

Upgrade Firepower Threat Defense

- Upgrade Checklist: Firepower Threat Defense with FMC, on page 1
- Upgrade FXOS on a Firepower 4100/9300 with Firepower Threat Defense Logical Devices, on page 6
- Upgrade Firepower Threat Defense with FMC (Version 7.0.0), on page 24
- Upgrade Firepower Threat Defense with FMC (Version 6.0.1–6.7.0), on page 27

Upgrade Checklist: Firepower Threat Defense with FMC

Complete this checklist before you upgrade Firepower Threat Defense.

Note At all times during the process, make sure you maintain deployment communication and health.

In most cases, do *not* restart an upgrade in progress. However, starting with major and maintenance FTD upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI. Note that by default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to *manually* cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 1:

✓	Action/Check
	Plan your upgrade path. This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next. **Note** In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first. See Upgrade Paths.
	Read *all* upgrade guidelines and plan configuration changes. Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with the release notes, which contain critical and release-specific information, including upgrade warnings, behavior changes, new and deprecated features, and known issues.
	Check appliance access. Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also able to access the FMC management interface without traversing the device.
	Check bandwidth. Make sure your management network has the bandwidth to perform large data transfers. In FMC deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you *must* perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

Upgrade packages are available on the Cisco Support & Download site.

Table 2:

✓	Action/Check
	Upload the upgrade package to the FMC or internal web server. In Version 6.6.0+ you can configure an internal web server instead of the FMC as the source for FTD upgrade packages. This is useful if you have limited bandwidth between the FMC and its devices, and saves space on the FMC. See Upload to an Internal Server (Version 6.6.0+ FTD with FMC).
	Copy the upgrade package to the device. When supported, we recommend you copy (*push*) packages to managed devices before you initiate the device upgrade: • Version 6.2.2 and earlier do not support pre-upgrade copy. • Version 6.2.3 allows you to manually copy upgrade packages from the FMC. • Version 6.6.0 adds the ability to manually copy upgrade packages from an internal web server. • Version 7.0.0 adds a FTD upgrade workflow that prompts you to copy upgrade packages. **Note** For the Firepower 4100/9300, we recommend (and sometimes require) you copy the upgrade package before you begin the required companion FXOS upgrade. See Copy to Managed Devices.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.

Caution We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 3:

✓	Action/Check
	Back up FTD. Use the FMC to back up devices. Not all FTD platforms and configurations support backup. Requires Version 6.3.0+. Back up before and after upgrade: • Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly. • After upgrade: This creates a snapshot of your freshly upgraded deployment. In FMC deployments, we recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.
	Back up FXOS on the Firepower 4100/9300. Use the Firepower Chassis Manager or the FXOS CLI to export chassis configurations before and after upgrade, including logical device and platform configuration settings.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 4:

✓	Action/Check
	Upgrade virtual hosting. If needed, upgrade the hosting environment for any virtual appliances. If this is required, it is usually because you are running an older version of VMware and are performing a major device upgrade.
	Upgrade FXOS on the Firepower 4100/9300. If needed, upgrade FXOS before you upgrade FTD. This is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To avoid interruptions in traffic flow and inspection, upgrade FXOS in FTD high availability pairs and inter-chassis clusters *one chassis at a time*. **Note** Before you upgrade FXOS, make sure you read all upgrade guidelines and plan configuration changes. Start with the FXOS release notes: Cisco Firepower 4100/9300 FXOS Release Notes.

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 5:

✓	Action/Check
	Check configurations. Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.
	Check NTP synchronization. Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually. To check time: • FMC: Choose **System > Configuration > Time**. • Devices: Use the **show time** CLI command.
	Check disk space. Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Deploy configurations. Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In FMC high availability deployments, you only need to deploy from the active peer. When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. See the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.
	Run readiness checks. If your FMC is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. Version 7.0.0 introduces a new FTD upgrade workflow that prompts you to complete these checks. See Firepower Software Readiness Checks.
	Check running tasks. Make sure essential tasks on the device are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them.

Upgrade FXOS on a Firepower 4100/9300 with Firepower Threat Defense Logical Devices

On the Firepower 4100/9300, you upgrade FXOS on each chassis independently, even if you have Firepower inter-chassis clustering or high availability pairs configured. You can use the FXOS CLI or Firepower Chassis Manager.

Upgrading FXOS reboots the chassis. Depending on your deployment, traffic can either drop or traverse the network without inspection; see the Cisco Firepower Release Notes for your version.

Upgrade FXOS: FTD Standalone Devices and Intra-chassis Clusters

For a standalone Firepower Threat Defense logical device, or for an FTD intra-chassis cluster (units on the same chassis), first upgrade the FXOS platform bundle then upgrade FTD logical devices. Use the Firepower Management Center to upgrade clustered devices as a unit.

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster 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 or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with one or more standalone FTD logical devices that are not part of a failover pair or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with FTD logical devices in an intra-chassis cluster.

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 for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster 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 or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with one or more standalone FTD devices that are not part of a failover pair or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with FTD logical devices in an intra-chassis cluster.

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: FTD High Availability Pairs

In Firepower Threat Defense high availability deployments, upgrade the FXOS platform bundle on *both chassis* before you upgrade either FTD logical device. To minimize disruption, always upgrade the standby.

In Firepower Management Center deployments, you upgrade the logical devices as a unit:

1. Upgrade FXOS on the standby.
2. Switch roles.
3. Upgrade FXOS on the new standby.
4. Upgrade FTD logical devices.

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 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.

Upgrade FXOS: FTD Inter-chassis Clusters

For Firepower Threat Defense inter-chassis clusters (units on different chassis), upgrade the FXOS platform bundle on *all chassis* before you upgrade the FTD logical devices. To minimize disruption, always upgrade FXOS on an all-data unit chassis. Then, use the Firepower Management Center to upgrade the logical devices as a unit.

For example, for a two-chassis cluster:

1. Upgrade FXOS on the all-data unit chassis.
2. Switch the control module to the chassis you just upgraded.
3. Upgrade FXOS on the new all-data unit chassis.
4. Upgrade FTD logical devices.

Upgrade FXOS on an FTD Inter-chassis Cluster Using Firepower Chassis Manager

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as an inter-chassis cluster, 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 Enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the control unit).
b) Enter **top**.
c) Enter **scope ssa**.
d) Enter **show slot**.
e) 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.
f) Enter **show app-instance**.
g) Verify that the Oper State is `Online` and that the Cluster State is `In Cluster` for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

Important
Verify that the control unit is not on this chassis. There should not be any Firepower Threat Defense instance with Cluster Role set to `Master`.

h) For any security modules installed on a Firepower 9300 appliance or for the security engine on a Firepower 4100 series appliance, verify that the FXOS version is correct:

scope server 1/*slot_id*, where *slot_id* is 1 for a Firepower 4100 series security engine.

show version.

Step 2 Connect to Firepower Chassis Manager on Chassis #2 (this should be a chassis that does not have the control unit).

Step 3 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 4 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 5 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 6 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 7 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.

d) Enter **top**.
e) Enter **scope ssa**.
f) Enter **show slot**.
g) 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.
h) Enter **show app-instance**.
i) Verify that the Oper State is `Online`, that the Cluster State is `In Cluster` and that the Cluster Role is `Slave` for any logical devices installed on the chassis.

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 #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ----------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                    In
 Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                    In
 Cluster      Slave
ftd        3          Disabled    Not Available                   6.2.2.81                    Not
 Applicable  None
FP9300-A /ssa #
```

Step 8 Set one of the security modules on Chassis #2 as control.

After setting one of the security modules on Chassis #2 to control, Chassis #1 no longer contains the control unit and can now be upgraded.

Step 9 Repeat Steps 1-7 for all other Chassis in the cluster.

Step 10 To return the control role to Chassis #1, set one of the security modules on Chassis #1 as control.

Upgrade FXOS on an FTD Inter-chassis Cluster Using the FXOS CLI

If you have Firepower 9300 or Firepower 4100 series security appliances with FTD logical devices configured as an inter-chassis cluster, 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 the FXOS CLI on Chassis #2 (this should be a chassis that does not have the control unit).

Step 2 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` and that the Cluster State is `In Cluster` for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

Important
Verify that the control unit is not on this chassis. There should not be any Firepower Threat Defense instance with Cluster Role set to `Master`.

g) For any security modules installed on a Firepower 9300 appliance or for the security engine on a Firepower 4100 series appliance, verify that the FXOS version is correct:

scope server 1/*slot_id*, where *slot_id* is 1 for a Firepower 4100 series security engine.

show version.

Step 3 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter **top**.
b) Enter firmware mode:

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

c) 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*

d) 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 4 If necessary, return to firmware mode:

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

Step 5 Enter auto-install mode:

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

Step 6 Install the FXOS platform bundle:

Firepower-chassis /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 7 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 8 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 9 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.

d) Enter **top**.
e) Enter **scope ssa**.
f) Enter **show slot**.
g) 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.
h) Enter **show app-instance**.
i) Verify that the Oper State is `Online`, that the Cluster State is `In Cluster` and that the Cluster Role is `Slave` for any logical devices installed on the chassis.

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 #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                    In
 Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                    In
 Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81                    Not
 Applicable  None
FP9300-A /ssa #
```

Step 10 Set one of the security modules on Chassis #2 as control.

After setting one of the security modules on Chassis #2 to control, Chassis #1 no longer contains the control unit and can now be upgraded.

Step 11 Repeat Steps 1-9 for all other Chassis in the cluster.

Step 12 To return the control role to Chassis #1, set one of the security modules on Chassis #1 as control.

Upgrade Firepower Threat Defense with FMC (Version 7.0.0)

The FMC provides a wizard to upgrade FTD. You must still use the System Updates page (**System > Updates**) page to upload or specify the location of upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as any older Classic devices.

The wizard walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and performing compatibility and readiness checks. As you proceed, the wizard displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage.

If you navigate away from the wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the workflow (unless you logged in with a CAC, in which case your progress is cleared 24 hours after you log out). Your progress is also synchronized between high availability FMCs.

Note In Version 7.0.x, the Device Upgrade page does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the workflow displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all.

To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the workflow before you click **Next**.

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. However, with major and maintenance upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI.

Note that by default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to *manually* cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

Before you begin

Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.

Procedure

Select devices to upgrade.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Select the devices you want to upgrade.

You can upgrade multiple devices at once. You must upgrade the members of device clusters and high availability pairs at the same time.

Important
Due to performance issues, if you are upgrading a device *to* (not from) Version 6.4.0.x through 6.6.x, we *strongly* recommend upgrading no more than five devices simultaneously.

Step 3 From the **Select Action** or **Select Bulk Action** menu, select **Upgrade Firepower Software**.

The Device Upgrade page appears, indicating how many devices you selected and prompting you to select a target version. The page has two panes: Device Selection on the left, and Device Details on the right. Click a device link in the Device Selection (such as '`4 devices`') to show the Device Details for those devices.

Note that if there is already an upgrade workflow in process, you must first either **Merge Devices** (add the newly selected devices to the previously selected devices and continue) or **Reset** (discard the previous selections and use only the newly selected devices).

Step 4 Verify your device selection.

To select additional devices, go back to the Device Management page—your progress will not be lost. To remove devices, click **Reset** to clear your device selection and start over.

Copy upgrade packages to devices.

Step 5 From the **Upgrade to** menu, select your target version.

The system determines which of your selected devices can be upgraded to that version. If any devices are ineligible, you can click the device link to see why. You do not have to remove ineligible devices if you don't want to; they will just not be included in the next step.

Note that the choices in the **Upgrade to** menu correspond to the device upgrade packages available to the system. If your target version is not listed, go to **System** > **Updates** and upload or specify the location of the correct upgrade package.

Step 6 For all devices that still need an upgrade package, click **Copy Upgrade Packages**, then confirm your choice.

To upgrade FTD, the software upgrade package must be on the appliance. Copying the upgrade package before upgrade reduces the length of your upgrade maintenance window.

Perform compatibility, readiness, and other final checks.

Step 7 For all devices that need to pass the readiness check, click **Run Readiness Check**, then confirm your choice.

Although you can skip checks by disabling the **Require passing compatibility and readiness checks option**, we recommend against it. Passing all checks greatly reduces the chance of upgrade failure. Do *not* deploy changes to, manually reboot, or shut down a device while running readiness checks. If a device fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, do not begin the upgrade. Instead, contact Cisco TAC.

Note that compatibility checks are automatic. For example, the system alerts you immediately if you need to upgrade FXOS on the Firepower 4100/9300, or if you need to deploy to managed devices.

Step 8 Perform final pre-upgrade checks.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks.

Step 9 If necessary, return to the Device Upgrade page.

Your progress should have been preserved. If it was not, someone else with Administrator access may have reset, modified, or completed the workflow.

Step 10 Click **Next**.

Upgrade.

Step 11 Verify your device selection and target version.

Step 12 Choose rollback options.

For major and maintenance upgrades, you can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

This option is not supported for patches.

Step 13 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

You can monitor upgrade progress in the Message Center. For information on traffic handling during the upgrade, see the Upgrade the Software chapter in the release notes.

Devices may reboot twice during the upgrade. This is expected behavior.

Verify success and complete post-upgrade tasks.

Step 14 Verify upgrade success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 15 (Optional) In high availability/scalability deployments, examine device roles.

The upgrade process switches device roles so that it is always upgrading a standby device or data unit. It does not return devices to the roles they had before upgrade. If you have preferred roles for specific devices, make those changes now.

Step 16 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 17 Complete any post-upgrade configuration changes described in the release notes.

Step 18 Redeploy configurations to the devices you just upgraded.

What to do next

(Optional) Clear the wizard by returning to the Device Upgrade page and clicking **Finish**. Until you do this, the Device Upgrade page continues to display details about the upgrade you just performed.

Upgrade Firepower Threat Defense with FMC (Version 6.0.1–6.7.0)

Use this procedure to upgrade FTD using the FMC's System Updates page. On this page, you can upgrade multiple devices at once only if they use the same upgrade package. You must upgrade the members of device clusters and high availability pairs at the same time.

Before you begin

- Decide whether you want to use this procedure. For FTD upgrades to Version 7.0.x we recommend you use the upgrade wizard instead; see Upgrade Firepower Threat Defense with FMC (Version 7.0.0), on page 24.
- Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.
- (Optional) Switch the active/standby roles of your high availability device pairs. Choose **Devices** > **Device Management**, click the **Switch Active Peer** icon next to the pair, and confirm your choice.

  The standby device in a high availability pair upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

Procedure

Step 1 Choose **System** > **Updates**.

Step 2 Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

Note
We *strongly* recommend upgrading no more than five devices simultaneously from the System Update page. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 3 (Version 6.7.0+) Choose rollback options.

For major and maintenance upgrades, you can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. Auto-cancel is not supported for patches.

Step 4 Click **Install**, then confirm that you want to upgrade and reboot the devices.

Some devices may reboot twice during the upgrade; this is expected behavior. Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see the *Upgrade the Software* chapter in the Cisco Firepower Release Notes for your target version.

Step 5 Monitor upgrade progress.

Caution
Do *not* deploy changes to, manually reboot, or shut down an upgrading device.

In most cases, do *not* restart an upgrade in progress. However, starting with major and maintenance FTD upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI. Note that by default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to *manually* cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

Step 6 Verify upgrade success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 7 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 8 Complete any post-upgrade configuration changes described in the release notes.

Step 9 Redeploy configurations to the devices you just upgraded.