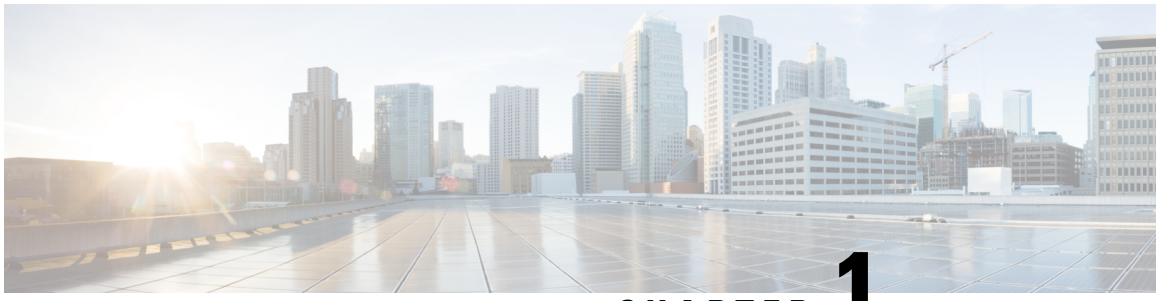
Firepower 1010 Threat Defense Getting Started: Management Center at a Central Headquarters

First Published: 2024-10-16

Last Modified: 2024-10-16

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CHAPTER 1

Before You Begin

Install the firewall at a branch office and manage it on the outside interface using a central Secure Firewall Management Center.

Note For high availability, you can use the outside interface with manual registration, but to use zero-touch provisioning, you must use the Management interface. This guide specifically covers outside management, but you can refer to the Cisco Secure Firewall Management Center Device Configuration Guide for management using the Management interface.

Power On the Firewall

System power is controlled by the power cord; there is no power button.

Note The first time you boot up the firewall, threat defense initialization can take approximately 15 to 30 minutes.

Before you begin

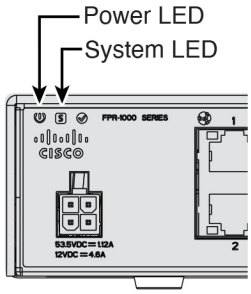
It's important that you provide reliable power for your firewall (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow the graceful shutdown of your system.

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

The power turns on automatically when you plug in the power cord.

Step 2 Check the Power LED on the back of the firewall; if it is solid green, the firewall is powered on.

Figure 1: System and Power LEDs



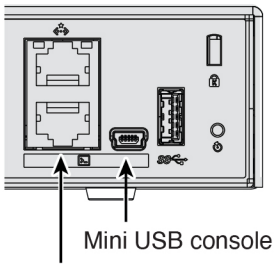
Step 3 Check the System LED on the back of the firewall; after it is solid green, the system has passed power-on diagnostics.

Which Application is Installed: Threat Defense or ASA?

Both applications, threat defense or ASA, are supported on the hardware. Connect to the console port and determine which application was installed at the factory.

Step 1 Connect to the console port using either port type.

Figure 2: Console Port



Step 2 See the CLI prompts to determine if your firewall is running threat defense or ASA.

Threat Defense

You see the firepower login (FXOS) prompt. You can disconnect without logging in and setting a new password. If you need to log in all the way, see Access the Threat Defense CLI, on page 3.

```
firepower login:
```

ASA

You see the ASA prompt.

```
ciscoasa>
```

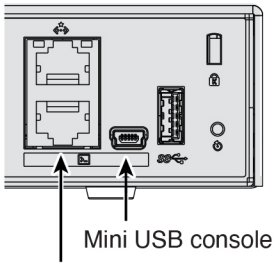
Step 3 If you are running the wrong application, see Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

Access the Threat Defense CLI

You might need to access the CLI for configuration or troubleshooting.

Step 1 Connect to the console port using either port type.

Figure 3: Console Port



Step 2 You connect to FXOS. Log in to the CLI using the **admin** username and the password (the default is **Admin123**). The first time you log in, you are prompted to change the password.

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

[...]

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

[...]

firepower#
```

Step 3 Change to the threat defense CLI.

Note If you want to use the device manager for initial setup or use zero-touch provisioning, do not access the threat defense CLI, which starts the CLI setup.

connect ftd

The first time you connect to the threat defense CLI, you are prompted to complete initial setup.

Example:

```
firepower# connect ftd
>
```

To exit the threat defense CLI, enter the **exit** or **logout** command. This command returns you to the FXOS prompt.

Example:

```
> exit
firepower#
```

Check the Version and Reimage

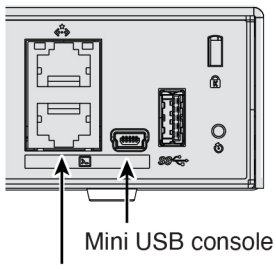
We recommend that you install your target version before you configure the firewall. Alternatively, you can perform an upgrade after you are up and running, but upgrading, which preserves your configuration, may take longer than using this procedure.

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.

Step 1 Connect to the console port using either port type.

Figure 4: Console Port



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) By default, the Management interface uses DHCP. If you need to set a static IP address for the Management interface, enter the following commands.

scope fabric-interconnect a

set out-of-band static ip *ip* **netmask** *netmask* **gw** *gateway*

commit-buffer

Note If you encounter the following error, you must disable DHCP before committing the change. Follow the commands below to disable DHCP.

```
firepower /fabric-interconnect* # commit-buffer
Error: Update failed: [Management ipv4 address (IP <ip> / net mask <netmask> ) is not
in the same network of current DHCP server IP range <ip - ip>.
Either disable DHCP server first or config with a different ipv4 address.]
firepower /fabric-interconnect* # exit
firepower* # scope system
firepower /system* # scope services
firepower /system/services* # disable dhcp-server
firepower /system/services* # commit-buffer
```

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

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

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 low-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 firewall. See (If Needed) Power Off the Firewall, on page 7.

Obtain Licenses

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 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.

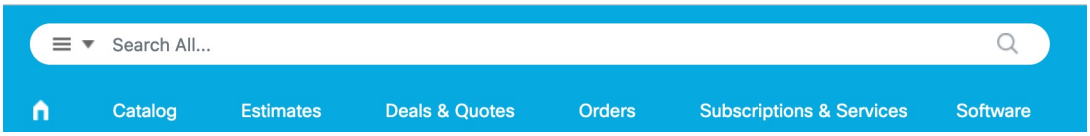
The threat defense has the following licenses:

- Essentials—Required
- IPS

- Malware Defense
- URL Filtering
- Cisco Secure Client

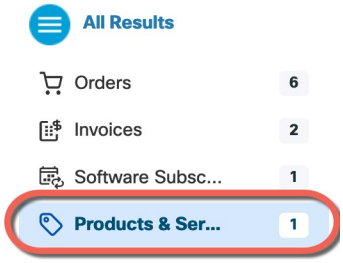
1. If you need to add licenses yourself, go to Cisco Commerce Workspace and use the **Search All** field.

Figure 5: License Search



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

Figure 6: Results



3. 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-FPR1010T-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-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- Cisco Secure Client—See the Cisco Secure Client Ordering Guide.

(If Needed) Power Off the Firewall

It's important that you shut down your system properly. Simply unplugging the power can cause serious file system damage. 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.

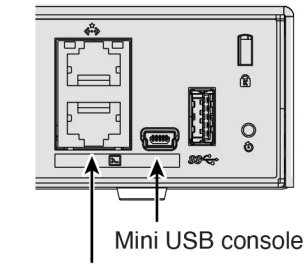
The Firepower 1010 chassis does not have an external power switch..

Power Off the Firewall at the CLI

You can use the FXOS CLI to safely shut down the system and power off the firewall.

Step 1 Connect to the console port using either port type.

Figure 7: Console Port



Step 2 In the FXOS CLI, connect to local-mgmt mode.

firepower # **connect local-mgmt**

Step 3 Shut down the system.

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 4 Monitor the system prompts as the firewall shuts down. When the shutdown is complete, 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 5 You can now unplug the power to physically remove power from the chassis if necessary.

Power Off the Firewall Using the Management Center

Shut down your system properly using the management center.

Step 1 Shut down the firewall.

a) Choose **Devices** > **Device Management**.

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

c) Click the **Device** tab.

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

e) When prompted, confirm that you want to shut down the device.

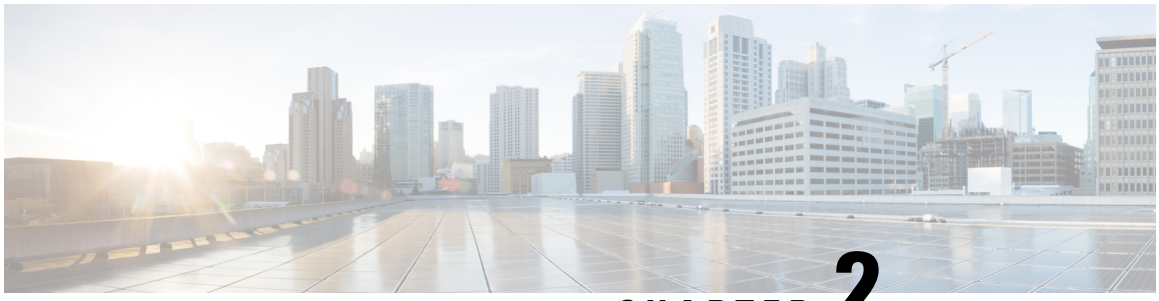
Step 2 If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. When shutdown is complete, you will see the following prompt.

```
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 3 You can now unplug the power to physically remove power from the chassis if necessary.



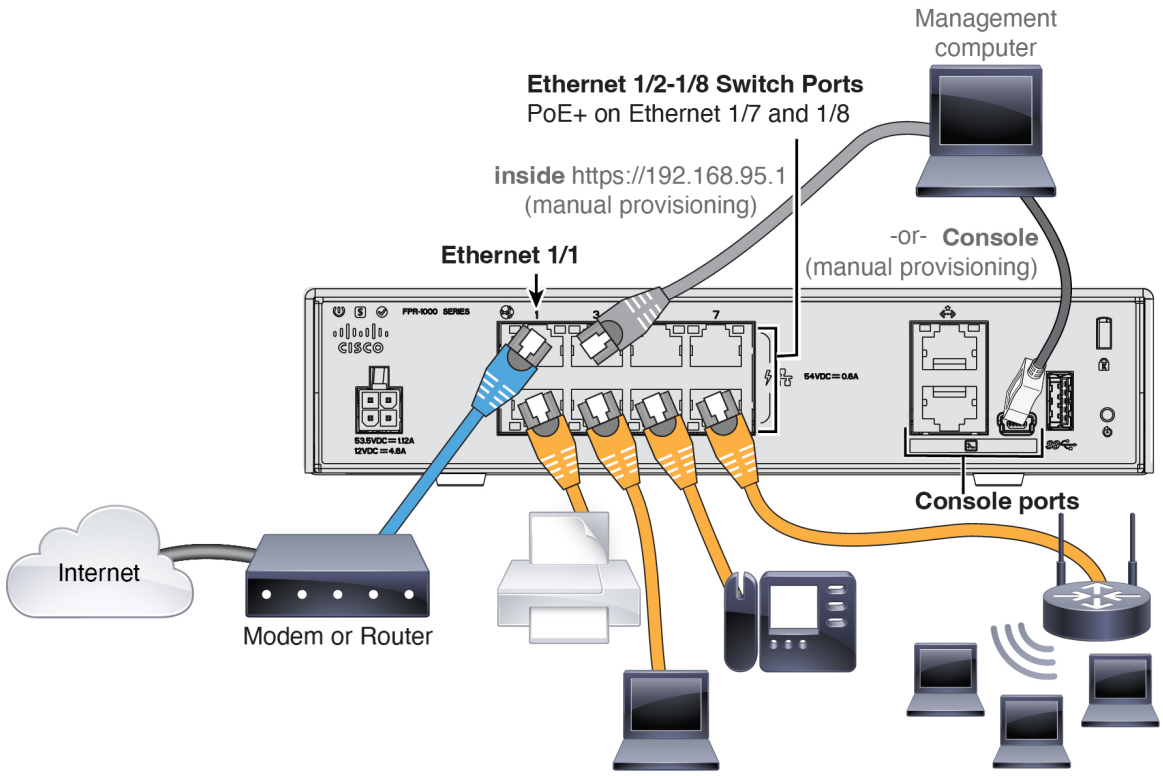
CHAPTER 2

Cable and Register the Firewall

Cable the firewall and then register the firewall to the management center.

Cable the Firewall

- See the hardware installation guide for more information.
- Do not cable the Management interface unless you are using high availability with zero-touch provisioning. In this case, see the Cisco Secure Firewall Management Center Device Configuration Guide. This guide covers only the outside interface.



Perform Initial Configuration (Manual Provisioning)

For manual provisioning, perfom initial configuration of the firewall using the Secure Firewall device manager or using the CLI.

Initial Configuration: Device Manager

Using this method, after you register the firewall, the following interfaces will be preconfigured in addition to the Management interface:

- Ethernet 1/1—**outside**, IP address from DHCP, IPv6 autoconfiguration
- VLAN1— **inside**, 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface
- Additional interfaces—Any interface configuration from the device manager is preserved.

Other settings, such as the DHCP server on inside, access control policy, or security zones, are not preserved.

Step 1 Connect your computer to the inside interface (Ethernet 1/2 through 1/8).

Step 2 Log into the device manager.

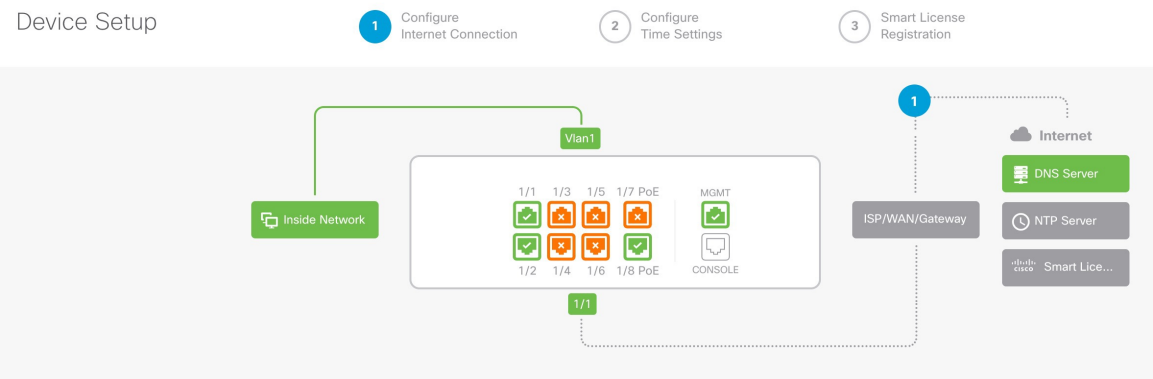
a) Go to https://192.168.95.1.

b) Log in with the username **admin** and the default password **Admin123**.

c) You are prompted to read and accept the General Terms and change the admin password.

Step 3 Use the setup wizard.

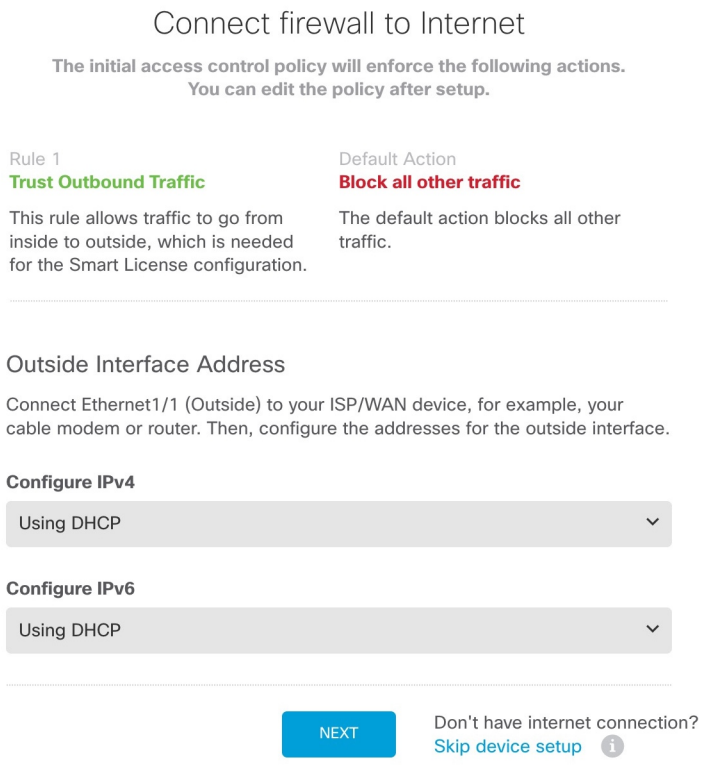
Figure 8: Device Setup



Note The exact port configuration depends on your model.

a) Configure the outside and management interfaces.

Figure 9: Connect firewall to internet



1. **Outside Interface Address**—Use a static IP address if you plan for high availability. You cannot configure PPPoE using the setup wizard; you can configure PPPoE after you complete the wizard.

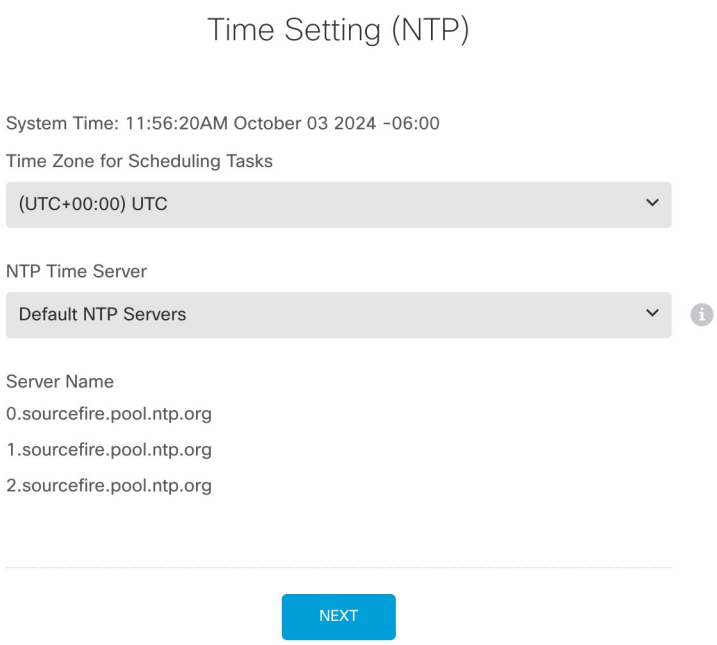
2. **Management Interface**—The Management interface settings are used even though you are using manager access on the outside interface. For example, management traffic that is routed over the backplane through the outside interface will resolve FQDNs using these Management interface DNS servers, and not the outside interface DNS servers.

   DNS Servers—The DNS server for the system's management address. The default is the OpenDNS public DNS servers. These will probably match the outside interface DNS servers you set later since they are both accessed from the outside interface.

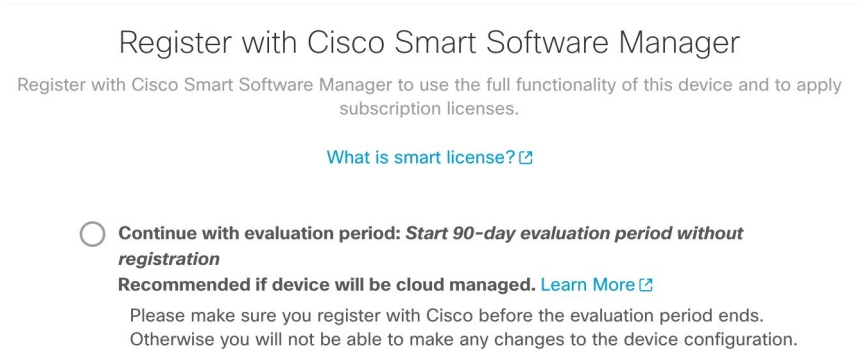
   Firewall Hostname

b) Configure the **Time Setting (NTP)** and click **Next**.

Figure 10: Time Setting (NTP)



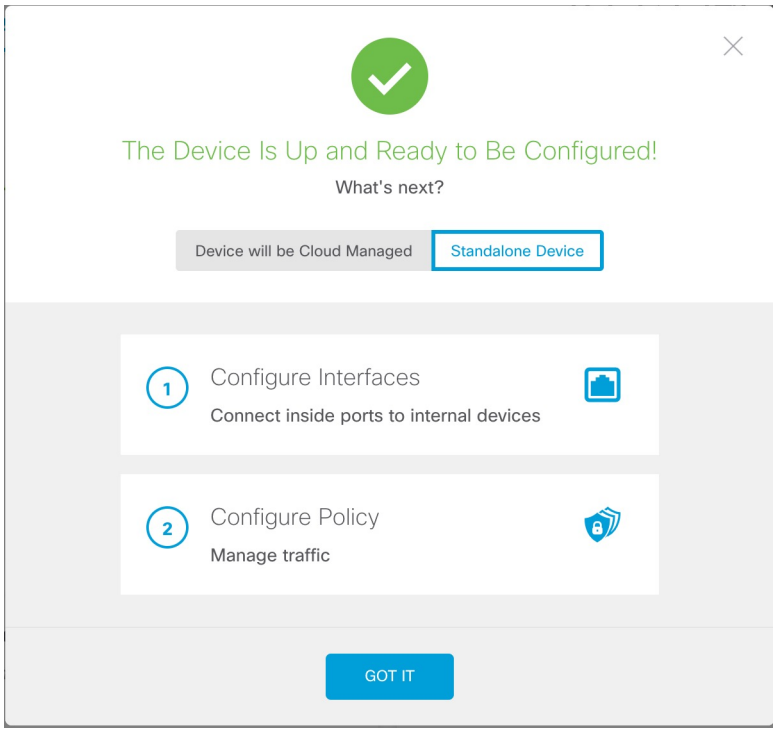
c) Select **Start 90 day evaluation period without registration**.



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

d) Click **Finish**.

Figure 11: What's Next



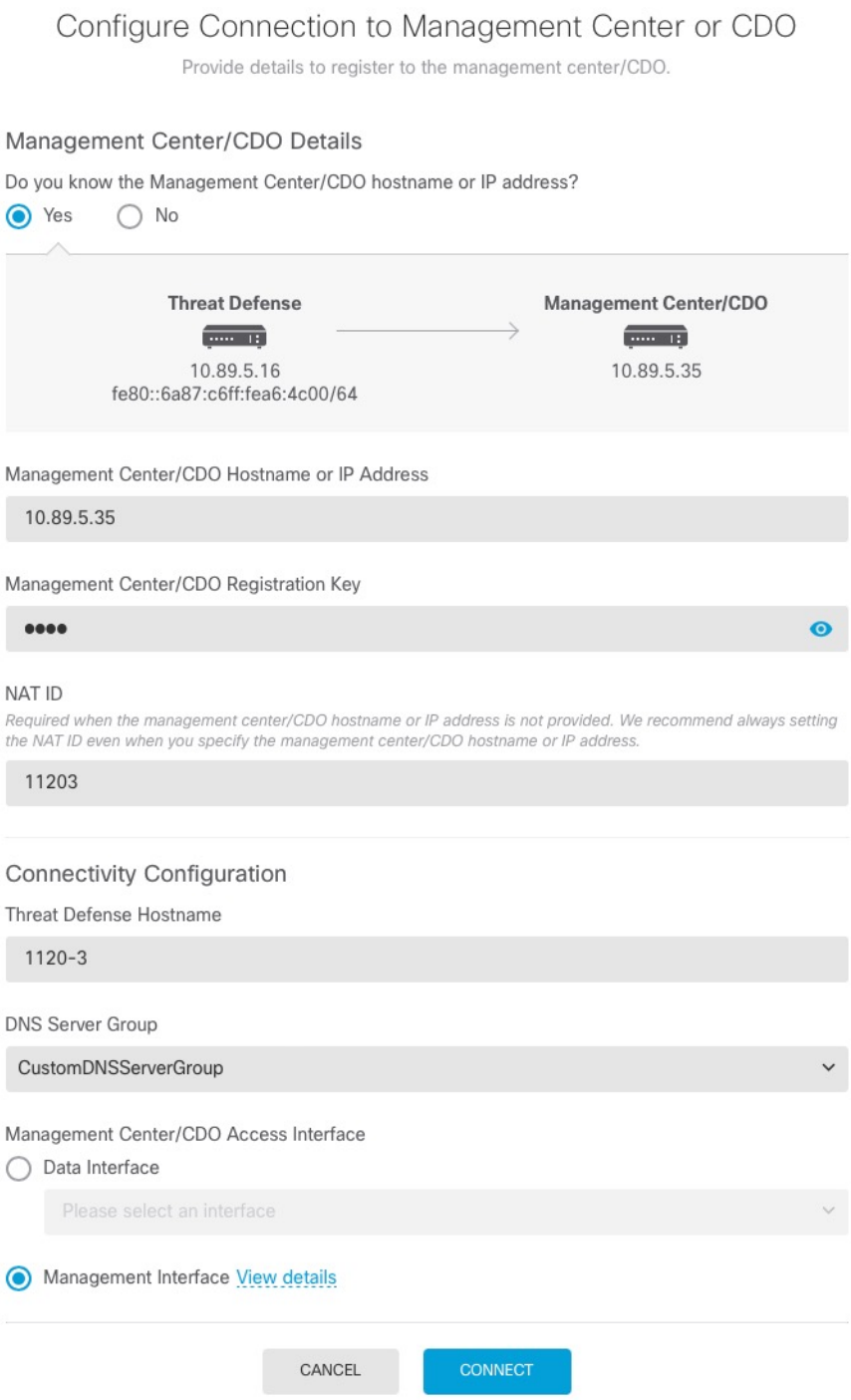
e) Choose **Standalone Device**, and then **Got It**.

Step 4 If you want to configure additional interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Step 5 Register with the management center by choosing **Device** > **System Settings** > **Central Management** and clicking **Proceed**

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

Figure 12: Management Center/CDO Details



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

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

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

d) Specify a **NAT ID**.

This ID is a unique, one-time string of your choice that you will also specify on the management center. We recommend that you specify the NAT ID even if you know the IP addresses of both devices. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID *cannot* be used for any other firewalls registering to the management center. The NAT ID is used in combination with the IP address to verify that the connection is coming from the correct device; only after authentication of the IP address/NAT ID will the registration key be checked.

Step 6 Configure the **Connectivity Configuration**.

a) Specify the **Threat Defense Hostname**.

This FQDN will be used for the outside 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.

To retain the outside DNS server setting after registration, you need to re-configure the DNS Platform Settings in the management center.

c) For the **Management Center/CDO Access Interface**, click **Data Interface**, and then choose **outside**.

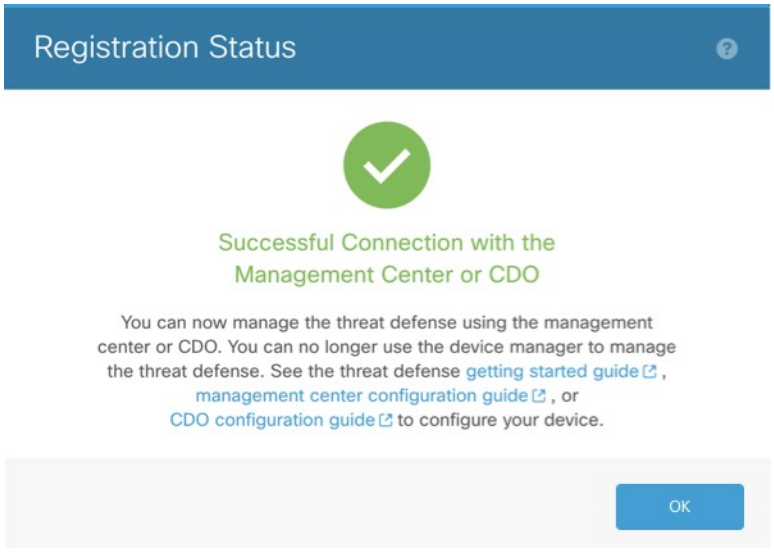
Step 7 (Optional) Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the management center can reach the threat defense at its FQDN if the threat defense's IP address changes.

Step 8 Click **Connect**.

The **Registration Status** dialog box shows the current status of the management center registration.

Figure 13: Successful Connection



Step 9 After the **Saving Management Center/CDO Registration Settings** step on the status screen, go to the management center and add the firewall. See Add the Firewall to the Management Center Using Manual Provisioning, on page 22.

Initial Configuration: CLI

Set the dedicated Management IP address, gateway, and other basic networking settings using the CLI setup script.

Step 1 Connect to the console port and access the threat defense CLI. See Access the Threat Defense CLI, on page 3.

Step 2 Complete the CLI setup script for the Management interface settings.

Note You cannot repeat the CLI setup script 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.

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
Cisco General Terms
[...]

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

System initialization in progress.  Please stand by.
You must configure the network to continue.
Configure at least one of IPv4 or IPv6 unless managing via data interfaces.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [y]: n
```

Guidance: 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? (dhcp/manual) [manual]:
```

Guidance: Choose **manual**. DHCP is not supported when using the outside interface for manager access. Make sure this interface is on a different subnet from the manager access interface to prevent routing issues.

```
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]:
```

Guidance: Set the gateway to be **data-interfaces**. This setting forwards management traffic over the backplane so it can be routed through the outside interface.

```
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
```

Guidance: Set the Management interface DNS servers. These will probably match the outside interface DNS servers you set later, since they are both accessed from the outside interface.

```
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
```

Guidance: Enter **no** to use the management center.

```
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'
```

Guidance: Enter **routed**. Outside manager access is only supported in routed firewall mode.

```
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 3 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.

Manual IP Address

```
> 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
```

Guidance: To retain the outside DNS servers after registration, you need to re-configure the DNS Platform Settings in the management center.

```
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.

>
```

IP Address from DHCP

```
> 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.

>
```

Step 4 Identify the management center.

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 management center. If the management center is not directly addressable, use **DONTRESOLVE**, in which case the firewall must have a reachable IP address or hostname.
- *reg_key*—Specifies a one-time registration key of your choice that you will also specify on the management center when you register the threat defense. The registration key must not exceed 37 characters. Valid characters include 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 management center. The NAT ID must not exceed 37 characters. Valid characters include alphanumerical characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the management center.

Example:

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

Step 5 Shut down the 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.

Register the Firewall with the Management Center

Register the firewall with the management center depending on which deployment method you are using.

Add the Firewall to the Management Center Using Zero-Touch Provisioning

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

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 Firepower 1010, the VLAN1 interface)— "inside", 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

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

Note For management center version 7.4, you need to add the device using CDO; see the 7.4 guide for more information. The native management center workflow was added in 7.6. Also, for cloud integration in 7.4, see the **SecureX Integration** page in the management center.

Before you begin

- If the device does not have a public IP address or FQDN, set a public IP address/FQDN for the management center (for example, if it is behind NAT), so the device can initiate the management connection. See .

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

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

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

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

For detailed information about this integration, see .

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

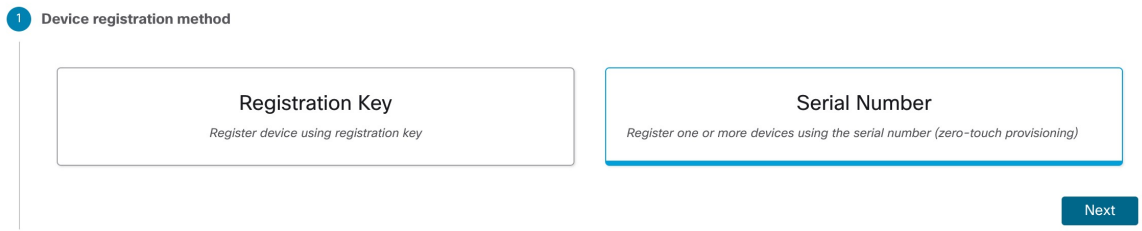
c) Make sure **Enable Zero-Touch Provisioning** is checked.
d) Click **Save**.

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

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

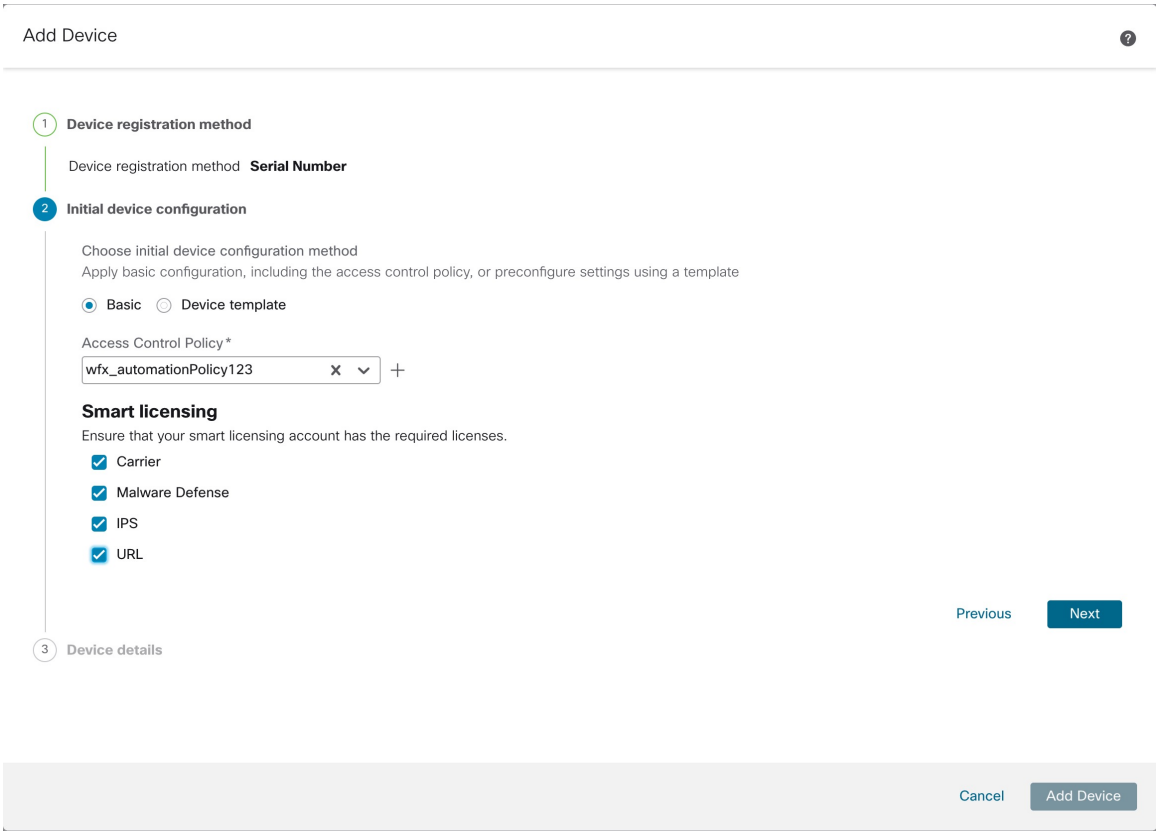
Step 4 Click **Use Serial Number**, and then click **Next**.

Figure 14: Device Registration Method



Step 5 For the **Initial device configuration**, click the **Basic** radio button.

Figure 15: Initial Device Configuration Method



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

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

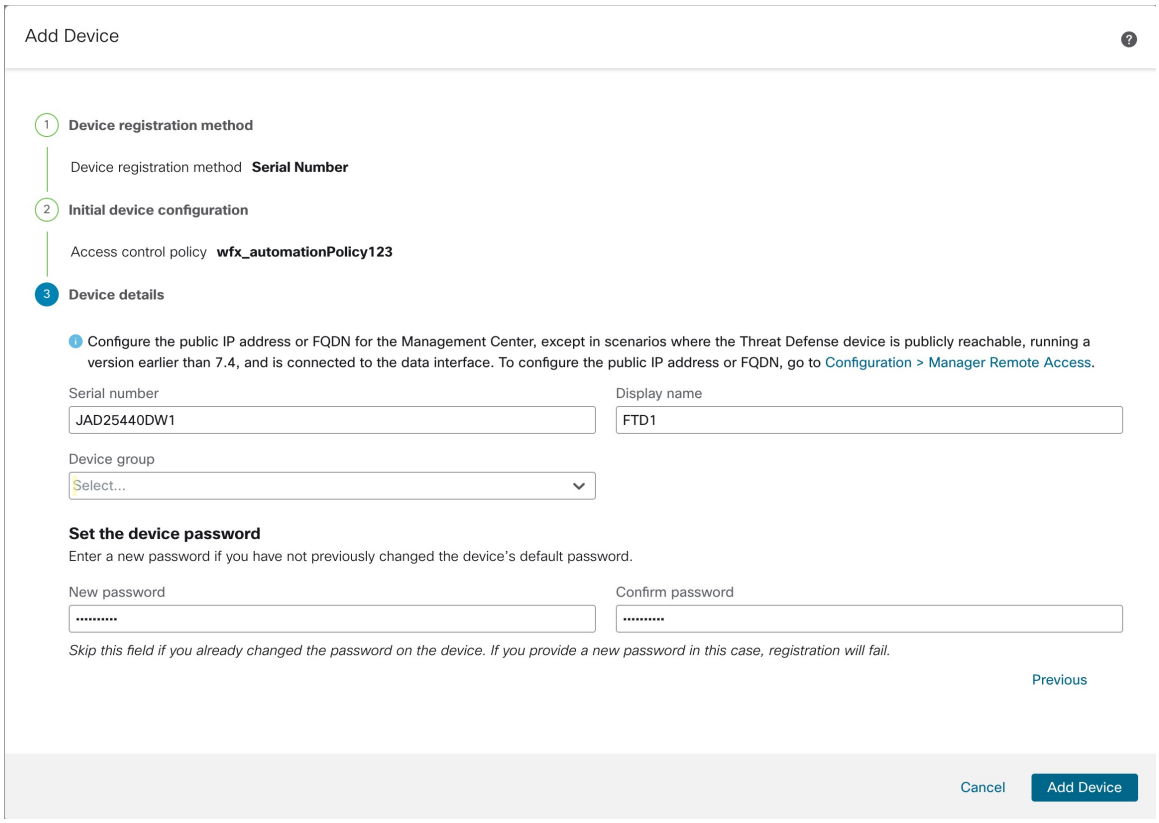
b) Choose **Smart licensing** licenses to apply to the device.

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

c) Click **Next**.

Step 6 Configure the **Device details**.

Figure 16: Device details



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

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

Step 7 Click **Add Device**.

It may take up to two minutes for the management center to verify the device's heartbeat and establish communication. If the registration succeeds, the device is added to the list.

Add the Firewall to the Management Center Using Manual Provisioning

Register the firewall to the management center manually using the device IP address or hostname and a registration key.

Step 1 Log into the management center.

a) Enter the following URL.

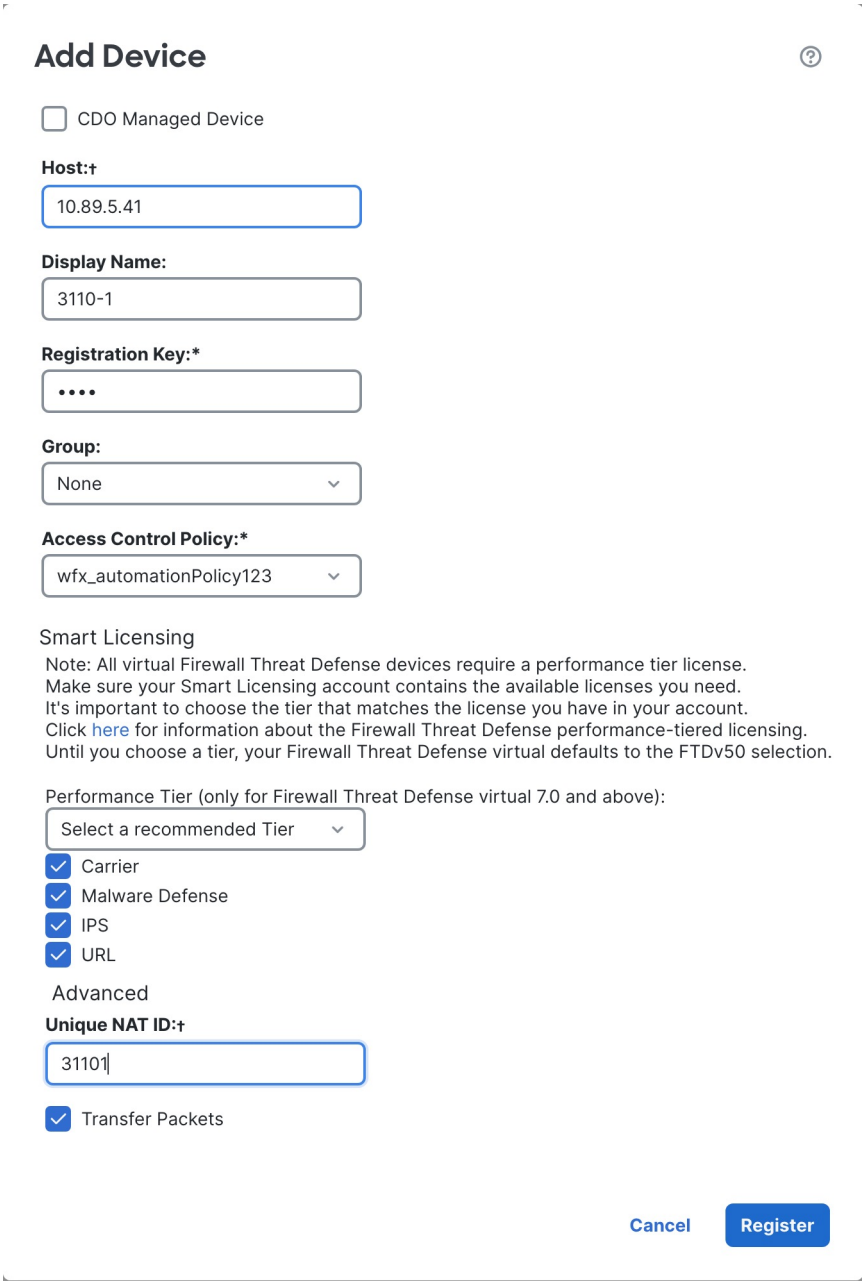
https://*fmc_ip_address*

b) Enter your username and password.
c) Click **Log In**.

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

Step 3 From the **Add** drop-down list, choose **Add Device**.

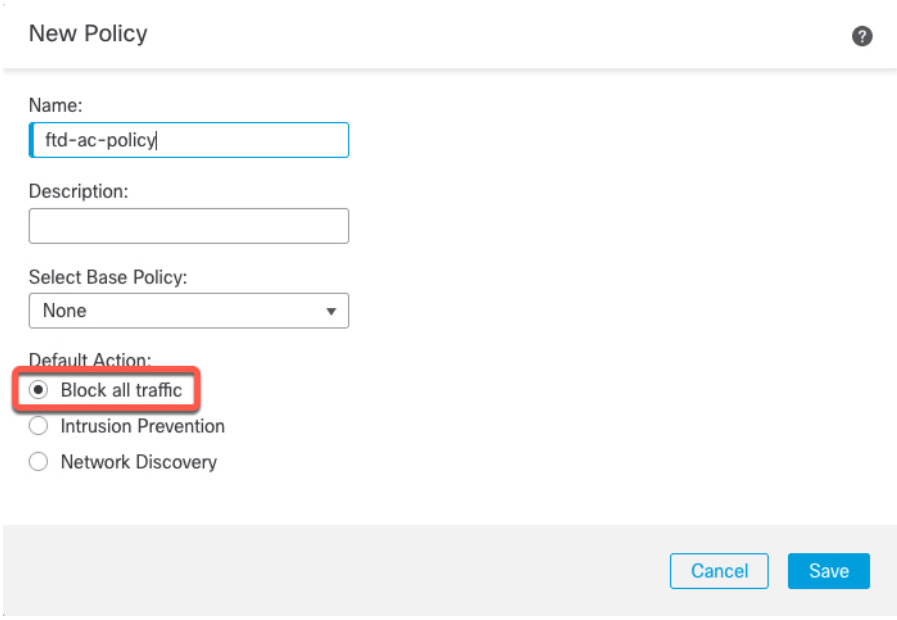
Figure 17: Add Device Using a Registration Key



Set the following parameters:

- **Host**—Enter the IP address or hostname of the firewall you want to add, if available. Leave this field blank if it is not available.
- **Display Name**—Enter the name for the firewall as you want it to display in the management center. You cannot change this name later.
- **Registration Key**—Enter the same registration key that you specified in the firewall 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 Configure an Access Control Rule, on page 36.

Figure 18: 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 initial configuration.
- **Transfer Packets**—Check the **Transfer Packets** check box so that for each intrusion event, the device transfers the packet to the management center for inspection.

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

Step 4 Click **Register**.

If the threat defense fails to register, check the following items:

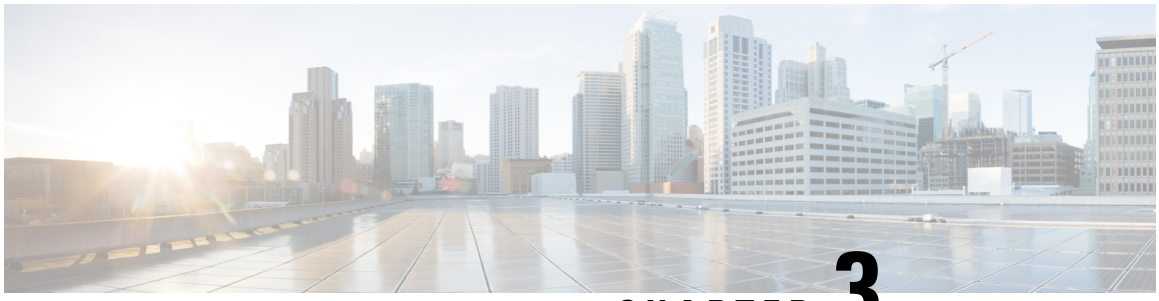
- Ping—Access the threat defense CLI (see Access the Threat Defense CLI, on page 3), and ping the management center IP address using the following command:

  ping system *fmc_ip_address*

  If the ping is not successful, check your network settings using the **show network** command. If you need to change the firewall Management IP address, use the **configure network management-data-interface** command.

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

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



CHAPTER 3

Configure a Basic Policy

Configure a basic security policy with the following settings:

- Inside and outside interfaces—Assign a static IP address to the inside interface, and use DHCP for the outside interface.
- DHCP server—Use a DHCP server on the inside interface for clients.
- Default route—Add a default route through the outside interface.
- NAT—Use interface PAT on the outside interface.
- Access control—Allow traffic from inside to outside.

You can also ccustomize your security policy to include more advanced inspections.

Configure Interfaces

When you use zero-touch provisioning or the device manager for initial setup instead of using the CLI, the following interfaces are preconfigured:

- Ethernet 1/1—**outside**, IP address from DHCP, IPv6 autoconfiguration
- VLAN1— **inside**, 192.168.95.1/24
- Default route—Obtained through DHCP on the outside interface

If you performed additional interface-specific configuration within device manager before registering with the management center, then that configuration is preserved.

If you used the CLI for initial setup, there is no preconfiguration of your device.

In both cases, you need to perform additional interface configuration after you register the device. For CLI initial setup, you must add the VLAN1 interface for the inside switch ports. Additional configuration includes

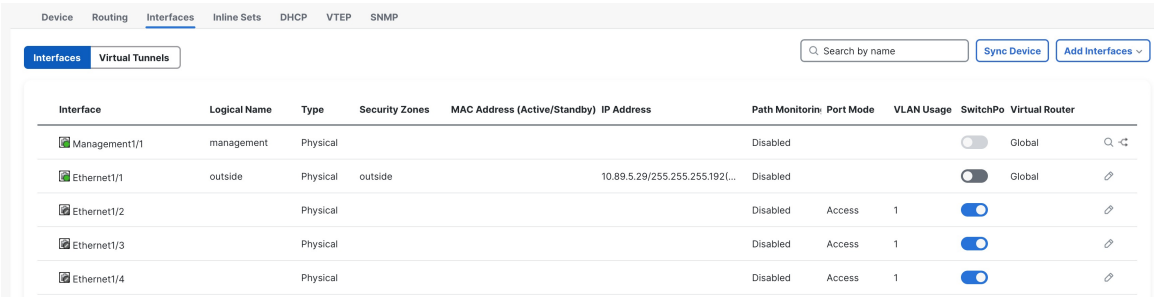
converting switch ports to firewall interfaces as desired, assigning interfaces to security zones, and changing IP addresses.

The following example configures a routed-mode inside interface (VLAN1) with a static address and a routed-mode outside interface using DHCP (Ethernet1/1). It also adds a DMZ interface for an internal web server.

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

Step 2 Click **Interfaces**.

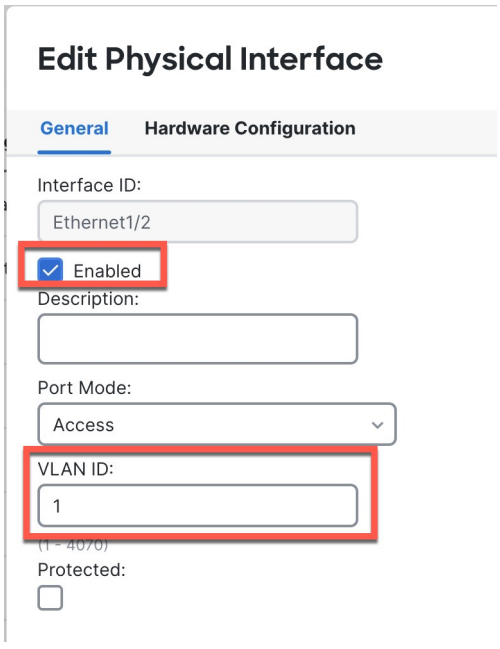
Figure 19: Interfaces



Step 3 If you used the CLI for initial setup, enable the switch ports.

a) Click **Edit** (✎) for the switch port.

Figure 20: Enable Switch Port



b) Enable the interface by checking the **Enabled** check box.

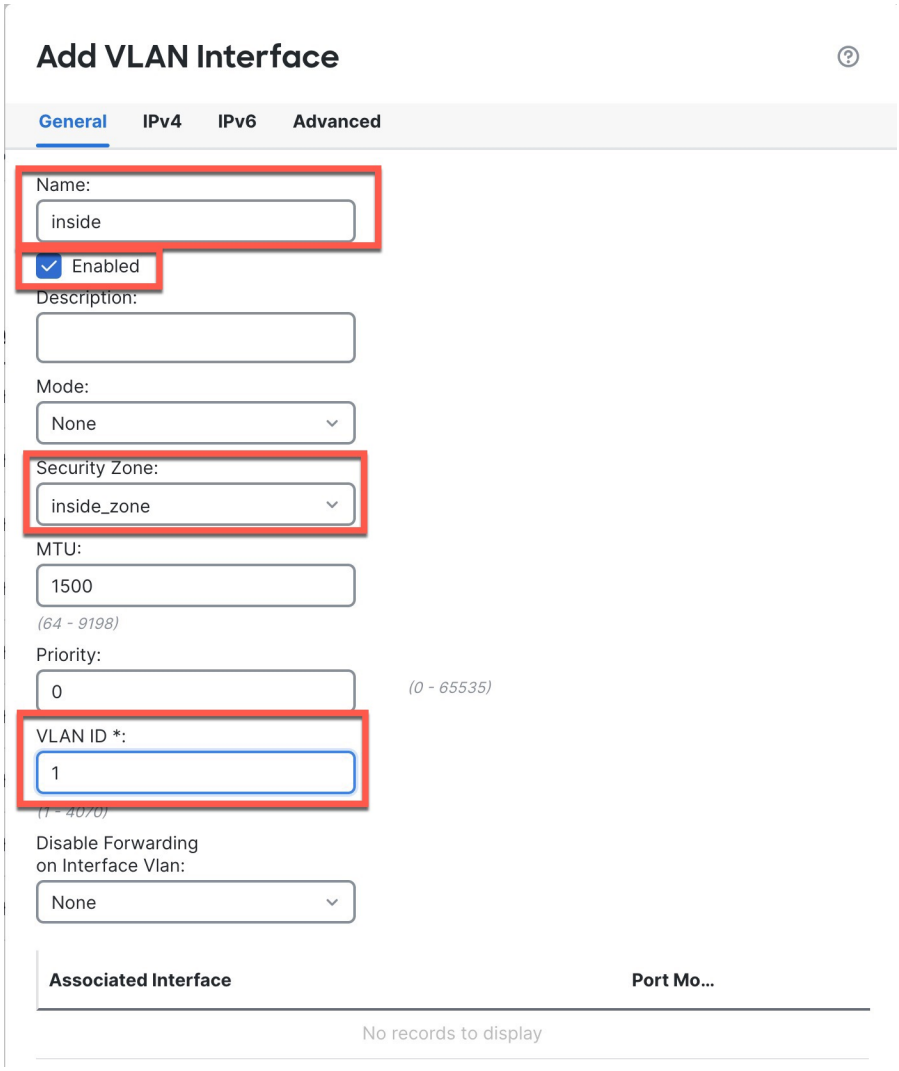
c) (Optional) Change the VLAN ID; the default is 1. You will next add a VLAN interface to match this ID.

d) Click **OK**.

Step 4 Add (or edit) the **inside** VLAN interface.

a) Click **Add Interfaces** > **VLAN Interface**, or if this interface already exists, click **Edit** (✎) for the interface.

Figure 21: Add VLAN Interface



b) 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**. You apply your security policy based on zones or groups.

If VLAN1 was preconfigured, the rest of these fields are optional.

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

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

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

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

f) Set the **VLAN ID** to **1**.

By default, all of the switchports are set to VLAN 1; if you choose a different VLAN ID here, you need to also edit each switchport to be on the new VLAN ID.

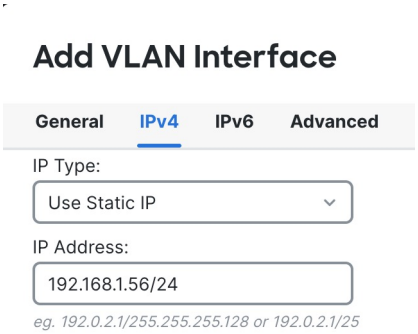
You cannot change the VLAN ID after you save the interface; the VLAN ID is both the VLAN tag used, and the interface ID in your configuration.

g) 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 **192.168.1.56/24**

  Figure 22: Set Inside IP Address



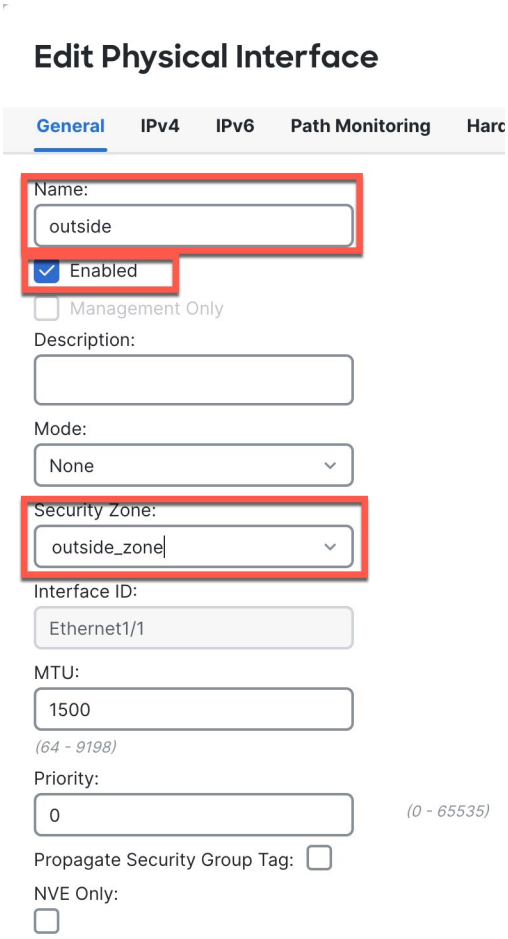
- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

h) Click **OK**.

Step 5 Click **Edit** (✎) for Ethernet1/1 that you want to use for **outside**.

The **General** page appears.

Figure 23: General



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**.

You should not alter any other basic settings because doing so will disrupt the management center management connection.

b) Click **OK**.

Step 6 Configure a DMZ interface to host a web server, for example.

a) Disable switch-port mode for the switch port you want to use for the DMZ by clicking the slider in the **SwitchPort** column so it shows as disabled ( ).

b) Click **Edit** ( ) for the interface.

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

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

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

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

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

f) Leave the **Mode** set to **None**.
g) Click the **IPv4** and/or **IPv6** tab and configure the IP address as desired.
h) Click **OK**.

Step 7 Click **Save**.

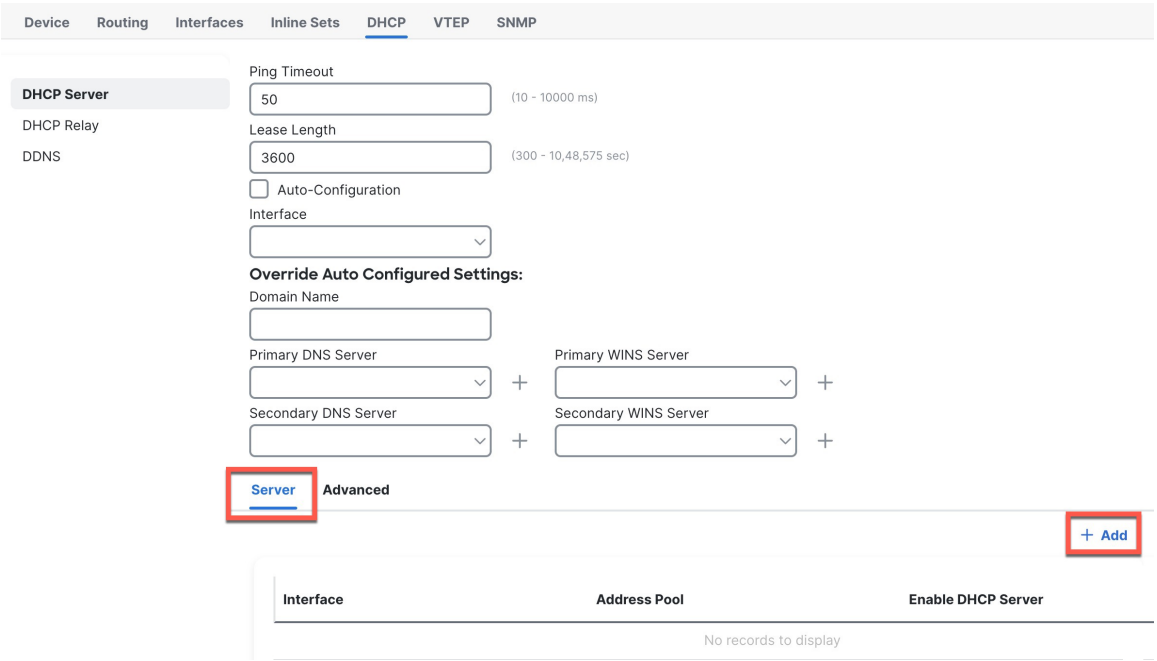
Configure the DHCP Server

Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the firewall.

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

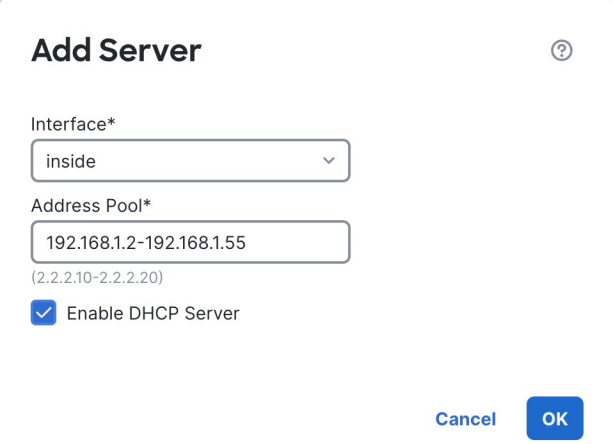
Step 2 Choose **DHCP** > **DHCP Server**.

Figure 24: DHCP Server



Step 3 In the **Server** area, click **Add** and configure the following options.

Figure 25: Add Server



- **Interface**—Choose the interface name from the drop-down list.
- **Address Pool**—Set the range of IP addresses. The 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**.

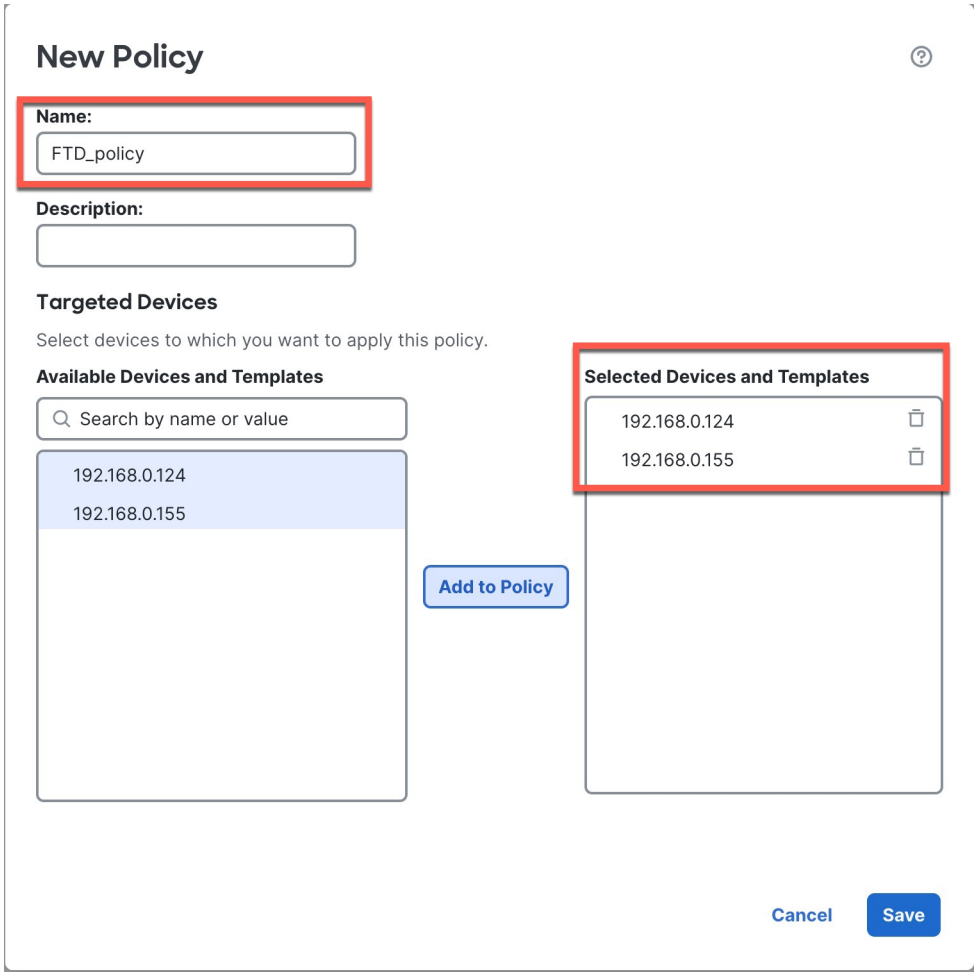
Configure NAT

This procedure creates a NAT rule for internal clients to convert the internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

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

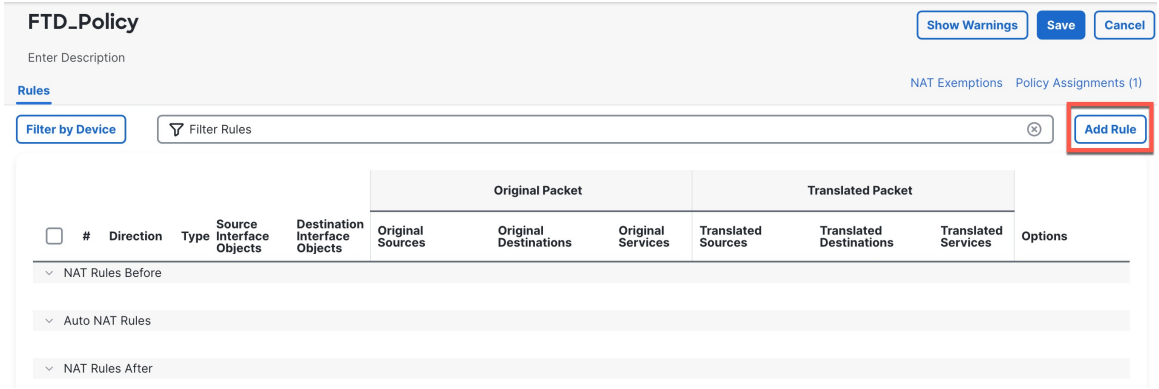
Step 2 Name the policy, select the devices that you want to use the policy, and click **Save**.

Figure 26: New Policy



The policy is added the management center. You still have to add rules to the policy.

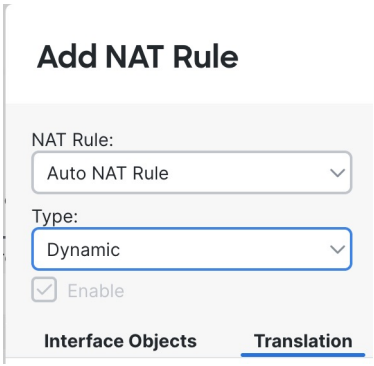
Figure 27: NAT Policy



Step 3 Click **Add Rule**.

Step 4 Configure the basic rule options:

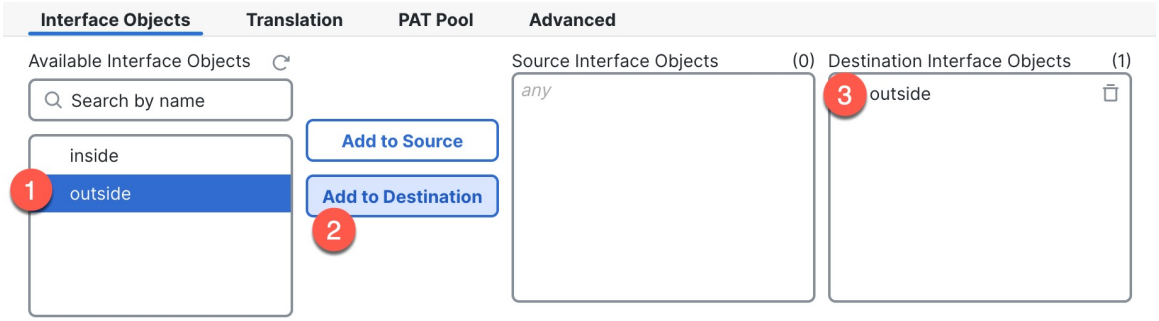
Figure 28: Basic Rule Options



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

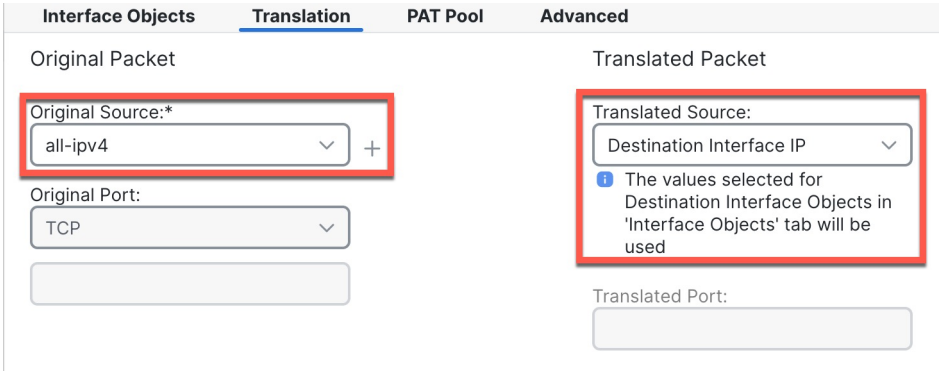
Step 5 On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 29: Interface Objects



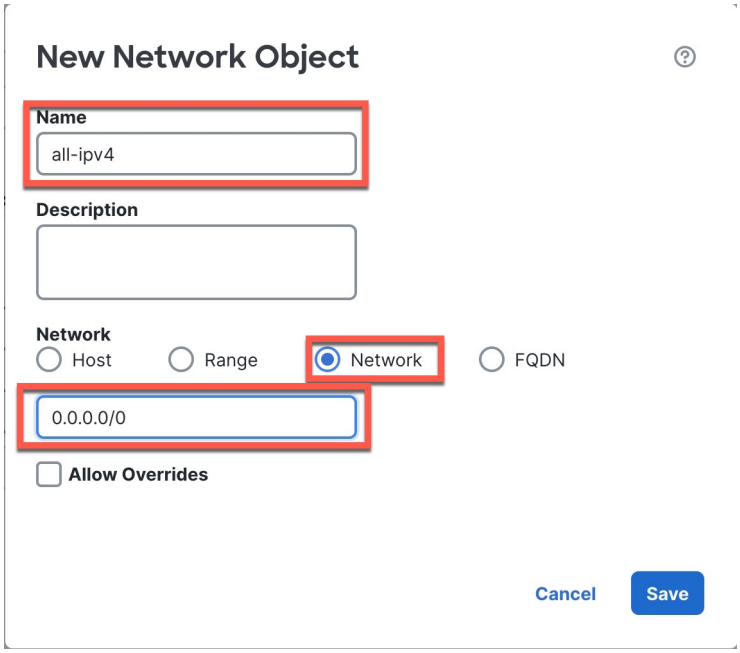
Step 6 On the **Translation** page, configure the following options:

Figure 30: Translation



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

Figure 31: 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.

Configure an Access Control Rule

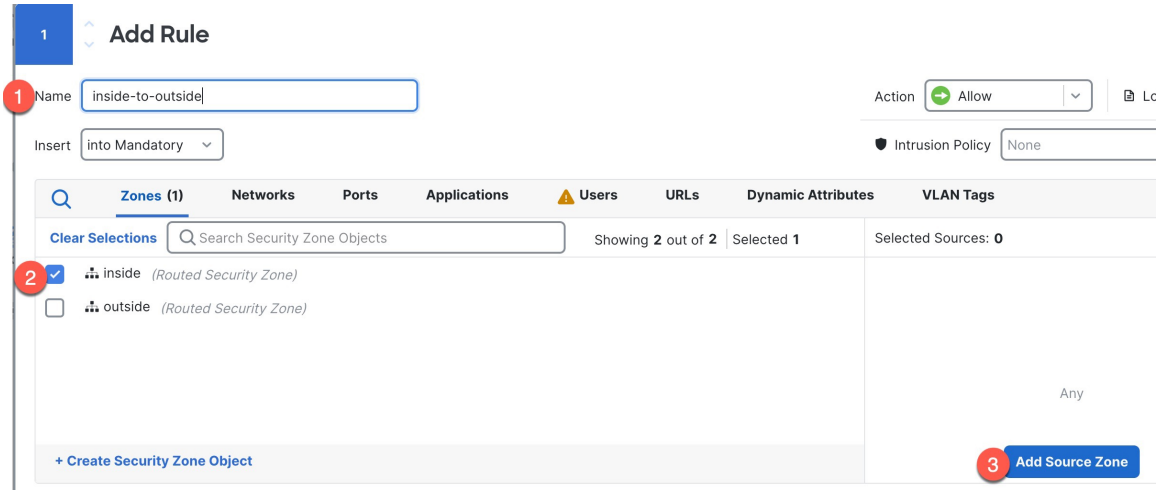
If you created a basic **Block all traffic** access control policy when you registered the device, then you need to add rules to the policy to allow traffic through the device. The access control policy can include multiple rules that are evaluated in order.

This procedure creates an access control rule to allow all traffic from the inside zone to the outside zone.

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

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

Figure 32: Source Zone

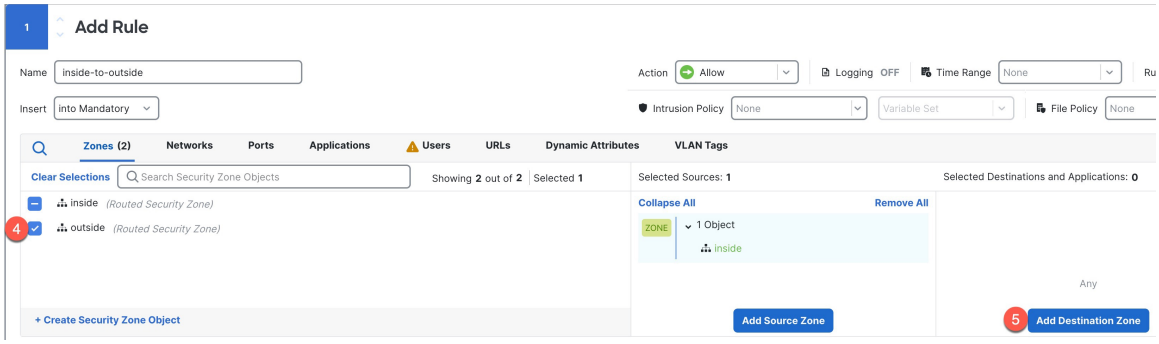


1. Name this rule, for example, **inside-to-outside**.

2. Select the inside zone from **Zones**

3. Click **Add Source Zone**.

Figure 33: Destination Zone



4. Select the outside zone from **Zones**.

5. Click **Add Destination Zone**.

Leave the other settings as is.

Step 3 (Optional) Customize associated policies by clicking on the policy type in the packet flow diagram.

Prefilter, Decryption, Security Intelligence, and Identity policies are applied before an access control rule. Customizing these policies is not required, but after you know your network's needs, they let you improve network performance by either fastpathing trusted traffic (bypassing processing) or blocking traffic so no further processing is required.

Figure 34: Policies Applied Before Access Control

- **Prefilter Rules**—The Default Prefilter Policy passes all traffic for the other rules to act on (analyzes). The only change to the default policy you can make is to **block** tunnel traffic. Otherwise, you can create a new prefilter policy to associate with the access control policy that can analyze (pass on), fastpath (bypass further checks) or block.

  Prefiltering lets you improve performance by dealing with traffic before it gets any further, by either blocking or fastpathing. In a new policy, you can add *tunnel* rules and *prefilter* rules. A tunnel rule lets you fastpath, block, or rezone plaintext (non-encrypted), passthrough tunnels. A prefilter rule lets you fastpath or block non-tunneled traffic identified by IP address, port, and protocol.

  For example, if you know you want to block all FTP traffic on your network, but fastpath SSH traffic from an administrator, you can add a new prefilter policy.

- **Decryption**—Decryption is not applied by default. Decryption is a way to expose network traffic to deep inspection. In most cases, you don't want to decrypt traffic, and can only do so if it is legally allowed. For maximum network protection, a decryption policy might be a good idea for traffic going to critical servers or coming from untrusted network segments.

- **Security Intelligence**—(Requires the IPS license) Security Intelligence is enabled by default. Security Intelligence is another early defense against malicious activity applied before passing connections to the access control policy for further processing. Security Intelligence uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domain names provided by Talos, the threat intelligence organization at Cisco. You can add or delete additional IP addresses, URLs, or domains if desired.

  Note If you do not have the IPS license, this policy will not be deployed even though it shows in your access control policy as enabled.

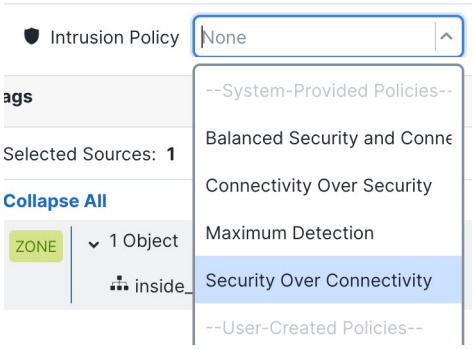
- **Identity**—Identity is not applied by default. You can require a user to authenticate before allowing traffic to be processed by the access control policy.

Step 4 (Optional) Add an Intrusion policy that is applied after the access control rule.

The Intrusion policy is a defined set of intrusion detection and prevention configurations that inspects traffic for security violations. The management center includes many system-provided policies you can enable as-is or that you can customize. This step enables a system-provided policy.

a) Click the **Intrusion Policy** drop-down list.

Figure 35: System-Provided Intrusion Policies

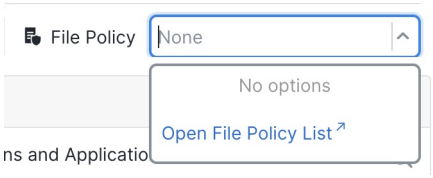


b) Choose one of the system-provided policies from the list.

Step 5 (Optional) Add a File policy that is applied after the access control rule.

a) Click the **File Policy** drop-down list and choose either an existing policy or add one by choosing the **Open File Policy List**.

Figure 36: File Policy



For a new policy, the **Policies** > **Malware & File** page opens in a separate tab.

b) See the Cisco Secure Firewall Device Manager Configuration Guide for details on creating the policy.
c) Return to the **Add Rule** page and select the newly created policy from the drop-down list.

Step 6 Click **Apply**.

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

Step 7 Click **Save**.

Enable SSH on the Outside Interface

This section describes how to enable SSH connections to the outside interface.

By default, you can use the **admin** user for which you configured the password during initial setup.

Step 1 Choose **Devices** > **Platform Settings** and create or edit the threat defense policy.

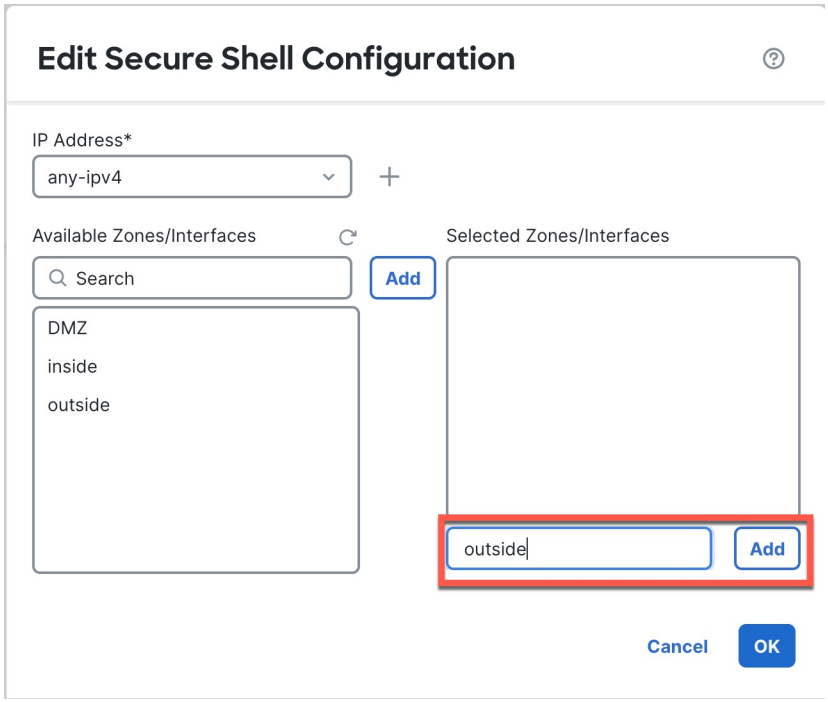
Step 2 Select **SSH Access**.

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

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 outside zone or type the **outside** interface name into the field below the **Selected Zones/Interfaces** list and click **Add**.

Figure 37: Enable SSH on the Outside Interface



c) Click **OK**.

Step 4 Click **Save**.

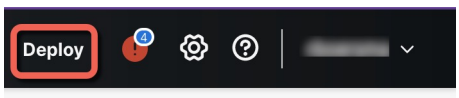
You can now go to **Deploy** > **Deployment** and deploy the policy to assigned devices. The changes are not active until you deploy them.

Deploy the Configuration

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

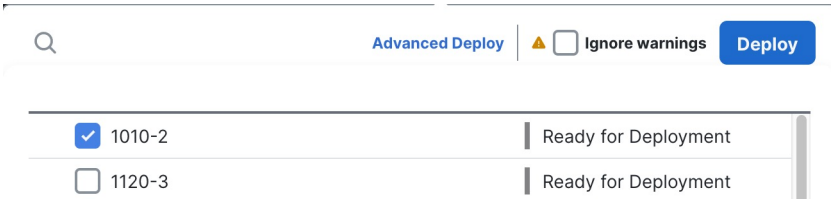
Step 1 Click **Deploy** in the upper right.

Figure 38: Deploy



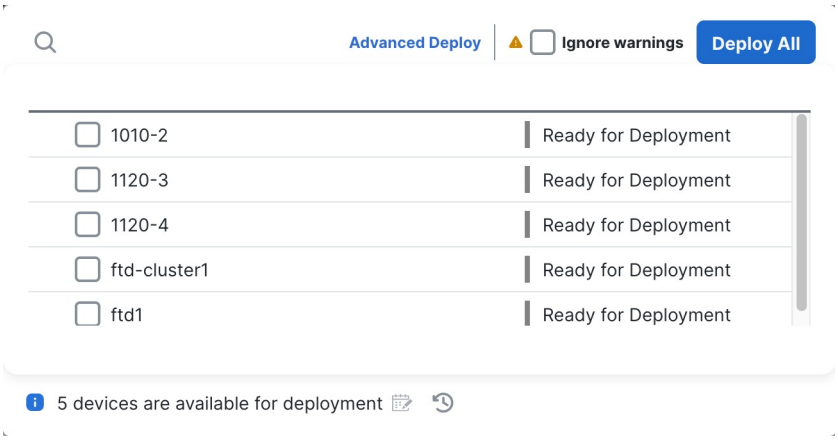
Step 2 For a quick deployment, check specific devices and then click **Deploy**.

Figure 39: Deploy Selected



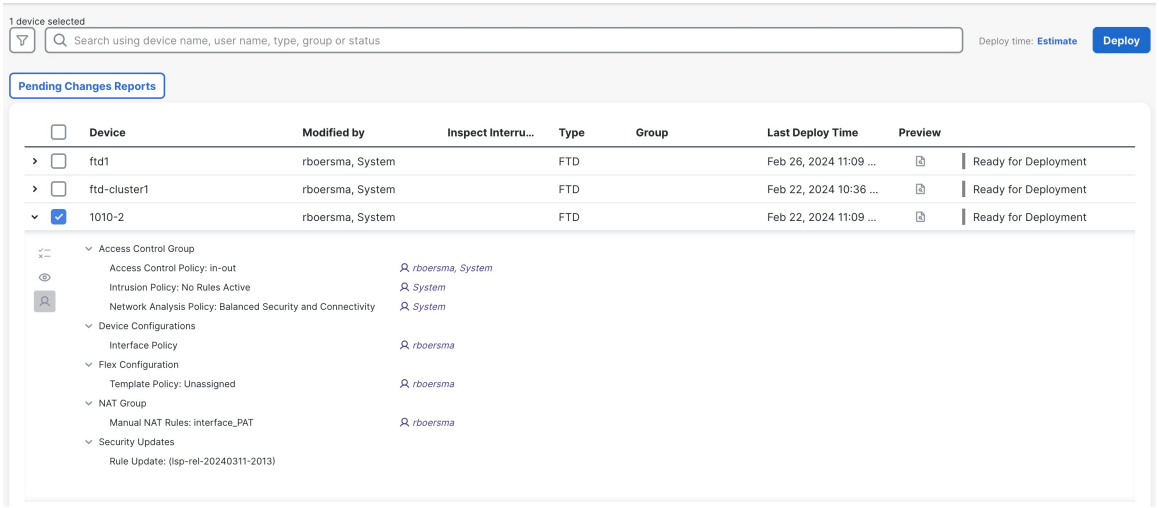
Or click **Deploy All** to deploy to all devices.

Figure 40: Deploy All



Otherwise, for additional deployment options, click **Advanced Deploy**.

Figure 41: Advanced Deployment



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 42: Deployment Status