Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.2.6–7.2.x

First Published: 2024-03-19

Last Modified: 2024-03-19

CONTENTS

CHAPTER **1**

Planning Your Upgrade

Use this guide to plan and complete threat defense and management center upgrades. 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.

Is This Guide for You?

The upgrade procedures in this guide are for:

- Upgrading the managagement center *from* Version Version 7.2.6 or later maintenance release.

- Upgrading threat defense (usually to Version 7.2) with a management center that is *already running* Version 7.2.6 or later maintenance release.

This means that after you use this guide to upgrade the management center, you need to use a different guide to upgrade threat defense.

Compatibility

Before you upgrade, make sure the target version is compatible with your deployment. If you cannot upgrade due to incompatibility, contact your Cisco representative or partner contact for refresh information.

For compatibility information, see:

- Cisco Secure Firewall Management Center Compatibility Guide

- Cisco Secure Firewall Threat Defense Compatibility Guide

- Cisco Firepower 4100/9300 FXOS Compatibility

Upgrade Guidelines

Software Upgrade Guidelines

This guide contains upgrade procedures for your current management center version. For release-specific upgrade guidelines, including features with upgrade impact, check the release notes for your target version.

Table 1: Cisco Secure Firewall Threat Defense Release Notes

Target Version	Release Notes
7.2.x	https://cisco.com/go/fmc-ftd-release-notes-72
7.1.x	Cisco Firepower Release Notes, Version 7.1.x
7.0.x	Cisco Firepower Release Notes, Version 7.0.x
6.7.x	Cisco Firepower Release Notes, Version 6.7.x
6.6.x	Cisco Firepower Release Notes, Version 6.6.x

FXOS Upgrade Guidelines for the Firepower 4100/9300

For release-specific FXOS upgrade guidelines, check the release notes for your target version. For bugs that could affect your deployment, check the release notes between your current and target version.

Table 2: Cisco Firepower 4100/9300 FXOS Release Notes

Target Threat Defense	Target FXOS	Release Notes
7.2	2.12	Cisco Firepower 4100/9300 FXOS Release Notes, 2.12(1)
7.1	2.11	Cisco Firepower 4100/9300 FXOS Release Notes, 2.11(1)
7.0	2.10	Cisco Firepower 4100/9300 FXOS Release Notes, 2.10(1)
6.7	2.9	Cisco Firepower 4100/9300 FXOS Release Notes, 2.9(1)
6.6	2.8	Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1)

Firmware Upgrade Guidelines for the Firepower 4100/9300

For firmware upgrade guidelines, check the firmware upgrade guide: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

Upgrade Path

Planning your upgrade path is especially important for large deployments, multi-hop upgrades, and situations where you need to coordinate related upgrades—operating systems, firmware, chassis, hosting environments, and so on.

Upgrade Path for Management Center

This table lists the minimum version to upgrade management center.

The management center must run the same or newer version as its managed devices. Upgrade the management center to your target version first, then upgrade devices. If you begin with devices running a much older version than the management center, further management center upgrades can be blocked. In this case you will need to perform a three (or more) step upgrade: devices first, then the management center, then devices again.

Table 3: Minimum Version to Upgrade Management Center

Target Version	Minimum Version to Upgrade	Oldest Device You Can Manage
7.4	7.0	7.0
7.3	7.0	6.7
7.2	6.6	6.6

Upgrade Path for Threat Defense

This table lists the minimum version to upgrade threat defense. If you are not running the minimum version, you will need to perform a multi-step upgrade. If a chassis upgrade is required, threat defense upgrade is blocked; see Upgrade Path for Threat Defense with Chassis Upgrade, on page 3.

Table 4: Minimum Version to Upgrade Threat Defense

Target Version	Minimum Version to Upgrade
7.4	7.0
7.3	7.0
7.2	6.6

Upgrade Path for Threat Defense with Chassis Upgrade

For the Firepower 4100/9300, major threat defense upgrades require chassis (FXOS and firmware) upgrades. Maintenance releases and patches rarely do. Chassis upgrades to FXOS 2.14.1+ include firmware, otherwise, see the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

Because you upgrade the chassis first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" ofthreat defense. If the chassis is already well ahead of its devices,

further chassis upgrades can be blocked. In this case you will need to perform a three (or more) step upgrade: devices first, then the chassis, then devices again. In high availability or clustered deployments, upgrade one chassis at a time; see Upgrade Order for Threat Defense with Chassis Upgrade and High Availability/Clusters, on page 4.

This table lists the minimum versions to upgrade threat defense when a chassis upgrade is required.

Table 5: Minimum Versions to Upgrade Threat Defense Chassis

Target Versions	Minimum Versions to Upgrade
Threat Defense 7.4 on FXOS 2.14.1.131+	Threat Defense 7.0 on FXOS 2.10
Threat Defense 7.3 on FXOS 2.13.0.198+	Threat Defense 7.0 on FXOS 2.10
Threat Defense 7.2 on FXOS 2.12.0.31+	Threat Defense 6.6 on FXOS 2.8

Upgrade Order for Threat Defense with Chassis Upgrade and High Availability/Clusters

When a chassis upgrade is required in high availability or clustered deployments, upgrade one chassis at a time.

Table 6: Chassis Upgrade Order for the Firepower 4100/9300 with Management Center

Threat Defense Deployment	Upgrade Order
Standalone	1. Upgrade chassis. 2. Upgrade threat defense.
High availability	Upgrade both chassis before you upgrade threat defense. To minimize disruption, always upgrade the standby. 1. Upgrade chassis with the standby. 2. Switch roles. 3. Upgrade chassis with the new standby. 4. Upgrade threat defense.
Intra-chassis cluster (units on the same chassis)	1. Upgrade chassis. 2. Upgrade threat defense.

Threat Defense Deployment	Upgrade Order
Inter-chassis cluster (units on different chassis)	Upgrade all chassis before you upgrade threat defense. To minimize disruption, always upgrade an all-data unit chassis. 1. Upgrade the all-data unit chassis. 2. Switch the control module to the chassis you just upgraded. 3. Upgrade all remaining chassis. 4. Upgrade threat defense.

Upgrade Packages

Uploading and Downloading Upgrade Packages to the Management Center

Manage upgrade packages on **System** (⚙) > **Product Upgrades**.

The page lists all upgrade packages that apply to you, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, or upload packages you manually downloaded: Upgrade Packages on Cisco.com, on page 9.

Table 7: Managing Upgrade Packages on the Management Center

To...	Do This...
Refresh the list of available upgrade packages.	Click **Refresh** (⟳) at the bottom left of the page.
Download an upgrade package to the management center from Cisco.	Click **Download** next to the upgrade package or version you want to download. Each family of devices has its own upgrade packages, so depending on your deployment you may need to download more than one upgrade package.
Manually upload an upgrade package to the management center.	Click **Add Upgrade Package** at the bottom right of the page, then **Choose File**.
Configure threat defense devices to get upgrade packages from an internal server.	Click **Add Upgrade Package** at the bottom right of the page, then **Specify Remote Location**. See Copy Upgrade Packages from an Internal Server, on page 7.

To...	Do This...
Delete an upgrade package from the management center.	Click the **Ellipsis (…)** next to the package you want to delete and select **Delete**. This deletes the package (or the pointer to the package) from the management center. It does not delete the package from any devices where you already copied the package. In most cases, upgrading threat defense removes the related upgrade package from the device.

Copying Upgrade Packages to Managed Devices

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

Copying Threat Defense Upgrade Packages

For threat defense upgrades, the easiest way to do this is to use the Product Upgrades page (**System (⚙)** > **Product Upgrades** on the management center to download the upgrade package from Cisco, then let the upgrade wizard prompt you to copy the package over.

The following table goes into more details about this and your other options.

Table 8: Copying Threat Defense Upgrade Packages to Managed Devices

Requirements	When to Use
Cisco → Management Center → Devices Major, maintenance, or patch upgrade (not a hotfix) that applies to the device *right now*. Internet access on the management center. Adequate disk space on the management center. Adequate bandwidth between the management center and devices.	Strongly recommended when all requirements are met. See: Uploading and Downloading Upgrade Packages to the Management Center, on page 5
Cisco → Your Computer → Management Center → Devices Adequate disk space on the management center. Adequate bandwidth between management center and devices.	You meet disk space and bandwidth requirements, but either the management center does not have internet access, or you are applying a hotfix. See: Upgrade Packages on Cisco.com, on page 9
Cisco → Your Computer → Internal Server → Devices Internal web server that devices can access.	You do not meet disk space requirements and/or bandwidth requirements (regardless of internet access or upgrade type). See: Copy Upgrade Packages from an Internal Server, on page 7

Requirements	When to Use
Device → Device Version 7.2+ standalone devices managed by the same standalone management center. At least one device that has obtained the upgrade package by another method.	You need to copy the upgrade package to devices without relying on the management center to mediate the transfer. See: Copy Threat Defense Upgrade Packages between Devices, on page 7

Copying Firepower 4100/9300 Chassis Upgrade Packages

For Firepower 4100/9300 chassis upgrade packages, download the upgrade package from Cisco, then use the chassis manager or CLI (FTP, SCP, SFTP, or TFTP) to copy the package to the device. See Upgrade Packages on Cisco.com, on page 9 and the upgrade procedure for your deployment.

Copy Upgrade Packages from an Internal Server

You can store threat defense upgrade packages on an internal server instead of 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.

After you get the packages from Cisco and set up your server, configure pointers to them. On the management center, start like you are uploading a a package: on the Product Upgrades page (**System** (⚙) > **Product Upgrades**, click **Add Upgrade Package**. But instead of choosing a file on your computer, click **Specify Remote Location** and provide the appropriate details. When it is time to get the package, the device will copy it from the internal server.

Table 9: Options for Copying Threat Defense Upgrade Packages from an Internal Server

Field	Description
URL	The source URL, including protocol (HTTP/HTTPS) and full path to the upgrade package; for example: `https://internal_web_server/upgrade_package.sh.REL.tar.`
CA Certificates	For secure web servers (HTTPS), the server's digital certificate (PEM format). Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines. You should be able to obtain the certificate from the server's administrator. You may also be able to use your browser, or a tool like OpenSSL, to view the server's certificate details and export or copy the certificate.

Copy Threat Defense Upgrade Packages between Devices

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 Firewall Management Center, but added to an on-prem 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.

Repeat the following procedure for all devices that need the upgrade package. For detailed information on all the CLI commands associated with this feature, see the Cisco Secure Firewall Threat Defense Command Reference.

Before you begin

- Upload the threat defense upgrade package to the management center or to an internal server.

- Copy the upgrade package to at least one device.

Step 1   As admin, SSH to any device that needs the package.

Step 2   Enable the feature.

configure p2psync enable

Step 3   If you do not already know, determine where you can get the upgrade package you need.

show peers: Lists the other eligible devices that also have this feature enabled.

show peer details *ip_address*: For the device at the IP address you specify, list the available upgrade packages and their paths.

Step 4   Copy the package from any device that has the package you need, by specifying the IP address and path you just discovered.

sync-from-peer *ip_address package_path*

After you confirm that you want to copy the package, the system displays a sync status UUID that you can use to monitor this transfer.

Step 5   Monitor transfer status from the CLI.

show p2p-sync-status: Shows the sync status for the last five transfers to this device, including completed and failed transfers.

show p2p-sync-status *sync_status_UUID*: Shows the sync status for a particular transfer to this device.

Upgrade Packages on Cisco.com

Manually download upgrade packages from Cisco when the system has no internet access, or when you cannot direct-download for another reason (hotfix, Beta release). You must also manually obtain upgrade packages if you plan to configure devices to get them from an internal server. And, you must manually obtain chassis upgrade packages for the Firepower 4100/9300.

Packages are available on the Cisco Support & Download site:

- Management Center: https://www.cisco.com/go/firepower-software

- Threat Defense: https://www.cisco.com/go/ftd-software

- ASA FirePOWER: https://www.cisco.com/go/asa-firepower-sw

- NGIPSv: https://www.cisco.com/go/ngipsv-software

Software Packages

You use the same upgrade package for all models in a family or series. To find the correct one, select or search for your model on the Cisco Support & Download site, then browse to the software download page for the appropriate version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), software version, and build. Upgrade packages are signed, and terminate in .sh.REL.tar. Do not untar or rename them.

Table 10: Management Center Packages

Platform	Package
Management Center	Cisco_Secure_FW_Mgmt_Center_Upgrade-*Version-build*.sh.REL.tar

Table 11: Threat Defense Packages

Platform	Package
Firepower 1000 series	Cisco_FTD_SSP-FP1K_Upgrade-*Version-build*.sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP-FP2K_Upgrade-*Version-build*.sh.REL.tar
Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-*Version-build*.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-*Version-build*.sh.REL.tar
ASA 5500-X series Last support: Version 7.0	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar
Threat Defense Virtual	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar
ISA 3000 with FTD	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar

Chassis Packages for the Firepower 4100/9300

To find the correct FXOS package, select or search for your device model and browse to the *Firepower Extensible Operating System* download page for your target FXOS version and build. The FXOS package is listed along with recovery and MIB packages.

Table 12: FXOS Packages

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

Upgrades to FXOS 2.14.1+ include firmware. If you are upgrading to an earlier version of FXOS, select or search for your device model and browse to the *Firepower Extensible Operating System* download page. Firmware packages are under *All Releases > Firmware*.

Table 13: Firmware Packages

Platform	Package
Firepower 4100	fxos-k9-fpr4k-firmware.*firmware_version*.SPA
Firepower 9300	fxos-k9-fpr9k-firmware.*firmware_version*.SPA

Upgrade Readiness

Network and Infrastructure Checks

Appliance Access

Devices can stop passing traffic during the upgrade or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. You should also able to access the management center's management interface without traversing the device.

Bandwidth

Make sure your management network has the bandwidth to perform large data transfers. Whenever possible, upload upgrade packages ahead of time. If you transfer an upgrade package to a device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. See Guidelines for Downloading Data from the Firepower Managemen t Center to Managed Devices (Troubleshooting TechNote).

Configuration and Deployment Checks

Configurations

Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes. Deploy configuration changes.

Note You will need to deploy again after upgrade. Deploying can affect traffic flow and inspection; see Traffic Flow and Inspection for Threat Defense Upgrades.

Deployment Health

Make sure your deployment is healthy and successfully communicating. If there are any issues reported by the health monitor, resolve them before continuing. You should especially make sure all appliances are synchronized with any NTP server you are using to serve time. Although the health monitor alerts if clocks are out of sync by more than 10 seconds, you should still check manually. Being out of sync can cause upgrade failure.

To check time:

- Management Center: Choose **System** (⚙) > **Configuration** > **Time**.

- Threat Defense: Use the **show time** CLI command.

Running and Scheduled Tasks

Make sure essential tasks are complete, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed.

Upgrades from Version 6.6.3+ automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. If you do not want this to happen (or if you are upgrading from an earlier version), check for tasks that are scheduled to run during the upgrade and cancel or postpone them.

Backups

With the exception of hotfixes, upgrade deletes all backups stored on the system. We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after any upgrade:

- Before upgrade: If an upgrade fails catastrophically, you may have to reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly.

- After upgrade: This creates a snapshot of your freshly upgraded deployment. Back up the management center after you upgrade its managed devices, so your new management center backup file 'knows' that its devices have been upgraded.

Table 14: Backups

Backup	Guide
Management center	Cisco Secure Firewall Management Center Administration Guide: *Backup/Restore*
	We recommend you back up configurations and events.

Backup	Guide
Threat defense	Cisco Secure Firewall Management Center Administration Guide: *Backup/Restore* Backup is not supported for clustered threat defense devices or threat defense virtual in the public cloud.
Firepower 4100/9300 chassis	Cisco Firepower 4100/9300 FXOS Configuration Guide: *Configuration Import/Export*
ASA on a Firepower 9300 chassis	Cisco ASA Series General Operations Configuration Guide: *Software and Configurations* For a Firepower 9300 chassis with threat defense and ASA logical devices, use ASDM or the ASA CLI to back up ASA configurations and other critical files, especially if there is an ASA configuration migration.

Software Upgrade Readiness Checks

Besides the checks you perform yourself, the system can also check its own upgrade readiness. The threat defense and management center upgrade wizards prompt you to run the checks at the appropriate time. For the management center, passing readiness checks is not optional. If you fail readiness checks, you cannot upgrade. For threat defense, you can disable this requirement although we recommend against it. Passing all checks greatly reduces the chance of upgrade failure. If the checks expose issues that you cannot resolve, do not begin the upgrade.

You can run readiness checks outside a maintenance window. The time required to run a readiness check varies depending on model and database size. Do not manually reboot or shut down during readiness checks.

Upgrade Management Center

Upgrade the Management Center: Standalone

Use this procedure to upgrade a standalone management center.

As you proceed, the management center upgrade wizard displays basic information about the upgrade, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If you navigate away from the wizard, your progress is preserved and other users cannot start a new upgrade workflow. (Exception: if you are logged in with a CAC, your progress is cleared 24 hours after you log out.) To return to your workflow, choose **System** (⚙) > **Product Upgrades** and click **Resume** in the system overview for the management center.

Management center upgrade does not start until you complete the wizard and click **Upgrade**. All steps up to that point can be performed outside of a maintenance window, including downloading upgrade packages and running readiness checks. For information on traffic handling during the first post-upgrade deploy, see Traffic Flow and Inspection when Deploying Configurations, on page 59. If you are managing any older ASA FirePOWER or NGIPSv devices, see the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 for traffic handling information.

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

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility, on page 1

- Plan the upgrade path: Upgrade Path, on page 3

- Review upgrade guidelines: Upgrade Guidelines, on page 2

- Check infrastructure and network: Network and Infrastructure Checks, on page 10

- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks, on page 10

- Perform backups: Backups, on page 11

Step 1 On the management center, choose **System (⚙)** > **Product Upgrades**.

Step 2 Get the upgrade package.

The Product Upgrades page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. In most cases, you can just click **Download** next to the upgrade package or version you want.

For more information, see Uploading and Downloading Upgrade Packages to the Management Center, on page 5 and Troubleshooting Upgrade Packages, on page 53.

Step 3 Launch the upgrade wizard.

Click **Upgrade** next to the target version. If you are given a drop-down menu, select **Management Center**.

The management center upgrade wizard appears. Compatibility and other quick prechecks are automatic. For example, the system alerts you immediately if you need to deploy configurations.

Step 4 Click **Next** to run readiness checks.

Click **Run Readiness Checks**. Do not manually reboot or shut down during readiness checks. For the management center, passing readiness checks is not optional. If you fail readiness checks, you cannot upgrade.

Step 5 Click **Next** and reconfirm you are ready to upgrade.

We recommend revisiting the configuration and deployment health checks you performed earlier: Configuration and Deployment Checks, on page 10.

Step 6 Click **Upgrade**, then confirm that you want to upgrade and reboot.

You can monitor precheck progress in the Message Center until you are logged out.

Step 7 Log back in when you can.

- Major and maintenance upgrades: You can log in before the upgrade is completed. The system displays a page you can use to monitor the upgrade's progress and view the upgrade log and any error messages. You are logged out again when the upgrade is completed and the system reboots. After the reboot, log back in again.

- Patches and hotfixes: You can log in after the upgrade and reboot are completed.

Step 8 Verify upgrade success.

If the system does not notify you of the upgrade's success when you log in, choose **Help** (❓) > **About** to display current software version information.

Step 9 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 10 Complete any required post-upgrade configuration changes.

Step 11 Redeploy configurations to all managed devices.

Upgrade the Management Center: High Availability

Use this procedure to upgrade high availability management centers one at a time. Neither your workflow nor upgrade packages are synchronized between high availability management centers.

With synchronization paused, upgrade the standby. When that upgrade completes, the management center comes back up as active, which allows you to upgrade the other management center. This temporary active-active state is called *split-brain* and is not supported except during upgrade (and patch uninstall). Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization.

As you proceed, the management center upgrade wizard displays basic information about the upgrade, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If you navigate away from the wizard, your progress is preserved and other users cannot start a new upgrade workflow. (Exception: if you are logged in with a CAC, your progress is cleared 24 hours after you log out.) To return to your workflow, choose **System** (⚙) > **Product Upgrades** and click **Resume** in the system overview for the management center.

Management center upgrade does not start until you complete the wizard, pause synchronization, and click **Upgrade**. All steps up to that point can be performed outside of a maintenance window, including downloading upgrade packages and running readiness checks. For information on traffic handling during the first post-upgrade deploy, see Traffic Flow and Inspection when Deploying Configurations, on page 59. If you are managing any older ASA FirePOWER or NGIPSv devices, see the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0 for traffic handling information.

Note 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.

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

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility, on page 1

- Plan the upgrade path: Upgrade Path, on page 3

- Review upgrade guidelines: Upgrade Guidelines, on page 2

- Check infrastructure and network: Network and Infrastructure Checks, on page 10

- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks, on page 10

- Perform backups: Backups, on page 11

Prepare to upgrade both management centers.

Step 1   On either management center, choose **System** (⚙) > **Product Upgrades**.

Step 2   Get the upgrade package.

The Product Upgrades page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. In most cases, you can just click **Download** next to the upgrade package or version you want. For more information, see Uploading and Downloading Upgrade Packages to the Management Center, on page 5 and Troubleshooting Upgrade Packages, on page 53.

You *must* do this on both management centers. Upgrade packages are not synchronized.

Step 3   Launch the upgrade wizard.

Click **Upgrade** next to the target version. If you are given a drop-down menu, select **Management Center**.

The management center upgrade wizard appears. Compatibility and other quick prechecks are automatic. For example, the system alerts you immediately if you need to deploy configurations.

Step 4   Click **Next** to run readiness checks.

Click **Run Readiness Checks**. Do not manually reboot or shut down during readiness checks. For the management center, passing readiness checks is not optional. If you fail readiness checks, you cannot upgrade.

Step 5   Click **Next** and reconfirm you are ready to upgrade.

We recommend revisiting the configuration and deployment health checks you performed earlier: Configuration and Deployment Checks, on page 10.

Step 6   Repeat Steps 1–5 for the other management center.

Pause synchronization.

Step 7   On the active management center, pause synchronization.

If you pause from the active, you can resume from either. If you pause from the standby, you must resume from the standby.

a) Choose **Integration** > **Other Integrations**.
b) On the **High Availability** tab, click **Pause Synchronization**.

Upgrade the standby, then the active.

Step 8   On the standby management center, click **Upgrade**, then confirm that you want to upgrade and reboot.

You can monitor precheck progress in the Message Center until you are logged out.

Step 9   Log back in when you can.

- Major and maintenance upgrades: You can log in before the upgrade is completed. The system displays a page you can use to monitor the upgrade's progress and view the upgrade log and any error messages. You are logged out again when the upgrade is completed and the system reboots. After the reboot, log back in again.

- Patches and hotfixes: You can log in after the upgrade and reboot are completed.

Step 10   Verify upgrade success.

If the system does not notify you of the upgrade's success when you log in, choose **Help** (❓) > **About** to display current software version information.

Step 11   Repeat Steps 8-10 on the other management center.

Resume synchronization and complete post-upgrade tasks.

Step 12   Still on the on the old active management center (the one you just upgraded), resume synchronization.

a) Choose **Integration** > **Other Integrations**.
b) On the **High Availability** tab, click **Resume Synchronization**.

Step 13   Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 14   Complete any required post-upgrade configuration changes.

Step 15   Redeploy configurations to all managed devices.

CHAPTER 3

Upgrade Threat Defense

Upgrade Threat Defense

Use this procedure to upgrade threat defense. As you proceed, the threat defense wizard 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 the wizard, your progress is preserved and other users cannot start a new upgrade workflow for any devices you have already selected. (Exception: if you are logged in with a CAC, your progress is cleared 24 hours after you log out.) To return to your workflow, choose **Devices** > **Device Upgrade**.

Device upgrade does not start until you complete the wizard and click **Start Upgrade**. All steps up to that point can be performed outside of a maintenance window, including downloading upgrade packages, copying them to devices, running readiness checks, and choosing upgrade options. For information on traffic handling during the upgrade and the first post-upgrade deploy, see Traffic Flow and Inspection, on page 57.

> ⚠️
>
> **Caution** Do not 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. Devices may reboot multiple times during the upgrade. This is expected behavior. If you encounter issues with the upgrade, including a failed upgrade or unresponsive device, see Unresponsive and Failed Threat Defense Upgrades, on page 55.

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility, on page 1

- Plan the upgrade path: Upgrade Path, on page 3

- Review upgrade guidelines: Upgrade Guidelines, on page 2

- Check infrastructure and network: Network and Infrastructure Checks, on page 10

- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks, on page 10

- Perform backups: Backups, on page 11

- Upgrade chassis, if required: Upgrade the Firepower 4100/9300 Chassis, on page 25

Step 1   On the management center, choose **System** (⚙) > **Product Upgrades**.

The Product Upgrades page provides an upgrade-centered overview of your deployment—how many devices you have, when they were last upgraded, whether there is an upgrade in progress, and so on.

Step 2   Get the device upgrade packages onto the management center.

Before you copy upgrade packages to managed devices, you must upload the packages to the management center (or to an internal server that the devices can access). The Product Upgrades page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. In most cases, you can just click **Download** next to the upgrade package or version you want. For more information, see Uploading and Downloading Upgrade Packages to the Management Center, on page 5 and Troubleshooting Upgrade Packages, on page 53.

Step 3   Launch the upgrade wizard.

Click **Upgrade** next to the target version. If you are given a drop-down menu, select **Threat Defense**.

The threat defense upgrade wizard appears. It has two panes: Device Selection on the left, and Device Details on the right. Click a device link in the Device Selection pane (such as '4 devices') to show the Device Details for those devices. Your target version is pre-selected in the **Upgrade to** menu. The system determines which devices can be upgraded to that version and displays them in the Device Details pane.

Step 4   Select devices to upgrade.

In the Device Details pane, select the devices you want to upgrade and click **Add to Selection**.

You can use the device links on the Device Selection pane to toggle the Device Details pane between selected devices, remaining upgrade candidates, ineligible devices (with reasons why), devices that need the upgrade package, and so on. You can add and remove devices from your selection, or click **Reset** to clear your device selection and start over. Note that you do not have to remove ineligible devices; they are automatically excluded from upgrade. You must upgrade the members of device clusters and high availability pairs together.

Tip   After you select devices to upgrade, you can begin upgrade in unattended mode (**Unattended Mode** > **Start**). After you specify a few options, the system automatically copies needed upgrade packages to devices, performs compatibility and readiness checks, and begins the upgrade. After the upgrade completes, pick up with the verification and post-upgrade tasks. For more information, see Upgrade Threat Defense in Unattended Mode, on page 22.

Step 5   Copy upgrade packages to devices.

Click **Copy Upgrade Package** and wait for the transfer to complete.

Step 6   Click **Next** to run compatibility and readiness checks.

Compatibility and other quick prechecks are automatic. For example, the system alerts you immediately if you need to deploy configurations. Other checks take more time. To begin these, click **Run Readiness Check**.

Do not deploy changes to, manually reboot, or shut down a device while running readiness checks. Although you can skip checks by disabling the **Require passing compatibility and readiness checks** option, we recommend against it.

Passing all checks greatly reduces the chance of upgrade failure. If the checks expose issues that you cannot resolve, do not begin the upgrade.

Step 7 Click **Next** to choose upgrade options.

These options allow you to revert from both successful and unsuccessful upgrades, to generate troubleshooting files, and to upgrade Snort. For information on why you might disable these options, see Threat Defense Upgrade Options, on page 22.

Step 8 Reconfirm you are ready to upgrade.

We recommend revisiting the configuration and deployment health checks you performed earlier: Configuration and Deployment Checks, on page 10.

Step 9 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

The wizard shows your overall upgrade progress, which you can also monitor in the Message Center. For detailed status, click **View Details** next to the device you want to see. This detailed status is also available from the Upgrade tab on the Device Management page.

> **Tip** If you need to cancel a failed or in-progress upgrade, or retry a failed upgrade, do it from the detailed status pop-up. If you have not cleared your workflow, you can view the detailed status by returning to the wizard. If you have, use the Upgrade tab on the Device Management page. You can also use the threat defense CLI.

Step 10 Verify success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 11 (Optional) In high availability/scalability deployments, examine device roles.

The upgrade process switches device roles so that it is always upgrading a standby unit or data node. It does not return devices to the roles they had before upgrade. If you have preferred roles for specific devices, make those changes now.

Step 12 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 13 Complete any required post-upgrade configuration changes.

Step 14 Redeploy configurations to the devices you just upgraded.

Before you deploy, you may want to review the changes made by the upgrade (as well as any changes you have made since upgrade). Choose **Deploy** > **Advanced Deploy**, select the devices you just upgraded, and click **Pending Changes Reports**. After they finish generating, you can download change reports from the Tasks tab on the Message Center.

What to do next

- (Optional) Clear the wizard by clicking **Clear Upgrade Information**. Until you do this, it continues to display details about the upgrade you just performed. After you clear the wizard, use the Upgrade tab on the Device Management page to see last-upgrade information for managed devices.

- Back up again: Backups, on page 11

Threat Defense Upgrade Options

Table 15: Threat Defense Upgrade Options

Option	When to Disable	Details
Require passing compatibility and readiness checks.	At the direction of Cisco TAC.	If you disable this option, you can begin the upgrade without passing compatibility and readiness checks. However, we recommend against it. Passing all checks greatly reduces the chance of upgrade failure. If the checks expose issues that you cannot resolve, do not begin the upgrade.
Automatically cancel on upgrade failure and roll back to the previous version.	To force manual (instead of automatic) cancel and retry of failed upgrades.	With this option enabled, the device automatically returns to its pre-upgrade state upon upgrade failure. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.
Generate troubleshooting files before upgrade begins.	To save time and disk space.	With upgrades to Version 7.3+, you can skip the automatic pre-upgrade generating of troubleshooting files. 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**.
Upgrade Snort 2 to Snort 3.	To prevent Snort 3 upgrades.	With upgrades to Version 7.2+, 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 migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.
Enable revert after successful upgrade.	To save time and disk space.	With upgrades to 7.1+, you have 30 days to revert threat defense upgrades. 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 upgrade. Not supported for container instances, patches, or hotfixes.

Upgrade Threat Defense in Unattended Mode

The threat defense upgrade wizard has an optional *unattended mode*. 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, pick up with the verification and post-upgrade tasks.

Table 16:

To...	Do This
Start an unattended upgrade.	In the threat defense upgrade wizard, select the target version and the devices you want to upgrade. Choose **Unattended Mode** > **Start**, choose upgrade options, and click **Start** again.
Pause an unattended upgrade during copy and checks phases.	In the threat defense upgrade wizard, choose **Unattended Mode** > **Stop**. 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. Note that you must pause unattended mode to perform any manual upgrade actions. Once the actual device upgrade begins, you cannot cancel it by stopping unattended mode. Instead, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page.
Monitor an unattended upgrade.	To monitor an unattended upgrade: • Copy and check status: **Unattended Mode** > **View Status** • Overall upgrade status: Message Center • Detailed upgrade status: Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page

Upgrade Older ASA FirePOWER and NGIPSv Devices

Use this procedure to upgrade older ASA FirePOWER or NGIPSv devices, last supported in Version 7.0.

Note Device upgrade does not start until you click **Install**. All steps up to that point can be performed outside of a maintenance window, including downloading upgrade packages, copying them to devices, and running readiness checks. For information on traffic handling during the upgrade and the first post-upgrade deploy, see the release notes for your target version: Cisco Secure Firewall Threat Defense Release Notes.

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

Before you begin

Make sure you are ready to upgrade. Note that this guide does not contain detailed checklists, planning information, or ASA upgrade instructions for these devices. For those, see the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Step 1   On the management center, choose **System** (⚙) > **Product Upgrades**.

Step 2   Get the device upgrade packages onto the management center.

Before you copy upgrade packages to managed devices, you must upload the packages to the management center. The Product Upgrades page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. In most cases, you can just click **Download** next to the upgrade package or version you want.

For more information, see Uploading and Downloading Upgrade Packages to the Management Center, on page 5 and Troubleshooting Upgrade Packages, on page 53.

Step 3   Click **Upgrade** next to the target version and select the type of device you want to upgrade: **ASA FirePOWER** or **NGIPSv**.

The Classic device upgrade page appears.

Step 4   Select the devices you want to upgrade.

We recommended upgrading no more than five devices at a time. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 5   Click **Install**, then confirm that you want to upgrade and reboot the devices.

You can monitor upgrade progress in the Message Center.

Step 6   Verify success.

After the upgrade completes, choose **Devices** > **Device Management** and confirm that the devices you upgraded have the correct software version.

Step 7   Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 8   Complete any required post-upgrade configuration changes.

Step 9   Redeploy configurations to the devices you just upgraded.

Upgrade the Firepower 4100/9300 Chassis

For the Firepower 4100/9300, major threat defense upgrades require chassis (FXOS and firmware) upgrades. Maintenance releases and patches rarely do. Chassis upgrades to FXOS 2.14.1+ include firmware, otherwise, see the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

Upgrade FXOS with Chassis Manager

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using Firepower Chassis Manager

This section describes how to upgrade the FXOS platform bundle for a standalone Firepower 4100/9300 chassis.

The section describes the upgrade process for the following types of devices:

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair or inter-chassis cluster.

- A Firepower 9300 chassis that is configured with one or more standalone FTD logical devices that are not part of a failover pair or inter-chassis cluster.

- A Firepower 9300 chassis that is configured with FTD logical devices in an intra-chassis cluster.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.

- Back up your FXOS and FTD configurations.

Step 1 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 2 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.

b) Click **Choose File** to navigate to and select the image that you want to upload.

c) Click **Upload**.

The selected image is uploaded to the Firepower 4100/9300 chassis.

d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 3 After the new platform bundle image has been successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 4 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 5 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.

b) Enter **show firmware monitor**.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Step 6 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.

b) Enter **scope ssa**.

c) Enter **show slot**.

d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

   e) Enter **show app-instance**.

   f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Upgrade FXOS on an FTD Inter-chassis Cluster Using Firepower Chassis Manager

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as an inter-chassis cluster, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.

- Back up your FXOS and FTD configurations.

Step 1   Enter the following commands to verify the status of the security modules/security engine and any installed applications:

   a) Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the control unit).

   b) Enter **top**.

   c) Enter **scope ssa**.

   d) Enter **show slot**.

   e) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

   f) Enter **show app-instance**.

   g) Verify that the Oper State is `Online` and that the Cluster State is `In Cluster` for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

       Important   Verify that the control unit is not on this chassis. There should not be any Firepower Threat Defense instance with Cluster Role set to `Master`.

   h) For any security modules installed on a Firepower 9300 appliance or for the security engine on a Firepower 4100 series appliance, verify that the FXOS version is correct:

       scope server 1/*slot_id*, where *slot_id* is 1 for a Firepower 4100 series security engine.

       show version.

Step 2   Connect to Firepower Chassis Manager on Chassis #2 (this should be a chassis that does not have the control unit).

Step 3   In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 4   Upload the new platform bundle image:

   a) Click **Upload Image** to open the Upload Image dialog box.

   b) Click **Choose File** to navigate to and select the image that you want to upload.

   c) Click **Upload**.

The selected image is uploaded to the Firepower 4100/9300 chassis.

d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 5 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 6 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 7 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

> **Note**   After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

d) Enter **top**.
e) Enter **scope ssa**.
f) Enter **show slot**.
g) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
h) Enter **show app-instance**.
i) Verify that the Oper State is `Online`, that the Cluster State is `In Cluster` and that the Cluster Role is `Slave` for any logical devices installed on the chassis.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot
```

```
Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name    Slot ID    Admin State Oper State      Running Version Startup Version Profile Name
Cluster State    Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                     In
 Cluster    Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                     In
 Cluster    Slave
ftd        3          Disabled    Not Available                    6.2.2.81                     Not
 Applicable  None
FP9300-A /ssa #
```

Step 8   Set one of the security modules on Chassis #2 as control.

After setting one of the security modules on Chassis #2 to control, Chassis #1 no longer contains the control unit and can now be upgraded.

Step 9   Repeat Steps 1-7 for all other Chassis in the cluster.

Step 10   To return the control role to Chassis #1, set one of the security modules on Chassis #1 as control.

Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as a high availability pair, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.

- Back up your FXOS and FTD configurations.

Step 1   Connect to Firepower Chassis Manager on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:

Step 2   In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 3   Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.

b) Click **Choose File** to navigate to and select the image that you want to upload.

c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.

d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 4 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 5 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 6 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.

b) Enter **show firmware monitor**.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show Upgrade-Status: Ready.

> **Note** After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Step 7 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.

b) Enter **scope ssa**.

c) Enter **show slot**.

d) Verify that the Admin State is Ok and the Oper State is Online for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

e) Enter **show app-instance**.

f) Verify that the Oper State is Online for any logical devices installed on the chassis.

Step 8 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

    a) Connect to Firepower Management Center.

    b) Choose **Devices** > **Device Management**.

    c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon (⟳).

    d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Step 9 Connect to Firepower Chassis Manager on the Firepower security appliance that contains the *new standby* Firepower Threat Defense logical device:

Step 10 In Firepower Chassis Manager, choose **System** > **Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.

Step 11 Upload the new platform bundle image:

    a) Click **Upload Image** to open the Upload Image dialog box.

    b) Click **Choose File** to navigate to and select the image that you want to upload.

    c) Click **Upload**.
       The selected image is uploaded to the Firepower 4100/9300 chassis.

    d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 12 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 13 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

Step 14 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

    a) Enter **scope system**.

    b) Enter **show firmware monitor**.

    c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

       Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
```

```
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
```

Step 15 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.

b) Enter **scope ssa**.

c) Enter **show slot**.

d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

e) Enter **show app-instance**.

f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 16 Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) Connect to Firepower Management Center.

b) Choose **Devices** > **Device Management**.

c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).

d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Upgrade FXOS with the CLI

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using the FXOS CLI

This section describes how to upgrade the FXOS platform bundle for a standalone Firepower 4100/9300 chassis.

The section describes the FXOS upgrade process for the following types of devices:

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair or inter-chassis cluster.

- A Firepower 9300 chassis that is configured with one or more standalone FTD devices that are not part of a failover pair or inter-chassis cluster.

- A Firepower 9300 chassis that is configured with FTD logical devices in an intra-chassis cluster.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.

- Back up your FXOS and FTD configurations.

- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:

  - IP address and authentication credentials for the server from which you are copying the image.

  - Fully qualified name of the image file.

Step 1 Connect to the FXOS CLI.

Step 2 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

Firepower-chassis-a # **scope firmware**

b) Download the FXOS platform bundle software image:

Firepower-chassis-a /firmware # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

- **ftp**://*username@hostname/path/image_name*

- **scp**://*username@hostname/path/image_name*

- **sftp**://*username@hostname/path/image_name*

- **tftp**://*hostname*:*port-num/path/image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 3 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 4 Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 5 Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

Step 6 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 7 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 8 To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show Upgrade-Status: Ready.

> **Note** After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 9 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is Ok and the Oper State is Online for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.

f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Upgrade FXOS on an FTD Inter-chassis Cluster Using the FXOS CLI

If you have Firepower 9300 or Firepower 4100 series security appliances with FTD logical devices configured as an inter-chassis cluster, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.

- Back up your FXOS and FTD configurations.

- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:

    - IP address and authentication credentials for the server from which you are copying the image.

    - Fully qualified name of the image file.

Step 1 Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the control unit).

Step 2 Enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.

b) Enter **scope ssa**.

c) Enter **show slot**.

d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

e) Enter **show app-instance**.

f) Verify that the Oper State is `Online` and that the Cluster State is `In Cluster` for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

> **Important** Verify that the control unit is not on this chassis. There should not be any Firepower Threat Defense instance with Cluster Role set to `Master`.

g) For any security modules installed on a Firepower 9300 appliance or for the security engine on a Firepower 4100 series appliance, verify that the FXOS version is correct:

scope server 1/*slot_id*, where *slot_id* is 1 for a Firepower 4100 series security engine.

show version.

Step 3 Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter **top**.

b) Enter firmware mode:

Firepower-chassis-a # **scope firmware**

c) Download the FXOS platform bundle software image:

Firepower-chassis-a /firmware # **download image** *URL*

Specify the URL for the file being imported using one of the following syntax:

• **ftp**://*username@hostname*/*path*/*image_name*

• **scp**://*username@hostname*/*path*/*image_name*

• **sftp**://*username@hostname*/*path*/*image_name*

• **tftp**://*hostname***:***port-num*/*path*/*image_name*

d) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 4 If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 5 Enter auto-install mode:

Firepower-chassis /firmware # **scope auto-install**

Step 6 Install the FXOS platform bundle:

Firepower-chassis /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing—for example, 2.3(1.58).

Step 7 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 8 Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 9 To monitor the upgrade process:

a) Enter **scope system**.

b) Enter **show firmware monitor**.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

> **Note**   After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

d) Enter **top**.

e) Enter **scope ssa**.

f) Enter **show slot**.

g) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

h) Enter **show app-instance**.

i) Verify that the Oper State is `Online`, that the Cluster State is `In Cluster` and that the Cluster Role is `Slave` for any logical devices installed on the chassis.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
    Slot ID    Log Level Admin State  Oper State
    ---------- --------- ------------ ----------
    1          Info      Ok           Online
    2          Info      Ok           Online
    3          Info      Ok           Not Available
FP9300-A /ssa #

FP9300-A /ssa # show app-instance
App Name    Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State    Cluster Role
---------- ---------- ---------- ---------------- --------------- --------------- ------------
--------------- ------------
ftd         1          Enabled    Online           6.2.2.81        6.2.2.81                     In
 Cluster     Slave
ftd         2          Enabled    Online           6.2.2.81        6.2.2.81                     In
 Cluster     Slave
ftd         3          Disabled   Not Available                    6.2.2.81                     Not
```

```
 Applicable  None
FP9300-A /ssa #
```

Step 10   Set one of the security modules on Chassis #2 as control.

After setting one of the security modules on Chassis #2 to control, Chassis #1 no longer contains the control unit and can now be upgraded.

Step 11   Repeat Steps 1-9 for all other Chassis in the cluster.

Step 12   To return the control role to Chassis #1, set one of the security modules on Chassis #1 as control.

Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as a high availability pair, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading.

- Back up your FXOS and FTD configurations.

- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:

    - IP address and authentication credentials for the server from which you are copying the image.

    - Fully qualified name of the image file.

Step 1   Connect to FXOS CLI on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:

Step 2   Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

   Firepower-chassis-a # **scope firmware**

b) Download the FXOS platform bundle software image:

   Firepower-chassis-a /firmware # **download image** *URL*

   Specify the URL for the file being imported using one of the following syntax:

   - **ftp**://*username@hostname*/*path*/*image_name*

   - **scp**://*username@hostname*/*path*/*image_name*

   - **sftp**://*username@hostname*/*path*/*image_name*

   - **tftp**://*hostname*:*port-num*/*path*/*image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 3   If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 4   Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 5   Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing; for example, 2.3(1.58).

Step 6   The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 7   Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 8   To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show Upgrade-Status: Ready.

> **Note**   After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 9   After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

    a) Enter **top**.

    b) Enter **scope ssa**.

    c) Enter **show slot**.

    d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

    e) Enter **show app-instance**.

    f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 10   Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

    a) Connect to Firepower Management Center.

    b) Choose **Devices** > **Device Management**.

    c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).

    d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Step 11   Connect to FXOS CLI on the Firepower security appliance that contains the *new standby* Firepower Threat Defense logical device:

Step 12   Download the new platform bundle image to the Firepower 4100/9300 chassis:

    a) Enter firmware mode:

        Firepower-chassis-a # **scope firmware**

    b) Download the FXOS platform bundle software image:

        Firepower-chassis-a /firmware # **download image** *URL*

        Specify the URL for the file being imported using one of the following syntax:

            • **ftp**://*username@hostname*/*path*/*image_name*

            • **scp**://*username@hostname*/*path*/*image_name*

            • **sftp**://*username@hostname*/*path*/*image_name*

            • **tftp**://*hostname*:*port-num*/*path*/*image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** *image_name*

Firepower-chassis-a /firmware/download-task # **show detail**

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
Download task:
    File Name: fxos-k9.2.3.1.58.SPA
    Protocol: scp
    Server: 192.168.1.1
    Userid:
    Path:
    Downloaded Image Size (KB): 853688
    State: Downloading
    Current Task: downloading image fxos-k9.2.3.1.58.SPA from
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 13   If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

Step 14   Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

Step 15   Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** *version_number*

version_number is the version number of the FXOS platform bundle you are installing; for example, 2.3(1.58).

Step 16   The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter **yes** to confirm that you want to proceed with verification.

Step 17   Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.

Step 18   To monitor the upgrade process:

a) Enter **scope system**.
b) Enter **show firmware monitor**.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show Upgrade-Status: Ready.

> **Note**   After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready
    Server 2:
        Package-Vers: 2.3(1.58)
        Upgrade-Status: Ready

FP9300-A /system #
```

Step 19   After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter **top**.

b) Enter **scope ssa**.

c) Enter **show slot**.

d) Verify that the Admin State is Ok and the Oper State is Online for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

e) Enter **show app-instance**.

f) Verify that the Oper State is Online for any logical devices installed on the chassis.

Step 20   Make the unit that you just upgraded the *active* unit as it was before the upgrade:

a) Connect to Firepower Management Center.

b) Choose **Devices** > **Device Management**.

c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).

d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Revert or Uninstall the Upgrade

If an upgrade succeeds but the system does not function to your expectations, you may be able to revert or uninstall:

- Revert is supported for major and maintenance upgrades to threat defense Version 7.1+.
- Uninstall is supported for patches to threat defense and to the management center.

If this will not work for you and you still need to return to an earlier version, you must reimage.

Revert Threat Defense

About Reverting Threat Defense

Reverting threat defense returns the software to its state just before the last major or maintenance upgrade. Reverting after patching necessarily removes patches as well. You must enable revert when you upgrade the device, so the system can save a revert snapshot.

Reverted Configurations

Configurations that are reverted include:

- Snort version.
- Device-specific configurations.

  General device settings, routing, interfaces, inline sets, DHCP, SNMP — anything you configure on the **Devices** > **Device Management** page.

- Objects used by your device-specific configurations.

  These include access list, AS path, key chain, interface, network, port, route map, and SLA monitor objects. If you edited these objects after you upgraded the device, the system creates new objects or configure object overrides for the reverted device to use. This allows your other devices to continue handling traffic according to their current configuration.

After a successful revert, we recommend you examine the objects used by the reverted device and make any necessary adjustments.

Configurations Not Reverted

Configurations that are not reverted include:

- Shared policies that can be used by multiple devices; for example, platform settings or access control policies.

  A successfully reverted device is marked out-of-date and you should redeploy configurations.

- For the Firepower 4100/9300, interface changes made using the Secure Firewall chassis manager or the FXOS CLI.

  Sync interface changes after a successful revert.

- For the Firepower 4100/9300, FXOS and firmware.

  If you are required to run the recommended combination of FXOS and threat defense, you may need a full reimage; see .

Guidelines for Reverting Threat Defense

System Requirements

Revert is supported for major and maintenance upgrades to threat defense Version 7.1+.

Revert is not supported for:

- Upgrades to earlier versions.

- Patches and hotfixes.

- Container instances.

- Management center upgrades.

Reverting High Availability or Clustered Devices

When you use the management center web interface to revert threat defense, you cannot select individual high availability units or clustered nodes.

Revert is more successful when all units/nodes are reverted simultaneously. When you initiate revert from the management center, the system automatically does this. If you need to use the device CLI, do this manually—open sessions with all units/nodes, verify that revert is possible on each, then start the processes at the same time. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

Note that revert is supported for fully and partially upgraded groups. In the case of a partially upgraded group, the system removes the upgrade from the upgraded units/nodes only. Revert will not break high availability or clusters, but you can break a group and revert its newly standalone devices.

Revert Does Not Downgrade FXOS

For the Firepower 4100/9300, major threat defense versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of threat defense, you may be running a non-recommended version of FXOS (too new).

Although newer versions of FXOS are backwards compatible with older threat defense versions, we do perform enhanced testing for the recommended combinations. You cannot manually downgrade FXOS, so if you find yourself in this situation and you want to run a recommended combination, you will need a full reimage.

Scenarios Preventing Revert

If you attempt to revert in any of these situations, the system displays an error.

Table 17: Scenarios Preventing Revert

Scenario	Solution
Revert snapshot is not available because: • You did not enable revert when you upgraded the device. • You deleted the snapshot from either the management center or the device, or it expired. • You upgraded the device with a different management center.	None. The revert snapshot is saved on the management center *and* the device for thirty days, after which it is automatically deleted and you can no longer revert. You can manually delete the snapshot from either appliance to save disk space, but this removes your ability to revert.
Last upgrade failed.	Return the device to its pre-upgrade state by canceling the upgrade. Or, fix the issues and try again. Revert is for situations where the upgrade succeeds, but the upgraded system does not function to your expectations. Reverting is not the same as canceling a failed or in-progress upgrade. If you cannot revert or cancel, you will have to reimage.
Management access interface changed since the upgrade.	Switch it back and try again.
Clusters where the units were upgraded from different versions.	Remove units until all match, reconcile cluster members, then revert the smaller cluster. You may also be able to revert the newly standalone units.
Clusters where one or more units were added to the cluster after upgrade.	Remove the new units, reconcile cluster members, then revert the smaller cluster. You may also be able to revert the newly standalone units.
Clusters where the management center and FXOS identify a different number of cluster units.	Reconcile cluster members and try again, although you may not be able to revert all units.

Revert Threat Defense with Management Center

You must use the management center to revert the device, unless communications between the management center and device are disrupted. In those cases, you can use the **upgrade revert** CLI command on the device. To see what version the system will revert to, use **show upgrade revert-info**.

> ⚠️
>
> **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.

Threat Defense History:

- 7.1: Initial support.

Before you begin

- Make sure revert is supported. Read and understand the guidelines.

- Back up to a secure external location. A failed revert may require a reimage, which returns most settings to factory defaults.

Step 1 Choose **Devices** > **Device Management**.

Step 2 Next to the device you want to revert, click **More** (⁝) and select **Revert Upgrade**.

With the exception of high availability pairs and clusters, you cannot select multiple devices to revert.

Step 3 Confirm that you want to revert and reboot.

Interruptions to traffic flow and inspection during revert depend on interface configurations only, as if every device were standalone. This is because even in high availability/scalability deployments, the system reverts all units simultaneously.

Step 4 Monitor revert progress.

In high availability/scalability deployments, traffic flow and inspection resume when the first unit comes back online. If the system shows no progress for several minutes or indicates that the revert has failed, contact Cisco TAC.

Step 5 Verify revert success.

After the revert completes, choose **Devices** > **Device Management** and confirm that the devices you reverted have the correct software version.

Step 6 (Firepower 4100/9300) Sync any interface changes you made to threat defense logical devices using the chassis manager or the FXOS CLI.

On the management center, choose **Devices** > **Device Management**, edit the device, and click **Sync**.

Step 7 Complete any other necessary post-revert configuration changes.

For example, if you edited objects used by device-specific configurations after you upgraded the device, the system creates new objects or configures object overrides for the reverted device to use. We recommend you examine the objects used by the reverted device and make any necessary adjustments.

Step 8 Redeploy configurations to the devices you just reverted.

A successfully reverted device is marked out-of-date. Because the device will be running an older version, newer configurations may not be supported even after a successful deploy.

Uninstall a Patch

Uninstalling a patch returns you to the version you upgraded from, and does not change configurations. Because the management center must run the same or newer version as its managed devices, uninstall patches from devices first. Uninstall is not supported for hotfixes.

Note   This guide describes how to uninstall management center and threat defense patches. To uninstall patches from older ASA FirePOWER or NGIPSv devices, see the Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0.

Uninstall Order for High Availability/Scalability

In high availability/scalability deployments, minimize disruption by uninstalling from one appliance at a time. Unlike upgrade, the system does not do this for you. Wait until the patch has fully uninstalled from one unit before you move on to the next.

Table 18: Uninstall Order for Management Center High Availability

Configuration	Uninstall Order
Management Center high availability	With synchronization paused, which is a state called *split-brain*, uninstall from peers one at a time. Do not make or deploy configuration changes while the pair is split-brain. 1. Pause synchronization (enter split-brain). 2. Uninstall from the standby. 3. Uninstall from the active. 4. Restart synchronization (exit split-brain).

Table 19: Uninstall Order for Threat Defense High Availability and Clusters

Configuration	Uninstall Order
Threat Defense high availability	You cannot uninstall a patch from devices configured for high availability. You must break high availability first. 1. Break high availability. 2. Uninstall from the former standby. 3. Uninstall from the former active. 4. Reestablish high availability.
Threat Defense cluster	Uninstall from one unit at a time, leaving the control unit for last. Clustered units operate in maintenance mode while the patch uninstalls. 1. Uninstall from the data modules one at a time. 2. Make one of the data modules the new control module. 3. Uninstall from the former control.

Uninstall Threat Defense Patches

Use the Linux shell (*expert mode*) to uninstall patches. You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. You cannot use a management center user account. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

⚠️

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

Before you begin

- Break threat defense high availability pairs; see Uninstall Order for High Availability/Scalability, on page 47.

- Make sure your deployment is healthy and successfully communicating.

Step 1 If the device's configurations are out of date, deploy now from the management center.

Deploying before you uninstall reduces the chance of failure. Make sure the deployment and other essential tasks complete. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

Step 2 Access the threat defense CLI on the device. Log in as `admin` or another CLI user with configuration access.

You can either SSH to the device's management interface (hostname or IP address) or use the console. If you use the console, some devices default to the operating system CLI and require an extra step to access the threat defense CLI, as listed in the following table.

Firepower 1000 series	`connect ftd`
Firepower 2100 series	`connect ftd`
Secure Firewall 3100 series	`connect ftd`
Firepower 4100/9300	`connect module` *slot_number* `console`, then `connect ftd` (first login only)

Step 3 Use the `expert` command to access the Linux shell.

Step 4 Verify the uninstall package is in the upgrade directory.

`ls /var/sf/updates`

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch a device, the uninstaller for that patch is automatically created in the upgrade directory. If the uninstaller is not there, contact Cisco TAC.

Step 5 Run the uninstall command, entering your password when prompted.

`sudo install_update.pl --detach /var/sf/updates/`*uninstaller_name*

> **Caution** The system does *not* ask you to confirm. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready. Note that using the `--detach` option ensures the uninstall process is not killed if your SSH session times out, which can leave the device in an unstable state.

Step 6 Monitor the uninstall until you are logged out.

For a detached uninstall, use `tail` or `tailf` to display logs:

`tail /ngfw/var/log/sf/update.status`

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

After the uninstall completes, confirm that the devices have the correct software version. On the management center, choose **Devices** > **Device Management**.

Step 8 In high availability/scalability deployments, repeat steps 2 through 6 for each unit.

For clusters, never uninstall from the control unit. After you uninstall from all the data units, make one of them the new control, then uninstall from the former control.

Step 9 Redeploy configurations.

Exception: Do not deploy to mixed-version high availability pairs or device clusters. Deploy before you uninstall from the first device, but not again until you have uninstalled the patch from all group members.

What to do next

- For high availability, reestablish high availability.

• For clusters, if you have preferred roles for specific devices, make those changes now.

Uninstall Standalone Management Center Patches

We recommend you use the web interface to uninstall management center patches. If you cannot use the web interface, you can use the Linux shell as either the `admin` user for the shell, or as an external user with shell access. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

⚠️

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

Before you begin

• If uninstalling will put the management center at a lower patch level than its managed devices, uninstall patches from the devices first.

• Make sure your deployment is healthy and successfully communicating.

Step 1   Deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2   Under Available Updates, click the **Install** icon next to the uninstall package, then choose the management center.

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch the management center, the uninstaller for that patch is automatically created. If the uninstaller is not there, contact Cisco TAC.

Step 3   Click **Install**, then confirm that you want to uninstall and reboot.

You can monitor uninstall progress in the Message Center until you are logged out.

Step 4   Log back in when you can and verify uninstall success.

If the system does not notify you of the uninstall's success when you log in, choose **Help** > **About** to display current software version information.

Step 5   Redeploy configurations to all managed devices.

Uninstall High Availability Management Center Patches

We recommend you use the web interface to uninstall management center patches. If you cannot use the web interface, you can use the Linux shell as either the `admin` user for the shell, or as an external user with shell access. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

Uninstall from high availability peers one at a time. With synchronization paused, first uninstall from the standby, then the active. When the standby starts the uninstall, its status switches from standby to active, so

that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade and uninstall.

> ⚠️
>
> **Caution** Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization. Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

Before you begin

- If uninstalling will put the management centers at a lower patch level than their managed devices, uninstall patches from the devices first.

- Make sure your deployment is healthy and successfully communicating.

Step 1 On the active management center, deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2 On the active management center, pause synchronization.

a) Choose **Integration** > **Other Integrations**.
b) On the **High Availability** tab, click **Pause Synchronization**.

Step 3 Uninstall the patch from peers one at a time — first the standby, then the active.

Follow the instructions in , but omit the initial deploy, stopping after you verify uninstall success on each peer. In summary, for each peer:

a) On the **System** > **Updates** page, uninstall the patch.
b) Monitor progress until you are logged out, then log back in when you can.
c) Verify uninstall success.

Step 4 On the management center you want to make the active peer, restart synchronization.

a) Choose **Integration** > **Other Integrations**.
b) On the **High Availability** tab, click **Make-Me-Active**.
c) Wait until synchronization restarts and the other management center switches to standby mode.

Step 5 Redeploy configurations to all managed devices.

CHAPTER 6

Troubleshooting and Reference

- Troubleshooting Upgrade Packages, on page 53
- Troubleshooting Threat Defense Upgrade, on page 54
- Unresponsive and Failed Upgrades, on page 55
- Traffic Flow and Inspection, on page 57
- Time and Disk Space, on page 60
- Upgrade Feature History, on page 61

Troubleshooting Upgrade Packages

Table 20:

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 *and* you have no upgrade packages loaded/configured.
Suggested release is not marked.	The suggested release is listed only if you are eligible for it. It is not listed if you are already running the suggested release or higher, or if you cannot upgrade that far. Note that patches to suggested releases are not marked as suggested, although we do recommend you apply them.
I don't see the packages I want.	Only major, maintenance, and patch upgrades that apply to your deployment *right now* are listed and available for direct download. Unless you manually upload, the following are not listed: • Device upgrades (major and maintenance) to a particular version, unless the management center is running that version or higher, *and* you have a device that supports that version. • Device patches, unless you have at least one device at the appropriate maintenance release. This also applies to management center patches. • Hotfixes. You must manually upload these.

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

Troubleshooting Threat Defense Upgrade

Table 21:

Issue	Solution
Upgrade button missing for my target version.	Either of: • You still need the upgrade package. • You do not have anything that can be upgraded to that version right now.
Devices not listed in the upgrade wizard.	If you accessed the wizard directly from **Devices** > **Device Upgrade**, the workflow may be blank. To begin, choose a target version from the **Upgrade to** 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 **Upgrade to** menu correspond to the device upgrade packages on the management center. If your target version is not listed, click **Manage Upgrade Packages** to upload it; see Uploading and Downloading Upgrade Packages to the Management Center, on page 5. 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.
Devices locked to someone else's upgrade workflow.	If you need to reset someone else's workflow, you must have Administrator access. You can either: • Delete or deactivate the user. • Update the user's role so they no longer have permission to use **System** (⚙) > **Product Upgrades**.

Issue	Solution

Copying upgrade packages from the management center to managed devices times out.	This often happens when there is limited bandwidth between the management center and its devices.
	
	You can try one of:
	
	• Configure devices to get upgrade packages directly from an internal web server.
	
	  To do this, delete the upgrade package from the management center (optional but saves disk space), then re-add the upgrade package except this time specify a pointer (URL) to its location instead. See Copy Upgrade Packages from an Internal Server, on page 7.
	
	• Copy upgrade packages from another device.
	
	  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 Copy Threat Defense Upgrade Packages between Devices, on page 7.

High availability management center failed over while setting up upgrade.	Neither your workflow nor threat defense upgrade packages are synchronized between high availability management centers. In case of failover, you must recreate your workflow on the new active management center, which includes downloading upgrade packages and copying them to devices. (Upgrade packages already copied to devices are not removed, but the management center still must have the package or a pointer to its location.)

Unresponsive and Failed Upgrades

Unresponsive and Failed Management Center Upgrades

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

Unresponsive and Failed Threat Defense Upgrades

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

Table 22:

Issue	Solution
Cannot reach the device.	Devices can stop passing traffic during the upgrade or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. You should also able to access the management center's management interface without traversing the device.
Upgrade or patch appears hung/device appears inactive.	If device upgrade status has stopped updating on the management center but there is no report of upgrade failure, you can try canceling the upgrade; see below. If you cannot cancel or canceling does not work, contact Cisco TAC. **Tip:** You can monitor upgrade logs on the device itself using expert mode and tail or tailf: `tail /ngfw/var/log/sf/update.status`.
Upgrade failed.	If an upgrade fails and: • The device reverted to its pre-upgrade state (auto-cancel is enabled), correct any issues and try again from the beginning. • The device is still in maintenance mode, correct any issues and resume the upgrade. Or, cancel and try again later. If you continue to have issues, contact Cisco TAC.
Patch failed.	You cannot cancel in-progress or failed patches. However, if a patch fails early, for example, during validation stages, the device may remain up and running normally. Simply correct any issues and try again. If a patch fails after the device has entered maintenance mode, check for an uninstaller. If one exists, you can try running it to remove the failed patch; see Uninstall Threat Defense Patches, on page 48. After the uninstall finishes, you can correct any issues and try again. If there is no uninstaller, if the uninstall fails, or if you continue to have issues, contact Cisco TAC.
I want to cancel an upgrade.	Canceling reverts the device to its pre-upgrade state. You can cancel failed and in-progress upgrades on the upgrade status pop-up, accessible from the Upgrade tab on the Device Management page. You cannot cancel patches. If you cannot cancel or canceling does not work, contact Cisco TAC.
I want to retry (resume) a failed upgrade.	You can resume an upgrade on the upgrade status pop-up, accessible from the Upgrade tab on the Device Management page. If you continue to have issues, contact Cisco TAC.

Issue	Solution
I want to change what happens when upgrade fails.	Part of the upgrade process is choosing what happens if it fails. This is done with the **Automatically cancel on upgrade failure...** (auto-cancel) option: • Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. This returns you to normal operations as quickly as possible while you regroup and try again. • Auto-cancel disabled: If upgrade fails, the device remains as it is. This allows you to correct any issues and resume the upgrade. For high availability and clustered devices, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. Auto-cancel is not supported for upgrades from Version 6.6

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 23: 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.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force**	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby**	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled**	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability and Clustered Devices

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

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

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

Software Revert (Major/Maintenance Releases)

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

Software Uninstall (Patches)

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

Traffic Flow and Inspection for Chassis Upgrades

Upgrading FXOS reboots the chassis. For FXOS upgrades to Version 2.14.1+ that include firmware upgrades, the device reboots twice—once for FXOS and once for the firmware.

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 Upgrade Order for Threat Defense with Chassis Upgrade and High Availability/Clusters, on page 4.

Table 24: Traffic Flow and Inspection: FXOS Upgrades

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

Traffic Flow and Inspection when Deploying Configurations

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

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

Table 25: Traffic Flow and Inspection: Deploying Configuration Changes

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

Time and Disk Space

Time to Upgrade

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

⚠️ **Caution**
Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive and Failed Upgrades, on page 55.

Table 26: Upgrade Time Considerations

Consideration	Details
Versions	Upgrade time usually increases if your upgrade skips versions.
Models	Upgrade time usually increases with lower-end models.
Virtual appliances	Upgrade time in virtual deployments is highly hardware dependent.

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

Disk Space to Upgrade

To upgrade, the upgrade package must be on the appliance. For device upgrades with management center, you must also have enough space on the management center (in either /Volume or /var) for the device upgrade package. Or, you can use an internal server to store them. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails.

Table 27: Checking Disk Space

Platform	Command
Management center	Choose **System** (⚙) > **Monitoring** > **Statistics** and select the management center. Under Disk Usage, expand the By Partition details.
Threat defense	Choose **System** (⚙) > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.

Upgrade Feature History

Table 28: Version 7.2.6 Features

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade			

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

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Unattended threat defense upgrades.	7.2.6	Any	The threat defense upgrade wizard now supports unattended upgrades, using a new **Unattended Mode** menu. You just need to select the target version and the devices you want to upgrade, specify a few upgrade options, and step away. You can even log out or close the browser. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Simultaneous threat defense upgrade workflows by different users.	7.2.6	Any	We now allow simultaneous upgrade workflows by different users, as long as you are upgrading different devices. The system prevents you from upgrading devices already in someone else's workflow. Previously, only one upgrade workflow was allowed at a time across all users. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Skip pre-upgrade troubleshoot generation for threat defense devices.	7.2.6	Any	You can now skip the automatic generating of troubleshooting files before major and maintenance upgrades by disabling the new **Generate troubleshooting files before upgrade begins** option. This saves time and disk space. To manually generate troubleshooting files for a threat defense device, choose **System** (⚙) > **Health** > **Monitor**, click the device in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Management Center Upgrade			
New upgrade wizard for the management center.	7.2.6 7.4.1	Any	A new upgrade starting page and wizard make it easier to perform management center upgrades. After you use **System** (⚙) > **Product Upgrades** to get the appropriate upgrade package onto the management center, click **Upgrade** to begin. Other version restrictions: Only supported for management center upgrades from Version 7.2.6+/7.4.1+. Not supported for upgrades from Version 7.3.x or 7.4.0. To upgrade the management center to any version, see the upgrade guide for the version your management center is *currently* running: : Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center. If you are running Version 7.4.0, you can use the Version 7.3.x guide.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Hotfix high availability management centers without pausing synchronization.	7.2.6 7.4.1	Any	Unless otherwise indicated by the hotfix release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability management centers. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center
Content Updates			
Scheduled tasks download patches and VDB updates only.	7.2.6 7.4.1	Any	**Upgrade impact. Scheduled download tasks stop retrieving maintenance releases.** The **Download Latest Update** scheduled task no longer downloads maintenance releases; now it only downloads the latest applicable patches and VDB updates. To direct-download maintenance (and major) releases to the management center, use **System** (⚙) > **Product Upgrades**. Other version restrictions: Not supported with management center Version 7.3.x or 7.4.0. See: Software Update Automation

Feature	Minimum Management Center	Minimum Threat Defense	Details
Download only the country code geolocation package.	7.2.6 7.4.0	Any	**Upgrade impact. Upgrading can delete the IP package.** In Version 7.2.6+/7.4.0+, you can 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 with contextual data is now optional. IP package download is: • Version 7.2.0–7.2.5: Always enabled. • Version 7.2.6–7.2.x: Disabled by default, but you can enable it. • Version 7.3.x: Always enabled. • Version 7.4.0–7.4.1: Enabled by default, but you can disable it. The first time you upgrade to any version where download is disabled by default, the system disables download and deletes any existing IP package. Without the IP package, you cannot view contextual geolocation data for IP addresses until you manually enable the option and update the GeoDB. New/modified screens: • Version 7.2.6/7.4.1: **System** (⚙) > **Content Updates** > **Geolocation Updates** • Version 7.4.0: **System** (⚙) > **Updates** > **Geolocation Updates** See : Update the Geolocation Database

Table 29: Version 7.2.0 Features

Feature	Details
Threat Defense Upgrade	

Feature	Details
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 Firewall Management Center, but added to an on-prem 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**
Auto-upgrade to Snort 3 after successful threat defense upgrade.	When you use a Version 7.2+ management center to upgrade threat defense to Version 7.2+, you can now choose whether to **Upgrade Snort 2 to Snort 3**.
	After the software upgrade, eligible devices upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For help, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.
	Version restrictions: Not supported for threat defense upgrades to Version 7.0.x or 7.1.x.
Upgrade for single-node clusters.	You can now use the device upgrade page (**Devices** > **Device Upgrade**) to upgrade clusters with only one active node. Any deactivated nodes are also upgraded. Previously, this type of upgrade would fail. This feature is not supported from the system updates page (**System** (⚙)**Updates**).
	Hitless upgrades are also not supported in this case. Interruptions to traffic flow and inspection depend on the interface configurations of the lone active unit, just as with standalone devices.
	Supported platforms: Firepower 4100/9300, Secure Firewall 3100

Feature	Details
Revert threat defense upgrades from the CLI.	You can now revert threat defense upgrades from the device CLI if communications between the management center and device are disrupted. Note that in high availability/scalability deployments, revert is more successful when all units are reverted simultaneously. When reverting with the CLI, open sessions with all units, verify that revert is possible on each, then start the processes at the same time.
	Caution Reverting from the CLI can cause configurations between the device and the management center to go out of sync, depending on what you changed post-upgrade. This can cause further communication and deployment issues.
	New/modified CLI commands: **upgrade revert**, **show upgrade revert-info**.
Management Center Upgrade	
Management center upgrade does not automatically generate troubleshooting files.	To save time and disk space, the management center upgrade process no longer automatically generates troubleshooting files before the upgrade begins. Note that device upgrades are unaffected and continue to generate troubleshooting files.
	To manually generate troubleshooting files for the management center, choose **System** (⚙) > **Health** > **Monitor**, click **Firewall Management Center** in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**.
Content Updates	
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 7.2.0–7.2.5 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 both packages. In Version 7.2.6+/7.4.0+, you can configure whether you want the system to obtain the IP package.
	If you manually download updates—for example, in an air-gapped deployment—you must import the packages separately:
	• Country code package: Cisco_GEODB_Update-*date-build*.sh.REL.tar
	• IP package: Cisco_IP_GEODB_Update-*date-build*.sh.REL.tar
	Help (❓) > **About** lists the versions of the packages currently being used by the system.

Table 30: Version 7.1.0 Features

Feature	Details
Threat Defense Upgrade	

Feature	Details
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
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 31: Version 7.0.0 Features

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

Feature	Details
Easy-to-follow upgrade workflow for FTD devices.	A new device upgrade page (**Devices > Device Upgrade**) on the FMC provides an easy-to-follow wizard for upgrading Version 6.4+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks.
	To begin, use the new **Upgrade Firepower Software** action on the Device Management page (**Devices > Device Management > Select Action**).
	As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage.
	If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard.
	Note You must still use **System** (✿) > **Updates** to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices.
	Note In Version 7.0, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all. To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the wizard before you click **Next**.

Feature	Details
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 32: Version 6.7.0 Features

Feature	Details
Threat Defense Upgrade	
Upgrades remove PCAP files to save disk space.	Upgrades now remove locally stored PCAP files. To upgrade, you must have enough free disk space or the upgrade fails.

Feature	Details
Improved FTD upgrade status reporting and cancel/retry options.	You can now view the status of FTD device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages.
	A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on.
	Also on this pop-up, you can manually cancel failed or in-progress upgrades (**Cancel Upgrade**), or retry failed upgrades (**Retry Upgrade**). Canceling an upgrade reverts the device to its pre-upgrade state.
	Note To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: **Automatically cancel on upgrade failure and roll back to the previous version**. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure.
	Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.
	New/modified screens:
	• **System** (⚙) > **Updates** > **Product Updates** > **Available Updates** > **Install** icon for the FTD upgrade package
	• **Devices** > **Device Management** > **Upgrade**
	• **Message Center > Tasks**
	New/modified CLI commands: **show upgrade status detail**, **show upgrade status continuous**, **show upgrade status**, **upgrade cancel**, **upgrade retry**
Content Updates	
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 33: Version 6.6.0 Features

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

Table 34: Version 6.5.0 Features

Feature	Details
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 35: Version 6.4.0 Features

Feature	Details
Management Center Upgrade	

Feature	Details
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 36: Version 6.2.3 Features

Feature	Details
Device Upgrade	
Copy upgrade packages to managed devices before the upgrade.	You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window.
	When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary.
	New/modified screens: **System** (⚙) > **Updates**

Feature	Details
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.