Getting Started

Is this Guide for You?

This guide explains how to use a **Secure Firewall Management Center** currently running **Version 7.2** to prepare for and successfully complete:

- Upgrade of currently managed threat defense devices *as far as* Version 7.2.
- Upgrade of the management center to releases *after* Version 7.2.

Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. We also may provide hotfixes, which are minor updates that address particular, urgent issues.

Additional Resources

If you are upgrading a different platform/component, upgrading to/from a different version, or are using a cloud-based manager, see one of these resources.

Table 1: Upgrading Management Center

Current Management Center Version	Guide
Cloud-delivered management center (no version)	None. We take care of updates.
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version.
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1.
7.0 or earlier	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Table 2: Upgrading Threat Defense with Management Center

Current Management Center Version	Guide
Cloud-delivered management center (no version)	The latest released version of the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center.
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version.
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1.
7.0 or earlier	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Table 3: Upgrading Threat Defense with Device Manager

Current Threat Defense Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager for your version.
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager, Version 7.1.
7.0 or earlier	*System Management* in the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager for your version. For the Firepower 4100/9300, also see the FXOS upgrade instructions in the Cisco Firepower 4100/9300 Upgrade Guide, FTD 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1.
Version 6.4+, with CDO	*Onboard Devices and Services* in Managing FDM Devices with Cisco Defense Orchestrator.

Table 4: Upgrading NGIPS Devices

Current Manager Version	Platform	Guide
Any	Firepower 7000/8000 series	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.
Any	ASA FirePOWER with FMC	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.
Any	ASA FirePOWER with ASDM	Cisco Secure Firewall ASA Upgrade Guide.

Table 5: Upgrading Other Components

Version	Component	Guide
Any	ASA logical devices on the Firepower 4100/9300	Cisco Secure Firewall ASA Upgrade Guide.
Latest	BIOS and firmware for management center	Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes.
Latest	Firmware for the Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide
Latest	ROMMON image for the ISA 3000	Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the upgrade chapters.

Table 6: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up configurations and events. Back up FXOS on the Firepower 4100/9300.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300.

Planning Phase	Includes
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Feature History

Table 7: Version 7.2.0 Features

Feature	Description
Threat Defense Upgrades	
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+ standalone devices managed by the same standalone management center. It is not supported for: • Container instances. • Device high availability pairs and clusters. These devices get the package from each other as part of their normal sync process. Copying the upgrade package to one group member automatically syncs it to all group members. • Devices managed by high availability management centers. • Devices managed by the cloud-delivered management center, but added to a customer-deployed management center in analytics mode. • Devices in different domains, or devices separated by a NAT gateway. • Devices upgrading from Version 7.1 or earlier, regardless of management center version. New/modified CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status** Minimum threat defense: 7.2

Feature	Description
Auto-upgrade to Snort 3 after successful threat defense upgrade.	When you use a Version 7.2+ management center to upgrade threat defense, you can now choose whether to **Upgrade Snort 2 to Snort 3**. 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 Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version. 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.
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
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 Upgrades	
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**.
Content Updates	

Feature	Description
GeoDB is split into two packages.	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. 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 & 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: • Country code package: Cisco_GEODB_Update-*date-build*.sh.REL.tar • IP package: Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar The Geolocation Updates (**System** (⚙) **> Updates > Geolocation Updates**) page and the About page (**Help > About**) list the versions of the packages currently being used by the system.

Table 8: Version 7.1.0 Features

Feature	Description
Product Upgrades	
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 Minimum threat defense: 7.1

Feature	Description
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 9: Version 7.0.0 Features

Feature	Description
Product Upgrades	
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	Description
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**.

Feature	Description
Upgrade more FTD devices at once.	The FTD upgrade wizard lifts the following restrictions: • Simultaneous device upgrades. 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+ 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. • Grouping upgrades by device model. 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. 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 10: Version 6.7.0 Features

Feature	Description
Product Upgrades	

Feature	Description
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**
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.
Content Updates	
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 11: Version 6.6.0 Features

Feature	Description
Product Upgrades	
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 12: Version 6.5.0 Features

Feature	Description
Content Updates	
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 13: Version 6.4.0 Features

Feature	Description
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	
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 14: Version 6.2.3 Features

Feature	Description
Product Upgrades	

Feature	Description
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.

For Assistance

Online Resources

Cisco provides the following online resources to download documentation, software, and tools; to query bugs; and to open service requests. Use these resources to install and configure Cisco software and to troubleshoot and resolve technical issues.

- Documentation: http://www.cisco.com/go/threatdefense-72-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts