

Firewall Threat Defense Deployment with a Remote Firewall Management Center

Note Version 7.4 is the final release for the Firepower 2100.

Is This Chapter for You?

To see all available applications and managers, see Which Application and Manager is Right for You?. This chapter applies to the Firewall Threat Defense with the Firewall Management Center.

This chapter explains how to manage the Firewall Threat Defense with a Firewall Management Center located at a central headquarters. For local deployment, where the Firewall Management Center resides on your local management network, see Firewall Threat Defense Deployment with the Firewall Management Center.

About the Firewall

The hardware can run either Firewall Threat Defense software or ASA software. Switching between Firewall Threat Defense and ASA requires you to reimage the device. You should also reimage if you need a different software version than is currently installed. See Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

The firewall runs an underlying operating system called the Secure Firewall eXtensible Operating System (FXOS). The firewall does not support the FXOS Secure Firewall Chassis Manager; only a limited CLI is supported for troubleshooting purposes. See the Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense for more information.

Privacy Collection Statement—The firewall does not require or actively collect personally identifiable information. However, you can use personally identifiable information in the configuration, for example for usernames. In this case, an administrator might be able to see this information when working with the configuration or when using SNMP.

- How Remote Management Works, on page 2
- Before You Start, on page 5
- End-to-End Tasks: Zero-Touch Provisioning, on page 6
- End-to-End Tasks: Manual Provisioning, on page 8
- Central Administrator Pre-Configuration, on page 9
- Branch Office Installation, on page 22
- Central Administrator Post-Configuration, on page 24

How Remote Management Works

To allow the Firewall Management Center to manage the Firewall Threat Defense over the internet, use the outside interface for Firewall Management Center manager access instead of the Management interface. Because most remote branch offices only have a single internet connection, outside manager access makes centralized management possible.

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.

Registration Methods

Use one of the following methods to provision your Firewall Threat Defense:

Zero-Touch Provisioning (Firewall Management Center 7.4 and later, Firewall Threat Defense 7.2 and later)

1. Send the Firewall Threat Defense to the remote branch office. Do not configure anything on the device, because zero-touch provisioning may not work with pre-configured devices.

Note You can preregister the Firewall Threat Defense on the Firewall Management Center using the Firewall Threat Defense serial number before sending the device to the branch office. The Firewall Management Center integrates with the Cisco Security Cloud and Security Cloud Control for this functionality.

2. At the branch office, cable and power on the Firewall Threat Defense.
3. Finish registering the Firewall Threat Defense using the Firewall Management Center.

Manual Provisioning

1. Pre-configure the Firewall Threat Defense at the CLI or using the Firewall Device Manager, and then send the Firewall Threat Defense to the remote branch office.
2. At the branch office, cable and power on the Firewall Threat Defense.
3. Finish registering the Firewall Threat Defense using the Firewall Management Center.

Firewall Threat Defense Manager Access Interface

This guide covers **outside** interface access because it is the most likely scenario for remote branch offices. Although manager access occurs on the outside interface, the dedicated Management interface is still relevant. The Management interface is a special interface configured separately from the Firewall Threat Defense data interfaces, and it has its own network settings.

- The Management interface network settings are still used even though you are enabling manager access on a data interface.
- All management traffic continues to be sourced from or destined to the Management interface.

- When you enable manager access on a data interface, the Firewall Threat Defense forwards incoming management traffic over the backplane to the Management interface.
- For outgoing management traffic, the Management interface forwards the traffic over the backplane to the data interface.

Manager Access Requirements

Manager access from a data interface has the following limitations:

- 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.

High Availability Requirements

When using a data interface with device high availability, see the following requirements.

- 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. Alternatively, you can use the Management interface instead; DHCP is supported on Management with high availability.

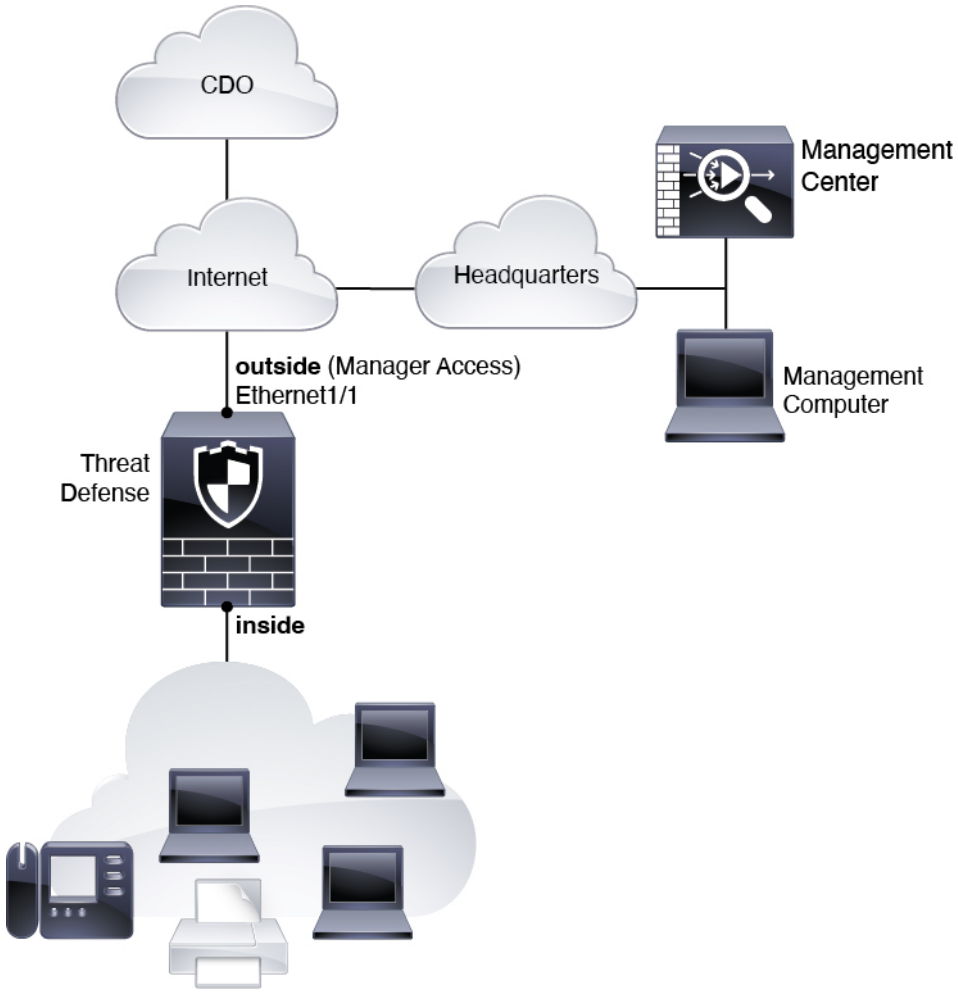
- Have different static IP addresses in the same subnet.
- Use the same manager configuration (**configure manager add** command) to ensure that the connectivity is the same.
- You cannot use the data interface as the failover or state link.

Zero-Touch Provisioning Network

The following figure shows a typical network deployment for the firewall where:

- The Firewall Management Center is at central headquarters.
- The Firewall Threat Defense uses the outside interface for manager access.
- Either the Firewall Threat Defense or Firewall Management Center needs a public IP address or hostname to allow the inbound management connection, although you do not need to know the IP address for registration. For pre-7.2(4) and 7.3 Firewall Threat Defense versions, the Firewall Management Center needs to be publicly reachable.
- Both the Firewall Management Center and Firewall Threat Defense initially communicate with the Cisco Security Cloud and Security Cloud Control to establish the management connection
- After initial establishment, Security Cloud Control is used to reestablish the management connection if it is disrupted; for example, if the Firewall Threat Defense IP address changes due to a new DHCP assignment, Security Cloud Control will inform the Firewall Management Center of the change.

Figure 1: Zero-Touch Provisioning Network

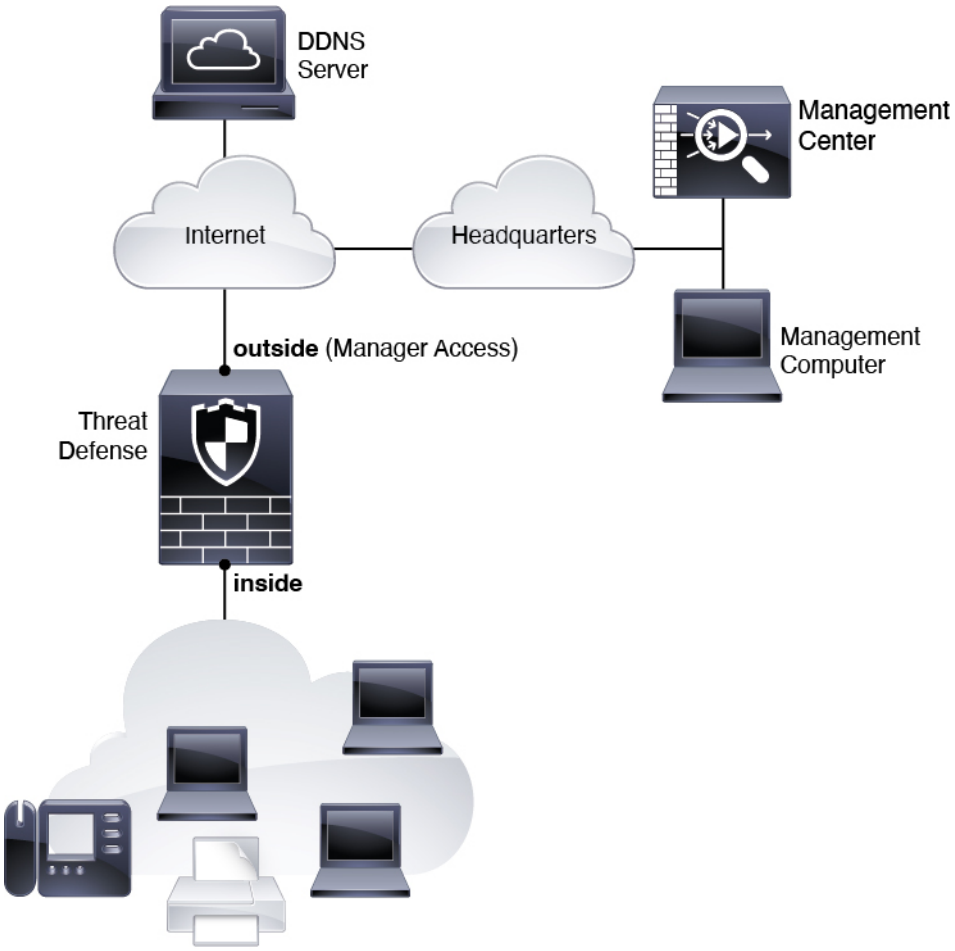


Manual Provisioning Network

The following figure shows a typical network deployment for the firewall where:

- The Firewall Management Center is at central headquarters.
- The Firewall Threat Defense uses the outside interface for manager access.
- Either the Firewall Threat Defense or Firewall Management Center needs a public IP address or hostname to allow to allow the inbound management connection; you need to know this IP address for initial setup. You can also optionally configure Dynamic DNS (DDNS) for the outside interface to accommodate changing DHCP IP assignments.

Figure 2: Manual Provisioning Network



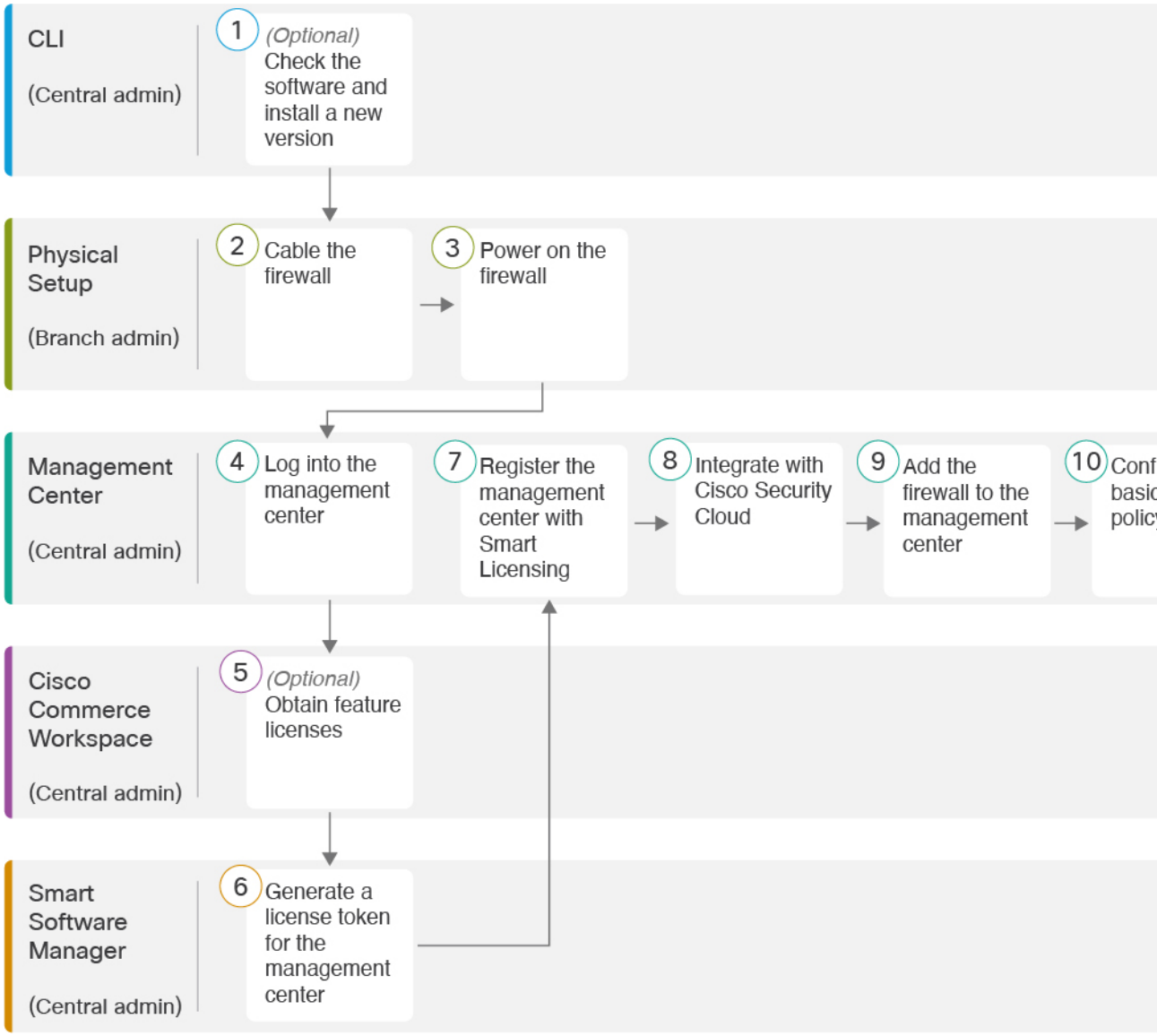
Before You Start

Deploy and perform initial configuration of the Firewall Management Center. See the getting started guide for your model.

End-to-End Tasks: Zero-Touch Provisioning

See the following tasks to deploy the Firewall Threat Defense with the Firewall Management Center using zero-touch provisioning.

Figure 3: End-to-End Tasks: Zero-Touch Provisioning



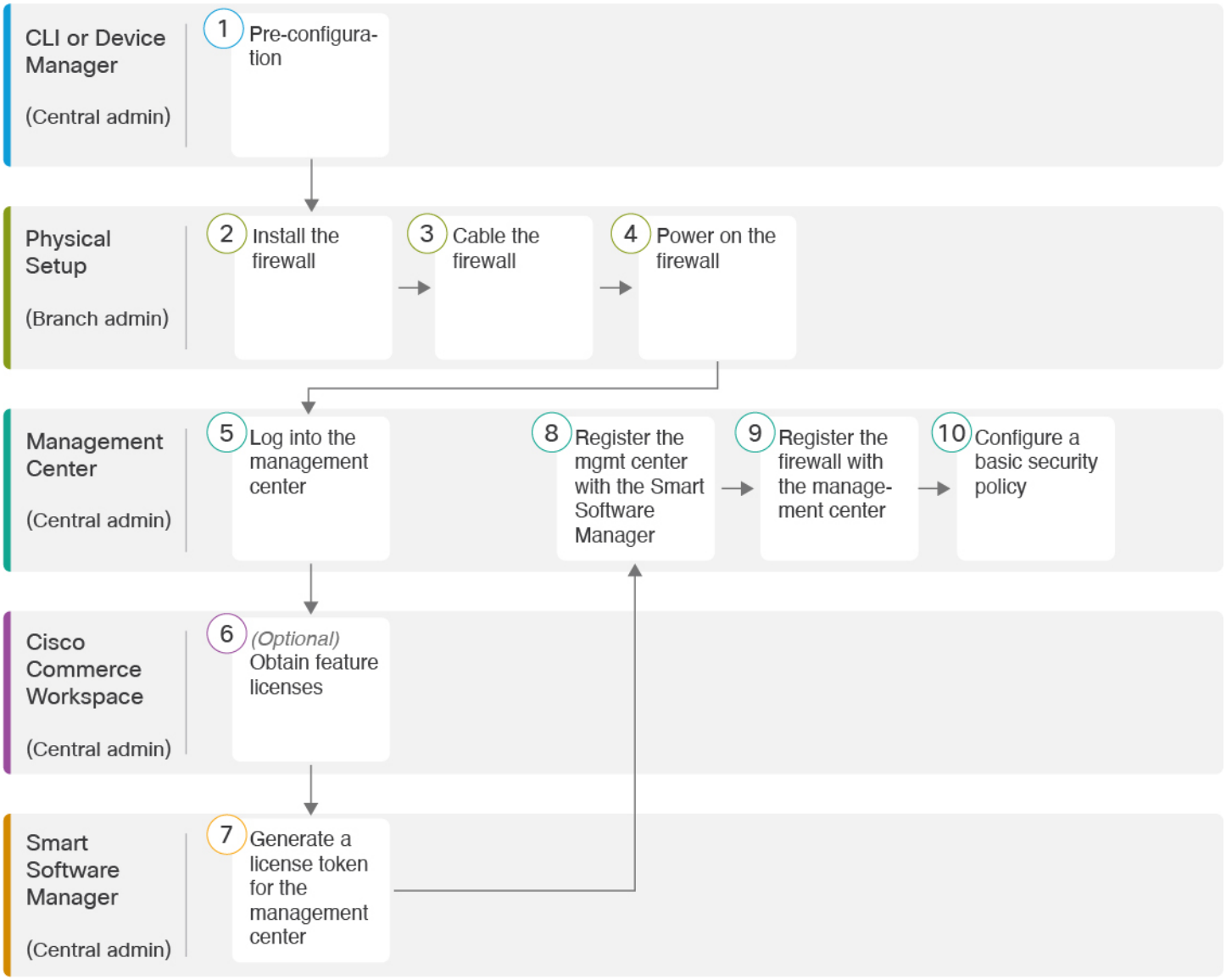
1	CLI (Central administrator)	(Optional) Check the Software and Install a New Version, on page 9.

2	Physical Setup (Branch administrator)	Cable the Firewall, on page 22.
3	Physical Setup (Branch administrator)	Power on the Device, on page 23
4	Firewall Management Center (Central administrator)	Log Into the Firewall Management Center.
5	Cisco Commerce Workspace (Central administrator)	Buy feature licenses (Obtain Licenses for the Firewall Management Center, on page 25).
6	Smart Software Manager (Central administrator)	Generate a license token for the Firewall Management Center (Obtain Licenses for the Firewall Management Center, on page 25).
7	Firewall Management Center (Central administrator)	Register the Firewall Management Center with the Smart Licensing server (Obtain Licenses for the Firewall Management Center, on page 25).
8	Firewall Management Center (Central administrator)	Add a Device Using the Serial Number (Zero-Touch Provisioning), on page 27: Integrate the Firewall Management Center with Cisco Security Cloud.
9	Firewall Management Center (Central administrator)	Add a Device Using the Serial Number (Zero-Touch Provisioning), on page 27
10	Firewall Management Center (Central administrator)	Configure a Basic Security Policy, on page 35 .

End-to-End Tasks: Manual Provisioning

See the following tasks to deploy the Firewall Threat Defense with the Firewall Management Center using manual provisioning.

Figure 4: End-to-End Tasks: Manual Provisioning



1	CLI or Firewall Device Manager (Central admin)	• (Optional) Check the Software and Install a New Version, on page 9 • Pre-Configuration Using the Firewall Device Manager, on page 11 • Pre-Configuration Using the CLI, on page 17

2	Physical Setup (Branch admin)	Install the firewall. See the Cisco Firepower 2100 Series Hardware Installation Guide.
3	Physical Setup (Branch admin)	Cable the Firewall, on page 22.
4	Physical Setup (Branch admin)	Power on the Device, on page 23
5	Firewall Management Center (Central admin)	Log Into the Firewall Management Center.
6	Cisco Commerce Workspace (Central admin)	Obtain Licenses for the Firewall Management Center, on page 25: Buy feature licenses.
7	Smart Software Manager (Central admin)	Obtain Licenses for the Firewall Management Center, on page 25: Generate a license token for the Firewall Management Center.
8	Firewall Management Center (Central admin)	Obtain Licenses for the Firewall Management Center, on page 25: Register the Firewall Management Center with the Smart Licensing server.
9	Firewall Management Center (Central admin)	Add a Device to the Firewall Management Center Manually, on page 32.
10	Firewall Management Center (Central admin)	Configure a Basic Security Policy.

Central Administrator Pre-Configuration

You might need to manually pre-configure the Firewall Threat Defense before you send it to the branch office.

(Optional) Check the Software and Install a New Version

To check the software version and, if necessary, install a different version, perform these steps. We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

What Version Should I Run?

Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html; for example, this bulletin describes short-term release numbering (with the latest features), long-term release numbering (maintenance releases and patches for a longer period of time), or extra long-term release numbering (maintenance releases and patches for the longest period of time, for government certification).

Procedure

Step 1 Connect to the CLI. See Access the Firewall Threat Defense and FXOS CLI, on page 49 for more information. This procedure shows using the console port, but you can use SSH instead.

Log in with the **admin** user and the default password, **Admin123**.

You connect to the FXOS CLI. The first time you log in, 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 perform a factory reset to reset the password to the default. See the FXOS troubleshooting guide for the factory reset procedure.

Example:

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

[...]

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

[...]

firepower#
```

Step 2 At the FXOS CLI, show the running version.

scope ssa

show app-instance

Example:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.6.0.65        7.6.0.65
        Not Applicable
```

Step 3 If you want to install a new version, perform these steps.

a) If you need to set a static IP address for the Management interface, see Complete the Firewall Threat Defense Initial Configuration Using the CLI. By default, the Management interface uses DHCP.

You will need to download the new image from a server accessible from the Management interface.

b) Perform the reimage procedure in the FXOS troubleshooting guide.

After the firewall reboots, you connect to the FXOS CLI again.

c) At the FXOS CLI, you are prompted to set the admin password again.

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.

d) Shut down the device. See Power Off the Device at the CLI, on page 56.

Perform Initial Configuration (Manual Provisioning)

For manual provisioning, perfom initial configuration of the Firewall Threat Defense using the CLI or using the Firewall Device Manager.

Pre-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— "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).

Procedure

Step 1 Connect your management computer to the Inside (Ethernet 1/2) interface.

Step 2 Power on the firewall.

Note
The first time you boot up the Firewall Threat Defense, initialization can take approximately 15 to 30 minutes.

Step 3 Log in to the Firewall Device Manager.

a) Enter the following URL in your browser: **https://192.168.95.1**

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 4 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 configuraton for the inside interface (Ethernet1/2), you will have configuration for an outside (Ethernet1/1) interface that will be maintained when you switch to 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 intial setup at the CLI.

   The Management interface settings are used even though you are enabling the 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 5 (Might be required) Configure the Management interface. See the Management interface on **Device** > **Interfaces**.

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.

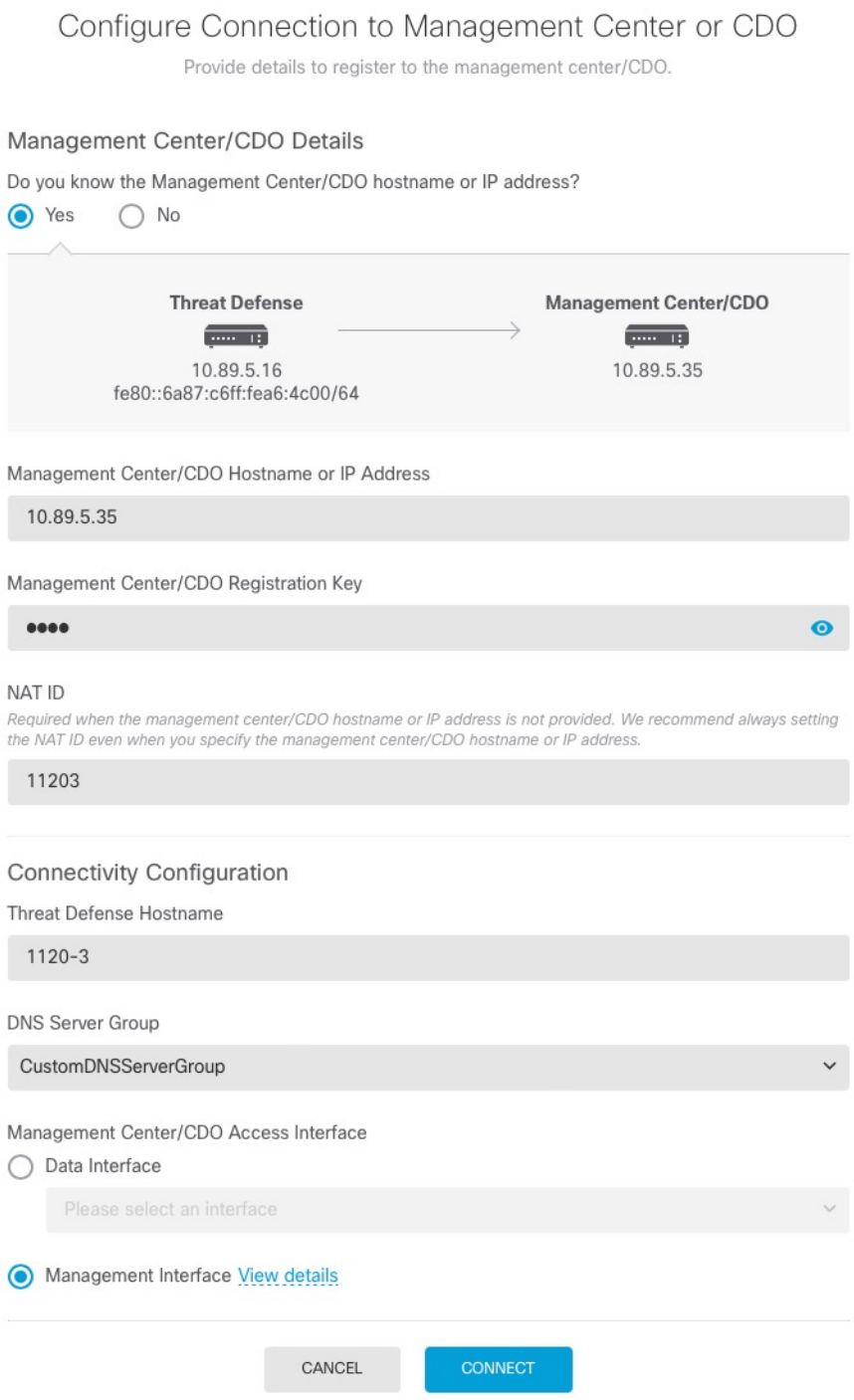
Step 6 If you want to configure additional interfaces, including an interface other than outside or inside that you want to use for the manager access, choose **Device**, and then click the link in the **Interfaces** summary.

See Configure the Firewall in the Firewall Device Manager for more information about configuring interfaces in the Firewall Device Manager. Other Firewall Device Manager configuration will not be retained when you register the device to the Firewall Management Center.

Step 7 Choose **Device** > **System Settings** > **Central Management**, and click **Proceed** to set up the Firewall Management Center management.

Step 8 Configure the **Management Center/CDO Details**.

Figure 5: 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 Center is behind NAT or does not have a public IP address or hostname.

At least one of the devices, either the Firewall Management Center or the Firewall Threat Defense device, must have a reachable IP address to establish the two-way, TLS-1.3-encrypted communication channel between the two devices.

b) If you chose **Yes**, then enter the **Management Center/CDO Hostname or IP Address**.

c) Specify the **Management Center/CDO Registration Key**.

This key is a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense device. The registration key must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID can be used for multiple devices registering to the Firewall Management Center.

a) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the Firewall Management Center. The NAT ID must be between 2 and 36 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other devices registering to the Firewall Management Center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked. We recommended that you always use the NAT ID even when it is optional, but it is required if:

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

Step 9 Configure the **Connectivity Configuration**.

a) Specify the **FTD Hostname**.

This FQDN will be used for the outside interface, or whichever interface you choose for the **Management Center/**Security Cloud Control**Access 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.

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 likley 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. 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.

c) For the **Management Center/**Security Cloud Control **Access Interface**, choose **outside**.

You can choose any configured interface, but this guide assumes you are using outside.

Step 10 If you chose a different data interface from outside, 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. See Configure the Firewall in the Firewall Device Manager for more information about configuring static routes in the Firewall Device Manager.

Step 11 Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense at its Fully-Qualified Domain Name (FQDN) if the Firewall Threat Defense's IP address changes. See **Device** > **System Settings** > **DDNS Service** to configure DDNS.

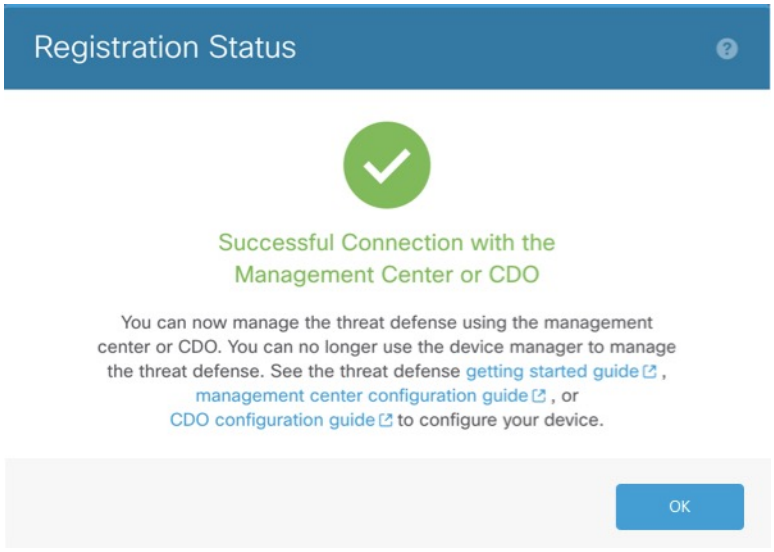
If you configure DDNS before you add the Firewall Threat Defense to the Firewall Management Center, the Firewall Threat Defense automatically adds certificates for all of the major CAs from the Cisco Trusted Root CA bundle so that the Firewall Threat Defense can validate the DDNS server certificate for 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/).

Step 12 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 6: Successful Connection



Pre-Configuration Using the CLI

Set the Management IP address, gateway, and other basic networking settings using the setup wizard. When you use the CLI for initial configuration, only the Management interface and manager access interface settings are retained. When you perform initial setup using the Firewall Device Manager (7.1 and later), *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.

Procedure

Step 1 Power on the firewall.

Note
The first time you boot up the Firewall Threat Defense, initialization can take approximately 15 to 30 minutes.

Step 2 Connect to the Firewall Threat Defense CLI on the console port.

The console port connects to the FXOS CLI.

Step 3 Log in with the username **admin** and the password **Admin123**.

The first time you log in to the 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, then you must reimage the device to reset the password to the default. See the FXOS troubleshooting guide for the reimage procedure.

Example:

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

[...]

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

[...]

firepower#
```

Step 4 Connect to the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

Step 5 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 for the Management interface settings.

The Management interface settings are used even though you are enabling manager access on a data interface.

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 Cisco Secure Firewall Threat Defense Command Reference.

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

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. Although you do not plan to use the Management interface, you must set an IP address, for example, a private address.
- **Configure IPv4 via DHCP or manually?** and/or **Configure IPv6 via DHCP, router, or manually?**—Choose **manual**. 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 **Enter the IPv6 gateway for 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.
- **Manage the device locally?**—Enter **no** to use the Firewall Management Center. A **yes** answer means you will use the Firewall Device Manager instead.
- **Configure firewall mode?**—Enter **routed**. Outside manager access is only supported in routed firewall mode.

Example:

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

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

System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
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: data 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 6 Configure the outside interface for manager access.

configure network management-data-interface

You are then prompted to configure basic network settings for the outside interface. See the following details for using this command:

- The 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 beforehand using the **configure network** {**ipv4** | **ipv6**} **manual** command. If you did not already set the Management interface gateway to **data-interfaces**, this command will set it now.
- When you add the 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 the 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.
- 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 Firewall Threat Defense 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 managemement, enter the **configure network management-data-interface disable** command.

Example:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://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 7 (Optional) Limit data interface access to the Firewall Management Center on a specific network.

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

By default, all networks are allowed.

Step 8 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*]

- {*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**. 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, SSL-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 not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-).
- *nat_id*—Specifies a unique, one-time string of your choice that you will also specify on the Firewall Management Center. When you use a data interface for management, then you must specify the NAT ID on *both* the Firewall Threat Defense and the Firewall Management Center for registration. 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.

Example:

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

Step 9 Shut down the Firewall Threat Defense so you can send the device to the remote branch office.

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 system.

a) Enter the **shutdown** command.
b) Observe the Power LED and Status LED to verify that the chassis is powered off (appear unlit).
c) After the chassis has successfully powered off, you can then unplug the power to physically remove power from the chassis if necessary.

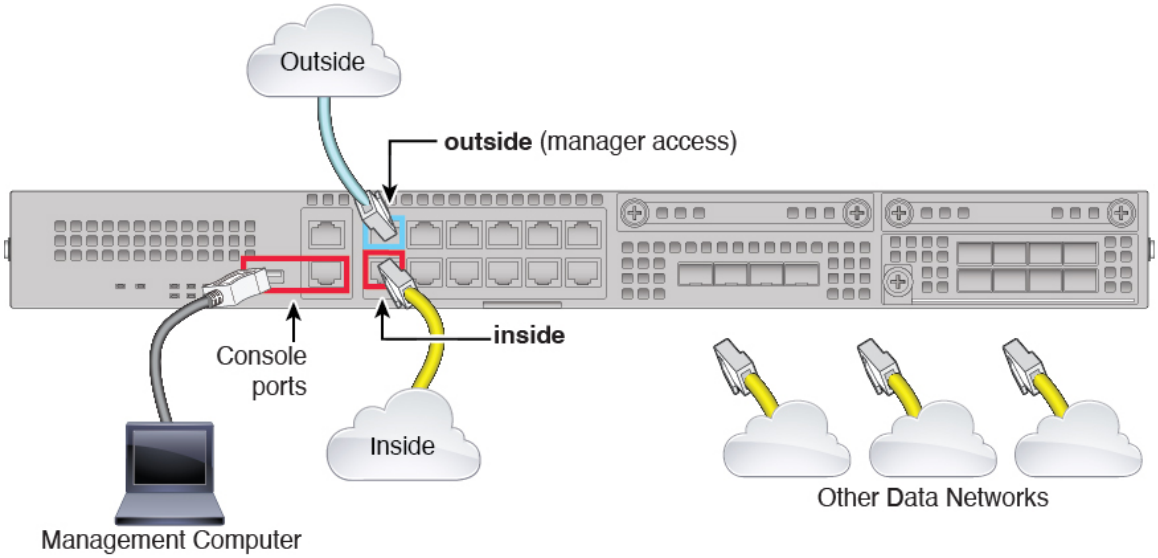
Branch Office Installation

After you receive the Firewall Threat Defense from central headquarters, you only need to cable and power on the firewall so that it has internet access from the outside interface. The central administrator can then complete the configuration.

Cable the Firewall

The Firewall Management Center and your management computer reside at a remote headquarters, and can reach the Firewall Threat Defense over the internet. To cable the Firepower 2100, see the following steps.

Figure 7: Cabling a Remote Management Deployment



Procedure

Step 1 Install the chassis. See the Cisco Firepower 2100 Series Hardware Installation Guide.

Step 2 Connect the outside interface (Ethernet 1/1) to your outside router.

Step 3 Connect the inside interface (for example, Ethernet 1/2) to your inside switch or router.

Step 4 Connect other networks to the remaining interfaces.

Step 5 (Optional) Connect the management computer to the console port.

At the branch office, the console connection is not required for everyday use; however, it may be required for troubleshooting purposes.

Power on the Device

The power switch is located to the left of power supply module 1 on the rear of the chassis. It is a toggle switch that controls power to the system. If the power switch is in standby position, only the 3.3-V standby power is enabled from the power supply module and the 12-V main power is OFF. When the switch is in the ON position, the 12-V main power is turned on and the system boots.

Note The first time you boot up the Firewall Threat Defense, initialization can take approximately 15 to 30 minutes.

Before you begin

It's important that you provide reliable power for your device (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are

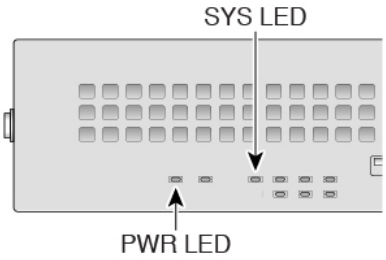
many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

Procedure

Step 1 Attach the power cord to the device and connect it to an electrical outlet.

Step 2 Press the power switch on the back of the device.

Step 3 Check the PWR LED on the front of the device; if it is solid green, the device is powered on.



Step 4 Check the SYS LED on the front of the device; after it is solid green, the system has passed power-on diagnostics.

Note
Before you move the power switch to the OFF position, use the shutdown commands so that the system can perform a graceful shutdown. This may take several minutes to complete. After the graceful shutdown is complete, the console displays `It is safe to power off now`. The front panel blue locator beacon LED lights up indicating the system is ready to be powered off. You can now move the switch to the OFF position. The front panel PWR LED flashes momentarily and turns off. Do not remove the power until the PWR LED is completely off.

See the FXOS Configuration Guide for more information on using the shutdown commands.

Central Administrator Post-Configuration

After the remote branch administrator cables the Firewall Threat Defense so it has internet access from the outside interface, you can register the Firewall Threat Defense to the Firewall Management Center and complete configuration of the device.

Log Into the Firewall Management Center

Use the Firewall Management Center to configure and monitor the Firewall Threat Defense.

Procedure

Step 1 Using a supported browser, enter the following URL.

https://*fmc_ip_address*

Step 2 Enter your username and password.

Step 3 Click **Log In**.

Obtain Licenses for the Firewall Management Center

All licenses are supplied to the Firewall Threat Defense by the Firewall Management Center. You can optionally purchase the following feature licenses:

- Essentials—Required
- IPS
- Malware Defense
- URL Filtering
- Cisco Secure Client

For a more detailed overview on Cisco Licensing, go to cisco.com/go/licensingguide

Before you begin

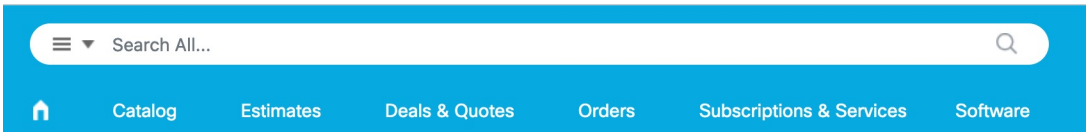
- When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. If you don't have an account on the Smart Software Manager, click the link to set up a new account.
- If you have not already done so, register the Firewall Management Center with the Smart Software Manager. Registering requires you to generate a registration token in the Smart Software Manager. See the Cisco Secure Firewall Management Center Administration Guide for detailed instructions.

Procedure

Step 1 Make sure your Smart Licensing account contains the available licenses you need.

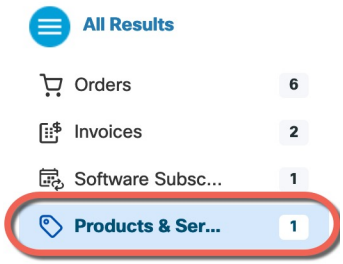
If you need to add licenses yourself, go to Cisco Commerce Workspace and use the **Search All** field.

Figure 8: License Search



Choose **Products & Services** from the results.

Figure 9: Results



Search for the following license PIDs:

Note
If a PID is not found, you can add the PID manually to your order.

- IPS, Malware Defense, and URL combination:
  - L-FPR2110T-TMC=
  - L-FPR2120T-TMC=
  - L-FPR2130T-TMC=
  - L-FPR2140T-TMC=

  When you add one of the above PIDs to your order, you can then choose a term-based subscription corresponding with one of the following PIDs:
  - L-FPR2110T-TMC-1Y
  - L-FPR2110T-TMC-3Y
  - L-FPR2110T-TMC-5Y
  - L-FPR2120T-TMC-1Y
  - L-FPR2120T-TMC-3Y
  - L-FPR2120T-TMC-5Y
  - L-FPR2130T-TMC-1Y
  - L-FPR2130T-TMC-3Y
  - L-FPR2130T-TMC-5Y
  - L-FPR2140T-TMC-1Y
  - L-FPR2140T-TMC-3Y
  - L-FPR2140T-TMC-5Y
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

Step 2 If you have not already done so, register the Firewall Management Center with the Smart Software Manager.

Registering requires you to generate a registration token in the Smart Software Manager. See the Firewall Management Center configuration guide for detailed instructions.

Register the Firewall Threat Defense with the Firewall Management Center

Register the Firewall Threat Defense with the Firewall Management Center depending on which deployment method you are using.

Add a Device Using the 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.

Note For Firewall Management Center version 7.4, you need to add the device using Security Cloud Control; see the 7.4 guide for more information. The native Firewall Management Center workflow was added in 7.6. Also, for cloud integration in 7.4, see the **SecureX Integration** page in the Firewall Management Center.

Default Configuration After Registration

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 , the VLAN1 interface)— "inside", 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

Requirements

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. Alternatively, you can use the Management interface instead; DHCP is supported on Management with high availability.

Before you begin

- If the device does not have a public IP address or FQDN, 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 .
- 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 1: 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

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 Security Cloud Control 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 the Cisco Security Cloud and Security Cloud Control account, you can add one during this procedure.

   For detailed information about this integration, see .

   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.

The device includes two serial numbers: the chassis serial number and the PCB (circuit board) serial number. Either serial number should work.

- If you have the shipping box, you can see the chassis serial number on the label.
- The chassis serial number is on the compliance label on a pull-out tab at the front of the device.
- The PCB serial number is on a label on the chassis called "S/N."
- You can view the serial numbers using the following CLI commands:
  - FXOS—**show chassis detail** shows both serial numbers.
  - Firewall Threat Defense—**show inventory** shows the chassis serial number. **show serial-number** shows the PCB serial number.

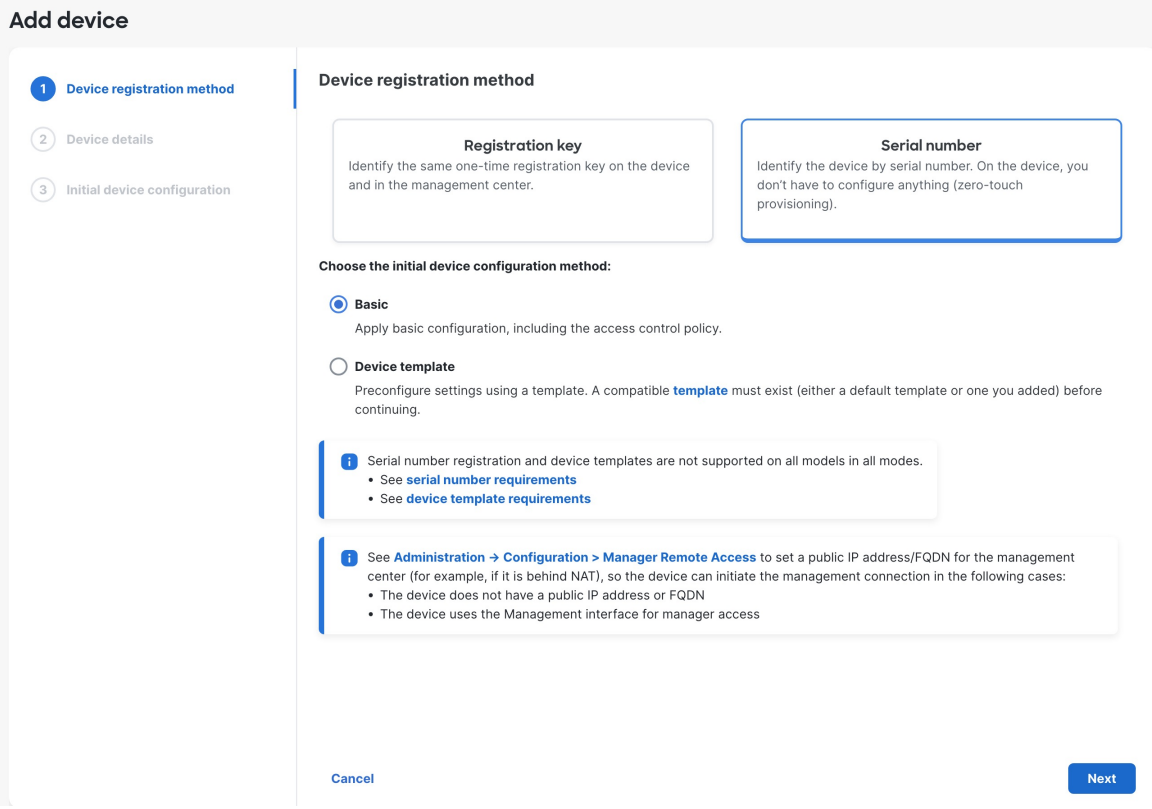
Step 3 Check your LEDs to make sure the firewall is ready for registration.

Step 4 Choose **Devices** > **Device Management**.

Step 5 From the **Add** drop-down menu, choose **Device (Wizard)**.

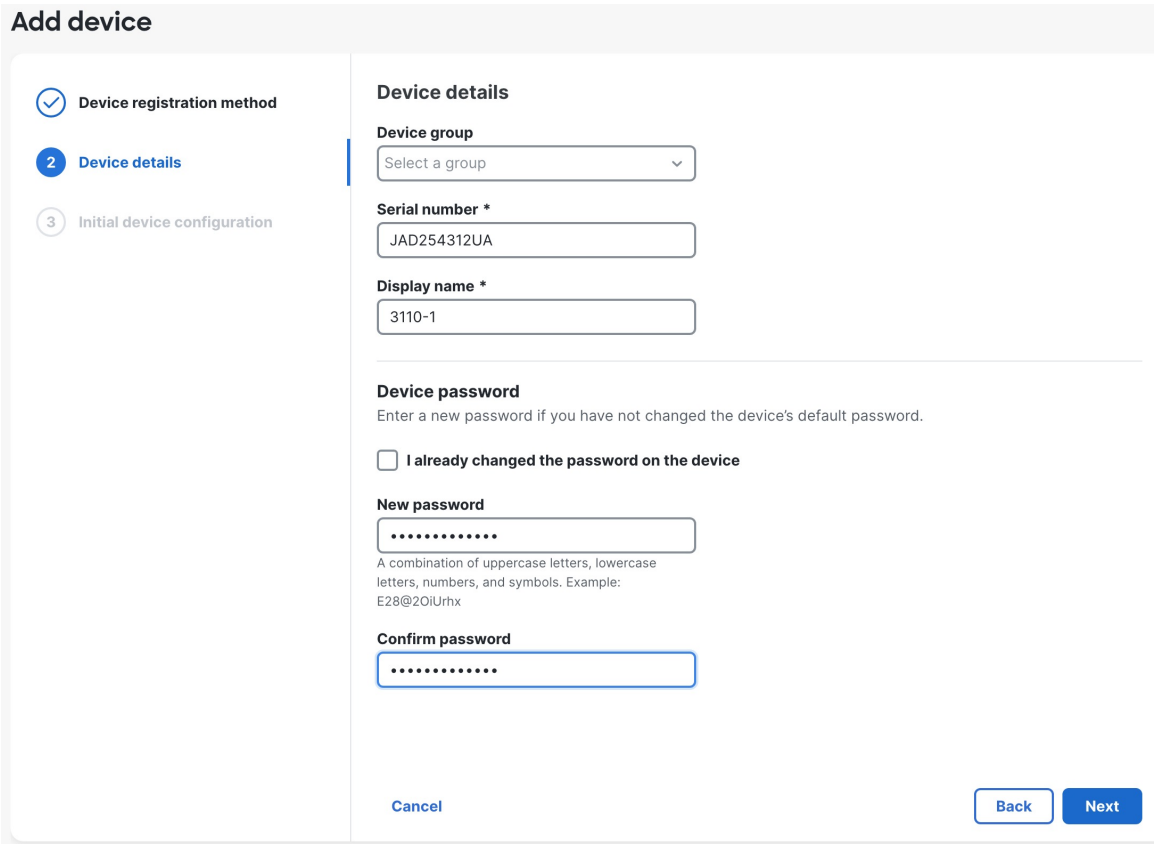
Step 6 Click **Serial Number**, click **Basic**, and then click **Next**.

Figure 10: Device Registration Method



Step 7 Configure the device details and click **Next**.

Figure 11: Device Details

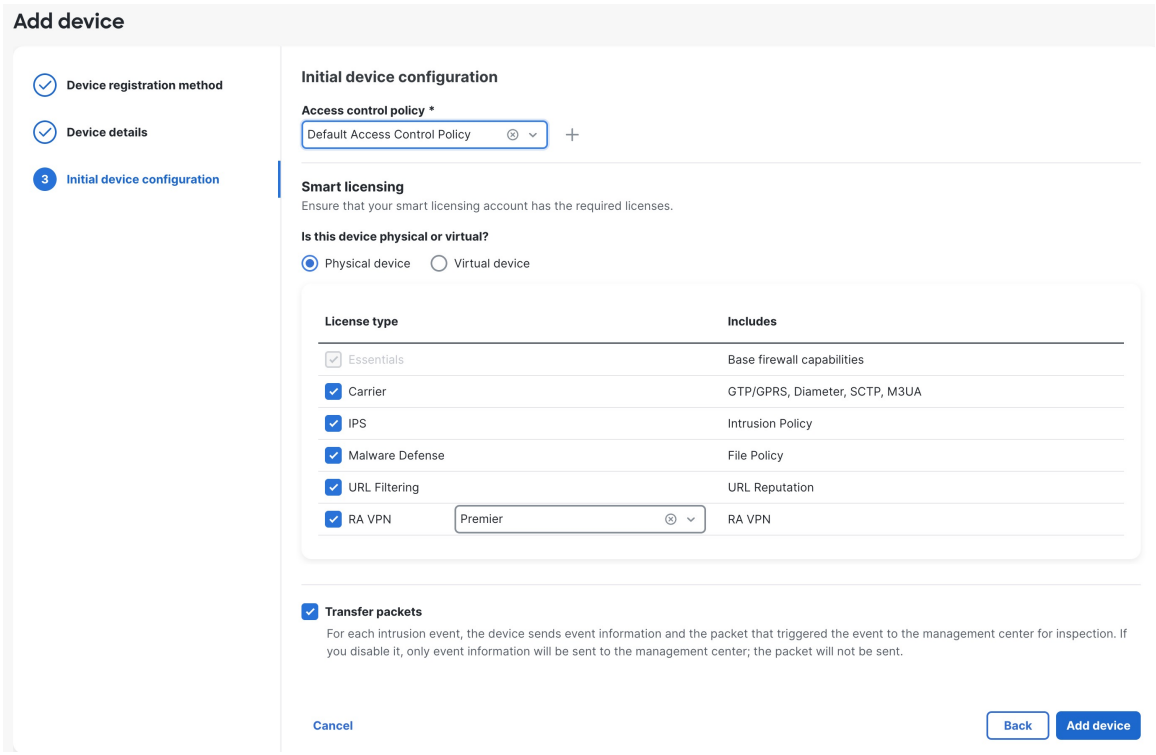


- **Domain**—In a multidomain environment, choose the leaf domain.
- **Device group**—In a single domain environment, add the device to a **Device group**.
- **Serial number**—Enter the IP address or the hostname of the device you want to add. Leave this field blank if you don't know the device IP address (for example, it's behind NAT).
- **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.
- **Device password**—If this device is unconfigured or a fresh install, then you need to set a **New Password** and confirm the password.

  Check **I already changed the password on the device** only if you already logged in and changed the password. Otherwise, registration will fail.

Step 8 Configure the initial device configuration.

Figure 12: Initial Device Configuration



- **Access control policy**—Choose an initial policy to deploy to the device at registration, or create a new policy. Unless you already have a customized policy you know you need to use, choose **Add** (+), and choose **Block all traffic**. You can change this later to allow traffic.
- **Smart licensing**—Choose your licenses.
  - **Is this device physical or virtual?**—Choose **Physical device**
  - **License type**—Check each license type to assign to the device.

  You can also apply licenses after you add the device.
- **Transfer packets**—Enable this option so that for each intrusion event, the device transfers the packet to the Firewall Management Center for inspection.

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

Step 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.

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.

Add a Device to the Firewall Management Center Manually

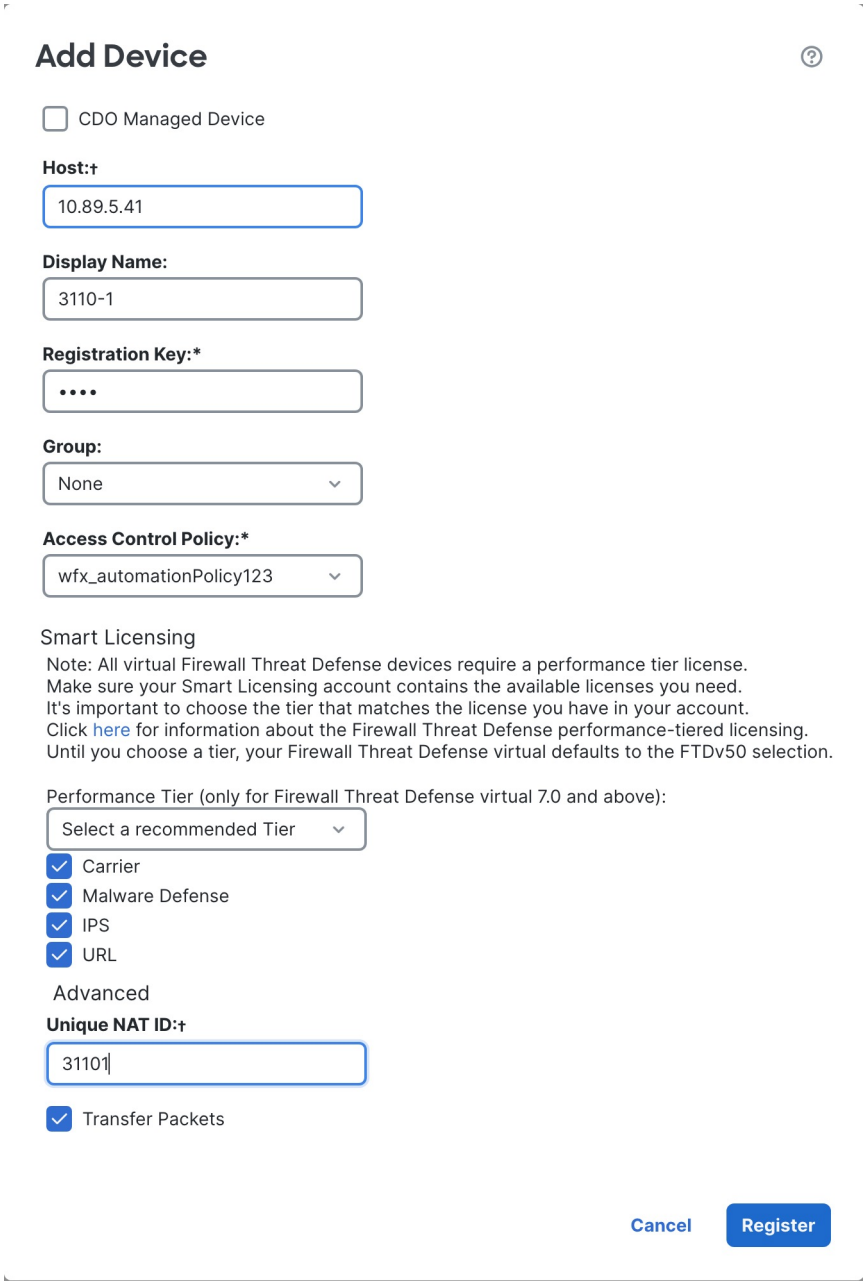
Register the Firewall Threat Defense to the Firewall Management Center manually using the device IP address or hostname and registration key.

Procedure

Step 1 In the Firewall Management Center, choose **Devices** > **Device Management**.

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

Figure 13: Add Device Using a Registration Key



Set the following parameters:

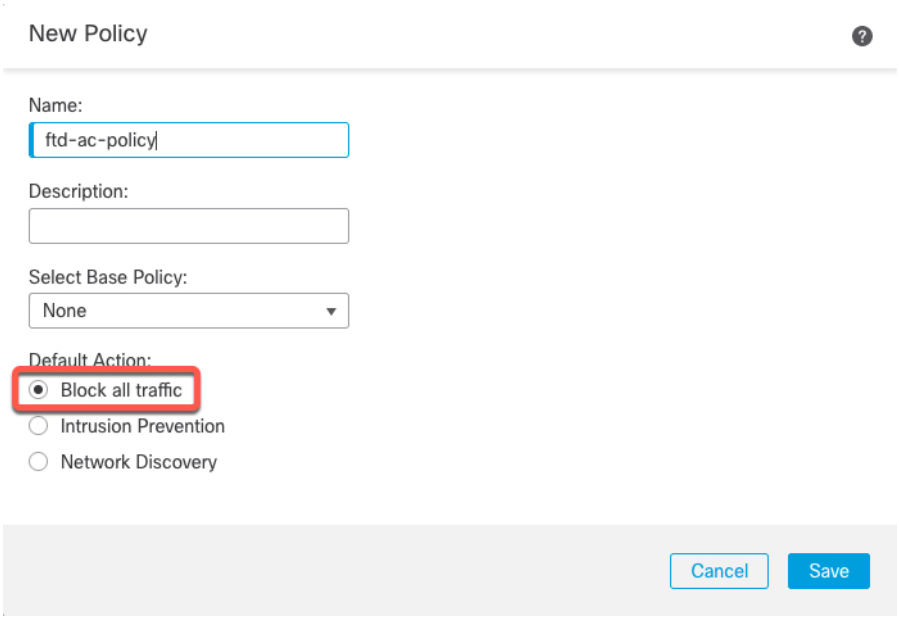
- **Host**—Enter the IP address or hostname of the Firewall Threat Defense you want to add. You can leave this field blank if you specified both the Firewall Management Center IP address and a NAT ID in the Firewall Threat Defense initial configuration.

  Note
  In an HA environment, when both the Firewall Management Centers are behind a NAT, you can register the Firewall Threat Defense without a host IP or name in the primary Firewall Management Center.

However, for registering the Firewall Threat Defense in a secondary Firewall Management Center, you must provide the IP address or hostname for the Firewall Threat Defense.

- **Display Name**—Enter the name for the Firewall Threat Defense as you want it to display in the Firewall Management Center.
- **Registration Key**—Enter the same registration key that you specified in the Firewall Threat Defense initial configuration.
- **Domain**—Assign the device to a leaf domain if you have a multidomain environment.
- **Group**—Assign it to a device group if you are using groups.
- **Access Control Policy**—Choose an initial policy. Unless you already have a customized policy you know you need to use, choose **Create new policy**, and choose **Block all traffic**. You can change this later to allow traffic; see Allow Traffic from Inside to Outside.

Figure 14: New Policy



- **Smart Licensing**—Assign the Smart Licenses you need for the features you want to deploy. **Note:** You can apply the Secure Client remote access VPN license after you add the device, from the **System** > **Licenses** > **Smart Licenses** page.
- **Unique NAT ID**—Specify the NAT ID that you specified in the Firewall Threat Defense initial configuration.
- **Transfer Packets**—Allow the device to transfer packets to the Firewall Management Center. When events like IPS or Snort are triggered with this option enabled, the device sends event metadata information and packet data to the Firewall Management Center for inspection. If you disable it, only event information will be sent to the Firewall Management Center, but packet data is not sent.

Step 3 Click **Register**, and confirm a successful registration.

If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the Firewall Threat Defense fails to register, check the following items:

- Ping—Access the Firewall Threat Defense 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 Firewall Threat Defense Management IP address, use the **configure network management-data-interface** 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 Firewall Threat Defense using the **configure manager add** command.

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

Configure a Basic Security Policy

This section describes how to configure a basic security policy with the following settings:

- Inside and outside interfaces—Assign a static IP address to the inside interface. You configured basic settings for the outside interface as part of the manager access setup, but you still need to assign it to a security zone.
- DHCP server—Use a DHCP server on the inside interface for clients.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.
- SSH—Enable SSH on the manager access interface.

Configure Interfaces

When you use zero-touch provisioning or the Firewall Device Manager for initial setup, the following interfaces are preconfigured:

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

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

In any case, you need to perform additional interface configuration after you register the device. Enable the Firewall Threat Defense interfaces, assign them to security zones, and set the IP addresses. .

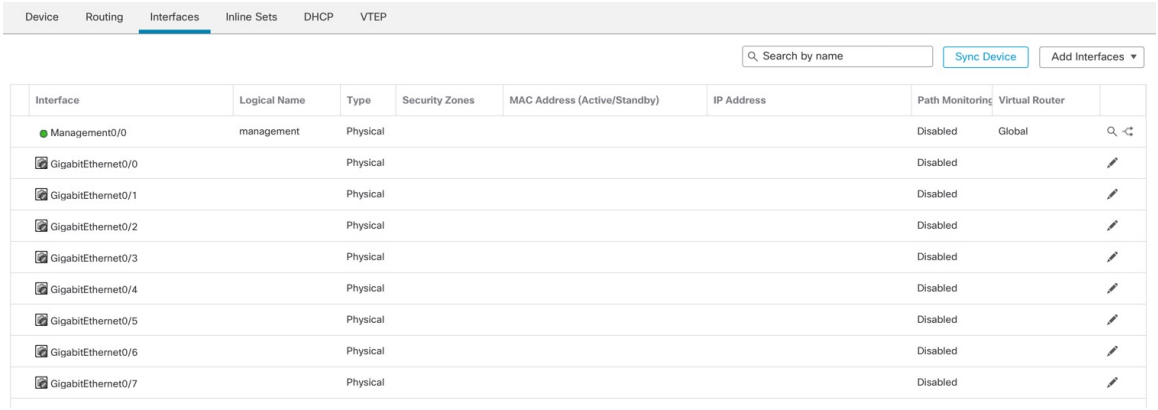
The following example configures a routed mode inside interface with a static address and a routed mode outside interface using DHCP.

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** (✎) for the firewall.

Step 2 Click **Interfaces**.

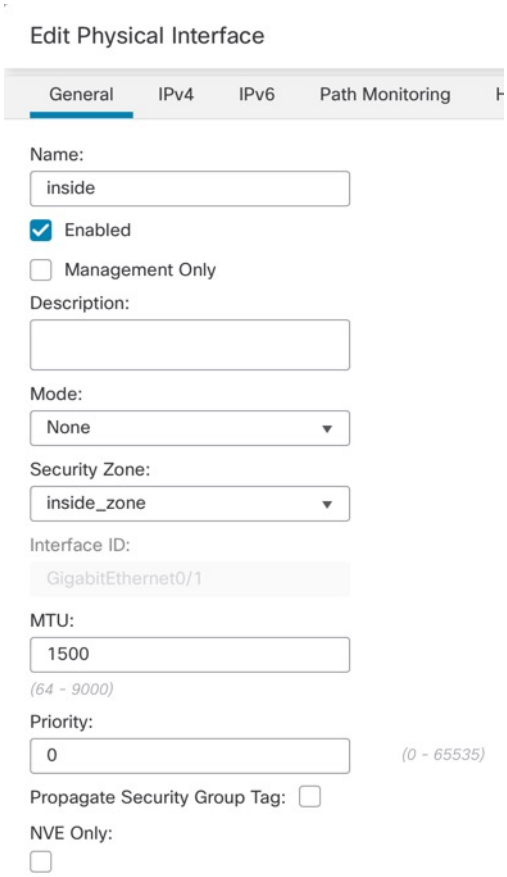
Figure 15: Interfaces



Step 3 Click **Edit** (✎) for the interface that you want to use for *inside*.

The **General** tab appears.

Figure 16: General Tab



a) Enter a **Name** up to 48 characters in length.

   For example, name the interface **inside**.

b) Check the **Enabled** check box.

c) Leave the **Mode** set to **None**.

d) From the **Security Zone** drop-down list, choose an existing inside security zone or add a new one by clicking **New**.

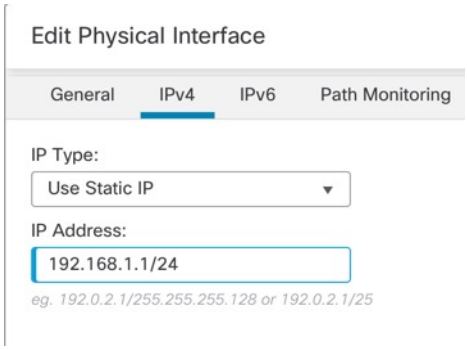
   For example, add a zone called **inside_zone**. Each interface must be assigned to a security zone and/or interface group. An interface can belong to only one security zone, but can also belong to multiple interface groups. You apply your security policy based on zones or groups. For example, you can assign the inside interface to the inside zone; and the outside interface to the outside zone. Then you can configure your access control policy to enable traffic to go from inside to outside, but not from outside to inside. Most policies only support security zones; you can use zones or interface groups in NAT policies, prefilter policies, and QoS policies.

e) Click the **IPv4** and/or **IPv6** tab.

   - **IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.

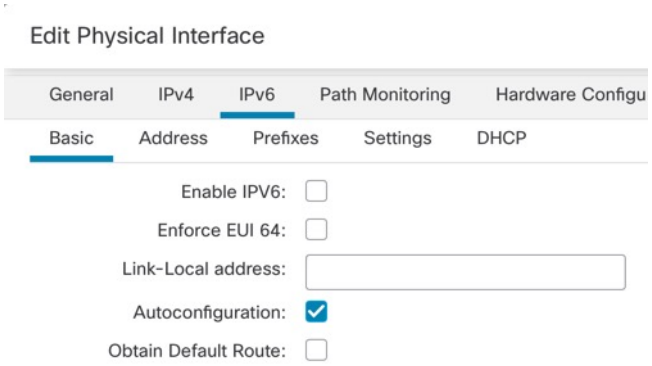
     For example, enter **192.168.1.1/24**

Figure 17: IPv4 Tab



- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

Figure 18: IPv6 Tab

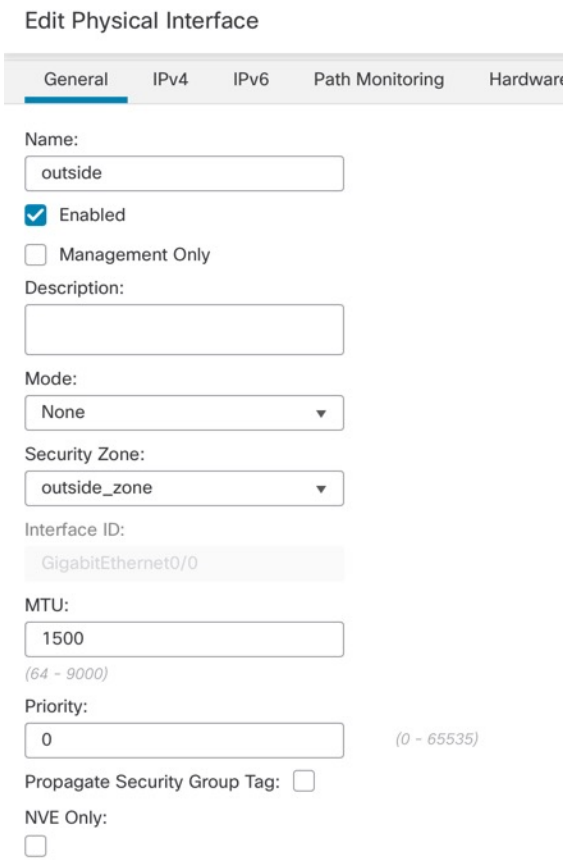


f) Click **OK**.

Step 4 Click **Edit** (✎) for the interface that you want to use for *outside*.

The **General** tab appears.

Figure 19: General Tab



You already pre-configured this interface for manager access, so the interface will already be named, enabled, and addressed. You should not alter any of these basic settings because doing so will disrupt the Firewall Management Center management connection. You must still configure the Security Zone on this screen for through traffic policies.

a) From the **Security Zone** drop-down list, choose an existing outside security zone or add a new one by clicking **New**.

   For example, add a zone called **outside_zone**.

b) Click **OK**.

Step 5 Click **Save**.

Configure the DHCP Server

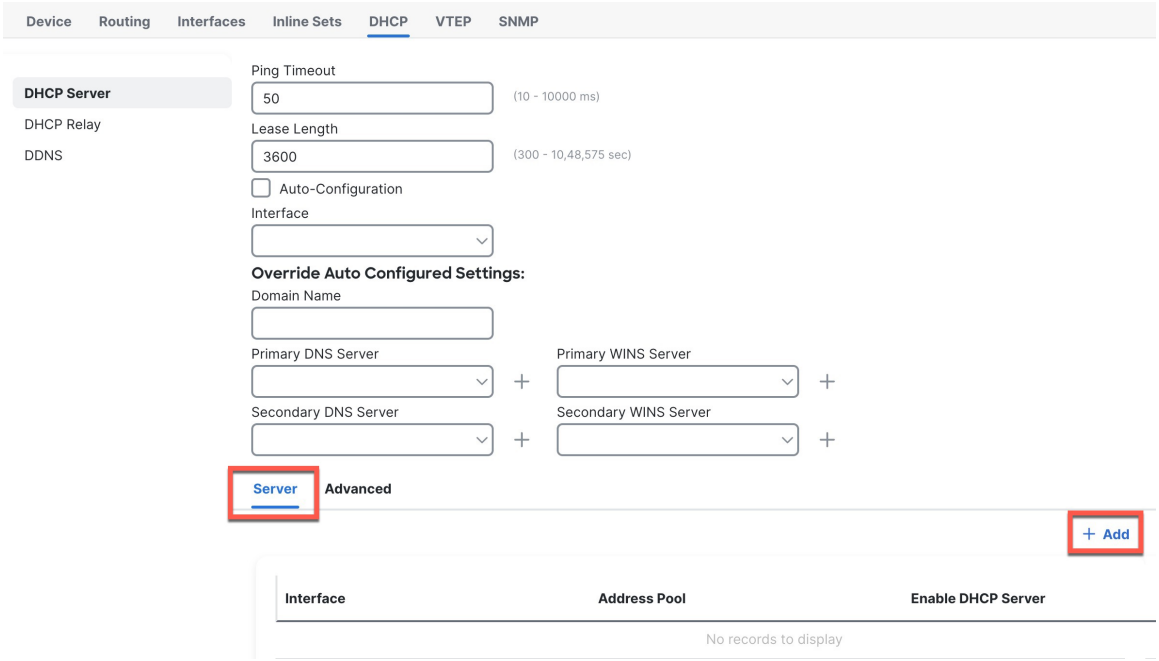
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the Firewall Threat Defense.

Procedure

Step 1 Choose **Devices** > **Device Management**, and click **Edit** (✎) for the device.

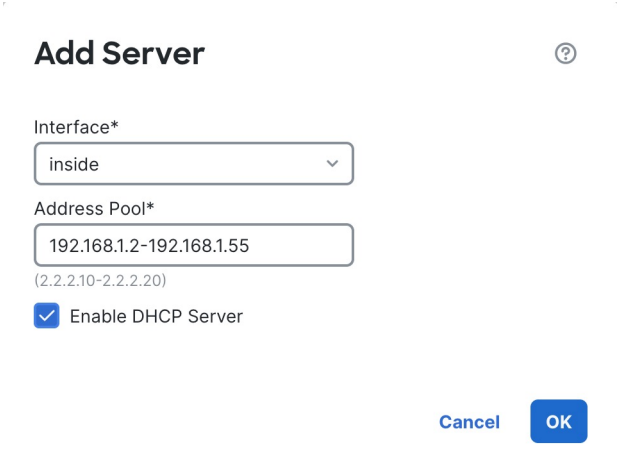
Step 2 Choose **DHCP** > **DHCP Server**.

Figure 20: DHCP Server



Step 3 On the **Server** page, click **Add**, and configure the following options:

Figure 21: Add Server



- **Interface**—Choose the interface from the drop-down list.

- **Address Pool**—Set the range of IP addresses from lowest to highest that are used by the DHCP server. The range of IP addresses must be on the same subnet as the selected interface and cannot include the IP address of the interface itself.
- **Enable DHCP Server**—Enable the DHCP server on the selected interface.

Step 4 Click **OK**.

Step 5 Click **Save**.

Configure NAT

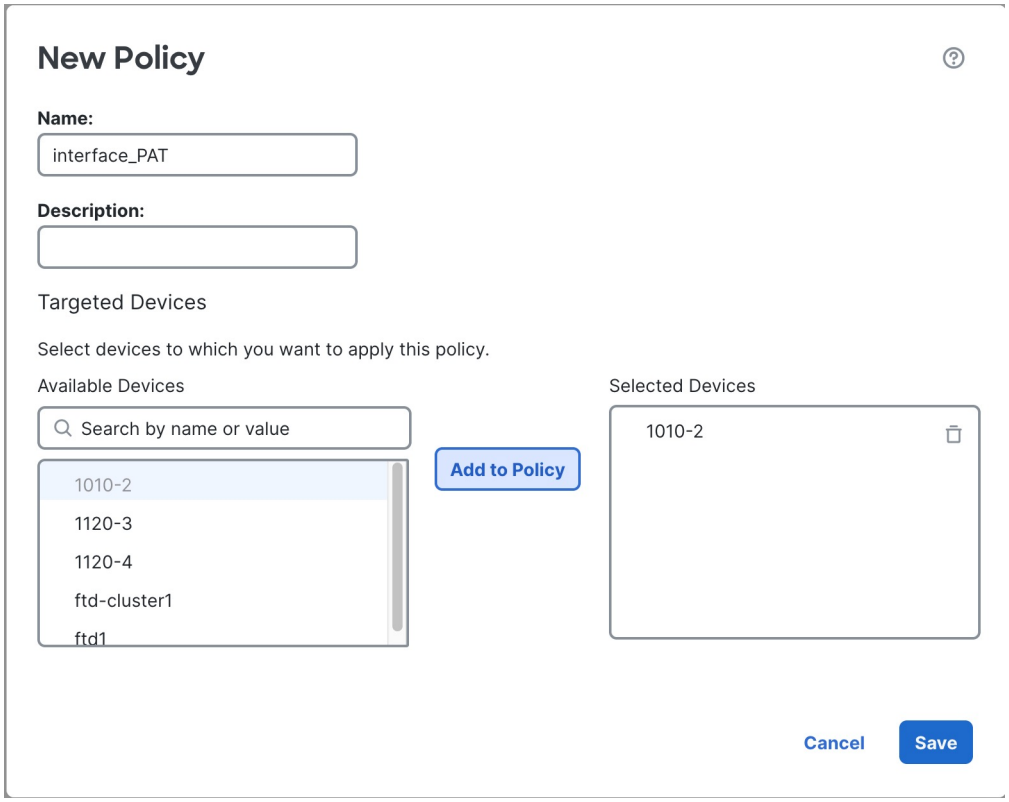
A typical NAT rule converts internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

Procedure

Step 1 Choose **Devices** > **NAT**, and click **New Policy** > **Threat Defense NAT**.

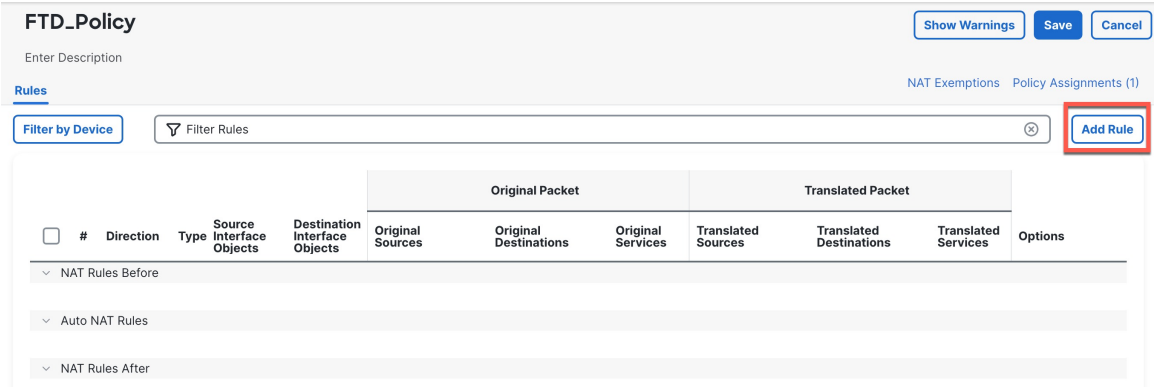
Step 2 Name the policy, select the device(s) that you want to use the policy, and click **Save**.

Figure 22: New Policy



The policy is added the Firewall Management Center. You still have to add rules to the policy.

Figure 23: NAT Policy

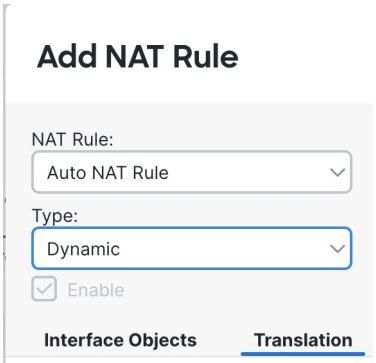


Step 3 Click **Add Rule**.

The **Add NAT Rule** dialog box appears.

Step 4 Configure the basic rule options:

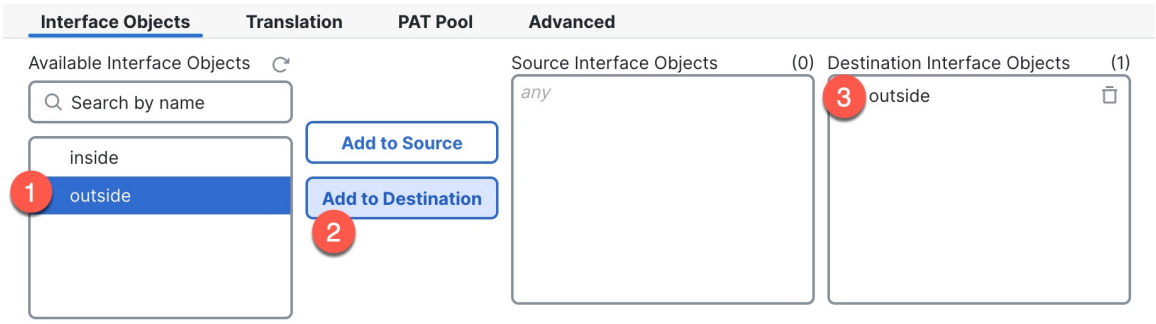
Figure 24: Basic Rule Options



- **NAT Rule**—Choose **Auto NAT Rule**.
- **Type**—Choose **Dynamic**.

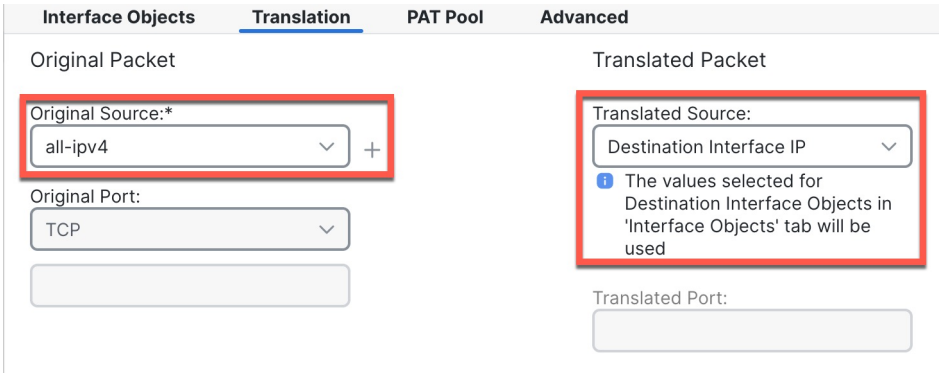
Step 5 On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 25: Interface Objects



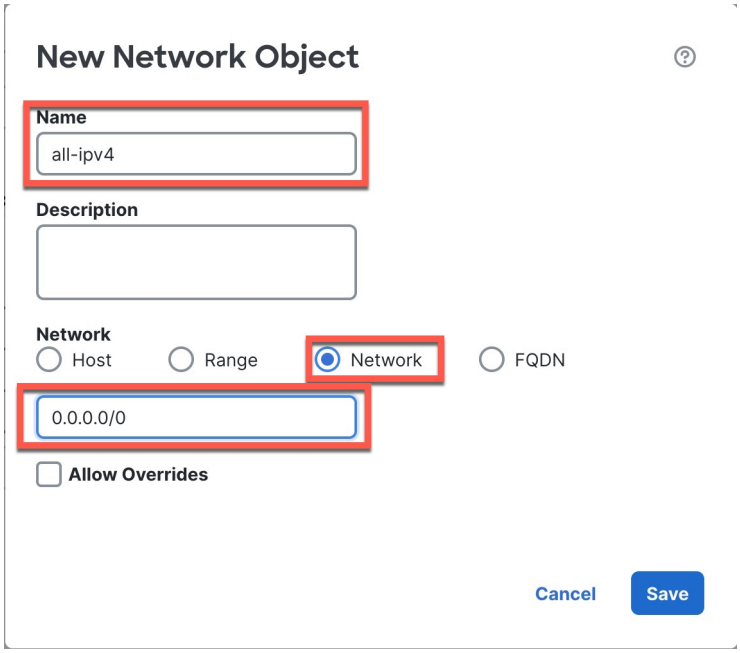
Step 6 On the **Translation** page, configure the following options:

Figure 26: Translation



- **Original Source**—Click **Add** (+) to add a network object for all IPv4 traffic (**0.0.0.0/0**).

Figure 27: New Network Object



Note
You cannot use the system-defined **any-ipv4** object, because Auto NAT rules add NAT as part of the object definition, and you cannot edit system-defined objects.

- **Translated Source**—Choose **Destination Interface IP**.

Step 7 Click **Save** to add the rule.

The rule is saved to the **Rules** table.

Step 8 Click **Save** on the **NAT** page to save your changes.

Allow Traffic from Inside to Outside

If you created a basic **Block all traffic** access control policy when you registered the Firewall Threat Defense, then you need to add rules to the policy to allow traffic through the device. The following procedure adds a rule to allow traffic from the inside zone to the outside zone. If you have other zones, be sure to add rules allowing traffic to the appropriate networks.

Procedure

Step 1 Choose **Policy** > **Access Policy** > **Access Policy**, and click **Edit** (✎) for the access control policy assigned to the Firewall Threat Defense.

Step 2 Click **Add Rule**, and set the following parameters:

Figure 28: Source Zone

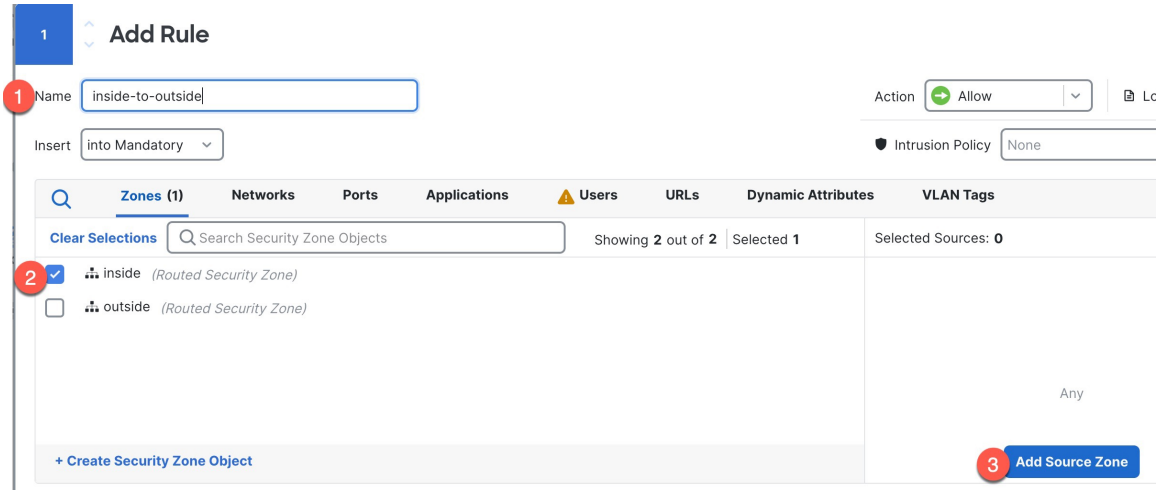


Figure 29: Destination Zone

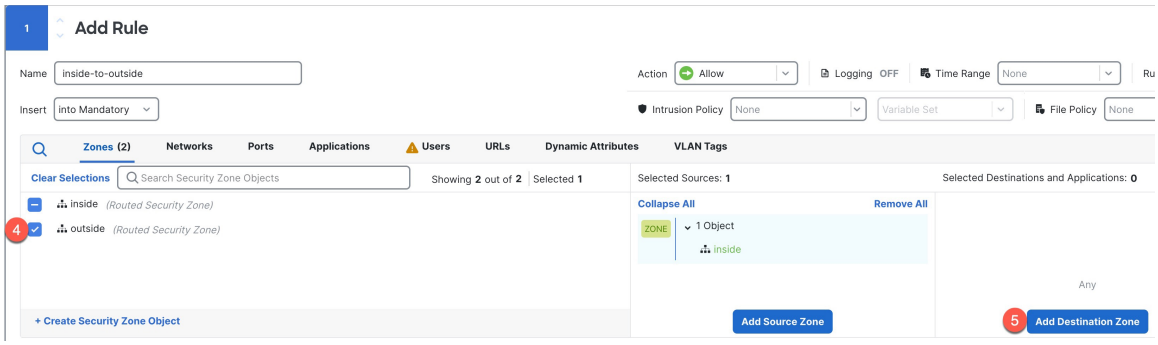
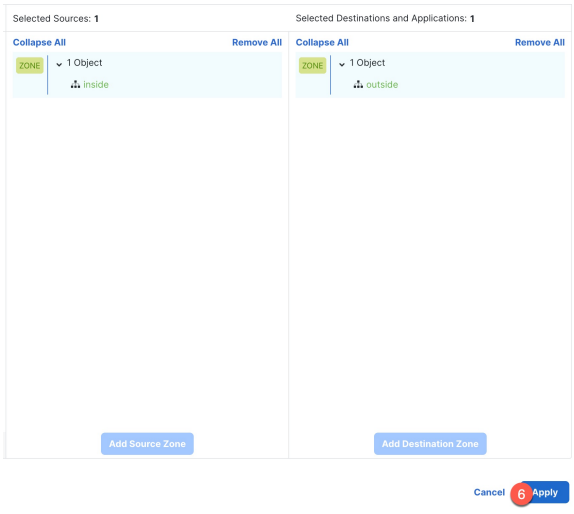


Figure 30: Apply



- **Name**—Name this rule, for example, **inside-to-outside**.

- **Selected Sources**—Select the inside zone from **Zones**, and click **Add Source Zone**.
- **Selected Destinations and Applications**—Select the outside zone from **Zones**, and click **Add Destination Zone**.

Leave the other settings as is.

Step 3 Click **Apply**.

The rule is added to the **Rules** table.

Step 4 Click **Save**.

Configure SSH on the Manager Access Data Interface

If you enabled Firewall Management Center access on a data interface, such as outside, you should enable SSH on that interface using this procedure. This section describes how to enable SSH connections to one or more *data* interfaces on the Firewall Threat Defense.

Note SSH is enabled by default on the Management interface; however, this screen does not affect Management SSH access.

To use SSH, you do not also need an access rule allowing the host IP address. You only need to configure SSH access according to this section.

Data vs. Management SSH

The Management interface is separate from the other interfaces on the device. It is used to set up and register the device to the Firewall Management Center. SSH for data interfaces shares the internal and external user list with SSH for the Management interface. Other settings are configured separately: for data interfaces, enable SSH and access lists using this screen; SSH traffic for data interfaces uses the regular routing configuration. Management interface routing configured at setup or at the CLI is not used.

For the Management interface, to configure an SSH access list, see the **configure ssh-access-list** command in the Cisco Secure Firewall Threat Defense Command Reference. To configure a static route, see the **configure network static-routes** command. By default, you configure the default route through the Management interface at initial setup.

Interface Access

You can SSH only to a reachable interface (including an interface in a user-defined virtual router); for example, if your SSH host is located on the outside interface, you can only initiate a management connection directly to the outside interface. When you enable SSH in a user-defined virtual router, and you want VPN users to access SSH, be sure to terminate the VPN on the same virtual router. If the VPN is terminated on another virtual router, then you must configure route leaks between the virtual routers.

Ciphers and Key Exchange

SSH supports the following ciphers and key exchange:

- Encryption—aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr
- Integrity—hmac-sha2-256

- Key exchange—dh-group14-sha256

SSH Stack

The Firewall Threat Defense uses the CiscoSSH stack, which is based on OpenSSH. CiscoSSH supports FIPS compliance and regular updates, including updates from Cisco and the open source community.

Maximum Attempts

After you make three consecutive failed attempts to log into the CLI using SSH, the device terminates the SSH connection.

Before you begin

- You can configure SSH internal users at the CLI using the **configure user add** command. By default, there is an **admin** user for which you configured the password during initial setup. You can also configure external users on LDAP or RADIUS by configuring **External Authentication** in platform settings.
- You need network objects that define the hosts or networks you will allow to make SSH connections to the device. You can add objects as part of the procedure, but if you want to use object groups to identify a group of IP addresses, ensure that the groups needed in the rules already exist. Select **Objects** > **Object Management** to configure objects.

Note You cannot use the system-provided **any** network object. Instead, use **any-ipv4** or **any-ipv6**.

Procedure

Step 1 Choose **Devices** > **Platform Settings** and create or edit the Firewall Threat Defense policy.

Step 2 Select **SSH Access**.

Step 3 Identify the interfaces and IP addresses that allow SSH connections.

Use this table to limit which interfaces will accept SSH connections, and the IP addresses of the clients who are allowed to make those connections. You can use network addresses rather than individual IP addresses.

a) Click **Add** to add a new rule, or click **Edit** to edit an existing rule.

b) Configure the rule properties:

- **IP Address**—The network object or group that identifies the hosts or networks you are allowing to make SSH connections. Choose an object from the drop-down menu, or click + to add a new network object.
- **Available Zones/Interfaces**—Add the zones that contain the interfaces to which you will allow SSH connections. For interfaces not in a zone, you can type the interface name into the field below the **Selected Zones/Interfaces** list and click **Add**. You can also add loopback interfaces and virtual-router-aware interfaces. These rules will be applied to a device only if the device includes the selected interfaces or zones.

c) Click **OK**.

Step 4 Click **Save**.

You can now go to **Deploy** > **Deploy** and deploy the policy to assigned devices. The changes are not active until you deploy them.

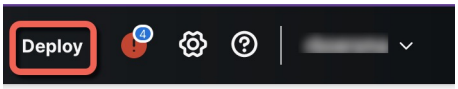
Deploy the Configuration

Deploy the configuration changes to the Firewall Threat Defense; none of your changes are active on the device until you deploy them.

Procedure

Step 1 Click **Deploy** in the upper right.

Figure 31: Deploy



Step 2 For a quick deployment, check specific devices and then click **Deploy**, or click **Deploy All** to deploy to all devices. Otherwise, for additional deployment options, click **Advanced Deploy**.

Figure 32: Deploy Selected

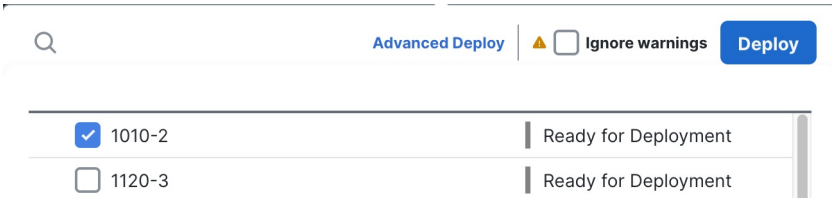


Figure 33: Deploy All

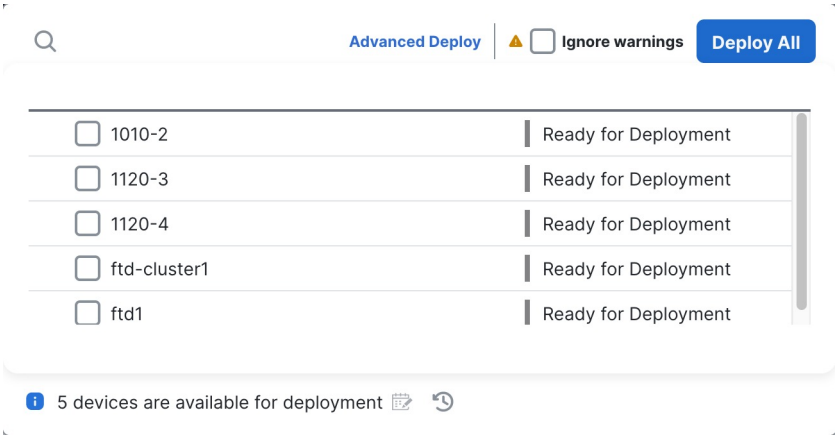
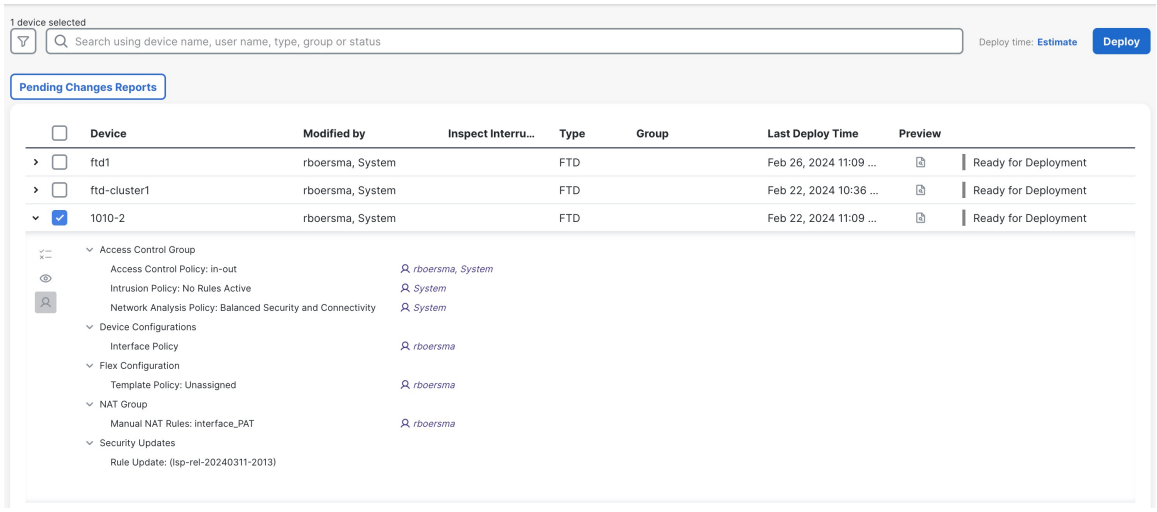
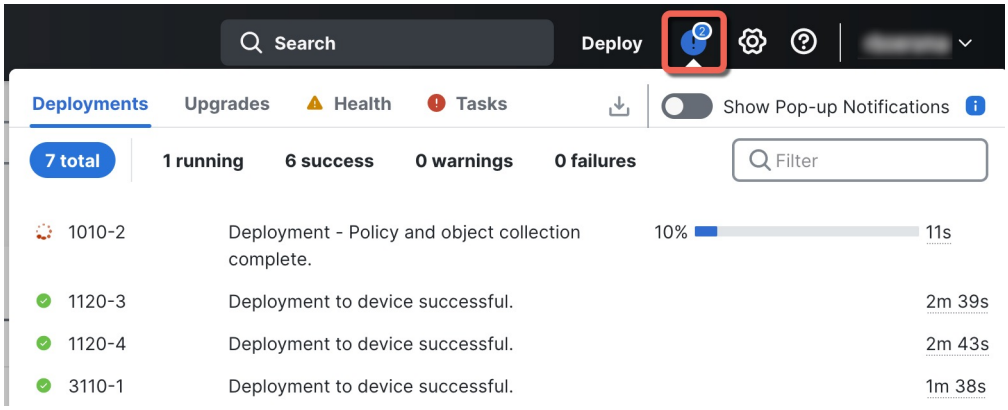


Figure 34: Advanced Deploy



Step 3 Ensure that the deployment succeeds. Click the icon to the right of the **Deploy** button in the menu bar to see status for deployments.

Figure 35: Deployment Status



Access the Firewall Threat Defense and FXOS CLI

Use the command-line interface (CLI) to set up the system and do basic system troubleshooting. You cannot configure policies through a CLI session. You can access the CLI by connecting to the console port.

You can also access the FXOS CLI for troubleshooting purposes.

Note You can alternatively SSH to the Management interface of the Firewall Threat Defense device. Unlike a console session, the SSH session defaults to the Firewall Threat Defense CLI, from which you can connect to the FXOS CLI using the **connect fxos** command. You can later 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. This procedure describes console port access, which defaults to the FXOS CLI.

Procedure

Step 1 To log into the CLI, connect your management computer to the console port. The Firepower 2100 ships with a DB-9 to RJ-45 serial cable, so you may need a third party DB-9-to-USB serial cable to make the connection. Be sure to install any necessary USB serial drivers for your operating system. The console port defaults to the FXOS CLI. Use the following serial settings:

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

You connect to the FXOS CLI. Log in to the CLI using the **admin** username and the password you set at initial setup (the default is **Admin123**).

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 2 Access the Firewall Threat Defense CLI.

connect ftd

Example:

```
firepower# connect ftd
>
```

After logging in, for information on the commands available in the CLI, enter **help** or **?**. For usage information, see Cisco Secure Firewall Threat Defense Command Reference.

Step 3 To exit the Firewall Threat Defense CLI, enter the **exit** or **logout** command.

This command returns you to the FXOS CLI prompt. For information on the commands available in the FXOS CLI, enter **?**.

Example:

```
> exit
firepower#
```

Troubleshoot Management Connectivity on a Data Interface

Model Support—Firewall Threat Defense

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

This topic helps you troubleshoot the loss of management connectivity.

View management connection status

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

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

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

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

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

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

View the Firewall Threat Defense network information

At the Firewall Threat Defense CLI, view the Management and the Firewall Management Center access data interface network settings:

show network

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

======================[ br1 ]=======================
State                   : Enabled
Link                    : Up
Channels                : Management & Events
Mode                    : Non-Autonegotiation
MDI/MDIX                : Auto/MDIX
MTU                     : 1500
MAC Address             : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration           : Manual
Address                 : 10.99.10.4
Netmask                 : 255.255.255.0
Gateway                 : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration           : Disabled

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

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

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

Check that the Firewall Threat Defense registered with the Firewall Management Center

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

show managers

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

```
>
```

Ping the Firewall Management Center

At the Firewall Threat Defense CLI, use the following command to ping the Firewall Management Center from the data interfaces:

ping *fmc_ip*

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

ping system *fmc_ip*

Capture packets on the Firewall Threat Defense internal interface

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

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

show capture*name* **trace detail**

Check the internal interface status, statistics, and packet count

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

show interace detail

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

```
 Interface state is active
```

Check routing and NAT

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

show route

```
> show route

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

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

>
```

show nat

```
> show nat

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

Check other settings

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

show running-config sftunnel

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

show running-config ip-client

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

show conn address *fmc_ip*

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

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

Check for a successful DDNS update

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

debug ddns

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

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

show crypto ca certificates *trustpoint_name*

To check the DDNS operation:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

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

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

Check Firewall Management Center log files

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

Power Off the Firewall

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 system.

You can power off the device using the Firewall Management Center device management page, or you can use the FXOS CLI.

Power Off the Firewall Using the Firewall Management Center

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.

You can shut down your system properly using the Firewall Management Center.

Procedure

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

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

Step 3 Click the **Device** tab.

Step 4 Click **Shut Down Device** ( ) in the **System** section.

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

Step 6 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.

Step 7 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

Power Off the Device at the CLI

You can use the FXOS CLI to safely shut down the system and power off the device. You access the CLI by connecting to the console port; see Access the Firewall Threat Defense and FXOS CLI, on page 49.

Procedure

Step 1 In the FXOS CLI, connect to local-mgmt:

firepower # **connect local-mgmt**

Step 2 Issue the **shutdown** command:

firepower(local-mgmt) # **shutdown**

Example:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Step 3 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]
```

Step 4 You can now turn off the power switch and unplug the power to physically remove power from the chassis if necessary.

What's Next?

To continue configuring your Firewall Threat Defense, see the documents available for your software version at Navigating the Cisco Secure Firewall Threat Defense Documentation.

For information related to using the Firewall Management Center, see the Cisco Secure Firewall Management Center Device Configuration Guide.