Upgrade FTD

This chapter explains how to use a Version 6.2.3 FMC to upgrade threat defense. If your FMC is running a different version, or if you are using the cloud-delivered management center, see Is this Guide for You?.

Upgrade Checklist for FTD

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

✓	Action/Check	Details
	Assess your deployment.	Understanding where you are determines how you get to where you want to go. In addition to current version and model information, determine if your deployment is configured for high availability.
	Plan your upgrade path.	This is especially important for deployments, multi-hop upgrades, and situations where you need to upgrade operating systems or hosting environments. Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. See: • Upgrade Paths for FTD, on page 4 • Upgrade Paths for FXOS

✓	Action/Check	Details
	Read 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 these: • Software Upgrade Guidelines, for critical and release-specific upgrade guidelines. • , for new and deprecated features that have upgrade impact. Check all versions between your current and target version. • Cisco Firepower Release Notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool. • Cisco Firepower 4100/9300 FXOS Release Notes, for FXOS upgrade guidelines for the Firepower 4100/9300.
	Check appliance access.	Devices can stop passing traffic during the upgrade 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.
	Check bandwidth.	Make sure your management network has the bandwidth to perform large data transfers. Whenever possible, upload upgrade packages ahead of time. If you transfer an upgrade package to a device at the time of upgrade, insufficient bandwidth can extend upgrade time. See Guidelines for Downloading Data from the Firepower Managemen t 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 upgrades are likely to take. Consider the tasks you must perform in the window, and those you can perform ahead of time. See: • Traffic Flow and Inspection for Chassis Upgrades • Time and Disk Space Tests

Backups

With the exception of hotfixes, upgrade deletes all backups stored on the system. We *strongly* recommend you back up to a secure remote location and verify transfer success, both 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.

✓	Action/Check	Details
	Back up FTD.	If you have a Firepower 9300 with FTD and ASA logical devices running on separate modules, use ASDM or the ASA CLI to back up ASA configurations and other critical files, especially if there is an ASA configuration migration. See the *Software and Configurations* chapter in the Cisco ASA Series General Operations Configuration Guide.
	Back up FXOS on the Firepower 4100/9300.	

Upgrade Packages

Uploading upgrade packages to the system before you begin upgrade can reduce the length of your maintenance window.

Associated Upgrades

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

✓	Action/Check	Details
	Upgrade virtual hosting.	If needed, upgrade the hosting environment. If this is required, it is usually because you are running an older version of VMware and are performing a major upgrade.
	Upgrade firmware on the Firepower 4100/9300.	We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
	Upgrade FXOS on the Firepower 4100/9300.	Upgrading FXOS is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To minimize disruption, upgrade FXOS in FTD high availability pairs one chassis at a time. See Upgrade the Chassis on the Firepower 4100/9300.

Final Checks

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

✓	Action/Check	Details
	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.
	Deploy configurations.	Deploying configurations before you upgrade reduces the chance of failure. Deploying can affect traffic flow and inspection; see .

✓	Action/Check	Details
	Run readiness checks.	Passing readiness checks reduces the chance of upgrade failure.
	Check disk space.	Readiness checks include a disk space check. Without enough free disk space, the upgrade fails.
	Check running tasks.	Make sure essential tasks are complete, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed.

Upgrade Paths for FTD

Choose the upgrade path that matches your deployment.

Upgrade Path for FTD without FXOS

This table provides the upgrade path for FTD when you do not have to upgrade the operating system. This includes the Secure Firewall 3100 in appliance mode, Firepower 1000/2100 series, ASA-5500-X series, and the ISA 3000.

Note that if your current FTD 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.

Table 1: FTD Direct Upgrades

Current Version	Target Version
7.4	→ Any later 7.4.x release
7.3	Any of: → 7.4.x → Any later 7.3.x release
7.2	Any of: → 7.4.x → 7.3.x → Any later 7.2.x release **Note** The Firepower 1010E, introduced in Version 7.2.3, is not supported in Version 7.3. Support returns in Version 7.4.1.

Current Version	Target Version
7.1	Any of: → 7.4.x → 7.3.x → 7.2.x → Any later 7.1.x release
7.0 Last support for ASA 5508-X and 5516-X.	Any of: → 7.4.x → 7.3.x → 7.2.x → 7.1.x → Any later 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** The cloud-delivered Firewall Management Center cannot manage FTD 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 Version 7.2+.
6.7	Any of: → 7.2.x → 7.1.x → 7.0.x → Any later 6.7.x release
6.6 Last support for ASA 5525-X, 5545-X, and 5555-X.	Any of: → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Any later 6.6.x release

Current Version	Target Version
6.5	Any of: → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 Last support for ASA 5515-X.	Any of: → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Any of: → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 Last support for ASA 5506-X series.	Any of: → 6.6.x → 6.5 → 6.4 → 6.3

Upgrade Path for FTD with FXOS

This table provides the upgrade path for FTD on the Firepower 4100/9300.

Note that if your current FTD 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 2: FTD Direct Upgrades on the Firepower 4100/9300

Current Versions	Target Versions
FXOS 2.13 with threat defense 7.3	→ FXOS 2.13 with any later threat defense 7.3.x release
FXOS 2.12 with 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 threat defense 7.3.x → FXOS 2.12 with any later threat defense 7.2.x release
FXOS 2.11.1 with threat defense 7.1	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with any later threat defense 7.1.x release
FXOS 2.10.1 with threat defense 7.0	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with 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** The cloud-delivered Firewall Management Center cannot manage FTD 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 Version 7.2+.
FXOS 2.9.1 with threat defense 6.7	Any of: → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with any later threat defense 6.7.x release

Current Versions	Target Versions
FXOS 2.8.1 with threat defense 6.6	Any of: → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with any later threat defense 6.6.x release
FXOS 2.7.1 with threat defense 6.5	Any of: → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with threat defense 6.6.x

Upgrade Order for FTD High Availability with FXOS

Upgrade Packages for FTD

You use the same upgrade package for all models in a family or series. To find the correct one, select or search for your model on the Cisco Support & Download site, then browse to the software download page for the appropriate version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), software version, and build.

Note that upgrade packages from Version 6.2.1+ are signed, and terminate in .sh.REL.tar, as listed in the following table. If you are upgrading from an older version, download the package that terminates in .sh instead. The Cisco Support & Download site indicates the correct package for your version. Do not untar signed upgrade packages. Do not rename upgrade packages or transfer them by email.

Table 3: Software Upgrade Packages

Platform	Upgrade Package
ASA 5500-X series with FTD	Cisco_FTD_Upgrade-6.2.3-999.sh.REL.tar

Upload FTD Upgrade Packages to the FMC

Upgrade packages are signed tar archives (.tar). After you upload a signed package, the System Updates page can take extra time to load as the package is verified. To speed up the display, delete unneeded upgrade packages. Do not untar signed packages.

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

Step 2 Click **Upload Update**.

Step 3 For the **Action**, click the **Upload local software update package** radio button.

Step 4 Click **Choose File**.

Step 5 Browse to the package and click **Upload**.

Step 6 (Optional) Copy upgrade packages to managed devices.

If you do not need to enable revert and therefore plan to use the FTD upgrade wizard, the wizard will prompt you to copy the package. If you will use the System Updates page to upgrade because you want to enable revert, we recommend you copy upgrade packages to the devices now, as follows:

a) Click the **Push or Stage Update** icon next to the upgrade package you want to copy.

b) Choose destination devices.

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

c) Click **Push**.

Upload FTD Upgrade Packages to an Internal Server

Use this procedure to configure FTD devices to get upgrade packages from an internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC.

To configure this feature, you save a pointer (URL) to an upgrade package's location on the web server. The upgrade process will then get the upgrade package from the web server instead of the FMC. Or, you can use the FMC to copy the package before you upgrade.

Repeat this procedure for each upgrade package. You can configure only one location per upgrade package.

Before you begin

Copy the upgrade packages to an internal web server that your devices can access. For secure web servers (HTTPS), obtain the server's digital certificate (PEM format). You should be able to obtain the certificate from the server's administrator. You may also be able to use your browser, or a tool like OpenSSL, to view the server's certificate details and export or copy the certificate.

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

Step 2 Click **Upload Update**.

Choose this option even though you will not upload anything. The next page will prompt you for a URL.

Step 3 For the **Action**, click the **Specify software update source** radio button.

Step 4 Enter a **Source URL** for the upgrade package.

Provide the protocol (HTTP/HTTPS) and full path, for example:

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and the software version you are upgrading to. Make sure you enter the correct file name.

Step 5 For HTTPS servers, provide a **CA Certificate**.

This is the server's digital certificate you obtained earlier. Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines.

Step 6 Click **Save**.
The location is saved. Uploaded upgrade packages and upgrade package URLs are listed together, but are labeled distinctly.

Step 7 (Optional) Copy upgrade packages to managed devices.

If you do not need to enable revert and therefore plan to use the FTD upgrade wizard, the wizard will prompt you to copy the package. If you will use the System Updates page to upgrade because you want to enable revert, we recommend you copy upgrade packages to the devices now, as follows:

a) Click the **Push or Stage Update** icon next to the upgrade package you want to copy.
b) Choose destination devices.

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

c) Click **Push**.

Upgrade FTD with the Wizard

Use this procedure to upgrade FTD using a wizard. Note that you must still use **System** (⚙) > **Updates** to manage upgrade packages and to upgrade the FMC and older Classic devices.

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 and other users cannot start a new upgrade workflow. (Exception: if you are logged in with a CAC, your progress is cleared 24 hours after you log out.) If you need to reset someone else's workflow, you must have Administrator access. You can delete or deactivate the user, or update their user role so they no longer have permission to use **Devices** > **Device Upgrade**.

Note that neither your workflow nor threat defense upgrade packages are synchronized between high availability FMCs. In case of failover, you must recreate your workflow on the new active FMC, which includes uploading upgrade packages to the FMC and performing readiness checks. (Upgrade packages already copied to devices are not removed, but the FMC still must have the package or a pointer to its location.)

Note The wizard 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**.

Before you begin

Complete the pre-upgrade checklist. Make sure your deployment is healthy and successfully communicating.

Begin workflow.

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

Select devices to upgrade and copy upgrade packages.

Step 2 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.

Step 3 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 6.6.x or earlier, we *strongly* recommend upgrading no more than five devices simultaneously.

Step 4 From the **Select Action** or **Select Bulk Action** menu, select **Upgrade Firepower Software**.

The device upgrade wizard 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 pane (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 5 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.

Step 6 From the **Upgrade to** menu, select a 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; they are automatically excluded from upgrade.

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. If you are upgrading different device models and therefore need multiple upgrade packages, do this for all necessary upgrade packages before continuing with the next step.

Step 7 For all devices that still need an upgrade package, click **Copy Upgrade Package**, then confirm your choice.

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

Step 8 Click **Next**.

Perform compatibility, readiness, and other final checks.

Step 9 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, or if you need to deploy to managed devices.

Step 10 Perform final pre-upgrade checks.

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

Step 11 If necessary, return to **Devices** > **Device Upgrade**.

Step 12 Click **Next**.

Upgrade devices.

Step 13 Verify your device selection and target version.

Step 14 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 15 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

You can monitor overall upgrade progress in the Message Center. For detailed progress, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center. For information on traffic handling during the upgrade, see .

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

Verify success and complete post-upgrade tasks.

Step 16 Verify success.

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

Step 17 (Optional) In high availability/scalability deployments, examine device roles.

The upgrade process switches device roles so that it is always upgrading a standby unit or data node. 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 18 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 19 Complete any required post-upgrade configuration changes.

Step 20 Redeploy configurations to the devices you just upgraded.

What to do next

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

Upgrade FTD with System > Updates

Use this procedure to upgrade FTD using the System Updates page.

Before you begin

Complete the pre-upgrade checklist. Make sure your deployment is healthy and successfully communicating.

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

Step 2 Under Available Updates, click the **Install** icon next to the upgrade package.

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

The system displays a list of eligible devices, along with pre-upgrade compatibility check results. This precheck prevents you from upgrading if there are obvious issues that will cause your upgrade to fail.

Step 3 Select the devices you want to check and click **Check Readiness**.

Readiness checks assess preparedness for major and maintenance upgrades. The time required to run a readiness check varies depending on model. Do not manually reboot or shut down during readiness checks.

Under Readiness Checks on this page, you can view check status for your whole deployment, including checks in progress and failed checks. You can also use this page to easily re-run checks after a failure. Or, monitor readiness check progress in the Message Center.

If you cannot select an otherwise eligible device, make sure it passed compatibility checks. If a device fails readiness checks, correct the issues before upgrading.

Step 4 Choose the devices to upgrade.

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.

Important 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 5 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 6 Click **Install**, 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 .

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

Step 7 Verify success.

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

Step 8 (Optional) In high availability/scalability deployments, examine device roles.

The upgrade process switches device roles so that it is always upgrading a standby unit or data node. 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 9 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 10 Complete any required post-upgrade configuration changes.

Step 11 Redeploy configurations to the devices you just upgraded.