

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 12
- Log into the Command-Line Interface on the device, on page 13
- Complete the Firewall Threat Defense initial configuration for manual registration, on page 15
- Device registration management, on page 30
- Switch managers, on page 84
- History for device registration, on page 90

About device registration

Register your devices to the Firewall Management Center.

Firewall management center overview

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.

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: Secure Firewall Threat Defense Management*.

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.

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.

Devices managed by a Secure Firewall Management Center

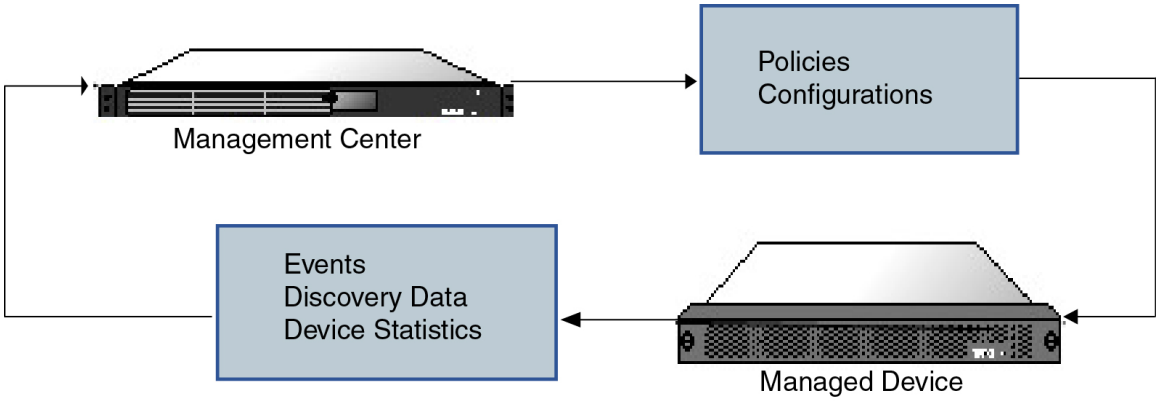
You can use the Secure Firewall Management Center as a central management point to manage Firewall Threat Defense devices.

Communication channel security

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.

This 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.



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.

Connection initiation behavior

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.

Device management tasks

These tasks provide essential functions for maintaining and updating your managed devices:

- **Backing up a device**:

  You cannot back up a physical managed device from its CLI. To back up configuration data, and, optionally, unified files, use the Firewall Management Center that manages the device.

  To back up event data, perform a backup of the Firewall Management Center that is managing the device.

- **Updating devices**:

  Cisco periodically 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 updates on the managed devices.

Device management interfaces

A device management interface is a network connection that

- enables communication with the Firewall Management Center,
- supports initial device setup through the management interface or console port, and
- facilitates communication with the Smart Licensing server, update downloads, and other management functions.

Interface configuration options

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

Management and event interfaces on the Firewall Threat Defense

Management and event interfaces on the Firewall Threat Defense are network connections that

- handle initial device registration and ongoing management communications between the Firewall Management Center and managed device
- transmit event data from the managed device to the Firewall Management Center, and

- can be configured as separate interfaces to isolate management and event traffic for enhanced performance and security.

Connection establishment behavior

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.

Separate event-only interface configuration requirements:

- Always enable an event interface on the Firewall Management Center before configuring a separate event-only interface on the managed device. 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.
- 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.
- Ensure that the Firewall Management Center and managed devices have consistent configurations regarding management and event interfaces to avoid communication issues.

Using the Firewall Threat Defense data interface for management

Using the Firewall Threat Defense data interface for management is a configuration option that

- allows communication with the Firewall Management Center through a regular data interface instead of the dedicated Management interface
- enables remote management from the outside interface when a separate management network is not available, and
- provides redundant secondary interface configuration to take over management functions if the primary interface goes down.

Manager access requirements

Manager access from a data interface has the requirements listed in this table.

- You can only enable manager access on a physical, data interface. You cannot use a subinterface or EtherChannel, nor can you create a subinterface on the manager access interface. You can also use the Firewall Management Center to enable manager access on a single secondary interface for redundancy.
- 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.

When using a data interface with device high availability, see the requirements that are listed in this table.

- Use the same data interface on both devices for manager access.
- Redundant manager access data interface is not supported.
- You cannot use DHCP; only a static IP address is supported. Features that rely on DHCP cannot be used, including DDNS and zero-touch provisioning.

Note If you use zero-touch provisioning to register the device, when you use the outside interface for manager access, it uses DHCP by default. Before you can enable high availability, you need to change the IP address to a static address. See Change the device IP address. Alternatively, you can use the Management interface instead; DHCP is supported on Management with high availability.

- Have different static IP addresses in the same subnet.
- Use the same manager configuration (**configure manager add** command) to ensure that the connectivity is the same.
- You cannot use the data interface as the failover or state link.

Management interface support per device model

This reference provides information about management interface support across different device models. 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.

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.

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
Secure Firewall 1200	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
Secure Firewall 4200	management0 **Note** management0 is the internal name of the Management 1/1 interface.	management1 **Note** management1 is the internal name of the Management 1/2 interface.
Firepower 4100 and 9300	management0 **Note** management0 is the internal name of this interface, regardless of the physical interface ID.	management1 **Note** management1 is the internal name of this interface, regardless of the physical interface ID.
ISA 3000	br1 **Note** br1 is the internal name of the Management 1/1 interface.	No support
Secure Firewall Threat Defense Virtual	eth0	No support

Network routes on device management interfaces

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

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

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

At least one static route is recommended per management interface to access remote networks. We recommend placing each interface on a separate network to avoid potential routing problems, including routing problems from other devices to the 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.

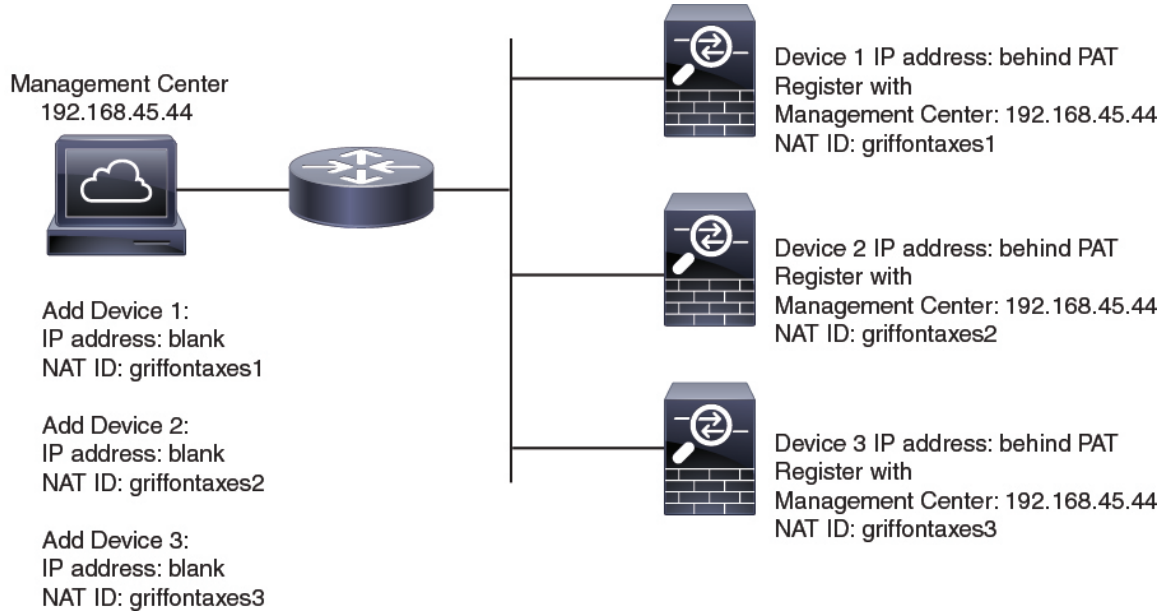
Normally, you need both IP addresses (along with a registration key) for both routing purposes and for authentication: the Firewall Management Center specifies the device IP address when you add a device, and the device specifies the Firewall Management Center IP address. However, if you only know one 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.

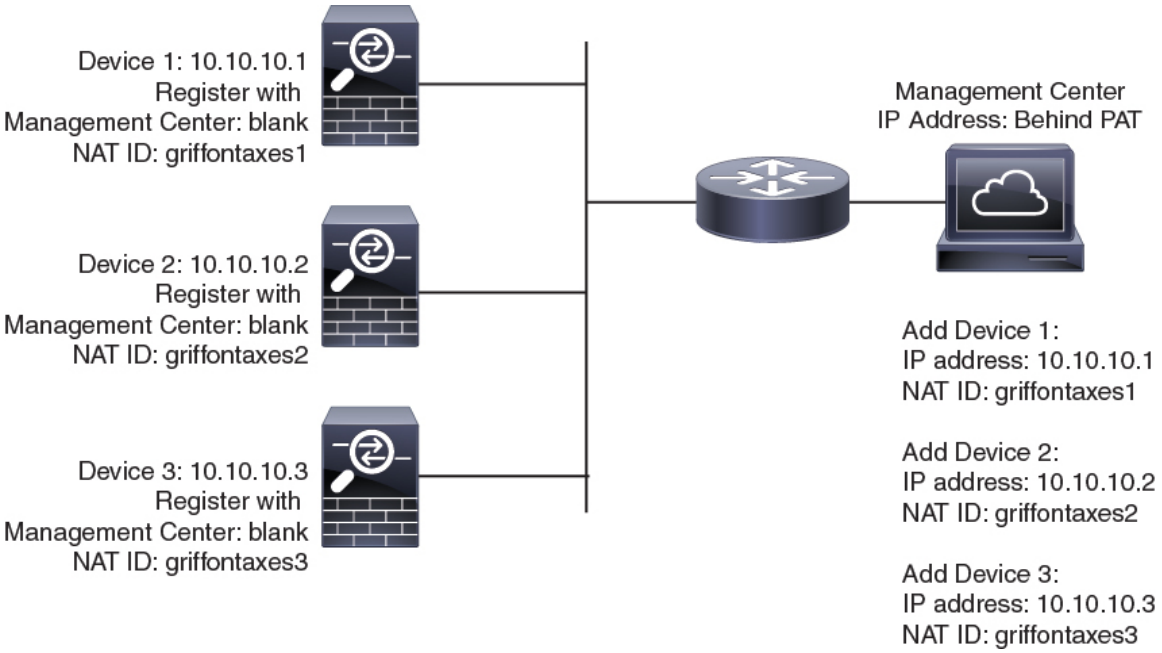
The following example shows three devices behind a PAT IP address. In this case, specify a unique NAT ID per device on both the Firewall Management Center and the devices, and specify the Firewall Management Center IP address on the devices.

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

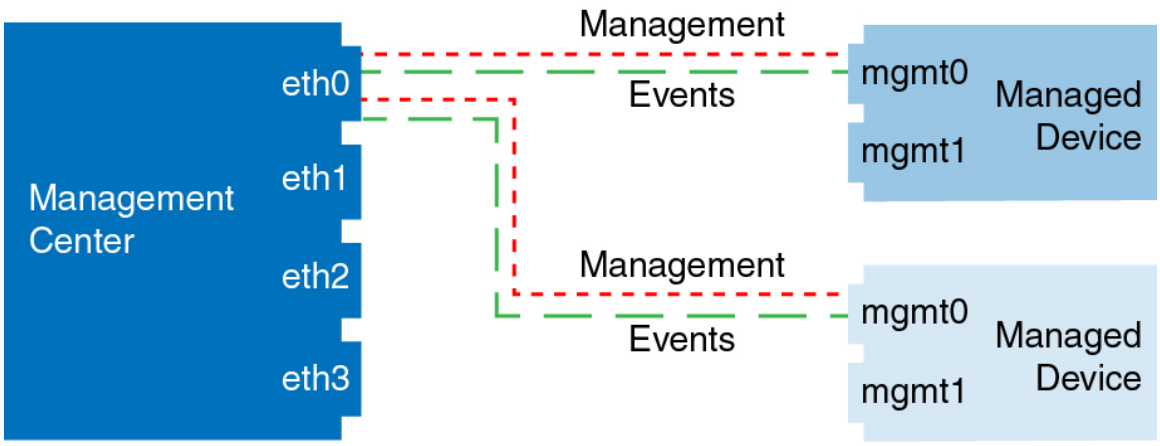
The management and event traffic channel examples illustrates the implementation and configuration of separate communication paths for network management and event reporting functions.

Note

- Configure a separate, dedicated event interface on both the Firewall Management Center and the managed device to segregate event traffic from management traffic. This separation improves performance and security by isolating event data flows.
- If Firewall Management Center uses a single interface for both management and event traffic, the managed device must send event traffic on that same interface. If the Firewall Management Center has a dedicated event interface, the managed device must also have a dedicated event interface configured.
- Mixing management and event channels on the same interface on the Firewall Management Center while the managed device uses a separate event interface can cause connectivity or event delivery issues. Ensure interface pairing is consistent between Firewall Management Center and managed devices.
- If you use a data interface for management on a Firewall Threat Defense, you cannot use separate management and event interfaces for that device.

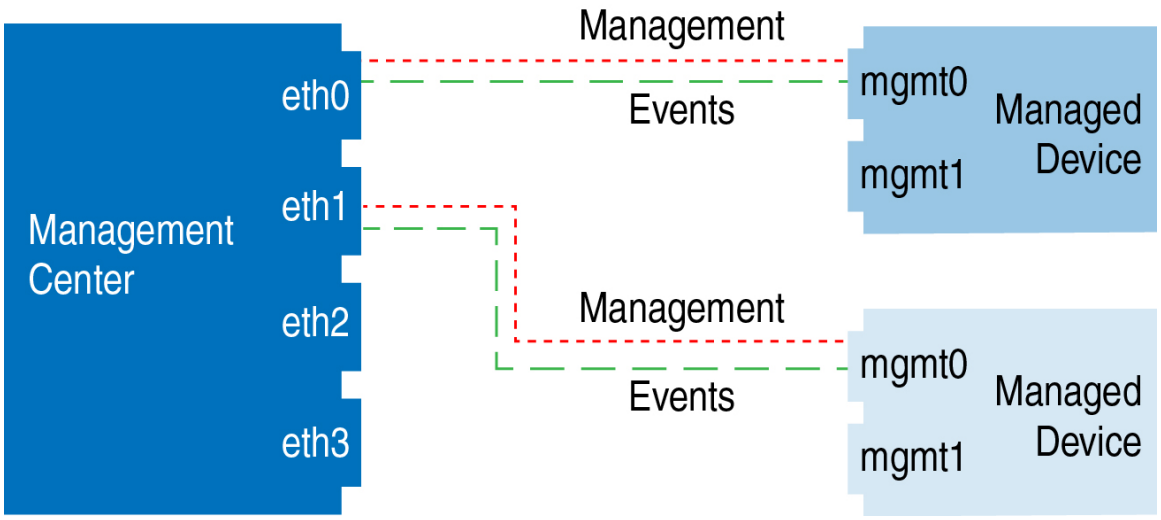
The following example shows the Firewall Management Center and managed devices using only the default management interfaces.

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



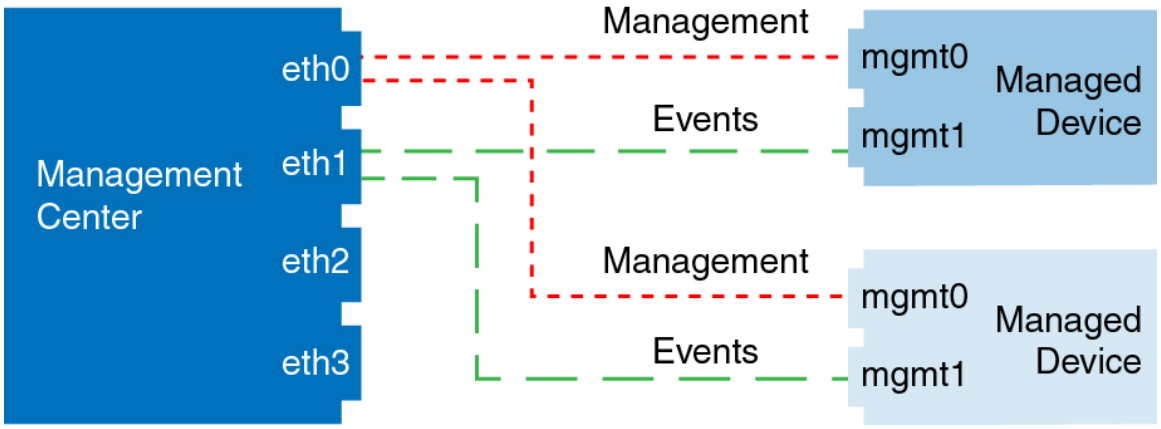
The following example shows the Firewall Management Center using separate management interfaces for devices; and each managed device using 1 management interface.

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



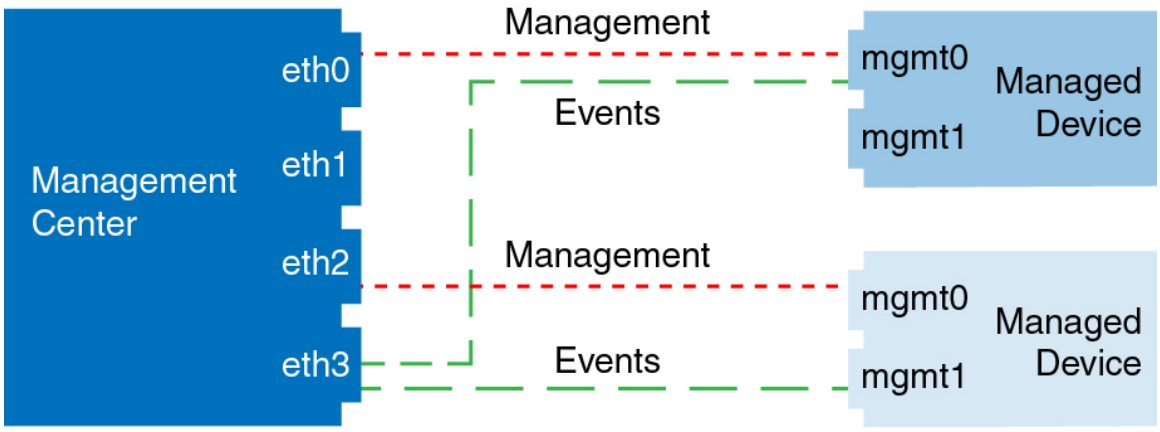
The following example shows the Firewall Management Center and managed devices using a separate event interface.

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

This reference provides the prerequisites and requirements that must be satisfied before registering a device with the management center, including domain requirements, user roles, connection specifications, and Zero-Touch Provisioning requirements.

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 these 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 21 .

For zero-touch provisioning , if you must access the Firewall Threat Defense CLI and run through the setup script, answer **n** when prompted: `Do you want to configure IPv4? (y/n) [y]:` and `Do you want to configure IPv6? (y/n) [y]:` . You also must accept the default local manager: `Manage the device locally? (yes/no) [yes]:` . These settings will preserve zero-touch provisioning capability.

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

Before you begin

- Create additional user accounts that can log in to 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 Configure Secure Shell (SSH) access 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.

For a chassis in multi-instance mode, you can connect to FXOS on the console port, or you can enable SSH for FXOS on the Management interface according to Configure SSH and SSH access list . SSH is disabled by default.

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

Multi-instance mode:

connect ftd *name*

To view the instance names, enter the command without a name.

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 for manual registration

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.

Platform-specific configuration methods

For the Firepower 4100/9300, you complete initial configuration when you deploy the logical device. See Logical Devices on the Firepower 4100/9300.

For zero-touch provisioning (serial number registration), you should not log in to the device or perform initial setup. See Add a device using serial number (Zero-Touch Provisioning) , on page 48.

Note Devices registered to a Firewall Management Center (FMC) for analytics-only purposes count toward the FMC platform device capacity limit. As the number of devices increases, event processing requirements also increase. Properly size your virtual FMC (vFMC) tier when planning analytics-only deployments.

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 / 1210 / 1220), 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).

- The Secure Firewall 4200 does not support the Firewall Device Manager . You need to use the CLI procedure: Complete the Firewall Threat Defense Initial Configuration Using the CLI , on page 21 .
- 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 21 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.

a) To configure additional interfaces, including an interface other than outside or inside that you want to use for manager access, choose **Device**

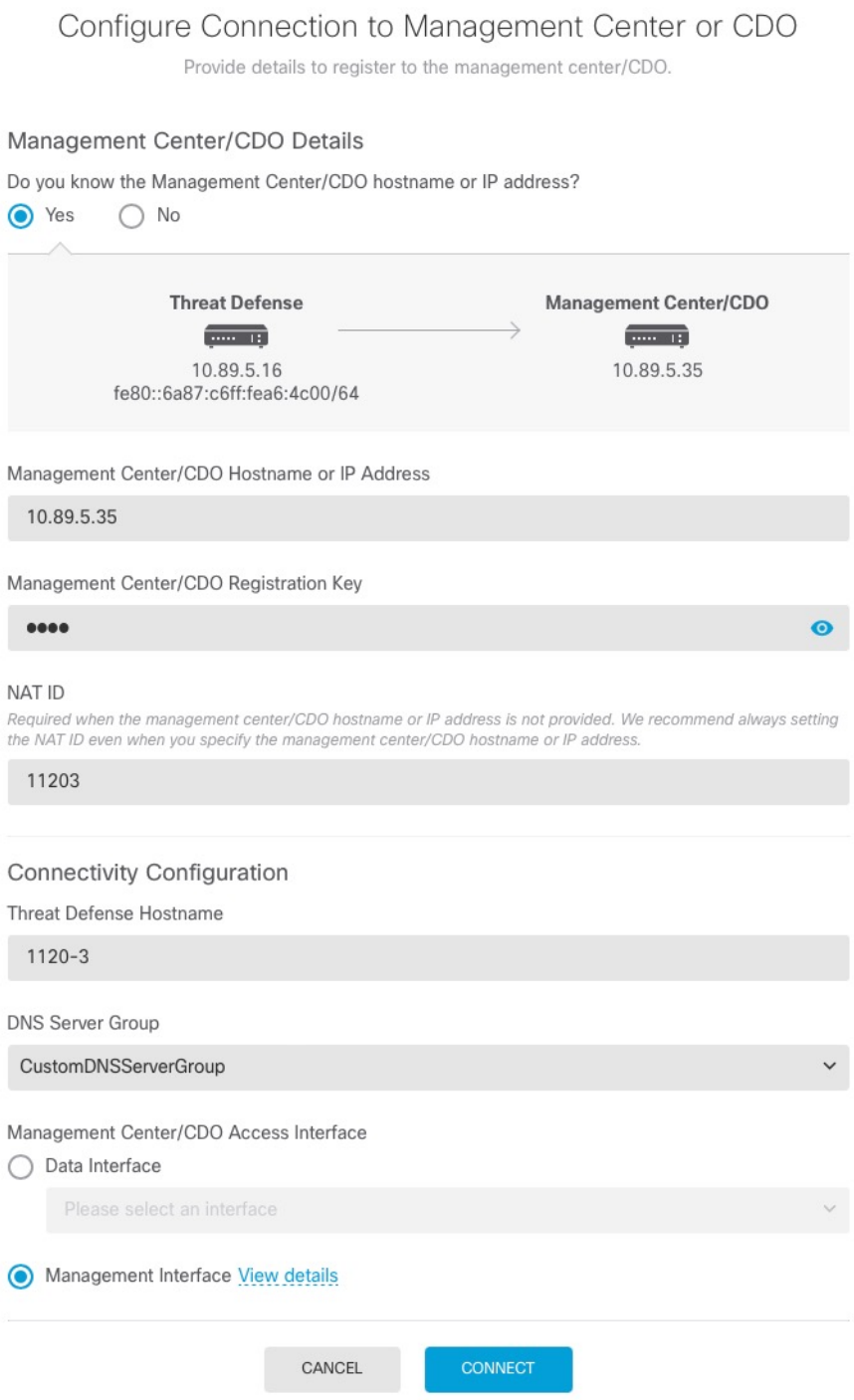
b) Click the link in the **Interfaces** summary.

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

Step 4 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the Firewall Management Center management.

Step 5 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.

d) 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 6 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 7 (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 8 (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/).

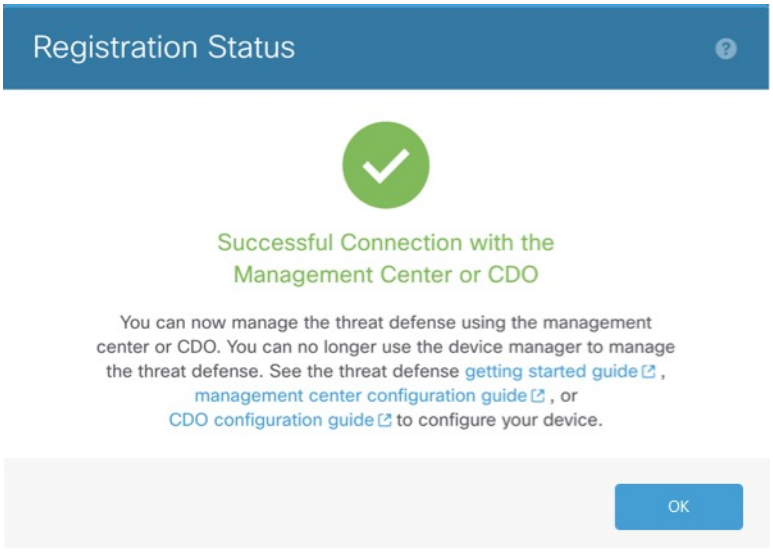
DDNS is not supported when using the Management interface for manager access.

Step 9 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 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.

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 and Secure Firewall 4200 , you can enable it for event-only traffic.

You can configure a separate event-only interface on both the Firewall Management Center and the managed device to isolate event traffic. This setup enhances performance and security by segregating event data from management operations.

If the event interface is unreachable, event traffic falls back to the management interface.

Before you begin

Ensure that you enable an event interface on the Firewall Management Center before configuring a separate event-only interface on the managed device. For more information, refer to *Cisco Secure Firewall Management Center Administration Guide* .

If you use a data interface for management on the managed device, you cannot configure separate management and event interfaces.

Procedure

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

configure network management-interface enable management1

configure network management-interface disable-management-channel management1

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

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

Example:

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

Step 2 Configure the IP address of the event interface.

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

a) Configure the IPv4 address:

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

Note that the *gateway_ip* in this command is used to create the default route for the device, so you should enter the value you already set for the management0 interface. It does not create a separate static route for the eventing interface. If you are using an event-only interface on a different network from the management interface, we recommend that you create a static route separately for the event-only interface.

Example:

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

b) Configure the IPv6 address:

- Stateless autoconfiguration:

  configure network ipv6 router management1

  Example:

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

- Manual configuration:

  configure network ipv6 manual *ip6_address ip6_prefix_length* **management1**

  Example:

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

```
Network settings changed.
>
```

Step 3 Add a static route for the event-only interface if the 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 29).

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
[…]
```

Device registration management

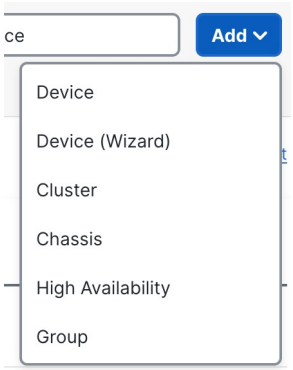
Register and unregister devices to the Firewall Management Center.

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, version, 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.

Figure 9: Add menu



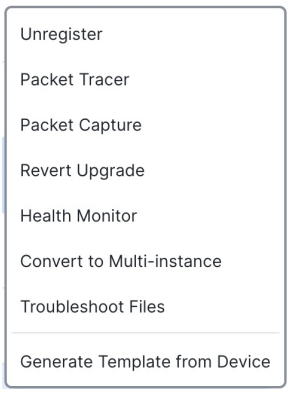
- Columns—Click the column head to sort by that column.
  - **Name**
  - **Model**
  - **Version**
  - **Chassis**—For supported models, click **Manage** to bring up the integrated Chassis Manager. For the Firepower 4100/9300, the link cross-launches the Firewall Chassis Manager.
  - **Licenses**
  - **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:

Figure 10: More menu



  - **Unregister**—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.
- **Convert to Multi-instance**—For supported models, convert the chassis to multi-instance mode.
- **Troubleshoot Files**—Generate troubleshooting files, where you can choose the type of data to be included in the report.
- **Generate Template from Device**—Generate a new device template from a registered device. The new template has the same configuration as the device from which it is generated. You can generate a new device template from standalone and HA devices. However, if you generate a template from HA devices, the new template will not contain the failover configurations.

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.

Registration with the management center

Registration with the Firewall Management Center is a process that establishes communication and management between devices and the central management platform.

Available registration methods

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

Registration key method

Add a device using a registration key that you specify in both the Firewall Management Center and the device initial configuration.

Add a Device Using a Registration Key—Basic Configuration

Use this procedure to add a device to the Firewall Management Center using a registration key and a basic configuration; to use a device template, see Add a Device Using a Registration Key—Device Template , on page 43. 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 for manual registration, on page 15
  - 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.

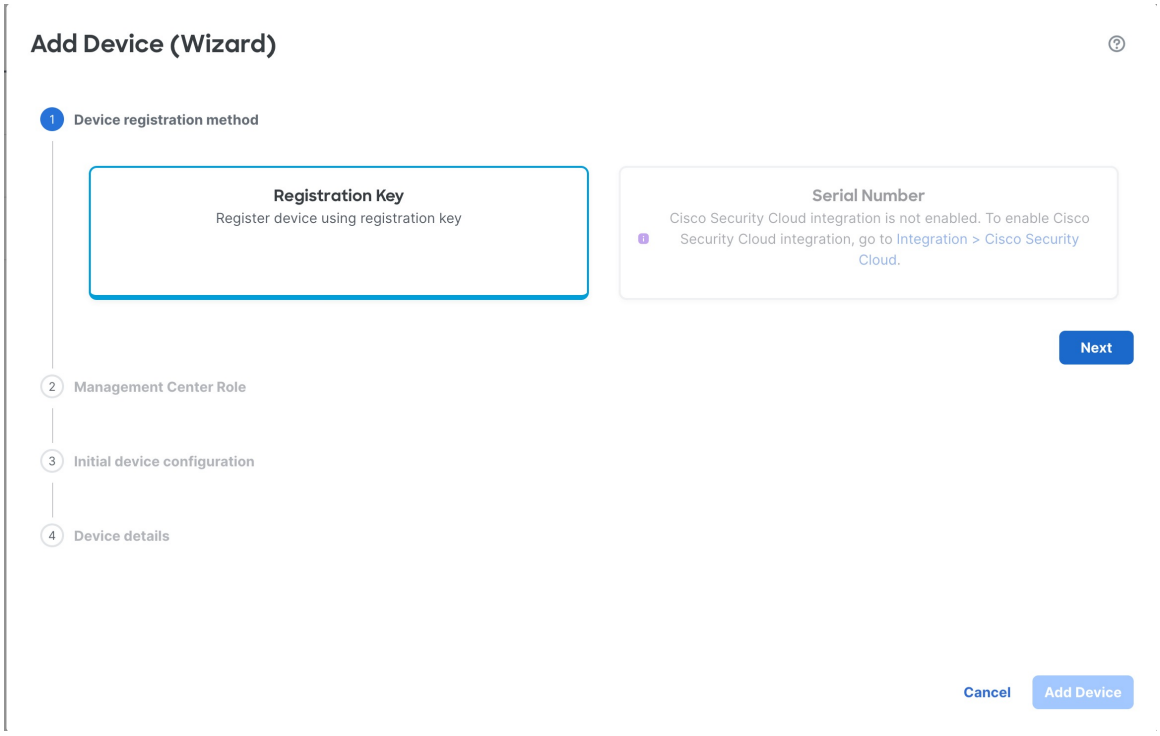
Procedure

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

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

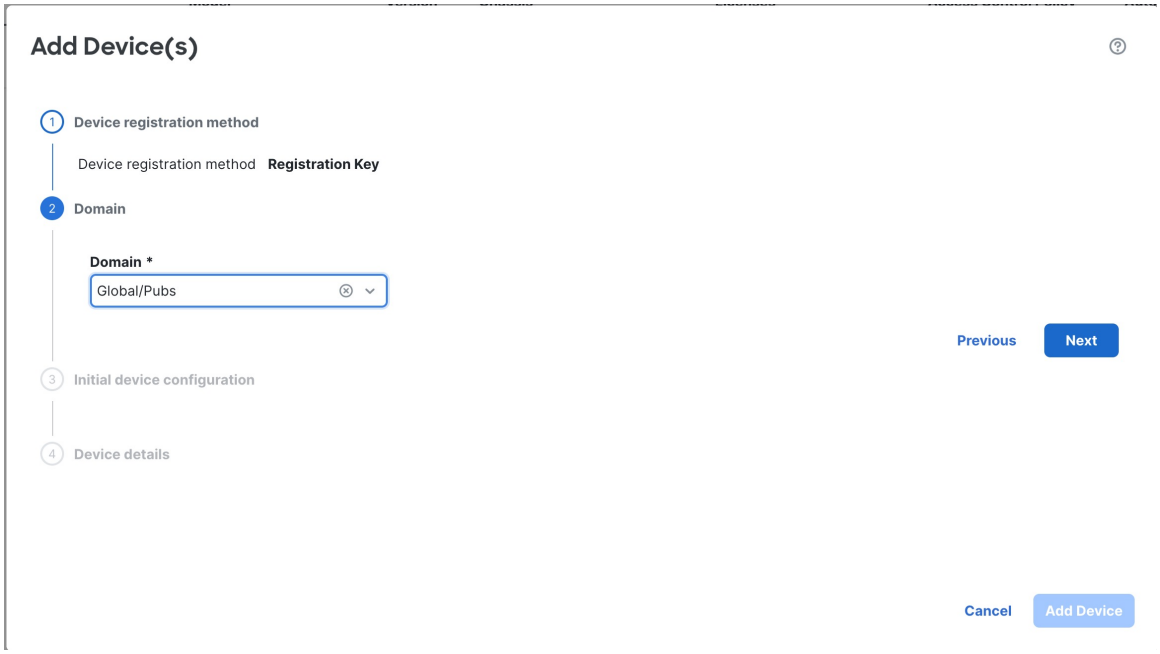
Step 3 Click **Registration Key** , and then click **Next** .

Figure 11: Device Registration Method



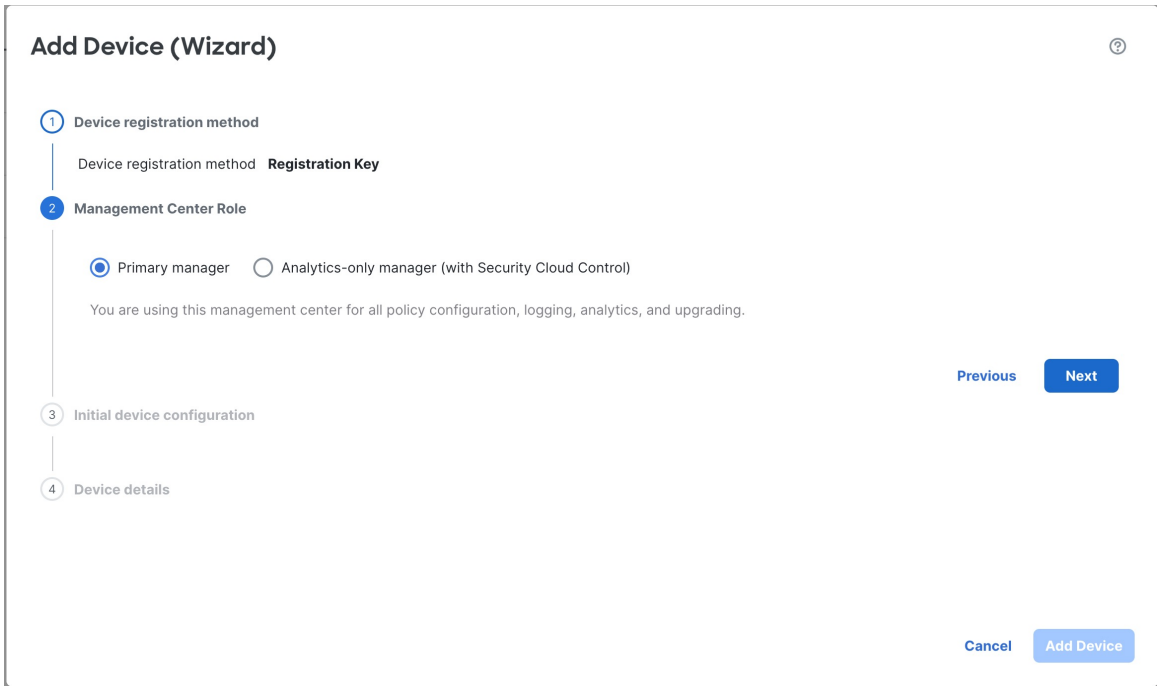
Step 4 In a multi-domain environment, choose the **Domain** from the drop-down list and click **Next**.

Figure 12: Domain



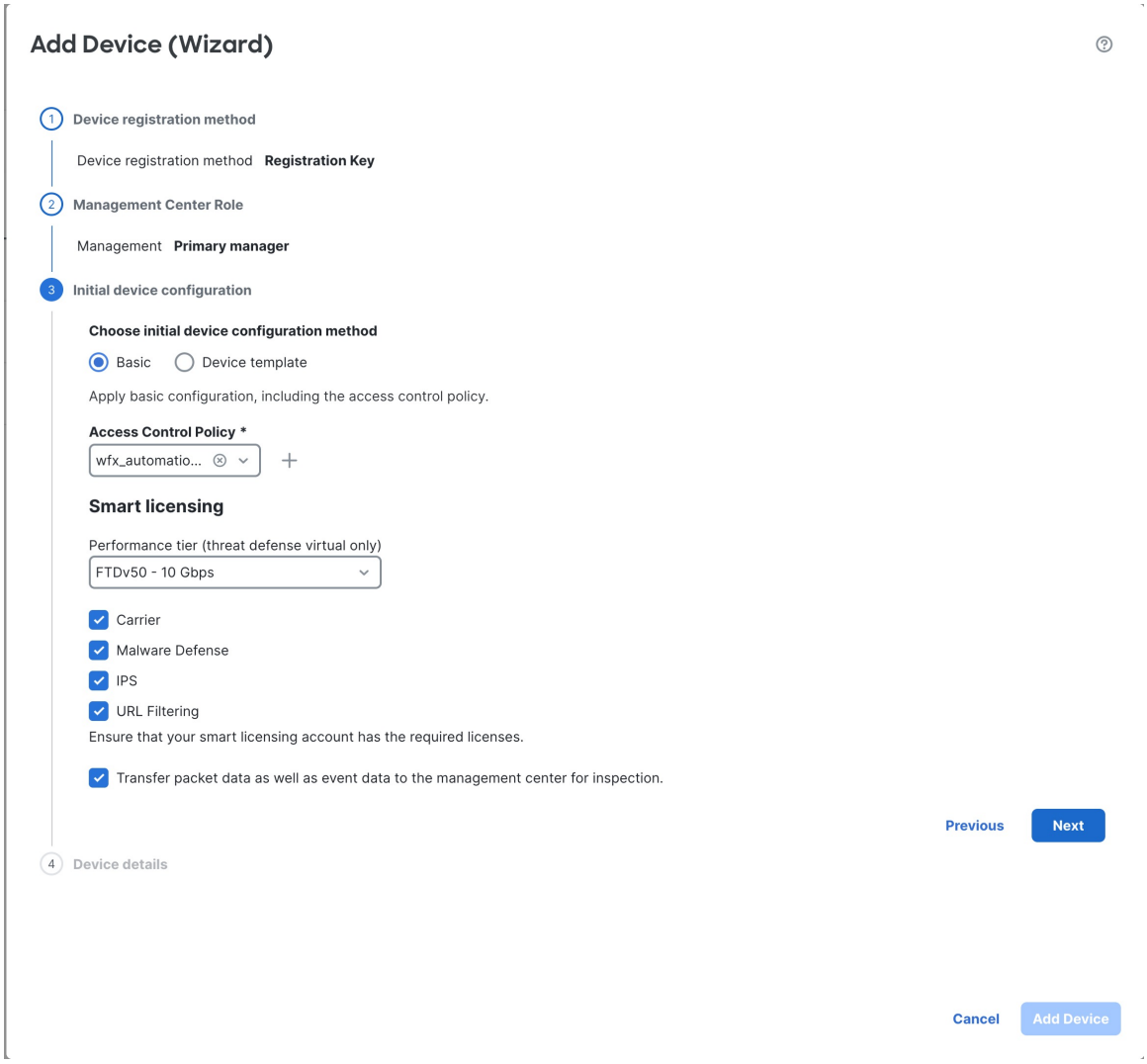
Step 5 Click **Primary manager** for normal management or **Analytics-only manager** for a device that is managed by a Cloud-Delivered Firewall Management Center. Analytics-only mode does not support a multi-domain environment, so this step doesn't appear in that case .

Figure 13: Management Center Role



Step 6 For the **Initial Device Configuration** , click **Basic**.

Figure 14: Initial Device Configuration



For analytics-only mode, the system hides **Initial Device Configuration** because these settings are managed by Security Cloud Control.

a) Choose an initial **Access Control Policy** to deploy to the device at registration, or create a new policy.
b) Choose **Smart Licensing** licenses to apply to the device.

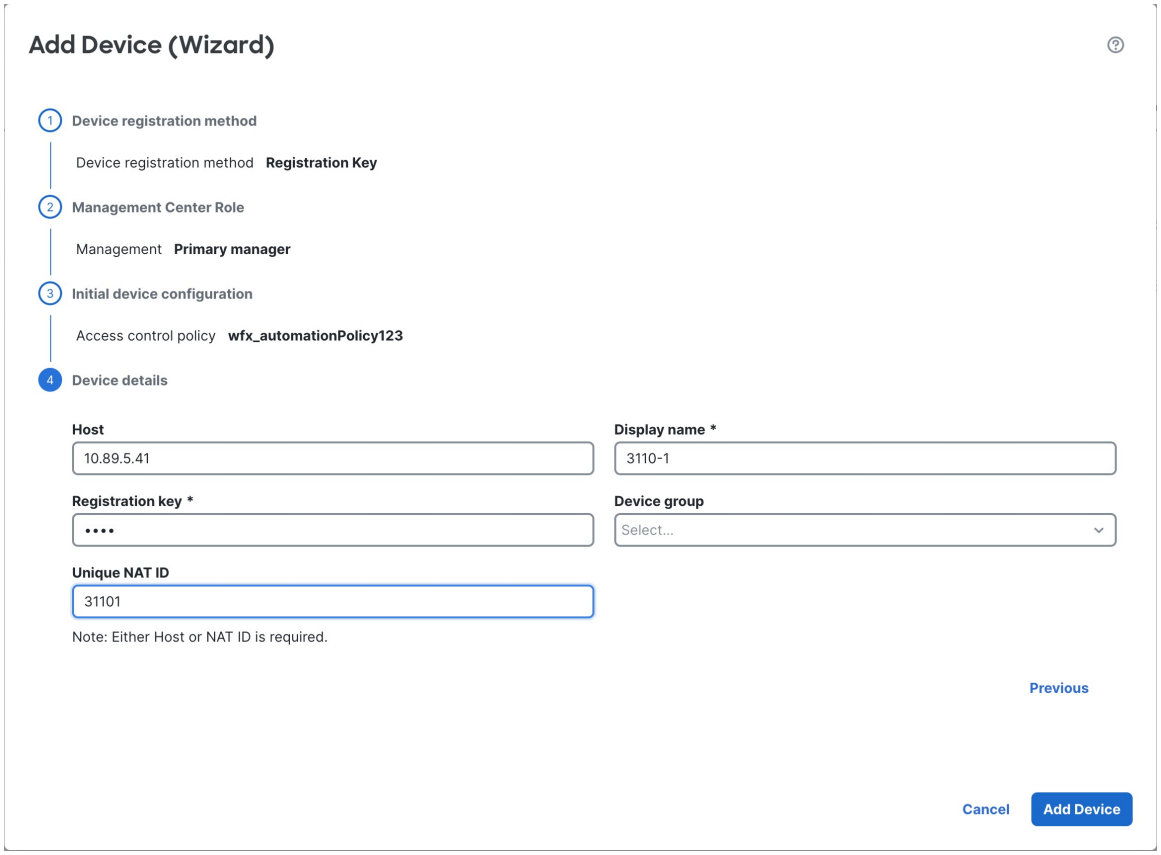
   You can also apply licenses after you add the device, from the **System** > **Licenses** > **Smart Licenses** page, including the Secure Client remote access VPN license.

   For the Firewall Threat Defense Virtual only, 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 FTDv50.

c) Click **Next**.

Step 7 Specify the **Device details**.

Figure 15: Device Details



a) 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 8.

b) 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.

c) For the **Registration Key**, enter the same registration key from 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.

d) (Optional) Add the device to a **Device group**

e) For the **Unique NAT ID** , enter the same ID from your initial configuration.

   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.

f) Select the **Transfer Packets** check box to allow the device to transfer event metadata and packet data associated with intrusion events to the Firewall Management Center.

This option is enabled by default. The transferred packet data is used for intrusion-event analysis. It does not necessarily contain the complete original packet as transmitted on the wire or the complete traffic session. For intrusion events generated by Snort inspection, the device can transfer only the Protocol Data Unit (PDU) or packet content associated with the intrusion-rule match.

If you disable this option, the device sends only event information to the Firewall Management Center; packet data is not sent.

Step 8 Click **Add Device**.

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, refer to https://cisco.com/go/fmc-reg-error.

Add a Device Using a Registration Key (Legacy Screen)—Basic Configuration

Use this procedure to add a single device to the Firewall Management Center using a registration key . 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.

You can use this legacy screen or you can use the **Device (Wizard)** to add your device. The **Device (Wizard)** has additional options, including adding a device by serial number (zero-touch provisioning) or adding one or more devices using templates. See Add a device using serial number (Zero-Touch Provisioning) , on page 48 .

To add a device using a template, see Add a Device Using a Registration Key—Device Template , on page 43 .

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 for manual registration, on page 15
- The getting started guide for your model

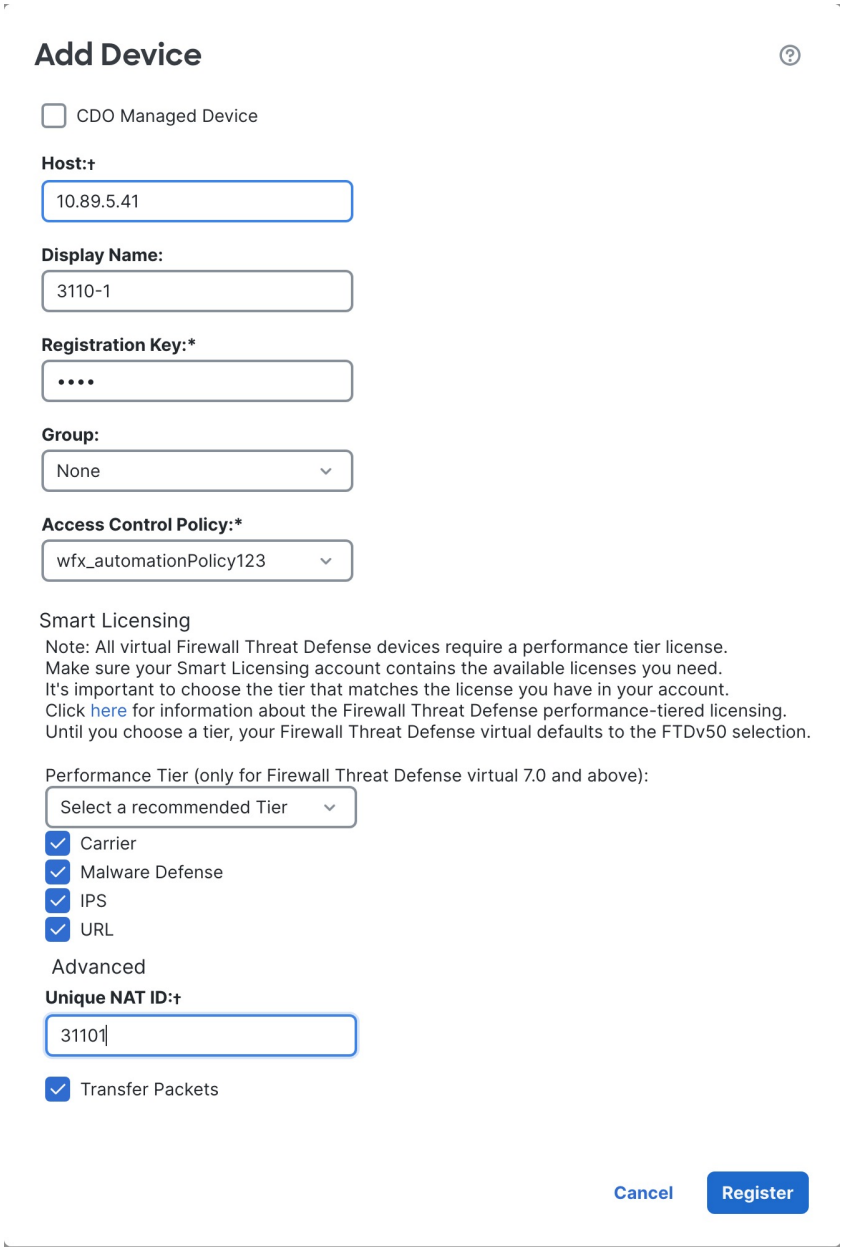
- The Firewall Management Center must be registered to the Smart Software Manager. A valid evaluation license is sufficient, but if it expires, you will not be able to add new devices until you successfully register.
- If you registered a device using IPv4 and want to convert it to IPv6, you must unregister and reregister the device.

Procedure

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

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

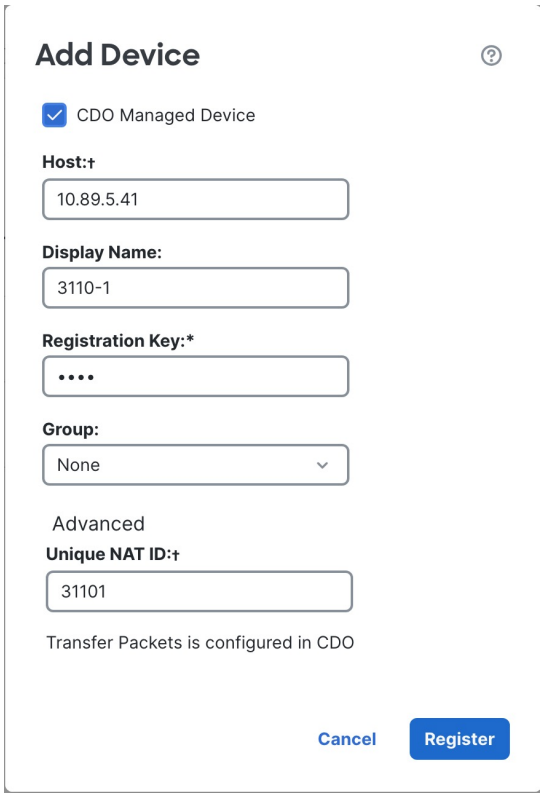
Figure 16: Add Device Using a Registration Key



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 17: 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 8 .

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. Add the device to a device **Group**.

Step 7 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 8 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.

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 9 Select the **Transfer Packets** check box to allow the device to transfer event metadata and packet data associated with intrusion events to the Firewall Management Center.

This option is enabled by default. The transferred packet data is used for intrusion-event analysis. It does not necessarily contain the complete original packet as transmitted on the wire or the complete traffic session. For intrusion events generated by Snort inspection, the device can transfer only the Protocol Data Unit (PDU) or packet content associated with the intrusion-rule match.

If you disable this option, the device sends only event information to the Firewall Management Center; packet data is not sent. 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 .

What to do next

Add a Device Using a Registration Key—Device Template

You can use a template to add a device, register the device with the Firewall Management Center and bring up the device with the given template configurations.

Before you begin

Create a device template according to Device Registration Using Device Templates. You must specify any required variables and network object overrides for each device and ensure that model mapping is done for the target device model.

We recommend that you create a checklist to ensure that all configurations in the template have been entered correctly before applying the template on the device.

A sample checklist is given below.

- Check version, model, operation modes.
- Check list of variables and overrides.
- Check sanity of variable and override values.
- Check if the required Model Mappings exist.
- Check if parallel device template operations are in progress.

Note If you are adding a device that will be managed by a data interface, ensure that you configure the template to be compatible with the connectivity parameters of the device. For more information, see Configure a Template for Threat Defense Devices Managed Through the Data Interface .

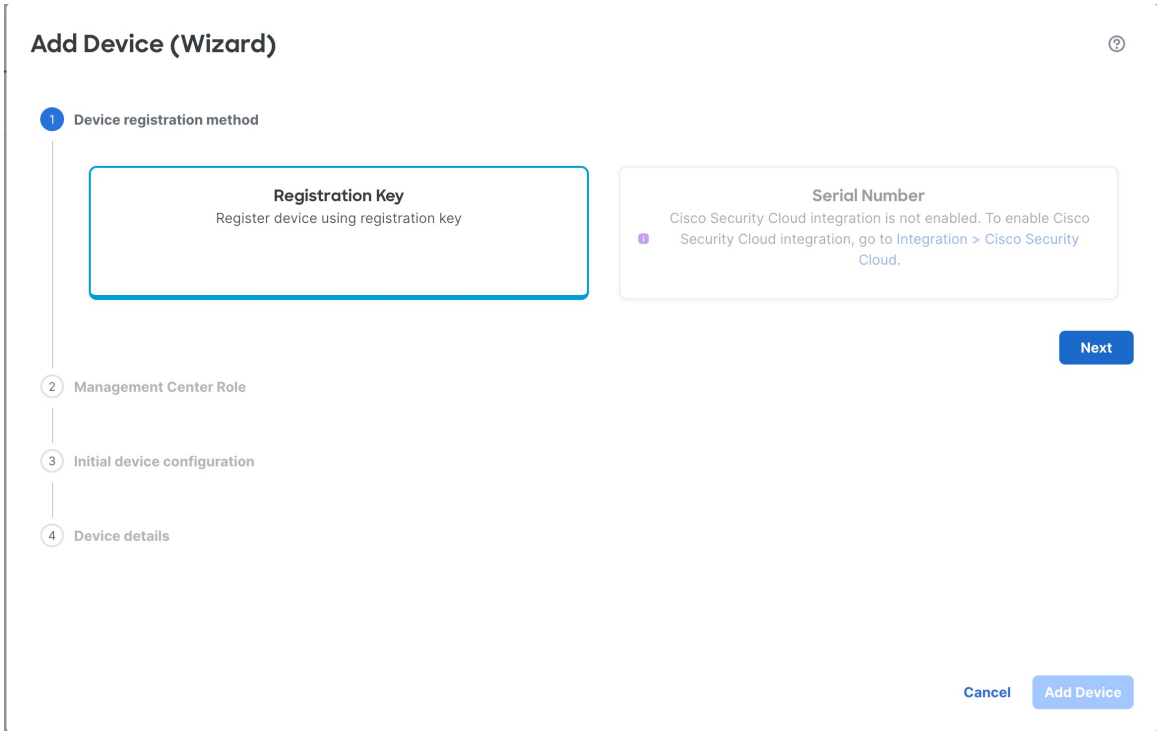
Procedure

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

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

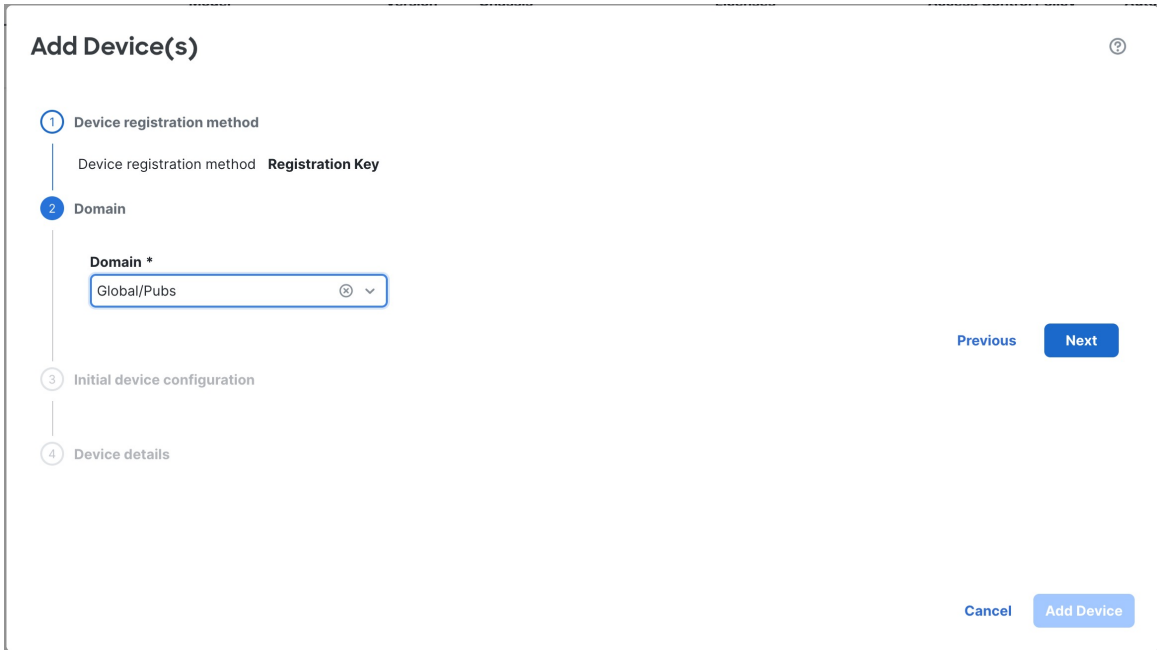
Step 3 Click **Registration Key** , and then click **Next** .

Figure 18: Device Registration Method



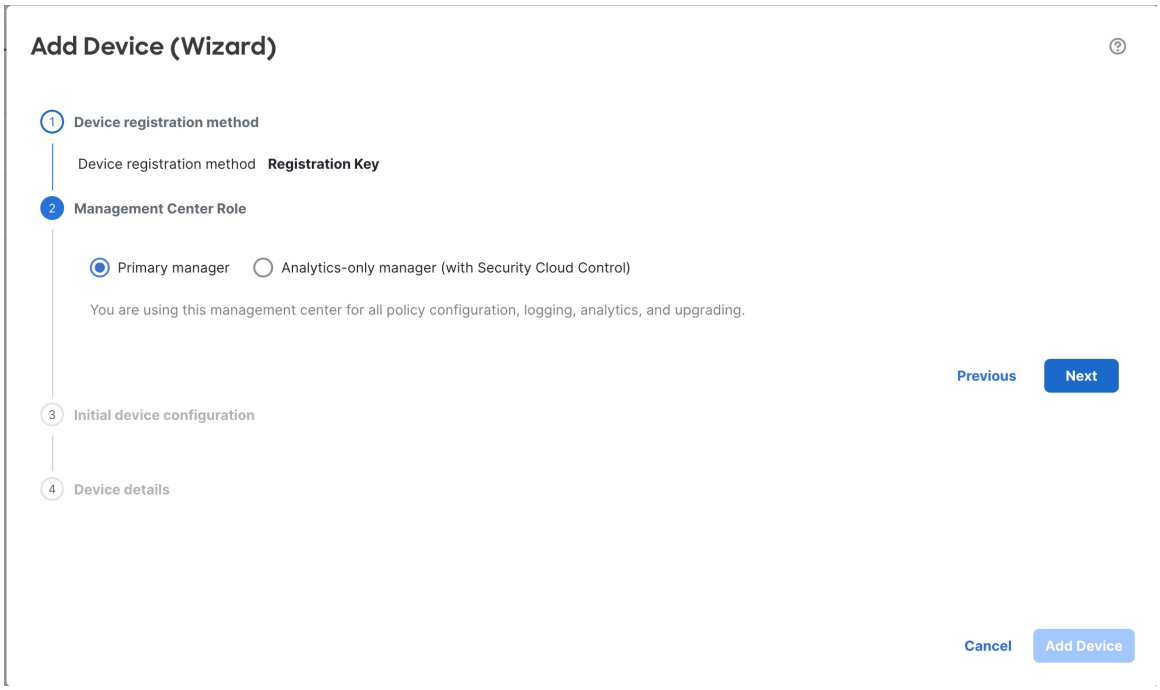
Step 4 In a multi-domain environment, choose the **Domain** from the drop-down list and click **Next**.

Figure 19: Domain



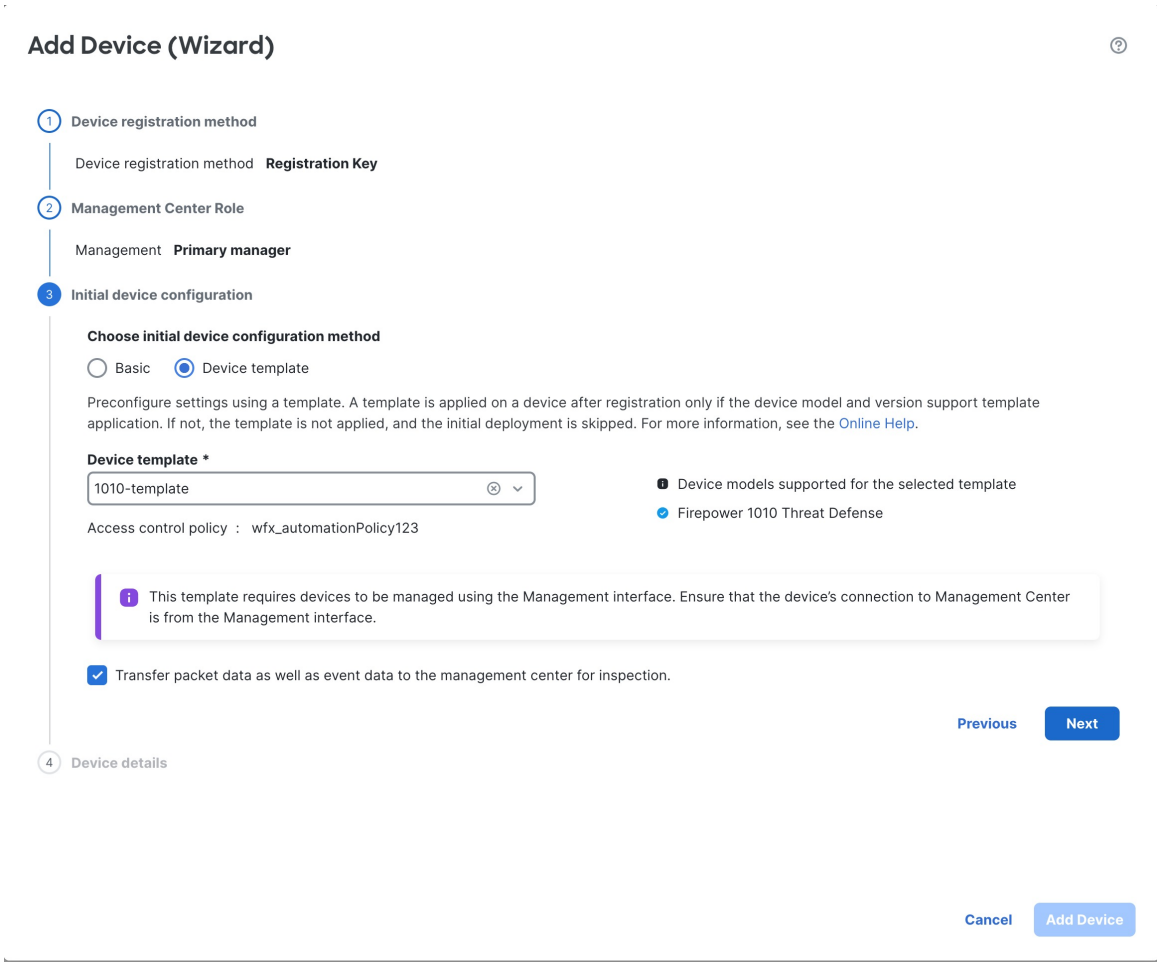
Step 5 For the **Management center role** , click **Primary manager** . Analytics-only mode does not support device templates. Analytics-only mode does not support a multi-domain environment, so this step doesn't appear in that case.

Figure 20: Management Center Role



Step 6 In **Initial device configuration** , configure the following settings.

Figure 21: Initial Device Configuration



a) Click **Device template** .
b) Choose a template from the **Device template** drop-down list.
c) (Optional) Click **Transfer packet data** to allow the device to transfer event metadata and packet data associated with intrusion events to the Firewall Management Center.

   This option is enabled by default. The transferred packet data is used for intrusion-event analysis. It does not necessarily contain the complete original packet as transmitted on the wire or the complete traffic session. For intrusion events generated by Snort inspection, the device can transfer only the Protocol Data Unit (PDU) or packet content associated with the intrusion-rule match.

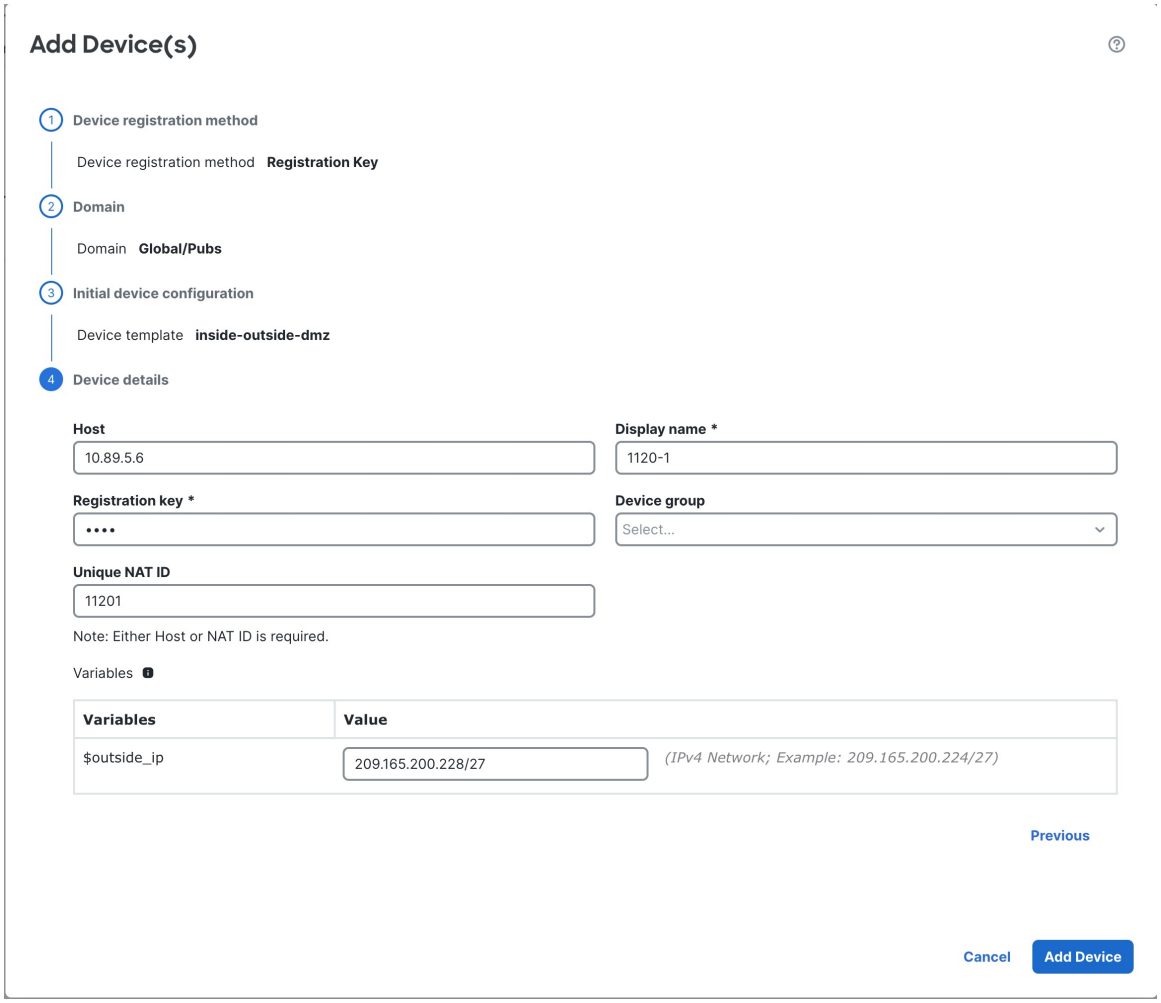
   If you disable this option, the device sends only event information to the Firewall Management Center; packet data is not sent.

d) Click **Next**.

Step 7

Step 8 Specify the **Device details** .

Figure 22: Device Details



a) 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 8 .

b) 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.

c) 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.

d) (Optional) Add the device to a **Device group**

e) If you specified a NAT ID during initial configuration, 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 .

f) Select the **Transfer Packets** check box to allow the device to transfer event metadata and packet data associated with intrusion events to the Firewall Management Center.

This option is enabled by default. The transferred packet data is used for intrusion-event analysis. It does not necessarily contain the complete original packet as transmitted on the wire or the complete traffic session. For intrusion events generated by Snort inspection, the device can transfer only the Protocol Data Unit (PDU) or packet content associated with the intrusion-rule match.

If you disable this option, the device sends only event information to the Firewall Management Center; packet data is not sent.

g) Enter values for the **Variables** and **Network object overrides** .

Step 9 Click **Add Device** to initiate device registration. The template configurations are applied after the device is successfully registered with the Firewall Management Center .

Serial number method (Zero-Touch Provisioning)

A serial number method is a zero-touch provisioning approach that lets you register devices to the Firewall Management Center by serial number without having to perform any initial setup on the device.

Add a device using serial number (Zero-Touch Provisioning)

Zero-Touch Provisioning lets you register devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with the Cisco Security Cloud and Security Cloud Control for this functionality.

Use this procedure to add a single device to the Firewall Management Center using a basic configuration. To add one or more devices using a template, see Add Devices Using Serial Numbers (Zero-Touch Provisioning)—Device Template , on page 55 .

Default Configuration:

When you use zero-touch provisioning , the following interfaces are preconfigured. Note that other settings, such as the DHCP server on inside, access control policy, or security zones, are not configured.

- Ethernet 1/1—"outside", IP address from DHCP, IPv6 autoconfiguration
- Ethernet 1/2 (or for the 1010 / 1210 / / 1220 , the VLAN1 interface)— "inside", 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

Requirements:

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

When you use the outside interface for manager access, it uses DHCP by default. Before you can enable high availability, you need to change the IP address to a static address. See Change the device IP address . Alternatively, you can use the Management interface instead; DHCP is supported on Management with high availability.

Zero-Touch Provisioning is only supported on the following models using 7.2 and 7.4 or later; prior to 7.2.4, the Firewall Management Center must be publicly reachable.

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

Before you begin

- Make sure the device is unconfigured or a fresh install. Zero-Touch Provisioning is meant for new devices only. Pre-configuration can disable zero-touch provisioning , depending on how you configure the device. If you disable zero-touch provisioning , see Resolve serial number (zero-touch provisioning) registration issues, on page 66 .
- Cable the outside interface or Management interface so it can reach the internet. If you use the outside interface for zero-touch provisioning , do not also cable the Management interface; if the Management interface gets an IP address from DHCP, the routing will be incorrect for the outside interface.
- If the device does not have a public IP address or FQDN , or you use the Management interface , set a public IP address/FQDN for the Firewall Management Center (for example, if it is behind NAT), so the device can initiate the management connection. See **System** > **Configuration** > **Manager Remote Access** .
- DHCP server for either Management or Ethernet 1/1 that provides an IP address and default gateway.
- Network access to the OpenDNS public DNS servers. IPv4: 208.67.220.220 and 208.67.222.222; IPv6: 2620:119:35::35. DNS servers obtained from DHCP are never used.

  The following names need to be resolved:

Table 2: FQDNs for zero-touch provisioning

FQDNs
*.cisco.com (many FQDNs)
*.defenseorchestrator.com (many FQDNs)
*.defenseorchestrator.eu (for the EU, many FQDNs)
0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
1.200.159.162.in-addr.arpa
60.19.239.178.in-addr.arpa
connected.by.freedominter.net
time.cloudflare.com
udc.neo4j.org

- 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 unregister and reregister the device.

Procedure

Step 1 The first time you add a device using a serial number, integrate the Firewall Management Center with Cisco Security Cloud.



Note For a Firewall Management Center high-availability pair, you also need to integrate the secondary Firewall Management Center with Cisco Security Cloud.

a) Choose **Integration** > **Cisco Security Cloud** .
b) Click **Enable Cisco Security Cloud** to open a separate browser tab to log you into your Cisco Security Cloud account and confirm the displayed code.

Make sure this page is not blocked by a pop-up blocker. If you do not already have a Cisco Security Cloud and Security Cloud Control account, you can add one during this procedure.

For detailed information about this integration, see the "System Configuration" chapter in the *Cisco Secure Firewall Management Center Administration Guide* .

Security Cloud Control onboards the on-prem Firewall Management Center after you integrate the Firewall Management Center with Cisco Security Cloud. Security Cloud Control needs the Firewall Management Center in its inventory for zero-touch provisioning to operate. However, you do not need to use Security Cloud Control directly. If you do use Security Cloud Control , its Firewall Management Center support is limited to device onboarding, viewing its managed devices, viewing objects associated with the Firewall Management Center , and cross-launching the Firewall Management Center .

c) Make sure **Enable Zero-Touch Provisioning** is checked.
d) Click **Save** .

Step 2 Obtain your device's serial number.

- If you have the shipping box, you can see the serial number on the label.
- The serial number is on a label on the bottom , or the back , or a pull-out tab at the front of the device .
- If you have console access, in FXOS, enter **show chassis detail** . Note that the correct serial number is called **Serial (SN)** . Do not use the **PCB Serial Number** . At the Firewall Threat Defense CLI, enter **show inventory** (not **show serial-number** , which shows the PCB serial number). Be careful not to disable zero-touch provisioning by entering certain settings at the Firewall Threat Defense startup script. If you disable zero-touch provisioning , see Resolve serial number (zero-touch provisioning) registration issues, on page 66 .

Step 3 Check your LEDs to make sure the firewall is ready for registration.

1000

Table 3: Zero-Touch Provisioning: System (S) LED behavior

S LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00

1200, 3100

Table 4: Zero-Touch Provisioning: Managed (M) LED behavior

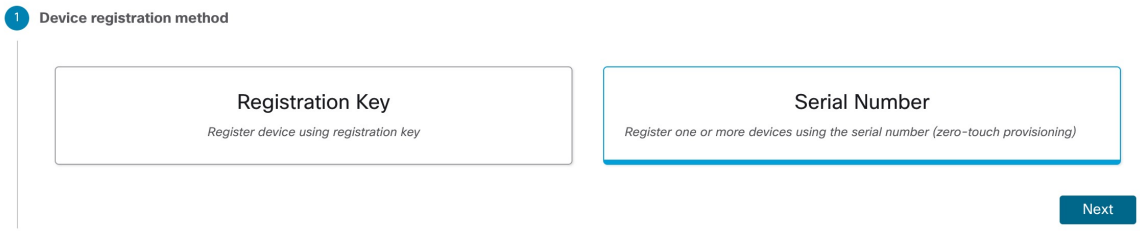
M LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00
Solid green	Onboarded	20:00 - 45:00

Choose **Devices** > **Device Management** .

Step 4 From the **Add** drop-down menu, choose **Device (Wizard)** .

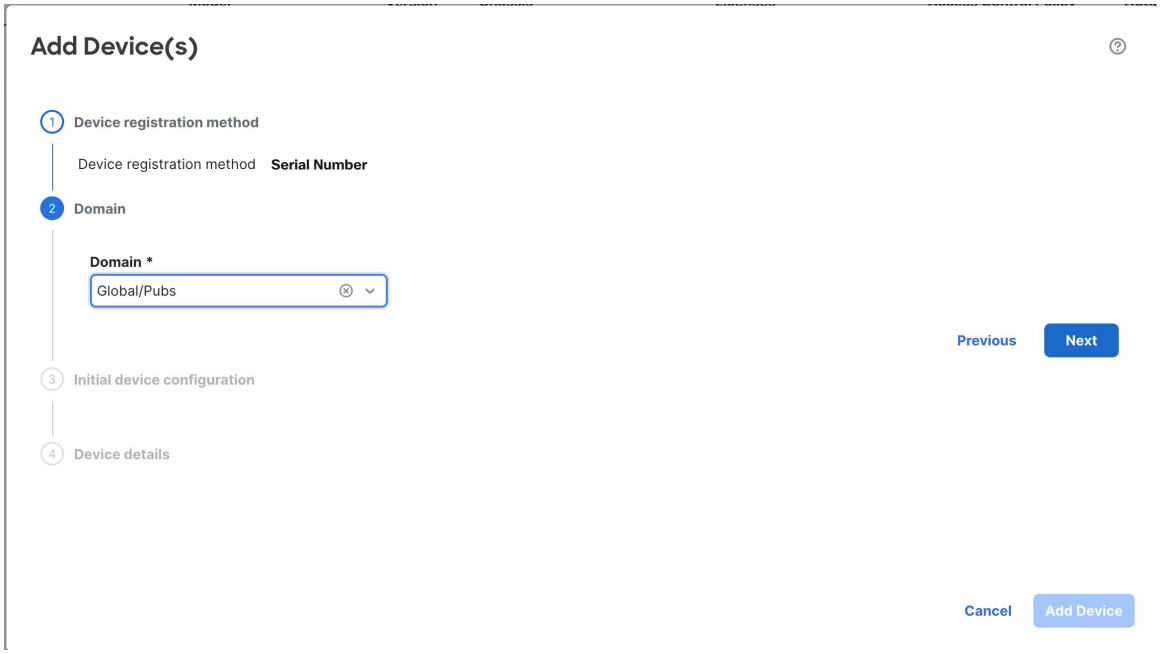
Step 5 Click **Use Serial Number** , and then click **Next** .

Figure 23: Device Registration Method



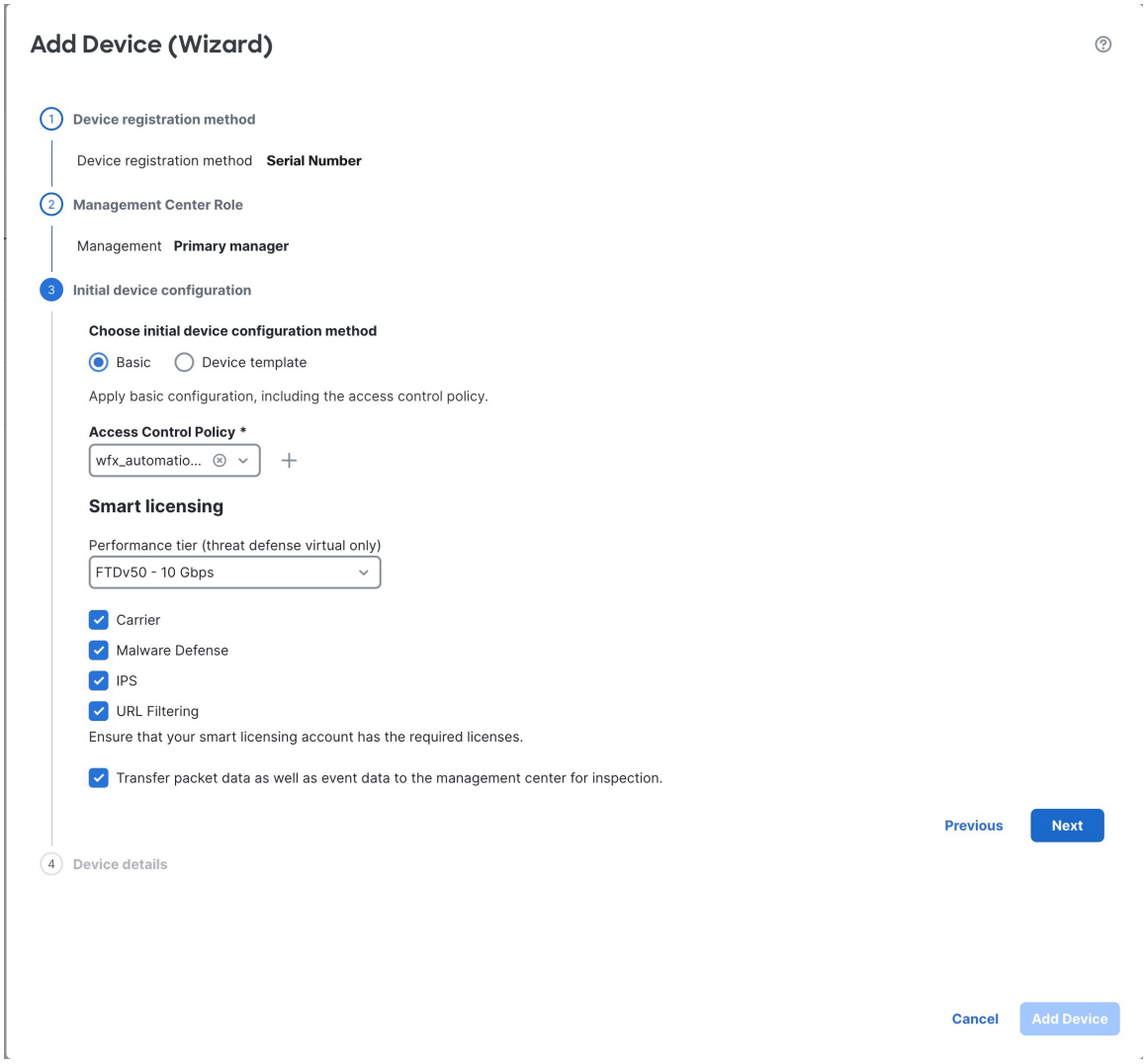
Step 6 In a multi-domain environment, choose the **Domain** from the drop-down list and click **Next** .

Figure 24: Domain



Step 7 For the **Initial device configuration**, click the **Basic** radio button.

Figure 25: Initial Device Configuration Method



a) 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.

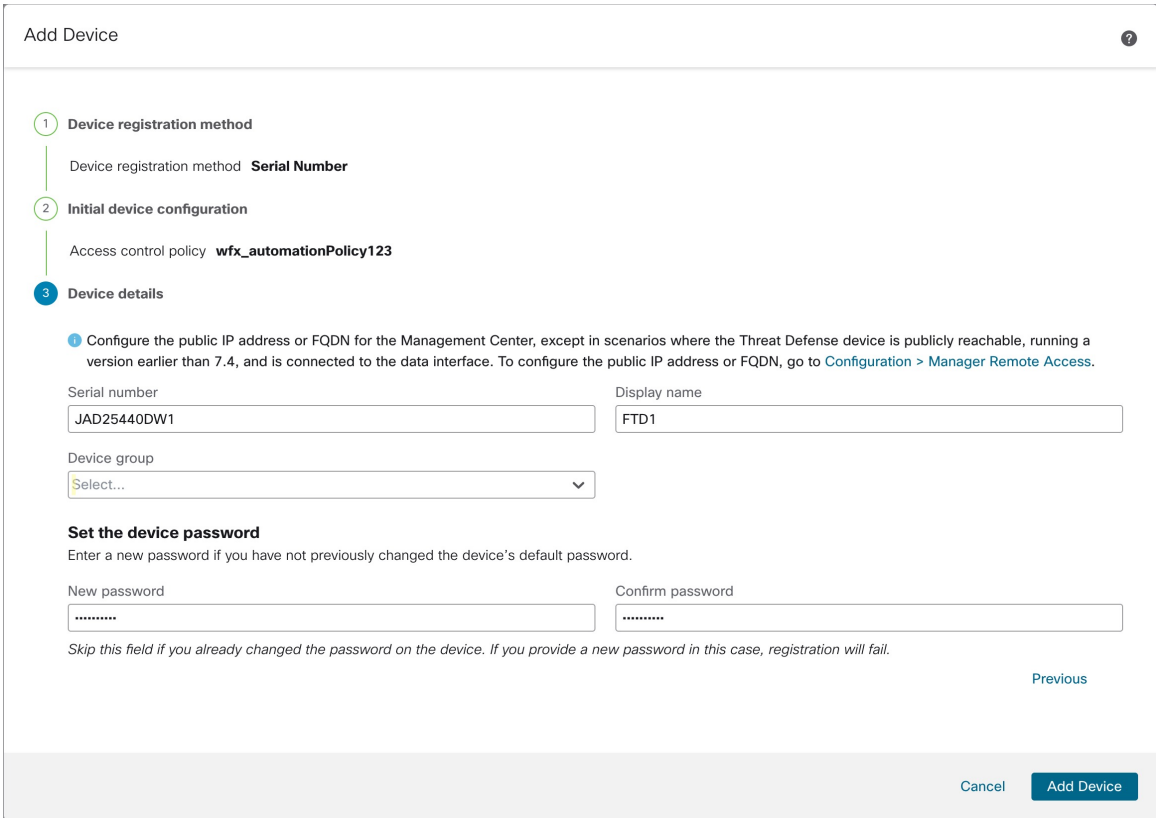
b) Choose **Smart licensing** licenses to apply to the device.

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

c) Click **Next** .

Step 8 Configure the **Device details** .

Figure 26: Device details



a) Enter the **Serial number** .
b) Enter the **Display name** as you want it to display in the Firewall Management Center
c) (Optional) Choose the **Device Group** .
d) **Set the device password** .

   If this device is unconfigured or a fresh install, then you need to set a new password. If you already logged in and changed the password, then leave this field blank. Otherwise, registration will fail.

Step 9 Click **Add Device** .

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.

When using zero-touch provisioning on the outside interface, Security Cloud Control acts as a DDNS provider and does the following:

- Enables DDNS on outside using the **FMC Only** method. This method is only supported for zero-touch provisioning devices.
- Maps the outside IP address with the following hostname: *serial-number* **.local** .
- Provides the IP address/hostname mapping to the Firewall Management Center so it can resolve the hostname to the correct IP address.
- Informs the Firewall Management Center if the IP address ever changes, for example, if the DHCP lease renews.

If you use zero-touch provisioning on the Management interface, DDNS is not supported. The Firewall Management Center must be publicly reachable so the device can initiate the management connection.

You can continue to use Security Cloud Control as the DDNS provider, or you can later change the DDNS configuration in the Firewall Management Center to a different method. See Configure Dynamic DNS for more information.

If the device fails to register, see Resolve serial number (zero-touch provisioning) registration issues, on page 66 .

Add Devices Using Serial Numbers (Zero-Touch Provisioning)—Device Template

Zero-Touch Provisioning lets you register devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with the Cisco Security Cloud and Security Cloud Control for this functionality.

You can use a template to add a device, register the device with the Firewall Management Center and bring up the device with template configurations.

Use this procedure to add devices to the Firewall Management Center using serial numbers and a device template. To add a device without using a template, see Add a device using serial number (Zero-Touch Provisioning) , on page 48 .

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 with templates 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

Before you begin

- Make sure the device is unconfigured or a fresh install. Zero-Touch Provisioning is meant for new devices only. Pre-configuration can disable zero-touch provisioning , depending on how you configure the device. If you disable zero-touch provisioning , see Resolve serial number (zero-touch provisioning) registration issues, on page 66 .
- Cable the outside interface or Management interface so it can reach the internet. If you use the outside interface for zero-touch provisioning , do not also cable the Management interface; if the Management interface gets an IP address from DHCP, the routing will be incorrect for the outside interface.
- If the device does not have a public IP address or FQDN , or you use the Management interface , set a public IP address/FQDN for the Firewall Management Center (for example, if it is behind NAT), so the device can initiate the management connection. See **System** > **Configuration** > **Manager Remote Access** .

- DHCP server for either Management or Ethernet 1/1 that provides an IP address and default gateway.
- Network access to the OpenDNS public DNS servers. IPv4: 208.67.220.220 and 208.67.222.222; IPv6: 2620:119:35::35. DNS servers obtained from DHCP are never used.

  The following names need to be resolved:

  Table 5: FQDNs for zero-touch provisioning

FQDNs
*.cisco.com (many FQDNs)
*.defenseorchestrator.com (many FQDNs)
*.defenseorchestrator.eu (for the EU, many FQDNs)
0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org
1.200.159.162.in-addr.arpa
60.19.239.178.in-addr.arpa
connected.by.freedominter.net
time.cloudflare.com
udc.neo4j.org

- 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 unregister and reregister the device.
- Create a device template according to Device Registration Using Device Templates . You must specify any required variables and network-object overrides for each device and ensure that model mapping is done for the target device model.

  We recommend that you create a checklist to ensure that all configurations in the template have been entered correctly before applying the template on the device.

  A sample checklist is given below.

  - Check version, model, operation modes.
  - Check list of variables and overrides.
  - Check sanity of variable and override values.
  - Check if the required Model Mappings exist.
  - Check if parallel device template operations are in progress.

Note If you are adding a device that will be managed by a data interface, ensure that you configure the template to be compatible with the connectivity parameters of the device. For more information, see Configure a Template for Threat Defense Devices Managed Through the Data Interface .

Procedure

Step 1 The first time you add a device using a serial number, integrate the Firewall Management Center with Cisco Security Cloud.

Note For a Firewall Management Center high-availability pair, you also need to integrate the secondary Firewall Management Center with Cisco Security Cloud.

a) Choose **Integration** > **Cisco Security Cloud** .

b) Click **Enable Cisco Security Cloud** to open a separate browser tab to log you into your Cisco Security Cloud account and confirm the displayed code.

Make sure this page is not blocked by a pop-up blocker. If you do not already have a Cisco Security Cloud and Security Cloud Control account, you can add one during this procedure.

For detailed information about this integration, see the "System Configuration" chapter in the *Cisco Secure Firewall Management Center Administration Guide* .

Security Cloud Control onboards the on-prem Firewall Management Center after you integrate the Firewall Management Center with Cisco Security Cloud. Security Cloud Control needs the Firewall Management Center in its inventory for zero-touch provisioning to operate. However, you do not need to use Security Cloud Control directly. If you do use Security Cloud Control , its Firewall Management Center support is limited to device onboarding, viewing its managed devices, viewing objects associated with the Firewall Management Center , and cross-launching the Firewall Management Center .

c) Make sure **Enable Zero-Touch Provisioning** is checked.

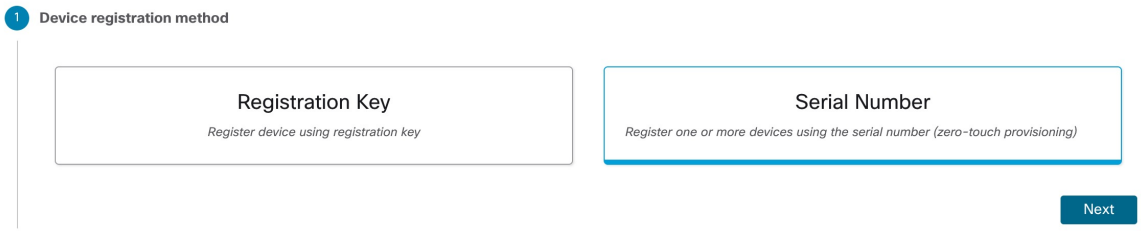
d) Click **Save** .

Step 2 Choose **Devices** > **Device Management.**.

Step 3 From the **Add** drop-down menu, choose **Device (Wizard)** .

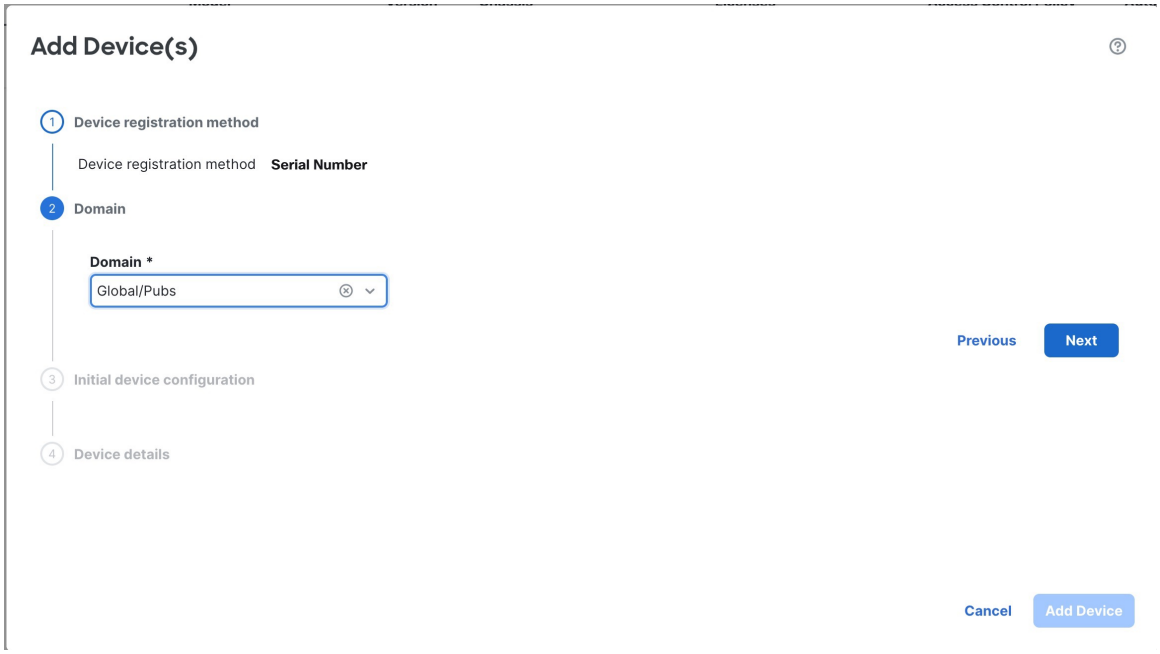
Step 4 Click **Use Serial Number** , and then click **Next** .

Figure 27: Device Registration Method



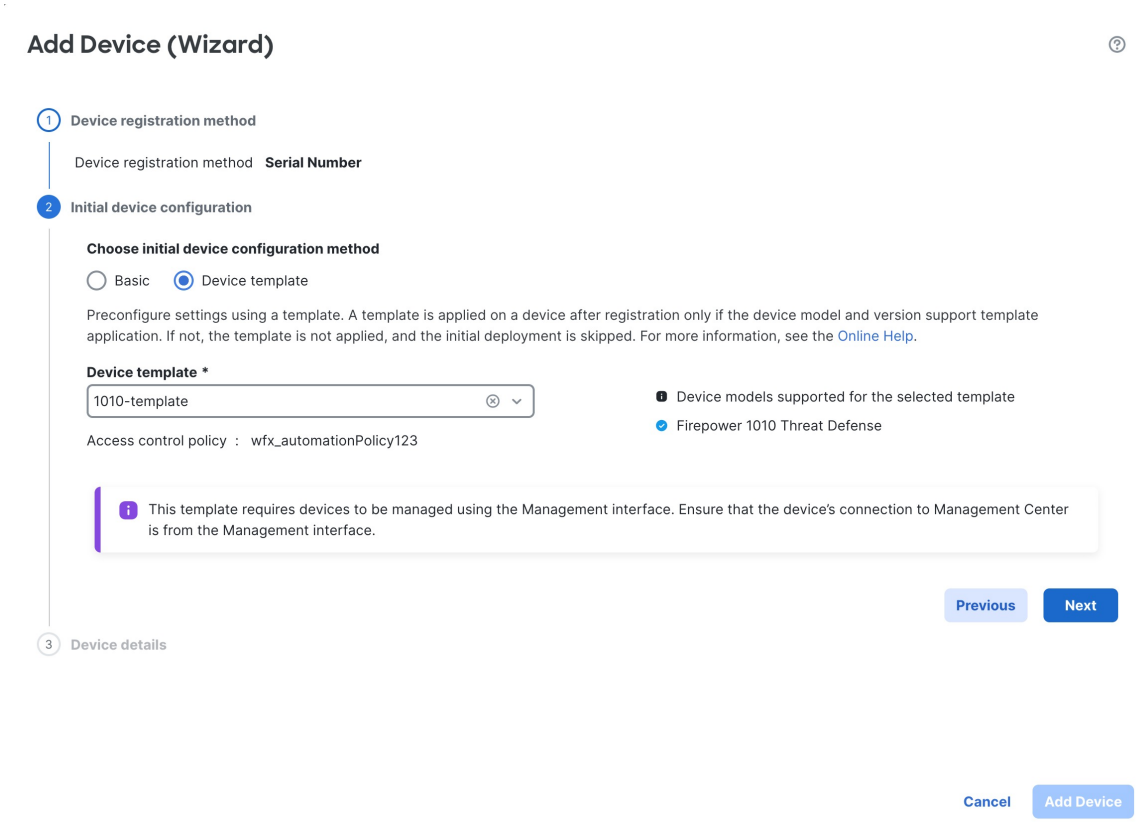
Step 5 In a multi-domain environment, choose the **Domain** from the drop-down list and click **Next** .

Figure 28: Domain



Step 6 For the **Initial device configuration** , click the **Device template** radio button.

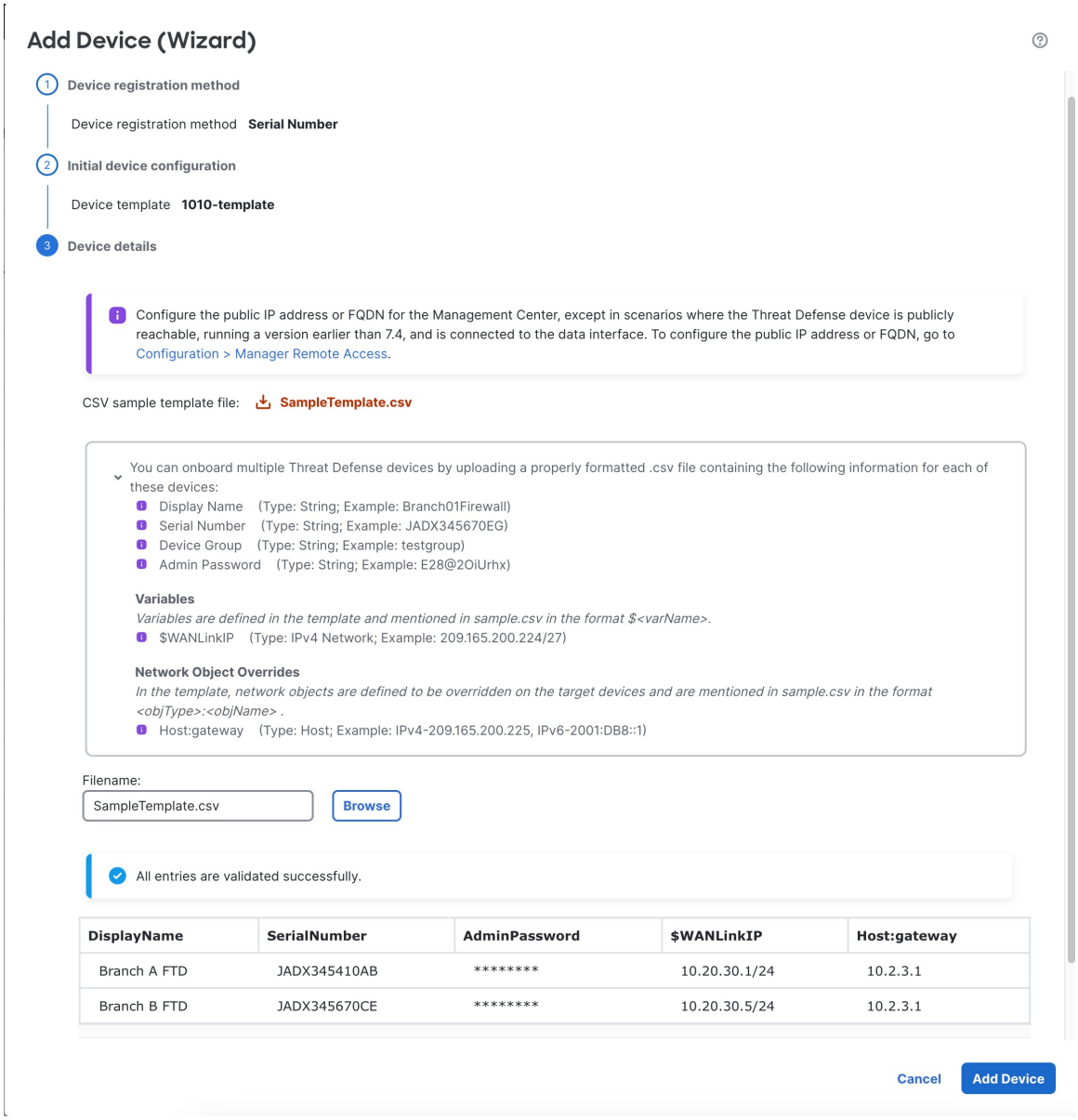
Figure 29: Initial Device Configuration



Step 7 Choose the **Device template** from the drop-down list, and click **Next** .

Step 8 In **Device details** , upload a CSV file with the device details required by the template.

Figure 30: Device Details



a) Download **SampleTemplate.csv** . This file includes all required headers for values that you need to define per device. For more information on the CSV template file fields, see CSV Template File .

b) **Drag & drop** your CSV template file or **Browse** to select the CSV template file that you want to upload. A validation check is done on the file after you upload it.

After the CSV template file has been uploaded successfully, the content of the CSV template file is displayed in a table format.

Step 9 Click **Add Device** to register the devices.

When using zero-touch provisioning on the outside interface, Security Cloud Control acts as a DDNS provider and does the following:

- Enables DDNS on outside using the "fmcOnly" method. This method is only supported for zero-touch provisioning devices.
- Maps the outside IP address with the following hostname: *serial-number* **.local** .
- Provides the IP address/hostname mapping to the Firewall Management Center so it can resolve the hostname to the correct IP address.
- Informs the Firewall Management Center if the IP address ever changes, for example, if the DHCP lease renews.

If you use zero-touch provisioning on the Management interface, DDNS is not supported. The Firewall Management Center must be publicly reachable so the device can initiate the management connection.

You can continue to use Security Cloud Control as the DDNS provider, or you can later change the DDNS configuration in the Firewall Management Center to a different method. See Configure Dynamic DNS for more information.

If the device fails to register, see Resolve serial number (zero-touch provisioning) registration issues, on page 66 .

CSV template file for serial number registration with a device template

The CSV template file must be less than 2 MB in size. The filename must satisfy specific criteria for alphanumeric characters, special characters, and length restrictions.

CSV template filename requirements:

- Can have a maximum of 64 characters.
- Only alphanumeric characters and special characters such as dash (-), period (.), and underscore (_) are allowed.
- Must not contain any spaces.

See this sample CSV template file containing configuration for two devices.

```
DisplayName,SerialNumber,AdminPassword,$WANLinkIP,Host:gateway
Branch A FTD,JADX345410AB,C15c05n0rt#,10.20.30.1/24,10.2.3.1
Branch B FTD,JADX345670CE,Admin123!,10.20.30.5/24,10.2.3.1
```

A properly formatted CSV file has the following fields.

Mandatory fields

- **DisplayName**—Name of the device. Type: string. Example: test1
- **SerialNumber**—Serial number of the device. Type: string, Example: JADX345670EG
- **AdminPassword**—(Might be required) Password for admin access, Type: string, Example: E28@2OiUrhx. If this device is unconfigured or a fresh install, then you need to set a **AdminPassword**. If you already logged in and changed the password, leave this field blank.

Optional fields

- **DeviceGroup**—Name of the device group, Type: string, Example: testgroup

Variables

Use this format: **$***varName*.

Sample variable: **$LAN-Devices-IPv4Address**—IPv4 address of the LAN device. Type: string. Example: 10.2.3.4/24.

Network object overrides

Use this format: *objType*:*objName*.

Sample network object override: **Network:LAN-Devices-Network**—IP address of the network of LAN devices. Type: string. Example: 10.2.3.0/24

FQDNs

For serial number registration, DDNS is automatically enabled. If you want to set different values from the default for the **FMC Only** type DDNS, then you can configure the settings in the template. In this case, when you provide the CSV value for the hostaname, be sure to specify it as *serialnumber***.local**.

Add a chassis

This task allows you to add a Firepower 4100/9300 chassis to the Firewall Management Center for chassis-level health monitoring and management.

You can add a Firepower 4100/9300 chassis to the Firewall Management Center. The management center and the chassis share a separate management connection using the chassis MGMT interface. The Firewall Management Center offers chassis-level health alerts. For configuration, you still need to use the Secure Firewall Chassis Manager or FXOS CLI.



Note For other models that support multi-instance mode, the chassis is added to the Firewall Management Center as part of the conversion to multi-instance mode. See Convert a device to Multi-Instance mode. However, if you used the CLI to convert to multi-instance mode (Enable multi-instance mode at the CLI), skip to Step 3, on page 63 of this procedure to add the chassis to the management center.

Procedure

Step 1 Connect to the chassis FXOS CLI, either using the console port or SSH.

Step 2 Configure the Firewall Management Center.

create device-manager *manager_name* [**hostname** {*hostname* | *ipv4_address* | *ipv6_address*}] [**NAT-ID** *nat_id*]

You are prompted for the registration key.

You can enter this command from any scope. This command is accepted immediately without using **commit-buffer**.

- **hostname** {*hostname* | *ipv4_address* | *ipv6_address*}—Specifies either the FQDN or IP address of the Firewall Management Center. At least one of the devices, either the Firewall Management Center or the chassis, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices. If you do not specify a **hostname**, then the chassis must have a reachable IP address or hostname and you must specify the **NAT-ID**.
- **NAT-ID** *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 chassis when one side does not specify a reachable IP address or hostname. It is required if you do not specify a **hostname**, however we recommend that you always set the NAT ID even when you specify a hostname or IP address. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the Firewall Management Center.
- **Registration Key:** *reg_key*—You will be prompted for a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the chassis. The registration key must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).

Example:

```
firepower# create device-manager boulder_fmc hostname 10.89.5.35 nat-id 93002
(Valid registration key characters: [a-z],[A-Z],[0-9],[-]. Length: [2-36])
Registration Key: Impala67
```

Step 3 In the Firewall Management Center, add the chassis using the chassis management IP address or hostname.

a) Choose **Devices** > **Device Management**, and then from **Add** drop-down list, choose **Chassis**.

Figure 31: Add chassis

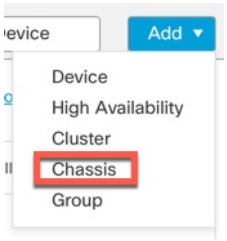
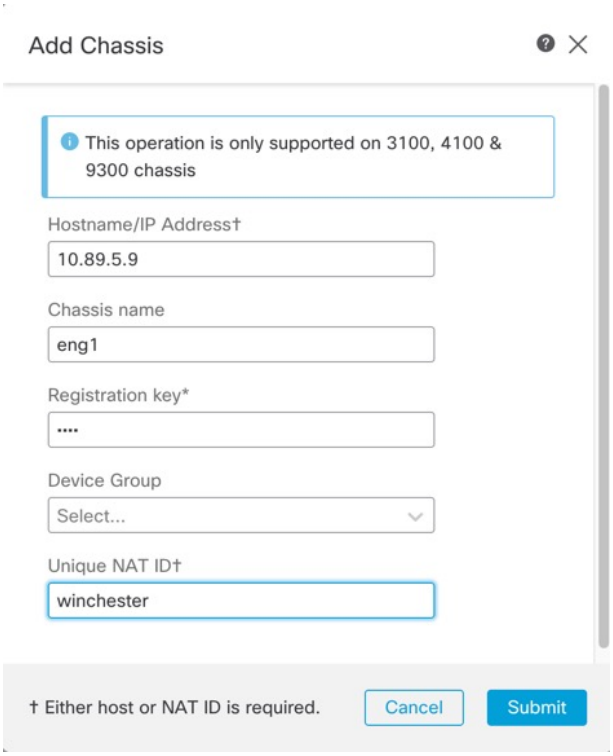


Figure 32: Add chassis



b) In the **Hostname/IP Address** field, enter the IP address or the hostname of the chassis you want to add.

If you don't know the hostname or IP address, you can leave this field blank specify the **Unique NAT ID**.

c) In the **Chassis Name** field, enter a name for the chassis as you want it to display in the Firewall Management Center.

d) In the **Registration Key** field, enter the same registration key that you used when you configured the chassis to be managed by the Firewall Management Center.

The registration key is a one-time-use shared secret. The key can include alphanumeric characters and hyphens (-).

e) In a multidomain deployment, regardless of your current domain, assign the chassis to a leaf **Domain**.

If your current domain is a leaf domain, the chassis is automatically added to the current domain. If your current domain is not a leaf domain, post-registration, you must switch to the leaf domain to configure the chassis. A chassis can only belong to one domain.

f) (Optional) Add the chassis to a **Device Group**.

g) If you used a NAT ID during chassis setup, expand enter the same NAT ID in the **Unique NAT ID** field.

The NAT ID can include alphanumeric characters and hyphens (-).

h) Click **Submit**.

The chassis is added to the **Devices** > **Device Management** page.

The chassis is successfully registered with the Firewall Management Center and appears in the device management interface for monitoring and management.

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, unregister the managed device. See Unregister a Device from the Firewall Management Center , on page 73 .

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.

Resolve serial number (zero-touch provisioning) registration issues

If the device fails to register using the serial number after 2-3 minutes, see the common causes for failure. If you have physical access to the device, Check the LED status, on page 67

If you want to bypass any serial number troubleshooting, you can always use Registration key method, on page 33.

For other requirements for serial number registration, see Add a device using serial number (Zero-Touch Provisioning) , on page 48.

"Waiting for Device to come Online" in Firewall Management Center

- **Cause**: You performed initial configuration at the CLI and unintentionally disabled zero-touch provisioning.

  Workaround: See Delete the Configured Manager at the CLI to Re-Enable Zero-Touch Provisioning, on page 69.

- **Cause**: You performed initial configuration in the Firewall Device Manager and disabled zero-touch provisioning.

  Workaround: See Restart Zero-Touch Provisioning Using the Firewall Device Manager, on page 69.

- **Cause**: Zero-Touch Provisioning is disabled, and you don't have access to the CLI.

  Workaround: See Reset the Device, on page 71.

"A device with serial number <serial-number> already exists in the Security Cloud Control tenant" in Firewall Management Center

Cause: The serial number was already claimed by another manager in your tenant.

Workaround: If you already unregistered the device or you're unsure which Firewall Management Center has claimed it, then see Check for Changes in Security Cloud Control, on page 70. If the Firewall Management Center is offline, and you need to remove its claim, see Remove a Serial-Number Claim at the CLI, on page 67.

Note If there is an active Firewall Management Center management connection, you cannot remove the claim from the current manager.

"A device with serial number <serial-number> already exists in another Security Cloud Control tenant" in Firewall Management Center

Cause: The serial number was already claimed by another manager in another tenant.

Workaround: See Remove a Serial-Number Claim at the CLI, on page 67.

Note If there is an active Firewall Management Center management connection, you cannot remove the claim from the current manager.

Check the LED status

The LED status tells you about zero-touch provisioning readiness.

Firepower 1010, 1100

Table 6: Zero-Touch Provisioning: System (S) LED behavior

S LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00

Secure Firewall 1200, 3100

Table 7: Zero-Touch Provisioning: Managed (M) LED behavior

M LED	Description	Time after firewall powered on (minutes:seconds)
Slow flashing green	Connected to the Cisco cloud and ready for onboarding	15:00 - 30:00
Alternating green and amber (error condition)	Failed to connect to the Cisco cloud	15:00 - 30:00
Solid green	Onboarded	20:00 - 45:00

Remove a Serial-Number Claim at the CLI

If the device was claimed previously, but the management connection is not active, you can clear the claim. In the Firewall Management Center , you will see an error message such as **A device with serial number <serial-number> already exists in the Security Cloud Control tenant**.

Note If there is an active Firewall Management Center management connection, you cannot remove the claim from the current manager.

Procedure

Step 1 Connect to the FXOS CLI using SSH or the console port. See Log into the Command-Line Interface on the device, on page 13 for more information.

If you used SSH, you connect to the Firewall Threat Defense CLI. In this case, enter **connect fxos** .

Note If you are accessing the Firewall Threat Defense CLI for the first time and have to run through the setup script, answer **n** when prompted: `Do you want to configure IPv4? (y/n) [y]:` and `Do you want to configure IPv6? (y/n) [y]:` . You also must accept the default local manager: `Manage the device locally? (yes/no) [yes]:` . These settings will preserve zero-touch provisioning capability.

If you used the console port, you connect directly to FXOS.

If this is the first time you connect to the CLI using either SSH or the console, you are prompted to change the password. For zero-touch provisioning when you onboard the device, for the **Password Reset** area, be sure to choose **No** because you already set the password.

```
> connect fxos
firepower#
```

Step 2 Enter local management.

connect local-mgmt

```
firepower# connect local-mgmt
firepower(local-mgmt)#
```

Step 3 Deregister the device from the Cisco cloud.

cloud deregister

```
firepower(local-mgmt)# cloud deregister
Release Image Detected RESULT=success MESSAGE=SUCCESS 10, X-Flow-Id:
2b3c9e8b-76c3-4764-91e4-cfd9828e73f9
```

Step 4 Erase the configuration to restore cloud connectivity.

erase configuration

```
firepower(local-mgmt)# erase configuration
All configurations will be erased and system will reboot. Are you sure? (yes/no):yes
Removing all the configuration. Please wait....
Configurations are cleaned up. Rebooting....
```

What to do next

-

Delete the Configured Manager at the CLI to Re-Enable Zero-Touch Provisioning

-

If you performed initial CLI setup and set the device to remote management, you can re-enable zero-touch provisioning by deleting the manager and re-adding the local manager. This setting doesn't mean you are intending to use the local manager; it just restores functionality required for zero-touch provisioning . Even if you set the manager to local, if you logged into Firewall Device Manager and completed initial setup, you may have disabled zero-touch provisioning . Deleting and re-adding the local manager will restore zero-touch provisioning .



Note You can only delete the manager if there is no current Firewall Management Center management connection.

Before you begin

-

Procedure

Step 1 Check the management status.

show managers

```
> show managers
No managers configured.
```

In this case, you opted for remote management but did not configure a Firewall Management Center . You need to set the manager to local.

```
> show managers
Managed locally.
```

This output shows you are already running the local manager. Even in this case, deleting the manager restores necessary services for zero-touch provisioning .

Step 2 Delete the manager.

configure manager delete

Step 3 Add the local manager.

configure manager local

What to do next

-

Restart Zero-Touch Provisioning Using the Firewall Device Manager

You can unintentionally disable low-touch provisioning if you log into the Firewall Device Manager and complete the initial setup in Firewall Device Manager . In this case, you can restart zero-touch provisioning

within the Firewall Device Manager . If you have access to the CLI, you can alternatively Delete the Configured Manager at the CLI to Re-Enable Zero-Touch Provisioning, on page 69 .

Procedure

Step 1 In the Firewall Device Manager , click **Device** , then click the **System Settings** > **Cloud Services** .

Step 2 Check **Auto-enroll with** Security Cloud Control **or Secure Firewall Management Center** .

Step 3 Click **Register** .

Check for Changes in Security Cloud Control

If you unregister the device from a Firewall Management Center , the claim on the serial number should be removed automatically. However, in rare cases if the claim is still active, you can force Security Cloud Control to remove the device from your inventory.

Before you begin

-

Procedure

Step 1 Log into Security Cloud Control at https://security.cisco.com.

Step 2 Choose **Security Devices** , and then search for your serial number.

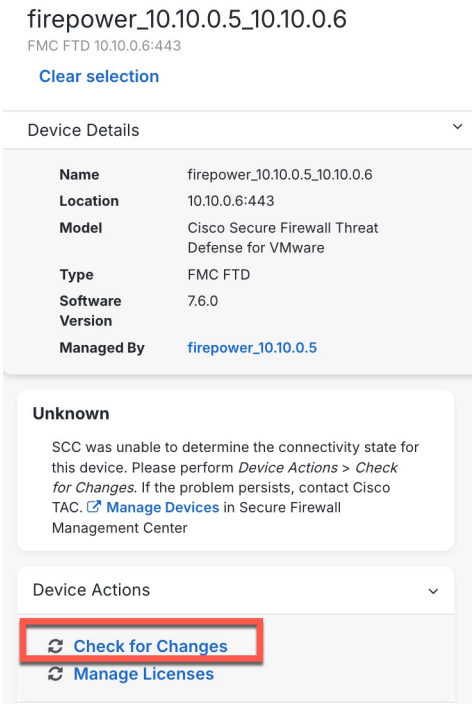
Figure 33: Search by Serial Number



If the device did not appear in the search results, it may be registered to a different tenant. In this case, see Remove a Serial-Number Claim at the CLI, on page 67.

Step 3 Select the device and click **Check for Changes** on the right.

Figure 34: Check for Changes



If the device was unregistered, it will disappear from the list and the device will attempt to connect to the cloud again.

If the device does not disappear, that means it's registered to another manager in the tenant. The name of the device includes the manager it is registered to, for example, **firepower_10.89.5.36**_1010-1. If you still want to register the device to a different manager, and you don't have access to the Firewall Management Center to unregister it, you can Remove a Serial-Number Claim at the CLI, on page 67 , but only if there is not an active management connection.

Reset the Device

If you do not have access to the CLI and want to make sure your device is unconfigured and ready for zero-touch provisioning , reset the device to its default state.

Procedure

Step 1 Press the small, recessed Reset button for longer than five seconds.

See your hardware installation guide for more information. It can take a long time to start Firewall Threat Defense for the first time after a reset.

Step 2 Check the LED status, on page 67 to monitor when the device is zero-touch provisioning -ready.

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, unregister the managed device. See Unregister a Device from the Firewall Management Center , on page 73 .

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.

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 unregister the device, be sure to export the configuration or create a template 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 or template , you will have to re-configure device settings.

After you re-add the device and either import a saved configuration , use a template, 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 , do one of the following :

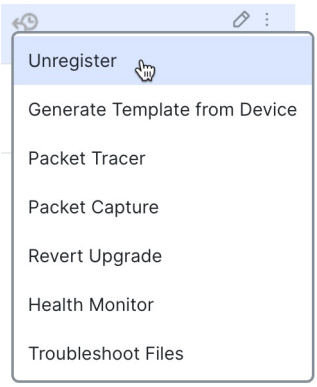
- Export the device configuration. See Export and import the device configuration .
- Create a template for the device.

Procedure

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

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

Figure 35: Unregister



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 Registration key method, on page 33 . 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 65 .
- Register to a new Firewall Management Center — Register with a new management center, on page 65 .
- Change to the Firewall Device Manager — Switch from Firewall Management Center to Firewall Device Manager , on page 88 .
- 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) Under **System**, click **Restart Device** ( ) .
b) When prompted, confirm that you want to restart the device.

Step 5 To shut down the device:

a) Under **System**, 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.

For the ISA 3000, when shutdown is complete, the System LED will turn off. Wait at least 10 seconds before you remove the power.

Download the managed device list

You can download a report of all the managed devices.

Before you begin

To perform the following task, you must be an Admin user.

Procedure

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

Step 2 Click the **Download Device List Report** link.

Step 3 You can download the device list in CSV or PDF format. Choose **Download CSV** or **Download PDF** to download the report.

Migrate Firewall Threat Defense devices

The Secure Firewall Threat Defense model migration wizard enables you to migrate configurations from an earlier Firewall Threat Defense model. After the migration, all routing and interface configurations from the source Firewall Threat Defense device are available in the target Firewall Threat Defense.

Supported devices and capabilities

The wizard supports multiple models as source and target devices, for more information see Supported Devices for Migration, on page 76.

In Version 7.6.1, the Firewall Threat Defense model migration wizard has an expanded device support, and a user-friendly interface designed to streamline your model migration. For more information, see Cisco Secure Firewall Threat Defense Model Migration Guide, Version 7.6.1.

When you migrate Firepower 4100 and 9300 Series devices to the supported models, you can now configure interface attributes according to your requirements. You can map the source device interfaces to the target device interfaces. The migration locks the source and target devices.

Supported Devices for Migration

Documents the supported migration paths and device compatibility for Cisco Firepower and Secure Firewall models.

License for Firewall Threat Defense migration

You must meet licensing requirements for Firewall Threat Defense migration.

- Your Smart Licensing account must have the license entitlements for the target device.
- You must register and enroll the device with the Smart Licensing account. The migration copies the source device licenses to the target device.

Prerequisites for migration

This reference provides comprehensive prerequisites that must be satisfied to successfully migrate configurations from a source device to a target device in Secure Firewall Management Center environments.

General device prerequisites

- Register the source and the target devices to the Firewall Management Center.
- Ensure that the target device is a newly registered device without any configurations.
- Source and target devices must be in the same state and modes:
  - Domain
  - Firewall mode: Routed or Transparent
  - Compliance mode (CC or UCAPL)
  - Management state

    Devices must have the same type of manager access interfaces (management interface or data interface).

    - Multi-instance mode or appliance mode

- Ensure that you have permission for modifications on the devices.
- Ensure that the configurations on the source device are valid and have no errors.
- Deployment, import, or export tasks must not run on either of the devices during the migration. The source device can have pending deployments.

Prerequisites for change management

- Ensure that source and target devices are not locked by a change management ticket.
- Ensure that shared policies assigned to the source device are not locked by a change management ticket.

Prerequisites for HA devices

- Migrate a device only from an active Firewall Management Center.

Prerequisites for devices in multi-instance mode

- Ensure that the source and target devices are in multi-instance mode.
- Manually migrate the chassis configurations. Create instances before migrating the instance configuration to the target instances. The target device must have compatible interfaces. For example, on the target device, you must create EtherChannel interfaces, and also create tagged, untagged, dedicated, or shared interfaces for these interfaces on the target device.

Prerequisite for devices with out-of-band configurations

- Ensure that you acknowledge out-of-band changes and match the configurations within the Firewall Management Center. You cannot migrate devices with these configurations. To view out-of-band configurations:

  1. Choose **Devices** > **Device Management**.
  2. Click the edit icon next to the device and click the **Interfaces** tab.

Prerequisites for devices with manager access interfaces

Ensure that the devices are not in Data Transit or Management Transit states. You cannot migrate if devices are in these states.

- Data Transit state: Device state when the manager access interface changes from data interface to management interface without deploying the changes on the device.
- Management Transit state: Device state when the manager access interface changes from management interface to data interface without deploying the changes on the device.

Prerequisite for devices with merged management and diagnostic interfaces

Ensure that the target device is always in merged mode.

Configurations that the wizard migrates

The migration wizard copies configurations from the source device to the target device, including licenses, interfaces, policies, routing settings, and other essential device configurations.

General configurations

The migration wizard copies these configurations from the source device to the target device:

- Licenses
- Interface configurations
- Inline sets configurations
- Routing configurations
- DHCP and DDNS configurations
- Policies
- Associated objects and object overrides
- Platform settings
- Remote branch deployment configurations

Policy configurations

The migration wizard copies these policy configurations from the source device to the target device:

- Health policy
- NAT and QoS policy
- Remote access VPN policy
- FlexConfig policy
- Access control and prefilter policy
- IPS and DNS policy
- Malware and File policy
- SSL and Identity policy
- Shared policy

Routing configurations

The migration wizard copies these routing configurations from the source device to the target device:

- ECMP
- BFD
- OSPFv2/v3
- EIGRP

- RIP
- BGP
- Policy Based Routing
- Static and Multicast Route
- Virtual Router

Interface configurations

The migration wizard copies these interfaces from the source device to the target device:

- Physical interfaces
- Sub-interfaces
- EtherChannel interfaces
  - On a standalone device, the wizard copies the EtherChannels from the source device to the target device.
  - For devices in multi-instance mode, you must create EtherChannels on the chassis and assign them to the instance.
- Bridge group interfaces
- VTI interfaces
- VNI interfaces
- Loopback interfaces
- VXLAN tunnel endpoint (VTEP) interfaces

The migration wizard retains the device group of the target device.

Guidelines and limitations for migration

Follow these guidelines to ensure successful migration of secure firewall threat defense models:

- **For devices in multi-instance mode**:

  During migration, ensure that you map the interfaces according to the table below:

Source Device	Target Device
Physical interface	Physical interface
EtherChannel interface	EtherChannel interface
Supervisor-provisioned subinterface	Supervisor-provisioned subinterface
Tagged interface	Tagged interface
Untagged interface	Untagged interface
Shared interface	Shared and dedicated interface

Source Device	Target Device
Dedicated interface	Dedicated interface

You cannot map a supervisor-provisioned subinterface to a subinterface created by an instance.

- **For HA devices**, you can migrate:
  - Source HA device to target HA device.
  - Source HA device to target standalone device.
- **For devices in remote branch deployment**:
  - Map the source manager access interface to the target manager access interface.
  - Ensure that the manager access interfaces of the source and target Firewall Management Centers are of the same IP address type (static or DHCP).
  - Both manager access interfaces must have IPv4 or IPv6 addresses.
  - If the manager access interfaces have static IP addresses, ensure that they are in the same subnet.
- **For Snort**:
- **For devices using diagnostic interfaces**:

  Only merged management interfaces are available on the target devices after migration.

Limitations

Be aware of these limitations when using the migration wizard:

- The migration wizard does not migrate:
  - Site-to-site VPN policies
  - SNMP device configurations for Firepower 2100 Series

    After the migration, you can configure SNMP using the platform settings for the device.
- You can perform only one migration at a time.
- Remote access VPN trustpoint certificates are not enrolled after migration.
- For HA devices:
  - Target device: You cannot migrate a standalone device to an HA device.
- Clustering is not supported.
- For devices in remote branch deployment:
  - The wizard does not migrate a single WAN manager access data interface to a dual WAN manager access data interface.

Migrate a secure Firewall Threat Defense

Migrate a Secure Firewall Threat Defense device from a source to a target Firewall, preserving configurations and minimizing disruptions.

Before you begin

Ensure you review Prerequisites for migration, on page 76 and Guidelines and limitations for migration, on page 79 .

Procedure

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

Step 2 Click **Migrate** in the top right corner of the page.

Step 3 In **Select source and target devices** :

a) From the **Source device** drop-down list, choose a device.

b) From the **Target device** drop-down list, choose a device.

The source and target devices can have these tags:

- Routed: Devices in routed firewall mode.
- Transparent: Devices in transparent firewall mode.
- Container: Devices in multi-instance mode.
- High Availability: Devices in high availability mode.
- Analytics Only: Devices managed by Security Cloud Control and the Firewall Management Center only recieves and displays the events (analytics-only Firewall Management Center).

If the device is part of an HA pair, only the HA pair name appears.

Step 4 Click **Next** .

Step 5 (Only for Firepower 4100 and 9300 Series devices in appliance mode) In **Chassis manager details** :

a) Check the **Skip chassis manager** check box, if required.

b) In the **Chassis hostname or IP address** field, enter the values.

Note

- Verify that the Secure Firewall Chassis Manager is reachable from the Firewall Management Center .
- Ensure you select the correct chassis manager for the source device, as Firewall Management Center does not validate your choice.

c) Click **Verify certificate** to verify the chassis manager's certificate.

d) In the **Username** and **Password** fields, enter the credentials of the chassis manager.

Step 6 Click **Next** .

Step 7 In **Configure interfaces** :

By default, the source and target interfaces are mapped using the interface hardware name. You must map named interfaces, logical interfaces, and interfaces that are part of other interfaces. Mapping of all other

interfaces is not mandatory. The wizard creates the logical interfaces according to the interface mapping that you provide.

You cannot map interfaces that are part of an HA failover configuration. These interfaces are disabled in the wizard.

Only data interfaces are available for interface mapping. Management, eventing, and diagnostic interfaces are not available for the interface mapping.

Firepower 4100 and 9300 Series devices in appliance mode :

For these devices, the Firewall Management Center fetches interface attributes such as speed, duplex, and auto-negotiation from the chassis manager.

a) Click one of the following options to configure these interface attributes on the target device:

   - **Retain target device values** : (Default) Retains the interface attributes configured on the target device.
   - **Copy from source device** : Copies the interface attributes from the source device.

     This option is enabled only when Firewall Management Center successfully connects to the chassis manager. We recommend that you use this option. The speed, duplex, and auto-negotiation values of physical interfaces are set to default values if they are incompatible in the target device.
   - **Customize device values** —Allows you to configure the values of the required interface attributes on the target device.

b) To change the interface mapping from the default ones, choose an interface from the **Mapped interface** drop-down list.
c) For EtherChannels, you can configure interface attributes and click **Add member interface** to add member interfaces.

   Interface attributes of an EtherChannel is configured based on the first member interface's interface attributes.You can add up to 16 member interfaces.

Firepower 1100 and 2100 Series devices, and Firepower 4100 and 9300 Series devices in multi-instance mode :

For these devices, you must map the source device interfaces to target device interfaces.

For Firepower 4100 and 9300 Series devices in multi-instance mode, you can only perform the interface mapping and you cannot configure the interface attributes such as speed, duplex, auto-negotiation, and FEC mode.

If you want to change the interface mapping from the default ones, choose an interface from the **Mapped interface** drop-down list.

Click **Reset** to configure the default interface mappings. For example, the wizard maps Ethernet1/1 in the source device to Ethernet1/1 in the target device.

The interfaces can have the following tags:

- Tagged: Physical interfaces on the chassis.
- Untagged: Physical interfaces on the chassis that have sub-interfaces.
- Dedicated: Interfaces that are assigned to specific instances and are not shared across multiple instances.
- Shared: Interfaces that are shared by multiple instances.

- Manager access: Data interface is the manager access interface.

Check the **Ignore warning** check box, if required.

Step 8 Click **Next** .

Step 9 Click **Submit** to start the migration.

To view the migration status, click **Notifications** (Message Center), and then click the **Tasks** tab.

A **Device Model Migration** report is generated after the migration is completed. You will see a link to this report in the **Notifications** > **Tasks** page.

What to do next

After a successful migration, you must complete these tasks:

- Review the recommendations in Best practices for Threat Defense device migration, on page 83 .
- Validate the configurations.
- Deploy the configurations on the device.

In case of a migration failure, the target device is rolled back to the initial state.

Best practices for Threat Defense device migration

After a successful migration, perform these actions before deployment to ensure proper device configuration and functionality.

- IP addresses of the interfaces are copied to the target device from the source device. Change the IP addresses of the target device interfaces if the source device is live
- Ensure that you update your NAT policies with the modified IP addresses.
- Configure the interface speeds if they are set to default values after migration.
- Re-enroll the device certificates, if any, on the target device.
- (Optional) Configure SNMP for Firepower 1100 and 2100 using the platform settings for the device.
- (Optional) Configure remote branch deployments.

  If the source or target device had manager access through a data interface, after the migration, the manager access will be lost. Update the manager access configuration on the target device. For more information, see the *Change the Manager Access Interface from Management to Data* topic in the Cisco Secure Firewall Management Center Device Configuration Guide or the Online Help.

- Configure site-to-site VPN, if required. These configurations are not migrated from the source device.
- View the deployment preview before the deployment. From the **Deploy** drop-down menu, click **Advanced Deploy**, and then click the **Preview** ( ) icon for the device.
- Monitor the health of the device in the health monitor (choose **System** ( ) > **Health** > **Monitor**). After migration, the health policy of the source device becomes the health policy of the target device. You can also configure a new health policy for the device.

After migration, the device monitoring dashboard may temporarily display redundant colored lines because the device has different UUIDs before and after migration. This redundancy appears only during the migration time. An hour after migration, the dashboard will show a single line per metric.

Switch managers

You can change between managers as 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.

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.

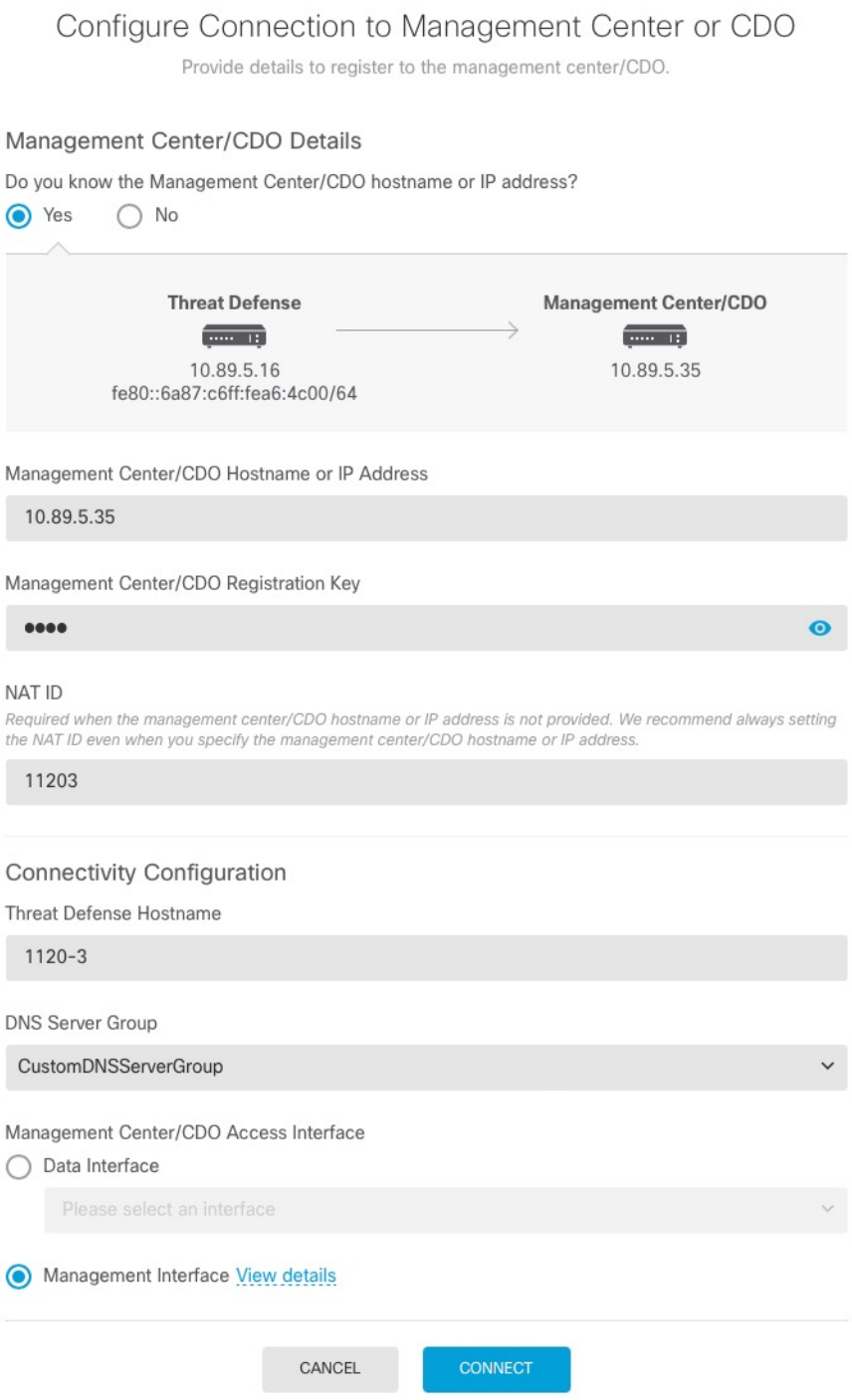
You may need to change the Management interface configuration, even if you intend to use a data interface for manager access. You will have to reconnect to the Firewall Device Manager if you were using the Management interface for the Firewall Device Manager connection.

- 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 36: 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.

d) 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/).

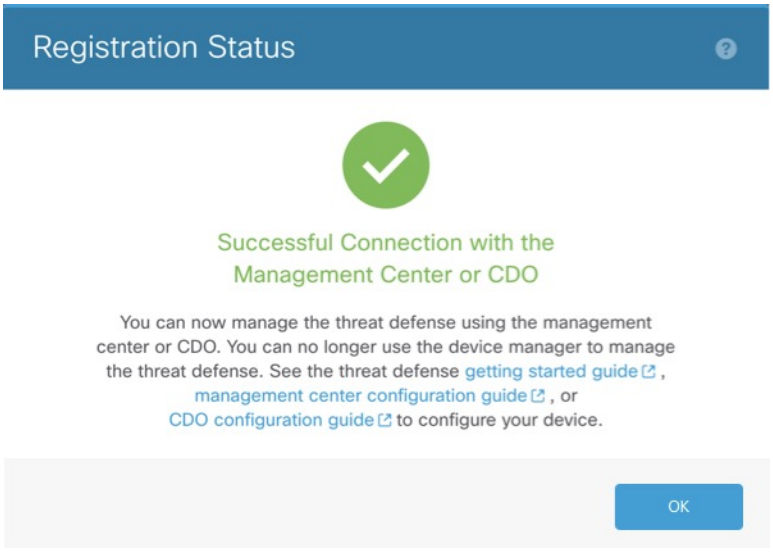
DDNS is not supported when using the Management interface for manager access.

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 37: 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 84.

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, unregister 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 in to 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
Add device by registration key using basic initial configuration added to the Device (Wizard)	7.6.1	Any	You can now use the Device (Wizard) to add a device using a registration key with a basic initial configuration. This functionality is still present on the **Add** > **Device** screen as well. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)**
Serial-number registration (zero-touch provisioning) supported from an on-prem Firewall Management Center.	7.6.0	Mgmt. center must be publicly reachable: 7.2.0 Restriction removed: 7.2.4/7.4.0	You can now register a device using its serial number from an on-prem Firewall Management Center. With templates (requires Firewall Threat Defense 7.4.1+ on the device), you can register multiple devices at once. This feature was previously known as low-touch provisioning. Requires Cisco Security Cloud. For upgraded Firewall Management Centers, your existing Security Cloud Control integration continues to work until you enable Cisco Security Cloud. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)** Supported platforms: Firepower 1000/2100, Secure Firewall 1200/3100. Note that Firepower 2100 support is for Firewall Threat Defense 7.4.1–7.4.x only; those devices cannot run Version 7.6.0.
Delete menu item renamed to **Unregister**	7.6.0	Any	The **Delete** menu choice was renamed to **Unregister** to better indicate that the device, high-availability pair, or cluster is being unregistered from the Firewall Management Center and not deleted from the high availability pair or cluster or having its configuration erased. The device, high-availability pair, or cluster continues to pass traffic until it is re-registered. New/modified screens: **Devices** > **Device Management** > **More**
Add devices using templates	7.6.0	7.4	The **Devices** > **Device Management** > **Add** > **Device (Wizard)** screen lets you add devices using a template. New/modified screens: **Devices** > **Device Management** > **Add** > **Device (Wizard)**
Disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200.	7.6.0	7.6.0	You can now disable the front panel USB-A port on the Firepower 1000 and Secure Firewall 3100/4200. By default, the port is enabled. New/modified Firewall Threat Defense CLI commands: **system support usb show**, **system support usb port disable**, **system support usb port enable** New/modified FXOS CLI commands for the Secure Firewall 3100/4200 in multi-instance mode: **show usb-port**, **disable USB port**, **enable usb-port** See: *Cisco Secure Firewall Threat Defense Command Reference* and *Cisco Firepower 4100/9300 FXOS Command Reference*

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Chassis-level health alerts for the Firepower 4100/9300.	7.4.1	7.4.1	You can now view chassis-level health alerts for Firepower 4100/9300 by registering the chassis to the Firewall Management Center as a read-only device. You must also enable the Firewall Threat Defense Platform Faults health module and apply the health policy. The alerts appear in the Message Center, the health monitor (in the left pane, under Devices, select the chassis), and in the health events view. You can also add a chassis (and view health alerts for) the Secure Firewall 3100 in multi-instance mode. For those devices, you use the Firewall Management Center to manage the chassis. But for the Firepower 4100/9300 chassis, you still must use the chassis manager or the FXOS CLI. New/modified screens: **Devices** > **Device Management** > **Add** > **Chassis**
Zero-Touch Provisioning to register the Firepower 1000/2100 and Secure Firewall 3100 to the Firewall Management Center using a serial number.	7.4.0	Mgmt. center *is* publicly reachable: 7.2.0 Mgmt. center *is not* publicly reachable: 7.2.4/7.4.0	Zero-Touch Provisioning (also called low-touch provisioning) lets you register Firepower 1000/2100 and Secure Firewall 3100 devices to the Firewall Management Center by serial number without having to perform any initial setup on the device. The Firewall Management Center integrates with SecureX and Security Cloud Control for this functionality. New/modified screens: **Devices** > **Device Management** > **Add** > **Device** > **Serial Number**

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Merged management and diagnostic interfaces.	7.4.0	7.4.0	**Upgrade impact. Merge interfaces after upgrade.** For new devices using 7.4 and later, you cannot use the legacy diagnostic interface. Only the merged management interface is available. If you upgraded to 7.4 or later and: • You did not have any configuration for the diagnostic interface, then the interfaces will merge automatically. • You have configuration for the diagnostic interface, then you have the choice to merge the interfaces manually, or you can continue to use the separate diagnostic interface. Note that support for the diagnostic interface will be removed in a later release, so you should plan to merge the interfaces as soon as possible. Merged mode also changes the behavior of AAA traffic to use the data routing table by default. The management-only routing table can now only be used if you specify the management-only interface (including Management) in the configuration. For platform settings, this means: • You can no longer enable HTTP, ICMP, or SMTP for diagnostic. • For SNMP, you can allow hosts on management instead of diagnostic. • For Syslog servers, you can reach them on management instead of diagnostic. • If Platform Settings for syslog servers or SNMP hosts specify the diagnostic interface by name, then you must use separate Platform Settings policies for merged and non-merged devices. • DNS lookups no longer fall back to the management-only routing table if you do not specify interfaces. New/modified screens: **Devices** > **Device Management** > **Interfaces** New/modified commands: **show management-interface convergence**
Migrate Firepower 1000/2100 to Secure Firewall 3100.	7.4.0	Any	You can now easily migrate configurations from the Firepower 1000/2100 to the Secure Firewall 3100. New/modified screens: **Devices** > **Device Management** > **Migrate** Platform restrictions: Migration not supported from the Firepower 1010 or 1010E.
Download a report of all registered devices.	7.4.0	Any	You can now download a report of all registered devices. On **Devices** > **Device Management** , click the new **Download Device List Report** link, at the top right of the page.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
Manage Firewall Threat Defense high availability pairs using a data interface.	7.4.0	7.4.0	Firewall Threat Defense high availability now supports using a regular data interface for communication with the Firewall Management Center. Previously, only standalone devices supported this feature. See: Device Management
ISA 3000 System LED support for shutting down.	7.0.5/7.3.0	7.0.5/7.3.0	When you shut down the ISA 3000, the System LED will turn off. You should wait at least 10 seconds before removing the power.
ISA 3000 support for shutting down.	7.0.2/7.2.0	7.0.2/7.2.0	You can now shut down the ISA 3000; previously, you could only reboot the device.
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.

Feature	Minimum Firewall Management Center	Minimum Firewall Threat Defense	Details
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**
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**