

Troubleshooting and Reference

- Troubleshooting Upgrade Packages, on page 1
- Troubleshooting Threat Defense Upgrade, on page 2
- Unresponsive and Failed Management Center Upgrades, on page 4
- Unresponsive and Failed Threat Defense Upgrades, on page 4
- Traffic Flow and Inspection, on page 5
- Time and Disk Space, on page 8
- Internet Access Requirements, on page 9
- Upgrade Feature History, on page 11

Troubleshooting Upgrade Packages

Table 1: Troubleshooting Upgrade Packages

Issue	Solution
No available upgrades even after I refresh.	Direct-downloading upgrade packages to the 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 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 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 management center. In a multidomain deployment, this can include devices that you cannot access right now.

Issue	Solution
I downloaded a management center upgrade package from the internet, but the download to its high availability peer failed.	If the peer 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.
I uploaded a 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 management center to devices times out.	This often happens when there is limited bandwidth between the 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 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. • Allow devices to download the upgrade package from the internet. Devices with internet access automatically try that first, and only fall back on the management center if internet download fails. Requires a Version 7.6.1+ management center. See Internet Access Requirements, on page 9.

Troubleshooting Threat Defense Upgrade

Table 2: Troubleshooting Threat Defense Upgrade

Issue	Solution
Upgrade button missing for my target version.	Either: • You do not have anything that can be upgraded to that version right now. • No eligible devices have internet access. Upload the package to the management center or configure an internal server; see Managing Upgrade Packages with the Management Center.
Devices not listed in the upgrade wizard.	If you accessed the wizard directly from **Devices** > **Threat Defense Upgrade** and therefore did not select a target version, the workflow may be blank. To begin, choose a target version from the **Upgrade to** menu. The system should display the devices that can be upgraded to that version.

Issue	Solution
Target version not listed in the **Upgrade to** menu.	The choices in the **Upgrade to** menu correspond to the device upgrade packages on the management center, plus any on the support site that apply to you. If you don't see the one you want, either: • The menu lists multiple versions but not the one you are looking for. You may not have any eligible devices. Or, the package may require manual upload (such as hotfixes). • The menu is blank/only lists versions corresponding to already uploaded packages. The management center does not have internet access (or you are running Version 7.6.0). You must manually upload the package you want. To upload an upgrade package, click **Manage Upgrade Packages**; see Managing Upgrade Packages with the Management Center.
Devices not listed in the upgrade wizard even though a target version is selected.	You have no devices that can be upgraded to that version. If you still think you should see devices here, your user role could be prohibiting you from managing (and therefore upgrading) devices. In a multidomain deployment, you could be logged into the wrong domain.
Devices locked to someone else's upgrade workflow.	If you need to reset someone else's workflow, you must have Administrator access. You can either: • Delete or deactivate the user. • Update the user's role so they no longer have permission to use **System** (⚙) > **Product Upgrades**.
High availability management center failed over while setting up upgrade.	Neither your workflow nor threat defense upgrade packages are synchronized between high availability management centers. In case of failover, you must recreate your workflow on the new active management center, which includes downloading upgrade packages and copying them to devices. (Upgrade packages already copied to devices are not removed, but the management center still must have the package or a pointer to its location.)
Pruning daemon errors in the Message Center.	This most commonly happens for devices running Version 7.6.x or earlier when you do not start the upgrade within 10 minutes after the readiness check completes. Regardless, you can safely ignore these messages and proceed with the upgrade. The full error is: `Process Status - device_name. The pruning daemon exited n time(s).`

Unresponsive and Failed Management Center Upgrades

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

In high availability deployments, do not make or deploy configuration changes while the pair is split-brain, even if you are not actively upgrading. Your changes will be lost after synchronization restarts; deploying could place the system in an unusable state and require a reimage.

Unresponsive and Failed Threat Defense Upgrades

The following table has troubleshooting information for unresponsive and failed threat defense upgrades. For issues with chassis upgrades, contact Cisco TAC.

Caution Do not reboot or shut down at any point during upgrade, even if the system appears inactive. You could place the system in an unusable state and require a reimage.

Table 3: Unresponsive and Failed Threat Defense Upgrades

Issue	Solution
Cannot reach the device.	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.
Upgrade or patch appears hung/device appears inactive.	If device upgrade status has stopped updating on the management center but there is no report of upgrade failure, you can try canceling the upgrade; see below. If you cannot cancel or canceling does not work, contact Cisco TAC. **Tip:** You can monitor upgrade logs on the device itself using expert mode and tail or tailf: `tail /ngfw/var/log/sf/update.status`.
Upgrade failed.	If an upgrade fails and: • The device reverted to its pre-upgrade state (auto-cancel is enabled), correct any issues and try again from the beginning. • The device is still in maintenance mode, correct any issues and resume the upgrade. Or, cancel and try again later. If you cannot retry or cancel, or if you continue to have issues, contact Cisco TAC.

Issue	Solution
Patch failed.	You cannot cancel in-progress or failed patches. However, if a patch fails early, for example, during validation stages, the device may remain up and running normally. Simply correct any issues and try again. If a patch fails after the device has entered maintenance mode, check for an uninstaller. If one exists, you can try running it to remove the failed patch; see Uninstall a Threat Defense Patch. After the uninstall finishes, you can correct any issues and try again. If there is no uninstaller, if the uninstall fails, or if you continue to have issues, contact Cisco TAC.
Upgrade or patch on a clustered device failed, and I want to reimage instead of retrying the upgrade.	If a cluster node upgrade fails and you choose to reimage the node, reimage it to the *current* version of the control node before you add it back to the cluster. Depending on when and how the upgrade failed, the current version of the control node can be the old version or the target version. We do not support mixed-version clusters except temporarily during upgrade. Deliberately creating a mixed-version cluster can cause outages. **Tip** Remove the failed node from the cluster and reimage it to the target version. Upgrade the rest of the cluster to the target version, then add your reimaged node.
I want to cancel an upgrade.	Canceling reverts the device to its pre-upgrade state. You can cancel failed and in-progress upgrades on the upgrade status pop-up, accessible from the Upgrade tab on the Device Management page. You cannot cancel patches. If you cannot cancel or canceling does not work, contact Cisco TAC.
I want to retry (resume) a failed upgrade.	You can resume an upgrade on the upgrade status pop-up, accessible from the Upgrade tab on the Device Management page. If you continue to have issues, contact Cisco TAC.
I want to change what happens when upgrade fails.	Part of the upgrade process is choosing what happens if it fails. This is done with the **Automatically cancel on upgrade failure...** (auto-cancel) option: • Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. This returns you to normal operations as quickly as possible while you regroup and try again. • Auto-cancel disabled: If upgrade fails, the device remains as it is. This allows you to correct any issues and resume the upgrade. For high availability and clustered devices, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

Traffic Flow and Inspection

Schedule maintenance windows when upgrade will have the least impact, considering any effect on traffic flow and inspection.

Traffic Flow and Inspection for Threat Defense Upgrades

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 4: Traffic Flow and Inspection: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped. For bridge group interfaces on the ISA 3000 only, you can use a FlexConfig policy to configure hardware bypass for power failure. This causes traffic to drop during software upgrades but pass without inspection while the device completes its post-upgrade reboot.
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force**	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby**	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled**	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability and Clustered Devices

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices. For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

For clusters, the data security module or modules upgrade first, then the control module. During the control security module upgrade, although traffic inspection and handling continues normally, the system stops logging events. Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the upgrade is completed. However, if the logging downtime is significant, the system may prune the oldest events before they can be logged.

Note that hitless upgrades are not supported for single-unit clusters. Interruptions to traffic flow and inspection depend on interface configurations of the active unit, just as with standalone devices.

Software Revert (Major/Maintenance Releases)

You should expect interruptions to traffic flow and inspection during revert, even in a high availability/scalability deployment. This is because revert is more successful when all units are reverted simultaneously. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

Software Uninstall (Patches)

For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

Traffic Flow and Inspection for Chassis Upgrades

Upgrading FXOS reboots the chassis. For FXOS upgrades to Version 2.14.1+ that include firmware upgrades, the chassis reboots twice—once for FXOS and once for the firmware. This includes Version 7.4.1+ chassis upgrades for the Secure Firewall 3100/4200 in multi-instance mode.

Even in high availability or clustered deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time; see Upgrade Order.

Table 5: Traffic Flow and Inspection: FXOS Upgrades

Threat Defense Deployment	Traffic Behavior	Method
Standalone	Dropped.	—
High availability	Unaffected.	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.
	Dropped until one peer is online.	Upgrade FXOS on the active peer before the standby is finished upgrading.
Inter-chassis cluster	Unaffected.	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.
	Dropped until at least one module is online.	Upgrade chassis at the same time, so all modules are down at some point.
Intra-chassis cluster (Firepower 9300 only)	Passed without inspection.	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**.
	Dropped until at least one module is online.	Hardware bypass disabled: **Bypass: Disabled**.
	Dropped until at least one module is online.	No hardware bypass module.

Traffic Flow and Inspection when Deploying Configurations

Snort typically restarts during the first deployment immediately after upgrade. This means that for management center upgrades, Snort could restart on all managed devices. Snort does not restart after subsequent deployments unless, before deploying, you modify specific policy or device configurations.

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Table 6: Traffic Flow and Inspection: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled.	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled.	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled.	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Time and Disk Space

Time to Upgrade

We recommend you track and record your own upgrade times so you can use them as future benchmarks. The following table lists some things that can affect upgrade time.

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive and Failed Threat Defense Upgrades, on page 4.

Table 7: Upgrade Time Considerations

Consideration	Details
Versions	Upgrade time usually increases if your upgrade skips versions.
Models	Upgrade time usually increases with lower-end models.
Virtual appliances	Upgrade time in virtual deployments is highly hardware dependent.
High availability and clustering	In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how they are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.
Components	You may need additional time to perform operating system or virtual hosting upgrades, upgrade package transfers, readiness checks, VDB and intrusion rule (SRU/LSP) updates, configuration deployment, and other related tasks.

Disk Space to Upgrade

To upgrade, the upgrade package must be on the appliance. For device upgrades where the device does not have access to the internet, you must also have enough space on the management center (in either /Volume or /var) for the device upgrade package. Or, you can use an internal server to store them. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails. For more information, see Configuration and Deployment Checks.

Internet Access Requirements

The management center can get device and management center upgrade packages from the internet. With a Version 7.6.1+ management center, managed devices can get their own upgrade packages.

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.

Download Location

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

Table 8: Device Download Location for Software Upgrades

Management Center Current Version	Resource
7.6.1+	https://cdo-ftd-images.s3-us-west-2.amazonaws.com/

Management Center Current Version	Resource
7.6.0 and earlier	Managed devices must get upgrade packages from the management center or an internal server.

Table 9: Management Center Download Location for Software Upgrades

Management Center Current Version	Resource
7.4.1+	https://cdo-ftd-images.s3-us-west-2.amazonaws.com/
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 **System** (⚙) > **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 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 **System** (⚙) > **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/Clustering Considerations

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

Table 10: High Availability/Clustering Considerations for Downloading Software Upgrades

Package Type	Management Center Current Version	Considerations
Management center upgrade	7.6.0+	Downloading the package on one HA 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 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 management center with internet access, you can direct-download the latest maintenance release and critical patches. You must manually upload all other packages.
Threat defense upgrade	Any	Threat defense upgrade packages do not sync between HA management centers, nor between high availability and clustered devices. Each device or unit must get its own upgrade package from the internet (with management center 7.6.1+), the active management center, or an internal server.

Upgrade Feature History

Table 11: Version 7.6.1 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Threat Defense Upgrade			
Devices with internet access download upgrade packages from the internet.	7.6.1 7.7.0	Any	You can now begin device and chassis upgrades without the upgrade package. At the appropriate time, devices will get the package directly from the internet. This saves time and management center disk space. Devices without internet access can continue to get the package from the management center or an internal server. Note that devices try the internal server (if configured) before either the internet or the management center. If the internal server download fails, newer devices with internet access try the internet then the management center, while older devices and devices without internet access just try the management center. (In this context, "newer" means threat defense 7.6+ or chassis 7.4.1+.) Restrictions: Management center and devices must be able to access the internet. There is no way to force a device with internet access to try the management center before it tries the internet. Not supported for hotfixes. Download location: https://cdo-ftd-images.s3-us-west-2.amazonaws.com/

Table 12: Version 7.6.0 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Threat Defense Upgrade			
Generate and download post-upgrade configuration change reports from the threat defense and chassis upgrade wizards.	7.6.0	Any	You can now generate and download post-upgrade configuration change reports from the threat defense and chassis upgrade wizards, as long as you have not cleared your upgrade workflow. Previously, you used the Advanced Deploy screens to generate the reports and the Message Center to download them. Note that you can still use this method, which is useful if you want to quickly generate change reports for multiple devices, or if you cleared your workflow. New/modified screens: • **Devices** > **Threat Defense Upgrade** > **Configuration Changes** • **Devices** > **Chassis Upgrade** > **Configuration Changes**
Deprecated: Copy upgrade packages ("peer-to-peer sync") from device to device.	7.6.0	7.6.0	You can no longer use the threat defense CLI to copy upgrade packages between devices over the management network. If you have limited bandwidth between the management center and its devices, configure devices to get upgrade packages directly from an internal web server. Deprecated CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
Management Center Upgrade			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved upgrade process for high availability management centers.	7.6.0	Any	Upgrading high availability management centers is now easier: • You no longer have to manually copy the upgrade package to both peers. Depending on your setup, you can have each peer get the package from the support site, or you can copy the package between peers. • You no longer have to manually run the readiness check on both peers. Running it on one runs it on both. • If you do not have enough disk space to run the upgrade, a new **Clean Up Disk Space** option can help. • You no longer have to manually pause synchronization before upgrade, or resolve split brain after the upgrade; the system now does this automatically. Also, your original active/standby roles are preserved. Note that although you can complete most of the upgrade process from one peer (we recommend the standby), you do have to log into the second peer to actually initiate its upgrade. New/modified screens: **System** (⚙) > **Product Upgrades** Version restrictions: This feature applies to upgrades *from* Version 7.6.0 and later, not *to* 7.6.0.

Table 13: Version 7.4.1 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Threat Defense Upgrade			
Firmware upgrades included in FXOS upgrades.	Any	Any	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware. Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade. See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide

Feature	Minimum Management Center	Minimum Threat Defense	Details
Chassis upgrade for the Secure Firewall 3100 in multi-instance mode.	7.4.1	7.4.1	For the Secure Firewall 3100 in multi-instance mode, you upgrade the operating system and the firmware (*chassis upgrade*) separately from the container instances (*threat defense upgrade*). New/modified screens: • Upgrade the chassis: **Devices** > **Chassis Upgrade** • Upgrade threat defense: **Devices** > **Threat Defense Upgrade**
Management Center Upgrade			
Automatically generate configuration change reports after management center upgrade.	Any	Any	You can automatically generate reports on configuration changes after major and maintenance management center upgrades. This helps you understand the changes you are about to deploy. After the system generates the reports, you can download them from the Tasks tab in the Message Center. Version restrictions: Only supported for management center upgrades from Version 7.4.1+. Not supported for upgrades to Version 7.4.1 or any earlier version. New/modified screens: **System**(⚙) > **Configuration** > **Upgrade Configuration** > **Enable Post-Upgrade Report**

Table 14: Version 7.3.0 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Threat Defense Upgrade			
Choose and direct-download upgrade packages to the management center from Cisco.	7.3.0	Any	You can now choose which threat defense upgrade packages you want to direct download to the management center. Use the new **Download Updates** sub-tab on > **Updates** > **Product Updates**. Version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1. See: Download Upgrade Packages with the Management Center
Upload upgrade packages to the management center from the threat defense wizard.	7.3.0	Any	You now use the wizard to upload threat defense upgrade packages or specify their location. Previously (depending on version), you used **System** (⚙) > **Updates** or **System** (⚙) > **Product Upgrades**. Version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1. See: Upgrade Threat Defense

Feature	Minimum Management Center	Minimum Threat Defense	Details
Auto-upgrade to Snort 3 after successful threat defense upgrade is no longer optional.	7.3.0	Any	**Upgrade impact. All eligible devices upgrade to Snort 3 when you deploy.** When you upgrade threat defense to Version 7.3+, you can no longer disable the **Upgrade Snort 2 to Snort 3** option. After the software upgrade, all eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. Although you can switch individual devices back, Snort 2 is not supported on threat defense 7.7+. You should stop using it now. For devices that are ineligible for auto-upgrade because they use custom intrusion or network analysis policies, manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Combined upgrade and install package for Secure Firewall 3100.	7.3.0	7.3.0	**Reimage Impact.** In Version 7.3, we combined the threat defense install and upgrade package for the Secure Firewall 3100, as follows: • Version 7.1–7.2 install package: cisco-ftd-fp3k.*version*.SPA • Version 7.1–7.2 upgrade package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Version 7.3+ combined package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Although you can upgrade threat defense without issue, you cannot reimage from older threat defense and ASA versions directly to threat defense Version 7.3+. This is due to a ROMMON update required by the new image type. To reimage from those older versions, you must "go through" ASA 9.19+, which is supported with the old ROMMON but also updates to the new ROMMON. There is no separate ROMMON updater. To get to threat defense Version 7.3+, your options are: • Upgrade from threat defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate Upgrade Guide. • Reimage from threat defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to threat defense Version 7.3+. See *Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from ASA 9.17 or 9.18 — upgrade to ASA 9.19+ first, then reimage to threat defense Version 7.3+. See the Cisco Secure Firewall ASA Upgrade Guide and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from threat defense Version 7.3+ — use the normal reimage process. See *Reimage the System with a New Software Version* in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 1200/3100/4200 with Firepower Threat Defense.
Content Updates			

Feature	Minimum Management Center	Minimum Threat Defense	Details
Automatic VDB downloads.	7.3.0	Any	The initial setup on the management center schedules a weekly task to download the latest available software updates, which now includes the latest vulnerability database (VDB). We recommend you review this weekly task and adjust if necessary. Optionally, schedule a new weekly task to actually update the VDB and deploy configurations. New/modified screens: The **Vulnerability Database** check box is now enabled by default in the system-created **Weekly Software Download** scheduled task.
Install any VDB.	7.3.0	Any	Starting with VDB 357, you can now install any VDB as far back as the baseline VDB for that management center. After you update the VDB, deploy configuration changes. If you based configurations on vulnerabilities, application detectors, or fingerprints that are no longer available, examine those configurations to make sure you are handling traffic as expected. Also, keep in mind a scheduled task to update the VDB can undo a rollback. To avoid this, change the scheduled task or delete any newer VDB packages. New/modified screens: On **System**(⚙) > **Updates** > **Product Updates** > **Available Updates**, if you upload an older VDB, a new **Rollback** icon appears instead of the **Install** icon.

Table 15: Version 7.2.10 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Threat Defense Upgrade			
Threat defense and chassis upgrade wizards optimized for lower resolution screens.	7.2.10 7.6.0	Any	We optimized the threat defense and chassis upgrade wizards for lower resolution screens (and smaller browser windows). Text appears smaller and certain screen elements are hidden. If you change your resolution or window size mid-session, you may need to refresh the page for the web interface to adjust. Note that the minimum screen resolution to use the management center is 1280 x 720. New/modified screens: • **Devices** > **Threat Defense Upgrade** • **Devices** > **Chassis Upgrade** Version restrictions: Not supported with Version 7.2.0–7.2.9, 7.3.x, 7.4.0–7.4.2.

Table 16: Version 7.2.6 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade			
Improved upgrade starting page and package management.	7.2.6 7.4.1	Any	A new upgrade page makes it easier to choose, download, manage, and apply upgrades to your entire deployment. This includes the management center, threat defense devices, and any older NGIPSv/ASA FirePOWER devices. The page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, as well as manually upload and delete packages. Internet access is required to retrieve the list/direct download upgrade packages. Otherwise, you are limited to manual management. Patches are not listed unless you have at least one appliance at the appropriate maintenance release (or you manually uploaded the patch). You must manually upload hotfixes. New/modified screens: • **System**(⚙) > **Product Upgrades** is now where you upgrade the management center and all managed devices, as well as manage upgrade packages. • **System**(⚙) > **Content Updates** is now where you update intrusion rules, the VDB, and the GeoDB. • **Devices** > **Threat Defense Upgrade** takes you directly to the threat defense upgrade wizard. • **System**(⚙) > **Users** > **User Role** > **Create User Role** > **Menu-Based Permissions** allows you to grant access to **Content Updates** (VDB, GeoDB, intrusion rules) without allowing access to **Product Upgrades** (system software). Deprecated screens/options: • **System**(⚙) > **Updates** is deprecated. All threat defense upgrades now use the wizard. • The **Add Upgrade Package** button on the threat defense upgrade wizard has been replaced by a **Manage Upgrade Packages** link to the new upgrade page. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Suggested release notifications.	7.2.6 7.4.1	Any	The management center now notifies you when a new suggested release is available. If you don't want to upgrade right now, you can have the system remind you later, or defer reminders until the next suggested release. The new upgrade page also indicates suggested releases. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Management Center New Features by Release
Updated internet access requirements for direct-downloading software upgrades.	7.2.6 7.4.1	Any	**Upgrade impact. The system connects to new resources.** The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.
Threat Defense Upgrade			
Enable revert from the threat defense upgrade wizard.	7.2.6 7.4.1	Any, if upgrading to 7.1+	You can now enable revert from the threat defense upgrade wizard. Other version restrictions: You must be upgrading threat defense to Version 7.1+. Not supported with management center Version 7.3.x or 7.4.0.
Select devices to upgrade from the threat defense upgrade wizard.	7.2.6	Any	Use the wizard to select devices to upgrade. You can now use the threat defense upgrade wizard to select or refine the devices to upgrade. On the wizard, you can toggle the view between selected devices, remaining upgrade candidates, ineligible devices (with reasons why), devices that need the upgrade package, and so on. Previously, you could only use the Device Management page and the process was much less flexible.
View detailed upgrade status from the threat defense upgrade wizard.	7.2.6 7.4.1	Any	The final page of the threat defense upgrade wizard now allows you to monitor upgrade progress. This is in addition to the existing monitoring capability on the Upgrade tab on the Device Management page, and on the Message Center. Note that as long as you have not started a new upgrade flow, **Devices** > **Threat Defense Upgrade** brings you back to this final wizard page, where you can view the detailed status for the current (or most recently complete) device upgrade. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.
Unattended threat defense upgrades.	7.2.6	Any	The threat defense upgrade wizard now supports unattended upgrades, using a new **Unattended Mode** menu. You just need to select the target version and the devices you want to upgrade, specify a few upgrade options, and step away. You can even log out or close the browser.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Simultaneous threat defense upgrade workflows by different users.	7.2.6	Any	We now allow simultaneous upgrade workflows by different users, as long as you are upgrading different devices. The system prevents you from upgrading devices already in someone else's workflow. Previously, only one upgrade workflow was allowed at a time across all users.
Skip pre-upgrade troubleshoot generation for threat defense devices.	7.2.6	Any	You can now skip the automatic generating of troubleshooting files before major and maintenance upgrades by disabling the new **Generate troubleshooting files before upgrade begins** option. This saves time and disk space. To manually generate troubleshooting files for a threat defense device, choose **System**(⚙) > **Health** > **Monitor**, click the device in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**.
Management Center Upgrade			
New upgrade wizard for the management center.	7.2.6 7.4.1	Any	A new upgrade starting page and wizard make it easier to perform management center upgrades. After you use **System**(⚙) > **Product Upgrades** to get the appropriate upgrade package onto the management center, click **Upgrade** to begin. Other version restrictions: Only supported for management center upgrades from Version 7.2.6+/7.4.1+. Not supported for upgrades from Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Hotfix high availability management centers without pausing synchronization.	7.2.6 7.4.1	Any	Unless otherwise indicated by the hotfix release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability management centers. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.
Content Updates			
Scheduled tasks download patches and VDB updates only.	7.2.6 7.4.1	Any	**Upgrade impact. Scheduled download tasks stop retrieving maintenance releases.** The **Download Latest Update** scheduled task no longer downloads maintenance releases; now it only downloads the latest applicable patches and VDB updates. To direct-download maintenance (and major) releases to the management center, use **System**(⚙) > **Product Upgrades**. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0.

Table 17: Version 7.2.0 Features

Feature	Details
Threat Defense Upgrade	
Copy upgrade packages ("peer-to-peer sync") from device to device.	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 in different domains, or devices separated by a NAT gateway. • Devices upgrading from Version 7.1 or earlier, regardless of management center version. • Devices running Version 7.6+. New/modified CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
Auto-upgrade to Snort 3 after successful threat defense upgrade.	When you use a Version 7.2+ management center to upgrade threat defense to Version 7.2+, you can now choose whether to **Upgrade Snort 2 to Snort 3**. After the software upgrade, eligible devices upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For help, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version. Version restrictions: Not supported for threat defense upgrades to Version 7.0.x or 7.1.x.
Upgrade for single-node clusters.	You can now use the device upgrade page (**Devices** > **Device Upgrade**) to upgrade clusters with only one active node. Any deactivated nodes are also upgraded. Previously, this type of upgrade would fail. This feature is not supported from the system updates page (**System**(⚙)**Updates**). Hitless upgrades are also not supported in this case. Interruptions to traffic flow and inspection depend on the interface configurations of the lone active unit, just as with standalone devices. Supported platforms: Firepower 4100/9300, Secure Firewall 3100

Feature	Details
Revert threat defense upgrades from the CLI.	You can now revert threat defense upgrades from the device CLI if communications between the management center and device are disrupted. Note that in high availability/scalability deployments, revert is more successful when all units are reverted simultaneously. When reverting with the CLI, open sessions with all units, verify that revert is possible on each, then start the processes at the same time. **Caution** Reverting from the CLI can cause configurations between the device and the management center to go out of sync, depending on what you changed post-upgrade. This can cause further communication and deployment issues. New/modified CLI commands: **upgrade revert**, **show upgrade revert-info**.
Management Center Upgrade	
Management center upgrade does not automatically generate troubleshooting files.	To save time and disk space, the management center upgrade process no longer automatically generates troubleshooting files before the upgrade begins. Note that device upgrades are unaffected and continue to generate troubleshooting files. To manually generate troubleshooting files for the management center, choose **System**(⚙) > **Health** > **Monitor**, click **Firewall Management Center** in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**.

Table 18: Version 7.1.0 Features

Feature	Details
Threat Defense Upgrade	
Revert a successful device upgrade.	You can now revert major and maintenance upgrades to FTD. Reverting returns the software to its state just before the last upgrade, also called a *snapshot*. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade. **Important** If you think you might need to revert, you must use **System**(⚙) > **Updates** to upgrade FTD. The System Updates page is the only place you can enable the **Enable revert after successful upgrade** option, which configures the system to save a revert snapshot when you initiate the upgrade. This is in contrast to our usual recommendation to use the wizard on the **Devices** > **Device Upgrade** page. This feature is not supported for container instances. Minimum FTD: 7.1

Feature	Details
Improvements to the upgrade workflow for clustered and high availability devices.	We made the following improvements to the upgrade workflow for clustered and high availability devices: • The upgrade wizard now correctly displays clustered and high availability units as groups, rather than as individual devices. The system can identify, report, and preemptively require fixes for group-related issues you might have. For example, you cannot upgrade a cluster on the Firepower 4100/9300 if you have made unsynced changes on Firepower Chassis Manager. • We improved the speed and efficiency of copying upgrade packages to clusters and high availability pairs. Previously, the FMC copied the package to each group member sequentially. Now, group members can get the package from each other as part of their normal sync process. • You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.

Table 19: Version 7.0.0 Features

Feature	Details
Threat Defense Upgrade	
Improved FTD upgrade performance and status reporting.	FTD upgrades are now easier faster, more reliable, and take up less disk space. A new **Upgrades** tab in the Message Center provides further enhancements to upgrade status and error reporting.

Feature	Details
Easy-to-follow upgrade workflow for FTD devices.	A new device upgrade page (**Devices > Device Upgrade**) on the FMC provides an easy-to-follow wizard for upgrading Version 6.4+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks. To begin, use the new **Upgrade Firepower Software** action on the Device Management page (**Devices > Device Management > Select Action**). As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage. If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard. **Note** You must still use **System**(⚙) > **Updates** to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices. **Note** In Version 7.0, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all. To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the wizard before you click **Next**.
Upgrade more FTD devices at once.	The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time. **Important** Only upgrades to FTD Version 6.7+ using the FTD upgrade wizard see this improvement. If you are upgrading devices to an older FTD release—even if you are using the new upgrade wizard—we still recommend you limit to five devices at a time.
Upgrade different device models together.	You can now use the FTD upgrade wizard to queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages. Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time *only* if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series.

Table 20: Version 6.7.0 Features

Feature	Details
Threat Defense Upgrade	
Upgrades remove PCAP files to save disk space.	Upgrades now remove locally stored PCAP files. To upgrade, you must have enough free disk space or the upgrade fails.
Improved FTD upgrade status reporting and cancel/retry options.	You can now view the status of FTD device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages. A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on. Also on this pop-up, you can manually cancel failed or in-progress upgrades (**Cancel Upgrade**), or retry failed upgrades (**Retry Upgrade**). Canceling an upgrade reverts the device to its pre-upgrade state. **Note** To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: **Automatically cancel on upgrade failure and roll back to the previous version**. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure. Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. New/modified screens: • **System**(⚙) > **Updates** > **Product Updates** > **Available Updates** > **Install** icon for the FTD upgrade package • **Devices** > **Device Management** > **Upgrade** • **Message Center > Tasks** New/modified CLI commands: **show upgrade status detail**, **show upgrade status continuous**, **show upgrade status**, **upgrade cancel**, **upgrade retry**
Content Updates	

Feature	Details
Custom intrusion rule import warns when rules collide.	The FMC now warns you of rule collisions when you import custom (local) intrusion rules. Previously, the system would silently skip the rules that cause collisions—with the exception of Version 6.6.0.1, where a rule import with collisions would fail entirely. On the Rule Updates page, if a rule import had collisions, a warning icon is displayed in the Status column. For more information, hover your pointer over the warning icon and read the tooltip. Note that a collision occurs when you try to import an intrusion rule that has the same SID/revision number as an existing rule. You should always make sure that updated versions of custom rules have new revision numbers. New/modified screens: We added a warning icon to **System**(⚙) > **Updates** > **Rule Updates**.

Table 21: Version 6.6.0 Features

Feature	Details
Threat Defense Upgrade	
Get FTD upgrade packages from an internal web server.	FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for FTD devices running Version 6.6+. It is not supported for upgrades *to* Version 6.6, nor is it supported for the FMC or Classic devices. New/modified screens: We added a **Specify software update source** option to the page where you upload upgrade packages.
Content Updates	
Automatic VDB update during initial setup.	When you set up a new or reimaged FMC, the system automatically attempts to update the vulnerability database (VDB). This is a one-time operation. If the FMC has internet access, we recommend you schedule tasks to perform automatic recurring VDB update downloads and installations.

Table 22: Version 6.5.0 Features

Feature	Details
Content Updates	

Feature	Details
Automatic software downloads and GeoDB updates.	When you set up a new or reimaged FMC, the system automatically schedules: • A weekly task to download software updates for the FMC and its managed devices. • Weekly updates for the GeoDB. The tasks are scheduled in UTC, which means that when they occur locally depends on the date and your specific location. Also, because tasks are scheduled in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour "later" in the summer than in the winter, according to local time. We recommend you review the auto-scheduled configurations and adjust them if necessary.

Table 23: Version 6.4.0 Features

Feature	Details
Management Center Upgrade	
Upgrades postpone scheduled tasks.	The management center upgrade process now postpones scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for all upgrades *from* a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades *to* a supported version from an unsupported version.
Content Updates	

Feature	Details
Signed SRU, VDB, and GeoDB updates.	So the system can verify that you are using the correct update files, Version 6.4+ uses *signed* updates for intrusion rules (SRU), the vulnerability database (VDB), and the geolocation database (GeoDB). Earlier versions continue to use unsigned updates. Unless you manually download updates from the Cisco Support & Download site—for example, in an air-gapped deployment—you should not notice any difference in functionality. If, however, you do manually download and install SRU, VDB, and GeoDB updates, make sure you download the correct package for your current version. Signed update files begin with 'Cisco' instead of 'Sourcefire,' and terminate in .sh.REL.tar instead of .sh, as follows: • SRU: Cisco_Firepower_SRU-*date-build*-vrt.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-*version*.sh.REL.tar • GeoDB: Cisco_GEODB_Update-*date-build*.sh.REL.tar We will provide both signed and unsigned updates until the end-of-support for versions that require unsigned updates. Do not untar signed (.tar) packages. If you accidentally upload a signed update to an older FMC or ASA FirePOWER device, you must manually delete it. Leaving the package takes up disk space, and also may cause issues with future upgrades.

Table 24: Version 6.2.3 Features

Feature	Details
Device Upgrade	
Copy upgrade packages to managed devices before the upgrade.	You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window. When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary. New/modified screens: **System**(⚙) > **Updates**
Content Updates	
FMC warns of Snort restart before VDB updates.	The FMC now warns you that Vulnerability Database (VDB) updates restart the Snort process. This interrupts traffic inspection and, depending on how the managed device handles traffic, possibly interrupts traffic flow. You can cancel the install until a more convenient time, such as during a maintenance window. These warnings can appear: • After you download and manually install a VDB. • When you create a scheduled task to install the VDB. • When the VDB installs in the background, such as during a previously scheduled task or as part of a software upgrade.

Feature	Details
Deprecated: Geolocation details	We no longer provide the geolocation IP package, which contained contextual data associated with routable IP addresses. This saves disk space and does not affect geolocation rules or traffic handling in any way. Any contextual data is now stale, and upgrading to most later versions deletes the IP package. Options to download the IP package or view contextual data have no effect, and are removed in later versions.