



## Troubleshooting and Reference

- [Troubleshooting Upgrade Package Management, on page 1](#)
- [Troubleshooting Threat Defense Upgrade, on page 2](#)
- [Traffic Flow and Inspection, on page 4](#)
- [Time and Disk Space, on page 7](#)
- [Upgrade Feature History, on page 9](#)

### Troubleshooting Upgrade Package Management

Table 1:

Issue	Solution
No available upgrades even after I refresh.	Direct-downloading upgrade packages requires internet access on the management center. You will also see a blank list if you are already running the latest version available for your deployment <i>and</i> you have no upgrade packages loaded/configured.
The 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 <i>right now</i> are listed and available for direct download. Unless you manually upload, the following are not listed: <ul style="list-style-type: none"><li>• Device upgrades (major and maintenance) to a particular version, unless the management center is running that version or higher, <i>and</i> you have a device that supports that version.</li><li>• Device patches, unless you have at least one device at the appropriate maintenance release. This also applies to management center patches.</li><li>• Hotfixes. You must manually upload these.</li></ul>

Issue	Solution
I see available, undownloaded packages that don't apply to my devices.	The system lists the downloadable upgrades that apply to <i>all</i> devices managed by this management center. In a multidomain deployment, this can include devices that you cannot access right now.

# Troubleshooting Threat Defense Upgrade

## Troubleshooting Upgrade Setup

Table 2:

Issue	Solution
<b>Upgrade</b> button missing for my target version on the Product Upgrades page.	Either of: <ul style="list-style-type: none"> <li>• You still need the upgrade package.</li> <li>• You do not have anything that can be upgraded to that version right now.</li> </ul>
Devices not listed in the upgrade wizard.	<p>If you accessed the wizard directly from <b>Devices &gt; Threat Defense Upgrade</b>, the workflow may be blank.</p> <p>To begin, choose a target version from the <b>Upgrade to</b> menu. The system determines which devices can be upgraded to that version and displays them in the Device Details pane. Note that the choices in the <b>Upgrade to</b> menu correspond to the device upgrade packages on the management center. If your target version is not listed, click <b>Manage Upgrade Packages</b> to upload it; see <a href="#">Uploading/Downloading Upgrade Packages to the Management Center</a>.</p> <p>If you have a target version but the wizard still does not list any devices, 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.</p>
Devices locked to someone else's upgrade workflow.	<p>If you need to reset someone else's workflow, you must have Administrator access. You can either:</p> <ul style="list-style-type: none"> <li>• Delete or deactivate the user.</li> <li>• Update the user's role so they no longer have permission to use <b>System (⚙️) &gt; Product Upgrades</b>.</li> </ul>

Issue	Solution
<p>Copying upgrade packages from the management center to managed devices times out.</p>	<p>This often happens when there is limited bandwidth between the management center and its devices.</p> <p>You can try one of:</p> <ul style="list-style-type: none"> <li>• Configure devices to get upgrade packages directly from an internal web server.</li> </ul> <p>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 <a href="#">Copy Upgrade Packages from an Internal Server</a>.</p> <ul style="list-style-type: none"> <li>• Copy upgrade packages from another device.</li> </ul> <p>If you can get the upgrade package to at least one standalone device, you can then use the threat defense CLI to copy upgrade packages ("peer to peer sync") to the other standalone devices managed by the same standalone management center. See <a href="#">Copy Threat Defense Upgrade Packages between Devices</a>.</p>
<p>High availability management center failed over while setting up upgrade.</p>	<p>Neither your workflow nor threat defense upgrade packages are synchronized between high availability management centers.</p> <p>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.)</p>

## Troubleshooting In-Progress Upgrade Issues and Failures

Table 3:

Issue	Solution
<p>Cannot reach the device.</p>	<p>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.</p> <p>You should also be able to access the management center's management interface without traversing the device.</p>
<p>Device appears inactive or is unresponsive.</p>	<p>You can manually cancel in-progress major and maintenance upgrades. If the device is unresponsive, or if you cannot cancel the upgrade, contact Cisco TAC. Do not manually reboot or shut down. You could place the system in an unusable state and require a reimage.</p>

Issue	Solution
Upgrade failed.	<p>When you initiate a major or maintenance upgrade, you use the <b>Automatically cancel on upgrade failure...</b> (auto-cancel) option to choose what happens if upgrade fails, as follows:</p> <ul style="list-style-type: none"> <li>• Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. Correct any issues and try again later.</li> <li>• Auto-cancel disabled: If upgrade fails, the device remains as it is. Correct the issues and retry immediately, or manually cancel the upgrade and try again later.</li> </ul> <p>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.</p> <p>If you cannot retry or cancel, or if you continue to have issues, contact Cisco TAC.</p>
I want to retry or cancel a failed upgrade.	Use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page.
I want to cancel an in-progress upgrade.	Use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page.

## 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: <b>Bypass: Force</b>	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: <b>Bypass: Standby</b>	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: <b>Bypass: Disabled</b>	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 device reboots twice—once for FXOS and once for the firmware. This includes Version 7.4.1+ chassis upgrades for the Secure Firewall 3100 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. For more information, see [Upgrading Chassis with High Availability or Clustered Devices](#).

**Table 5: Traffic Flow and Inspection: FXOS Upgrades**

Threat Defense Deployment	Traffic Behavior	Method
Standalone	Dropped.	—
High availability	Unaffected.	<b>Best Practice:</b> 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.	<b>Best Practice:</b> 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: <b>Bypass: Standby</b> or <b>Bypass-Force</b> .
	Dropped until at least one module is online.	Hardware bypass disabled: <b>Bypass: Disabled</b> .
	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, <b>Failsafe</b> enabled or disabled.	Passed without inspection.  A few packets might drop if <b>Failsafe</b> is disabled and Snort is busy but not down.
	Inline set, <b>Snort Fail Open: Down:</b> disabled.	Dropped.
	Inline set, <b>Snort Fail Open: Down:</b> 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 Upgrades](#).

**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.

Consideration	Details
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 those things 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

The readiness check should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails.

**Table 8: Checking Disk Space**

Platform	Command
Management Center	Choose <b>System &gt; Monitoring &gt; Statistics</b> and select the management center. Under Disk Usage, expand the By Partition details.
Threat Defense with management center	Choose <b>System &gt; Monitoring &gt; Statistics</b> and select the device you want to check. Under Disk Usage, expand the By Partition details.



# Upgrade Feature History

Table 9: Version 7.4.1 Features

Feature	Min. Threat Defense	Description
<p>Improved upgrade starting page and package management.</p>	<p>Any</p>	<p>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.</p> <p>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.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• <b>System (⚙️) &gt; Product Upgrades</b> is now where you upgrade the management center and all managed devices, as well as manage upgrade packages.</li> <li>• <b>System (⚙️) &gt; Content Updates</b> is now where you update intrusion rules, the VDB, and the GeoDB.</li> <li>• <b>Devices &gt; Threat Defense Upgrade</b> takes you directly to the threat defense upgrade wizard.</li> <li>• <b>System (⚙️) &gt; Users &gt; User Role &gt; Create User Role &gt; Menu-Based Permissions</b> allows you to grant access to <b>Content Updates</b> (VDB, GeoDB, intrusion rules) without allowing access to <b>Product Upgrades</b> (system software).</li> </ul> <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> <li>• <b>System (⚙️) &gt; Updates</b> is deprecated. All threat defense upgrades now use the wizard.</li> <li>• The <b>Add Upgrade Package</b> button on the threat defense upgrade wizard has been replaced by a <b>Manage Upgrade Packages</b> link to the new upgrade page.</li> </ul> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a></p>
<p>Enable revert from the threat defense upgrade wizard.</p>	<p>Any, if upgrading to 7.1+</p>	<p>You can now enable revert from the threat defense upgrade wizard.</p> <p>Other version restrictions: You must be upgrading threat defense to Version 7.1+.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a></p>

Feature	Min. Threat Defense	Description
View detailed upgrade status from the threat defense upgrade wizard.	Any	<p>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, <b>Devices &gt; Threat Defense Upgrade</b> brings you back to this final wizard page, where you can view the detailed status for the current (or most recently complete) device upgrade.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a></p>
Automatically generate configuration change reports after management center upgrade.	Any	<p>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.</p> <p>Other 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.</p> <p>New/modified screens: <b>System (⚙️) &gt; Configuration &gt; Upgrade Configuration &gt; Enable Post-Upgrade Report</b></p> <p>See: <a href="#">Upgrade Configuration</a></p>
Suggested release notifications.	Any	<p>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.</p> <p>See: <a href="#">Cisco Secure Firewall Management Center New Features by Release</a></p>
New upgrade wizard for the management center.	Any	<p>A new upgrade starting page and wizard make it easier to perform management center upgrades. After you use <b>System (⚙️) &gt; Product Upgrades</b> to get the appropriate upgrade package onto the management center, click <b>Upgrade</b> to begin.</p> <p>Other version restrictions: Only supported for management center upgrades from Version 7.4.1+.</p> <p>To upgrade the management center to any version, see the upgrade guide for the version your management center is <i>currently</i> running: : <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a>. If you are running Version 7.4.0, you can use the Version 7.3.x guide.</p>
Hotfix high availability management centers without pausing synchronization.	Any	<p>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.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a></p>

Feature	Min. Threat Defense	Description
Firmware upgrades included in FXOS upgrades.	Any	<p><b>Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.</b></p> <p>For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. Secure Firewall 3100 in multi-instance mode (new in Version 7.4.1) also bundles FXOS and 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.</p> <p>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.</p> <p>See: <a href="#">Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide</a></p>
Chassis upgrade for the Secure Firewall 3100 in multi-instance mode.	7.4.1	<p>For the Secure Firewall 3100 in multi-instance mode, you upgrade the operating system and the firmware (<i>chassis upgrade</i>) separately from the container instances (<i>threat defense upgrade</i>).</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• Upgrade the chassis: <b>Devices &gt; Chassis Upgrade</b></li> <li>• Upgrade threat defense: <b>Devices &gt; Threat Defense Upgrade</b></li> </ul> <p>Supported platforms: Secure Firewall 3100, excluding the Secure Firewall 3105</p> <p>Minimum management center: 7.4.1</p>
Updated internet access requirements for direct-downloading software upgrades.	Any	<p><b>Upgrade impact. The system connects to new resources.</b></p> <p>The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com.</p> <p>See: <a href="#">Internet Access Requirements</a></p>
Scheduled tasks download patches and VDB updates only.	Any	<p><b>Upgrade impact. Scheduled download tasks stop retrieving maintenance releases.</b></p> <p>The <b>Download Latest Update</b> 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 <b>System (⚙️) &gt; Product Upgrades</b>.</p> <p>See: <a href="#">Software Update Automation</a></p>

Table 10: Version 7.4.0 Features

Feature	Min. Threat Defense	Description
<b>Content Updates</b>		

Feature	Min. Threat Defense	Description
Download only the country code geolocation package.	Any	<p>You can now configure the system to download only the country code package of the geolocation database (GeoDB), which maps IP addresses to countries/continents. The larger IP package that contains contextual data, including additional location details and connection information, is now optional. By default, the system downloads both packages.</p> <p>New/modified screens: <b>System (⚙️) &gt; Updates &gt; Geolocation Updates &gt; IP Package Configuration</b></p> <p>See : <a href="#">Update the Geolocation Database</a></p>

Table 11: Version 7.3.0 Features

Feature	Min. Threat Defense	Description
<b>Product Upgrades</b>		
Choose and direct-download upgrade packages to the management center from Cisco.	Any	<p>You can now choose which threat defense upgrade packages you want to direct download to the management center. Use the new <b>Download Updates</b> sub-tab on <b>&gt; Updates &gt; Product Updates</b>.</p> <p>Minimum management center: 7.3.0. In Version 7.4.1+, this feature is replaced by an improved package management system.</p> <p>See: <a href="#">Download Upgrade Packages with the Management Center</a></p>
Upload upgrade packages to the management center from the threat defense wizard.	Any	<p>You now use the wizard to upload threat defense upgrade packages or specify their location. Previously you used <b>System (⚙️) &gt; Updates</b>.</p> <p>Minimum management center: 7.3.0. In Version 7.4.1+, this feature is replaced by an improved package management system.</p> <p>See: <a href="#">Upgrade Threat Defense</a></p>
Select devices to upgrade from the threat defense upgrade wizard.	Any	<p>Use the wizard to select devices to upgrade.</p> <p>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.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a></p>
Unattended threat defense upgrades.	Any	<p>The threat defense upgrade wizard now supports unattended upgrades, using a new <b>Unattended Mode</b> 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.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a></p>

Feature	Min. Threat Defense	Description
Simultaneous threat defense upgrade workflows by different users.	Any	<p>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.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a></p>
Skip pre-upgrade troubleshoot generation for threat defense devices.	Any	<p>You can now skip the automatic generating of troubleshooting files before major and maintenance upgrades by disabling the new <b>Generate troubleshooting files before upgrade begins</b> option. This saves time and disk space.</p> <p>To manually generate troubleshooting files for a threat defense device, choose <b>System (⚙️) &gt; Health &gt; Monitor</b>, click the device in the left panel, then <b>View System &amp; Troubleshoot Details</b>, then <b>Generate Troubleshooting Files</b>.</p> <p>See: <a href="#">Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</a></p>
Auto-upgrade to Snort 3 after successful threat defense upgrade is no longer optional.	Any	<p><b>Upgrade impact.</b></p> <p>When you upgrade threat defense to Version 7.3+, you can no longer disable the <b>Upgrade Snort 2 to Snort 3</b> option.</p> <p>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 will be deprecated in a future release and we strongly recommend you stop using it now.</p> <p>For devices that are ineligible for auto-upgrade because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the <a href="#">Cisco Secure Firewall Management Center Snort 3 Configuration Guide</a> for your version.</p>

Feature	Min. Threat Defense	Description
Combined upgrade and install package for Secure Firewall 3100.	7.3.0	<p><b>Reimage Impact.</b></p> <p>In Version 7.3, we combined the threat defense install and upgrade package for the Secure Firewall 3100, as follows:</p> <ul style="list-style-type: none"> <li>• Version 7.1–7.2 install package: <code>cisco-ftd-fp3k.version.SPA</code></li> <li>• Version 7.1–7.2 upgrade package: <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code></li> <li>• Version 7.3+ combined package: <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code></li> </ul> <p>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.</p> <p>To get to threat defense Version 7.3+, your options are:</p> <ul style="list-style-type: none"> <li>• Upgrade from threat defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate <a href="#">Upgrade Guide</a>.</li> <li>• Reimage from threat defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to threat defense Version 7.3+. <ul style="list-style-type: none"> <li>See <i>Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100</i> and then <i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i> in the <a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a>.</li> </ul> </li> <li>• Reimage from ASA 9.17 or 9.18 — upgrade to ASA 9.19+ first, then reimage to threat defense Version 7.3+. <ul style="list-style-type: none"> <li>See the <a href="#">Cisco Secure Firewall ASA Upgrade Guide</a> and then <i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i> in the <a href="#">Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide</a>.</li> </ul> </li> <li>• Reimage from threat defense Version 7.3+ — use the normal reimage process. <ul style="list-style-type: none"> <li>See <i>Reimage the System with a New Software Version</i> in the <a href="#">Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense</a>.</li> </ul> </li> </ul>

## Content Updates

Feature	Min. Threat Defense	Description
Automatic VDB downloads.	Any	<p>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.</p> <p>New/modified screens: The <b>Vulnerability Database</b> check box is now enabled by default in the system-created <b>Weekly Software Download</b> scheduled task.</p>
Install any VDB.	Any	<p>Starting with VDB 357, you can now install any VDB as far back as the baseline VDB for that management center.</p> <p>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.</p> <p>New/modified screens: On <b>System</b> (⚙️) &gt; <b>Updates</b> &gt; <b>Product Updates</b> &gt; <b>Available Updates</b>, if you upload an older VDB, a new <b>Rollback</b> icon appears instead of the <b>Install</b> icon.</p>

Table 12: Version 7.2.0 Features

Feature	Description
<b>Threat Defense Upgrades</b>	

Feature	Description
<p>Copy upgrade packages ("peer-to-peer sync") from device to device.</p>	<p>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.</p> <p>This feature is supported for Version 7.2+ standalone devices managed by the same standalone management center. It is not supported for:</p> <ul style="list-style-type: none"> <li>• Container instances.</li> <li>• Device high availability pairs and clusters.</li> </ul> <p>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.</p> <ul style="list-style-type: none"> <li>• Devices managed by high availability management centers.</li> <li>• Devices managed by the cloud-delivered management center, but added to a customer-deployed management center in analytics mode.</li> <li>• Devices in different domains, or devices separated by a NAT gateway.</li> <li>• Devices upgrading from Version 7.1 or earlier, regardless of management center version.</li> </ul> <p>New/modified CLI commands: <b>configure p2psync enable</b>, <b>configure p2psync disable</b>, <b>show peers</b>, <b>show peer details</b>, <b>sync-from-peer</b>, <b>show p2p-sync-status</b></p>
<p>Auto-upgrade to Snort 3 after successful threat defense upgrade.</p>	<p>When you use a Version 7.2+ management center to upgrade threat defense, you can now choose whether to <b>Upgrade Snort 2 to Snort 3</b>.</p> <p>After the software upgrade, eligible devices will 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 migration assistance, see the <a href="#">Cisco Secure Firewall Management Center Snort 3 Configuration Guide</a> for your version.</p> <p>This option is supported for major and maintenance threat defense upgrades to Version 7.2+. It is not supported for threat defense upgrades to Version 7.0 or 7.1, or for patches to any version.</p>
<p>Upgrade for single-node clusters.</p>	<p>You can now use the device upgrade page (<b>Devices &gt; Device Upgrade</b>) 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 (<b>System (⚙️)Updates</b>).</p> <p>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.</p> <p>Supported platforms: Firepower 4100/9300, Secure Firewall 3100</p>



Feature	Description
Revert threat defense upgrades from the CLI.	<p>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.</p> <p><b>Caution</b> 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.</p> <p>New/modified CLI commands: <b>upgrade revert</b>, <b>show upgrade revert-info</b>.</p>
<b>Management Center Upgrades</b>	
Management center upgrade does not automatically generate troubleshooting files.	<p>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.</p> <p>To manually generate troubleshooting files for the management center, choose <b>System (⚙️) &gt; Health &gt; Monitor</b>, click <b>Firewall Management Center</b> in the left panel, then <b>View System &amp; Troubleshoot Details</b>, then <b>Generate Troubleshooting Files</b>.</p>
<b>Content Updates</b>	
GeoDB is split into two packages.	<p>In May 2022, shortly before the Version 7.2 release, we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on.</p> <p>If your Version 7.2+ management center has internet access and you enable recurring updates or you manually kick off a one-time update from the Cisco Support &amp; Download site, the system automatically obtains and imports both packages. However, if you manually download updates—for example, in an air-gapped deployment—make sure you get and import both GeoDB packages:</p> <ul style="list-style-type: none"> <li>• Country code package: Cisco_GEODB_Update-<i>date-build</i>.sh.REL.tar</li> <li>• IP package: Cisco_IP_GEODB_Update-<i>date-build</i>.sh.REL.tar</li> </ul> <p>The Geolocation Updates (<b>System (⚙️) &gt; Updates &gt; Geolocation Updates</b>) page and the About page (<b>Help &gt; About</b>) list the versions of the packages currently being used by the system.</p>

Table 13: Version 7.1.0 Features

Feature	Description
<b>Product Upgrades</b>	

Feature	Description
<p>Revert a successful device upgrade.</p>	<p>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 <i>snapshot</i>. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade.</p> <p><b>Important</b> If you think you might need to revert, you must use <b>System (⚙️) &gt; Updates</b> to upgrade FTD. The System Updates page is the only place you can enable the <b>Enable revert after successful upgrade</b> 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 <b>Devices &gt; Device Upgrade</b> page.</p> <p>This feature is not supported for container instances.</p> <p>Minimum FTD: 7.1</p> <p>Minimum threat defense: 7.1</p>
<p>Improvements to the upgrade workflow for clustered and high availability devices.</p>	<p>We made the following improvements to the upgrade workflow for clustered and high availability devices:</p> <ul style="list-style-type: none"> <li>• 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.</li> <li>• 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.</li> <li>• You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.</li> </ul>

Table 14: Version 7.0.0 Features

Feature	Description
<p><b>Product Upgrades</b></p>	
<p>Improved FTD upgrade performance and status reporting.</p>	<p>FTD upgrades are now easier faster, more reliable, and take up less disk space. A new <b>Upgrades</b> tab in the Message Center provides further enhancements to upgrade status and error reporting.</p>

Feature	Description
<p>Easy-to-follow upgrade workflow for FTD devices.</p>	<p>A new device upgrade page (<b>Devices &gt; Device Upgrade</b>) 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.</p> <p>To begin, use the new <b>Upgrade Firepower Software</b> action on the Device Management page (<b>Devices &gt; Device Management &gt; Select Action</b>).</p> <p>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.</p> <p>If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard.</p> <p><b>Note</b> You must still use <b>System (⚙️) &gt; Updates</b> 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.</p> <p><b>Note</b> 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.</p> <p>To avoid possible time-consuming upgrade failures, <i>manually</i> ensure all group members are ready to move on to the next step of the wizard before you click <b>Next</b>.</p>

Feature	Description
Upgrade more FTD devices at once.	<p>The FTD upgrade wizard lifts the following restrictions:</p> <ul style="list-style-type: none"> <li>• Simultaneous device upgrades.</li> </ul> <p>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.</p> <p><b>Important</b> Only upgrades to FTD Version 6.7+ 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.</p> <ul style="list-style-type: none"> <li>• Grouping upgrades by device model.</li> </ul> <p>You can now queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages.</p> <p>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 <i>only</i> 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.</p>

Table 15: Version 6.7.0 Features

Feature	Description
Product Upgrades	

Feature	Description
<p>Improved FTD upgrade status reporting and cancel/retry options.</p>	<p>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.</p> <p>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.</p> <p>Also on this pop-up, you can manually cancel failed or in-progress upgrades (<b>Cancel Upgrade</b>), or retry failed upgrades (<b>Retry Upgrade</b>). Canceling an upgrade reverts the device to its pre-upgrade state.</p> <p><b>Note</b> 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: <b>Automatically cancel on upgrade failure and roll back to the previous version</b>. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure.</p> <p>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.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> <li>• <b>System (⚙️) &gt; Updates &gt; Product Updates &gt; Available Updates &gt; Install</b> icon for the FTD upgrade package</li> <li>• <b>Devices &gt; Device Management &gt; Upgrade</b></li> <li>• <b>Message Center &gt; Tasks</b></li> </ul> <p>New/modified CLI commands: <b>show upgrade status detail, show upgrade status continuous, show upgrade status, upgrade cancel, upgrade retry</b></p>
<p>Upgrades remove PCAP files to save disk space.</p>	<p>Upgrades now remove locally stored PCAP files. To upgrade, you must have enough free disk space or the upgrade fails.</p>
<p><b>Content Updates</b></p>	
<p>Custom intrusion rule import warns when rules collide.</p>	<p>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.</p> <p>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.</p> <p>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.</p> <p>New/modified screens: We added a warning icon to <b>System (⚙️) &gt; Updates &gt; Rule Updates</b>.</p>

Table 16: Version 6.6.0 Features

Feature	Description
<b>Product Upgrades</b>	
Get FTD upgrade packages from an internal web server.	<p>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.</p> <p><b>Note</b> This feature is supported only for FTD devices running Version 6.6+. It is not supported for upgrades <i>to</i> Version 6.6, nor is it supported for the FMC or Classic devices.</p> <p>New/modified screens: We added a <b>Specify software update source</b> option to the page where you upload upgrade packages.</p>
<b>Content Updates</b>	
Automatic VDB update during initial setup.	<p>When you set up a new or reimaged FMC, the system automatically attempts to update the vulnerability database (VDB).</p> <p>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.</p>

Table 17: Version 6.5.0 Features

Feature	Description
<b>Content Updates</b>	
Automatic software downloads and GeoDB updates.	<p>When you set up a new or reimaged FMC, the system automatically schedules:</p> <ul style="list-style-type: none"> <li>• A weekly task to download software updates for the FMC and its managed devices.</li> <li>• Weekly updates for the GeoDB.</li> </ul> <p>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.</p>

Table 18: Version 6.4.0 Features

Feature	Description
Upgrades postpone scheduled tasks.	<p>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.</p> <p><b>Note</b> 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.</p> <p>Note that this feature is supported for all upgrades <i>from</i> 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 <i>to</i> a supported version from an unsupported version.</p>
<b>Content Updates</b>	
Signed SRU, VDB, and GeoDB updates.	<p>So the system can verify that you are using the correct update files, Version 6.4+ uses <i>signed</i> updates for intrusion rules (SRU), the vulnerability database (VDB), and the geolocation database (GeoDB). Earlier versions continue to use unsigned updates.</p> <p>Unless you manually download updates from the Cisco Support &amp; 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.</p> <p>Signed update files begin with 'Cisco' instead of 'Sourcefire,' and terminate in .sh.REL.tar instead of .sh, as follows:</p> <ul style="list-style-type: none"> <li>• SRU: Cisco_Firepower_SRU-<i>date-build-vrt</i>.sh.REL.tar</li> <li>• VDB: Cisco_VDB_Fingerprint_Database-4.5.0-<i>version</i>.sh.REL.tar</li> <li>• GeoDB: Cisco_GEODB_Update-<i>date-build</i>.sh.REL.tar</li> </ul> <p>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.</p>

Table 19: Version 6.2.3 Features

Feature	Description
<b>Product Upgrades</b>	

Feature	Description
<p>Copy upgrade packages to managed devices before the upgrade.</p>	<p>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.</p> <p>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.</p> <p>New/modified screens: <b>System</b> (⚙️) &gt; <b>Updates</b></p>
<p><b>Content Updates</b></p>	
<p>FMC warns of Snort restart before VDB updates.</p>	<p>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.</p> <p>These warnings can appear:</p> <ul style="list-style-type: none"> <li>• After you download and manually install a VDB.</li> <li>• When you create a scheduled task to install the VDB.</li> <li>• When the VDB installs in the background, such as during a previously scheduled task or as part of a software upgrade.</li> </ul>