

Upgrade the Chassis on the Firepower 4100/9300

Cisco Firepower 4100/9300 FXOS Release Notes, 2.12

- Upgrade Packages for FXOS, on page 1
- Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 1
- Upgrade Paths for FXOS, on page 3
- Upgrade FXOS with Firewall Chassis Manager, on page 7
- Upgrade FXOS with the CLI, on page 12

Upgrade Packages for FXOS

FXOS images and firmware updates are available on the Cisco Support & Download site:

- Firepower 4100 series: http://www.cisco.com/go/firepower4100-software
- Firepower 9300: http://www.cisco.com/go/firepower9300-software

To find the correct FXOS image, select or search for your device model and browse to the *Firepower Extensible Operating System* download page for your target FXOS version and build. The FXOS image is listed along with recovery and MIB packages. If you need to upgrade the firmware, those packages are under *All Releases > Firmware*.

The packages are:

- Firepower 4100/9300 FXOS image: fxos-k9.*fxos_version*.SPA
- Firepower 4100 series firmware: fxos-k9-fpr4k-firmware.*firmware_version*.SPA
- Firepower 9300 firmware: fxos-k9-fpr9k-firmware.*firmware_version*.SPA

Upgrade Guidelines for the Firepower 4100/9300 Chassis

For the Firepower 4100/9300, major Firewall Threat Defense upgrades also require a chassis upgrade (FXOS and firmware). Maintenance release and patches rarely require this, but you may still want to upgrade to the latest build to take advantage of resolved issues.

Table 1: Upgrade Guidelines for the Firepower 4100/9300 Chassis

Guideline	Details
FXOS upgrades.	FXOS 2.12.1.95+ is required to run threat defense Version 7.2 on the Firepower 4100/9300. You can upgrade to any later FXOS version from as far back as FXOS 2.2.2. For critical and release-specific upgrade guidelines, new and deprecated features, and open and resolved bugs, see the Firepower 4100/9300 FXOS release notes.
Firmware upgrades.	FXOS 2.14.1+ upgrades include firmware. If you are upgrading to an earlier FXOS version, see the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.
Time to upgrade.	Chassis upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see Traffic Flow and Inspection for Chassis Upgrades, on page 2.
Chassis upgrade order with Firewall Threat Defense high availability/scalability.	In high availability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade FXOS one chassis at a time. You must also upgrade the Firewall Threat Defense devices one at a time. For more information, see Upgrade Order for FXOS with Firewall Threat Defense High Availability, on page 7.
Chassis upgrade order with Firewall Threat Defense and ASA logical devices.	If you have Firewall Threat Defense *and* ASA logical devices configured on the Firepower 9300, use the procedures in this chapter to upgrade FXOS and Firewall Threat Defense. Make sure that upgrading FXOS does not bring you out of compatibility with either type of logical device; see Upgrade Path for FXOS with Firewall Threat Defense and ASA, on page 5. For ASA upgrade procedures, see the *Cisco Secure Firewall ASA Upgrade Guide*.
Chassis upgrade with no logical devices.	If you have no logical devices configured, use the procedures in this chapter for upgrading FXOS on standalone Firewall Threat Defense devices, disregarding any instructions on logical devices. Or, perform a full reimage of the chassis to the FXOS version you need.

Traffic Flow and Inspection for Chassis Upgrades

Upgrading FXOS reboots the chassis. For FXOS upgrades to Version 2.14.1+ that include firmware upgrades, the device reboots twice—once for FXOS and once for the firmware.

Even in high availability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time. For more information, see Upgrade Order for FXOS with Firewall Threat Defense High Availability, on page 7.

Table 2: Traffic Flow and Inspection: FXOS Upgrades

Firewall Threat Defense Deployment	Traffic Behavior	Method
Standalone	Dropped.	—

Firewall Threat Defense Deployment	Traffic Behavior	Method
High availability	Unaffected.	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.
	Dropped until one peer is online.	Upgrade FXOS on the active peer before the standby is finished upgrading.

Upgrade Paths for FXOS

Choose the upgrade path that matches your deployment.

Upgrade Path for FXOS with Firewall Threat Defense

This table provides the upgrade path for Firewall Threat Defense on the Firepower 4100/9300.

Note that if your current Firewall Threat Defense version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

The table lists our specially qualified version combinations. Because you upgrade FXOS first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of the device software. Make sure upgrading FXOS does not bring you out of compatibility with any logical devices. For minimum builds and other detailed compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Table 3: Firewall Threat Defense Direct Upgrades on the Firepower 4100/9300

Current Versions	Target Versions
FXOS 2.13 with Firewall Threat Defense 7.3	→ FXOS 2.13 with any later Firewall Threat Defense 7.3.x release
FXOS 2.12 with Firewall Threat Defense 7.2 Last support for Firepower 4110, 4120, 4140, 4150. Last support for the Firepower 9300 with SM-24, SM-36, or SM-44 modules.	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with any later Firewall Threat Defense 7.2.x release
FXOS 2.11.1 with Firewall Threat Defense 7.1	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with any later Firewall Threat Defense 7.1.x release

Current Versions	Target Versions
FXOS 2.10.1 with Firewall Threat Defense 7.0	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with any later Firewall Threat Defense 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+. **Note** cannot manage Firewall Threat Defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade directly to a later version.
FXOS 2.9.1 with Firewall Threat Defense 6.7	Any of: → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with any later Firewall Threat Defense 6.7.x release
FXOS 2.8.1 with Firewall Threat Defense 6.6	Any of: → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with any later Firewall Threat Defense 6.6.x release
FXOS 2.7.1 with Firewall Threat Defense 6.5	Any of: → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with Firewall Threat Defense 6.6.x

Upgrade Path for FXOS with Firewall Threat Defense and ASA

This table provides upgrade paths for the Firepower 9300 with Firewall Threat Defense and ASA logical devices running on separate modules.

Note This document does not contain procedures for upgrading ASA logical devices. For those, see the *Cisco Secure Firewall ASA Upgrade Guide*.

Note that if your current Firewall Threat Defense version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

The table lists our specially qualified version combinations. Because you upgrade FXOS first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of the device software. Make sure upgrading FXOS does not bring you out of compatibility with any logical devices (including ASA devices). If you need to skip multiple versions, Firewall Threat Defense will usually be the limiter—FXOS and ASA can usually upgrade further in one hop. After you reach the target FXOS version, it does not matter which type of logical device you upgrade first. For minimum builds and other detailed compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*

Table 4: Firewall Threat Defense and ASA Direct Upgrades on the Firepower 9300

Current Versions	Target Versions
FXOS 2.13 with: • Threat defense 7.3 • ASA 9.19(x)	→ FXOS 2.13 with ASA 9.19(x) and any later threat defense 7.3.x release
FXOS 2.12 with: • Threat defense 7.2 • ASA 9.18(x) Last support for the Firepower 9300 with SM-24, SM-36, or SM-44 modules.	Any of: → FXOS 2.13 with ASA 9.19(x) and threat defense 7.3.x → FXOS 2.12 with ASA 9.18(x) and any later threat defense 7.2.x release
FXOS 2.11.1 with: • Threat defense 7.1 • ASA 9.17(x)	→ FXOS 2.13 with ASA 9.19(x) and threat defense 7.3.x → FXOS 2.12 with ASA 9.18(x) and threat defense 7.2.x → FXOS 2.11.1 with ASA 9.17(x) and any later threat defense 7.1.x release

Current Versions	Target Versions
FXOS 2.10.1 with: • Threat defense 7.0 • ASA 9.16(x)	Any of: → FXOS 2.13 with ASA 9.19(x) and threat defense 7.3.x → FXOS 2.12 with ASA 9.18(x) and threat defense 7.2.x → FXOS 2.11.1 with ASA 9.17(x) and threat defense 7.1.x → FXOS 2.10.1 with ASA 9.16(x) and any later threat defense 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+. **Note** cannot manage Firewall Threat Defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade directly to a later version.
FXOS 2.9.1 with: • Threat defense 6.7 • ASA 9.15(x)	Any of: → FXOS 2.12 with ASA 9.18(x) and threat defense 7.2.x → FXOS 2.11.1 with ASA 9.17(x) and threat defense 7.1.x → FXOS 2.10.1 with ASA 9.16(x) and threat defense 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and any later threat defense 6.7.x release
FXOS 2.8.1 with: • Threat defense 6.6 • ASA 9.14(x)	Any of: → FXOS 2.12 with ASA 9.18(x) and threat defense 7.2.x → FXOS 2.11.1 with ASA 9.17(x) and threat defense 7.1.x → FXOS 2.10.1 with ASA 9.16(x) and threat defense 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and threat defense 6.7.x → FXOS 2.8.1 with ASA 9.14(x) and any later threat defense 6.6.x release
FXOS 2.7.1 with: • Threat defense 6.5 • ASA 9.13(x)	Any of: → FXOS 2.11.1 with ASA 9.17(x) and threat defense 7.1.x → FXOS 2.10.1 with ASA 9.16(x) and threat defense 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and threat defense 6.7.x → FXOS 2.8.1 with ASA 9.14(x) and threat defense 6.6.x

Upgrade Order for FXOS with Firewall Threat Defense High Availability

In high availability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade FXOS one chassis at a time. You must also upgrade the Firewall Threat Defense devices one at a time.

Table 5:

Firewall Threat Defense Deployment	Upgrade Order
Standalone	**1.** Upgrade FXOS. **2.** Upgrade Firewall Threat Defense.
High availability	Upgrade FXOS on both chassis before you upgrade Firewall Threat Defense. To minimize disruption, always upgrade the standby. In the following scenario, Device A is the original active device and Device B is the original standby. **1.** Upgrade FXOS on the chassis with the standby device (B). **2.** Switch roles. **3.** Upgrade FXOS on the chassis with the new standby device (A). **4.** Upgrade Firewall Threat Defense on the new standby device (A). **5.** Switch roles again. **6.** Upgrade Firewall Threat Defense on the original standby device (B).

Upgrade FXOS with Firewall Chassis Manager

Upgrade FXOS for Standalone FTD Logical Devices Using Firepower Chassis Manager

The section describes the upgrade process for the following types of devices:

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair.
- A Firepower 9300 chassis that is configured with one or more standalone FTD logical devices that are not part of a failover pair.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.

- Back up your FXOS and FTD configurations.

Procedure

Step 1 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 2 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 3 After the new platform bundle image has been successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 4 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 5 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note
After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
```

```
Upgrade-Status: Ready
```

Step 6 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as a high availability pair, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.

Procedure

Step 1 Connect to Firepower Chassis Manager on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:

Step 2 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 3 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 4 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 5 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 6 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note
After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Step 7 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 8 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

a) Connect to Firepower Management Center.
b) Choose **Devices** > **Device Management**.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).
d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Step 9 Connect to Firepower Chassis Manager on the Firepower security appliance that contains the *new standby* Firepower Threat Defense logical device:

Step 10 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 11 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 12 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 13 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

Step 14 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note
After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Step 15 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 16 Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) Connect to Firepower Management Center.
b) Choose **Devices** > **Device Management**.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).
d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Upgrade FXOS with the CLI

Upgrade FXOS for Standalone FTD Logical Devices Using the FXOS CLI

The section describes the FXOS upgrade process for the following types of devices:

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair.
- A Firepower 9300 chassis that is configured with one or more standalone FTD devices that are not part of a failover pair.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.
- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

Firepower-chassis-a # **scope firmware**

b) Download the FXOS platform bundle software image:

Firepower-chassis-a /firmware # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 3 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 4 Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 5 Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

Step 6 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 7 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 8 To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note
After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 9 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as a high availability pair, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.
- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Procedure

Step 1 Connect to FXOS CLI on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:

Step 2 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

Firepower-chassis-a # **scope firmware**

b) Download the FXOS platform bundle software image:

Firepower-chassis-a /firmware # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname*/*path*/*image_name*
- **scp**://*username@hostname*/*path*/*image_name*
- **sftp**://*username@hostname*/*path*/*image_name*
- **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
```

```
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 3 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 4 Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 5 Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing; for example, 2.3(1.58).

Step 6 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 7 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 8 To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note
After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
```

```
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 9 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 10 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

a) Connect to Firepower Management Center.
b) Choose **Devices** > **Device Management**.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).
d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Step 11 Connect to FXOS CLI on the Firepower security appliance that contains the *new standby* Firepower Threat Defense logical device:

Step 12 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

   Firepower-chassis-a # **scope firmware**

b) Download the FXOS platform bundle software image:

   Firepower-chassis-a /firmware # **download image** *URL*

   Specify the URL for the file being imported using one of the following syntax:

   - **ftp**://*username@hostname*/*path*/*image_name*
   - **scp**://*username@hostname*/*path*/*image_name*
   - **sftp**://*username@hostname*/*path*/*image_name*
   - **tftp**://*hostname***:***port-num*/*path*/*image_name*

c) To monitor the download process:

   Firepower-chassis-a /firmware # **scope download-task** *image_name*

   Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
```

```
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 13 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 14 Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 15 Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing; for example, 2.3(1.58).

Step 16 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 17 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 18 To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note
After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
```

```
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 19 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 20 Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) Connect to Firepower Management Center.
b) Choose **Devices** > **Device Management**.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).
d) Click **Yes** to immediately make the standby device the active device in the high availability pair.