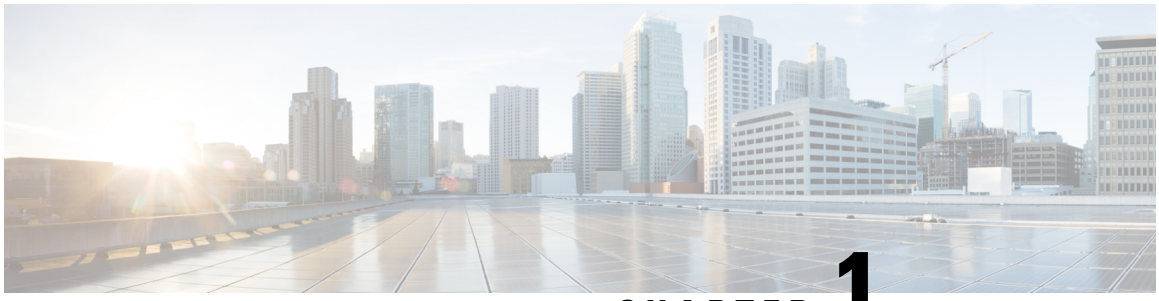
Firepower 1010 Threat Defense Getting Started: Cloud-delivered Firewall Management Center

First Published: 2024-10-16

Last Modified: 2026-03-19

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

The Firepower 1000 delivers business resiliency, management ease-of-use, and threat defense. It offers exceptional sustained performance when advanced threat functions are enabled. The Firepower 1000 addresses use cases from small offices to remote branches.

Install the firewall at a branch office and manage it on the outside interface using the Security Cloud Control (formerly Cisco Defense Orchestrator).

Note For high availability if you use zero-touch provisioning, we recommend using the Management interface. If you use zero-touch provisioning on outside and want to use high availability, you will have to change the outside IP address to a static address after registration.

This guide specifically covers outside management, but you can refer to *Cisco Security Cloud Control: Cloud-Delivered Firewall Management Center for Firewall Threat Defense* 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, 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.

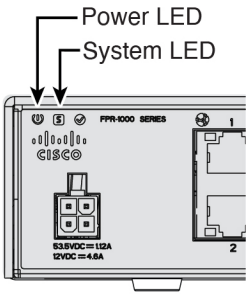
Procedure

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 LEDs for the current status.

Figure 1: LEDs



- Power LED—Solid green means the firewall is powered on.
- System (S) LED—See the following behavior:

Table 1: System (S) LED Behavior

LED Behavior	Description	Time After Device Powered On (minutes:seconds)
Fast flashing green	Booting up	01:00
Fast flashing amber (error condition)	Failed to boot up	01:00
Solid green	Application loaded	15:00 - 30:00
Solid amber (error condition)	Application failed to load	15:00 - 30:00

After you connect the outside interface to the internet (see Cable the firewall, on page 11), check the System LED to check the cloud connection status for zero-touch provisioning.

Table 2: Zero-Touch Provisioning: System (S) LED behavior

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

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

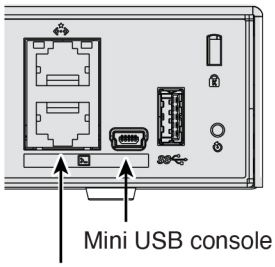
Which application is installed: Firewall Threat Defense or ASA?

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

Procedure

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 Firewall Threat Defense or ASA.

Firewall 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 Firewall Threat Defense CLI, on page 4.

```
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*.

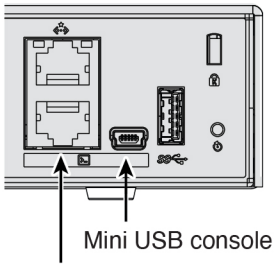
Access the Firewall Threat Defense CLI

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

Procedure

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 Firewall Threat Defense CLI.

Note
If you want to use the Firewall Device Manager for initial setup, do not access the Firewall Threat Defense CLI, which starts the CLI setup.

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

connect ftd

The first time you connect to the Firewall Threat Defense CLI, you are prompted to complete initial setup.

Example:

```
firepower# connect ftd
>
```

To exit the Firewall 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.

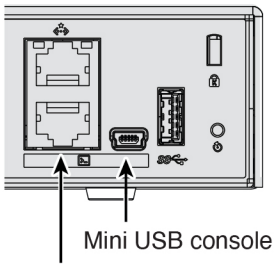
What version should I run?

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.

Procedure

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

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 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 firewall. See (If Needed) Power off the firewall, on page 8.

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 Security Cloud Control with the Smart Software Manager. Registering requires you to generate a registration token in the Smart Software Manager. See the Security Cloud Control documentation for detailed instructions.

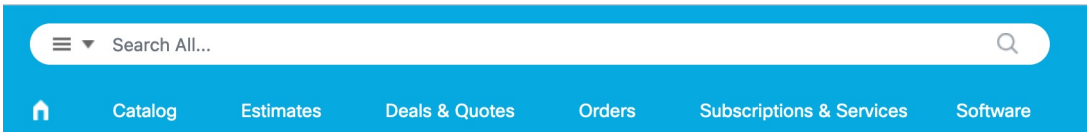
The Firewall Threat Defense has the following licenses:

- 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. Search for the following license PIDs.

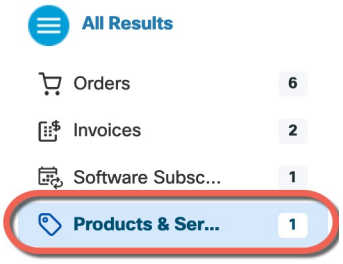
Note If a PID is not found, you can add the PID manually to your order.

- 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.

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

Figure 6: Results



(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..

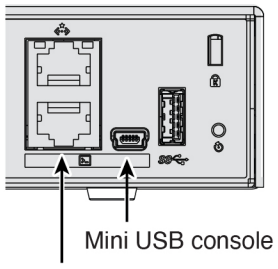
Power off the firewall at the CLI

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

Procedure

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 Firewall Management Center

Shut down your system properly using the Firewall Management Center.

Procedure

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.

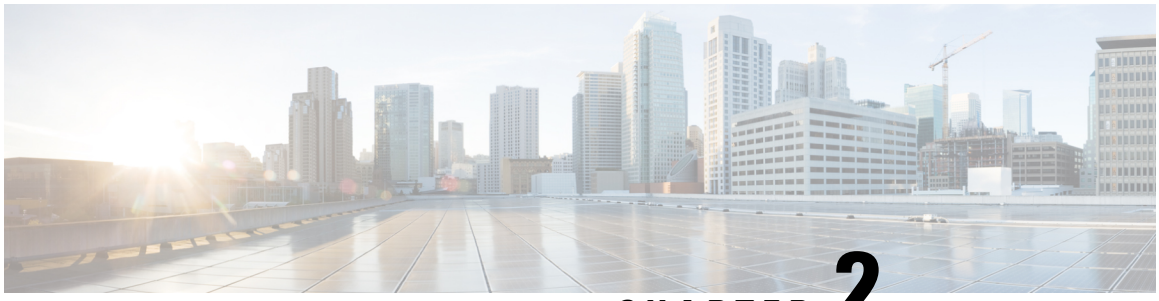
Step 2 If you have a console connection to the firewall, monitor the system prompts as the firewall shuts down. When shutdown is complete, you will see the following prompt.

```
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.



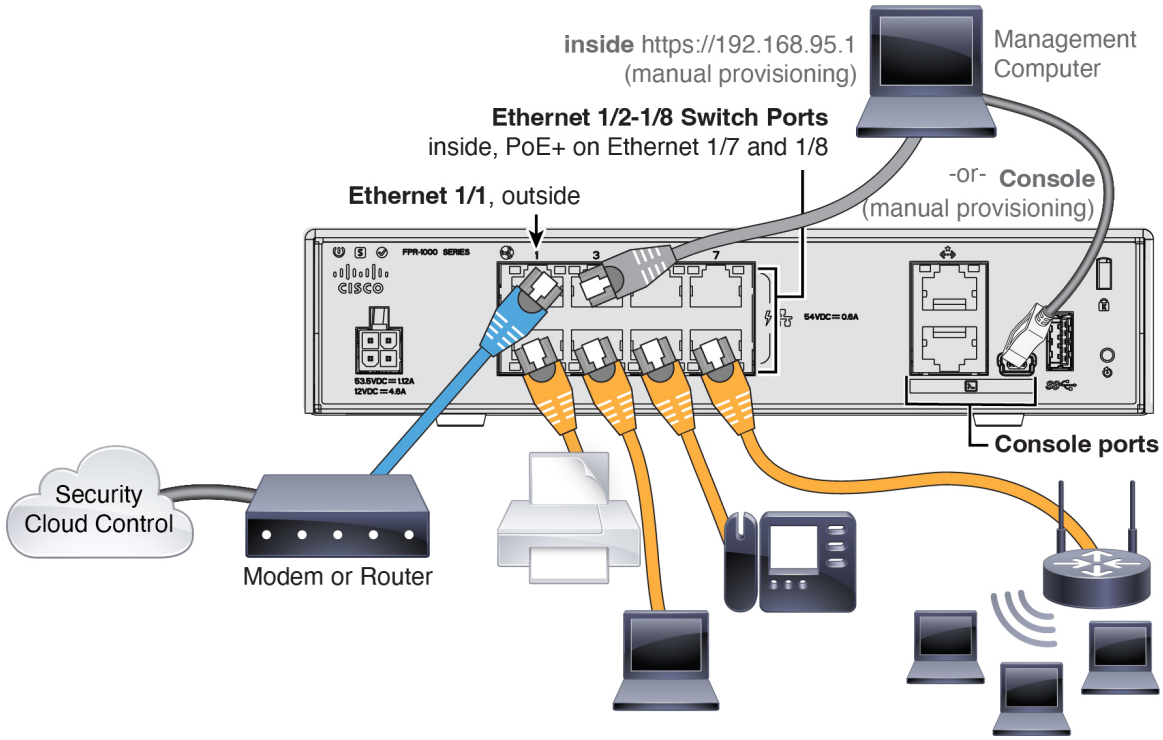
CHAPTER 2

Cable and Onboard the Firewall

Cable and onboard the firewall to Security Cloud Control.

Cable the firewall

- See the hardware installation guide for more information.
- If you use zero-touch provisioning, do not cable both the outside and the Management interface. This guide covers management on the outside interface, but you may want to use zero-touch provisioning on Management with high availability. If you use zero-touch provisioning on outside and want to use high availability, you will have to change the outside IP address to a static address after registration.



Onboard the firewall to Security Cloud Control

Onboard the firewall using zero-touch provisioning or manual provisioning. Log into Security Cloud Control at https://security.cisco.com.

Onboard the firewall with zero-touch provisioning

Onboard the Firewall Threat Defense using zero-touch provisioning and the device serial number.

Before you begin

- Obtain your device's serial number.
  - 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 the bottom.
  - 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.
- Check your LEDs to make sure the firewall is ready for registration.

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

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

Procedure

Step 1 In the Security Cloud Control navigation menu, click **Security Devices**, then click the blue plus button (+) to **Onboard** a device.

Step 2 Select the **FTD** tile.

Step 3 Under **Management Mode**, be sure **FTD** is selected.

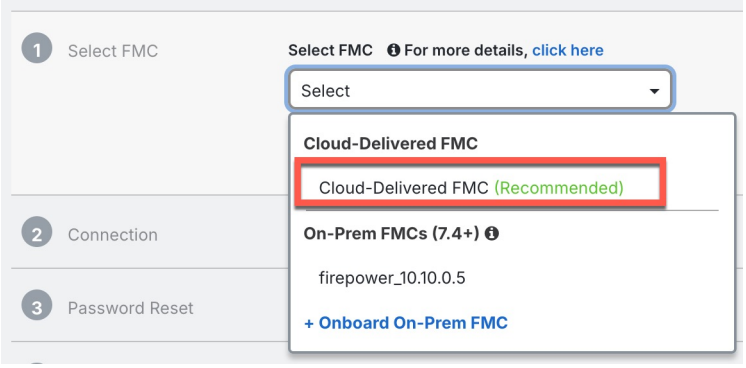
At any point after selecting **FTD** as the management mode, you can click **Manage Smart License** to enroll in or modify the existing smart licenses available for your device. See Obtain licenses, on page 6 to see which licenses are available.

Step 4 Select **Use Serial Number** as the onboarding method.

Figure 8: Use Serial Number

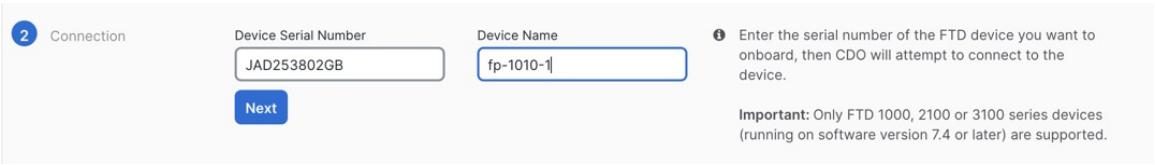
Step 5 In **Select FMC**, choose the **Cloud-Delivered FMC** > **Cloud-Delivered FMC** from the list, and click **Next**.

Figure 9: Select FMC



Step 6 In the **Connection** area, enter the **Device Serial Number** and the **Device Name** and then click **Next**.

Figure 10: Connection

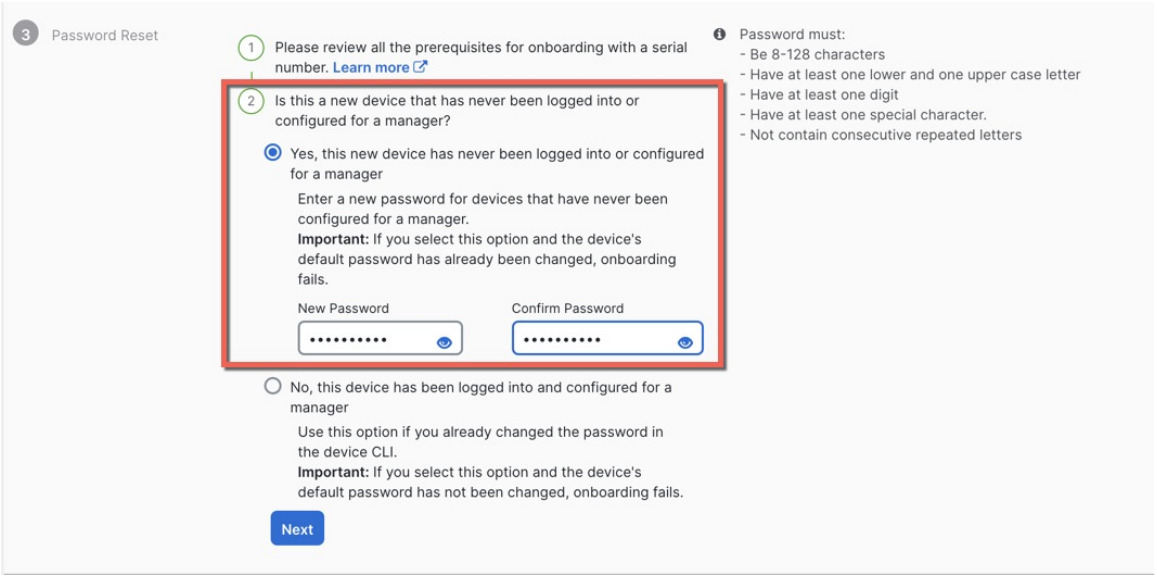


Step 7 In **Password Reset**, click **Yes...**. Enter a new password and confirm the new password for the device, then click **Next**.

For zero-touch provisioning, the device must be brand new or has been reimaged.

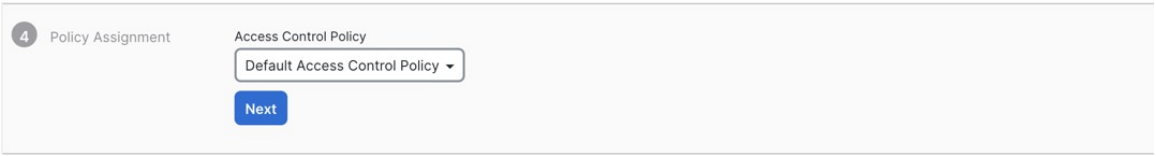
Note
If you logged into the device and reset the password, and you did not change the configuration in a way that would disable zero-touch provisioning, then you should choose the **No...** option. There are a number of configurations that disable zero-touch provisioning provisioning, so we don't recommend logging into the device unless you need to, for example, to perform a reimage.

Figure 11: Password Reset



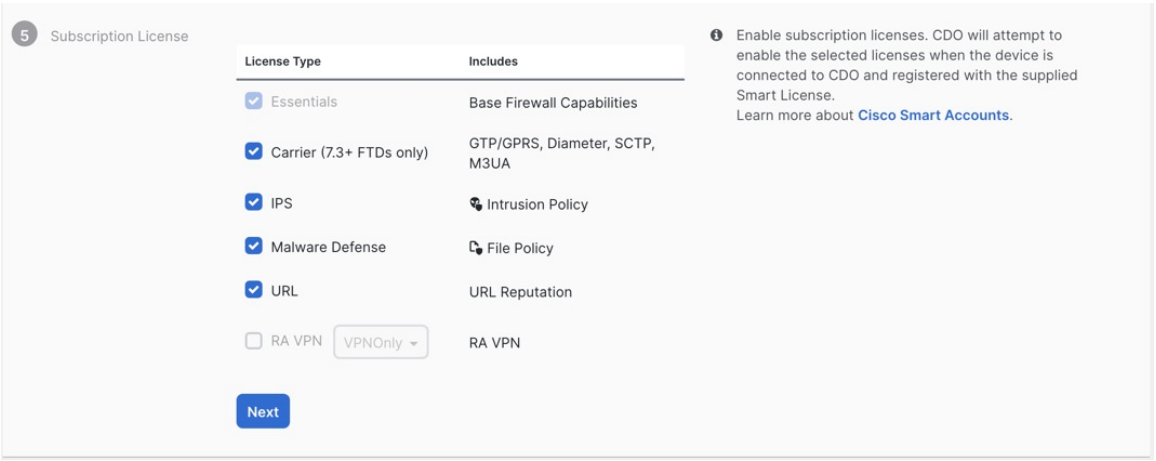
Step 8 For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 12: Policy Assignment



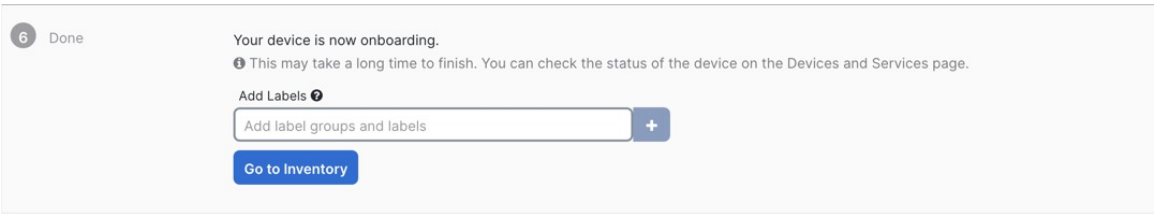
Step 9 For the **Subscription License**, check each of the feature licenses you want to enable. Click **Next**.

Figure 13: Subscription License



Step 10 (Optional) Add labels to your device to help sort and filter the **Security Devices** page. Enter a label and select the blue plus button (+). Labels are applied to the device after it's onboarded to Security Cloud Control.

Figure 14: Done



What to do next

From the **Security Devices** page, select the device you just onboarded and select any of the option listed under the **Management** pane located to the right.

Onboard the firewall with manual provisioning

Onboard the firewall using a CLI registration key.

Procedure

Step 1 In the Security Cloud Control navigation menu, click **Security Devices**, then click the blue plus button (+) to **Onboard** a device.

Step 2 Click the **FTD** tile.

Step 3 Under **Management Mode**, be sure **FTD** is selected.

Step 4 Select **Use CLI Registration Key** as the onboarding method.

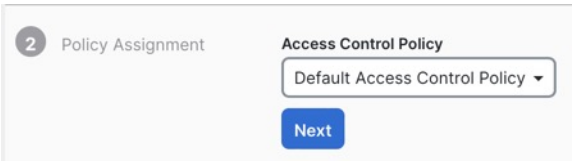
Figure 15: Use CLI Registration Key

Step 5 Enter the **Device Name** and click **Next**.

Figure 16: Device Name

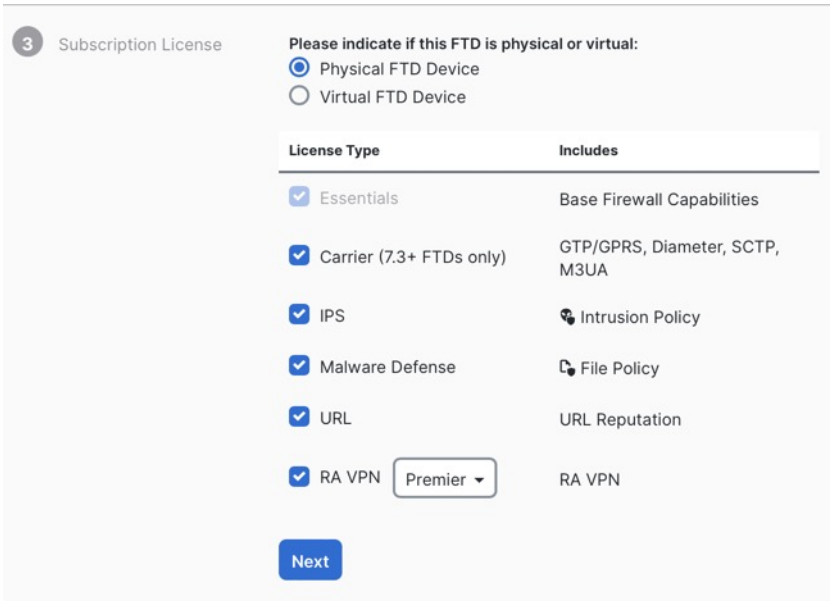
Step 6 For the **Policy Assignment**, use the drop-down menu to choose an access control policy for the device. If you have no policies configured, choose the **Default Access Control Policy**.

Figure 17: Access Control Policy



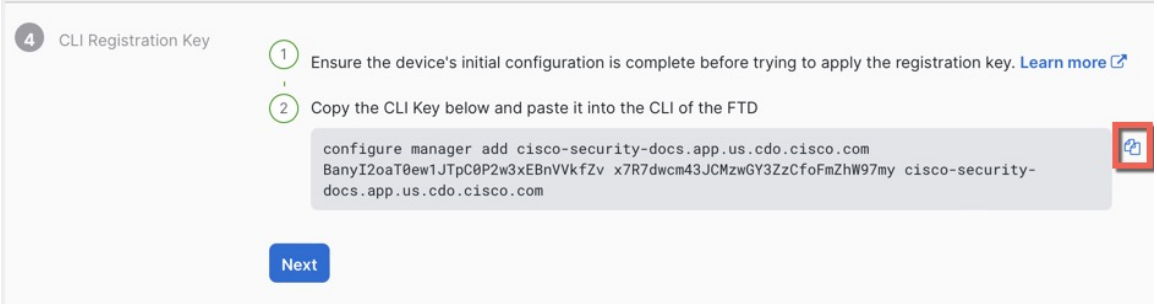
Step 7 For the **Subscription License**, click the **Physical FTD Device** radio button, and then check each of the feature licenses you want to enable. Click **Next**.

Figure 18: Subscription License



Step 8 For the **CLI Registration Key**, Security Cloud Control generates a command with the registration key and other parameters. You must copy this command and use it in the intial configuration of the Firewall Threat Defense.

Figure 19: CLI Registration Key



configure manager add Security Cloud Control_*hostname registration_key nat_id display_name*

Complete initial configuration at the CLI or using the Firewall Device Manager:

- Initial configuration: CLI, on page 25—Copy this command at the Firewall Threat Defense CLI after you complete the startup script.
- Initial configuration: Firewall Device Manager, on page 19—Copy the *scc_hostname*, *registration_key*, and *nat_id* parts of the command into the **Management Center/Security Cloud Control Hostname/IP Address**, **Management Center/Security Cloud Control Registration Key**, and **NAT ID** fields.

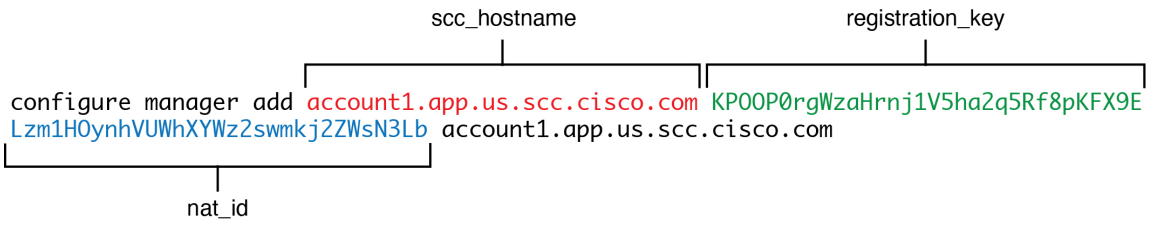
Example:

Sample command for CLI setup:

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

Sample command components for GUI setup:

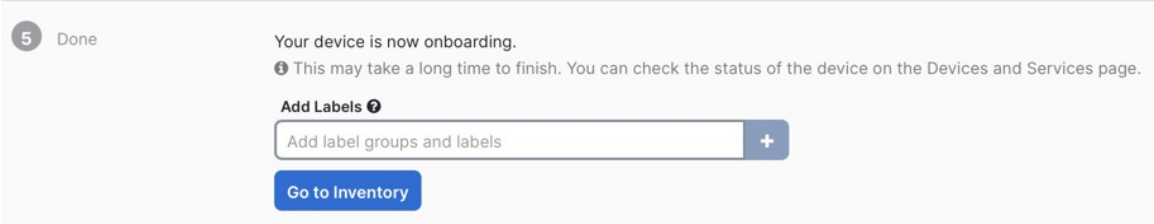
Figure 20: configure manager add command components



Step 9 Click **Next** in the onboarding wizard to start registering the device.

Step 10 (Optional) Add labels to your device to help sort and filter the **Security Devices** page. Enter a label and select the blue plus button (+). Labels are applied to the device after it's onboarded to Security Cloud Control.

Figure 21: Done



Perform initial configuration (manual provisioning only)

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

Initial configuration: Firewall 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 Firewall Device Manager is preserved.

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

Procedure

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

Step 2 Log into the Firewall Device Manager.

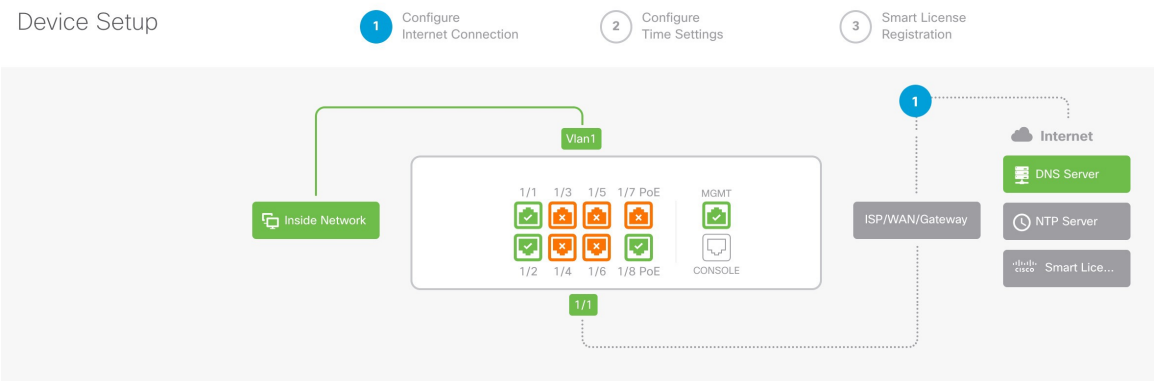
a) Go to https://192.168.95.1.

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.

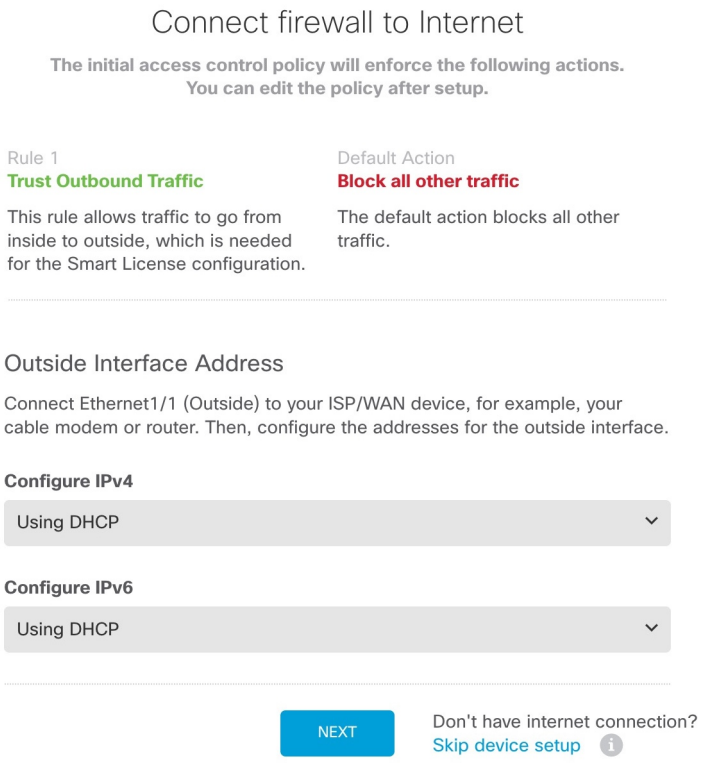
Figure 22: Device Setup



Note
The exact port configuration depends on your model.

a) Configure the outside and management interfaces.

Figure 23: 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

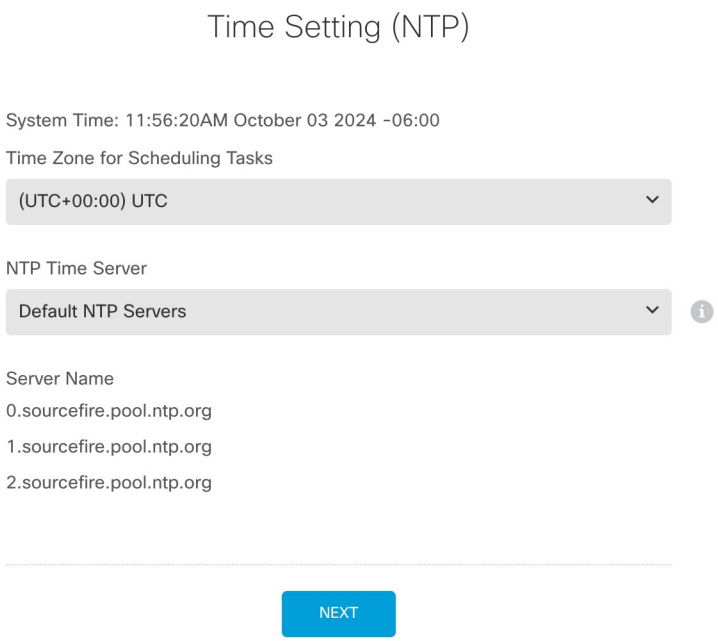
interface will resolve FQDNs using these Management interface DNS servers, and not the outside interface DNS servers.

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.

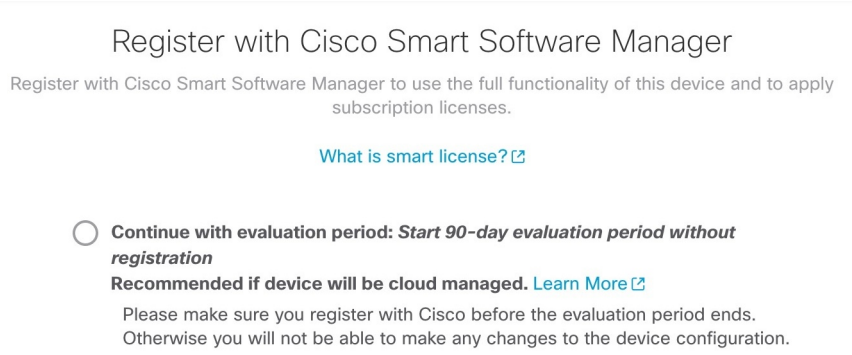
Firewall Hostname

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

Figure 24: Time Setting (NTP)



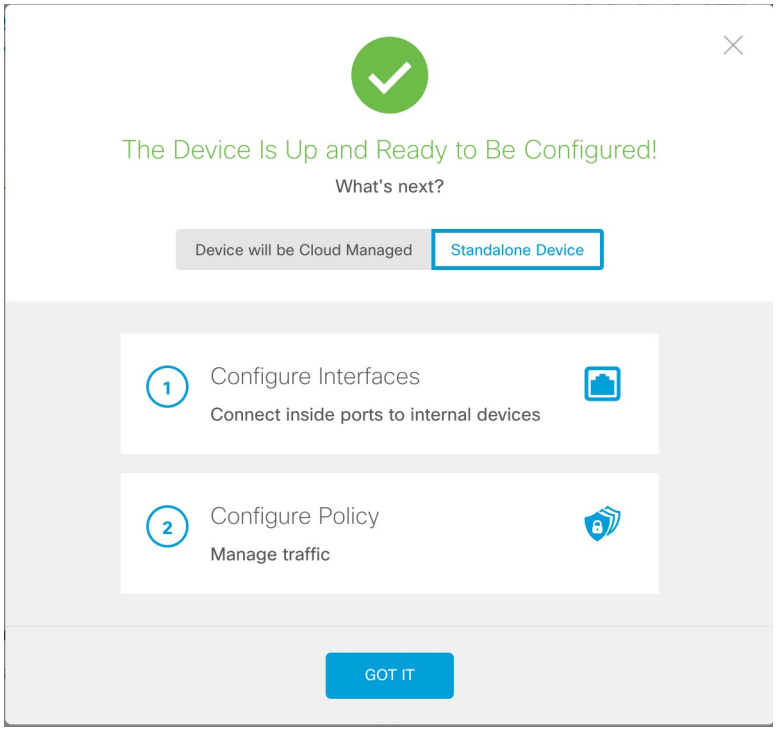
c) Select **Start 90 day evaluation period without registration**.



Do not register the Firewall Threat Defense with the Smart Software Manager; all licensing is performed on the Security Cloud Control.

d) Click **Finish**.

Figure 25: What's Next



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

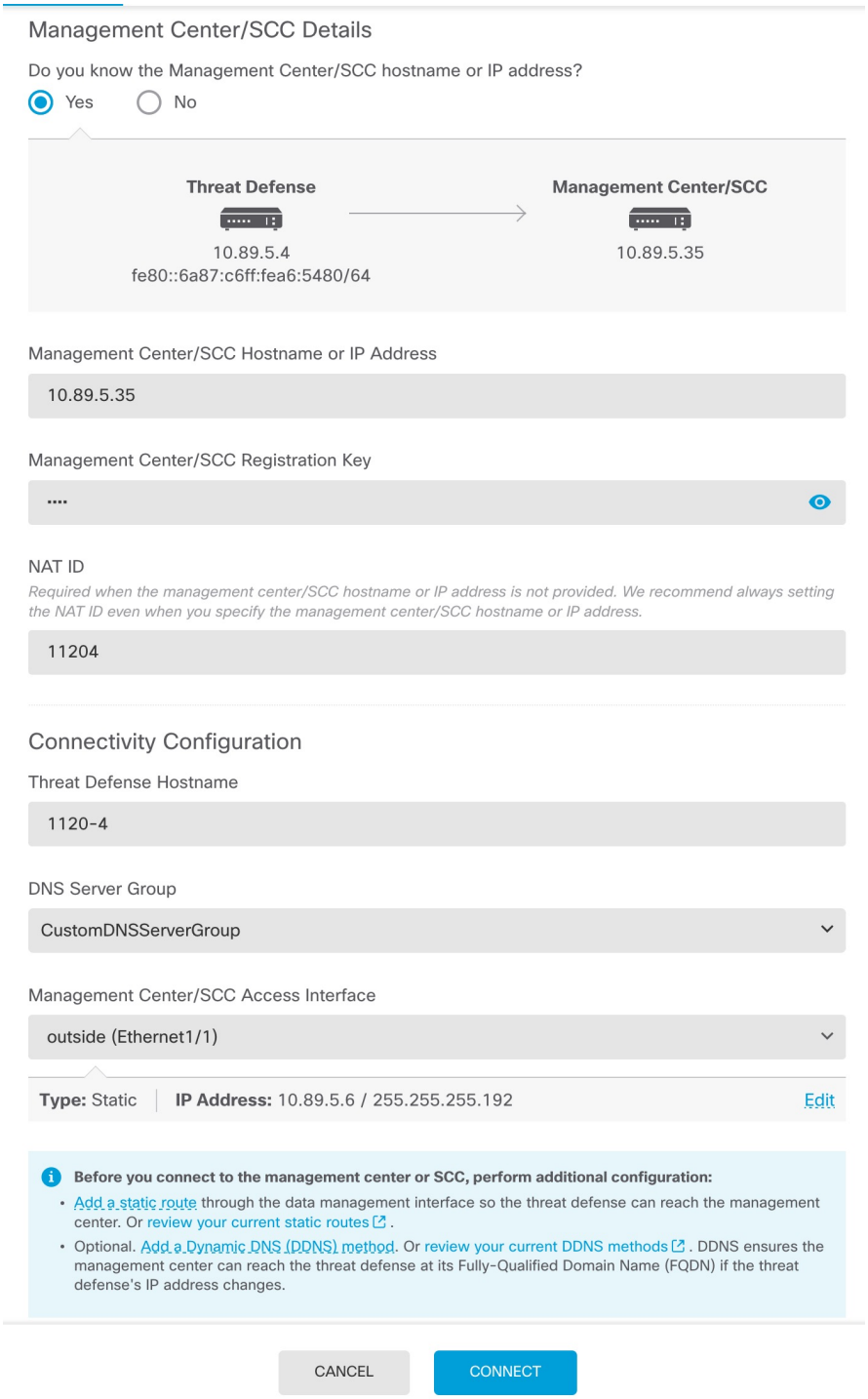
Step 4 If you want to configure additional interfaces, choose **Device**, and then click the link in the **Interfaces** summary.

Step 5 Register with the Security Cloud Control by choosing **Device** > **System Settings** > **Central Management** and clicking **Proceed**

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

Note
Older versions may show "CDO" instead of "SCC."

Figure 26: Management Center/SCC Details



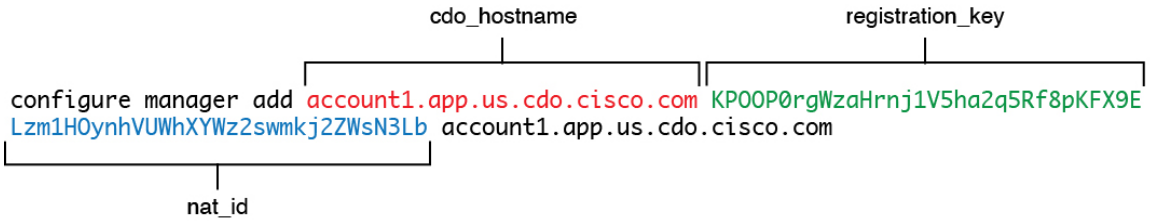
a) For **Do you know the Management Center/SCC Hostname or IP address**, click **Yes**.

Security Cloud Control generates the **configure manager add** command. See Onboard the firewall with manual provisioning, on page 16 to generate the command.

configure manager add *_hostname registration_key nat_id display_name*

Example:

Figure 27: configure manager add command components



b) Copy the *cdo_hostname*, *registration_key*, and *nat_id* parts of the command into the following fields:

- **Management Center/SCC Hostname/IP Address**
- **Management Center/SCC Registration Key**
- **NAT ID**

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 Firewall Management Center.

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

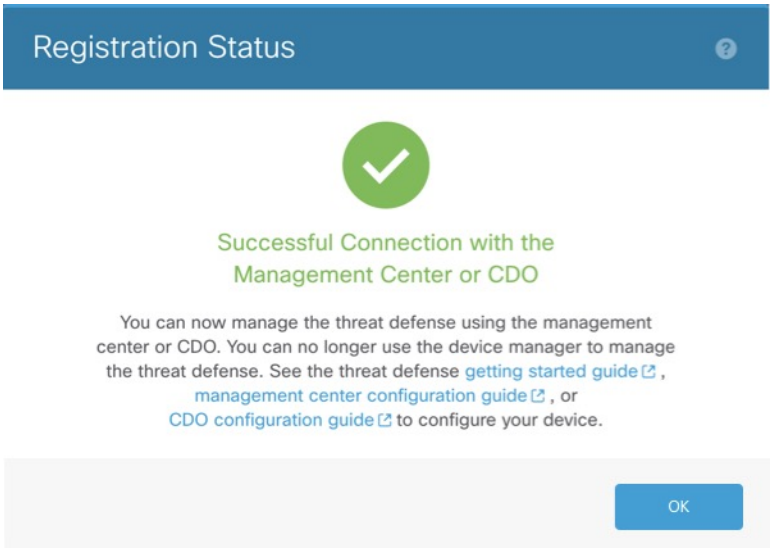
Step 7 (Optional) Click **Add a Dynamic DNS (DDNS) method**.

DDNS ensures the Firewall Management Center can reach the Firewall Threat Defense at its FQDN if the Firewall Threat Defense's IP address changes.

Step 8 Click **Connect**.

The **Registration Status** dialog box shows the current status of the Security Cloud Control registration.

Figure 28: Successful Connection



Step 9 After the **Saving Management Center/SCC Registration Settings** step on the status screen, go to the Security Cloud Control and add the firewall. See Onboard the firewall with manual provisioning, on page 16.

Initial configuration: CLI

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

Procedure

Step 1 Connect to the console port and access the Firewall Threat Defense CLI. See Access the Firewall Threat Defense CLI, on page 4.

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 Firewall 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

After you press **Enter**, you are 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 Firewall 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 Security Cloud Control that will manage this Firewall Threat Defense using the **configure manager add** command that Security Cloud Control generated. See Onboard the firewall with manual provisioning, on page 16 to generate the command.

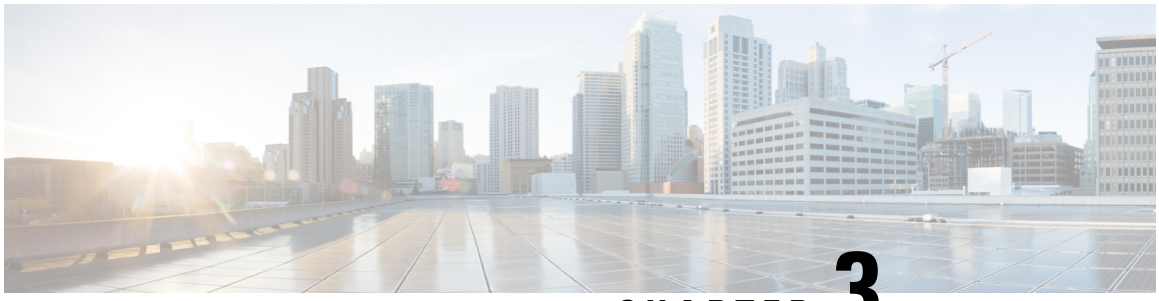
Example:

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

Step 5 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.



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.

Navigate to the Cloud-delivered Firewall Management Center

The Cloud-Delivered Firewall Management Center launches in its own tab from Security Cloud Control.

Procedure

Step 1 Choose **Administration** > **Integrations** > **Firewall Management Center**.

Step 2 Select **Cloud-Delivered FMC** and click the links in the **Actions**, **Management**, or **Settings** pane to open the Cloud-Delivered Firewall Management Center in a new tab.

Tip

To navigate back to Security Cloud Control from the Cloud-Delivered Firewall Management Center, click **Home**.

Configure interfaces

When you use zero-touch provisioning or the Firewall 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 Firewall Device Manager before registering with the Firewall 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.

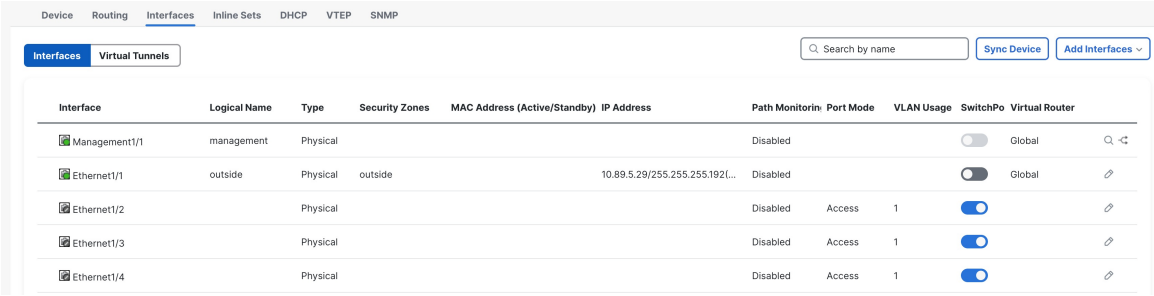
The following example configures a routed-mode inside interface (VLAN1) with a static address and a routed-mode outside interface using DHCP (Ethernet1/1). It also adds a DMZ interface for an internal web server.

Procedure

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

Step 2 Click **Interfaces**.

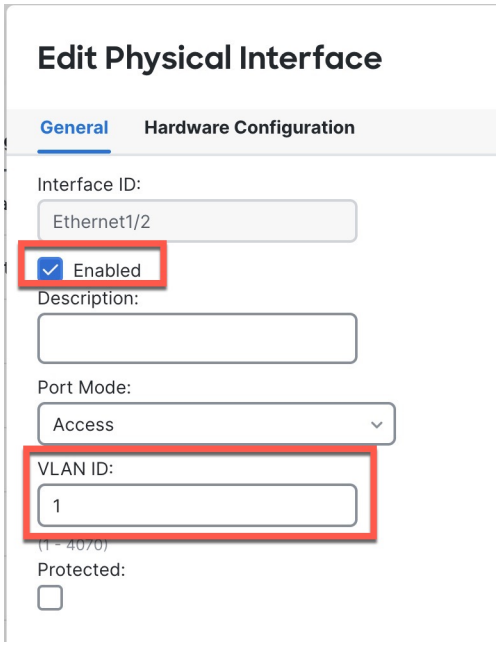
Figure 29: Interfaces



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

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

Figure 30: Enable Switch Port

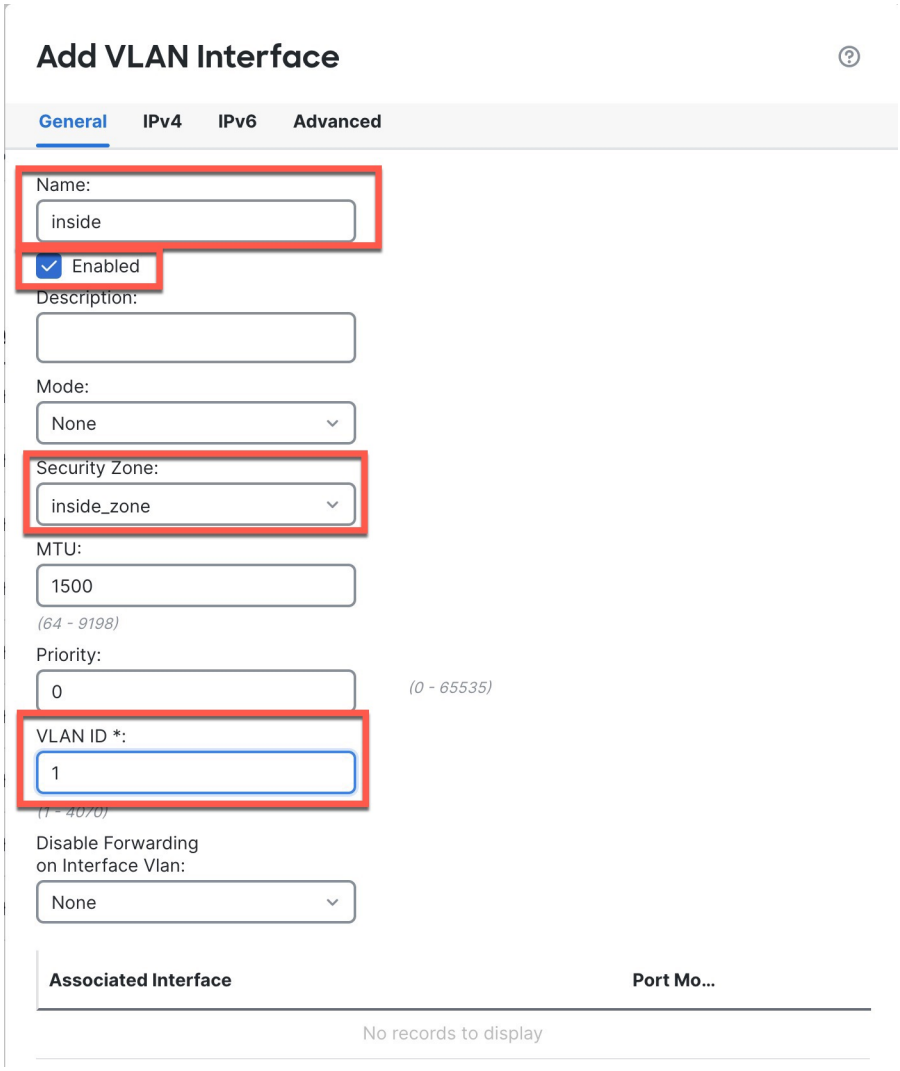


b) Enable the interface by checking the **Enabled** check box.
c) (Optional) Change the VLAN ID; the default is 1. You will next add a VLAN interface to match this ID.
d) Click **OK**.

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 31: 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.

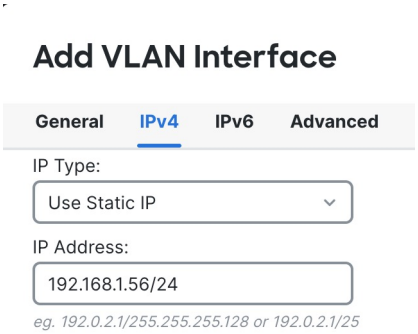
You cannot change the VLAN ID after you save the interface; the VLAN ID is both the VLAN tag used, and the interface ID in your configuration.

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 32: Set Inside IP Address



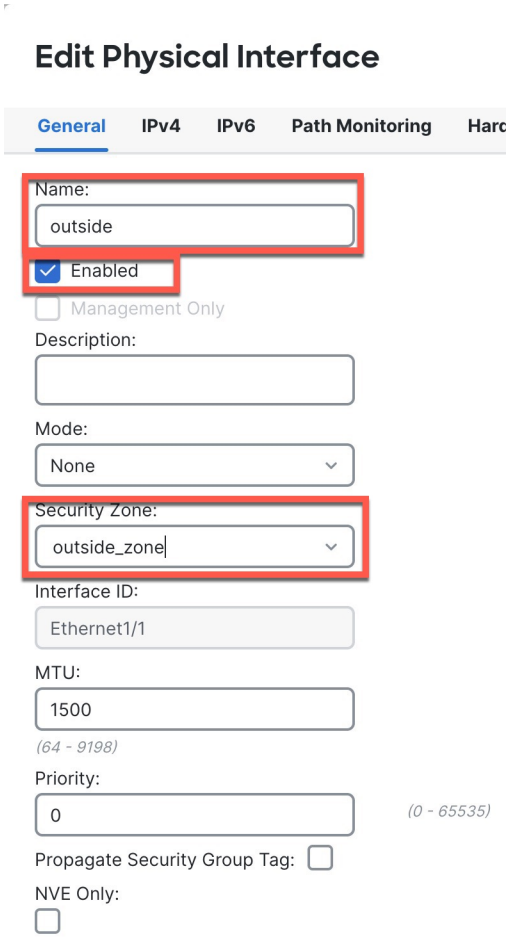
- **IPv6**—Check the **Autoconfiguration** check box for stateless autoconfiguration.

h) Click **OK**.

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

The **General** page appears.

Figure 33: 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 Firewall 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

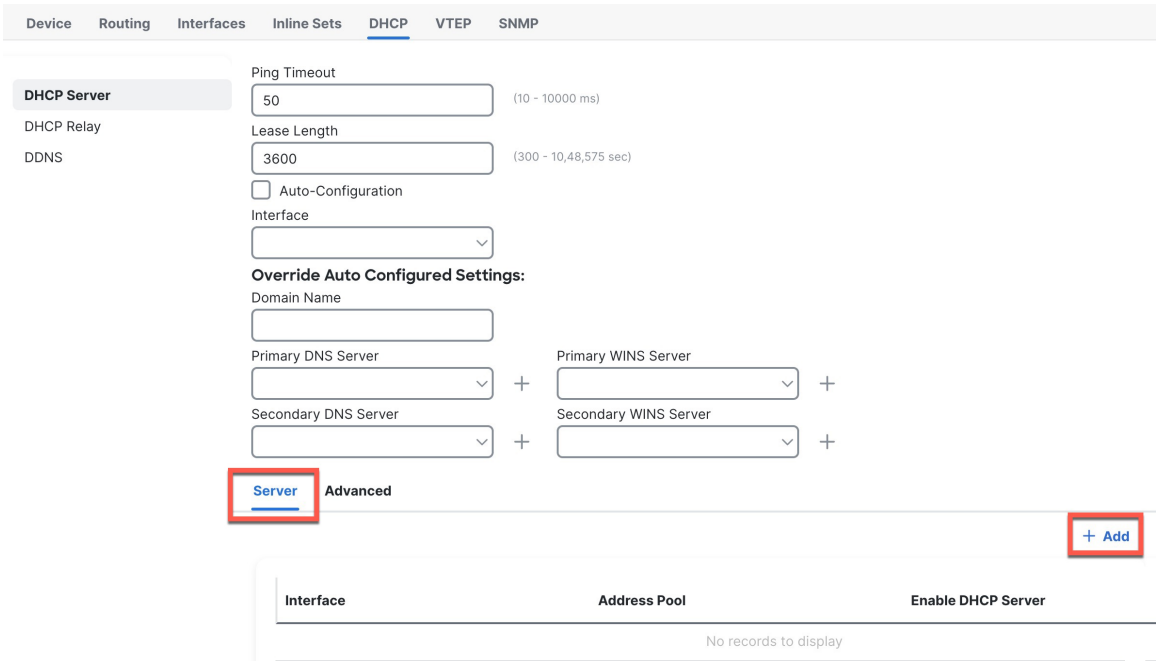
Enable the DHCP server if you want clients to use DHCP to obtain IP addresses from the firewall.

Procedure

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

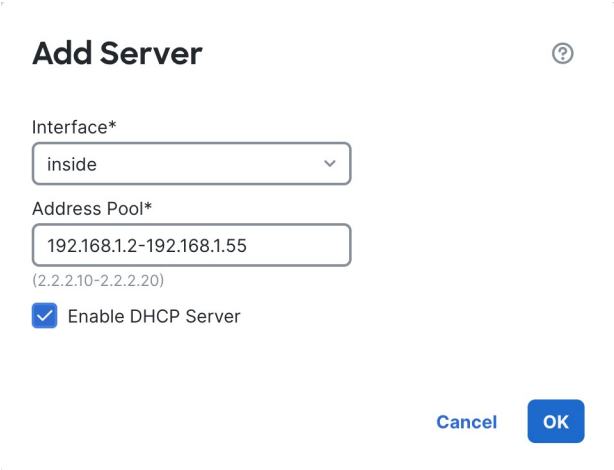
Step 2 Choose **DHCP** > **DHCP Server**.

Figure 34: DHCP Server



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

Figure 35: 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

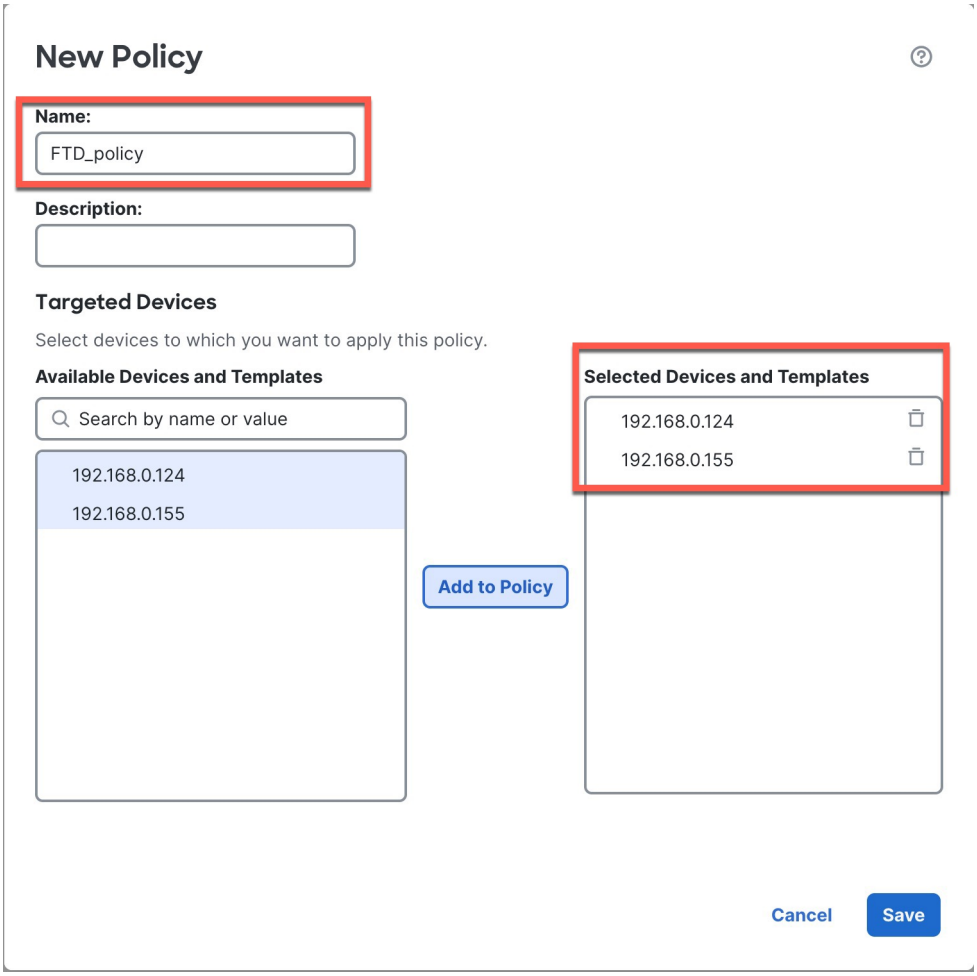
This procedure creates a NAT rule for internal clients to convert the internal addresses to a port on the outside interface IP address. This type of NAT rule is called *interface Port Address Translation (PAT)*.

Procedure

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

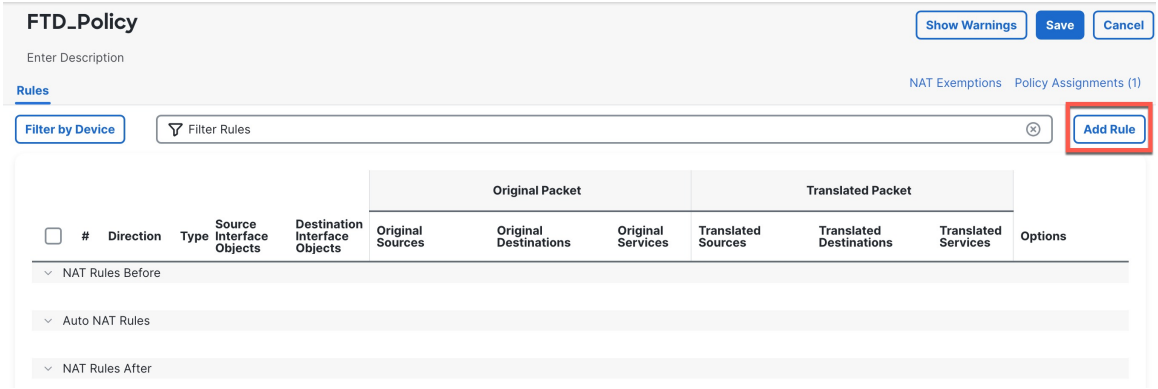
Step 2 Name the policy, select the devices that you want to use the policy, and click **Save**.

Figure 36: New Policy



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

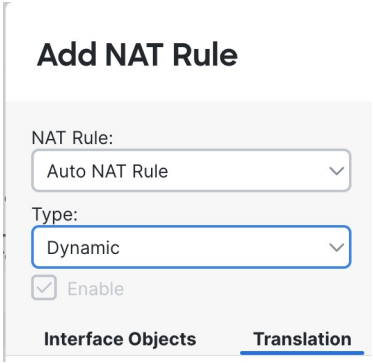
Figure 37: NAT Policy



Step 3 Click **Add Rule**.

Step 4 Configure the basic rule options:

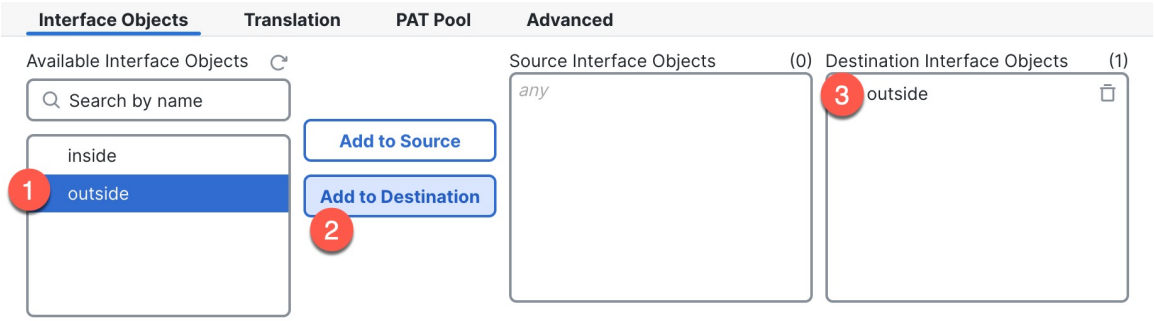
Figure 38: Basic Rule Options



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

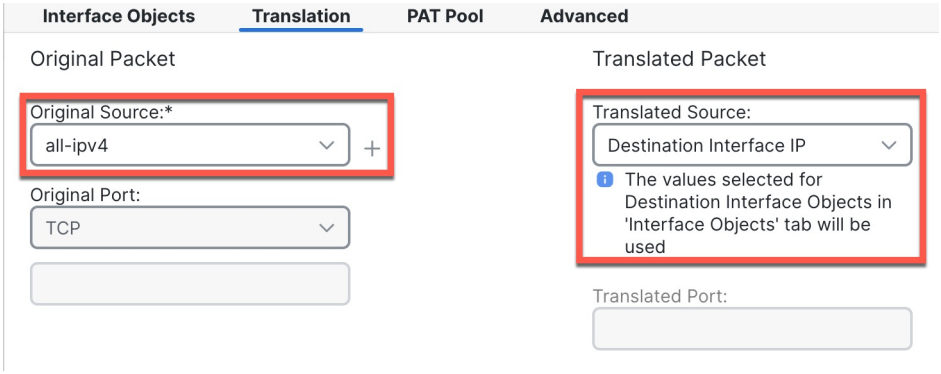
Step 5 On the **Interface Objects** page, add the outside zone from the **Available Interface Objects** area to the **Destination Interface Objects** area.

Figure 39: Interface Objects



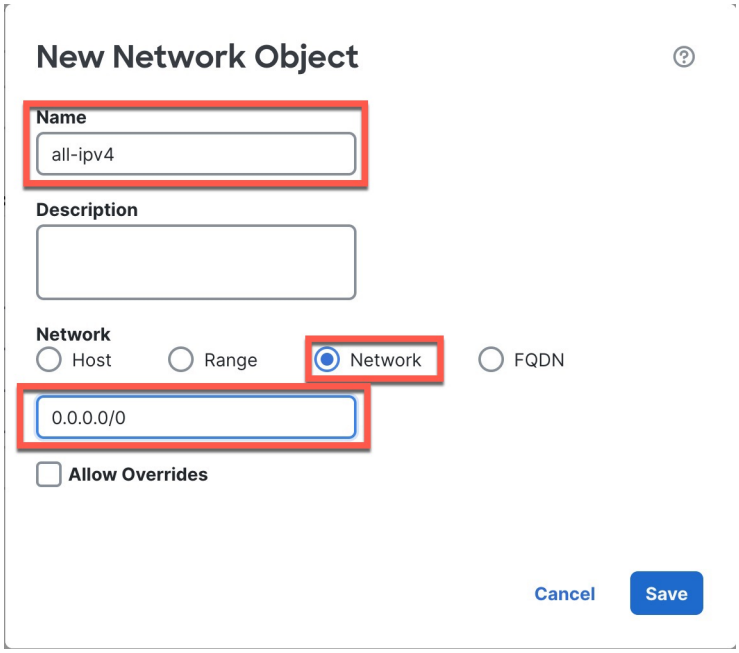
Step 6 On the **Translation** page, configure the following options:

Figure 40: Translation



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

Figure 41: 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 firewall, then you need to add rules to the policy to allow traffic through the firewall. The access control policy can include multiple rules that are evaluated in order.

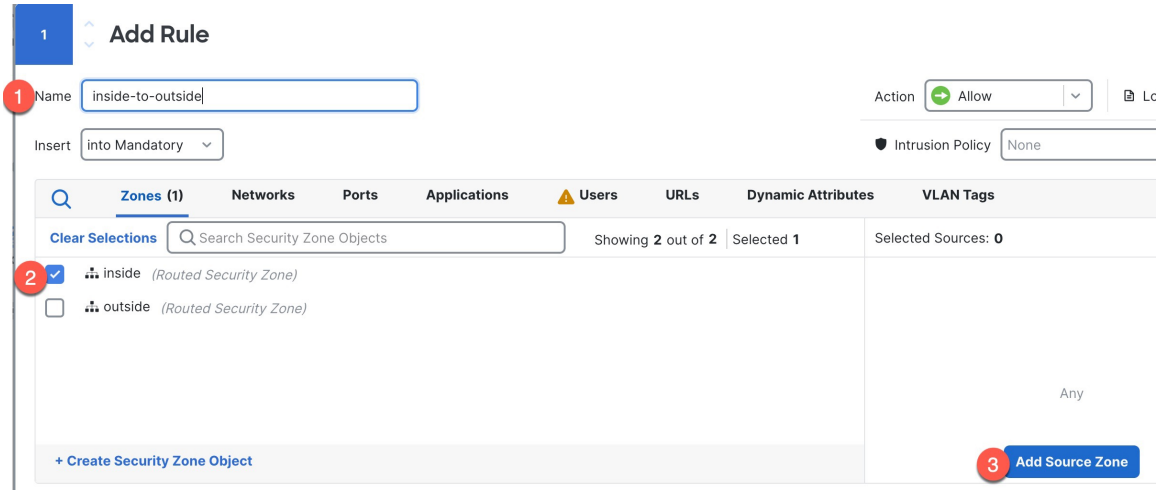
This procedure creates an access control rule to allow all traffic from the inside zone to the outside zone.

Procedure

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

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

Figure 42: Source Zone

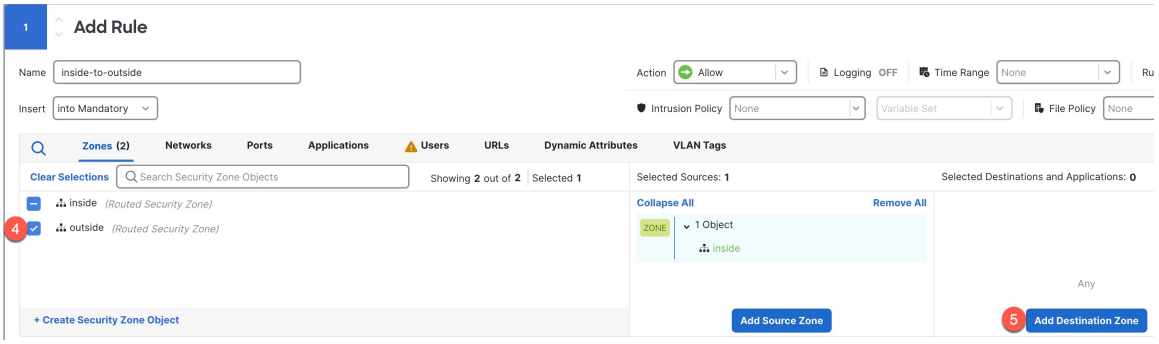


1. Name this rule, for example, **inside-to-outside**.

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

3. Click **Add Source Zone**.

Figure 43: 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 44: 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.

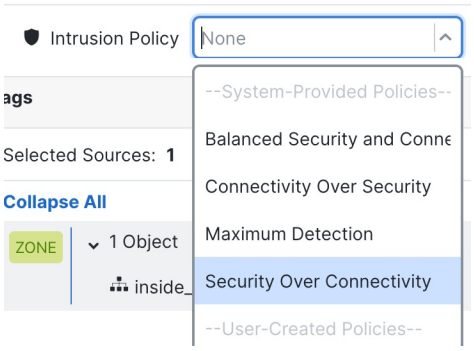
- **Identity**—Identity is not applied by default. You can require a user to authenticate before allowing traffic to be processed by the access control policy.

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 Firewall 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 45: System-Provided Intrusion Policies



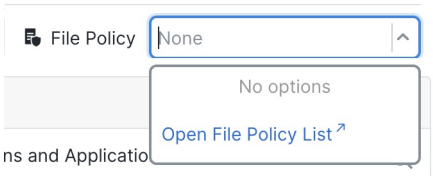
b) Choose one of the system-provided policies from the list.

We recommend **Balanced Security and Connections** for most use cases.

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 46: File Policy



For a new policy, the **Policies** > **Security 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 so you can manage the firewall remotely.

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

Procedure

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

Step 2 Select **SSH Access**.

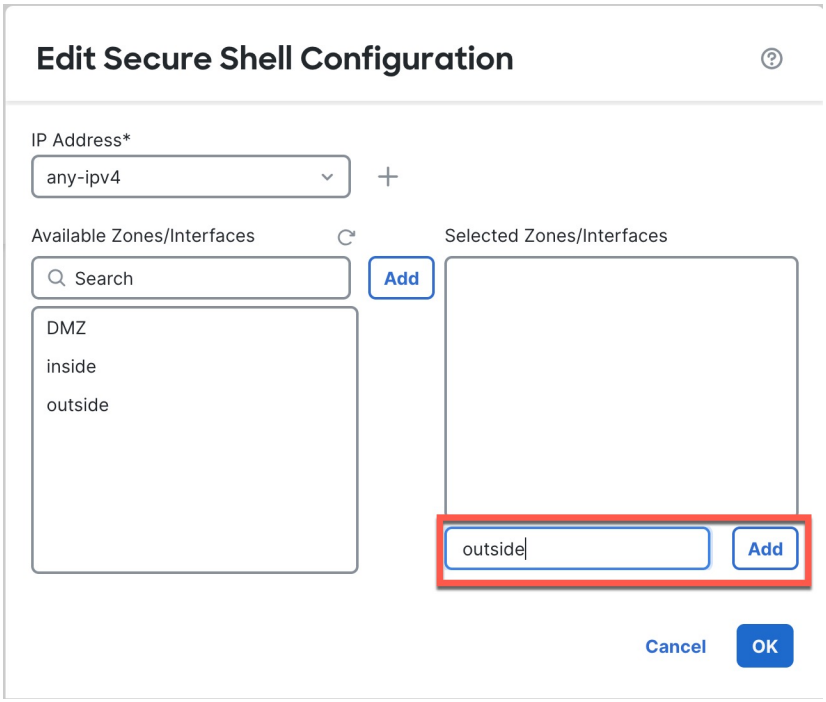
Step 3 Identify the outside interface and IP addresses that allow SSH connections.

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 47: Enable SSH on the Outside Interface



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.

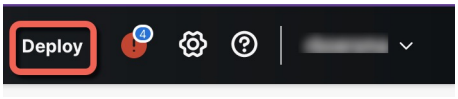
Deploy the configuration

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

Procedure

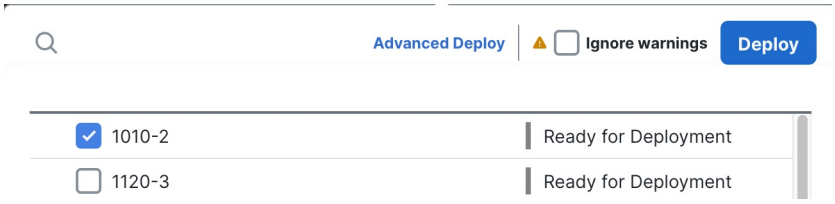
Step 1 Click **Deploy** in the upper right.

Figure 48: Deploy



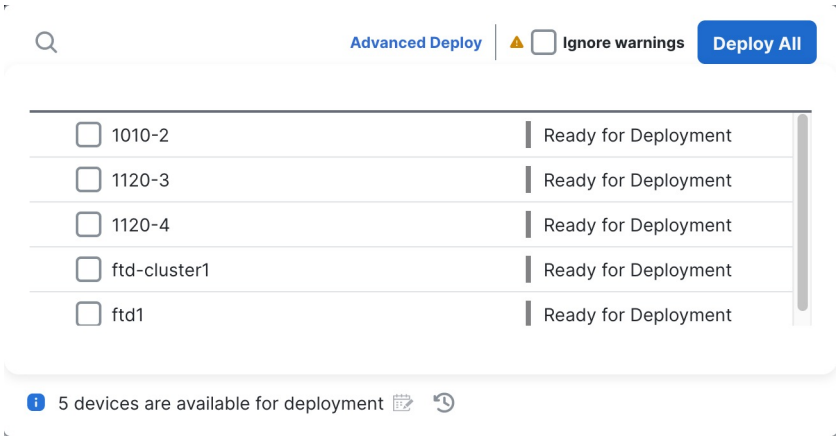
Step 2 For a quick deployment, check specific devices and then click **Deploy**.

Figure 49: Deploy Selected



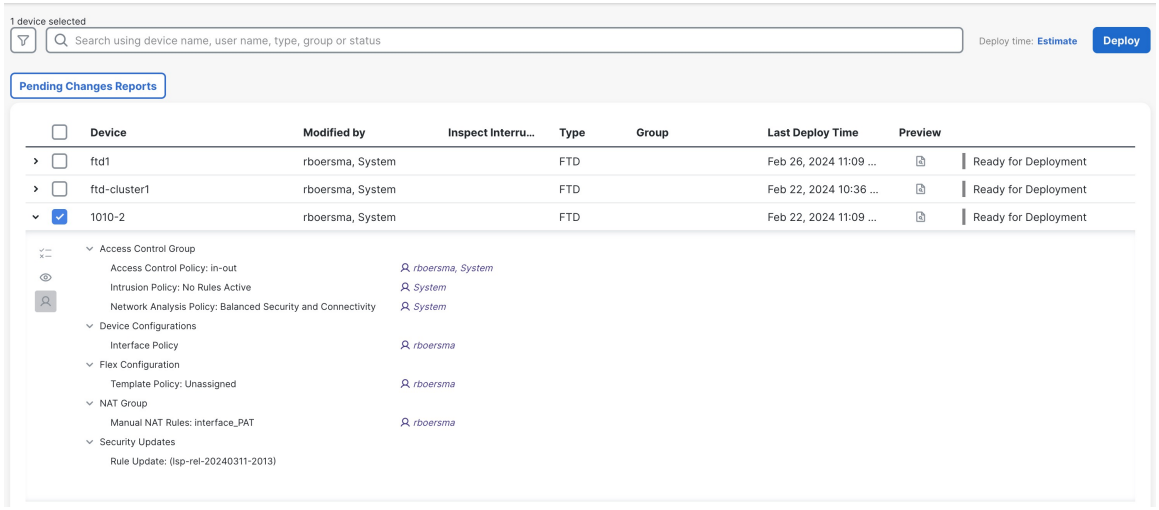
Or click **Deploy All** to deploy to all devices.

Figure 50: Deploy All



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

Figure 51: 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 52: Deployment Status