Planning Your Upgrade

Use this guide to plan and complete threat defense upgrades. Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. We also may provide hotfixes, which are minor updates that address particular, urgent issues.

Compatibility

Before you upgrade or reimage, make sure the target version is compatible with your deployment. If you cannot upgrade or reimage due to incompatibility, contact your Cisco representative or partner contact for refresh information.

For compatibility information, see:

- Cisco Secure Firewall Threat Defense Compatibility Guide
- Cisco Firepower 4100/9300 FXOS Compatibility

Upgrade Guidelines

See the release notes for release-specific upgrade warnings and guidelines, and for information on features and bugs with upgrade impact. For general information on time/disk space requirements and on system behavior during upgrade—which can include interruptions to traffic flow and inspection—see Troubleshooting and Reference.

Software Upgrade Guidelines

For release-specific upgrade warnings and guidelines, as well as features and bugs with upgrade impact, check all release notes between your current and target version: http://www.cisco.com/go/ftd-notes.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

In most cases, we recommend you use the latest build for your FXOS major version.

For release-specific FXOS upgrade warnings and guidelines, as well as features and bugs with upgrade impact, check all release notes between your current and target version: http://www.cisco.com/go/firepower9300-rns.

For firmware upgrade guidelines (for upgrades to FXOS 2.13 and earlier), see the firmware upgrade guide: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

Upgrade Path

Planning your upgrade path is especially important for large deployments, high availability/clustering, multi-hop upgrades, and situations where you need to coordinate chassis, hosting environment or other upgrades.

Supported Direct Upgrades

This table shows the supported direct upgrades for threat defense software. Note that although you can upgrade directly to maintenance (third-digit) releases, patches change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release.

For the Firepower 4100/9300, the table also lists companion FXOS versions. If a chassis upgrade is required, threat defense upgrade is blocked. In most cases we recommend the latest build in each version; for minimum builds see the Cisco Secure Firewall Threat Defense Compatibility Guide.

Table 1: Supported Direct Upgrades for Major and Maintenance Releases

Current Version	Target Threat Defense Version						
	***to* 7.7**	**7.6**	**7.4**	**7.3**	**7.2**	**7.1**	**7.0**
	Firepower 4100/9300 FXOS Version for Chassis Upgrades						
	***to* 2.17**	**2.16**	**2.14**	**2.13**	**2.12**	**2.11**	**2.10**
***from* 7.7**	**YES**	—	—	—	—	—	—
7.6	**YES**	**YES**	—	—	—	—	—
7.4	**YES**	**YES**	**YES ***	—	—	—	—
7.3	**YES**	**YES**	**YES**	**YES**	—	—	—
7.2	**YES**	**YES**	**YES**	**YES**	**YES**	—	—
7.1	—	—	—	—	—	—	—
7.0	—	—	**YES**	**YES**	**YES**	—	**YES**

* You cannot upgrade threat defense to Version 7.4.0, which is available as a fresh install on the Secure Firewall 4200 only. Instead, upgrade your devices to Version 7.4.1+.

Upgrade Order

Chassis Before Threat Defense

Some devices may require a chassis upgrade (FXOS and firmware) before you upgrade the software:

- Secure Firewall 3100/4200 in multi-instance mode: Any upgrade can require a chassis upgrade.

  Although you upgrade the chassis and threat defense separately, one package contains the chassis and threat defense upgrades and you perform both from the management center. The compatibility work is done for you. It is possible to have a chassis-only upgrade or a threat defense-only upgrade.

- Firepower 4100/9300: Major versions require a chassis upgrade.

Because you upgrade the chassis first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of threat defense. If the chassis is already well ahead of its devices, further chassis upgrades can be blocked. In this case perform a three (or more) step upgrade: devices first, then the chassis, then devices again. Or, perform a full reimage. In high availability or clustered deployments, upgrade one chassis at a time.

Chassis with High Availability/Clustered Threat Defense

When a chassis upgrade is required in high availability or clustered deployments, upgrade one chassis at a time.

Table 2: Chassis Upgrade Order for the Firepower 4100/9300

Threat Defense Deployment	Upgrade Order
Standalone	**1.** Upgrade chassis. **2.** Upgrade threat defense.
High availability	Upgrade both chassis before you upgrade threat defense. To minimize disruption, always upgrade the standby. **1.** Upgrade chassis with the standby. **2.** Switch roles. **3.** Upgrade chassis with the new standby. **4.** Upgrade threat defense.
Intra-chassis cluster (units on the same chassis)	**1.** Upgrade chassis. **2.** Upgrade threat defense.

Threat Defense Deployment	Upgrade Order
Inter-chassis cluster (units on different chassis)	Upgrade all chassis before you upgrade threat defense. To minimize disruption, always upgrade an all-data unit chassis. **1.** Upgrade the all-data unit chassis. **2.** Switch the control module to the chassis you just upgraded. **3.** Upgrade all remaining chassis. **4.** Upgrade threat defense.

Table 3: Chassis Upgrade Order for the Secure Firewall 3100/4200 in Multi-Instance Mode

Threat Defense Deployment	Upgrade Order
Standalone	**1.** Upgrade chassis. **2.** Upgrade threat defense.
High availability	Upgrade both chassis before you upgrade threat defense. **1.** Upgrade chassis. With the chassis upgrade wizard, you have three options: • Parallel upgrade: Not recommended for high availability. • Serial upgrade: Automatically fail over when the active unit goes down. We recommend you place the standby unit first in the upgrade order. • Two workflows (run the upgrade wizard twice): Upgrade the chassis with the standby, switch roles, and upgrade the chassis with the new standby. **2.** Upgrade threat defense.

Upgrade Packages

Managing Upgrade Packages with the Management Center

System (⚙) > **Product Upgrades** lists all upgrades that apply to you, with suggested releases specially marked. You can easily choose and direct-download packages from the internet to the management center, or upload packages you manually downloaded. For details, see the following table. For answers to common issues, see Troubleshooting Upgrade Packages.

Tip For devices with internet access, you can begin upgrade without downloading the package to the management center. The device will get the package at the appropriate time; see Copying Upgrade Packages to Devices, on page 5.

Table 4: Managing Upgrade Packages with the Management Center

To...	Do This...
Refresh the list of available upgrades.	Click **Refresh** ( ) at the bottom left of the page.
Download an upgrade package to the management center from the internet.	Click **Download** next to the upgrade package or version you want to download. Each family of devices has its own upgrade packages, so depending on your deployment you may need to download more than one upgrade package.
Manually upload an upgrade package to the management center.	Click **Add Upgrade Package** at the bottom right of the page, then **Choose File**. See: Upgrade Packages on Cisco.com, on page 8
Configure threat defense devices to get upgrade packages from an internal server.	Click **Add Upgrade Package** at the bottom right of the page, then **Specify Remote Location**. See: Copying Upgrade Packages to Devices from an Internal Server, on page 6
Delete upgrade packages from the management center.	Click the **Ellipsis (…)** next to the package or package version you want to delete and select **Delete**. This deletes the packages (or the pointer to the package) from the management center. It does not delete packages from any devices where you already copied them. In most cases, upgrading removes the related package from the upgraded appliance. However, for the Secure Firewall 3100/4200 in multi-instance mode, chassis upgrade packages must be removed manually. See Deleting Chassis Upgrade Packages from the Secure Firewall 3100/4200, on page 7.

Copying Upgrade Packages to Devices

To upgrade, the upgrade package must be on the device.

Copying Threat Defense Upgrade Packages

After you select devices to upgrade, the upgrade wizard prompts you to copy upgrade packages. Devices try the following sources in order. If one fails, in most cases the device tries the next one.

Internal server.

When configured, this takes priority. Recommended when it is not possible or practical to get the upgrade package from the internet or management center, for example, if devices do not have internet access, there is not enough disk space on the management center, or there is poor bandwidth between devices

and the download location. The cloud-delivered Firewall Management Center in particular has limited disk space for device upgrade packages.

If download from the internal server fails, newer devices (threat defense 7.6+ or chassis 7.4.1+) with internet access try that next. Older devices and devices without internet access try the management center.

See: Copying Upgrade Packages to Devices from an Internal Server, on page 6

Internet. Recommended in most cases.

Recommended when devices have internet access, with good bandwidth between devices and the download location. Internet access is tested weekly. If internet download fails, the device tries the management center. However, a device with internet access always tries the internet first. There is no way to disable this or force it to try the management center first. Not supported for hotfixes.

Management center.

Recommended when devices cannot reach the internet, but there is enough disk space on the management center, and good bandwidth between the management center and devices. You can also keep device upgrade packages on the management center as a fallback in case internal server or direct download fails.

The management center can get most device upgrade packages directly from the internet. If you are applying a hotfix, manually upload upgrade packages.

See: Managing Upgrade Packages with the Management Center, on page 4

Copying Chassis Upgrade Packages

For the Secure Firewall 3100/4200 in multi-instance mode, use the threat defense methods above. Note that these chassis upgrade packages are stored outside any application instances. This allows you to upgrade the chassis while also making the threat defense upgrade accessible to all instances. However, this means that you must manually remove unneeded chassis upgrade packages (instead of the upgrade process automatically removing them).

For Firepower 4100/9300 chassis upgrade packages, manually download the upgrade package from the Cisco Support & Download site, then use the chassis manager or CLI (FTP, SCP, SFTP, or TFTP) to copy the package to the device. See Upgrade Packages on Cisco.com, on page 8 and the upgrade procedure for your deployment.

Copying Upgrade Packages to Devices from an Internal Server

Managed devices without internet access must get upgrade packages from either the management center or an internal server. An internal server is especially useful if you have limited bandwidth between the management center and its devices (or, between the devices and the internet download location). It also saves space on the management center. The cloud-delivered Firewall Management Center in particular has limited disk space for device upgrade packages.

After you get upgrade packages (Upgrade Packages on Cisco.com, on page 8) and set up your server, configure pointers. On the management center, start like you are uploading a package: on the Product Upgrades page (**System** (⚙) > **Product Upgrades**), click **Add Upgrade Package**. But instead of choosing a file on your computer, click **Specify Remote Location** and provide the appropriate details. When it is time to get the package, the device will copy it from the internal server.

Note When configured, an internal server takes priority. If copying from the internal server fails, newer devices (threat defense 7.6+ or chassis 7.4.1+) with internet access try the internet, then the management center. There is no way to disable this or force it to try the management center first. Older devices and devices without internet access just try the management center.

Table 5: Options for Copying Threat Defense Upgrade Packages from an Internal Server

Field	Description
URL	The source URL, including protocol (HTTP/HTTPS) and full path to the upgrade package; for example: `https://internal_web_server/upgrade_package.sh.REL.tar`.
CA Certificates	For secure web servers (HTTPS), the server's digital certificate (PEM format). Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines. 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.

Deleting Chassis Upgrade Packages from the Secure Firewall 3100/4200

For the Secure Firewall 3100/4200 in multi-instance mode, chassis upgrade packages are stored outside any application instances. This allows you to upgrade the chassis while also making the threat defense upgrade accessible to all instances. However, this means that you must manually remove unneeded chassis upgrade packages (instead of the upgrade process automatically removing them).

Note You must remove unneeded chassis upgrade packages in the context of a chassis upgrade workflow. The best time to do this is when you are upgrading to the next version.

Use this procedure to delete chassis upgrade packages when you are not actively upgrading the chassis.

Before you begin

Download (or configure a pointer to) at least one chassis upgrade package other than the one corresponding to the package you want to delete.

Procedure

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

Step 2 Select the chassis that have the unneeded packages and under **Select Action** or **Select Bulk Action**, choose **Upgrade FXOS and Firmware (Chassis Only)**.

The chassis upgrade wizard appears.

Step 3 Choose a target version from the **Upgrade to** menu.

Choose any version other than the one corresponding to the package you want to delete. You will not be upgrading to this version so it doesn't matter which you choose.

Step 4 In the Device Selection pane, click the message that says: `X devices have packages that might not be needed`.

The chassis that have unneeded packages are listed in the Device Details pane. Note that you cannot delete a package for the version the chassis is currently running, nor a package for the "target version" you selected. Only chassis with packages other than these are counted.

Step 5 In the Device Details pane, select a chassis, click **Manage Upgrade Packages on Device**, select the packages you want to remove and click **Remove**.

Repeat this step for each chassis you want to clean up.

Step 6 Back in the chassis upgrade wizard, click **Reset** to reset the workflow.

Upgrade Packages on Cisco.com

Manually download upgrade packages when you cannot or do not want to direct-download for another reason; for example, for hotfixes, Firepower 4100/9300 chassis upgrades, or if you use an internal server.

Packages are available on the Cisco Support & Download site: https://www.cisco.com/go/ftd-software

Threat Defense Packages

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, 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, software version, and build. Upgrade packages are signed, and terminate in .sh.REL.tar. Do not untar or rename them.

Table 6: Upgrade Packages

Platform	Package	Notes
Threat Defense Packages		
Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-*Version-build*.sh.REL.tar	—
Firepower 2100	Cisco_FTD_SSP-FP2K_Upgrade-*Version-build*.sh.REL.tar	Cannot upgrade past Version 7.4.x.
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-*Version-build*.sh.REL.tar	—
Secure Firewall 1200	Cisco_Secure_FW_TD_1200-*Version-build*.sh.REL.tar	—
Secure Firewall 3100	Cisco_FTD_SSP-FP3K_Upgrade-*Version-build*.sh.REL.tar	—
Secure Firewall 4200	Cisco_Secure_FW_TD_4200-*Version-build*.sh.REL.tar	—

Platform	Package	Notes
ASA 5500-X	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar	Cannot upgrade past Version 7.0.x.
Threat defense virtual	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar	—
ISA 3000 with FTD	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar	—

Chassis Packages for the Secure Firewall 3100/4200

For the Secure Firewall 3100/4200 in multi-instance mode, the threat defense and chassis upgrades share a package.

Chassis Packages for the Firepower 4100/9300

To find the correct FXOS package, 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 package is listed along with recovery and MIB packages. Firmware is included in FXOS upgrades to 2.14.1+.

Table 7: FXOS Packages

Platform	Package
Firepower 4100/9300	fxos-k9.*fxos_version*.SPA

Firmware is included in FXOS upgrades to 2.14.1+ (companion to threat defense 7.4.1). If you are upgrading older devices, select or search for your device model and browse to the *Firepower Extensible Operating System* download page. Firmware packages are under *All Releases* > *Firmware*.

Table 8: Firmware Packages

Platform	Package
Firepower 4100	fxos-k9-fpr4k-firmware.*firmware_version*.SPA
Firepower 9300	fxos-k9-fpr9k-firmware.*firmware_version*.SPA

Upgrade Readiness

Network and Infrastructure Checks

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. You should also able to access the management center's management interface without traversing the device.

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 or even cause the upgrade to time out. See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

Configuration and Deployment Checks

Configurations

Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes. Resolve any change management workflows. Deploy configuration changes. Note that you will need to deploy again after upgrade.

Deploying typically restarts Snort, which can affect traffic flow and inspection; see Traffic Flow and Inspection when Deploying Configurations.

Deployment Health

Make sure your deployment is healthy and successfully communicating. If there are any issues reported by the health monitor, resolve them before continuing.

Some failed health tests can prevent you from upgrading or cause upgrade failure. With the exception of NTP issues that you can resolve yourself, contact Cisco TAC if your deployment is failing any of the following tests. Results are reported on the Health Status (Home) page of the health monitor: **System** (⚙) > **Health** > **Monitor**.

Note Disabling these regular health tests does not prevent the system from enforcing them before upgrade. If there are no existing results, readiness checks will run as part of the upgrade, increasing upgrade time.

Table 9: Upgrade-Related Health Tests

Health Test	Description
Database	Monitors database schema and configuration data (*EO*) integrity.
Disk Status	Monitors disk and RAID controller health for hardware devices.
Disk Usage	Monitors device disk usage. The upgrade calculates how much disk space it needs; not having enough will prevent upgrade. If this module is alerting before you begin upgrade, you probably do not have enough. On device health dashboards, the Disk Usage widget has a **Clear disk space** button that safely removes unneeded files such as old backups, content updates, and troubleshooting files.
FXOS Health	Monitors the FXOS httpd service on FXOS-based devices. Upgrade will fail without this service running.

Health Test	Description
Time Synchronization Status	Monitors device NTP synchronization. Being out of sync can cause upgrade failure. The system only alerts when you are offset by more than 10 seconds, so we recommend you manually check for a smaller offset (click **see more** next to the test results).

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 any 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.

Table 10: Backups

Backup	Guide
Threat defense	Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Security Cloud Control: *Backup/Restore* Note that backup is not supported in all cases, for example, for threat defense virtual in the public cloud. But if you can back up, you should.
Secure Firewall 3100/4200 chassis	Managing Firewall Threat Defense with Cloud-Delivered Firewall Management Center in Cisco Security Cloud Control: *Multi-Instance Mode for the Secure Firewall 3100/4200*
Firepower 4100/9300 chassis	Cisco Firepower 4100/9300 FXOS Configuration Guide: *Configuration Import/Export*
ASA on a Firepower 9300 chassis	Cisco ASA Series General Operations Configuration Guide: *Software and Configurations* For a Firepower 9300 chassis with threat defense and ASA logical devices, use ASDM or the ASA CLI to back up ASA configurations and other critical files, especially if there is an ASA configuration migration.