Planning Your Upgrade

Use this guide to plan and complete Firewall Threat Defense and Firewall Management Center upgrades. Upgrades can be minor (A.x), maintenance (A.x.y), or vulnerability (A.x.y.z) releases. We also may provide hotfixes, which are minor updates that address particular, urgent issues.

Note Version 10 begins a new release numbering scheme and cadence. For more information, see the Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin.

Is This Guide for You?

The procedures in this guide are for:

- Upgrading a Firewall Management Center that is *currently running* Version 10.
- Upgrading an older Firewall Threat Defense device using a Version 10 Firewall Management Center.

This means that after you use this guide to upgrade the Firewall Management Center, you will use a *different guide* to upgrade Firewall Threat Defense.

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, see:

- Cisco Secure Firewall Management Center Compatibility Guide
- Cisco Secure Firewall Threat Defense Compatibility Guide

Upgrade Guidelines

In addition to the guidelines and resource links in the following topics, see Reference for general information on time and disk space requirements, and for details on system behavior during upgrade, which can include interruptions to traffic flow and inspection.

Software Upgrade Guidelines

For release-specific upgrade warnings and guidelines for Firewall Management Center and Firewall Threat Defense, and for information on 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 Firewall Threat Defense Virtual

Upgrade does not change the serial number or UUID of Firewall 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 Firewall Threat Defense Virtual instance running the correct version, with no instance-specific (day 0) configurations.

Suspend health checks before autoscaled cluster upgrade

For Firewall 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.

Choosing your upgrade target

Go **directly to the latest Version 10 release possible** to minimize upgrade and other impact.

Features, enhancements, and critical fixes can skip "future" releases that are ahead by version, but not by release date. For example, if you are up-to-date within major Version A, upgrading to dot-zero Version B can deprecate features and fixes.

If you cannot go to the latest release, at least make sure your current version was released on a date before your target version; see the Cisco Secure Firewall Threat Defense Release Notes for your target version.

Upgrading from a patched deployment

Critical fixes in patches/vulnerability (fourth-digit) releases can also skip future releases. If you depend on these critical fixes, verify that your target version contains them. For a full list of release dates, see Cisco Secure Firewall Management Center New Features by Release.

Supported upgrades and downgrades

Supported upgrades

This table shows the supported direct upgrades for Firewall Management Center and Firewall Threat Defense software.

Note You can upgrade directly to any major (first and second-digit) or maintenance (third digit) release. 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 Firewall Management Center, fully patched deployments undergo enhanced testing.

Table 1: Supported direct upgrades

Current version	Target software version							
	to 10.0	7.7	7.6	7.4 *	7.3	7.2	7.1	7.0
from 10.0	YES	—	—	—	—	—	—	—
from 7.7	YES	YES	—	—	—	—	—	—
from 7.6	YES	YES	YES	—	—	—	—	—
from 7.4	YES	YES	YES	YES	—	—	—	—

Current version	Target software version							
	to 10.0	7.7	7.6	7.4 *	7.3	7.2	7.1	7.0
from 7.3	YES	YES	YES	YES	YES	—	—	—
from 7.2	—	YES	YES	YES	YES	YES	—	—
from 7.1	—	—	YES	YES	YES	YES	YES	—
from 7.0	—	—	—	YES	YES	YES	YES	YES
from 6.4	—	—	—	—	—	—	—	YES

* You cannot upgrade Firewall Threat Defense to Version 7.4.0, which is available as a fresh install on the Secure Firewall 4200 only, and is not supported with Firewall Device Manager. It removes significant features, enhancements, and critical fixes included in earlier versions. Upgrade to a later release.

For the Firepower 4100/9300, this table lists companion FXOS versions. If a chassis upgrade is required, Firewall 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 2: Supported FXOS versions for Firepower 4100/9300 upgrades

Target Firewall Threat Defense version	Minimum FXOS version
10.x	2.18.0
7.7	2.17.0
7.6	2.16.0
7.4.1–7.4.x	2.14.1
7.4.0	—
7.3	2.13.0
7.2	2.12.0
7.1	2.11.1
7.0	2.10.1
6.7	2.9.1
6.6	2.8.1
6.4	2.6.1

Supported downgrades

If an upgrade or patch succeeds but the system does not function to your expectations, you may be able to revert (Firewall Threat Defense upgrades) or uninstall (Firewall Threat Defense and Firewall Management

Center patches). For general information, particularly on common scenarios where returning to a previous version is not supported or recommended, see the upgrade guide: https://cisco.com/go/ftd-upgrade.

Upgrade Order

Firewall Management Center Before Devices

The Firewall 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 Firewall Management Center and its devices, including patches.

Upgrade the Firewall 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 Firewall Management Center, further Firewall Management Center upgrades can be blocked. In this case perform a three (or more) step upgrade: devices first, then the Firewall Management Center, then devices again.

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

Chassis Before Firewall 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 Firewall Threat Defense separately, one package contains the chassis and Firewall Threat Defense upgrades and you perform both from the Firewall Management Center. The compatibility work is done for you. It is possible to have a chassis-only upgrade or a Firewall 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 Firewall 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 Firewall 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. Firewall 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

Firewall Threat Defense Deployment	Upgrade Order
Standalone	1. Upgrade chassis. 2. Upgrade Firewall Threat Defense.
High availability	Upgrade both chassis before you upgrade Firewall 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 Firewall Threat Defense.
Intra-chassis cluster (units on the same chassis)	1. Upgrade chassis. 2. Upgrade Firewall Threat Defense.
Inter-chassis cluster (units on different chassis)	Upgrade all chassis before you upgrade Firewall 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 Firewall Threat Defense.

Table 4: Chassis Upgrade Order for the Secure Firewall 3100/4200 in Multi-Instance Mode

Firewall Threat Defense Deployment	Upgrade Order
Standalone	1. Upgrade chassis. 2. Upgrade Firewall Threat Defense.

Firewall Threat Defense Deployment	Upgrade Order
High availability	Upgrade both chassis before you upgrade Firewall Threat Defense. **1.** Upgrade chassis. With the chassis upgrade wizard, you have three options: • Two workflows (run the upgrade wizard twice) Best practice. Upgrade the chassis with the standby, switch roles, verify health, and upgrade the chassis with the new standby. This has the least risk of disruption. • Serial upgrade Recommended with reservations. Automatically fail over when the active unit goes down. If you use serial upgrade, place the standby unit first in the upgrade order. This avoids the total disruption of a parallel upgrade, but can still cause issues if the second chassis starts upgrading *after* the first chassis comes back up, but *before* high availability can resync. • Parallel upgrade Not recommended for high availability. **2.** Upgrade Firewall Threat Defense.

Upgrade Packages

To upgrade, the upgrade package must be on the Firewall Management Center or managed device.

The Firewall Management Center can get upgrade packages from the internet before or during upgrade, or you can upload packages you manually downloaded. Managed devices can get upgrade packages from the internet, the Firewall Management Center, or an internal server.

Especially for deployments without reliable, fast internet access, use these sections to plan how you will get upgrade packages where they need to be.

Managing Upgrade Packages with the Firewall Management Center

If the Firewall Management Center can reach the internet, **Administration** > **Upgrades & updates** > **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 Firewall Management Center, or upload packages you manually downloaded. For details, see the following table. For answers to common issues, see Troubleshooting Upgrade Packages, on page 15.

Tip Devices with internet access can be upgraded without the package on the Firewall Management Center. The device will get the package at the appropriate time; see Copying Upgrade Packages to Devices, on page 9.

Table 5: Managing Upgrade Packages with the Firewall 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 Firewall 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 Firewall Management Center.	Click **Add upgrade package** at the bottom right of the page, then **Choose file**. If you are uploading a Firewall Management Center upgrade package in a high availability deployment, the option to **Copy to peer Firewall Management Center** is enabled by default. See: Manually Downloading Upgrade Packages, on page 11
Configure 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 10
Force devices to get upgrade packages from the Firewall Management Center instead of the internet.	Click **Global upgrade settings**, then disable the option to **Allow devices to download from the support site**. By default, a device with internet access downloads upgrade packages from the internet before the Firewall Management Center, including as fallback when download from an internal server fails. See: Copying Upgrade Packages to Devices, on page 9
Configure the retry length for partial downloads.	Click **Global upgrade settings**, then choose an option from the **Retry failed downloads for** drop-down list. Partial downloads from the internet (Firewall Management Center and device) or internal server (device only) are saved and retried for the interval you specify. The default is 24 hours. This setting does not apply to device downloads from the Firewall Management Center over the management network. For device downloads, retry requires at least Version 7.4.3, 7.6.1, or 7.7.0.
Delete upgrade packages from the Firewall 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 Firewall Management Center. It does not delete packages from any devices where you already copied them. For Firewall 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. 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 10.

Copying Upgrade Packages to Devices

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

Copying Firewall 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 Firewall Management Center, for example, if devices do not have internet access, there is not enough disk space on the Firewall Management Center, or there is poor bandwidth between devices and the download location.

If download from the internal server fails, newer devices (Firewall Threat Defense 7.6+ or chassis 7.4.1+) with internet access try that next. Older devices and devices without internet access try the Firewall Management Center.

See: Copying Upgrade Packages to Devices from an Internal Server, on page 10

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. Not supported for hotfixes.

By default, a device with internet access tries the internet before the Firewall Management Center, but if devices have slow or unreliable internet access you can use the **Global upgrade settings** to force devices to get upgrade packages from the Firewall Management Center. If internet download fails, the device tries the Firewall Management Center.

See: Internet Access Requirements, on page 13 and Managing Upgrade Packages with the Firewall Management Center, on page 7

Firewall Management Center.

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

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

See: Managing Upgrade Packages with the Firewall Management Center, on page 7

Copying Chassis Upgrade Packages

For the Secure Firewall 3100/4200 in multi-instance mode, use the Firewall 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 Firewall 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 Firewall Chassis Manager or CLI (FTP, SCP, SFTP, or TFTP) to copy the package to the device. See Manually Downloading Upgrade Packages, on page 11 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 Firewall Management Center or an internal server. An internal server is especially useful if you have limited bandwidth between the Firewall Management Center and its devices (or, between the devices and the internet download location). It also saves space on the Firewall Management Center.

After you get upgrade packages (Manually Downloading Upgrade Packages, on page 11) and set up your server, configure pointers. On the Firewall Management Center, start like you are uploading a package: on the Product Upgrades page (**Administration** > **Upgrades & updates** > **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 (Firewall Threat Defense 7.6+ or chassis 7.4.1+) with internet access try the internet, then the Firewall Management Center. There is no way to disable this or force it to try the Firewall Management Center first. Older devices and devices without internet access just try the Firewall Management Center.

Table 6: Options for Copying Firewall 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 Firewall 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. The **Details** column indicates which chassis have packages that might not be needed.

Step 4 Use the **Warning** filter to display the affected chassis.

Step 5 In the filtered view, click **View and clean up packages** next to a chassis, select the packages you want to remove, and click **Delete selected packages**. Repeat this step for each chassis you want to clean up.

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

Manually Downloading Upgrade Packages

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:

- Firewall Management Center: https://www.cisco.com/go/firepower-software
- Firewall 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 Firewall Management Center can manage older devices (and apply maintenance releases and patches to them). For older devices not listed here, see the Firewall Management Center upgrade guide corresponding to the last supported device version.

Table 7: Upgrade Packages

Platform	Package
Firewall Management Center Packages	
Firewall Management Center hardware Firewall Management Center Virtual	Cisco_Secure_FW_Mgmt_Center_Upgrade-*Version-build*.sh.REL.tar
Firewall Threat Defense Packages	
Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-*Version-build*.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-*Version-build*.sh.REL.tar
Secure Firewall 200	Cisco_Secure_FW_TD_200-*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
Secure Firewall 6100	Cisco_Secure_FW_TD_6100-*Version-build*.sh.REL.tar
ISA 3000 with FTD	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar
Firewall Threat Defense Virtual	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 8: FXOS Packages

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

Internet Access Requirements

By default, the system is configured to connect to the internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP). If you do not want your appliances to have direct access to the internet, you can configure a proxy server.

Upgrade package download location depends on the Firewall Management Center's current version. Note that download *capability* can further depend on release type (major, maintenance, patch, hotfix) and package type (Firewall Management Center, device).

Firewall Threat Defense Download Location

With a Version 7.6.1+ Firewall Management Center, managed devices can get their own upgrade packages from the internet.

Table 9: Where devices get software upgrades

Devices with this Management Center Version	Download From
7.6.1+	https://cdo-ftd-images.s3-us-west-2.amazonaws.com/ The Firewall Management Center must also have access to this resource.
7.6.0 and earlier	Managed devices must get upgrade packages from the Firewall Management Center or an internal server.

Firewall Management Center Download Location

The Firewall Management Center can get upgrade packages from the internet. This includes upgrade packages for devices they manage.

Table 10: Where the Firewall Management Center gets software upgrades

Management Center Version	Downloads From
7.4.1+	https://cdo-ftd-images.s3-us-west-2.amazonaws.com/

Management Center Version	Downloads From
7.4.0 7.3.x	One of: • https://support.sourcefire.com/ For on-demand or scheduled downloads of applicable new releases. Used when you click the **Download Upgrades** button on the top right of > **Updates** > **Product Updates**. This immediately downloads the latest VDB, latest maintenance release, and the latest critical patches for your deployment. Also used by the task scheduler. • http://cdo-ftd-images.s3-us-west-2.amazonaws.com/ For on-demand downloads of specific Firewall Threat Defense upgrade packages. Used when you choose packages to download, then click the **Download Major Upgrades** button on the **Download Updates** sub-tab of > **Updates** > **Product Updates**.
7.2.6 to 7.2.x	https://cdo-ftd-images.s3-us-west-2.amazonaws.com/
7.2.5 and earlier	https://support.sourcefire.com/

High Availability and Clustering Considerations

If not all appliances in your deployment have internet access, use the following table to determine what to do.

Table 11: High Availability/Clustering Considerations for Downloading Software Upgrades

Package Type	Management Center Version	Considerations
Firewall Management Center upgrade	7.6.0+	Downloading the package on one HA Firewall Management Center attempts the download on both. If only one peer has internet access, you can sync the package during the upgrade process.
	7.4.1 to 7.4.x 7.2.6 to 7.2.x	Packages do not sync. For each HA Firewall Management Center with internet access, you can direct-download any applicable package.
	7.4.0 7.3.x 7.2.5 and earlier	Packages do not sync. For each HA Firewall Management Center with internet access, you can direct-download the latest maintenance release and critical patches. You must manually upload all other packages.

Package Type	Management Center Version	Considerations
Firewall Threat Defense upgrade	Any	Firewall Threat Defense upgrade packages do not sync between HA Firewall Management Centers, nor between high availability and clustered devices. Each device or unit must get its own upgrade package from the internet (with Firewall Management Center 7.6.1+), the active Firewall Management Center, or an internal server.

Troubleshooting Upgrade Packages

Table 12: Troubleshooting Upgrade Packages

Issue	Solution
No available upgrades even after I refresh.	Direct-downloading upgrade packages to the Firewall Management Center requires internet access. You will also see a blank list if you are already running the latest version available for your deployment *and* you have no upgrade packages loaded/configured.
Suggested release is not marked.	The suggested release is listed only if you are eligible for it. It is not listed if you are already running the suggested release or higher, or if you cannot upgrade that far. Note that patches to suggested releases are not marked as suggested, although we do recommend you apply them.
I don't see the packages I want.	Only major, maintenance, and patch upgrades that apply to your deployment *right now* are listed and available for direct download. Unless you manually upload, the following are not listed: • Device upgrades (major and maintenance) to a particular version, unless the Firewall Management Center is running that version or higher, *and* you have a device that supports that version. • Device patches, unless you have at least one device at the appropriate maintenance release. This also applies to Firewall Management Center patches. • Hotfixes. You must manually upload these.
I see available, undownloaded packages that don't apply to my devices.	The system lists the downloadable upgrades that apply to *all* devices managed by this Firewall Management Center. In a multidomain deployment, this can include devices that you cannot access right now.
I downloaded a Firewall Management Center upgrade package from the internet, but the download to its high availability peer failed.	If the peer Firewall Management Center does not have internet access or the download fails for any other reason, you can: • Start the upgrade anyway. The upgrade wizard has options to retry the download, or sync the file between the peers. • Log into the peer and manually upload the upgrade package.

Issue	Solution
I uploaded a Firewall Management Center upgrade package, but the sync to its high availability peer failed.	If the upgrade package sync fails for any reason, you can: • Start the upgrade anyway. The upgrade wizard has options to attempt a download from the internet, or retry the sync. • Log into the peer and manually upload the upgrade package.
Copying upgrade packages from the Firewall Management Center to devices times out.	This often happens when there is limited bandwidth between the Firewall Management Center and its devices. You can try one of: • Configure devices to get upgrade packages directly from an internal web server. To do this, delete the upgrade package from the Firewall Management Center (optional but saves disk space), then re-add the upgrade package except this time specify a pointer (URL) to its location instead. See Copying Upgrade Packages to Devices from an Internal Server, on page 10. • Allow devices to download the upgrade package from the internet. Devices with internet access automatically try that first, and only fall back on the Firewall Management Center if internet download fails. See Internet Access Requirements, on page 13.

Upgrade Readiness

After you check compatibility, plan your upgrade path and order, and review upgrade guidelines, you need to assess upgrade readiness. The system does some of these checks for you, but you still need to perform additional checks (and actions) yourself, like deploying configuration changes and making backups.

Use the following sections to perform last minute-tasks and confirm 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 Firewall 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 any required pre-upgrade configuration changes, and prepare to make required post-upgrade configuration changes. Resolve any change management workflows.

The following table indicates when you have to deploy to managed devices. Deploying typically restarts Snort, which can affect traffic flow and inspection; see Traffic Flow and Inspection when Deploying Configurations.

Table 13: When to Deploy

Platform	Deploy Before Upgrade	Deploy After Upgrade
Firewall Management Center	No.	Sometimes. If redeploy is required, affected devices are marked out of date. Note that devices may not be marked out of date if you schedule intrusion rule updates; in that case the redeploy will take place on schedule. Additionally, you must deploy at least once between Firewall Management Center and device upgrade, even if devices are not marked out of date.
Firewall Threat Defense	Yes.	Yes.

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: **Troubleshooting** > **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 14: 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.

Health Test	Description
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. On 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.
Firewall Threat Defense HA (Firewall Management Center and devices) Cluster/HA Failure Status (devices)	High availability pairs and clusters should be in sync, not split brain, and so on. Firewall Threat Defense upgrades will not proceed for most issues of this type. However, for the Firepower 4100/9300 and Secure Firewall 3100/4200 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.
FXOS Health	Monitors the FXOS httpd service on FXOS-based devices. Upgrade will fail without this service running.
Time Server Status (Firewall 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 and cannot be resumed; they become failed tasks.

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 Firewall Management Center after you upgrade its managed devices, so your new Firewall Management Center backup file 'knows' that its devices have been upgraded.

Table 15: Backups

Backup	Guide
Firewall Management Center	Cisco Secure Firewall Management Center Administration Guide: *Backup/Restore* We recommend you back up configurations and events.
Firewall Threat Defense	Cisco Secure Firewall Management Center Administration Guide: *Backup/Restore* Note that backup is not supported in all cases, for example, for Firewall Threat Defense Virtual in the public cloud. But if you can back up, you should.
Secure Firewall 3100/4200 chassis	Cisco Secure Firewall Management Center Device Configuration Guide: *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 Firewall 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.