



Secure Firewall 4200 Threat Defense Getting Started: Cloud-Delivered Firewall Management Center

First Published: 2024-10-15

Last Modified: 2026-03-18

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 Secure Firewall 4200 is a high-end firewall designed to meet the security requirements of large enterprises, datacenters, and service providers. It provides superior threat defense within a compact 1 RU form factor. Key features and benefits include:

- Cryptographic acceleration architecture preserves performance with SSL and VPN decryption
- Space saving 1 RU form factor
- 16-node cluster
- 2 interface module bays for additional interface support, up to 400G interfaces and fail-to-wire network modules
- 2 SSDs for event storage and malware analysis
- Resilience with dual management interfaces
- SD-WAN capable with simplified site-to-site communication using on-demand tunnels and dynamic application path selection across multiple WAN interfaces
- AI/ML-powered to detect anomalies, remediate threats, and optimize the policy for peak performance with Cisco's native AI/ML solution.

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



Note

Outside management is not supported with clustering or multi-instance mode. In this case, use the Management interface for Security Cloud Control access.

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, on page 2](#)
- [Which application is installed: Firewall Threat Defense or ASA?, on page 3](#)
- [Access the Firewall Threat Defense CLI, on page 4](#)
- [Check the version and reimage, on page 5](#)
- [Obtain licenses, on page 6](#)
- [\(If Needed\) Power off the firewall, on page 8](#)

Power on the firewall

System power is controlled by a rocker power switch located on the rear of the firewall. The rocker power switch provides a soft notification that supports graceful shutdown of the system to reduce the risk of system software and data corruption.



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

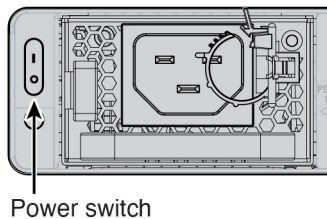
Before you begin

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

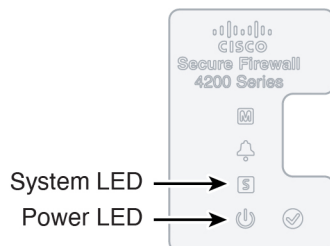
- Step 1** Attach the power cord to the firewall, and connect it to an electrical outlet.
- Step 2** Turn the power on using the rocker power switch located on the rear of the chassis, adjacent to the power cord.

Figure 1: Power switch



- Step 3** Check the LEDs for the current status.

Figure 2: 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
<i>Fast flashing amber (error condition)</i>	Failed to boot up	01:00
Solid green	Application loaded	15:00 - 30:00
<i>Solid amber (error condition)</i>	Application failed to load	15:00 - 30:00

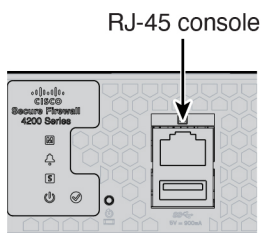
Which application is installed: Firewall Threat Defense or ASA?

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.

Figure 3: 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](#).

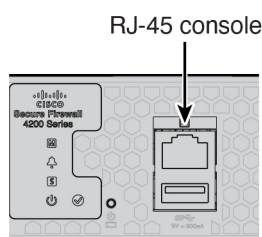
Access the Firewall Threat Defense CLI

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

Procedure

- Step 1** Connect to the console port.

Figure 4: 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.

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.

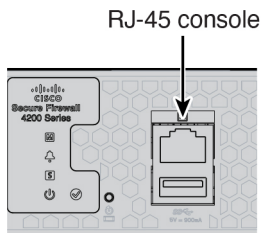
What version should I run?

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.

Figure 5: 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.
- 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](#).

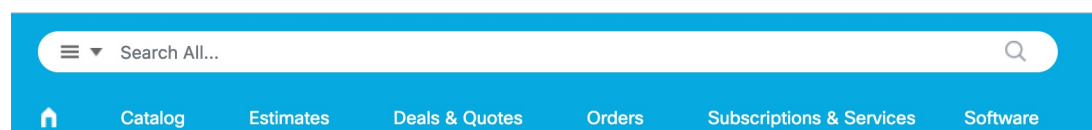
If you have not already done so, register Security Cloud Control with the Smart Software Manager. Registering requires you to generate a registration token in the Smart Software Manager. See the [Security Cloud Control documentation](#) for detailed instructions.

The Firewall Threat Defense has the following licenses:

- Essentials—Required
- IPS
- Malware Defense
- URL Filtering
- Cisco Secure Client
- Carrier—Diameter, GTP/GPRS, M3UA, SCTP

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

Figure 6: 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.

- Essentials:

- *Included automatically*

- IPS, Malware Defense, and URL combination:

- L-FPR4215T-TMC=

- L-FPR4225T-TMC=

- L-FPR4245T-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-FPR4215T-TMC-1Y

- L-FPR4215T-TMC-3Y

- L-FPR4215T-TMC-5Y

- L-FPR4225T-TMC-1Y

- L-FPR4225T-TMC-3Y

- L-FPR4225T-TMC-5Y

- L-FPR4245T-TMC-1Y

- L-FPR4245T-TMC-3Y

- L-FPR4245T-TMC-5Y

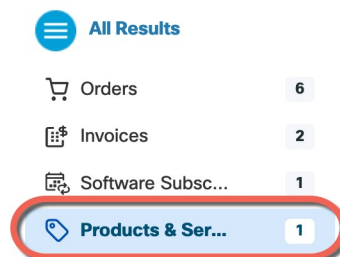
- Carrier:

- L-FPR4200-FTD-CAR=

- Cisco Secure Client—See the [Cisco Secure Client Ordering Guide](#).

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

Figure 7: Results



(If Needed) Power off the firewall

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

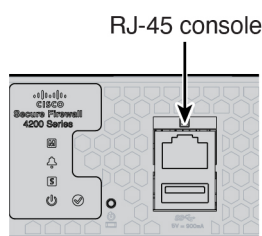
Power off the firewall at the CLI

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.

Figure 8: 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 turn off the power switch and 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 turn off the power switch and unplug the power to physically remove power from the chassis if necessary.
-





## CHAPTER 2

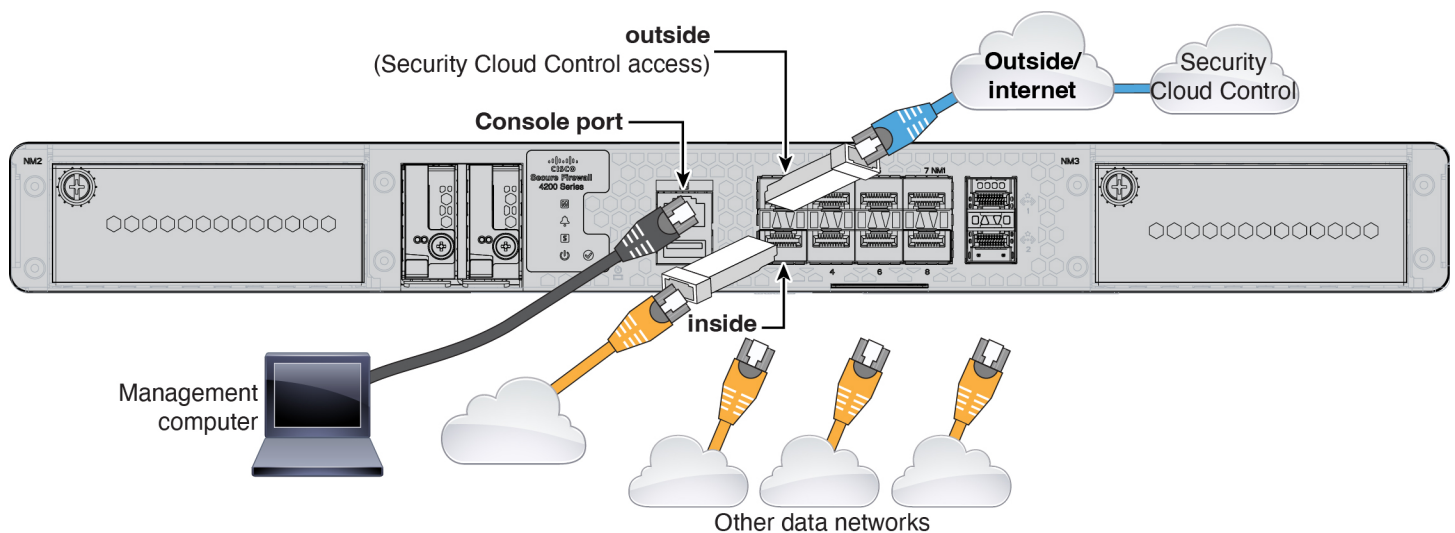
# Cable and Onboard the Firewall

Cable and onboard the firewall to Security Cloud Control.

- [Cable the firewall, on page 11](#)
- [Onboard the firewall, on page 12](#)
- [Perform initial configuration, on page 14](#)

## Cable the firewall

- Obtain a console cable—The firewall does not ship with a console cable by default, so you will need to buy a third-party USB-to-RJ-45 serial cable, for example.
- Install SFPs into the data interface ports—The fixed ports are 1/10/25-Gbps SFP28 ports that require SFP/SFP+/SFP28 modules.
- See the [hardware installation guide](#) for more information.



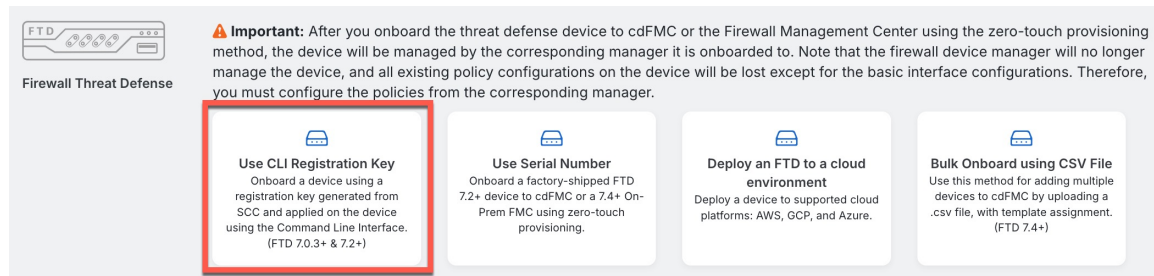
# Onboard the firewall

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 9: Use CLI Registration Key*



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

*Figure 10: Device Name*

1 Device Name

Device Name

ftd1

Next

- 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 11: Access Control Policy*

2 Policy Assignment

Access Control Policy

Default Access Control Policy ▼

Next

- 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 12: Subscription License

3 Subscription License

Please indicate if this FTD is physical or virtual:

☒ Physical FTD Device

☐ Virtual FTD Device

| License Type                                                 | Includes                       |
|--------------------------------------------------------------|--------------------------------|
| <input checked="" type="checkbox"/> Essentials               | Base Firewall Capabilities     |
| <input checked="" type="checkbox"/> Carrier (7.3+ FTDs only) | GTP/GPRS, Diameter, SCTP, M3UA |
| <input checked="" type="checkbox"/> IPS                      | Intrusion Policy               |
| <input checked="" type="checkbox"/> Malware Defense          | File Policy                    |
| <input checked="" type="checkbox"/> URL                      | URL Reputation                 |
| <input checked="" type="checkbox"/> RA VPN                   | RA VPN                         |

Next

**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 initial configuration of the Firewall Threat Defense.

Figure 13: CLI Registration Key

4 CLI Registration Key

- 1 Ensure the device's initial configuration is complete before trying to apply the registration key. [Learn more](#)
- 2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cisco-security-docs.app.us.cdo.cisco.com
BanyI2oaT0ew1JTpc0P2w3xEBnVVkfZv x7R7dwcM43JCMzwGY3ZzCfoFmZhW97my cisco-security-
docs.app.us.cdo.cisco.com
```

Next

**configure manager add** Security Cloud Control\_hostname registration\_key nat\_id display\_name

Copy this command at the Firewall Threat Defense CLI after you complete the startup script. See [Perform initial configuration, on page 14](#).

**Example:**

Sample command for CLI setup:

```
configure manager add account1.app.us.scc.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsn3Lb account1.app.us.scc.cisco.com
```

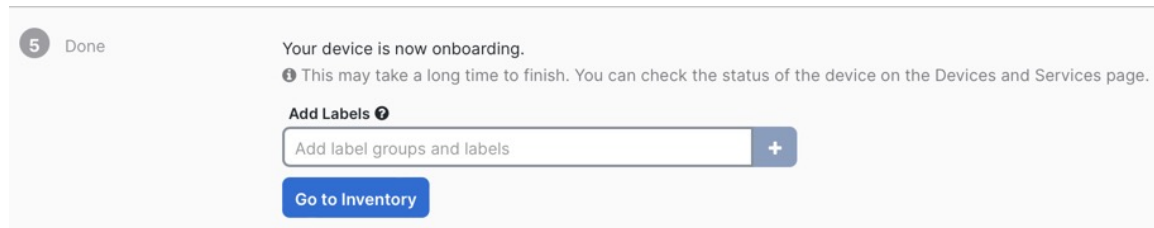
**Step 9**

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 14: Done



## Perform initial configuration

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'
```

```
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, on page 12](#) 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 customize your security policy to include more advanced inspections.

- [Navigate to the Cloud-delivered Firewall Management Center, on page 19](#)
- [Configure interfaces, on page 20](#)
- [Configure the DHCP server, on page 24](#)
- [Configure NAT, on page 25](#)
- [Configure an access control rule, on page 28](#)
- [Enable SSH on the outside interface, on page 31](#)
- [Deploy the configuration, on page 32](#)

## 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

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

### Procedure

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

**Step 2** Click **Interfaces**.

**Figure 15: Interfaces**

| Device   Routing <u>Interfaces</u> Inline Sets   DHCP   VTEP |              |          |                |                              |                  |                 |                  |       |
|--------------------------------------------------------------|--------------|----------|----------------|------------------------------|------------------|-----------------|------------------|-------|
|                                                              |              |          |                |                              | Q Search by name | Sync Device     | Add Interfaces ▼ |       |
| Interface                                                    | Logical Name | Type     | Security Zones | MAC Address (Active/Standby) | IP Address       | Path Monitoring | Virtual Router   |       |
| ● Management0/0                                              | management   | Physical |                |                              |                  | Disabled        | Global           | Q < > |
| 🔌 GigabitEthernet0/0                                         |              | Physical |                |                              |                  | Disabled        |                  | ✎     |
| 🔌 GigabitEthernet0/1                                         |              | Physical |                |                              |                  | Disabled        |                  | ✎     |
| 🔌 GigabitEthernet0/2                                         |              | Physical |                |                              |                  | Disabled        |                  | ✎     |
| 🔌 GigabitEthernet0/3                                         |              | Physical |                |                              |                  | Disabled        |                  | ✎     |
| 🔌 GigabitEthernet0/4                                         |              | Physical |                |                              |                  | Disabled        |                  | ✎     |
| 🔌 GigabitEthernet0/5                                         |              | Physical |                |                              |                  | Disabled        |                  | ✎     |
| 🔌 GigabitEthernet0/6                                         |              | Physical |                |                              |                  | Disabled        |                  | ✎     |
| 🔌 GigabitEthernet0/7                                         |              | Physical |                |                              |                  | Disabled        |                  | ✎     |

**Step 3** To create breakout ports from a 40-Gb or larger interface, click the **Break** icon for the interface.

If you already used the full interface in your configuration, you will have to remove the configuration before you can proceed with the breakout.

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

Figure 16: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

Name:  
inside

☒ Enabled  
☐ Management Only

Description:

Mode:  
None

Security Zone:  
inside\_zone

Interface ID:  
GigabitEthernet0/1

MTU:  
1500  
(64 - 9000)

Priority:  
0 (0 - 65535)

Propagate Security Group Tag: ☐

NVE Only:  
☐

- 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. For example, configure your access control policy to enable traffic to go from the inside zone to the outside zone, but not from outside to inside.  
If the inside interface was preconfigured, the rest of these fields are optional.
- Enter a **Name** up to 48 characters in length.  
For example, name the interface **inside**.
- Check the **Enabled** check box.
- Leave the **Mode** set to **None**.
- Click the **IPv4** and/or **IPv6** tab.
  - IPv4**—Choose **Use Static IP** from the drop-down list, and enter an IP address and subnet mask in slash notation.  
For example, enter **192.168.1.1/24**

**Figure 17: IPv4 Tab**

The screenshot shows the 'Edit Physical Interface' window with the 'IPv4' tab selected. The 'IP Type' dropdown is set to 'Use Static IP'. The 'IP Address' field contains '192.168.1.1/24'. Below the field, a hint text reads: 'eg. 192.0.2.1/255.255.255.128 or 192.0.2.1/25'.

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

**Figure 18: IPv6 Tab**

The screenshot shows the 'Edit Physical Interface' window with the 'IPv6' tab selected. The 'Basic' sub-tab is active. The 'Enable IPV6' checkbox is unchecked. The 'Enforce EUI 64' checkbox is unchecked. The 'Link-Local address' field is empty. The 'Autoconfiguration' checkbox is checked. The 'Obtain Default Route' checkbox is unchecked.

f) Click **OK**.

**Step 5** Click **Edit** (✎) for the interface that you want to use for outside.



Figure 19: General Tab

Edit Physical Interface

| General                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | IPv4 | IPv6 | Path Monitoring | Hardware |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------|------|-----------------|----------|
| <p>Name:<br/> <input type="text" value="outside"/></p> <p><input checked="" type="checkbox"/> Enabled<br/> <input type="checkbox"/> Management Only</p> <p>Description:<br/> <input type="text"/></p> <p>Mode:<br/> <input type="text" value="None"/></p> <p>Security Zone:<br/> <input type="text" value="outside_zone"/></p> <p>Interface ID:<br/> <input type="text" value="GigabitEthernet0/0"/></p> <p>MTU:<br/> <input type="text" value="1500"/><br/> <small>(64 - 9000)</small></p> <p>Priority:<br/> <input type="text" value="0"/><br/> <small>(0 - 65535)</small></p> <p>Propagate Security Group Tag: <input type="checkbox"/></p> <p>NVE Only:<br/> <input type="checkbox"/></p> |      |      |                 |          |

- 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) Click **Edit** (🔗) for the interface you want to use.  
 b) 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**.

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

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

- d) Check the **Enabled** check box.  
 e) Leave the **Mode** set to **None**.  
 f) Click the **IPv4** and/or **IPv6** tab and configure the IP address as desired.  
 g) 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**.

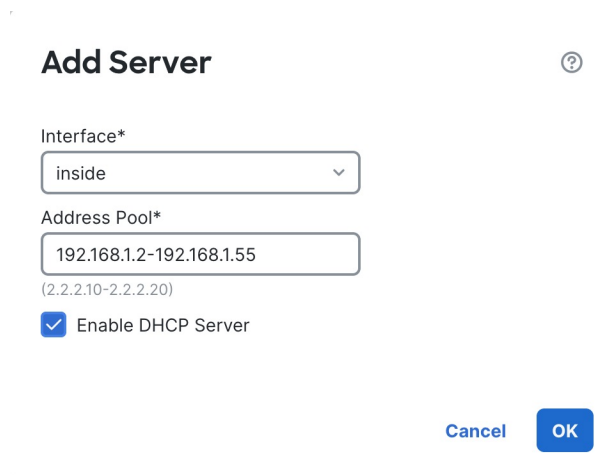
**Figure 20: DHCP Server**

The screenshot displays the DHCP Server configuration page. The top navigation bar includes tabs for Device, Routing, Interfaces, Inline Sets, DHCP (selected), VTEP, and SNMP. On the left, a sidebar lists DHCP Server, DHCP Relay, and DDNS. The main configuration area includes fields for Ping Timeout (50 ms), Lease Length (3600 sec), and an unchecked Auto-Configuration checkbox. Below these are dropdown menus for Interface, Domain Name, Primary DNS Server, Secondary DNS Server, Primary WINS Server, and Secondary WINS Server. The 'Override Auto Configured Settings' section is expanded, showing the 'Server' tab and an 'Advanced' section. A table at the bottom shows the configuration for the selected interface, with columns for Interface, Address Pool, and Enable DHCP Server. The 'Add' button is highlighted.

| Interface             | Address Pool | Enable DHCP Server |
|-----------------------|--------------|--------------------|
| No records to display |              |                    |

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

Figure 21: Add Server



**Add Server** ⓘ

Interface\*  
inside

Address Pool\*  
192.168.1.2-192.168.1.55  
(2.2.2.10-2.2.2.20)

☒ Enable DHCP Server

Cancel OK

- **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 22: New Policy

**New Policy**

**Name:**  
FTD\_policy

**Description:**

**Targeted Devices**  
Select devices to which you want to apply this policy.

**Available Devices and Templates**  
Search by name or value

192.168.0.124  
192.168.0.155

**Selected Devices and Templates**

192.168.0.124  
192.168.0.155

Add to Policy

Cancel Save

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

Figure 23: NAT Policy

**FTD\_Policy** Show Warnings Save Cancel

Enter Description

Rules NAT Exemptions Policy Assignments (1)

Filter by Device Filter Rules Add Rule

|                  | # | Direction | Type | Source Interface Objects | Destination Interface Objects | Original Packet  |                       |                   | Translated Packet  |                         |                     | Options |
|------------------|---|-----------|------|--------------------------|-------------------------------|------------------|-----------------------|-------------------|--------------------|-------------------------|---------------------|---------|
|                  |   |           |      |                          |                               | Original Sources | Original Destinations | Original Services | Translated Sources | Translated Destinations | Translated Services |         |
| NAT Rules Before |   |           |      |                          |                               |                  |                       |                   |                    |                         |                     |         |
| Auto NAT Rules   |   |           |      |                          |                               |                  |                       |                   |                    |                         |                     |         |
| NAT Rules After  |   |           |      |                          |                               |                  |                       |                   |                    |                         |                     |         |

**Step 3** Click **Add Rule**.

**Step 4** Configure the basic rule options:

Figure 24: Basic Rule Options

**Add NAT Rule**

NAT Rule:  
Auto NAT Rule

Type:  
Dynamic

☒ Enable

Interface Objects    Translation

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

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

Figure 25: Interface Objects

Interface Objects    Translation    PAT Pool    Advanced

Available Interface Objects

Search by name

inside

outside

Add to Source

Add to Destination

Source Interface Objects (0)

any

Destination Interface Objects (1)

outside

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

Figure 26: Translation

Interface Objects    Translation    PAT Pool    Advanced

Original Packet

Original Source:\*

all-ipv4

Original Port:

TCP

Translated Packet

Translated Source:

Destination Interface IP

The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

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

Figure 27: New Network Object

**New Network Object**

Name  
all-ipv4

Description

Network  
☐ Host
 ☐ Range
 ☒ Network
 ☐ FQDN

0.0.0.0/0

☐ Allow Overrides

Cancel Save

**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 28: Source Zone**

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is 'inside-to-outside'. The 'Zones' tab is selected, showing 'inside' and 'outside' zones. The 'inside' zone is selected. The 'Add Source Zone' button is highlighted with a red circle and the number 3.

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

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

3. Click **Add Source Zone**.

**Figure 29: Destination Zone**

The screenshot shows the 'Add Rule' configuration page. The 'Name' field is 'inside-to-outside'. The 'Zones' tab is selected, showing 'inside' and 'outside' zones. The 'outside' zone is selected. The 'Add Destination Zone' button is highlighted with a red circle and the number 5.

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 30: 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.

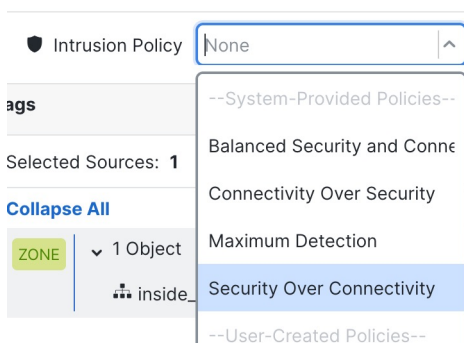
- **Identity**—Identity is not applied by default. You can require a user to authenticate before allowing traffic to be processed by the access control policy.

#### 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.

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

**Figure 31: System-Provided Intrusion Policies**



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

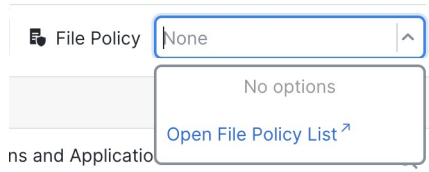
We recommend **Balanced Security and Connections** for most use cases.



**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 32: 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 33: Enable SSH on the Outside Interface

**Edit Secure Shell Configuration**

IP Address\*  
any-ipv4

Available Zones/Interfaces  
Search  
DMZ  
inside  
outside

Selected Zones/Interfaces  
outside Add

Cancel OK

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

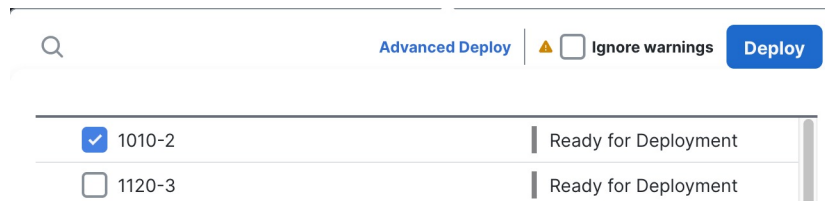
**Step 1** Click **Deploy** in the upper right.

Figure 34: Deploy



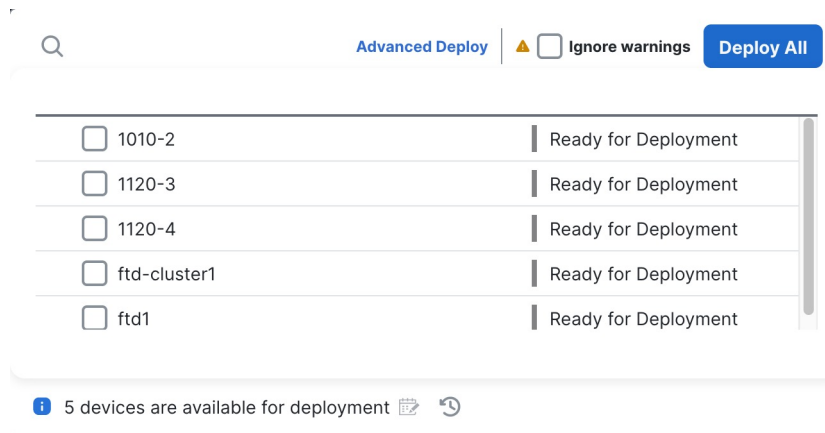
**Step 2** For a quick deployment, check specific devices and then click **Deploy**.

Figure 35: Deploy Selected



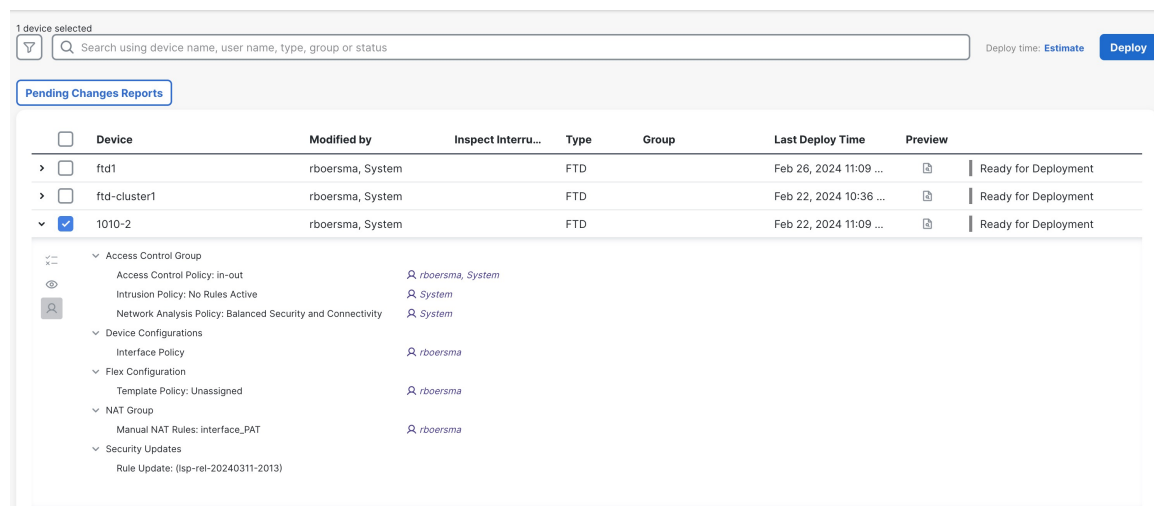
Or click **Deploy All** to deploy to all devices.

Figure 36: Deploy All



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

Figure 37: 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 38: Deployment Status

