Planning Your Upgrade

Use this guide to plan and complete threat defense and management center 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.

Is This Guide for You?

The procedures in this guide are for:

- Management center: Upgrading a management center that is *currently running* Version 7.4.1–7.4.x.
- Threat defense: Upgrading devices *using* a management center that is currently running Version 7.4.1–7.4.x.

This means that after you use this guide to upgrade the management center, you will use a *different guide* to upgrade threat defense.

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 Management Center Compatibility Guide
- 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, see Troubleshooting and Reference.

Software Upgrade Guidelines

For release-specific upgrade warnings and guidelines, as well as features and bugs with upgrade impact, see the threat defense release notes. 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 FXOS build in each major version. For release-specific FXOS upgrade warnings and guidelines, as well as features and bugs with upgrade impact, see the FXOS release notes. 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, multi-hop upgrades, and situations where you need to coordinate chassis, hosting environment or other upgrades.

Upgrading the Management Center

The management center must run the same or newer version as its devices. Upgrade the management center to your target version first, then upgrade devices. If you begin with devices running a much older version than the management center, further management center upgrades can be blocked. In this case perform a three (or more) step upgrade: devices first, then the management center, then devices again.

Upgrading Threat Defense with Chassis Upgrade

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

- Secure Firewall 3100 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.

Supported Direct Upgrades

This table shows the supported direct upgrades for management center and threat defense software. Note that although you can upgrade directly to major and maintenance 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 Software Version									
	7.4	7.3	7.2	7.1	7.0	6.7	6.6	6.5	6.4	6.3
	Firepower 4100/9300 FXOS Version									
	2.14	2.13	2.12	2.11	2.10	2.9	2.8	2.7	2.6	2.4
7.4	YES †	—	—	—	—	—	—	—	—	—
7.3	YES	YES	—	—	—	—	—	—	—	—
7.2	YES	YES	YES	—	—	—	—	—	—	—
7.1	YES	YES	YES	YES	—	—	—	—	—	—
7.0	YES	YES	YES	YES	YES	—	—	—	—	—
6.7	—	— *	YES	YES	YES	YES	—	—	—	—
6.6	—	—	YES	YES	YES	YES	YES	—	—	—
6.5	—	—	—	YES	YES	YES	YES	—	—	—
6.4	—	—	—	—	YES	YES	YES	YES	—	—
6.3	—	—	—	—	—	YES	YES	YES	YES	—
6.2.3	—	—	—	—	—	—	YES	YES	YES	YES

* You cannot upgrade from Version 6.7.x to 7.3.x. You can, however, manage Version 6.7.x devices with a Version 7.3.x management center.

† 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 management center and devices to Version 7.4.1+.

Upgrade Order for Threat Defense with Chassis Upgrade and High Availability/Clusters

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 with Management Center

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.
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 in Multi-Instance Mode with Management Center

Threat Defense Deployment	Upgrade Order
Standalone	1. Upgrade chassis. 2. Upgrade threat defense.

Threat Defense Deployment	Upgrade Order
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

Manage upgrade packages on **System** (⚙) > **Product Upgrades**.

The page lists all upgrade packages that apply to you, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, or upload packages you manually downloaded: Upgrade Packages on Cisco.com, on page 10.

Table 4: Managing Upgrade Packages with the Management Center

To...	Do This...
Refresh the list of available upgrade packages.	Click **Refresh** (↻) at the bottom left of the page.
Download an upgrade package to the management center from Cisco.	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**.
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 7.

To...	Do This...
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. For management centers in high availability, it does not delete the package from the peer. In most cases, upgrading removes the related package from the upgraded appliance. However, for the Secure Firewall 3100 in multi-instance mode, chassis upgrade packages must be removed manually; see Deleting Chassis Upgrade Packages from the Secure Firewall 3100, on page 9.

Copying Upgrade Packages to Devices

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

Copying Threat Defense and Secure Firewall 3100 Chassis Upgrade Packages

For threat defense and Secure Firewall 3100 chassis upgrades, the easiest way to do this is to use the Product Upgrades page (**System** (⚙) > **Product Upgrades** on the management center to download the upgrade package from Cisco, then let the upgrade wizard prompt you to copy the package over.

Note that for the Secure Firewall 3100 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).

The following table goes into more details about this and your other options.

Table 5: Copying Threat Defense and Secure Firewall 3100 Chassis Upgrade Packages to Managed Devices

Requirements	When to Use
Cisco → Management Center → Devices Major, maintenance, or patch upgrade (not a hotfix) that applies to the device *right now*. Management center can access the Cisco Support & Download site. Adequate disk space on the management center. Adequate bandwidth between the management center and devices.	Strongly recommended when all requirements are met. See: Managing Upgrade Packages with the Management Center, on page 5

Requirements	When to Use
Cisco → Your Computer → Management Center → Devices Adequate disk space on the management center. Adequate bandwidth between management center and devices.	You meet disk space and bandwidth requirements, but either the management center cannot access the Cisco Support & Download site, or you are applying a hotfix. See: Upgrade Packages on Cisco.com, on page 10
Cisco → Your Computer → Internal Server → Devices Internal web server that devices can access.	You do not meet disk space requirements and/or bandwidth requirements (regardless of support site access or upgrade type). See: Copying Upgrade Packages to Devices from an Internal Server, on page 7
Device → Device Version 7.2+ standalone devices managed by the same standalone management center. At least one device that has obtained the upgrade package by another method.	You need to copy the upgrade package to devices without relying on the management center to mediate the transfer. See: Copy Threat Defense Upgrade Packages between Devices, on page 8

Copying Firepower 4100/9300 Chassis Upgrade Packages

For Firepower 4100/9300 chassis upgrade packages, download the upgrade package from Cisco, 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 10 and the upgrade procedure for your deployment.

Copying Upgrade Packages to Devices from an Internal Server

You can store threat defense upgrade packages on an internal server instead of the management center. This is especially useful if you have limited bandwidth between the management center and its devices. It also saves space on the management center.

After you get the packages from Cisco and set up your server, configure pointers to them. On the management center, start like you are uploading a 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.

Table 6: 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.`

Field	Description
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.

Copy Threat Defense Upgrade Packages between Devices

Instead of copying upgrade packages to each device from the management center or internal web server, you can use the threat defense CLI to copy upgrade packages between devices ("peer to peer sync"). This secure and reliable resource-sharing goes over the management network but does not rely on the management center. Each device can accommodate 5 package concurrent transfers.

This feature is supported for Version 7.2.x–7.4.x standalone devices managed by the same Version 7.2.x–7.4.x standalone management center. It is not supported for:

- Container instances.
- Device high availability pairs and clusters. These devices get the package from each other as part of their normal sync process. Copying the upgrade package to one group member automatically syncs it to all group members.
- Devices managed by high availability management centers.
- Devices managed by the cloud-delivered Firewall Management Center, but added to an on-prem management center in analytics mode.
- Devices in different domains, or devices separated by a NAT gateway.
- Devices upgrading from Version 7.1 or earlier, regardless of management center version.

Repeat the following procedure for all devices that need the upgrade package.

Before you begin

- Upload the threat defense upgrade package to the management center or to an internal server.
- Copy the upgrade package to at least one device.

Step 1 As `admin`, SSH to any device that needs the package.

Step 2 Enable the feature.

configure p2psync enable

Step 3 If you do not already know, determine where you can get the upgrade package you need.

show peers: Lists the other eligible devices that also have this feature enabled.

show peer details *ip_address*: For the device at the IP address you specify, list the available upgrade packages and their paths.

Step 4 Copy the package from any device that has the package you need, by specifying the IP address and path you just discovered.

sync-from-peer *ip_address package_path*

After you confirm that you want to copy the package, the system displays a sync status UUID that you can use to monitor this transfer.

Step 5 Monitor transfer status from the CLI.

show p2p-sync-status: Shows the sync status for the last five transfers to this device, including completed and failed transfers.

show p2p-sync-status *sync_status_UUID*: Shows the sync status for a particular transfer to this device.

Deleting Chassis Upgrade Packages from the Secure Firewall 3100

For the Secure Firewall 3100 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.

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 from Cisco when the system cannot access the Cisco Support & Download site, or when you cannot direct-download for another reason; for example, for hotfixes. You must also manually obtain upgrade packages if you plan to configure devices to get them from an internal server. And, you must manually obtain chassis upgrade packages for the Firepower 4100/9300.

Packages are available on the Cisco Support & Download site:

- Management Center: https://www.cisco.com/go/firepower-software
- Threat Defense: https://www.cisco.com/go/ftd-software

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

Table 7: Upgrade Packages

Platform	Package	Notes
Management Center Packages		
Management center hardware Management center virtual	Cisco_Secure_FW_Mgmt_Center_Upgrade-*Version-build*.sh.REL.tar	—
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.
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	—
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-*Version-build*.sh.REL.tar	—
ASA 5500-X	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar	Cannot upgrade past Version 7.0.x.

Platform	Package	Notes
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

For the Secure Firewall 3100 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 8: 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 9: 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 Managemen t 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.

You will need to deploy again after upgrade. Deploying can affect traffic flow and inspection; see the appropriate upgrade guide for details: Cisco Secure Firewall Threat Defense: Install and Upgrade Guides.

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. You should especially make sure all appliances are synchronized with any NTP server you are using to serve time. Although the health monitor alerts if clocks are out of sync by more than 10 seconds, you should still check manually. Being out of sync can cause upgrade failure.

To check time:

- Management Center: Choose **System** (⚙) > **Configuration** > **Time**.
- Threat Defense: Use the **show time** CLI command.

Running and Scheduled 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.

Upgrades automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. If you do not want this to happen, check for tasks that are scheduled to run during the upgrade and cancel or postpone them.

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. Back up the management center after you upgrade its managed devices, so your new management center backup file 'knows' that its devices have been upgraded.

Table 10: Backups

Backup	Guide
Management center	Cisco Secure Firewall Management Center Administration Guide: *Backup/Restore* We recommend you back up configurations and events.
Threat defense	Cisco Secure Firewall Management Center Administration Guide: *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 chassis	Cisco Secure Firewall Management Center Device Configuration Guide: *Multi-Instance Mode for the Secure Firewall 3100*
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.

Software Upgrade Readiness Checks

Besides the checks you perform yourself, the system can also check its own upgrade readiness. The threat defense and management center upgrade wizards prompt you to run the checks at the appropriate time. For the management center, passing readiness checks is not optional. If you fail readiness checks, you cannot upgrade. For threat defense, you can disable this requirement although we recommend against it. Passing all checks greatly reduces the chance of upgrade failure. If the checks expose issues that you cannot resolve, do not begin the upgrade.

You can run readiness checks outside a maintenance window. The time required to run a readiness check varies depending on model and database size. Do not manually reboot or shut down during readiness checks. For high availability management centers, do not run readiness checks on both peers at the same time.