Getting Started

Is this Guide for You?

This guide explains how to use a **Secure Firewall Management Center** currently running **Version 7.3** to prepare for and successfully complete:

- Upgrade of currently managed threat defense devices *as far as* Version 7.3.
- Upgrade of the management center to releases *after* Version 7.3.

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 7.3.0 Features

Feature	Description
Usability improvements.	We introduced some usability improvements to the threat defense upgrade wizard: • You can now use the wizard to select devices to upgrade. 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. • You can now use the wizard to upload threat defense upgrade packages or specify upgrade package locations. Previously, you could only use the System Updates page. • 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. For all threat defense upgrades, we offer smaller upgrade packages and faster upgrades and readiness checks.

Feature	Description
Unattended upgrades.	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. With an unattended upgrade, the system automatically copies needed upgrade packages to devices, performs compatibility and readiness checks, and begins the upgrade. Just as happens when you manually step through the wizard, any devices that do not "pass" a stage in the upgrade (for example, failing checks) are not included in the next stage. After the upgrade completes, you pick up with the verification and post-upgrade tasks. You can pause and restart unattended mode during the copy and checks phases. However, pausing unattended mode does *not* stop tasks in progress. Copies and checks that have started will run to completion. Similarly, you cannot cancel an upgrade in progress by stopping unattended mode; to cancel an upgrade, use the Upgrade Status pop-up, accessible from the Upgrade tab on Device Management page, and from the Message Center.
Skip pre-upgrade troubleshoot generation.	From the threat defense upgrade wizard, 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**.
Auto-upgrade to Snort 3 after successful threat defense upgrade is no longer optional.	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 will be deprecated in a future release and we strongly recommend you stop using it now. 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 Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version. Minimum threat defense: Any
Choose and direct-download select upgrade packages from Cisco.	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**.

Table 8: Version 7.2.0 Features

Feature	Description
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
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.

Feature	Description
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**.
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 9: Version 7.1.0 Features

Feature	Description
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 threat defense, customer-deployed managagement center: 7.1 Minimum threat defense, cloud-delivered Firewall Management Center: 7.2
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 10: Version 7.0.0 Features

Feature	Description
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 11: Version 6.7.0 Features

Feature	Description
Improved threat defense upgrade status reporting and cancel/retry options.	You can now view the status of threat defense 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 upgrade: **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 a high availability/scalability 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** > **Update** > **Product Updates** > **Available Updates** > **Install** icon for the threat defense upgrade package • **Devices** > **Device Management** > **Upgrade** • **Message Center > Tasks** New threat defense 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.

Table 12: Version 6.6.0 Features

Feature	Description
Get device upgrade packages from an internal web server.	Devices can now get upgrade packages from your own internal web server, rather than from the management center. This is especially useful if you have limited bandwidth between the management center and its devices. It also saves space on the management center. New/modified screens: **System** > **Updates** > **Upload Update** button > **Specify software update source** option
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.

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.

Table 14: Version 6.2.3 Features

Feature	Description
Copy upgrade packages to managed devices before the upgrade.	You can now copy (or push) an upgrade package from the management center 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**

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-73-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