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, make sure the target version is compatible with your deployment. If you cannot upgrade 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

Important Upgrade Guidelines

Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade.

Threat Defense Upgrade Guidelines and Bugs

For release-specific upgrade guidelines, including features with upgrade impact, check the release notes for your target version. For bugs that could affect your deployment, check all release notes between your current and target version.

Table 1: Cisco Secure Firewall Threat Defense Release Notes

Target Version	Release Notes
7.4.x	https://cisco.com/go/fmc-ftd-release-notes-74
7.3.x	https://cisco.com/go/fmc-ftd-release-notes-73
7.2.x	https://cisco.com/go/fmc-ftd-release-notes-72
7.1.x	Cisco Firepower Release Notes, Version 7.1.x
7.0.x	Cisco Firepower Release Notes, Version 7.0.x

Chassis Upgrade Guidelines for the Firepower 4100/9300

For release-specific FXOS upgrade guidelines, check the release notes for your target version. For bugs that could affect your deployment, check the release notes between your current and target version.

Table 2: Cisco Firepower 4100/9300 FXOS Release Notes

Target Version	Release Notes
2.14	Cisco Firepower 4100/9300 FXOS Release Notes, 2.14(1)
2.13	Cisco Firepower 4100/9300 FXOS Release Notes, 2.13
2.12	Cisco Firepower 4100/9300 FXOS Release Notes, 2.12
2.10	Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1)

For firmware upgrade guidelines, check 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 related upgrades—operating systems, firmware, chassis, hosting environments, and so on.

Upgrade Path for Threat Defense

This table lists the minimum version to upgrade threat defense. If you are not running the minimum version, you will need to perform a multi-step upgrade. If a chassis upgrade is required, threat defense upgrade is blocked; see Upgrade Path for Threat Defense with Chassis Upgrade, on page 3.

Table 3: Minimum Version to Upgrade Threat Defense

Target Version	Minimum Version to Upgrade
7.4	7.0.3

Target Version	Minimum Version to Upgrade
7.3	7.0.3
7.2	7.0.3

Upgrade Path for Threat Defense with Chassis Upgrade

For the Firepower 4100/9300, major threat defense upgrades require chassis (FXOS and firmware) upgrades. Maintenance releases and patches rarely do. Chassis upgrades to FXOS 2.14.1+ include firmware, otherwise, see the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

Because you upgrade the chassis first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" ofthreat defense. If the chassis is already well ahead of its devices, further chassis upgrades can be blocked. In this case you will need to perform a three (or more) step upgrade: devices first, then the chassis, then devices again. In high availability or clustered deployments, upgrade one chassis at a time; see Upgrade Path for High Availability or Clustered Threat Defense with Chassis Upgrade, on page 3.

This table lists the minimum versions to upgrade threat defense when a chassis upgrade is required.

Table 4: Minimum Versions to Upgrade Threat Defense Chassis

Target Versions	Minimum Versions to Upgrade
Threat Defense 7.4 on FXOS 2.14.1.131+	Threat Defense 7.0.3 on FXOS 2.10
Threat Defense 7.3 on FXOS 2.13.0.198+	Threat Defense 7.0.3 on FXOS 2.10
Threat Defense 7.2 on FXOS 2.12.0.31+	Threat Defense 7.0.3 on FXOS 2.10

Upgrade Path for High Availability or Clustered Threat Defense with Chassis Upgrade

In high availability or clustered deployments, upgrade one chassis at a time.

Table 5: 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

Uploading and Downloading Upgrade Packages to 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 8.

Table 6: Managing Upgrade Packages on 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.

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**.
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 Copy Upgrade Packages from an Internal Server, on page 6.
Delete an upgrade package from the management center.	Click the **Ellipsis (…)** next to the package you want to delete and select **Delete**. This deletes the package (or the pointer to the package) from the management center. It does not delete the package from any devices where you already copied the package. In most cases, upgrading threat defense removes the related upgrade package from the device.

Copying Upgrade Packages to Managed Devices

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

Copying Threat Defense Upgrade Packages

For threat defense 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.

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

Table 7: Copying Threat Defense 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*. Adequate disk space on the management center. Adequate bandwidth between the management center and devices.	Strongly recommended when all requirements are met. See: Uploading and Downloading Upgrade Packages to the Management Center, on page 4

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 you cannot direct-download; for example, for device hotfixes. See: Upgrade Packages on Cisco.com, on page 8
Cisco → Your Computer → Internal Server → Devices Internal web server that devices can access.	You do not meet disk space requirements and/or bandwidth requirements. The cloud-delivered Firewall Management Center in particular has limited disk space for device upgrade packages. See: Copy Upgrade Packages from an Internal Server, on page 6
Device → Device Version 7.2+ standalone devices managed by the same 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 7

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 8 and the upgrade procedure for your deployment.

Copy Upgrade Packages 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 8: 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+ standalone devices managed by the same 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 added to an on-prem management center in analytics mode.
- Devices separated by a NAT gateway.
- Devices upgrading from Version 7.0.x.

Repeat the following procedure for all devices that need the upgrade package. For detailed information on all the CLI commands associated with this feature, see the Cisco Secure Firewall Threat Defense Command Reference.

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.

Upgrade Packages on Cisco.com

Manually download upgrade packages from Cisco when you cannot direct-download; 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: 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 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. Upgrade packages are signed, and terminate in .sh.REL.tar. Do not untar or rename them.

Table 9: Threat Defense Packages

Platform	Package
Firepower 1000 series	Cisco_FTD_SSP-FP1K_Upgrade-*Version-build*.sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP-FP2K_Upgrade-*Version-build*.sh.REL.tar
Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-*Version-build*.sh.REL.tar
Secure Firewall 4200 series	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 series	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar
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 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 10: FXOS Packages

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

Upgrades to FXOS 2.14.1+ include firmware. If you are upgrading to an earlier version of FXOS, 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 11: 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.

Note You will need to deploy again after upgrade. Deploying can affect traffic flow and inspection; see Traffic Flow and Inspection for Threat Defense Upgrades.

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.

Table 12: Backups

Backup	Guide
Threat defense	Cisco Secure Firewall Management Center Administration Guide: *Backup/Restore* Backup is not supported for clustered threat defense virtual for KVM devices or threat defense virtual in the public cloud.
Firepower 4100/9300 chassis	Cisco Firepower 4100/9300 FXOS Configuration Guide: *Configuration Import/Export*

Backup	Guide
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 upgrade wizard prompts you to run the checks at the appropriate time. Although you can disable readiness checks, 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.