



Secure Firewall 4200 Threat Defense Getting Started: Firewall Management Center on a Local Management Network

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.

Manage the firewall using the Secure Firewall Management Center on a dedicated management network.

- [Power on the firewall, on page 1](#)
- [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

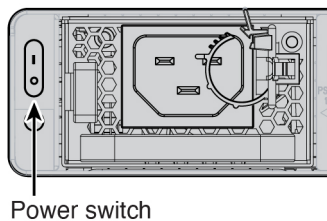
It's important that you provide reliable power for your firewall (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow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

Procedure

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

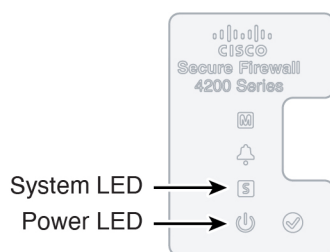
Step 2 Turn the power on using the rocker power switch located on the rear of the chassis, adjacent to the power cord.

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

LED Behavior	Description	Time After Device Powered On (minutes:seconds)
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

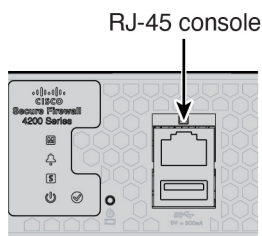
Which application is installed: Firewall Threat Defense or ASA?

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](#).

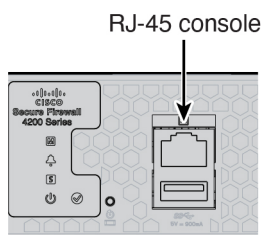
Access the Firewall Threat Defense CLI

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.

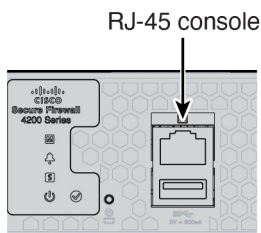
What version should I run?

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.

Obtain licenses

When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. If you don't have an account on the [Smart Software Manager](#), click the link to [set up a new account](#).

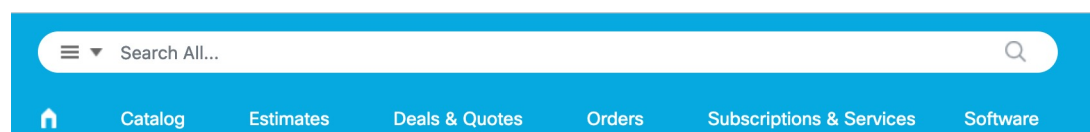
If you have not already done so, register the Firewall Management Center with the Smart Software Manager. Registering requires you to generate a registration token in the Smart Software Manager. See the [Cisco Secure Firewall Management Center Administration Guide](#) for detailed instructions.

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

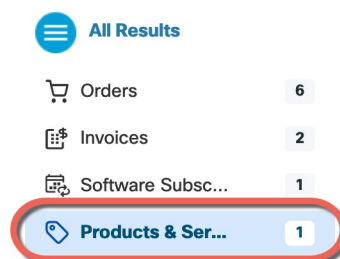
- Carrier:

- 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.

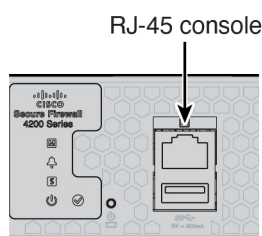
Power off the firewall at the CLI

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.
- Choose **Devices > Device Management**.
 - Next to the device that you want to restart, click **Edit** (✎).
 - Click the **Device** tab.
 - Click **Shut Down Device** (🔌) in the **System** section.
 - 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 Register the Firewall

---

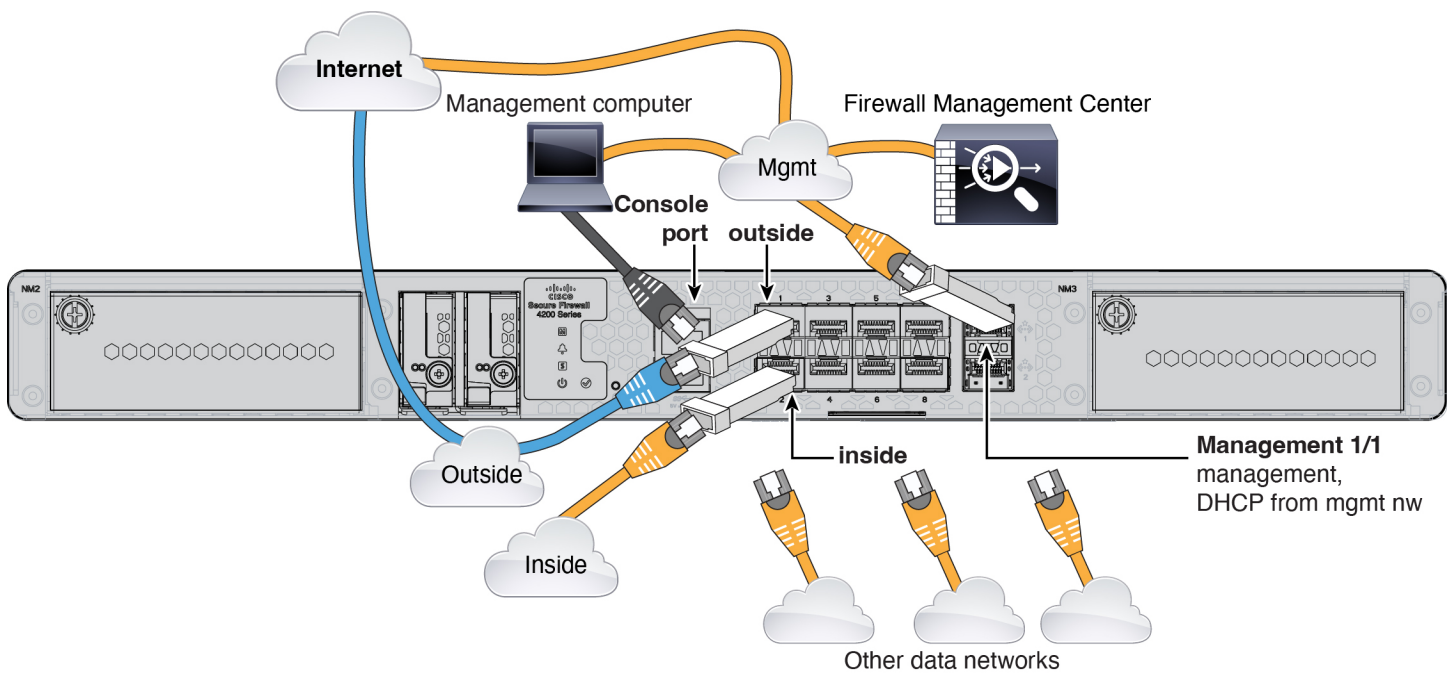
Cable the firewall and then register the firewall to the Firewall Management Center.

- [Cable the firewall, on page 11](#)
- [Perform initial configuration, on page 12](#)
- [Register the firewall with the Firewall Management Center, on page 14](#)

## Cable the firewall

Connect the Firewall Management Center to the dedicated Management 1/1 interface. The management network needs access to the internet for updates. For example, you can connect the management network to the internet through the firewall itself (for example, by connecting to the inside network).

- 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 an SFP into Management 1/1—It is a 1/10/25-Gbps SFP28 port that requires an SFP/SFP+/SFP28 module.
- 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.



## 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.

```
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:

Enter an IPv4 address for the management interface [192.168.45.61]: 10.89.5.17
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192

Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1

Enter a fully qualified hostname for this system [firepower]: 1010-3
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220,2620:119:35::35]:
Enter a comma-separated list of search domains or 'none' []: cisco.com
If your networking information has changed, you will need to reconnect.
Disabling IPv6 configuration: management0
Setting DNS servers: 208.67.222.222,208.67.220.220,2620:119:35::35
Setting DNS domains:cisco.com

Setting hostname as 1010-3
Setting static IPv4: 10.89.5.17 netmask: 255.255.255.192 gateway: 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'

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 Identify the Firewall Management Center.

**configure manager add** {hostname | IPv4\_address | IPv6\_address | **DONTRESOLVE**} reg\_key nat\_id

- `{hostname | IPv4_address | IPv6_address | DONTRESOLVE}`—Specifies either the FQDN or IP address of the Firewall Management Center. If the Firewall Management Center is not directly addressable, use **DONTRESOLVE**, in which case the firewall must have a reachable IP address or hostname.
- `reg_key`—Specifies a one-time registration key of your choice that you will also specify on the Firewall Management Center when you register the Firewall Threat Defense. The registration key must be between 2 and 36 characters. Valid characters include alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-).
- `nat_id`—Specifies a unique, one-time string of your choice that you will also specify on the Firewall Management Center. The NAT ID must be between 2 and 36 characters. Valid characters include alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-). This ID cannot be used for any other devices registering to the Firewall Management Center.

**Example:**

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

## Register the firewall with the Firewall Management Center

Register the firewall to the Firewall Management Center.

**Procedure**

- 
- Step 1** Log into the Firewall Management Center.
- a) Enter the following URL.  
`https://fmc_ip_address`
  - b) Enter your username and password.
  - c) Click **Log In**.
- Step 2** Choose **Devices > Device Management**.
- Step 3** From the **Add** drop-down menu, choose **Device**.
- Step 4** Click **Registration Key**, click **Basic**, and then click **Next**.



**Figure 9: Device Registration Method**

The screenshot shows the 'Add device' wizard with three steps: 1. Device registration method (active), 2. Device details, and 3. Initial device configuration. The main content area is titled 'Device registration method' and contains two options: 'Registration key' and 'Serial number'. The 'Registration key' option is highlighted with a blue border and includes a description: 'Identify the same one-time registration key on the device and in the management center.' The 'Serial number' option includes a description: 'Identify the device by serial number. On the device, you don't have to configure anything (zero-touch provisioning).' Below these options, there is a section titled 'Choose the initial device configuration method:' with two radio buttons: 'Basic' (selected) and 'Device template'. The 'Basic' option has a description: 'Apply basic configuration, including the access control policy.' The 'Device template' option has a description: 'Preconfigure settings using a template. A compatible **template** must exist (either a default template or one you added) before continuing.' At the bottom of the wizard, there are 'Cancel' and 'Next' buttons.

**Add device**

1 Device registration method

2 Device details

3 Initial device configuration

**Device registration method**

**Registration key**  
Identify the same one-time registration key on the device and in the management center.

**Serial number**  
Identify the device by serial number. On the device, you don't have to configure anything (zero-touch provisioning).

Choose the initial device configuration method:

☒ **Basic**  
Apply basic configuration, including the access control policy.

☐ **Device template**  
Preconfigure settings using a template. A compatible **template** must exist (either a default template or one you added) before continuing.

Cancel Next

**Step 5** Configure the device details and click **Next**.

Figure 10: Device Details

**Add device**

✓ Device registration method

**2 Device details**

3 Initial device configuration

**Device details**

**Domain \***

Global/Leaf1

**Hostname or IP address**

10.89.5.41

e.g. server.example.com or 192.168.1.1

**Display name \***

3110-1

**Registration key \***

....

Enter the same registration key you set on the device. This key doesn't have to be unique per device. Use alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-), between 2 and 36 characters.

**Unique NAT ID ⓘ**

31101

Enter the same NAT ID if you set one on the device. This key needs to be unique per device. Use alphanumeric characters (A–Z, a–z, 0–9) and the hyphen (-), between 2 and 36 characters.

☐ **Analytics-only management center**

When using Security Cloud Control as your primary manager, you can use an On-Prem management center for analytics.

[Cancel](#) [Back](#) [Next](#)

- **Domain**—In a multidomain environment, choose the leaf domain.
- **Device group**—In a single domain environment, add the device to a **Device group**.
- **Hostname or IP address**—Enter the IP address or the hostname of the device you want to add. Leave this field blank if you don't know the device IP address (for example, it's behind NAT).
- **Display name**—Enter a name for the device as you want it to display in the Firewall Management Center. You cannot change this name later.
- **Registration key**—Enter the same registration key from your initial configuration.
- **Unique NAT ID**—Enter the same ID from your initial configuration.
- **Analytics-only management center**—Leave this unchecked.

**Step 6** Configure the initial device configuration.

Figure 11: Initial Device Configuration

**Add device**

Initial device configuration

Access control policy \*

Default Access Control Policy +

**Smart licensing**

Ensure that your smart licensing account has the required licenses.

Is this device physical or virtual?

☒ Physical device ☐ Virtual device

| License type                                        | Includes                       |
|-----------------------------------------------------|--------------------------------|
| <input checked="" type="checkbox"/> Essentials      | Base firewall capabilities     |
| <input checked="" type="checkbox"/> Carrier         | 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 Filtering   | URL Reputation                 |
| <input checked="" type="checkbox"/> RA VPN Premier  | RA VPN                         |

☒ **Transfer packets**

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

Cancel Back Add device

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

You can also apply licenses after you add the device.

- **Transfer packets**—Enable this option so that for each intrusion event, the device transfers the packet to the Firewall Management Center for inspection.

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

## Step 7 Click **Add device**.

It may take up to two minutes for the Firewall Management Center to verify the device's heartbeat and establish communication. If the registration succeeds, the device is added to the list. If it fails, you will see an error message. If the device fails to register, check the following items:

- **Ping**—Access the device CLI, and ping the Firewall Management Center IP address using the following command:  
**ping system ip\_address**

If the ping is not successful, check your network settings using the **show network** command. If you need to change the device IP address, use the **configure network {ipv4 | ipv6} manual** command.

- Registration key, NAT ID, and Firewall Management Center IP address—Make sure you are using the same registration key, and if used, NAT ID, on both devices. You can set the registration key and NAT ID on the device using the **configure manager add** command.

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

---



## CHAPTER 3

# Configure a Basic Policy

---

Configure a basic security policy with the following settings:

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

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

- [Configure interfaces, on page 19](#)
- [Configure the DHCP server, on page 24](#)
- [Add the default route, on page 25](#)
- [Configure NAT, on page 28](#)
- [Configure an access control rule, on page 31](#)
- [Deploy the configuration, on page 33](#)

## 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 12: Interfaces

| Device   Routing <b>Interfaces</b> 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           | 🔍 ↺ |
| 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 13: General Tab

### Edit Physical Interface

General   IPv4   IPv6   Path Monitoring   ⌵

Name:

☒ Enabled

☐ Management Only

Description:

Mode:

Security Zone:

Interface ID:

MTU:

(64 - 9000)

Priority:

(0 - 65535)

Propagate Security Group Tag: ☐

NVE Only:

☐

- a) 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.

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

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

- c) Check the **Enabled** check box.

- d) Leave the **Mode** set to **None**.

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

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

For example, enter **192.168.1.1/24**

**Figure 14: IPv4 Tab**

Edit Physical Interface

General IPv4 IPv6 Path Monitoring

IP Type:  
Use Static IP

IP Address:  
192.168.1.1/24  
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 15: IPv6 Tab**

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address:

Autoconfiguration: ☒

Obtain Default Route: ☐

- f) Click **OK**.

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

Figure 16: General Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware

Name:  
outside

☒ Enabled  
☐ Management Only

Description:

Mode:  
None

Security Zone:  
outside\_zone

Interface ID:  
GigabitEthernet0/0

MTU:  
1500  
(64 - 9000)

Priority:  
0 (0 - 65535)

Propagate Security Group Tag: ☐

NVE Only:  
☐

- 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**.  
If the outside interface was pre-configured, the rest of these fields are optional.
- b) Enter a **Name** up to 48 characters in length.  
For example, name the interface **outside**.
- c) Check the **Enabled** check box.
- d) Leave the **Mode** set to **None**.
- e) Click the **IPv4** and/or **IPv6** tab.
  - **IPv4**—Choose **Use DHCP**, and configure the following optional parameters:
    - **Obtain default route using DHCP**—Obtains the default route from the DHCP server.
    - **DHCP route metric**—Assigns an administrative distance to the learned route, between 1 and 255. The default administrative distance for the learned routes is 1.



Figure 17: IPv4 Tab

Edit Physical Interface

General IPv4 IPv6 Path Mc

IP Type:  
Use DHCP

Obtain default route using DHCP: ☒

DHCP route metric:  
1  
(1 - 255)

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

Figure 18: IPv6 Tab

Edit Physical Interface

General IPv4 IPv6 Path Monitoring Hardware Configu

Basic Address Prefixes Settings DHCP

Enable IPV6: ☐

Enforce EUI 64: ☐

Link-Local address:

Autoconfiguration: ☒

Obtain Default Route: ☐

f) Click **OK**.

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

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

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

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

- Check the **Enabled** check box.
- Leave the **Mode** set to **None**.
- Click the **IPv4** and/or **IPv6** tab and configure the IP address as desired.
- 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 19: DHCP Server**

The screenshot shows 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, there is a sidebar with options: DHCP Server (selected), DHCP Relay, and DDNS. The main configuration area includes fields for Ping Timeout (50), Lease Length (3600), and an unchecked Auto-Configuration checkbox. Below these is an Interface dropdown menu. The 'Override Auto Configured Settings' section includes fields for Domain Name, Primary DNS Server, Secondary DNS Server, Primary WINS Server, and Secondary WINS Server. At the bottom, there is a 'Server' tab (highlighted with a red box) and an 'Advanced' section. A '+ Add' button (also highlighted with a red box) is located in the bottom right corner. Below the configuration fields is a table with columns: Interface, Address Pool, and Enable DHCP Server. The table is currently empty, displaying 'No records to display'.

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

Figure 20: 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**.

## Add the default route

The default route normally points to the upstream router reachable from the outside interface. If you obtained the outside address from DHCP, your device might have already received a default route. If you need to manually add the route, complete this procedure.

### Procedure

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

**Step 2** Choose **Routing** > **Static Route**.

**Figure 21: Static Route**

Device **Routing** Interfaces Inline Sets DHCP VTEP SNMP

Manage Virtual Routers

Global

Virtual Router Properties

ECMP

BFD

OSPF

OSPFv3

EIGRP

RIP

Policy Based Routing

BGP
 

- IPv4
- IPv6
- Static Route**
- Multicast Routing

| Network     | Interface | Leaked from Virtual Router | Gateway | Tunneled | Metric | Tracked |
|-------------|-----------|----------------------------|---------|----------|--------|---------|
| IPv4 Routes |           |                            |         |          |        |         |
| IPv6 Routes |           |                            |         |          |        |         |

+ Add Route

If you received a default route from the DHCP server, it will show in this table.

**Step 3** Click **Add Route**, and set the following options.

Figure 22: Add Static Route Configuration

**Add Static Route Configuration**

Type: ☒ IPv4 ☐ IPv6

Interface\*  
outside

(Interface starting with this icon signifies it is available for route leak)

Available Network +

Search

any-ipv4  
gateway  
IPv4-Benchmark-Tests  
IPv4-Link-Local  
IPv4-Multicast  
IPv4-Private-10.0.0.0-8

Add

Selected Network

any-ipv4

Gateway\*  
gateway +

Metric:  
1  
(1 - 254)

Tunneled: ☐ (Used only for default Route)

Route Tracking:  
+

Cancel OK

- **Type**—Click the **IPv4** or **IPv6** radio button depending on the type of static route that you are adding.
- **Interface**—Choose the egress interface; typically the outside interface.
- **Available Network**—Choose **any-ipv4** for an IPv4 default route, or **any-ipv6** for an IPv6 default route, and click **Add** to move it to the **Selected Network** list.
- **Gateway** or **IPv6 Gateway**—Enter or choose the gateway router that is the next hop for this route. You can provide an IP address or a Networks/Hosts object.

**Step 4** Click **OK**.

The route is added to the static route table.

**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 23: 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 24: NAT Policy

The screenshot shows the 'FTD\_Policy' configuration page. At the top right are buttons for 'Show Warnings', 'Save', and 'Cancel'. Below the title bar, there's a 'Rules' tab and links for 'NAT Exemptions' and 'Policy Assignments (1)'. A 'Filter Rules' search bar is present. The 'Add Rule' button is highlighted with a red box. Below the filter bar is a table with columns for '#', 'Direction', 'Type', 'Source Interface Objects', 'Destination Interface Objects', 'Original Packet' (with sub-columns: Original Sources, Original Destinations, Original Services), 'Translated Packet' (with sub-columns: Translated Sources, Translated Destinations, Translated Services), and 'Options'. The table is divided into sections: 'NAT Rules Before', 'Auto NAT Rules', and 'NAT Rules After'.

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

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

Figure 25: Basic Rule Options

The screenshot shows the 'Add NAT Rule' dialog box. It has two tabs: 'Interface Objects' and 'Translation'. Under 'Interface Objects', there are dropdowns for 'NAT Rule' (set to 'Auto NAT Rule') and 'Type' (set to 'Dynamic'), and a checked 'Enable' checkbox. The 'Translation' tab is currently selected.

- **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 26: Interface Objects

The screenshot shows the 'Interface Objects' configuration page with tabs for 'Interface Objects', 'Translation', 'PAT Pool', and 'Advanced'. The 'Interface Objects' tab is active. It shows 'Available Interface Objects' on the left with a search bar and a list containing 'inside' and 'outside'. The 'outside' object is highlighted with a red circle '1'. Below the list are 'Add to Source' and 'Add to Destination' buttons. The 'Add to Destination' button is highlighted with a red circle '2'. On the right, there are two boxes: 'Source Interface Objects' (containing 'any') and 'Destination Interface Objects' (containing 'outside'). The 'outside' object in the destination box is highlighted with a red circle '3'.

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

Figure 27: Translation

| Interface Objects                                            | Translation | PAT Pool                                                                    | Advanced |
|--------------------------------------------------------------|-------------|-----------------------------------------------------------------------------|----------|
| Original Packet                                              |             | Translated Packet                                                           |          |
| Original Source:*<br><input type="text" value="all-ipv4"/> + |             | Translated Source:<br><input type="text" value="Destination Interface IP"/> |          |
| Original Port:<br><input type="text" value="TCP"/>           |             | <input type="text"/>                                                        |          |
| <input type="text"/>                                         |             | Translated Port:<br><input type="text"/>                                    |          |

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

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

Figure 28: New Network Object

### New Network Object

Name

Description

Network  
☐ Host ☐ Range ☒ Network ☐ FQDN

☐ 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 29: Source Zone**

The screenshot shows the 'Add Rule' configuration page. The rule name is 'inside-to-outside'. The 'Zones' tab is selected, showing a list of zones: 'inside' (Routed Security Zone) and 'outside' (Routed Security Zone). The 'inside' zone is selected. The 'Add Source Zone' button is highlighted.

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

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

3. Click **Add Source Zone**.

**Figure 30: Destination Zone**

The screenshot shows the 'Add Rule' configuration page. The rule name is 'inside-to-outside'. The 'Zones' tab is selected, showing a list of zones: 'inside' (Routed Security Zone) and 'outside' (Routed Security Zone). The 'outside' zone is selected. The 'Add Destination Zone' button is highlighted.

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 31: 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.

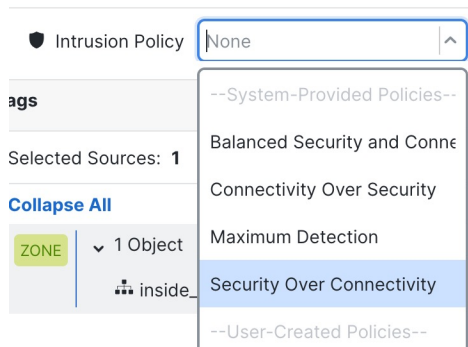
- **Identity**—Identity is not applied by default. You can require a user to authenticate before allowing traffic to be processed by the access control policy.

**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 32: System-Provided Intrusion Policies



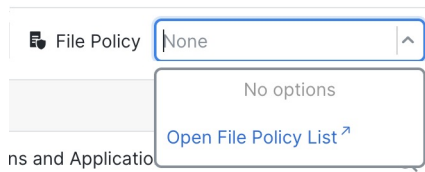
- b) Choose one of the system-provided policies from the list.

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 33: 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**.

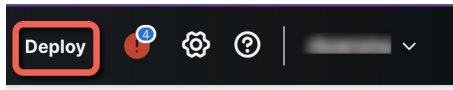
## Deploy the configuration

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

### Procedure

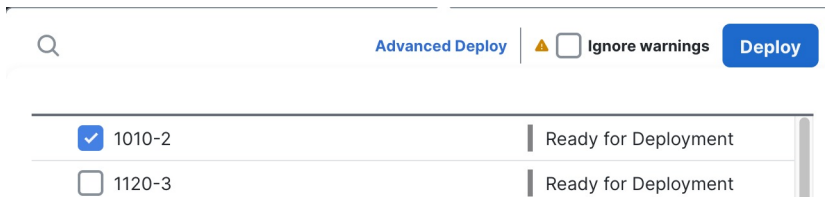
**Step 1** Click **Deploy** in the upper right.

Figure 34: Deploy



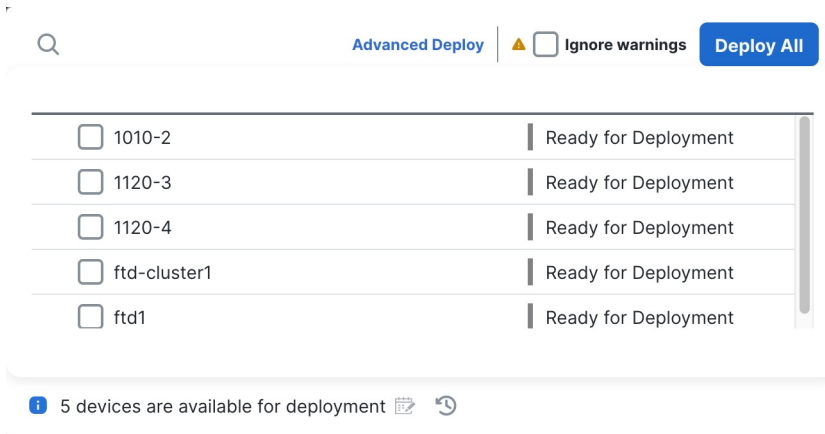
**Step 2** For a quick deployment, check specific devices and then click **Deploy**.

Figure 35: Deploy Selected



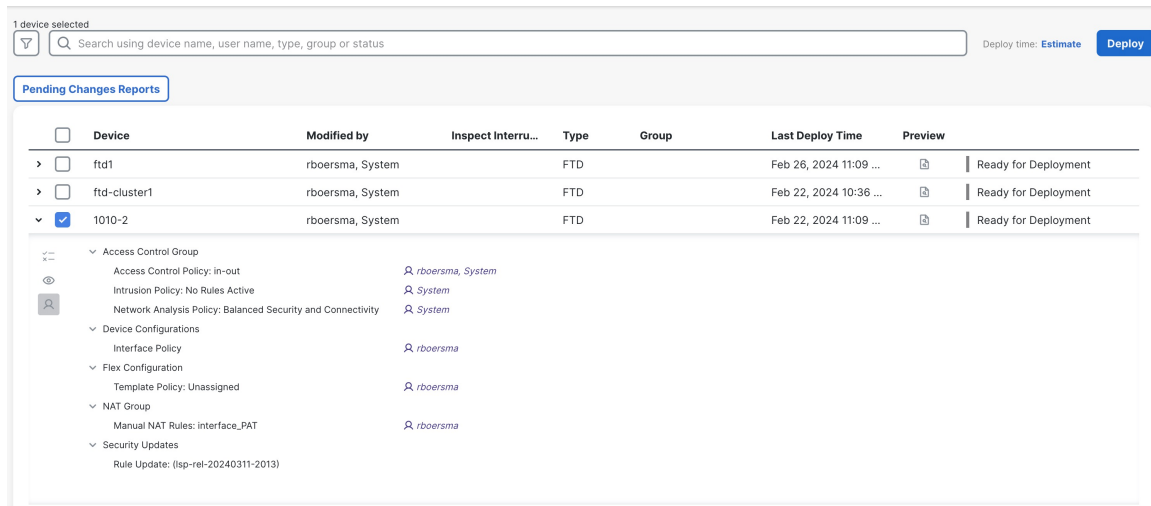
Or click **Deploy All** to deploy to all devices.

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

