



Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.4.1

First Published: 2023-12-13

Last Modified: 2023-12-13

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

Planning Your Upgrade 1

- Is This Guide for You? 1
- Important Upgrade Guidelines 2
 - Threat Defense and Management Center Upgrade Guidelines 2
 - Version 7.4.1 Guidelines 2
 - Chassis Upgrade Guidelines for the Firepower 4100/9300 3
- Compatibility 3
- Upgrade Path 4
 - Minimum Version to Upgrade Management Center 4
 - Minimum Version to Upgrade Threat Defense and Threat Defense Chassis 4
 - Upgrading Chassis with High Availability or Clustered Devices 5
- Upgrade Packages 6
 - Uploading/Downloading Upgrade Packages to the Management Center 6
 - Copying Upgrade Packages to Managed Devices 7
 - Copy Upgrade Packages from an Internal Server 8
 - Copy Threat Defense Upgrade Packages between Devices 9
 - Deleting Chassis Upgrade Packages from the Secure Firewall 3100 10
 - Upgrade Packages on Cisco.com 11
- Upgrade Readiness 13
 - Network and Infrastructure Checks 13
 - Configuration and Deployment Checks 13
 - Backups 14
 - Software Upgrade Readiness Checks 14

CHAPTER 2

Upgrade Management Center 17

- Upgrade the Management Center: Standalone 17

Upgrade the Management Center: High Availability 19

CHAPTER 3

Upgrade Threat Defense 23

Upgrade Threat Defense 23

Threat Defense Upgrade Options 26

Upgrading Threat Defense in Unattended Mode 27

Upgrade Older ASA FirePOWER and NGIPSv Devices 28

CHAPTER 4

Upgrade the Secure Firewall 3100 or Firepower 4100/9300 Chassis 31

Upgrade the Secure Firewall 3100 Chassis 31

Upgrade FXOS on the Firepower 4100/9300 with Chassis Manager 34

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using Firepower Chassis Manager 34

Upgrade FXOS on an FTD Inter-chassis Cluster Using Firepower Chassis Manager 35

Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager 38

Upgrade FXOS on the Firepower 4100/9300 with the CLI 41

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using the FXOS CLI 41

Upgrade FXOS on an FTD Inter-chassis Cluster Using the FXOS CLI 43

Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI 47

CHAPTER 5

Revert Threat Defense 53

About Reverting Threat Defense 53

Revert Guidelines for Threat Defense 54

Revert Threat Defense with Management Center 55

CHAPTER 6

Troubleshooting and Reference 57

Troubleshooting Upgrade Package Management 57

Troubleshooting Threat Defense Upgrade 58

Troubleshooting Upgrade Setup 58

Troubleshooting In-Progress Upgrade Issues and Failures 59

Traffic Flow and Inspection 60

Traffic Flow and Inspection for Threat Defense Upgrades 60

Traffic Flow and Inspection for Chassis Upgrades 62

Traffic Flow and Inspection when Deploying Configurations	62
Time and Disk Space	63
Upgrade Feature History	65



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?](#), on page 1
- [Important Upgrade Guidelines](#), on page 2
- [Compatibility](#), on page 3
- [Upgrade Path](#), on page 4
- [Upgrade Packages](#), on page 6
- [Upgrade Readiness](#), on page 13

Is This Guide for You?

Assess your deployment. Understanding where you are determines how you get to where you want to go. In addition to current version and model information, determine if your deployment is configured for high availability/clustering, if your devices are deployed as an IPS or as firewalls, and so on.

Upgrade Guidelines

The upgrade *guidelines* in this guide are for upgrading the management center or threat defense to *Version 7.4.1* or later maintenance release.

Upgrade Procedures

The upgrade *procedures* in this guide require a management center that is *already running Version 7.4.1* or later maintenance release.

Additional Resources

For upgrade procedures when:

- Upgrading the management center from Version 7.0–7.3.x, see the management center upgrade guide for the version you are currently running: <https://www.cisco.com/go/ftd-fmc-upgrade>

Note: If you are upgrading from Version 7.4.0, use the Version 7.3 guide.

- Upgrading threat defense with cloud-delivered Firewall Management Center, see: <https://www.cisco.com/go/ftd-cdfmc-upgrade>

- Upgrading threat defense with device manager Version 7.1 or later, see the device manager upgrade guide for the version you are currently running: <http://www.cisco.com/go/ftd-quick>
- Upgrading threat defense with device manager Version 7.0 or earlier, see the device manager configuration guide for the version you are currently running: <http://www.cisco.com/go/ftd-config>
- Upgrading the Firepower 4100/9300 to FXOS Version 2.13 or earlier, and need to upgrade the firmware, see: [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#)
- Upgrading the Firepower 9300 with threat defense and ASA logical devices on the same chassis, and you need to upgrade ASA, see: [Cisco Secure Firewall ASA Upgrade Guide](#)

Important Upgrade Guidelines

Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade.

Threat Defense and Management Center Upgrade Guidelines

In addition to the guidelines listed here, see the [Cisco Secure Firewall Threat Defense Release Notes](#) for features and bugs that could affect upgrade. Check all guidelines and release notes between your current and target version.

Version 7.4.1 Guidelines

Table 1:

Guideline	Details
Features with threat defense upgrade impact.	<p>The following features in Version 7.4.1 have threat defense upgrade impact:</p> <ul style="list-style-type: none"> • IPsec flow offload on the VTI loopback interface for the Secure Firewall 3100. • Captive portal support for multiple Active Directory realms (realm sequences). • Firmware upgrades included in FXOS upgrades. <p>The following features from Version 7.4.0 have threat defense upgrade impact for devices upgrading to Version 7.4.1:</p> <ul style="list-style-type: none"> • Merged management and diagnostic interfaces. • Sensitive data detection and masking.

Guideline	Details
Features with management center upgrade impact.	<p>The following features in Version 7.4.1 have management center upgrade impact:</p> <ul style="list-style-type: none"> • Configure DHCP relay trusted interfaces from the management center web interface. • Chassis-level health alerts for the Firepower 4100/9300. • Health alerts for excessive disk space used by deployment history (rollback) files. • Health alerts for NTP sync issues. • Improved management center memory usage calculation, alerting, and swap memory monitoring. • Updated internet access requirements for direct-downloading software upgrades. • Scheduled tasks download patches and VDB updates only.

Chassis Upgrade Guidelines for the Firepower 4100/9300

For the Firepower 4100/9300, use the chassis manager or CLI to upgrade FXOS, use the CLI to upgrade firmware, and the management center to upgrade threat defense.

For critical and release-specific guidelines, see:

- FXOS upgrades: [Cisco Firepower 4100/9300 FXOS Release Notes](#)
- Firmware upgrades: [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#)
- Threat defense upgrades: [Cisco Secure Firewall Threat Defense Release Notes](#)

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 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.

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.

Minimum Version to Upgrade Management Center

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. If you cannot upgrade because your hardware does not support the target version, contact your Cisco representative or partner contact for refresh information.

Table 2: Minimum Version to Upgrade Management Center

Target Version	Min. 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

Minimum Version to Upgrade Threat Defense and Threat Defense Chassis

For the Secure Firewall 3100 in multi-instance mode, any upgrade can require a chassis upgrade. Although you upgrade the chassis and threat defense separately, one package contains the chassis and threat defense upgrades and you perform both from the management center. The compatibility work is done for you. It is possible to have a chassis-only upgrade or a threat defense-only upgrade.

For the Firepower 4100/9300, major threat defense upgrades require chassis upgrades (FXOS and firmware). Maintenance releases and patches rarely require FXOS upgrades, but you may still want to upgrade to the latest FXOS build to take advantage of resolved issues. Upgrades to FXOS 2.14.1 and later include firmware, otherwise, see the [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).

If a chassis upgrade is required, threat defense is blocked. Because you upgrade the chassis first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of threat 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.

Table 3: Minimum Version to Upgrade Threat Defense and Threat Defense Chassis

Threat Defense Requirements		Additional Firepower 4100/9300 Requirements	
Target Version	Min. Version to Upgrade	Required FXOS Version	Min. Versions to Upgrade to Required FXOS Version
7.4	7.0	FXOS 2.14.1.131 or later build	Threat Defense 7.0 on FXOS 2.10
7.3	7.0	FXOS 2.13.0.198 or later build	Threat Defense 7.0 on FXOS 2.10
7.2	6.6	FXOS 2.12.0.31 or later build	Threat Defense 6.6 on FXOS 2.8

For detailed threat defense compatibility information, see the [Cisco Secure Firewall Threat Defense Compatibility Guide](#). For a Firepower 9300 with threat defense *and* ASA logical devices, make sure that upgrading FXOS does not bring you out of compatibility with either type of logical device; see [Cisco Firepower 4100/9300 FXOS Compatibility](#).

Upgrading Chassis with High Availability or Clustered Devices

For the Firepower 4100/9300 and Secure Firewall 3100 in multi-instance mode in high availability/clustered deployments, upgrade one chassis at a time.

Table 4: Chassis-Threat Defense Upgrade Order for the Firepower 4100/9300

Threat Defense Deployment	Upgrade Order
Standalone	<ol style="list-style-type: none"> 1. Upgrade chassis. 2. Upgrade threat defense.
High availability	<p>Upgrade both chassis before you upgrade threat defense. To minimize disruption, always upgrade the standby.</p> <ol style="list-style-type: none"> 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)	<ol style="list-style-type: none"> 1. Upgrade chassis. 2. Upgrade threat defense.

Threat Defense Deployment	Upgrade Order
Inter-chassis cluster (units on different chassis)	<p>Upgrade all chassis before you upgrade threat defense. To minimize disruption, always upgrade an all-data unit chassis.</p> <ol style="list-style-type: none"> 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.

Table 5: Chassis-Threat Defense Upgrade Order for the Secure Firewall 3100 in Multi-Instance Mode


Threat Defense Deployment	Upgrade Order
Standalone	<ol style="list-style-type: none"> 1. Upgrade chassis. 2. Upgrade threat defense.
High availability	<p>Upgrade both chassis before you upgrade threat defense.</p> <ol style="list-style-type: none"> 1. Upgrade chassis. With the chassis upgrade wizard, you have three options: <ul style="list-style-type: none"> • Parallel upgrade: Not recommended for high availability. • Serial upgrade: Automatically fail over when the active unit goes down. We recommend you place the standby unit first in the upgrade order. • Two workflows (run the upgrade wizard twice): Upgrade the chassis with the standby, switch roles, and upgrade the chassis with the new standby. 2. Upgrade threat defense.

Upgrade Packages

Uploading/Downloading Upgrade Packages to the Management Center

Use the Product Upgrades page (**System** (⚙️) > **Product Upgrades**) to manage software upgrade packages for your deployment. 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. If you cannot direct-download, manually download upgrade packages from Cisco and upload them here. See [Upgrade Packages on Cisco.com, on page 11](#).


Table 6: 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 8 .
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. For the Secure Firewall 3100 in multi-instance mode, chassis upgrade packages must be removed manually; see Deleting Chassis Upgrade Packages from the Secure Firewall 3100, on page 10 .

Copying Upgrade Packages to Managed Devices

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

Copying Threat Defense and Secure Firewall 3100 Chassis Upgrade Packages

For threat defense and Secure Firewall 3100 chassis 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 threat defense or chassis upgrade wizard prompt you to copy the package over.

Note that for the Secure Firewall 3100 in multi-instance mode, chassis upgrade packages are stored outside any application instances. This allows you to upgrade the chassis while also making the threat defense upgrade accessible to all instances. However, this means that you must manually remove unneeded chassis upgrade packages (instead of the upgrade process automatically removing them).

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

Table 7: Copying Threat Defense and Secure Firewall 3100 Chassis Upgrade Packages to Managed Devices

Method	Requirements	When to Use
Cisco → management center → devices.	Major, maintenance, or patch upgrade (not a hotfix) that applies to the device <i>right now</i> . 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/Downloading Upgrade Packages to the Management Center, on page 6
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 11
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 8
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 9

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 11](#) 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 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 8: 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: <code>https://internal_web_server/upgrade_package.sh.REL.tar.</code>
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 management center, but added to a customer-deployed management center in analytics mode.
- Devices in different domains, or devices separated by a NAT gateway.
- Devices upgrading from Version 7.1 or earlier, regardless of management center version.

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.

Deleting Chassis Upgrade Packages from the Secure Firewall 3100

For the Secure Firewall 3100 in multi-instance mode, chassis upgrade packages are stored outside any application instances. This allows you to upgrade the chassis while also making the threat defense upgrade accessible to all instances. However, this means that you must manually remove unneeded chassis upgrade packages (instead of the upgrade process automatically removing them).



Note You must remove unneeded chassis upgrade packages in the context of a chassis upgrade workflow. The best time to do this is when you are upgrading to the next version.

Use this procedure to delete chassis upgrade packages when you are not actively upgrading the chassis.

Before you begin

Download (or configure a pointer to) at least one chassis upgrade package other than the one corresponding to the package you want to delete.

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

Step 2 Select the chassis that have the unneeded packages and under **Select Action** or **Select Bulk Action**, choose **Upgrade FXOS and Firmware (Chassis Only)**.

The chassis upgrade wizard appears.

Step 3 Choose a target version from the **Upgrade to** menu.

Choose any version other than the one corresponding to the package you want to delete. You will not be upgrading to this version so it doesn't matter which you choose.

- Step 4** In the Device Selection pane, click the message that says: X devices have packages that might not be needed.
- The chassis that have unneeded packages are listed in the Device Details pane. Note that you cannot delete a package for the version the chassis is currently running, nor a package for the "target version" you selected. Only chassis with packages other than these are counted.
- Step 5** In the Device Details pane, select a chassis, click **Manage Upgrade Packages on Device**, select the packages you want to remove and click **Remove**.
- Repeat this step for each chassis you want to clean up.
- Step 6** Back in the chassis upgrade wizard, click **Reset** to reset the workflow.

Upgrade Packages on Cisco.com

Manually download upgrade packages from Cisco when the management center 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 Upgrade 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 signed upgrade packages. Do not rename upgrade packages or transfer them by email.

Table 9: Software Upgrade Packages

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

Platform	Upgrade Package
Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade- <i>Version-build</i> .sh.REL.tar Also contains the FXOS companion version, for multi-instance mode upgrades.
Secure Firewall 4200 series	Cisco_Secure_FW_TD_4200_Upgrade- <i>Version-build</i> .sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade- <i>Version-build</i> .sh.REL.tar
ASA 5500-X series with FTD	Cisco_FTD_Upgrade- <i>Version-build</i> .sh.REL.tar
Threat Defense Virtual	Cisco_FTD_Upgrade- <i>Version-build</i> .sh.REL.tar
ISA 3000 with FTD	Cisco_FTD_Upgrade- <i>Version-build</i> .sh.REL.tar
ASA FirePOWER	Cisco_Firepower_NGIPS_Appliance_Upgrade- <i>Version-build</i> .sh.REL.tar
NGIPSv	Cisco_Firepower_NGIPS_Virtual_Upgrade- <i>Version-build</i> .sh.REL.tar

Chassis Upgrade Packages for the Firepower 4100/9300

To find the correct FXOS image, 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 image is listed along with recovery and MIB packages.

Table 10: FXOS Upgrade Packages

Platform	Upgrade Package
Firepower 4100/9300	fxos-k9. <i>fxos_version</i> .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 11: Firmware Upgrade Packages

Platform	Upgrade Package
Firepower 4100	fxos-k9-fpr4k-firmware. <i>firmware_version</i> .SPA
Firepower 9300	fxos-k9-fpr9k-firmware. <i>firmware_version</i> .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 be 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 Management 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. Resolve any change management workflows. 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 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, 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 12: Backups

Platform	Guide	Details
Management center	<i>Backup/Restore</i> in the Cisco Secure Firewall Management Center Administration Guide .	We recommend you back up configurations and events.
Threat defense	<i>Backup/Restore</i> in the Cisco Secure Firewall Management Center Administration Guide .	Backup is not supported for clustered threat defense virtual for KVM devices or threat defense virtual in the public cloud.
Secure Firewall 3100 chassis	<i>Multi-Instance Mode for the Secure Firewall 3100</i> in the Cisco Secure Firewall Management Center Device Configuration Guide .	—
Firepower 4100/9300 chassis	<i>Configuration Import/Export</i> in the Cisco Firepower 4100/9300 FXOS Configuration Guide .	—
Firepower 9300 chassis with ASA	<i>Software and Configurations</i> in the Cisco ASA Series General Operations Configuration Guide .	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.



CHAPTER 2

Upgrade Management Center

- [Upgrade the Management Center: Standalone, on page 17](#)
- [Upgrade the Management Center: High Availability, on page 19](#)

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 62](#). 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 3](#)
- Plan the upgrade path: [Upgrade Path, on page 4](#)
- Review the upgrade guidelines: [Important Upgrade Guidelines, on page 2](#)
- Check infrastructure and network: [Network and Infrastructure Checks, on page 13](#)

- Check configurations, tasks, and overall deployment health: [Configuration and Deployment Checks, on page 13](#)
- Perform backups: [Backups, on page 14](#)

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/Downloading Upgrade Packages to the Management Center, on page 6](#) and [Troubleshooting Upgrade Package Management, on page 57](#).

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 13](#).

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 62](#). 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 reimaging. 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 3](#)
- Plan the upgrade path: [Upgrade Path, on page 4](#)
- Review the upgrade guidelines: [Important Upgrade Guidelines, on page 2](#)
- Check infrastructure and network: [Network and Infrastructure Checks, on page 13](#)

- Check configurations, tasks, and overall deployment health: [Configuration and Deployment Checks, on page 13](#)
- Perform backups: [Backups, on page 14](#)

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/Downloading Upgrade Packages to the Management Center, on page 6](#) and [Troubleshooting Upgrade Package Management, on page 57](#).

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 13](#).

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.

- Choose **Integration > Other Integrations**.
- 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, on page 23](#)
- [Upgrade Older ASA FirePOWER and NGIPSv Devices, on page 28](#)

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 > Threat Defense 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 60](#).



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 [Troubleshooting In-Progress Upgrade Issues and Failures, on page 59](#)

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: [Compatibility, on page 3](#)
- Plan the upgrade path: [Upgrade Path, on page 4](#)
- Review the upgrade guidelines: [Important Upgrade Guidelines, on page 2](#)
- Check infrastructure and network: [Network and Infrastructure Checks, on page 13](#)

- Check configurations, tasks, and overall deployment health: [Configuration and Deployment Checks, on page 13](#)
- Perform backups: [Backups, on page 14](#)
- Upgrade the chassis, if required: [Upgrade the Secure Firewall 3100 or Firepower 4100/9300 Chassis, on page 31](#)

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/Downloading Upgrade Packages to the Management Center, on page 6](#) and [Troubleshooting Upgrade Package Management, on page 57](#).

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.

(Optional) 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 [Upgrading Threat Defense in Unattended Mode, on page 27](#).

Step 5 Copy upgrade packages to devices.

Click **Copy Upgrade Package** and wait for the transfer to complete. For the Secure Firewall 3100 in multi-instance mode, if you upgraded the chassis, the upgrade package should already be on the device (unless you deleted it).

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 26](#).

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 13](#).

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 14](#)

Threat Defense Upgrade Options

Table 13: 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. With upgrades to Version 7.3+, you can no longer disable this option. Although you can switch individual devices back, Snort 2 will be deprecated in a future release and we strongly recommend you stop using it now. For devices that are ineligible 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.

Option	When to Disable	Details
Enable revert after successful upgrade.	To save time and disk space.	<p>With upgrades to 7.1+, you have 30 days to revert threat defense upgrades.</p> <p>Reverting returns the software to its state just before the last upgrade, also called a <i>snapshot</i>. If you revert an upgrade after installing a patch, you revert the patch as well as the upgrade.</p> <p>Not supported for container instances, patches, or hotfixes.</p>

Upgrading 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 14:

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.	<p>In the threat defense upgrade wizard, choose Unattended Mode > Stop.</p> <p>You can pause and restart unattended mode during the copy and checks phases. However, pausing unattended mode does <i>not</i> 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.</p> <p>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.</p>
Monitor an unattended upgrade.	<p>To monitor an unattended upgrade:</p> <ul style="list-style-type: none"> • 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](#).

SUMMARY STEPS

1. On the management center, choose **System** (⚙) > **Product Upgrades**.
2. Get the device upgrade packages onto the management center.
3. Click **Upgrade** next to the target version and select the type of device you want to upgrade: **ASA FirePOWER** or **NGIPSv**.
4. Select the devices you want to upgrade.
5. Click **Install**, then confirm that you want to upgrade and reboot the devices.
6. Verify success.
7. Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).
8. Complete any required post-upgrade configuration changes.
9. Redeploy configurations to the devices you just upgraded.

DETAILED STEPS

	Command or Action	Purpose
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

	Command or Action	Purpose
		<p>specially marked. In most cases, you can just click Download next to the upgrade package or version you want.</p> <p>For more information, see Uploading/Downloading Upgrade Packages to the Management Center, on page 6 and Troubleshooting Upgrade Package Management, on page 57.</p>
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.	



CHAPTER 4

Upgrade the Secure Firewall 3100 or Firepower 4100/9300 Chassis

For the Secure Firewall 3100 in multi-instance mode, any upgrade can require a chassis upgrade. Although you upgrade the chassis and threat defense separately, one package contains the chassis and threat defense upgrades and you perform both from the management center. The compatibility work is done for you. It is possible to have a chassis-only upgrade or a threat defense-only upgrade.

For the Firepower 4100/9300, major threat defense upgrades require chassis upgrades (FXOS and firmware). Maintenance releases and patches rarely require FXOS upgrades, but you may still want to upgrade to the latest FXOS build to take advantage of resolved issues. Upgrades to FXOS 2.14.1 and later include firmware, otherwise, see the [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).

- [Upgrade the Secure Firewall 3100 Chassis, on page 31](#)
- [Upgrade FXOS on the Firepower 4100/9300 with Chassis Manager, on page 34](#)
- [Upgrade FXOS on the Firepower 4100/9300 with the CLI, on page 41](#)

Upgrade the Secure Firewall 3100 Chassis

Use this procedure to upgrade the chassis on the Secure Firewall 3100 in multi-instance mode. As you proceed, the chassis upgrade wizard displays basic information about your selected chassis, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a chassis 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 chassis 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 > Chassis Upgrade**.

Chassis 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 chassis, and choosing upgrade options. For information on traffic handling during the upgrade, see [Traffic Flow and Inspection for Chassis Upgrades, on page 62](#).



Caution Do not make or deploy configuration changes to the chassis or threat defense instances during the 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. Chassis may reboot multiple times during the upgrade. This is expected behavior. If you encounter issues with the upgrade, including a failed upgrade or unresponsive chassis, contact Cisco TAC.

Feature History:

- 7.4.1: Chassis upgrade introduced.

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: [Compatibility, on page 3](#)
 - Plan the upgrade path: [Upgrade Path, on page 4](#)
 - Review the upgrade guidelines: [Important Upgrade Guidelines, on page 2](#)
 - Check infrastructure and network: [Network and Infrastructure Checks, on page 13](#)
 - Check configurations, tasks, and overall deployment health: [Configuration and Deployment Checks, on page 13](#)
 - Perform backups: [Backups, on page 14](#)
-

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 chassis upgrade packages onto the management center.

Before you copy upgrade packages to managed chassis, you must upload the packages to the management center (or to an internal server that the chassis 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/Downloading Upgrade Packages to the Management Center, on page 6](#) and [Troubleshooting Upgrade Package Management, on page 57](#).

Step 3 Launch the upgrade wizard.

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

The chassis 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 chassis. Your target version is pre-selected in the **Upgrade to** menu. The system determines which chassis can be upgraded to that version and displays them in the Device Details pane. The Device Selection pane also displays the FXOS and firmware versions contained in the upgrade package.

Step 4 Select chassis to upgrade.

In the Device Details pane, select the chassis 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 chassis, remaining upgrade candidates, ineligible chassis (with reasons why), chassis that need the upgrade package, and so on. You can add and remove chassis from your selection, or click **Reset** to clear your device selection and start over. Note that you do not have to remove ineligible chassis; they are automatically excluded from upgrade.

Step 5 (Optional) Remove unneeded upgrade packages from your selected chassis.

You must manually manage chassis upgrade packages. Right now is a good time to clean up.

- a) In the Device Selection pane, click the message that says: `X devices have packages that might not be needed`.
- b) In the Device Details pane, select a chassis, click **Manage Upgrade Packages on Device**, select the packages you want to remove and click **Remove**.

Repeat this step for each chassis you want to clean up.

Step 6 Copy the new upgrade package to the chassis.

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

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

By default, chassis upgrades run in parallel.

For chassis with high availability instances, we recommend serial upgrade order. Select the appropriate chassis in the Device Details pane and click **Move to Serial Upgrade**. We also recommend you place the chassis with the standby unit first in the upgrade order. To change serial upgrade order, click **Change Upgrade Order**. For more information, see [Upgrading Chassis with High Availability or Clustered Devices, on page 5](#).

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 13](#).

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

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.

Step 10 Verify success.

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

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

Depending on how you performed the upgrade, high availability instances may have switched roles. Keeping in mind that any subsequent threat defense upgrade will also switch device roles, make any desired changes.

What to do next

(Optional) Clear the wizard by clicking **Clear Upgrade Information**. Until you do this, the page continues to display details about the upgrade you just performed.

Upgrade FXOS on the Firepower 4100/9300 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:
- Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the control unit).
 - Enter **top**.
 - Enter **scope ssa**.
 - Enter **show slot**.
 - 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.
 - Enter **show app-instance**.
 - 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`.
- 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:
- Click **Upload Image** to open the Upload Image dialog box.
 - Click **Choose File** to navigate to and select the image that you want to upload.
 - Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
 - 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:
- Enter **scope system**.
 - 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
Cluster   Slave
ftd        2         Enabled   Online      6.2.2.81    6.2.2.81
Cluster   Slave
ftd        3         Disabled  Not Available 6.2.2.81
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 on the Firepower 4100/9300 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:
- Enter **top**.
 - Enter **scope ssa**.
 - Enter **show slot**.
 - 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.
 - Enter **show app-instance**.
 - 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:
- Connect to Firepower Management Center.
 - Choose **Devices > Device Management**.
 - Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ()
 - 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:
- Enter firmware mode:
Firepower-chassis-a # **scope firmware**
 - 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**
 - 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.
-



CHAPTER 5

Revert Threat Defense

If a threat defense upgrade succeeds but the system does not function to your expectations, you may be able to revert. If this will not work for you and you still need to return to an earlier version, you must reimage. You cannot revert the management center.

- [About Reverting Threat Defense, on page 53](#)
- [Revert Guidelines for Threat Defense, on page 54](#)
- [Revert Threat Defense with Management Center, on page 55](#)

About Reverting Threat Defense

Reverting threat defense returns the software to its state just before the last upgrade. 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 [Revert Guidelines for Threat Defense, on page 54](#).

Revert Guidelines for Threat Defense

System Requirements

Revert is supported for major and maintenance threat defense upgrades.

Reverting threat defense requires Version 7.1+ on the device and the management center. For example, even though a Version 7.1 management center can manage a device as far back as Version 6.5, and even though you can use that Version 7.1 management center to upgrade a device to intermediate versions (6.6, 6.7, 7.0), revert is not supported until you upgrade the device to Version 7.1.

Revert is not supported for:

- Patches and hotfixes
- Threat defense container instances
- Management centers

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 15: Scenarios Preventing Revert

Scenario	Solution
Revert snapshot is not available because: <ul style="list-style-type: none"> • 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 <i>and</i> 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 reimagine.
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.



CHAPTER 6

Troubleshooting and Reference

- [Troubleshooting Upgrade Package Management](#), on page 57
- [Troubleshooting Threat Defense Upgrade](#), on page 58
- [Traffic Flow and Inspection](#), on page 60
- [Time and Disk Space](#), on page 63
- [Upgrade Feature History](#), on page 65

Troubleshooting Upgrade Package Management

Table 16:

Issue	Solution
No available upgrades even after I refresh.	Direct-downloading upgrade packages requires internet access on the management center. You will also see a blank list if you are already running the latest version available for your deployment <i>and</i> you have no upgrade packages loaded/configured.
The suggested release is not marked.	The suggested release is listed only if you are eligible for it. It is not listed if you are already running the suggested release or higher, or if you cannot upgrade that far. Note that patches to suggested releases are not marked as suggested, although we do recommend you apply them.
I don't see the packages I want.	Only major, maintenance, and patch upgrades that apply to your deployment <i>right now</i> are listed and available for direct download. Unless you manually upload, the following are not listed: <ul style="list-style-type: none">• Device upgrades (major and maintenance) to a particular version, unless the management center is running that version or higher, <i>and</i> you have a device that supports that version.• 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 <i>all</i> devices managed by this management center. In a multidomain deployment, this can include devices that you cannot access right now.

Troubleshooting Threat Defense Upgrade

Troubleshooting Upgrade Setup

Table 17:

Issue	Solution
Upgrade button missing for my target version on the Product Upgrades page.	Either of: <ul style="list-style-type: none"> • 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.	<p>If you accessed the wizard directly from Devices > Threat Defense Upgrade, the workflow may be blank.</p> <p>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/Downloading Upgrade Packages to the Management Center, on page 6.</p> <p>If you have a target version but the wizard still does not list any devices, you have no devices that can be upgraded to that version. If you still think you should see devices here, your user role could be prohibiting you from managing (and therefore upgrading) devices. In a multidomain deployment, you could be logged into the wrong domain.</p>
Devices locked to someone else's upgrade workflow.	<p>If you need to reset someone else's workflow, you must have Administrator access. You can either:</p> <ul style="list-style-type: none"> • Delete or deactivate the user. • Update the user's role so they no longer have permission to use System (⚙️) > Product Upgrades.

Issue	Solution
<p>Copying upgrade packages from the management center to managed devices times out.</p>	<p>This often happens when there is limited bandwidth between the management center and its devices.</p> <p>You can try one of:</p> <ul style="list-style-type: none"> • Configure devices to get upgrade packages directly from an internal web server. <p>To do this, delete the upgrade package from the management center (optional but saves disk space), then re-add the upgrade package except this time specify a pointer (URL) to its location instead. See Copy Upgrade Packages from an Internal Server, on page 8.</p> <ul style="list-style-type: none"> • Copy upgrade packages from another device. <p>If you can get the upgrade package to at least one standalone device, you can then use the threat defense CLI to copy upgrade packages ("peer to peer sync") to the other standalone devices managed by the same standalone management center. See Copy Threat Defense Upgrade Packages between Devices, on page 9.</p>
<p>High availability management center failed over while setting up upgrade.</p>	<p>Neither your workflow nor threat defense upgrade packages are synchronized between high availability management centers.</p> <p>In case of failover, you must recreate your workflow on the new active management center, which includes downloading upgrade packages and copying them to devices. (Upgrade packages already copied to devices are not removed, but the management center still must have the package or a pointer to its location.)</p>

Troubleshooting In-Progress Upgrade Issues and Failures

Table 18:

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

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

Traffic Flow and Inspection

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

Traffic Flow and Inspection for Threat Defense Upgrades

Software Upgrades for Standalone Devices

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

Table 19: Traffic Flow and Inspection: Software Upgrades for Standalone Devices

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

Software Upgrades for High Availability and Clustered Devices

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

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

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

Software Revert (Major/Maintenance Releases)

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

Software Uninstall (Patches)

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

Traffic Flow and Inspection for Chassis Upgrades

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

Even in high availability or clustered deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time. For more information, see [Upgrading Chassis with High Availability or Clustered Devices, on page 5](#).

Table 20: 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 21: 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 Upgrades](#).

Table 22: Upgrade Time Considerations

Consideration	Details
Versions	Upgrade time usually increases if your upgrade skips versions.
Models	Upgrade time usually increases with lower-end models.

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

Disk Space to Upgrade

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

Table 23: 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 with management center	Choose System > Monitoring > Statistics and select the device you want to check. Under Disk Usage, expand the By Partition details.

Upgrade Feature History

Table 24: Version 7.4.1 Features

Feature	Min. Threat Defense	Description
<p>Improved upgrade starting page and package management.</p>	<p>Any</p>	<p>A new upgrade page makes it easier to choose, download, manage, and apply upgrades to your entire deployment. This includes the management center, threat defense devices, and any older NGIPSv/ASA FirePOWER devices. The page lists all upgrade packages that apply to your current deployment, with suggested releases specially marked. You can easily choose and direct-download packages from Cisco, as well as manually upload and delete packages.</p> <p>Internet access is required to retrieve the list/direct download upgrade packages. Otherwise, you are limited to manual management. Patches are not listed unless you have at least one appliance at the appropriate maintenance release (or you manually uploaded the patch). You must manually upload hotfixes.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • 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). <p>Deprecated screens/options:</p> <ul style="list-style-type: none"> • 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. <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>
<p>Enable revert from the threat defense upgrade wizard.</p>	<p>Any, if upgrading to 7.1+</p>	<p>You can now enable revert from the threat defense upgrade wizard.</p> <p>Other version restrictions: You must be upgrading threat defense to Version 7.1+.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>

Feature	Min. Threat Defense	Description
View detailed upgrade status from the threat defense upgrade wizard.	Any	<p>The final page of the threat defense upgrade wizard now allows you to monitor upgrade progress. This is in addition to the existing monitoring capability on the Upgrade tab on the Device Management page, and on the Message Center. Note that as long as you have not started a new upgrade flow, 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.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>
Automatically generate configuration change reports after management center upgrade.	Any	<p>You can automatically generate reports on configuration changes after major and maintenance management center upgrades. This helps you understand the changes you are about to deploy. After the system generates the reports, you can download them from the Tasks tab in the Message Center.</p> <p>Other version restrictions: Only supported for management center upgrades from Version 7.4.1+. Not supported for upgrades to Version 7.4.1 or any earlier version.</p> <p>New/modified screens: System (⚙️) > Configuration > Upgrade Configuration > Enable Post-Upgrade Report</p> <p>See: Upgrade Configuration</p>
Suggested release notifications.	Any	<p>The management center now notifies you when a new suggested release is available. If you don't want to upgrade right now, you can have the system remind you later, or defer reminders until the next suggested release. The new upgrade page also indicates suggested releases.</p> <p>See: Cisco Secure Firewall Management Center New Features by Release</p>
New upgrade wizard for the management center.	Any	<p>A new upgrade starting page and wizard make it easier to perform management center upgrades. After you use System (⚙️) > Product Upgrades to get the appropriate upgrade package onto the management center, click Upgrade to begin.</p> <p>Other version restrictions: Only supported for management center upgrades from Version 7.4.1+.</p> <p>To upgrade the management center to any version, see the upgrade guide for the version your management center is <i>currently</i> running: : 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.</p>
Hotfix high availability management centers without pausing synchronization.	Any	<p>Unless otherwise indicated by the hotfix release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability management centers.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>

Feature	Min. Threat Defense	Description
Firmware upgrades included in FXOS upgrades.	Any	<p>Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.</p> <p>For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include firmware upgrades. Secure Firewall 3100 in multi-instance mode (new in Version 7.4.1) also bundles FXOS and firmware upgrades. If any firmware component on the device is older than the one included in the FXOS bundle, the FXOS upgrade also updates the firmware. If the firmware is upgraded, the device reboots twice—once for FXOS and once for the firmware.</p> <p>Just as with software and operating system upgrades, do not make or deploy configuration changes during firmware upgrade. Even if the system appears inactive, do not manually reboot or shut down during firmware upgrade.</p> <p>See: Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide</p>
Chassis upgrade for the Secure Firewall 3100 in multi-instance mode.	7.4.1	<p>For the Secure Firewall 3100 in multi-instance mode, you upgrade the operating system and the firmware (<i>chassis upgrade</i>) separately from the container instances (<i>threat defense upgrade</i>).</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • Upgrade the chassis: Devices > Chassis Upgrade • Upgrade threat defense: Devices > Threat Defense Upgrade <p>Supported platforms: Secure Firewall 3100, excluding the Secure Firewall 3105</p> <p>Minimum management center: 7.4.1</p>
Updated internet access requirements for direct-downloading software upgrades.	Any	<p>Upgrade impact. The system connects to new resources.</p> <p>The management center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com.</p> <p>See: Internet Access Requirements</p>
Scheduled tasks download patches and VDB updates only.	Any	<p>Upgrade impact. Scheduled download tasks stop retrieving maintenance releases.</p> <p>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.</p> <p>See: Software Update Automation</p>

Table 25: Version 7.4.0 Features

Feature	Min. Threat Defense	Description
Content Updates		

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

Table 26: Version 7.3.0 Features

Feature	Min. Threat Defense	Description
Product Upgrades		
Choose and direct-download upgrade packages to the management center from Cisco.	Any	<p>You can now choose which threat defense upgrade packages you want to direct download to the management center. Use the new Download Updates sub-tab on > Updates > Product Updates.</p> <p>Minimum management center: 7.3.0. In Version 7.4.1+, this feature is replaced by an improved package management system.</p> <p>See: Download Upgrade Packages with the Management Center</p>
Upload upgrade packages to the management center from the threat defense wizard.	Any	<p>You now use the wizard to upload threat defense upgrade packages or specify their location. Previously you used System (⚙️) > Updates.</p> <p>Minimum management center: 7.3.0. In Version 7.4.1+, this feature is replaced by an improved package management system.</p> <p>See: Upgrade Threat Defense</p>
Select devices to upgrade from the threat defense upgrade wizard.	Any	<p>Use the wizard to select devices to upgrade.</p> <p>You can now use the threat defense upgrade wizard to select or refine the devices to upgrade. On the wizard, you can toggle the view between selected devices, remaining upgrade candidates, ineligible devices (with reasons why), devices that need the upgrade package, and so on. Previously, you could only use the Device Management page and the process was much less flexible.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>
Unattended threat defense upgrades.	Any	<p>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.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>

Feature	Min. Threat Defense	Description
<p>Simultaneous threat defense upgrade workflows by different users.</p>	<p>Any</p>	<p>We now allow simultaneous upgrade workflows by different users, as long as you are upgrading different devices. The system prevents you from upgrading devices already in someone else's workflow. Previously, only one upgrade workflow was allowed at a time across all users.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>
<p>Skip pre-upgrade troubleshoot generation for threat defense devices.</p>	<p>Any</p>	<p>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.</p> <p>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.</p> <p>See: Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center</p>
<p>Auto-upgrade to Snort 3 after successful threat defense upgrade is no longer optional.</p>	<p>Any</p>	<p>Upgrade impact.</p> <p>When you upgrade threat defense to Version 7.3+, you can no longer disable the Upgrade Snort 2 to Snort 3 option.</p> <p>After the software upgrade, all eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. Although you can switch individual devices back, Snort 2 will be deprecated in a future release and we strongly recommend you stop using it now.</p> <p>For devices that are ineligible for auto-upgrade because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.</p>

Feature	Min. Threat Defense	Description
<p>Combined upgrade and install package for Secure Firewall 3100.</p>	<p>7.3.0</p>	<p>Reimage Impact.</p> <p>In Version 7.3, we combined the threat defense install and upgrade package for the Secure Firewall 3100, as follows:</p> <ul style="list-style-type: none"> • Version 7.1–7.2 install package: <code>cisco-ftd-fp3k.version.SPA</code> • Version 7.1–7.2 upgrade package: <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code> • Version 7.3+ combined package: <code>Cisco_FTD_SSP_FP3K_Upgrade-version-build.sh.REL.tar</code> <p>Although you can upgrade threat defense without issue, you cannot reimage from older threat defense and ASA versions directly to threat defense Version 7.3+. This is due to a ROMMON update required by the new image type. To reimage from those older versions, you must "go through" ASA 9.19+, which is supported with the old ROMMON but also updates to the new ROMMON. There is no separate ROMMON updater.</p> <p>To get to threat defense Version 7.3+, your options are:</p> <ul style="list-style-type: none"> • Upgrade from threat defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate Upgrade Guide. • Reimage from threat defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to threat defense Version 7.3+. <ul style="list-style-type: none"> See <i>Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100</i> and then <i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i> in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from ASA 9.17 or 9.18 — upgrade to ASA 9.19+ first, then reimage to threat defense Version 7.3+. <ul style="list-style-type: none"> See the Cisco Secure Firewall ASA Upgrade Guide and then <i>ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100</i> in the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide. • Reimage from threat defense Version 7.3+ — use the normal reimage process. <ul style="list-style-type: none"> See <i>Reimage the System with a New Software Version</i> in the Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower Threat Defense.

Content Updates

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

Table 27: Version 7.2.0 Features

Feature	Description
Threat Defense Upgrades	

Feature	Description
<p>Copy upgrade packages ("peer-to-peer sync") from device to device.</p>	<p>Instead of copying upgrade packages to each device from the management center or internal web server, you can use the threat defense CLI to copy upgrade packages between devices ("peer to peer sync"). This secure and reliable resource-sharing goes over the management network but does not rely on the management center. Each device can accommodate 5 package concurrent transfers.</p> <p>This feature is supported for Version 7.2+ standalone devices managed by the same standalone management center. It is not supported for:</p> <ul style="list-style-type: none"> • Container instances. • Device high availability pairs and clusters. <p>These devices get the package from each other as part of their normal sync process. Copying the upgrade package to one group member automatically syncs it to all group members.</p> <ul style="list-style-type: none"> • Devices managed by high availability management centers. • Devices managed by the cloud-delivered management center, but added to a customer-deployed management center in analytics mode. • Devices in different domains, or devices separated by a NAT gateway. • Devices upgrading from Version 7.1 or earlier, regardless of management center version. <p>New/modified CLI commands: configure p2psync enable, configure p2psync disable, show peers, show peer details, sync-from-peer, show p2p-sync-status</p>
<p>Auto-upgrade to Snort 3 after successful threat defense upgrade.</p>	<p>When you use a Version 7.2+ management center to upgrade threat defense, you can now choose whether to Upgrade Snort 2 to Snort 3.</p> <p>After the software upgrade, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the Cisco Secure Firewall Management Center Snort 3 Configuration Guide for your version.</p> <p>This option is supported for major and maintenance threat defense upgrades to Version 7.2+. It is not supported for threat defense upgrades to Version 7.0 or 7.1, or for patches to any version.</p>
<p>Upgrade for single-node clusters.</p>	<p>You can now use the device upgrade page (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).</p> <p>Hitless upgrades are also not supported in this case. Interruptions to traffic flow and inspection depend on the interface configurations of the lone active unit, just as with standalone devices.</p> <p>Supported platforms: Firepower 4100/9300, Secure Firewall 3100</p>

Feature	Description
Revert threat defense upgrades from the CLI.	<p>You can now revert threat defense upgrades from the device CLI if communications between the management center and device are disrupted. Note that in high availability/scalability deployments, revert is more successful when all units are reverted simultaneously. When reverting with the CLI, open sessions with all units, verify that revert is possible on each, then start the processes at the same time.</p> <p>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.</p> <p>New/modified CLI commands: upgrade revert, show upgrade revert-info.</p>
Management Center Upgrades	
Management center upgrade does not automatically generate troubleshooting files.	<p>To save time and disk space, the management center upgrade process no longer automatically generates troubleshooting files before the upgrade begins. Note that device upgrades are unaffected and continue to generate troubleshooting files.</p> <p>To manually generate troubleshooting files for the management center, choose System (⚙️) > Health > Monitor, click Firewall Management Center in the left panel, then View System & Troubleshoot Details, then Generate Troubleshooting Files.</p>
Content Updates	
GeoDB is split into two packages.	<p>In May 2022, shortly before the Version 7.2 release, we split the GeoDB into two packages: a country code package that maps IP addresses to countries/continents, and an IP package that contains additional contextual data associated with routable IP addresses. The contextual data in the IP package can include additional location details, as well as connection information such as ISP, connection type, proxy type, domain name, and so on.</p> <p>If your Version 7.2+ management center has internet access and you enable recurring updates or you manually kick off a one-time update from the Cisco Support & Download site, the system automatically obtains and imports both packages. However, if you manually download updates—for example, in an air-gapped deployment—make sure you get and import both GeoDB packages:</p> <ul style="list-style-type: none"> • Country code package: Cisco_GEODB_Update-<i>date-build</i>.sh.REL.tar • IP package: Cisco_IP_GEODB_Update-<i>date-build</i>.sh.REL.tar <p>The Geolocation Updates (System (⚙️) > Updates > Geolocation Updates) page and the About page (Help > About) list the versions of the packages currently being used by the system.</p>

Table 28: Version 7.1.0 Features

Feature	Description
Product Upgrades	

Feature	Description
<p>Revert a successful device upgrade.</p>	<p>You can now revert major and maintenance upgrades to FTD. Reverting returns the software to its state just before the last upgrade, also called a <i>snapshot</i>. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade.</p> <p>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.</p> <p>This feature is not supported for container instances.</p> <p>Minimum FTD: 7.1</p> <p>Minimum threat defense: 7.1</p>
<p>Improvements to the upgrade workflow for clustered and high availability devices.</p>	<p>We made the following improvements to the upgrade workflow for clustered and high availability devices:</p> <ul style="list-style-type: none"> • 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 29: Version 7.0.0 Features

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

Feature	Description
<p>Easy-to-follow upgrade workflow for FTD devices.</p>	<p>A new device upgrade page (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.</p> <p>To begin, use the new Upgrade Firepower Software action on the Device Management page (Devices > Device Management > Select Action).</p> <p>As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage.</p> <p>If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard.</p> <p>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.</p> <p>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.</p> <p>To avoid possible time-consuming upgrade failures, <i>manually</i> ensure all group members are ready to move on to the next step of the wizard before you click Next.</p>

Feature	Description
Upgrade more FTD devices at once.	<p>The FTD upgrade wizard lifts the following restrictions:</p> <ul style="list-style-type: none"> • Simultaneous device upgrades. <p>The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time.</p> <p>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.</p> <ul style="list-style-type: none"> • Grouping upgrades by device model. <p>You can now queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages.</p> <p>Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time <i>only</i> if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series.</p>

Table 30: Version 6.7.0 Features

Feature	Description
Product Upgrades	

Feature	Description
<p>Improved FTD upgrade status reporting and cancel/retry options.</p>	<p>You can now view the status of FTD device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages.</p> <p>A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on.</p> <p>Also on this pop-up, you can manually cancel failed or in-progress upgrades (Cancel Upgrade), or retry failed upgrades (Retry Upgrade). Canceling an upgrade reverts the device to its pre-upgrade state.</p> <p>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.</p> <p>Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.</p> <p>New/modified screens:</p> <ul style="list-style-type: none"> • System (⚙️) > Updates > Product Updates > Available Updates > Install icon for the FTD upgrade package • Devices > Device Management > Upgrade • Message Center > Tasks <p>New/modified CLI commands: show upgrade status detail, show upgrade status continuous, show upgrade status, upgrade cancel, upgrade retry</p>
<p>Upgrades remove PCAP files to save disk space.</p>	<p>Upgrades now remove locally stored PCAP files. To upgrade, you must have enough free disk space or the upgrade fails.</p>
<p>Content Updates</p>	
<p>Custom intrusion rule import warns when rules collide.</p>	<p>The FMC now warns you of rule collisions when you import custom (local) intrusion rules. Previously, the system would silently skip the rules that cause collisions—with the exception of Version 6.6.0.1, where a rule import with collisions would fail entirely.</p> <p>On the Rule Updates page, if a rule import had collisions, a warning icon is displayed in the Status column. For more information, hover your pointer over the warning icon and read the tooltip.</p> <p>Note that a collision occurs when you try to import an intrusion rule that has the same SID/revision number as an existing rule. You should always make sure that updated versions of custom rules have new revision numbers.</p> <p>New/modified screens: We added a warning icon to System (⚙️) > Updates > Rule Updates.</p>

Table 31: Version 6.6.0 Features

Feature	Description
Product Upgrades	
<p>Get FTD upgrade packages from an internal web server.</p>	<p>FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC.</p> <p>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.</p> <p>New/modified screens: We added a Specify software update source option to the page where you upload upgrade packages.</p>
Content Updates	
<p>Automatic VDB update during initial setup.</p>	<p>When you set up a new or reimaged FMC, the system automatically attempts to update the vulnerability database (VDB).</p> <p>This is a one-time operation. If the FMC has internet access, we recommend you schedule tasks to perform automatic recurring VDB update downloads and installations.</p>

Table 32: Version 6.5.0 Features

Feature	Description
Content Updates	
<p>Automatic software downloads and GeoDB updates.</p>	<p>When you set up a new or reimaged FMC, the system automatically schedules:</p> <ul style="list-style-type: none"> • A weekly task to download software updates for the FMC and its managed devices. • Weekly updates for the GeoDB. <p>The tasks are scheduled in UTC, which means that when they occur locally depends on the date and your specific location. Also, because tasks are scheduled in UTC, they do not adjust for Daylight Saving Time, summer time, or any such seasonal adjustments that you may observe in your location. If you are affected, scheduled tasks occur one hour “later” in the summer than in the winter, according to local time. We recommend you review the auto-scheduled configurations and adjust them if necessary.</p>

Table 33: Version 6.4.0 Features

Feature	Description
Upgrades postpone scheduled tasks.	<p>The management center upgrade process now postpones scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot.</p> <p>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.</p> <p>Note that this feature is supported for all upgrades <i>from</i> a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades <i>to</i> a supported version from an unsupported version.</p>
Content Updates	
Signed SRU, VDB, and GeoDB updates.	<p>So the system can verify that you are using the correct update files, Version 6.4+ uses <i>signed</i> updates for intrusion rules (SRU), the vulnerability database (VDB), and the geolocation database (GeoDB). Earlier versions continue to use unsigned updates.</p> <p>Unless you manually download updates from the Cisco Support & Download site—for example, in an air-gapped deployment—you should not notice any difference in functionality. If, however, you do manually download and install SRU, VDB, and GeoDB updates, make sure you download the correct package for your current version.</p> <p>Signed update files begin with 'Cisco' instead of 'Sourcefire,' and terminate in .sh.REL.tar instead of .sh, as follows:</p> <ul style="list-style-type: none"> • SRU: Cisco_Firepower_SRU-<i>date-build-vrt</i>.sh.REL.tar • VDB: Cisco_VDB_Fingerprint_Database-4.5.0-<i>version</i>.sh.REL.tar • GeoDB: Cisco_GEODB_Update-<i>date-build</i>.sh.REL.tar <p>We will provide both signed and unsigned updates until the end-of-support for versions that require unsigned updates. Do not untar signed (.tar) packages. If you accidentally upload a signed update to an older FMC or ASA FirePOWER device, you must manually delete it. Leaving the package takes up disk space, and also may cause issues with future upgrades.</p>

Table 34: Version 6.2.3 Features

Feature	Description
Product Upgrades	

Feature	Description
<p>Copy upgrade packages to managed devices before the upgrade.</p>	<p>You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window.</p> <p>When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first, then to the standby/data/secondary.</p> <p>New/modified screens: System (⚙️) > Updates</p>
<p>Content Updates</p>	
<p>FMC warns of Snort restart before VDB updates.</p>	<p>The FMC now warns you that Vulnerability Database (VDB) updates restart the Snort process. This interrupts traffic inspection and, depending on how the managed device handles traffic, possibly interrupts traffic flow. You can cancel the install until a more convenient time, such as during a maintenance window.</p> <p>These warnings can appear:</p> <ul style="list-style-type: none"> • 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.