



## 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.

Configure an ASA using ASDM.



---

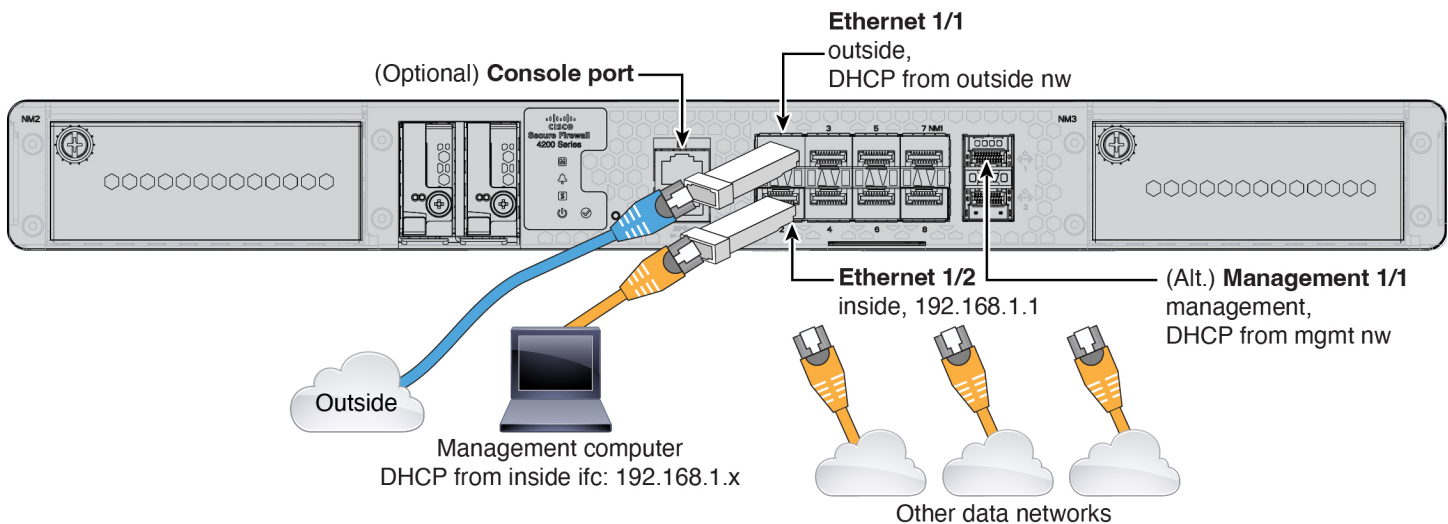
**Note** The Secure Firewall 4200 runs in appliance mode only; it does not support platform mode, which uses FXOS as the chassis manager. Appliance mode lets you configure all settings in the ASA. Only advanced troubleshooting commands are available from the FXOS CLI.

---

- [Cable the firewall, on page 2](#)
- [Power on the firewall, on page 2](#)
- [Which application is installed: Firewall Threat Defense or ASA?, on page 3](#)
- [Access the ASA CLI, on page 4](#)
- [Obtain licenses, on page 6](#)

## Cable the firewall

- (Optional) 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 interfaces and optional Management ports—The built-in ports are 1/10/25-Gbps SFP28 ports that require SFP/SFP+/SFP28 modules.
- See the [hardware installation guide](#) for more information.



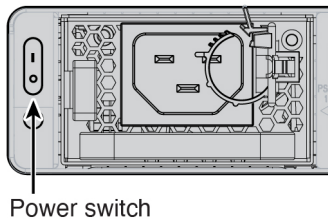
## Power on the firewall

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.

### Procedure

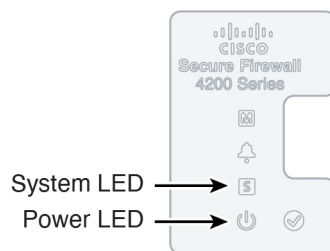
- 
- Step 1** Attach the power cord to the firewall, and connect it to an electrical outlet.
- Step 2** Turn the power on using the rocker power switch located on the rear of the chassis, adjacent to the power cord.

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

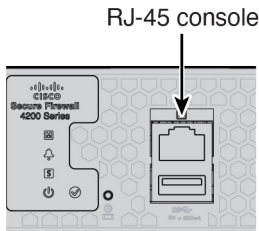
## Which application is installed: Firewall Threat Defense or ASA?

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.

```
firepower login:
```

### ASA

You see the ASA prompt.

```
ciscoasa>
```

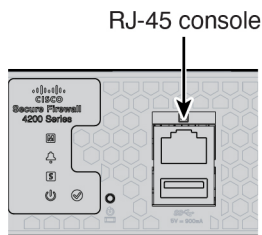
**Step 3** If you are running the wrong application, see [Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide](#).

# Access the ASA 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 the ASA CLI in user EXEC mode. This mode lets you use many **show** commands.

```
ciscoasa>
```

**Step 3** Access privileged EXEC mode. This password-protected mode lets you perform many actions, including accessing configuration modes.

**enable**

You are prompted to change the password the first time you enter the **enable** command.

**Example:**

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: *****
Repeat Password: *****
ciscoasa#
```

**Step 4** Access global configuration mode.

**configure terminal**

**Example:**

```
ciscoasa# configure terminal
ciscoasa(config)#
```

**Step 5** Access the FXOS CLI. Use this CLI for troubleshooting at the hardware level.

**connect fxos [admin]**

- **admin**—Provides admin-level access. Without this option, you have read-only access. Note that no configuration commands are available even in admin mode.

You are not prompted for user credentials. The current ASA username is passed through to FXOS, and no additional login is required. To return to the ASA CLI, enter **exit** or type **Ctrl-Shift-6, x**.

**Example:**

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
```

```
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

## Obtain licenses

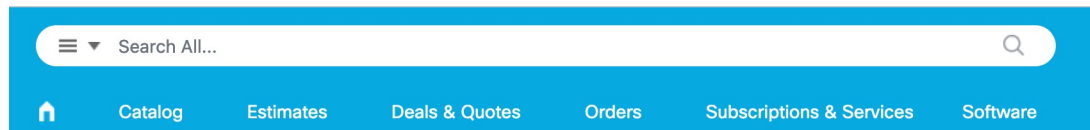
When you bought your device from Cisco or a reseller, your licenses should have been linked to your Smart Software License account. If you don't have an account on the [Smart Software Manager](#), click the link to [set up a new account](#).

The ASA has the following licenses:

- Essentials—Required
- Security Contexts
- Carrier—Diameter, GTP/GPRS, M3UA, SCTP
- Cisco Secure Client

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

**Figure 5: License Search**



2. Search for the following license PIDs.



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

- Essentials—*Included automatically*.
- 5 context—L-FPR4200-ASASC-5=. Context licenses are additive; buy multiple licenses.
- 10 context—L-FPR4200-ASASC-10=. Context licenses are additive; buy multiple licenses.
- Carrier (Diameter, GTP/GPRS, M3UA, SCTP)—L-FPR4200-ASA-CAR=
- Cisco Secure Client—See the [Cisco Secure Client Ordering Guide](#). You do not enable this license directly in the ASA.

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

*Figure 6: Results*