



Before You Begin

The Secure Firewall 6100 is an AI-ready, ultra-high-end firewall, engineered to deliver exceptional throughput per rack unit. Optimized for high-performing data center and telecommunications mobility infrastructure environments, the Secure Firewall 6100 features a multi-socket, multi-core architecture that enables rapid threat inspection. Its dedicated cryptographic modules facilitate high-throughput IPSec and TLS connection termination at scale, providing industry-leading cryptographic performance within its two rack unit (RU) form factor.

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



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

This guide specifically covers outside management, but you can refer to [Cisco Security Cloud Control: Cloud-Delivered Firewall Management Center for Firewall Threat Defense](#) for management using the Management interface.

- [Power on the firewall, on page 1](#)
- [Which application is installed: Firewall Threat Defense or ASA?, on page 3](#)
- [Access the Firewall Threat Defense CLI, on page 3](#)
- [Check the version and reimage, on page 5](#)
- [Obtain licenses, on page 6](#)
- [\(If Needed\) Power off the firewall, on page 7](#)

Power on the firewall

System power is controlled by a power button located on the rear of the firewall. The power button 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.

Power on the firewall

Before you begin

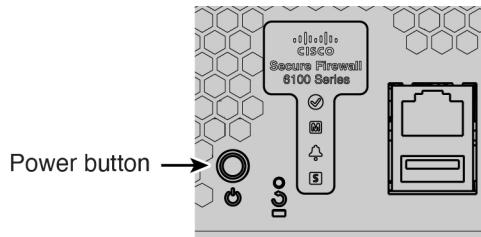
It's important that you provide reliable power for your firewall (for example, using an uninterruptable power supply (UPS)). Loss of power without first shutting down can cause serious file system damage. There are many processes running in the background all the time, and losing power does not allow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

Procedure

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

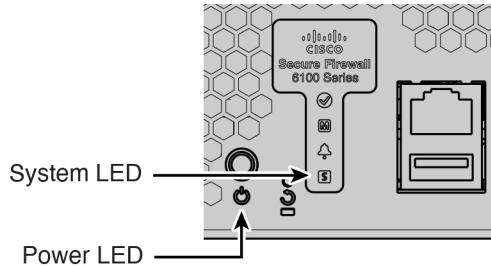
Step 2 Turn the power on using the power button located on the rear of the chassis, adjacent to the power cord.

Figure 1: Power button



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
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?

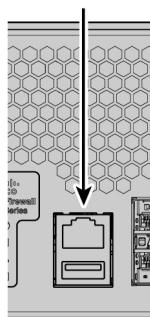
Both applications, Firewall Threat Defense or ASA, are supported on the hardware. Connect to the console port and determine which application was installed at the factory.

Procedure

Step 1 Connect to the console port.

Figure 3: Console port

RJ-45 console



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 3](#).

```
firepower login:
```

ASA

You see the ASA prompt.

```
ciscoasa>
```

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

Access the Firewall Threat Defense CLI

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

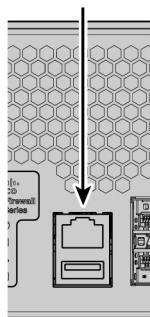
Procedure

Step 1

Connect to the console port.

Figure 4: Console port

RJ-45 console



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?

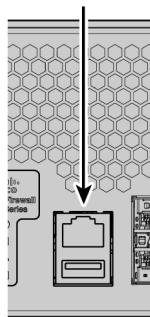
Cisco recommends running a Gold Star release indicated by a gold star next to the release number on the software download page. You can also refer to the release strategy described in <https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html>.

Procedure

Step 1 Connect to the console port.

Figure 5: Console port

RJ-45 console



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.

- 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

- 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.

- At the FXOS CLI, you are prompted to set the admin password again.
- Shut down the firewall. See [\(If Needed\) Power off the firewall](#), on page 7.

Obtain licenses

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

If you have not already done so, register 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

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

Figure 6: License Search



- Search for the following license PIDs.

**Note**

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

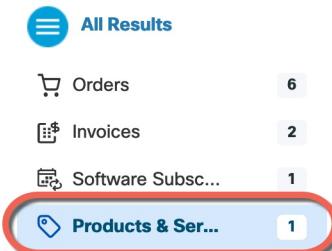
- IPS, Malware Defense, and URL combination:
 - CSF_6160_TD_TMC
 - CSF_6170_TD_TMC

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:

- CSF_6160_TD_TMC-1Y
- CSF_6160_TD_TMC-3Y
- CSF_6160_TD_TMC-5Y
- CSF_6170_TD_TMC-1Y
- CSF_6170_TD_TMC-3Y
- CSF_6170_TD_TMC-5Y
- Carrier:
 - CSF_6100_FTD_CARRIER
- 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

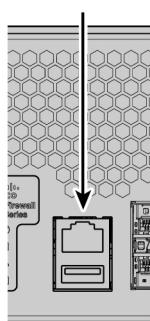
You can use the FXOS CLI to safely shut down the system and power off the firewall.

Procedure

Step 1 Connect to the console port.

Figure 8: Console port

RJ-45 console



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** (edit icon).
- Click the **Device** tab.
- Click **Shut Down Device** (power off icon) 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.

■ Power off the firewall using the Firewall Management Center