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 7.2.6–7.2.x.
- Threat defense: Upgrading devices *using* a management center that is currently running Version 7.2.6–7.2.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—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 Guidelines for Threat Defense Virtual

Upgrade does not change the serial number or UUID of threat defense virtual instances.

Update base image and template image ID before cluster upgrade

Before you upgrade a cluster in the public cloud, copy the target version image to your cloud image repository and update the image ID in the cluster deployment template (we actually recommend replacing the existing template with a modified copy). This ensures that after the upgrade, new instances — for example, instances launched during cluster scaling — will use the correct version. If the marketplace does not have the image you need, such as when the cluster has been patched, create a custom image from a snapshot of a standalone threat defense virtual instance running the correct version, with no instance-specific (day 0) configurations.

Suspend health checks before autoscaled cluster upgrade

For threat defense virtual for AWS, suspend the HealthCheck and ReplaceUnhealthy processes before autoscaled cluster upgrade. This ensures that instances are not terminated by the Auto Scaling group during the post-upgrade reboot. You can resume the suspended processes afterwards. For instructions, see the Amazon EC2 Auto Scaling user guide: Suspend and resume Amazon EC2 Auto Scaling processes.

Upgrade Path

Planning your upgrade path and order 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 Upgrades

This table shows the supported direct upgrades for management center and threat defense software. You can upgrade directly to major (first and second-digit) and maintenance (third-digit) releases.

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								
	to 7.7	7.6	7.4	7.3	7.2	7.1	7.0	6.6	6.4
	Firepower 4100/9300 FXOS Version for Chassis Upgrades								
	to 2.17	2.16	2.14	2.13	2.12	2.11	2.10	2.8	2.6
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	—	YES	YES	YES	YES	YES	—	—	—
7.0	—	—	YES	YES	YES	YES	YES	—	—
6.6	—	—	—	—	YES	YES	YES	YES	—
6.4	—	—	—	—	—	—	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 management center and devices to Version 7.4.1+.

Supported Patches

Patches change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release. Although a patched device (fourth-digit) can be managed with an unpatched management center, fully patched deployments undergo enhanced testing.

Choosing a Maintenance Release

You can upgrade directly to major (first and second-digit) and maintenance (third-digit) releases. However, features, enhancements, and critical fixes included in maintenance releases can skip future releases, depending on release date, release type (short term vs. long term), and other factors. To minimize upgrade and other impact, do not upgrade to a release that deprecates features or fixes.

Important In most cases, we recommend you go directly to the latest maintenance release in your chosen major version.

If you cannot go to the latest maintenance release, at least make sure your target version was released on a date after your current version. That is, if your current version is ***not*** listed next to your target version in the following table, choose a later target.

Table 2: Released Before Version 7.2.x, by Date

Target Version		**Current Version: Is yours listed?**				
		***from* 6.6**	**6.7**	**7.0**	**7.1**	**7.2**
***to* 7.2.10**	2025-05-22	6.6.0–6.6.7	6.7.0	7.0.0–7.0.7	7.1.0	7.2.0–7.2.9
7.2.9	2024-10-22	6.6.0–6.6.7	6.7.0	7.0.0–7.0.6	7.1.0	7.2.0–7.2.8
7.2.8	2024-06-24	6.6.0–6.6.7	6.7.0	7.0.0–7.0.6	7.1.0	7.2.0–7.2.7
7.2.7	2024-04-29	6.6.0–6.6.7	6.7.0	7.0.0–7.0.6	7.1.0	7.2.0–7.2.6
7.2.6 *	2024-03-19	—	—	—	—	—
7.2.5	2023-07-27	6.6.0–6.6.7	6.7.0	7.0.0–7.0.6	7.1.0	7.2.0–7.2.4
7.2.4	2023-05-03	6.6.0–6.6.7	6.7.0	7.0.0–7.0.5	7.1.0	7.2.0–7.2.3
7.2.3	2023-02-27	6.6.0–6.6.7	6.7.0	7.0.0–7.0.5	7.1.0	7.2.0–7.2.2
7.2.2	2022-11-29	6.6.0–6.6.7	6.7.0	7.0.0–7.0.5	7.1.0	7.2.0–7.2.1
7.2.1	2022-10-03	6.6.0–6.6.7	6.7.0	7.0.0–7.0.4	7.1.0	7.2.0
7.2.0	2022-06-06	6.6.0–6.6.5	6.7.0	7.0.0–7.0.2	7.1.0	—

* Version 7.2.6 is longer available.

If you are running a patch, you may also want to check that the patch was also released after your target version, depending on the included fixes. For a full list of release dates including patches, see Cisco Secure Firewall Management Center New Features by Release.

Upgrade Order

Management Center Before Devices

The management center should run the same or newer version as its devices. This is because features and resolved issues often require the latest version on both the management center and its devices, including patches.

Upgrade the management center first—you will still be able to manage older devices, usually a few major versions back. 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.

Note You cannot upgrade a device past the management center to a newer major or maintenance version. Although a patched device (fourth-digit) can be managed with an unpatched management center, fully patched deployments undergo enhanced testing.

Chassis Before Threat Defense

For the Firepower 4100/9300, major versions require a FXOS upgrade. You should also check for firmware upgrades.

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. For high availability, although it is best practice to always upgrade the standby, a chassis could have both standby and active instances (belonging to different high availabilty pairs). In that case, any active units on the upgrading chassis automatically fail over. For clustering, the same applies: it is always best to upgrade an all-data unit chassis.

Before upgrade, high availability pairs and clusters should be in sync, not split brain, and so on. Threat defense upgrades will not proceed for most issues of this type, but the chassis is not aware of the status of its instances. This means that even if you upgrade the chassis one at a time, you can still experience disruption if you do not make sure your deployment is healthy before each chassis upgrade.

Table 3: Chassis Upgrade Order for the Firepower 4100/9300

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. 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.

Upgrade Packages

Managing Upgrade Packages with the Management Center

If the management center can reach the internet, **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.

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.

To...	Do This...
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 10
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 8
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 center in high availability, it does not delete the package from the peer. In most cases, upgrading removes the related package from the upgraded appliance.

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.

Internal server.

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

See: Copying Upgrade Packages to Devices from an Internal Server, on page 8

Management center.

Recommended when there is enough disk space on the management center, and good bandwidth between the management center and devices.

The management center can get most device upgrade packages directly from the internet. If the management center cannot reach the internet, or you are applying a hotfix, manually upload upgrade packages.

See: Managing Upgrade Packages with the Management Center, on page 6

Tip Version 7.2.0–7.4.x standalone devices managed by the same standalone management center can copy devices to each other without relying on the management center to mediate the transfer; see Copy Threat Defense Upgrade Packages between Devices, on page 8.

Copying Chassis Upgrade Packages

For the Secure Firewall 3100 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 10 and the upgrade procedure for your deployment.

Copying Upgrade Packages to Devices from an Internal Server

Managed devices 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. It also saves space on the management center.

After you get upgrade packages (Upgrade Packages on Cisco.com, on page 10) 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.

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.

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 7.0.x.
- Devices upgrading from Version 7.1 or earlier, regardless of management center version.
- Devices running Version 7.6+.

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.

Procedure

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.

Upgrade Packages on Cisco.com

Manually download upgrade packages when the system cannot reach the internet, or 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:

- 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, 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.

Note that a newer management center can manage older devices (and apply maintenance releases and patches to them). For older devices not listed here, see the management center upgrade guide corresponding to the last supported device version.

Table 6: Upgrade Packages

Platform	Package
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
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
ISA 3000 with FTD	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar
Threat defense virtual	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar

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.

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. 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 or on the Device Management page, 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**.

Table 9: Upgrade-Related Health Tests

Health Test	Description
Disk Status	Monitors disk and RAID controller health for hardware devices.
Disk Usage	Monitors 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.
Firewall Threat Defense HA (management center and devices) Cluster/HA Failure Status (devices)	High availability pairs and clusters should be in sync, not split brain, and so on. Threat defense upgrades will not proceed for most issues of this type. However, for the Firepower 4100/9300 and Secure Firewall 3100 in multi-instance mode, the chassis is not aware of the status of its instances. This means that even if you upgrade the chassis one at a time, you can still experience disruption if you do not make sure your deployment is healthy before each chassis upgrade.
Time Server Status (management center) Time Synchronization Status (devices)	Monitors 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).

Running Tasks and Scheduled Tasks

Make sure essential tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed.

Upgrades from Version 6.6.3+ 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 (or if you are upgrading from an earlier version), 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.
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.