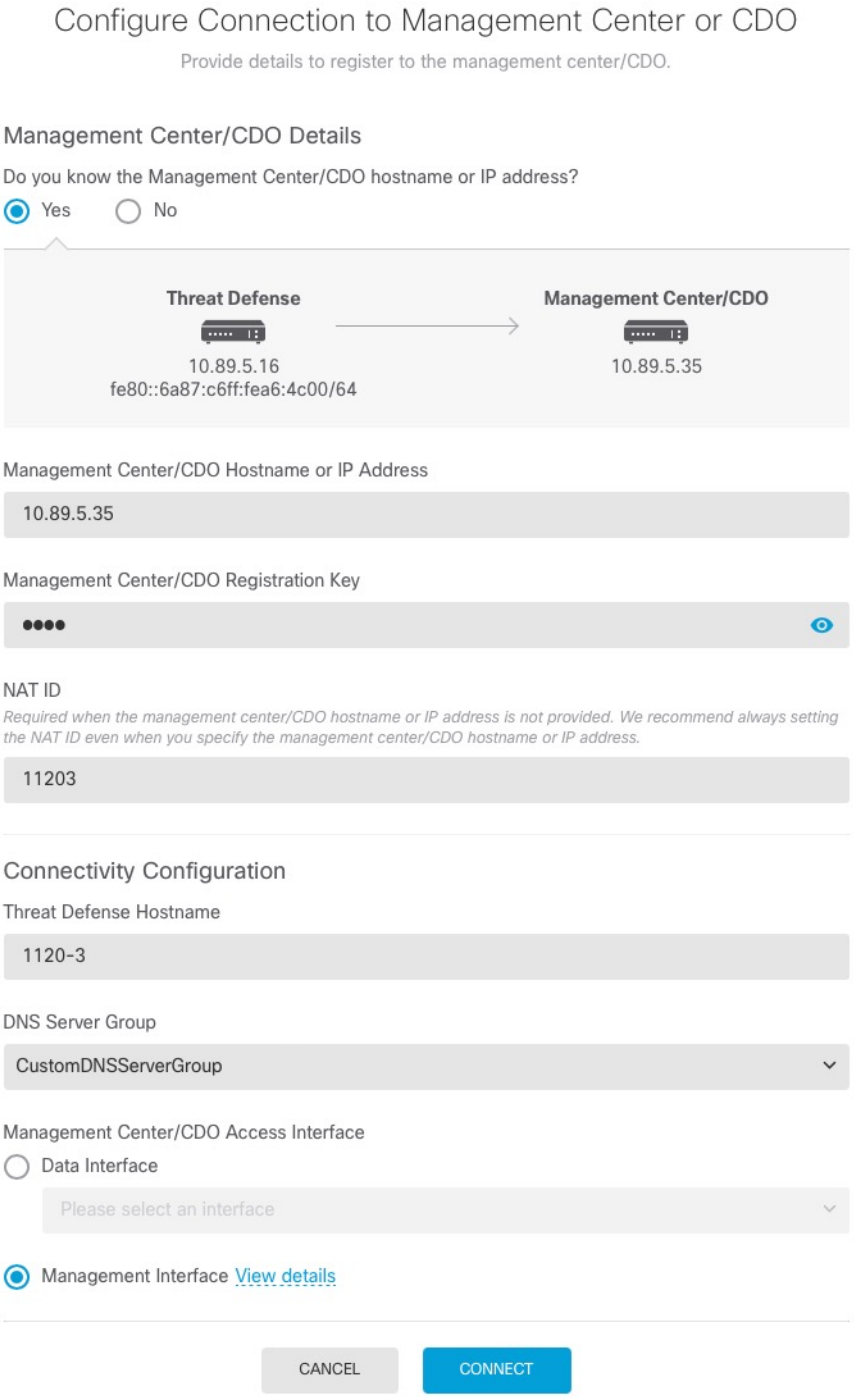
You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the Firewall Device Manager if you were using the Management interface for the Firewall Device Manager connection.

- 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 Firewall Management Center management.

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

Figure 12: Management Center/Security Cloud Control Details



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

At least one of the devices, either the Firewall Management Center or the Firewall 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 or 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 Firewall Management Center when you register the Firewall Threat Defense device. The registration key must be between 2 and 36 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 Firewall Management Center.

a) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the Firewall Management Center. The NAT ID must be between 2 and 36 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 Firewall 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. We recommended that you always use the NAT ID even when it is optional, but it is required if:

- You set the Firewall Management Center IP address to **DONTRESOLVE**.
- When adding the device on the Firewall Management Center, you do not specify a reachable device IP address or hostname.
- You use the data interface for management, even if you specify IP addresses on both sides.
- The Firewall Management Center uses multiple management interfaces.

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 Firewall Management Center, the data interface DNS servers are configured in the Platform Settings policy that you assign to this Firewall Threat Defense device. When you add the Firewall Threat Defense device to the Firewall 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 Firewall 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 Firewall Management Center and the Firewall Threat Defense device into sync.

Also, local DNS servers are only retained by the Firewall Management Center if the DNS servers were discovered at initial registration.

If you intend to choose the Management interface for the **Management Center/CDO Access InterfaceFMC 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 Firewall Threat Defense device to the Firewall 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 Firewall 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 Firewall Management Center can reach the Firewall 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 Firewall Threat Defense device to the Firewall Management Center, the Firewall Threat Defense device automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense device can validate the DDNS server certificate for the HTTPS connection. Firewall Threat Defense supports any DDNS server that uses the DynDNS Remote API specification (https://help.dyn.com/remote-access-api/).

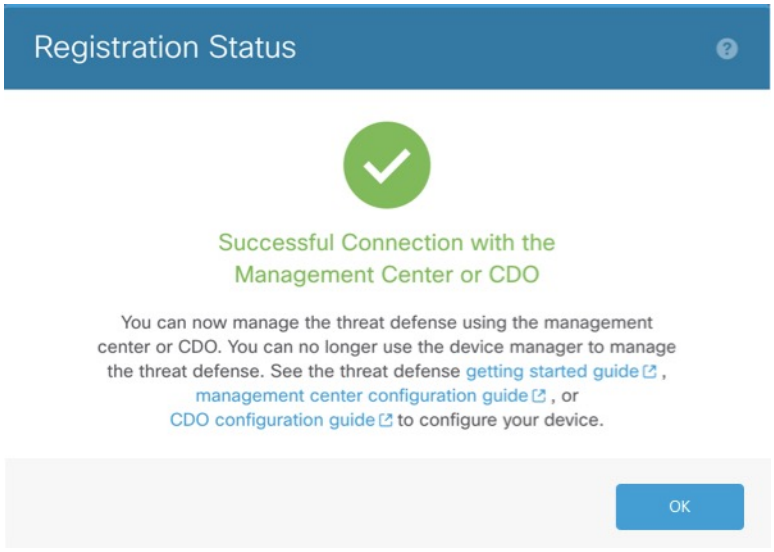
DDNS is not supported when using the Management interface for manager access.

Step 8 Click **Connect**. The **Registration Status** dialog box shows the current status of the switch to the Firewall Management Center. After the **Saving Management Center/CDO Registration Settings** step, go to the Firewall Management Center, and add the firewall.

If you want to cancel the switch to the Firewall Management Center, click **Cancel Registration**. Otherwise, do not close the Firewall 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 Firewall Device Manager.

If you remain connected to the Firewall Device Manager after the **Saving Management Center/CDO Registration Settings** step, you will eventually see the **Successful Connection with Management Center/CDO** dialog box, after which you will be disconnected from the Firewall Device Manager.

Figure 13: Successful Connection



Switch from Firewall Management Center to Firewall Device Manager

You can configure the Firewall Threat Defense device currently being managed by the on-premises or cloud-delivered Firewall Management Center to use the Firewall Device Manager instead.

You can switch from the Firewall Management Center to the Firewall Device Manager without reinstalling the software. Before switching from the Firewall Management Center to the Firewall Device Manager, verify that the Firewall Device Manager meets all of your configuration requirements. If you want to switch from the Firewall Device Manager to the Firewall Management Center, see Switch from the Firewall Device Manager to the Firewall Management Center, on page 37.

Caution Switching to the Firewall 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 Firewall Management Center, delete the firewall from the **Devices** > **Device Management** page.

Step 2 Connect to the Firewall Threat Defense CLI using SSH or the console port. For SSH, open a connection to the **management IP address**, and log into the Firewall 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 Firewall Threat Defense CLI using the **connect ftd** command. The SSH session connects directly to the Firewall 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.
```

History for device registration

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Multi-manager support.	7.2.0	7.2.0	We introduced the cloud-delivered management center. The cloud-delivered management center uses the Security Cloud Control (Security Cloud Control) platform and unites management across multiple Cisco security solutions. We take care of manager updates. 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. New/modified commands: **configure manager add**, **configure manager delete**, **configure manager edit**, **show managers** New/modified screens: • When you add a cloud-managed device to a hardware or virtual management center, use the new **Security Cloud Control Managed Device** check box to specify that it is analytics-only. • View which devices are analytics-only on **Devices** > **Device Management**. For more information, see Security Cloud Control documentation.
RAID support for SSDs on the Secure Firewall 3100.	7.1.0	7.1.0	The SSDs are self-encrypting drives (SEDs), and if you have 2 SSDs, they form a software RAID. New/modified commands: **configure raid, show raid, show ssd**
Support for TLS 1.3 for the management connection.	7.1.0	7.1.0	The FMC-device management connection now uses TLS 1.3. Previously, TLS 1.2 was supported.
Use FDM to configure FTD for management by the FMC.	7.1.0	7.1.0	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). After you switch to FMC, you can no longer use FDM to manage FTD. New/modified FDM screens: **System Settings** > **Management Center**

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