

Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 10.x

First Published: 2025-12-03

Last Modified: 2026-09-03

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2025–2026 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Planning Your Upgrade** 1

- Is This Guide for You? 1
- Compatibility 1
- Upgrade Guidelines 2
  - Software Upgrade Guidelines 2
  - Upgrade Guidelines for the Firepower 4100/9300 Chassis 2
  - Upgrade Guidelines for Firewall Threat Defense Virtual 2
- Upgrade Path 3
  - Choosing your upgrade target 3
  - Supported upgrades and downgrades 3
- Upgrade Order 5
- Upgrade Packages 7
  - Managing upgrade packages with the Firewall Management Center 7
  - Copying Upgrade Packages to Devices 9
    - Copying Upgrade Packages to Devices from an Internal Server 10
  - Deleting Chassis Upgrade Packages from the Secure Firewall 3100/4200 10
  - Manually Downloading Upgrade Packages 11
  - Internet Access Requirements 13
  - Troubleshooting upgrade packages 15
- Upgrade Readiness 16
  - Network and Infrastructure Checks 16
  - Configuration and Deployment Checks 17
  - Backups 18

CHAPTER 2 **Upgrade Firewall Management Center** 21

- Upgrade the Firewall Management Center: Standalone 21

Upgrade the Firewall Management Center: High Availability 23
Unresponsive and Failed Firewall Management Center Upgrades 25

CHAPTER 3 **Upgrade Firewall Threat Defense 27**
Upgrade Firewall Threat Defense 27
Upgrade Firewall Threat Defense in Unattended Mode 30
Monitor Firewall Threat Defense Upgrades 32
Upgrade Options for Firewall Threat Defense 32
Troubleshooting Firewall Threat Defense Upgrade 34
Unresponsive and Failed Firewall Threat Defense Upgrades 35

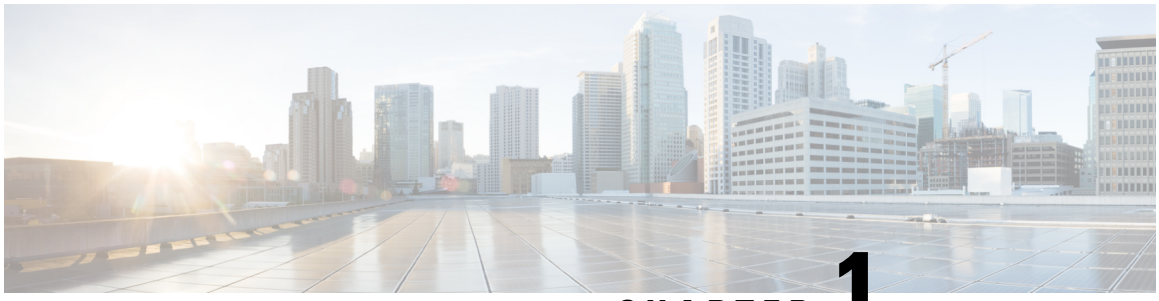
CHAPTER 4 **Upgrade Chassis for Firewall Threat Defense 3100, 4100, 4200, 9300 39**
Upgrade the Secure Firewall 3100/4200 Chassis 39
Upgrade FXOS on the Firepower 4100/9300 with Firewall Chassis Manager 42
Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using Firepower Chassis Manager 42
Upgrade FXOS on an FTD Inter-chassis Cluster Using Firepower Chassis Manager 43
Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager 46
Upgrade FXOS on the Firepower 4100/9300 with the CLI 49
Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using the FXOS CLI 49
Upgrade FXOS on an FTD Inter-chassis Cluster Using the FXOS CLI 52
Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI 55
Upgrade Firmware on the Firepower 4100/9300 59

CHAPTER 5 **Revert or Uninstall 61**
Revert vs Uninstall 61
Revert Firewall Threat Defense Upgrades 62
Revert Guidelines 62
Scenarios Preventing Revert 63
Reverted Configurations 64
Revert a Firewall Threat Defense Upgrade 65
Uninstall Firewall Threat Defense and Firewall Management Center Patches 66
Uninstall Guidelines 66

Uninstall a Firewall Threat Defense Patch 68
Uninstall a Firewall Management Center Patch: Standalone 70
Uninstall a Firewall Management Center Patch: High Availability 71

CHAPTER 6 **Reference** 73

Traffic Flow and Inspection 73
Traffic Flow and Inspection for Firewall Threat Defense Upgrades 73
Traffic Flow and Inspection for Chassis Upgrades 75
Traffic Flow and Inspection when Deploying Configurations 75
Time and Disk Space 76
Upgrade Feature History 77



CHAPTER 1

Planning Your Upgrade

Use this guide to plan and complete Firewall Threat Defense and Firewall Management Center upgrades. Upgrades can be minor (A.x), maintenance (A.x.y), or vulnerability (A.x.y.z) releases. We also may provide hotfixes, which are minor updates that address particular, urgent issues.

Note Version 10 begins a new release numbering scheme and cadence. For more information, see the *Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin*.

- Is This Guide for You?, on page 1
- Compatibility, on page 1
- Upgrade Guidelines, on page 2
- Upgrade Path, on page 3
- Upgrade Order, on page 5
- Upgrade Packages, on page 7
- Upgrade Readiness, on page 16

Is This Guide for You?

The procedures in this guide are for:

- Upgrading a Firewall Management Center that is *currently running* Version 10.
- Upgrading an older Firewall Threat Defense device using a Version 10 Firewall Management Center.

This means that after you use this guide to upgrade the Firewall Management Center, you will use a *different guide* to upgrade Firewall Threat Defense.

Compatibility

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

For compatibility, see:

- *Cisco Secure Firewall Management Center Compatibility Guide*
- *Cisco Secure Firewall Threat Defense Compatibility Guide*

Upgrade Guidelines

In addition to the guidelines and resource links in the following topics, see Reference, on page 73 for general information on time and disk space requirements, and for details on system behavior during upgrade, which can include interruptions to traffic flow and inspection.

Software Upgrade Guidelines

For release-specific upgrade warnings and guidelines for Firewall Management Center and Firewall Threat Defense, and for information on features and bugs with upgrade impact, check all release notes between your current and target version: http://www.cisco.com/go/ftd-notes.

Upgrade Guidelines for the Firepower 4100/9300 Chassis

In most cases, we recommend you use the latest build for your FXOS major version.

For release-specific FXOS upgrade warnings and guidelines, as well as features and bugs with upgrade impact, check all release notes between your current and target version: http://www.cisco.com/go/firepower9300-rns.

For firmware upgrade guidelines (for upgrades to FXOS 2.13 and earlier), see the firmware upgrade guide: *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.

Upgrade Guidelines for Firewall Threat Defense Virtual

Upgrade does not change the serial number or UUID of Firewall Threat Defense Virtual instances.

Update base image and template image ID before cluster upgrade

Before you upgrade a cluster in the public cloud, copy the target version image to your cloud image repository and update the image ID in the cluster deployment template (we actually recommend replacing the existing template with a modified copy). This ensures that after the upgrade, new instances — for example, instances launched during cluster scaling — will use the correct version. If the marketplace does not have the image you need, such as when the cluster has been patched, create a custom image from a snapshot of a standalone Firewall Threat Defense Virtual instance running the correct version, with no instance-specific (day 0) configurations.

Suspend health checks before autoscaled cluster upgrade

For Firewall Threat Defense Virtual for AWS, suspend the HealthCheck and ReplaceUnhealthy processes before autoscaled cluster upgrade. This ensures that instances are not terminated by the Auto Scaling group during the post-upgrade reboot. You can resume the suspended processes afterwards. For instructions, see the Amazon EC2 Auto Scaling user guide: Suspend and resume Amazon EC2 Auto Scaling processes.

Upgrade Path

Planning your upgrade path and order is especially important for large deployments, high availability/clustering, multi-hop upgrades, and situations where you need to coordinate chassis, hosting environment, or other upgrades.

Choosing your upgrade target

Go **directly to the latest Version 10 release possible** to minimize upgrade and other impact. This is because features, enhancements, and critical fixes can skip "future" releases that are ahead by version, but not by release date. For example, if you are up-to-date within major Version A, upgrading to dot-zero Version B can deprecate features and fixes.

If you cannot go to the latest release, at least make sure your current version was released on a date before your target version; see the Release Notes for Secure Firewall Threat Defense for your target version.

Upgrading a patched deployment

Critical fixes in patches/vulnerability (fourth-digit) releases can also skip future releases. If you depend on these critical fixes, verify that your target version contains them. For a full list of release dates, see *Cisco Secure Firewall Management Center New Features by Release*.

Supported upgrades and downgrades

This section summarizes upgrade and downgrade capability.

Supported upgrades

This table shows the supported direct upgrades for Firewall Management Center and Firewall Threat Defense software.

Note Patches can change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release. Although a patched device can be managed with an unpatched Firewall Management Center, fully patched deployments undergo enhanced testing.

Table 1: Supported direct upgrades

Current version	Target software version							
	to 10.x	7.7	7.6	7.4	7.3	7.2	7.1	7.0
from 10.x	YES	—	—	—	—	—	—	—
from 7.7	YES	YES	—	—	—	—	—	—
from 7.6	YES	YES	YES	—	—	—	—	—

Current version	Target software version							
	to 10.x	7.7	7.6	7.4	7.3	7.2	7.1	7.0
from 7.4	YES	YES	YES	YES	—	—	—	—
from 7.3	YES	YES	YES	YES	YES	—	—	—
from 7.2	—	YES	YES	YES	YES	YES	—	—
from 7.1	—	—	YES	YES	YES	YES	YES	—
from 7.0	—	—	—	YES	YES	YES	YES	YES
from 6.4	—	—	—	—	—	—	—	YES

Supported FXOS versions for Firepower 4100/9300 upgrades

For the Firepower 4100/9300, this table lists companion FXOS versions. If a chassis upgrade is required, Firewall Threat Defense upgrade is blocked. In most cases we recommend the latest build in each version; for minimum builds see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Table 2: Supported FXOS versions for Firepower 4100/9300 upgrades

Target Firewall Threat Defense version	Minimum FXOS version
10.x	2.18.0
7.7	2.17.0
7.6	2.16.0
7.4.1–7.4.x	2.14.1
7.4.0	—
7.3	2.13.0
7.2	2.12.0
7.1	2.11.1
7.0	2.10.1
6.7	2.9.1
6.6	2.8.1
6.4	2.6.1

Supported downgrades

If an upgrade succeeds but the system does not function to your expectations, you may be able to return to a previous version; see Revert or Uninstall, on page 61.

Upgrade Order

Firewall Management Center Before Devices

The Firewall Management Center should run the same or newer version as its devices. This is because features and resolved issues often require the latest version on both the Firewall Management Center and its devices, including patches.

Upgrade the Firewall Management Center first—you will still be able to manage older devices, usually a few major versions back. If you begin with devices running a much older version than the Firewall Management Center, further Firewall Management Center upgrades can be blocked. In this case perform a three (or more) step upgrade: devices first, then the Firewall Management Center, then devices again.



Note You cannot upgrade a device past the Firewall Management Center to a newer major or maintenance version. Although a patched device (fourth-digit) can be managed with an unpatched Firewall Management Center, fully patched deployments undergo enhanced testing.

Chassis Before Firewall Threat Defense

Some devices may require a chassis upgrade (FXOS and firmware) before you upgrade the software:

- Secure Firewall 3100/4200 in multi-instance mode: Any upgrade can require a chassis upgrade.

  Although you upgrade the chassis and Firewall Threat Defense separately, one package contains the chassis and Firewall Threat Defense upgrades and you perform both from the Firewall Management Center. The compatibility work is done for you. It is possible to have a chassis-only upgrade or a Firewall Threat Defense-only upgrade.

- Firepower 4100/9300: Major versions require a chassis upgrade.

Because you upgrade the chassis first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of Firewall Threat Defense. If the chassis is already well ahead of its devices, further chassis upgrades can be blocked. In this case perform a three (or more) step upgrade: devices first, then the chassis, then devices again. Or, perform a full reimage. In high availability or clustered deployments, upgrade one chassis at a time.

Chassis with High Availability/Clustered Firewall Threat Defense

When a chassis upgrade is required in high availability or clustered deployments, upgrade one chassis at a time. For high availability, although it is best practice to always upgrade the standby, a chassis could have both standby and active instances (belonging to different high availabilty pairs). In that case, any active units on the upgrading chassis automatically fail over. For clustering, the same applies: it is always best to upgrade an all-data unit chassis.

Before upgrade, high availability pairs and clusters should be in sync, not split brain, and so on. Firewall Threat Defense upgrades will not proceed for most issues of this type, but the chassis is not aware of the status of its instances. This means that even if you upgrade the chassis one at a time, you can still experience disruption if you do not make sure your deployment is healthy before each chassis upgrade.

Table 3: Chassis Upgrade Order for the Firepower 4100/9300

Firewall Threat Defense Deployment	Upgrade Order
Standalone	**1.** Upgrade chassis. **2.** Upgrade Firewall Threat Defense.
High availability	Upgrade both chassis before you upgrade Firewall Threat Defense. To minimize disruption, always upgrade the standby. **1.** Upgrade chassis with the standby. **2.** Switch roles. **3.** Upgrade chassis with the new standby. **4.** Upgrade Firewall Threat Defense.
Intra-chassis cluster (units on the same chassis)	**1.** Upgrade chassis. **2.** Upgrade Firewall Threat Defense.
Inter-chassis cluster (units on different chassis)	Upgrade all chassis before you upgrade Firewall Threat Defense. To minimize disruption, always upgrade an all-data unit chassis. **1.** Upgrade the all-data unit chassis. **2.** Switch the control module to the chassis you just upgraded. **3.** Upgrade all remaining chassis. **4.** Upgrade Firewall Threat Defense.

Table 4: Chassis Upgrade Order for the Secure Firewall 3100/4200 in Multi-Instance Mode

Firewall Threat Defense Deployment	Upgrade Order
Standalone	**1.** Upgrade chassis. **2.** Upgrade Firewall Threat Defense.

Firewall Threat Defense Deployment	Upgrade Order
High availability	Upgrade both chassis before you upgrade Firewall Threat Defense. **1.** Upgrade chassis. With the chassis upgrade wizard, you have three options: • Two workflows (run the upgrade wizard twice) Best practice. Upgrade the chassis with the standby, switch roles, verify health, and upgrade the chassis with the new standby. This has the least risk of disruption. • Serial upgrade Recommended with reservations. Automatically fail over when the active unit goes down. If you use serial upgrade, place the standby unit first in the upgrade order. This avoids the total disruption of a parallel upgrade, but can still cause issues if the second chassis starts upgrading *after* the first chassis comes back up, but *before* high availability can resync. • Parallel upgrade Not recommended for high availability. **2.** Upgrade Firewall Threat Defense.

Upgrade Packages

To upgrade, the upgrade package must be on the Firewall Management Center or managed device.

The Firewall Management Center can get upgrade packages from the internet before or during upgrade, or you can upload packages you manually downloaded. Managed devices can get upgrade packages from the internet, the Firewall Management Center, or an internal server.

Especially for deployments without reliable, fast internet access, use these sections to plan how you will get upgrade packages where they need to be.

Managing upgrade packages with the Firewall Management Center

If the Firewall Management Center can reach the internet, **Administration** > **Upgrades & updates** > **Product Upgrades** lists all upgrades that apply to you, with suggested releases specially marked. You can easily choose and direct-download packages from the internet to the Firewall Management Center, or upload packages you manually downloaded. For details, see the following table. For answers to common issues, see Troubleshooting upgrade packages, on page 15.



Note Devices with internet access can be upgraded without the package on the Firewall Management Center. The device will get the package at the appropriate time; see Copying Upgrade Packages to Devices, on page 9.

Table 5: Managing upgrade packages with the Firewall Management Center

To...	Do This...
Refresh the list of available upgrades.	Click **Refresh** ( ) at the bottom left of the page.
Download an upgrade package to the Firewall Management Center from the internet.	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 Firewall Management Center.	Click **Add upgrade package** at the bottom right of the page, then **Choose file**. If you are uploading a Firewall Management Center upgrade package in a high availability deployment, the option to **Copy to peer Firewall Management Center** is enabled by default. See: Manually Downloading Upgrade Packages, on page 11
Configure 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: Copying Upgrade Packages to Devices from an Internal Server, on page 10
Force devices to get upgrade packages from the Firewall Management Center instead of the internet.	Click **Global upgrade settings**, then disable the option to **Allow devices to download from the support site**. By default, a device with internet access downloads upgrade packages from the internet before the Firewall Management Center, including as fallback when download from an internal server fails. See: Copying Upgrade Packages to Devices, on page 9
Configure the retry length for partial downloads.	Click **Global upgrade settings**, then choose an option from the **Retry failed downloads for** drop-down list. Partial downloads from the internet (Firewall Management Center and device) or internal server (device only) are saved and retried for the interval you specify. The default is 24 hours. This setting does not apply to device downloads from the Firewall Management Center over the management network. For device downloads, retry requires at least Version 7.4.3, 7.6.1, or 7.7.0.
Delete upgrade packages from the Firewall Management Center.	Click the **Ellipsis (…)** next to the package or package version you want to delete and select **Delete**. This deletes the packages (or the pointer to the package) from the Firewall Management Center. It does not delete packages from any devices where you already copied them. For Firewall Management Center in high availability, it does not delete the package from the peer. In most cases, upgrading removes the related package from the upgraded appliance. However, for the Secure Firewall 3100/4200 in multi-instance mode, chassis upgrade packages must be removed manually. See Deleting Chassis Upgrade Packages from the Secure Firewall 3100/4200, on page 10.

Copying Upgrade Packages to Devices

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

Copying Firewall Threat Defense Upgrade Packages

After you select devices to upgrade, the upgrade wizard prompts you to copy upgrade packages. Devices try the following sources in order. If one fails, in most cases the device tries the next one.

Internal server.

When configured, this takes priority. Recommended when it is not possible or practical to get the upgrade package from the internet or Firewall Management Center, for example, if devices do not have internet access, there is not enough disk space on the Firewall Management Center, or there is poor bandwidth between devices and the download location.

If download from the internal server fails, newer devices (Firewall Threat Defense 7.6+ or chassis 7.4.1+) with internet access try that next. Older devices and devices without internet access try the Firewall Management Center.

See: Copying Upgrade Packages to Devices from an Internal Server, on page 10

Internet. Recommended in most cases.

Recommended when devices have internet access, with good bandwidth between devices and the download location. Internet access is tested weekly. Not supported for hotfixes.

By default, a device with internet access tries the internet before the Firewall Management Center, but if devices have slow or unreliable internet access you can use the **Global upgrade settings** to force devices to get upgrade packages from the Firewall Management Center. If internet download fails, the device tries the Firewall Management Center.

See: Internet Access Requirements, on page 13 and Managing upgrade packages with the Firewall Management Center, on page 7

Firewall Management Center.

Recommended when devices cannot reach the internet or have slow or unreliable internet access, but there is enough disk space on the Firewall Management Center, and there is good bandwidth between the Firewall Management Center and devices. You can also keep device upgrade packages on the Firewall Management Center as a fallback in case internal server or direct download fails.

The Firewall Management Center can get most device upgrade packages directly from the internet. If the Firewall Management Center cannot reach the internet, or you are applying a hotfix, manually upload upgrade packages.

See: Managing upgrade packages with the Firewall Management Center, on page 7

Copying Chassis Upgrade Packages

For the Secure Firewall 3100/4200 in multi-instance mode, use the Firewall Threat Defense methods above. Note that these chassis upgrade packages are stored outside any application instances. This allows you to upgrade the chassis while also making the Firewall 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).

For Firepower 4100/9300 chassis upgrade packages, manually download the upgrade package from the Cisco Support & Download site, then use the Firewall Chassis Manager or CLI (FTP, SCP, SFTP, or TFTP) to copy

the package to the device. See Manually Downloading Upgrade Packages, on page 11 and the upgrade procedure for your deployment.

Copying Upgrade Packages to Devices from an Internal Server

Managed devices without internet access must get upgrade packages from either the Firewall Management Center or an internal server. An internal server is especially useful if you have limited bandwidth between the Firewall Management Center and its devices (or, between the devices and the internet download location). It also saves space on the Firewall Management Center.

After you get upgrade packages (Manually Downloading Upgrade Packages, on page 11) and set up your server, configure pointers. On the Firewall Management Center, start like you are uploading a package: on the Product Upgrades page (**Administration** > **Upgrades & updates** > **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.

Note When configured, an internal server takes priority. If copying from the internal server fails, newer devices (Firewall Threat Defense 7.6+ or chassis 7.4.1+) with internet access try the internet, then the Firewall Management Center, unless you disabled support-site downloads in the global upgrade settings. Older devices and devices without internet access just try the Firewall Management Center.

Table 6: Options for Copying Firewall Threat Defense Upgrade Packages from an Internal Server

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

Deleting Chassis Upgrade Packages from the Secure Firewall 3100/4200

For the Secure Firewall 3100/4200 in multi-instance mode, chassis upgrade packages are stored outside any application instances. This allows you to upgrade the chassis while also making the Firewall 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.

Procedure

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. The **Details** column indicates which chassis have packages that might not be needed.

Step 4 Use the **Warning** filter to display the affected chassis.

Step 5 In the filtered view, click **View and clean up packages** next to a chassis, select the packages you want to remove, and click **Delete selected packages**. Repeat this step for each chassis you want to clean up.

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 6 Back in the chassis upgrade wizard, click **Reset** to reset the workflow.

Manually Downloading Upgrade Packages

Manually download upgrade packages when the system cannot reach the internet, or when you cannot or do not want to direct-download for another reason; for example, for hotfixes, Firepower 4100/9300 chassis upgrades, or if you use an internal server.

Packages are available on the Cisco Support & Download site:

- Firewall Management Center: https://www.cisco.com/go/firepower-software
- Firewall Threat Defense: https://www.cisco.com/go/ftd-software

Software Packages

You use the same upgrade package for all models in a family or series. To find the correct one, select or search for your model, 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, software version, and build. Upgrade packages are signed, and terminate in .sh.REL.tar. Do not untar or rename them.

Note that a newer Firewall Management Center can manage older devices (and apply maintenance releases and patches to them). For older devices not listed here, see the Firewall Management Center upgrade guide corresponding to the last supported device version.

Table 7: Upgrade Packages

Platform	Package
Firewall Management Center Packages	
Firewall Management Center hardware Firewall Management Center Virtual	Cisco_Secure_FW_Mgmt_Center_Upgrade-*Version-build*.sh.REL.tar
Firewall Threat Defense Packages	
Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-*Version-build*.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-*Version-build*.sh.REL.tar
Secure Firewall 200	Cisco_Secure_FW_TD_200-*Version-build*.sh.REL.tar
Secure Firewall 1200	Cisco_Secure_FW_TD_1200-*Version-build*.sh.REL.tar
Secure Firewall 3100	Cisco_FTD_SSP-FP3K_Upgrade-*Version-build*.sh.REL.tar
Secure Firewall 4200	Cisco_Secure_FW_TD_4200-*Version-build*.sh.REL.tar
Secure Firewall 6100	Cisco_Secure_FW_TD_6100-*Version-build*.sh.REL.tar
ISA 3000 with FTD	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar
Firewall Threat Defense Virtual	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar

Chassis Packages for the Secure Firewall 3100/4200

For the Secure Firewall 3100/4200 in multi-instance mode, the threat defense and chassis upgrades share a package.

Chassis Packages for the Firepower 4100/9300

To find the correct FXOS package, select or search for your device model and browse to the *Firepower Extensible Operating System* download page for your target FXOS version and build. The FXOS package is listed along with recovery and MIB packages. Firmware is included in FXOS upgrades to 2.14.1+.

Table 8: FXOS Packages

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

Internet Access Requirements

By default, the system is configured to connect to the internet on ports 443/tcp (HTTPS) and 80/tcp (HTTP). If you do not want your appliances to have direct access to the internet, you can configure a proxy server.

Upgrade package download location depends on the Firewall Management Center's current version. Note that download *capability* can further depend on release type (major, maintenance, patch, hotfix) and package type (Firewall Management Center, device).

Firewall Threat Defense Download Location

With a Version 7.6.1+ Firewall Management Center, managed devices can get their own upgrade packages from the internet.

Table 9: Where devices get software upgrades

Devices with this Management Center Version	Download From
7.6.1+	https://cdo-ftd-images.s3-us-west-2.amazonaws.com/ The Firewall Management Center must also have access to this resource.
7.6.0 and earlier	Managed devices must get upgrade packages from the Firewall Management Center or an internal server.

Firewall Management Center Download Location

The Firewall Management Center can get upgrade packages from the internet. This includes upgrade packages for devices they manage.

Table 10: Where the Firewall Management Center gets software upgrades

Management Center Version	Downloads From
7.4.1+	https://cdo-ftd-images.s3-us-west-2.amazonaws.com/

Management Center Version	Downloads From
7.4.0 7.3.x	One of: • https://support.sourcefire.com/ For on-demand or scheduled downloads of applicable new releases. Used when you click the **Download Upgrades** button on the top right of > **Updates** > **Product Updates**. This immediately downloads the latest VDB, latest maintenance release, and the latest critical patches for your deployment. Also used by the task scheduler. • http://cdo-ftd-images.s3-us-west-2.amazonaws.com/ For on-demand downloads of specific Firewall Threat Defense upgrade packages. Used when you choose packages to download, then click the **Download Major Upgrades** button on the **Download Updates** sub-tab of > **Updates** > **Product Updates**.
7.2.6 to 7.2.x	https://cdo-ftd-images.s3-us-west-2.amazonaws.com/
7.2.5 and earlier	https://support.sourcefire.com/

High Availability and Clustering Considerations

If not all appliances in your deployment have internet access, use the following table to determine what to do.

Table 11: High Availability/Clustering Considerations for Downloading Software Upgrades

Package Type	Management Center Version	Considerations
Firewall Management Center upgrade	7.6.0+	Downloading the package on one HA Firewall Management Center attempts the download on both. If only one peer has internet access, you can sync the package during the upgrade process.
	7.4.1 to 7.4.x 7.2.6 to 7.2.x	Packages do not sync. For each HA Firewall Management Center with internet access, you can direct-download any applicable package.
	7.4.0 7.3.x 7.2.5 and earlier	Packages do not sync. For each HA Firewall Management Center with internet access, you can direct-download the latest maintenance release and critical patches. You must manually upload all other packages.

Package Type	Management Center Version	Considerations
Firewall Threat Defense upgrade	Any	Firewall Threat Defense upgrade packages do not sync between HA Firewall Management Centers, nor between high availability and clustered devices. Each device or unit must get its own upgrade package from the internet (with Firewall Management Center 7.6.1+), the active Firewall Management Center, or an internal server.

Troubleshooting upgrade packages

Table 12: Troubleshooting upgrade packages

Issue	Solution
No available upgrades even after I refresh.	Direct-downloading upgrade packages to the Firewall Management Center requires internet access. You will also see a blank list if you are already running the latest version available for your deployment *and* you have no upgrade packages loaded/configured.
Suggested release is not marked.	The suggested release is listed only if you are eligible for it. It is not listed if you are already running the suggested release or higher, or if you cannot upgrade that far. Note that patches to suggested releases are not marked as suggested, although we do recommend you apply them.
I don't see the packages I want.	Only major, maintenance, and patch upgrades that apply to your deployment *right now* are listed and available for direct download. These are not listed unless manually uploaded: • Device upgrades (major and maintenance) to a particular version, unless the Firewall Management Center is running that version or higher, *and* you have a device that supports that version. • Device patches, unless you have at least one device at the appropriate maintenance release. • Firewall Management Center patches, unless you are running the appropriate maintenance release. • Hotfixes. You must manually upload these.
A package was deleted from the page when I upgraded the Firewall Management Center.	When the Firewall Management Center is upgraded, some locally saved upgrade packages may be deleted, including device upgrade packages for versions that can no longer be managed.
I see available, undownloaded packages that don't apply to my devices.	The system lists the downloadable upgrades that apply to *all* devices managed by this Firewall Management Center. In a multidomain deployment, this can include devices that you cannot access right now.
I downloaded a Firewall Management Center upgrade package from the internet, but the download to its high availability peer failed.	If the peer Firewall Management Center does not have internet access or the download fails for any other reason, you can: • Start the upgrade anyway. The upgrade wizard has options to retry the download, or sync the file between the peers. • Log into the peer and manually upload the upgrade package.

Issue	Solution
I uploaded a Firewall Management Center upgrade package, but the sync to its high availability peer failed.	If the upgrade package sync fails for any reason, you can: • Start the upgrade anyway. The upgrade wizard has options to attempt a download from the internet, or retry the sync. • Log into the peer and manually upload the upgrade package.
Copying upgrade packages from the Firewall Management Center to devices times out.	This often happens when there is limited bandwidth between the Firewall Management Center and its devices. You can try one of: • Configure devices to get upgrade packages directly from an internal web server. To do this, delete the upgrade package from the Firewall 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 Copying Upgrade Packages to Devices from an Internal Server, on page 10. • Allow devices to download the upgrade package from the internet. Devices with internet access automatically try that first, and only fall back on the Firewall Management Center if internet download fails. See Internet Access Requirements, on page 13.

Upgrade Readiness

After you check compatibility, plan your upgrade path and order, and review upgrade guidelines, you need to assess upgrade readiness. The system does some of these checks for you, but you still need to perform additional checks (and actions) yourself, like deploying configuration changes and making backups.

Use the following sections to perform last minute-tasks and confirm upgrade readiness.

Network and Infrastructure Checks

Appliance Access

Devices can stop passing traffic during the upgrade or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. You should also able to access the Firewall 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 any required pre-upgrade configuration changes, and prepare to make required post-upgrade configuration changes. Resolve any change management workflows.

The following table indicates when you have to deploy to managed devices. Deploying typically restarts Snort, which can affect traffic flow and inspection; see Traffic Flow and Inspection when Deploying Configurations, on page 75.

Table 13: When to Deploy

Platform	Deploy Before Upgrade	Deploy After Upgrade
Firewall Management Center	No.	Sometimes. If redeploy is required, affected devices are marked out of date. Note that devices may not be marked out of date if you schedule intrusion rule updates; in that case the redeploy will take place on schedule. Additionally, you must deploy at least once between Firewall Management Center and device upgrade, even if devices are not marked out of date.
Firewall Threat Defense	Yes.	Yes.

Deployment Health

Make sure your deployment is healthy and successfully communicating. If there are any issues reported by the health monitor or on the Device Management page, resolve them before continuing.

Some failed health tests can prevent you from upgrading or cause upgrade failure. With the exception of NTP issues that you can resolve yourself, contact Cisco TAC if your deployment is failing any of the following tests. Results are reported on the Health Status (Home) page of the health monitor: **Troubleshooting** > **Health** > **Monitor**.

Note Disabling these regular health tests does not prevent the system from enforcing them before upgrade. If there are no existing results, readiness checks will run as part of the upgrade, increasing upgrade time.

Table 14: Upgrade-Related Health Tests

Health Test	Description
Database	Monitors database schema and configuration data (*EO*) integrity.
Disk Status	Monitors disk and RAID controller health for hardware devices.

Health Test	Description
Disk Usage	Monitors disk usage. The upgrade calculates how much disk space it needs; not having enough will prevent upgrade. If this module is alerting before you begin upgrade, you probably do not have enough. On health dashboards, the Disk Usage widget has a **Clear disk space** button that safely removes unneeded files such as old backups, content updates, and troubleshooting files.
Firewall Threat Defense HA (Firewall Management Center and devices) Cluster/HA Failure Status (devices)	High availability pairs and clusters should be in sync, not split brain, and so on. Firewall Threat Defense upgrades will not proceed for most issues of this type. However, for the Firepower 4100/9300 and Secure Firewall 3100/4200 in multi-instance mode, the chassis is not aware of the status of its instances. This means that even if you upgrade the chassis one at a time, you can still experience disruption if you do not make sure your deployment is healthy before each chassis upgrade.
FXOS Health	Monitors the FXOS httpd service on FXOS-based devices. Upgrade will fail without this service running.
Time Server Status (Firewall Management Center) Time Synchronization Status (devices)	Monitors NTP synchronization. Being out of sync can cause upgrade failure. The system only alerts when you are offset by more than 10 seconds, so we recommend you manually check for a smaller offset (click **see more** next to the test results).

Running Tasks and Scheduled Tasks

Make sure essential tasks are complete. Tasks running when the upgrade begins are stopped and cannot be resumed; they become failed tasks.

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.

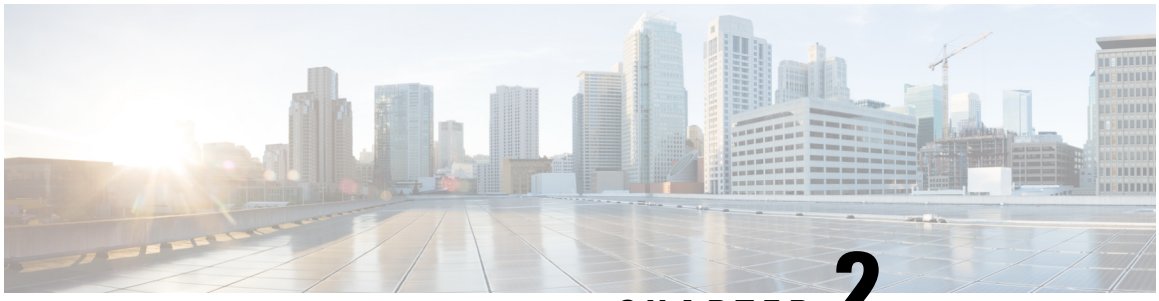
Backups

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 Firewall Management Center after you upgrade its managed devices, so your new Firewall Management Center backup file 'knows' that its devices have been upgraded.

Table 15: Backups

Backup	Guide
Firewall Management Center	*Cisco Secure Firewall Management Center Administration Guide*: *Backup/Restore* We recommend you back up configurations and events.
Firewall Threat Defense	*Cisco Secure Firewall Management Center Administration Guide*: *Backup/Restore* Note that backup is not supported in all cases, for example, for Firewall Threat Defense Virtual in the public cloud. But if you can back up, you should.
Secure Firewall 3100/4200 chassis	*Cisco Secure Firewall Management Center Device Configuration Guide*: *Multi-Instance Mode for the Secure Firewall 3100/4200*
Firepower 4100/9300 chassis	Cisco Firepower 4100/9300 FXOS Configuration Guide: *Configuration Import/Export*
ASA on a Firepower 9300 chassis	Cisco ASA Series General Operations Configuration Guide: *Software and Configurations* For a Firepower 9300 chassis with Firewall 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.



CHAPTER 2

Upgrade Firewall Management Center

The procedures in this guide are for upgrading a Firewall Management Center that is *currently running* Version 10. If you are upgrading *to* Version 10, see the upgrade guide for the version you are running now.

- Upgrade the Firewall Management Center: Standalone, on page 21
- Upgrade the Firewall Management Center: High Availability, on page 23
- Unresponsive and Failed Firewall Management Center Upgrades, on page 25

Upgrade the Firewall Management Center: Standalone

Use this procedure to upgrade a standalone Firewall Management Center. As you proceed, the system displays basic information about the upgrade, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade.

Upgrade does not start until you complete the upgrade wizard and click **Upgrade**. All steps up to that point can be performed outside of a maintenance window, including checking readiness, copying upgrade packages, and choosing upgrade options. For information on traffic handling during the first post-upgrade deploy (which typically restarts Snort), see Traffic Flow and Inspection when Deploying Configurations, on page 75.



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

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility, on page 1
- Plan your upgrade path: Upgrade Path, on page 3
- Review upgrade guidelines: Upgrade Guidelines, on page 2
- Check infrastructure and network: Network and Infrastructure Checks, on page 16
- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks, on page 17

- Perform backups: Backups, on page 18

Procedure

Step 1 Choose **Administration** > **Upgrades & updates** > **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 Managing upgrade packages with the Firewall Management Center, on page 7 and Troubleshooting upgrade packages, on page 15.

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 Firewall Management Center upgrade wizard appears. Prechecks are automatic. We also recommend revisiting the configuration and deployment health checks you performed earlier: Configuration and Deployment Checks, on page 17.

Step 4 Click **Upgrade**, then confirm that you want to upgrade and reboot.

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

Step 5 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 and post-reboot initialization, log back in again.
- Patches and hotfixes: You can log in after the upgrade, reboot, and post-reboot initialization are completed.

Step 6 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 7 Update intrusion rules and the vulnerability database.

Although the upgrade often updates these components, there could be newer ones available. If the Cisco Support & Download site has a newer version, install it. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Note
The system updates intrusion rules for Snort 2 devices (SRU) after the upgrade completes and the management center reboots. While this is happening, you cannot update intrusion rules, add devices, or deploy configuration changes. This occurs regardless of whether you are managing any Snort 2 devices.

Step 8 Complete any required post-upgrade configuration changes.

Step 9 Redeploy configurations to out-of-date devices.

If redeploy is required, affected devices are marked out of date.

Note that devices may not be marked out of date if you schedule intrusion rule updates; in that case the redeploy will take place on schedule. Additionally, you cannot upgrade managed devices until you redeploy, even if they are not marked out of date.

Upgrade the Firewall Management Center: High Availability

Use this procedure to upgrade high availability Firewall Management Centers. As you proceed, the system displays basic information about the upgrade, as well as the current upgrade-related status.

First, upgrade the standby. When it comes back up, upgrade the active. Synchronization automatically pauses when you begin and resumes when you are done, with the peers in their original roles. (Exception: some patches and hotfixes do not pause synchronization. And if synchronization does pause, you must manually resume.)



Note Best practice is to avoid making or deploying changes while synchronization is paused, although if done from the active peer while (or after) the standby upgrades, changes will be synchronized later. If you urgently need to make changes or deploy from the standby while the active is upgrading, you can break high availability and use the standby as a standalone Firewall Management Center. You may also be able to switch roles, but this can be blocked depending on upgrade progress on the active. Note that if you switch roles mid-upgrade, when the active comes back up, it will also be active and you will be split-brain, which is not supported for general operations. In either case, you must manually resume high availability, making sure to choose the old standby (the Firewall Management Center where you deployed) as the new active. Otherwise, your changes will be lost.

Upgrade does not start until you complete the upgrade wizard and click **Upgrade**. All steps up to that point can be performed outside of a maintenance window, including checking readiness, copying upgrade packages, and choosing upgrade options. For information on traffic handling during the first post-upgrade deploy (which typically restarts Snort), see Traffic Flow and Inspection when Deploying Configurations, on page 75.



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

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility, on page 1
- Plan your upgrade path: Upgrade Path, on page 3
- Review upgrade guidelines: Upgrade Guidelines, on page 2
- Check infrastructure and network: Network and Infrastructure Checks, on page 16

- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks, on page 17
- Perform backups: Backups, on page 18

Procedure

Prepare to upgrade.

Step 1 On the standby peer, choose **Administration** > **Upgrades & updates** > **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. If the remote peer has internet access the package will download there as well.

For more information, see Managing upgrade packages with the Firewall Management Center, on page 7 and Troubleshooting upgrade packages, on page 15.

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 Firewall Management Center upgrade wizard appears. Prechecks automatically run on both peers. You are also given a chance to fix common upgrade issues, such as:

- If the remote peer does not have the upgrade package yet, you can retry the download or sync the file.
- If you do not have enough disk space to run the upgrade, a **Clean Up Disk Space** option deletes old upgrade, VDB, and SRU/LSP packages, as well as old configuration data and log files.

We also recommend revisiting the configuration and deployment health checks you performed earlier: Configuration and Deployment Checks, on page 17.

Upgrade the standby, then the active.

Step 4 On the standby peer, click **Upgrade**, then confirm that you want to upgrade and reboot.

Synchronization pauses if necessary, and the upgrade begins. You can monitor progress in the Message Center until you are logged out.

Step 5 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 and post-reboot initialization, log back in again.
- Patches and hotfixes: You can log in after the upgrade, reboot, and post-reboot initialization are completed.

Step 6 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 7 Repeat the previous steps on the active peer.

The upgrade package should already be there, and all checks should have passed. You can quickly click through those tasks.

Resume synchronization if necessary, and complete post-upgrade tasks.

Step 8 On the active peer (the one you just upgraded), verify or resume high availability synchronization.

Synchronization should automatically resume after most upgrades. For patches and hotfixes, you must manually resume (unless the system never paused it).

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

Step 9 Update intrusion rules and the vulnerability database.

Although the upgrade often updates these components, there could be newer ones available. If the Cisco Support & Download site has a newer version, install it. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Note
The system updates intrusion rules for Snort 2 devices (SRU) after the upgrade completes and the management center reboots. While this is happening, you cannot update intrusion rules, add devices, or deploy configuration changes. This occurs regardless of whether you are managing any Snort 2 devices.

Step 10 Complete any required post-upgrade configuration changes.

Step 11 Redeploy configurations to out-of-date devices.

If redeploy is required, affected devices are marked out of date.

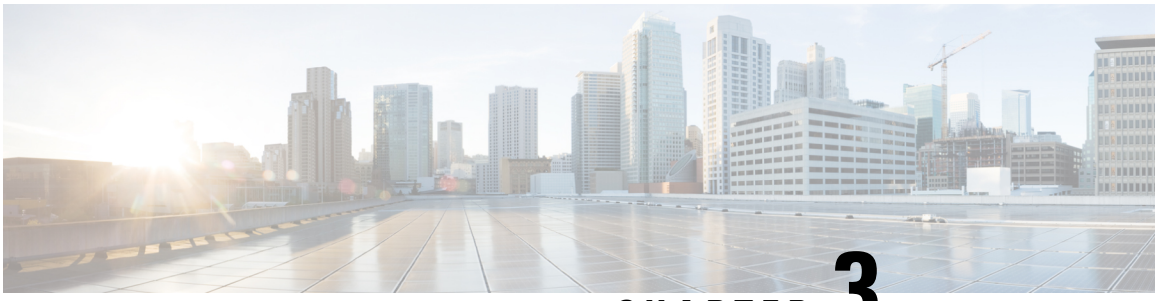
Note that devices may not be marked out of date if you schedule intrusion rule updates; in that case the redeploy will take place on schedule. Additionally, you cannot upgrade managed devices until you redeploy, even if they are not marked out of date.

Unresponsive and Failed Firewall Management Center Upgrades



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.

In high availability deployments, do not make or deploy configuration changes while the pair is split-brain, even if you are not actively upgrading. Your changes will be lost after synchronization restarts; deploying could place the system in an unusable state and require a reimage.



CHAPTER 3

Upgrade Firewall Threat Defense

- Upgrade Firewall Threat Defense, on page 27
- Upgrade Firewall Threat Defense in Unattended Mode, on page 30
- Monitor Firewall Threat Defense Upgrades, on page 32
- Upgrade Options for Firewall Threat Defense, on page 32
- Troubleshooting Firewall Threat Defense Upgrade, on page 34
- Unresponsive and Failed Firewall Threat Defense Upgrades, on page 35

Upgrade Firewall Threat Defense

Use this procedure to upgrade Firewall Threat Defense with the upgrade wizard.

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 you navigate away from the upgrade 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** > **+ Show more** > **Upgrade** > **Threat Defense Upgrade**.

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 checking readiness, copying upgrade packages, and choosing upgrade options.



Caution Do not deploy configuration changes during upgrade. Even if the device appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. Devices may reboot multiple times during the upgrade. This is expected behavior. If you encounter issues with the upgrade, including a failed upgrade or unresponsive device, see Unresponsive and Failed Firewall Threat Defense Upgrades, on page 35.

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility, on page 1
- Plan your upgrade path: Upgrade Path, on page 3

- Review upgrade guidelines: Upgrade Guidelines, on page 2
- Check infrastructure and network: Network and Infrastructure Checks, on page 16
- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks, on page 17
- Perform backups: Backups, on page 18
- Upgrade chassis, if required: Upgrade Chassis for Firewall Threat Defense 3100, 4100, 4200, 9300, on page 39

Procedure

Step 1 On the Firewall Management Center, choose **Administration** > **Upgrades & updates** > **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. If the Firewall Management Center has internet access, it lists upgrades that apply to you, with suggested releases specially marked.

Step 2 (Optional) Get upgrade packages onto the Firewall Management Center, or put them on an internal server.

Skip this step if your devices can get upgrade packages directly from the internet. For other options, see Managing upgrade packages with the Firewall Management Center, on page 7.

Step 3 Launch the upgrade wizard.

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

Note
The upgrade wizard was updated in Version 10.0. If you prefer, click **Switch to legacy wizard**. For information on using the legacy wizard, see Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.7.x.

Step 4 Select devices to upgrade.

To help you select devices to upgrade, the upgrade wizard allows you to search and filter based on various useful criteria. The **Ready to proceed** filter shows all selected devices that are currently eligible for upgrade. Before proceeding with any upgrade step, the **Selected** number should match the **Ready to proceed** number. If they don't match, use the **Not candidates** filter to see why. You don't have to remove ineligible devices, but they are automatically excluded from upgrade. You must upgrade the members of device clusters and high availability pairs together.

Note
After you select devices, you can use unattended mode to automatically prepare for and begin the upgrade. After the upgrade completes, pick up with the verification and post-upgrade tasks. For more information, see Upgrade Firewall Threat Defense in Unattended Mode, on page 30.

Step 5 Click **Prepare for upgrade** to immediately begin copying upgrade packages to devices and checking readiness.

Where upgrade packages come from depends on your deployment and previous configurations. For more information, see Copying Upgrade Packages to Devices, on page 9.

Many readiness checks are based on current device health, but checks on devices currently running Version 7.6.x and earlier may take longer. Passing all checks greatly reduces the chance of upgrade failure. If the checks expose issues

that you cannot resolve, do not begin the upgrade. Disable checks only at the direction of Cisco TAC. For more information, see Configuration and Deployment Checks, on page 17.

Note
This process takes advantage of a prepare-only option for unattended mode. This means that while the wizard copies packages and checks readiness, you may see messages about unattended mode running even if you did not explicitly start it.

Step 6 (Optional) Click **Advanced settings** to choose upgrade options.

For information on why you might disable these options, see Upgrade Options for Firewall Threat Defense, on page 32.

Step 7 Click **Start upgrade** and confirm your choice.

Devices operate in maintenance mode while they upgrade. For information on traffic handling during the upgrade, see Traffic Flow and Inspection, on page 73.

Step 8 Monitor the upgrade.

The wizard shows your overall upgrade progress. For more upgrade monitoring options, including special considerations for monitoring high availability upgrades, see Monitor Firewall Threat Defense Upgrades, on page 32.

Step 9 Verify success.

After the upgrade completes, verify success on **Devices** > **Device Management**.

Step 10 (Optional) In high availability or clustered 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 11 Update intrusion rules and the vulnerability database (VDB).

Choose **Administration** > **Upgrades & updates** > **Content Updates** to verify the currently installed versions and perform any updates.

Although the upgrade often updates these components, there could be newer ones available. If the Cisco Support & Download site has a newer version, install it. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 12 Complete any required post-upgrade configuration changes.

Step 13 Redeploy configurations to the devices you just upgraded.

Snort typically restarts during the first deployment after upgrade. Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability or clustering. For more information, see Traffic Flow and Inspection when Deploying Configurations, on page 75.

Before you deploy, you may want to review the changes made by the upgrade (as well as any changes you have made since upgrade):

- If you have not cleared your workflow, you can return to the wizard. Choose **Devices** > **+ Show more** > **Upgrade** > **Threat Defense Upgrade** and click **Configuration Changes** next to each device.
- If you have cleared the workflow, or if you want to quickly generate change reports for multiple devices, use the Advanced Deploy page. Choose **Deploy** > **Advanced Deploy**, select the devices you upgraded, and click **Pending**

Changes Reports. After the reports finish generating, you can download them 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, the page 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, and the Advanced Deploy screens to see configuration changes.
- For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for each upgraded logical device. You can use the **Logical Devices** tab on the Secure Firewall Chassis Manager or the `set startup-version` FXOS command. This ensures that if you need to restore the logical device from the post-upgrade backup, the backup and startup versions match. For more information, see the *Image Management* chapter in the *Cisco Firepower 4100/9300 FXOS Secure Firewall Chassis Manager Configuration Guide*, or the *Cisco Firepower 4100/9300 FXOS Command Reference*.
- Back up again: Backups, on page 18

Upgrade Firewall Threat Defense in Unattended Mode

The Firewall Threat Defense upgrade wizard has an optional *unattended mode*. Start the wizard, select the target version and the devices you want to upgrade, choose upgrade options, and step away. You can even log out or close the browser. The system automatically copies upgrade packages to devices, checks readiness, and, if specified, begins the upgrade. After the upgrade completes, pick up with the verification and post-upgrade tasks.

Note During a regular (attended) upgrade, after you click **Prepare for upgrade**, you may see messages about unattended mode. This is because the wizard uses the unattended mode prepare-only capability to copy packages and check readiness.

Table 16: Upgrade Firewall Threat Defense in Unattended Mode

To...	Do this in the wizard...
Start an unattended upgrade.	Choose **Unattended mode** > **Start** after selecting the target version and the devices you want to upgrade. For unattended mode options, see the next table.

To...	Do this in the wizard...
Pause an unattended upgrade during copy and checks phases.	Choose **Unattended mode** > **Stop**. You can pause and restart unattended mode during the copy and checks phases. However, pausing unattended mode does *not* stop tasks in progress. Copies and checks that have started will run to completion. Note that you must pause unattended mode to perform any manual upgrade actions. Once the actual device upgrade begins, you cannot cancel it by stopping unattended mode. Instead, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page.
Monitor an unattended upgrade during copy and checks phases.	Choose **Unattended mode** > **View status**. Once the actual device upgrade begins, see Monitor Firewall Threat Defense Upgrades, on page 32

Unattended Mode Options

These options apply to unattended upgrades and are disabled by default.

Table 17: Unattended Mode Options

Option	When to Enable	Details
Start upgrade after device preparation completes.	If you don't need to carefully time the upgrade.	Starting the upgrade requires a maintenance window, but staging does not. The system will copy upgrade packages to devices and check readiness, but will not perform the actual upgrade. Note that running an unattended upgrade with this option disabled does the same thing as clicking **Prepare for Upgrade** in the main upgrade wizard. This is why you may see messages about unattended mode even if you did not explicitly start it.
Re-run readiness checks for devices that already passed.	If you are unsure about device readiness.	We recommend re-running checks for devices that passed more than 24 hours ago, or if you made changes after a device last passed. You may have recently run readiness checks on some devices and don't need to run them again.
Require all devices to be eligible to advance.	If you have an "all or none" upgrade requirement.	Enforces an "all or none" requirement for unattended upgrades. If a selected device cannot upgrade for any reason, no devices upgrade. For example, if one device cannot get the upgrade package or pass required checks, the entire process stops. Disable this option to let eligible devices proceed independently.

Monitor Firewall Threat Defense Upgrades

Caution Do not deploy configuration changes during upgrade. Even if the device appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. Devices may reboot multiple times during the upgrade. This is expected behavior. If you encounter issues with the upgrade, including a failed upgrade or unresponsive device, see Unresponsive and Failed Firewall Threat Defense Upgrades, on page 35.

Monitoring device and chassis upgrades

To monitor Firewall Threat Defense and chassis upgrades, you can use:

- The **Upgrade Status** screen of the upgrade wizard (**Devices** > **Threat Defense Upgrade/Chassis Upgrade**), if you have not cleared your workflow or started a new one. For detailed status, click **Detailed Status** next to the device you want to see.
- The **Upgrade** tab on the Device Management page (**Devices** > **Device Management**). For detailed status, click **View Details** next to the device you want to see.
- The **Upgrades** tab in the Message Center.

High availability state during upgrade

For Firewall Threat Defense high availability pairs, the standby upgrades first. The devices switch roles, then the new standby upgrades. During upgrade, the system can report inconsistent states:

- The Message Center and the upgrade wizard associate the units with their states *when you clicked* ***Start Upgrade***. That is, they report upgrading the "standby" and then the "active," even though failover occurs and you are only ever upgrading the standby.
- The Device Management page always shows the correct current states of the units, which can be different from the original states displayed by the Message Center or the wizard.

High availability upgrade success

For Firewall Threat Defense high availability pairs, the Message Center reports upgrade success for each unit in separate tasks.

Important Regardless of what the Message Center says, do not redeploy configurations to the high availability pair until both devices have finished upgrading.

Upgrade Options for Firewall Threat Defense

To choose upgrade options, click **Advanced settings** in the upgrade wizard or start unattended mode.

General Upgrade Options

These options apply to all upgrades and are enabled by default.

Table 18: General Upgrade Options

Option	When to Disable	Details
Compatibility and readiness checks 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.
Upgrade failure 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. Not supported for patches or hotfixes.
Enable revert Enable revert after successful upgrade.	To save time and disk space.	You have 30 days to revert most Firewall Threat Defense upgrades. Reverting returns the software to its state just before the last upgrade, also called a *snapshot*. If you revert an upgrade after installing a patch, you revert the patch as well as the upgrade. Not supported for container instances, patches, or hotfixes.
Upgrade Snort Convert eligible devices from Snort 2 to Snort 3.	To prevent Snort 3 upgrades.	With upgrades to Version 7.2–7.6, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. With upgrades to Version 7.3+, you cannot disable this option. Although you can switch individual devices back, Snort 2 is deprecated in Version 7.7, which will prevent Firewall Threat Defense upgrade. For devices that are ineligible because they use custom intrusion or network analysis policies, manually upgrade to Snort 3. For migration assistance, see the *Custom Snort 3 Intrusion Policies for Access Control* for your version.

Unattended Mode Options

These options apply only to unattended upgrades and are disabled by default; see Upgrade Firewall Threat Defense in Unattended Mode, on page 30.

Table 19: Unattended Mode Options

Option	When to Enable	Details
Start upgrade after device preparation completes.	If you don't need to carefully time the upgrade.	Starting the upgrade requires a maintenance window, but staging does not. The system will copy upgrade packages to devices and check readiness, but will not perform the actual upgrade. Note that running an unattended upgrade with this option disabled does the same thing as clicking **Prepare for Upgrade** in the main upgrade wizard. This is why you may see messages about unattended mode even if you did not explicitly start it.
Re-run readiness checks for devices that already passed.	If you are unsure about device readiness.	We recommend re-running checks for devices that passed more than 24 hours ago, or if you made changes after a device last passed. You may have recently run readiness checks on some devices and don't need to run them again.
Require all devices to be eligible to advance.	If you have an "all or none" upgrade requirement.	Enforces an "all or none" requirement for unattended upgrades. If a selected device cannot upgrade for any reason, no devices upgrade. For example, if one device cannot get the upgrade package or pass required checks, the entire process stops. Disable this option to let eligible devices proceed independently.

Troubleshooting Firewall Threat Defense Upgrade

Table 20: Troubleshooting Threat Defense Upgrade

Issue	Solution
Upgrade button missing for my target version.	Either: • You do not have anything that can be upgraded to that version right now. • No eligible devices have internet access. Upload the package to the Firewall Management Center or configure an internal server; see Managing upgrade packages with the Firewall Management Center, on page 7.
Devices not listed in the upgrade wizard.	If you accessed the wizard directly from **Devices** > **+ Show more** > **Upgrade** > **Threat Defense Upgrade** and therefore did not select a target version, the workflow may be blank. To begin, choose a target version from the **Upgrade to** menu. The system should display the devices that can be upgraded to that version.

Issue	Solution
Target version not listed in the **Upgrade to** menu.	The choices in the **Upgrade to** menu correspond to the device upgrade packages on the Firewall Management Center, plus any on the support site that apply to you. If you don't see the one you want, either: • The menu lists multiple versions but not the one you are looking for. You may not have any eligible devices. Or, the package may require manual upload (such as hotfixes). • The menu is blank/only lists versions corresponding to already uploaded packages. The Firewall Management Center does not have internet access. You must manually upload the package you want. To upload an upgrade package, click **Manage Upgrade Packages**; see Managing upgrade packages with the Firewall Management Center, on page 7.
Devices not listed in the upgrade wizard even though a target version is selected.	You have no devices that can be upgraded to that version. If you still think you should see devices here, your user role could be prohibiting you from managing (and therefore upgrading) devices. In a multidomain deployment, you could be logged into the wrong domain.
Devices locked to someone else's upgrade workflow.	If you need to reset someone else's workflow, you must have Administrator access. You can either: • Delete or deactivate the user. • Update the user's role so they no longer have permission to use **Administration** > **Upgrades & updates** > **Product Upgrades**.
High availability Firewall Management Center failed over while setting up upgrade.	Neither your workflow nor Firewall Threat Defense upgrade packages are synchronized between high availability Firewall Management Centers. In case of failover, you must recreate your workflow on the new active Firewall Management Center, which includes downloading upgrade packages and copying them to devices. (Upgrade packages already copied to devices are not removed, but the Firewall Management Center still must have the package or a pointer to its location.)
Pruning daemon errors in the Message Center.	This most commonly happens for devices running Version 7.6.x or earlier when you do not start the upgrade within 10 minutes after the readiness check completes. Regardless, you can safely ignore these messages and proceed with the upgrade. The full error is: `Process Status - device_name. The pruning daemon exited n time(s).`

Unresponsive and Failed Firewall Threat Defense Upgrades

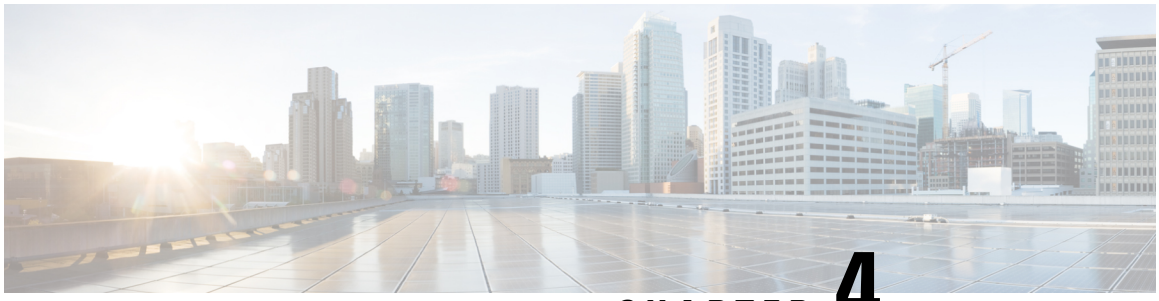
The following table has troubleshooting information for unresponsive and failed Firewall Threat Defense upgrades. For issues with chassis upgrades, contact Cisco TAC.

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

Table 21: Unresponsive and Failed Firewall Threat Defense Upgrades

Issue	Solution
Cannot reach the device.	Devices can stop passing traffic during the upgrade or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. You should also able to access the Firewall Management Center's management interface without traversing the device.
Upgrade or patch appears hung/device appears inactive.	If device upgrade status has stopped updating on the Firewall Management Center but there is no report of upgrade failure, you can try canceling the upgrade; see below. If you cannot cancel or canceling does not work, contact Cisco TAC. **Tip:** You can monitor upgrade logs on the device itself using expert mode and tail or tailf: `tail /ngfw/var/log/sf/update.status`.
Upgrade failed.	If an upgrade fails and: • The device reverted to its pre-upgrade state (auto-cancel is enabled), correct any issues and try again from the beginning. • The device is still in maintenance mode, correct any issues and resume the upgrade. Or, cancel and try again later. If you cannot retry or cancel, or if you continue to have issues, contact Cisco TAC.
Patch failed.	You cannot cancel in-progress or failed patches. However, if a patch fails early, for example, during validation stages, the device may remain up and running normally. Simply correct any issues and try again. If a patch fails after the device has entered maintenance mode, check for an uninstaller. If one exists, you can try running it to remove the failed patch; see the instructions in the Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.7.x. After the uninstall finishes, you can correct any issues and try again. If there is no uninstaller, if the uninstall fails, or if you continue to have issues, contact Cisco TAC.
Upgrade on a clustered device failed, and I want to reimage instead of retrying the upgrade.	If a cluster node upgrade fails and you choose to reimage the node, reimage it to the *current* version of the control node before you add it back to the cluster. Depending on when and how the upgrade failed, the current version of the control node can be the old version or the target version. We do not support mixed-version clusters except temporarily during upgrade. Deliberately creating a mixed-version cluster can cause outages. **Tip** Remove the failed node from the cluster and reimage it to the target version. Upgrade the rest of the cluster to the target version, then add your reimaged node.

Issue	Solution
I want to cancel an upgrade.	Canceling reverts the device to its pre-upgrade state. You can cancel failed and in-progress upgrades on the upgrade status pop-up, accessible from the Upgrade tab on the Device Management page. You cannot cancel patches. If you cannot cancel or canceling does not work, contact Cisco TAC.
I want to retry (resume) a failed upgrade.	You can resume an upgrade on the upgrade status pop-up, accessible from the Upgrade tab on the Device Management page. If you continue to have issues, contact Cisco TAC.
I want to change what happens when upgrade fails.	Part of the upgrade process is choosing what happens if it fails. This is done with the **Automatically cancel on upgrade failure...** (auto-cancel) option: • Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. This returns you to normal operations as quickly as possible while you regroup and try again. • Auto-cancel disabled: If upgrade fails, the device remains as it is. This allows you to correct any issues and resume the upgrade. For high availability and clustered devices, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.



CHAPTER 4

Upgrade Chassis for Firewall Threat Defense 3100, 4100, 4200, 9300

- Upgrade the Secure Firewall 3100/4200 Chassis, on page 39
- Upgrade FXOS on the Firepower 4100/9300 with Firewall Chassis Manager, on page 42
- Upgrade FXOS on the Firepower 4100/9300 with the CLI, on page 49
- Upgrade Firmware on the Firepower 4100/9300, on page 59

Upgrade the Secure Firewall 3100/4200 Chassis

Use this procedure to upgrade the chassis on the Secure Firewall 3100/4200 in multi-instance mode with the upgrade wizard.

For the Secure Firewall 3100/4200 in multi-instance mode, any upgrade can require a chassis upgrade. Although you upgrade the chassis and firewall separately, one package contains the chassis and firewall upgrades, and you perform both from the Firewall Management Center. It is possible to have a chassis-only upgrade or a firewall-only upgrade.

As you proceed, the system displays basic information about your selected chassis, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade.

If you navigate away from the upgrade 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** > **+ Show more** > **Upgrade** > **Chassis Upgrade**.

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 copying upgrade packages and choosing upgrade options.



Caution Do not deploy configuration changes during upgrade. Even if the chassis or its devices appear inactive, do not manually reboot or shut down. Do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. The 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 or device, contact Cisco TAC.

Before you begin

Make sure you are ready to upgrade:

- Determine if you can run the target version: Compatibility, on page 1
- Plan your upgrade path: Upgrade Path, on page 3
- Review upgrade guidelines: Upgrade Guidelines, on page 2
- Check infrastructure and network: Network and Infrastructure Checks, on page 16
- Check configurations, tasks, and overall deployment health: Configuration and Deployment Checks, on page 17
- Perform backups: Backups, on page 18

Procedure

Step 1 On the Firewall Management Center, choose **Administration** > **Upgrades & updates** > **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. If the Firewall Management Center has internet access, it lists upgrades that apply to you, with suggested releases specially marked.

Step 2 (Optional) Get upgrade packages onto the Firewall Management Center, or put them on an internal server.

Skip this step if your devices can get upgrade packages directly from the internet. For other options, see Managing upgrade packages with the Firewall Management Center, on page 7.

Step 3 Launch the upgrade wizard.

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

Note
The upgrade wizard was updated in Version 10.0. If you prefer, click **Switch to legacy wizard**. For information on using the legacy wizard, see Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.7.x.

Step 4 Select chassis to upgrade.

To help you select chassis to upgrade, the upgrade wizard allows you to search and filter based on various useful criteria. The **Ready to proceed** filter shows all selected chassis that are currently eligible for upgrade. Before proceeding with any upgrade step, the **Selected** number should match the **Ready to proceed** number. If they don't match, use the **Not candidates** filter to see why. You don't have to remove ineligible chassis, but 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. The **Details** column indicates which chassis have packages that might not be needed. If any do:

a) Use the **Warning** filter to display the affected chassis.
b) In the filtered view, click **View and clean up packages** next to a chassis, select the packages you want to remove, and click **Delete selected packages**. Repeat this step for each chassis you want to clean up.

Step 6 Click **Prepare for Upgrade** to immediately begin copying upgrade packages to chassis.

Where upgrade packages come from depends on your deployment and previous configurations. For more information, see Copying Upgrade Packages to Devices, on page 9.

Step 7 Choose upgrade order.

By default, chassis upgrades run in parallel. For serial order, select the appropriate chassis and click **Move to serial upgrade**. To change the serial upgrade order, click **Change upgrade order**.

Note
For chassis with high availability instances, we recommend two workflows (run the upgrade wizard twice) over either parallel or serial upgrade. For more information, see Upgrade Order, 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 17.

Step 9 Click **Start upgrade** and confirm your choice.

For information on traffic handling during the upgrade, see Traffic Flow and Inspection for Chassis Upgrades, on page 75.

Step 10 Monitor the upgrade.

The wizard shows your overall upgrade progress. For more information, see Monitor Firewall Threat Defense Upgrades, on page 32.

Step 11 Verify success.

After the upgrade completes, verify success on **Devices** > **Device Management**.

Step 12 (Optional) Examine configuration changes.

Before you upgrade Firewall Threat Defense, you may want to review the changes made by the chassis upgrade:

- If you have not cleared your workflow, you can return to the wizard. Choose **Devices** > **+ Show more** > **Upgrade** > **Chassis Upgrade** and click **Configuration Changes** next to each chassis.
- If you have cleared the workflow, or if you want to quickly generate change reports for multiple chassis, use the Advanced Deploy page. Choose **Deploy** > **Advanced Deploy**, select the chassis you upgraded, and click **Pending Changes Reports**. After the reports finish generating, you can download them from the Tasks tab on the Message Center.

Step 13 (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 Firewall 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. After you clear the wizard, use the Upgrade tab on the Device Management page to see last-upgrade information, and the Advanced Deploy screens to see configuration changes.

- Back up again: Backups, on page 18

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

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

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.

Procedure

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.

Procedure

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

a) Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the control unit).
b) Enter **top**.
c) Enter **scope ssa**.
d) Enter **show slot**.
e) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
f) Enter **show app-instance**.
g) Verify that the Oper State is `Online` and that the Cluster State is `In Cluster` for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

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

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

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

show version.

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

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

Step 4 Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.
c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

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

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

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

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

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

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

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

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

Example:

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

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

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

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

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

FP9300-A /ssa # show app-instance
App Name   Slot ID    Admin State Oper State       Running Version Startup Version Profile Name
Cluster State   Cluster Role
---------- ---------- ----------- ---------------- --------------- --------------- ------------
--------------- ------------
```

```
ftd        1          Enabled     Online           6.2.2.81        6.2.2.81                    In
 Cluster      Slave
ftd        2          Enabled     Online           6.2.2.81        6.2.2.81                    In
 Cluster      Slave
ftd        3          Disabled    Not Available                    6.2.2.81                    Not
 Applicable  None
FP9300-A /ssa #
```

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

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

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

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

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

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

Before you begin

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

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.

Procedure

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

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.

Procedure

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.

Procedure

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.

Procedure

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

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

a) Enter firmware mode:

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

b) Download the FXOS platform bundle software image:

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

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

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

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

c) To monitor the download process:

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

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

Example:

The following example copies an image using the SCP protocol:

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

Step 3 If necessary, return to firmware mode:

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

Step 4 Enter auto-install mode:

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

Step 5 Install the FXOS platform bundle:

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

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

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

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

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

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

Step 8 To monitor the upgrade process:

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

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

Example:

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

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

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

FP9300-A /system #
```

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

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

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

a) Connect to Firepower Management Center.
b) Choose **Devices** > **Device Management**.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).
d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

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

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

a) Enter firmware mode:

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

b) Download the FXOS platform bundle software image:

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

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

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

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

c) To monitor the download process:

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

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

Example:

The following example copies an image using the SCP protocol:

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

Step 13 If necessary, return to firmware mode:

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

Step 14 Enter auto-install mode:

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

Step 15 Install the FXOS platform bundle:

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

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

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

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

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

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

Step 18 To monitor the upgrade process:

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

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

Example:

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

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

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

FP9300-A /system #
```

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

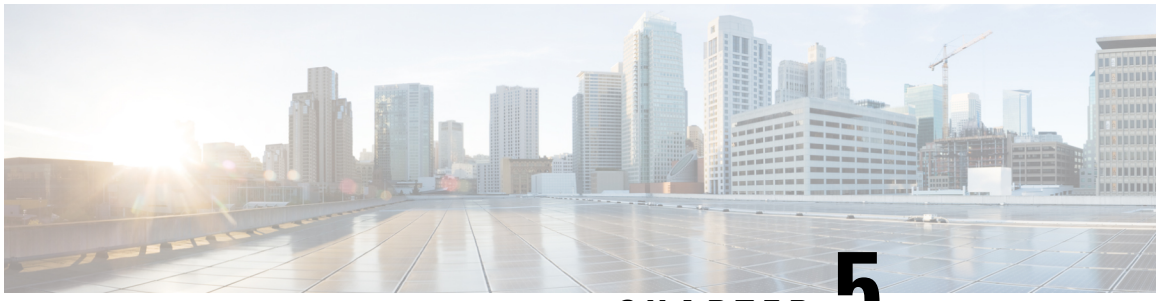
a) Enter **top**.
b) Enter **scope ssa**.
c) Enter **show slot**.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter **show app-instance**.
f)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

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

a) Connect to Firepower Management Center.
b) Choose **Devices** > **Device Management**.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).
d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Upgrade Firmware on the Firepower 4100/9300

Chassis upgrades to FXOS 2.14.1+ (the companion release to Firewall Threat Defense 7.4) include firmware. If you are upgrading older devices, see *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.



CHAPTER 5

Revert or Uninstall

If an upgrade succeeds but the system does not function to your expectations, you may be able to return to the previous version.

- Revert vs Uninstall, on page 61
- Revert Firewall Threat Defense Upgrades, on page 62
- Uninstall Firewall Threat Defense and Firewall Management Center Patches, on page 66

Revert vs Uninstall

Whether you revert or uninstall depends on the platform and release type.

Table 22: Revert vs Uninstall

	Revert	Uninstall
Platforms	Firewall Threat Defense only.	Firewall Management Center and Firewall Threat Defense.
Releases	First-digit (major), second-digit (major or minor), and third-digit (maintenance) upgrades to Version 7.1.x–10.0.x. **Note** Before Version 10.0, second-digit releases are called *major* releases. In Version 10.0+ they are called *minor* releases. Third-digit releases are always maintenance releases. You can revert all of these, regardless of label.	Patches (fourth-digit upgrades) to Version 10.0 and earlier.
Details	Returns the software to its state just before the last upgrade (a *snapshot*). For details, see Reverted Configurations, on page 64.	Returns the software to the version you patched from. Does not change configurations.
Restrictions	Not supported for container instances or the Secure Firewall 200. For more scenarios that prevent revert, see Scenarios Preventing Revert, on page 63.	For scenarios where uninstall is not supported or recommended, see the Uninstall Guidelines, on page 66.

	Revert	Uninstall
Revert/Uninstall From	Use **Devices** > **Device Management** to revert Firewall Threat Defense upgrades.	Use **Administration** > **Upgrades & updates** > **Product Upgrades** to uninstall Firewall Management Center patches. Use expert mode (CLI) on the device to uninstall Firewall Threat Defense patches.

Example: Revert vs Uninstall

Reverting after patching also removes the patch. For example:

1. Upgrade Firewall Threat Defense from Version 7.2.0 → 7.2.5.
2. Patch from Version 7.2.5 → 7.2.5.2.
3. You can now either:
   - Uninstall the patch to go back to Version 7.2.5.

     This removes the patch only.
   - Revert the upgrade to go back to Version 7.2.0.

     This removes the patch and the maintenance release.

Revert Firewall Threat Defense Upgrades

Revert Guidelines

This section discusses general guidelines for revert. To check for version-specific revert issues, see the release notes: https://cisco.com/go/fmc-ftd-release-notes-100.

Reverting High Availability or Clustered Devices

When you use the Firewall Management Center web interface to revert Firewall 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 Firewall 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 only on interface configurations, as if every device were standalone.

Revert is supported for fully and partially upgraded high availability pairs and clusters. In the case of partial upgrade, the upgraded units/nodes are reverted. Revert will not break high availability or clusters, but you can do it manually and revert the newly standalone devices.

Revert is supported only for high availability pairs and clusters whose members were upgraded as a unit (or where upgrade was attempted as a unit) by the current Firewall Management Center. For example, you cannot

upgrade standalone devices, form a high availability pair, and then revert the pair. Similarly, you cannot revert a cluster until all units match (that is, all active cluster units were upgraded as a cluster, together).

Reverting the Firepower 4100/9300

For the Firepower 4100/9300, reverting Firewall Threat Defense does not revert the chassis (FXOS). In multi-instance mode, revert is not supported for container instances.

Major Firewall Threat Defense versions have a specially qualified and recommended companion FXOS version. After you return to the earlier version of Firewall Threat Defense, you may be running a non-recommended version of FXOS (too new).

Although newer versions of FXOS are backwards compatible with older Firewall 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.

Reverting the Secure Firewall 3100/4200

For the Secure Firewall 3100/4200 in multi-instance mode, revert is not supported for container instances, so there is no need to revert the chassis. In appliance mode, revert is fully supported.

Scenarios Preventing Revert

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

Table 23: Scenarios Preventing Revert

Scenario	Solution
Lower-memory devices: • Container instances • Secure Firewall 200	None. Some devices do not have enough memory to store a revert snapshot, so revert is not supported.
Revert snapshot is not available because: • You did not enable revert when you upgraded the device. • You deleted the snapshot from either the Firewall Management Center or the device, or it expired. • You upgraded the device with a different Firewall Management Center. • You reverted to the version you are running now (you are trying to perform multiple reverts in succession).	None. The revert snapshot is saved on the Firewall Management Center and the device for 30 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. The system only saves one snapshot. You cannot revert more than once, that is: • Supported: A → B → C → B • Not supported: A → B → C → B → A

Scenario	Solution
Firewall Management Center changed version since the device upgrade.	None. You cannot revert a device if the Firewall Management Center has changed version (upgrade, patch, or patch uninstall) since the device upgrade.
Last upgrade failed.	Return the device to its pre-upgrade state by canceling the upgrade. Or, fix the issues and try again. Use revert when an upgrade succeeds but the upgraded device does not function as expected. This is not the same as canceling a failed or in-progress upgrade. If you cannot revert or cancel, you will have to reimage.
Management access interface changed since the upgrade.	Switch it back and try again.
High availability pair formed after either device, or both devices, were upgraded.	Break high availability and revert the newly standalone units, if possible.
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. This includes newly formed clusters using upgraded devices.	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 Firewall 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.

Reverted Configurations

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 Firewall Threat Defense, you may need a full reimage; see Revert Guidelines, on page 62.

Revert a Firewall Threat Defense Upgrade

You must use the Firewall Management Center to revert the device.

Note If communications between the Firewall Management Center and the device are disrupted, use the device CLI to delete the device from management (**configure manager delete**), then revert (**upgrade revert**). Deleting the manager does invalidate the device configuration, but this can still save time over a reimage. You should also use the Firewall Management Center web interface to unregister the stale device. After the revert completes, you can re-register and deploy configurations. To see what version the system will revert to, use **show upgrade revert-info**.

Before you begin

- Make sure revert is supported. Read and understand the guidelines.
- Revisit the Planning Your Upgrade, on page 1 chapter. In general, prepare for reverting an upgrade in the same way you prepared for installing it. It is especially important that you back up to a secure external location. A failed revert may require a reimage, which returns most settings to factory defaults.

Procedure

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/clustered deployments, the system reverts all units simultaneously.

Step 4 Monitor revert progress.

In high availability/clustered 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 Firewall Threat Defense logical devices using the Firewall Chassis Manager or the FXOS CLI.

On the Firewall 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.

What to do next

For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for each reverted logical device. You can use the **Logical Devices** tab on the Secure Firewall Chassis Manager or the `set startup-version` FXOS command. This ensures that if you need to restore the logical device from a post-revert backup, the backup and startup versions match. For more information, see the *Image Management* chapter in the *Cisco Firepower 4100/9300 FXOS Secure Firewall Chassis Manager Configuration Guide*, or the *Cisco Firepower 4100/9300 FXOS Command Reference*.

Uninstall Firewall Threat Defense and Firewall Management Center Patches

Uninstall Guidelines

This topic discusses general guidelines for uninstall. To check for version-specific uninstall issues, see the upgrade guidelines in the release notes: https://cisco.com/go/fmc-ftd-release-notes-100.

Maintaining Compatibility

Because the Firewall Management Center should run the same or newer version as its managed devices, uninstall patches from devices first.

Uninstalling from High Availability Firewall Management Centers

Minimize disruption by uninstalling from one Firewall Management Center at a time. Wait until the patch has fully uninstalled from one unit before you move on to the next.

1. Pause synchronization (enter split-brain). Do not make or deploy configuration changes during split-brain.
2. Uninstall from the standby.
3. Uninstall from the active.
4. Restart synchronization (exit split-brain).

Uninstalling from High Availability or Clustered Devices

Minimize disruption by uninstalling from one device at a time. Unlike upgrade, the system does not do this for you. Wait until the patch has fully uninstalled from one unit before you move on to the next.

High Availability: You cannot uninstall a patch from devices configured for high availability. You must break high availability first.

1. Break high availability.
2. Uninstall from the former standby.
3. Uninstall from the former active.
4. Reestablish high availability.

Clusters: Uninstall from one unit at a time, leaving the control unit for last. Clustered units operate in maintenance mode while the patch uninstalls.

1. Uninstall from the data modules one at a time.
2. Make one of the data modules the new control module.
3. Uninstall from the former control.

Scenarios Preventing or Restricting Uninstall

If you attempt to uninstall in any of these situations, you may have significant issues.

Table 24: Scenarios Preventing or Restricting Uninstall

Scenario	Solution
The release notes say that a specific patch does not support or recommend uninstall.	Uninstalling a patch applies only to the software. After uninstalling a patch that updates the operating system or other components not reversed by the uninstall, you may be unable to deploy configuration changes, or you may experience other incompatibilities between the newer components and the older software. In these cases, we recommend you do not uninstall. Because patches are cumulative, and because uninstalling a patch returns the software to the version you started from, we also recommend against uninstalling later patches if it will take you to a version earlier than the affected patch. For example, if Patch 5 updates the operating system, do not uninstall Patch 5, but also do not uninstall Patch 6+ if you started at Patch 4 or earlier (including the base version). Specific patches that you should not uninstall due to this or any other reason are listed in the release notes. If you need to uninstall one of these patches, contact Cisco TAC.
You are in Security Certifications Compliance (CC/UCAPL) mode.	If a patch updates the operating system and security certifications compliance is enabled, FSIC (file system integrity check) fails when the appliance reboots. The software does not start, remote SSH access is disabled, and you can access the appliance only via local console. Uninstall is not recommended in security certifications compliance mode. If you need to do this, contact Cisco TAC.
You need to uninstall a hotfix or a hotfixed patch.	You must uninstall hotfixes and patches in the exact reverse order from their installation (last in, first out). For example: • Install: Patch A → Hotfix B → Hotfix C → Patch D → Hotfix E • Uninstall: Hotfix E → Patch D → Hotfix C → Hotfix B → Patch A For Firewall Management Center patches and hotfixes, the web interface enforces the correct order. For Firewall Threat Defense, where you use expert mode to uninstall, you must do it yourself. To view your update history, use expert mode: **`cat /etc/sf/patch_history`**. Uninstall is not recommended for hotfixes and hotfixed patches. If you need to do this, contact Cisco TAC.
You reverted to the version you are running now.	None. Upgrading to a major or maintenance release deletes upgrade packages and uninstallers that do not apply to the new version.

Uninstall a Firewall Threat Defense Patch

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

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

Before you begin

- Make sure uninstall is supported. Read and understand the guidelines.
- Revisit the Planning Your Upgrade, on page 1 chapter. In general, you should prepare for uninstalling a patch in the same way you prepared for installing it.
- Break high availability pairs.

Procedure

Step 1 If the device's configurations are out of date, deploy now from the Firewall Management Center.

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

Step 2 Access the Firewall Threat Defense CLI on the device. Log in as `admin` or another CLI user with configuration access.

You can either SSH to the device's management interface (hostname or IP address) or use the console. If you use the console, some devices default to the operating system CLI and require an extra step to access the Firewall Threat Defense CLI, as follows.

ISA 3000	—
Firewall Threat Defense Virtual	—
Firepower 4100/9300	`connect module` *`slot_number`* `console`, then `connect ftd` (first login only)
All other models	`connect ftd`

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

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

```
ls /var/sf/updates
```

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

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

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

Caution

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

Step 6 Monitor the uninstall until you are logged out.

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

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

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

After the uninstall completes, confirm that the device has the correct software version. On the Firewall Management Center, choose **Devices** > **Device Management**.

Step 8 In high availability and clustered deployments, repeat steps 2 through 7 for each unit.

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

Step 9 Redeploy configurations.

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

What to do next

- For high availability, reestablish high availability.
- For clusters, if you have preferred roles for specific devices, make those changes now.

Uninstall a Firewall Management Center Patch: Standalone

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



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

Before you begin

- Make sure uninstall is supported. Read and understand the guidelines.
- Revisit the Planning Your Upgrade, on page 1 chapter. In general, prepare for uninstalling a patch in the same way you prepared for installing it.

- If uninstalling will put the Firewall Management Center at a lower patch level than its managed devices, uninstall patches from the devices first.

Procedure

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

Deploying before you uninstall reduces the chance of failure.

Step 2 Choose **Administration** > **Upgrades & updates** > **Product Upgrades**.

Step 3 In the System Overview, where it displays the last upgrade performed for the Firewall Management Center, click **Uninstall** and confirm your choice.

You can monitor uninstall progress in the Message Center. If the patch reboots the Firewall Management Center, you will be logged out. Log back in when you can.

Step 4 Verify uninstall success.

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

Step 5 Redeploy configurations to all managed devices.

Uninstall a Firewall Management Center Patch: High Availability

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

Uninstall from high availability peers one at a time. With synchronization paused, first uninstall from the standby, then the active. When the standby starts the uninstall, its status switches from standby to active, so that both peers are active. This temporary state is called *split-brain* and is *not* supported except during upgrade and uninstall.



Caution Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after synchronization restarts; deploying could place the system in an unusable state and require a reimage. 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 uninstall is supported. Read and understand the guidelines.
- Revisit the Planning Your Upgrade, on page 1 chapter. In general, prepare for uninstalling a patch in the same way you prepared for installing it.

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

Procedure

Step 1 On the active Firewall Management Center, deploy to managed devices whose configurations are out of date.

Deploying before you uninstall reduces the chance of failure.

Step 2 On the active Firewall Management Center, pause synchronization.

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

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

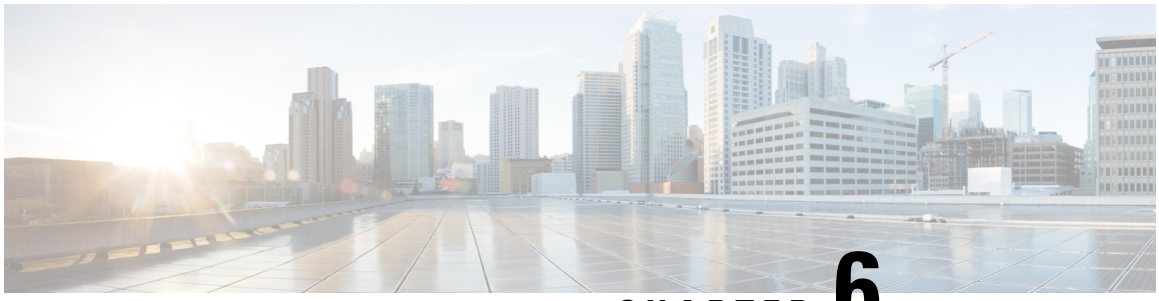
Follow the instructions in Uninstall a Firewall Management Center Patch: Standalone, on page 70, but omit the initial deploy, stopping after you verify uninstall success on each peer. In summary, for each peer:

a) On **Administration** > **Upgrades & updates** > **Product Upgrades**, uninstall the patch.
b) Monitor progress until you are logged out, then log back in when you can.
c) Verify uninstall success.

Step 4 On the Firewall Management Center you want to make the active peer, restart synchronization.

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

Step 5 Redeploy configurations to all managed devices.



CHAPTER 6

Reference

- Traffic Flow and Inspection, on page 73
- Time and Disk Space, on page 76
- Upgrade Feature History, on page 77

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 Firewall 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 25: Traffic Flow and Inspection: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped. For bridge group interfaces on the ISA 3000 only, you can use a FlexConfig policy to configure hardware bypass for power failure. This causes traffic to drop during software upgrades but pass without inspection while the device completes its post-upgrade reboot.

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

Software Upgrades for High Availability and Clustered Devices

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

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

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

Software Revert (Major/Maintenance Releases)

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

Software Uninstall (Patches)

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

Traffic Flow and Inspection for Chassis Upgrades

Upgrading FXOS reboots the chassis. For FXOS upgrades to Version 2.14.1+ that include firmware upgrades, the chassis reboots twice—once for FXOS and once for the firmware. This includes Version 7.4.1+ chassis upgrades for the Secure Firewall 3100/4200 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; see Upgrade Order, on page 5.

Table 26: Traffic Flow and Inspection: FXOS Upgrades

Firewall 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 Firewall 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 27: Traffic Flow and Inspection: Deploying Configuration Changes

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

Time and Disk Space

Time to Upgrade

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

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive and Failed Firewall Threat Defense Upgrades, on page 35.

Table 28: Upgrade Time Considerations

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

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

Disk Space to Upgrade

To upgrade, the upgrade package must be on the appliance. For device upgrades where the device does not have access to the internet, you must also have enough space on the Firewall Management Center (in either /Volume or /var) for the device upgrade package. Or, you can use an internal server to store them. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails. For more information, see Configuration and Deployment Checks, on page 17.

Upgrade Feature History

Table 29: Device Upgrade Feature History

Feature	Minimum Management Center	Minimum Threat Defense	Details
All-or-none option for unattended device upgrade	10.1.0	Any	When you start an unattended upgrade, a new **Require all devices to be eligible to advance** option allows you to enforce an "all or none" requirement. If a selected device cannot upgrade for any reason, no devices upgrade. For example, if one device cannot get the upgrade package or pass required checks, the entire process stops. Disable this option to let eligible devices proceed independently.
New device and chassis upgrade wizard	10.0.0	Any	A new, streamlined upgrade wizard makes it easier to select and prepare devices for upgrade, and to identify issues preventing upgrade. Note that the Firewall Threat Defense wizard takes advantage of a new prepare-only option for unattended mode. This means that while the wizard copies packages and checks readiness, you may see messages about unattended mode running even if you did not explicitly start it.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Prepare-only and skip-checks options for unattended Firewall Threat Defense upgrade	10.0.0	Any	With unattended Firewall Threat Defense upgrades: • Prepare for upgrade only—copy packages and check readiness, but do not perform the actual upgrade. • Skip readiness checks for devices that already passed. These new options are available when you start unattended mode.
New options for downloading upgrade packages	10.0.0	Any	You can now: • Prevent devices from downloading upgrade packages from the internet. That is, you can now require that devices get upgrade packages from the Firewall Management Center or an internal server, even if the devices have internet access. • Specify how long the system retries failed downloads from an internal server (devices only) or the internet. This setting does not apply to transfers between the Firewall Management Center and device. New/modified screens: **Administration** > **Product Upgrades** > **Global upgrade settings**
Deprecated: Monitor device revert in the Message Center	10.0.0	Any	You can no longer monitor device revert from the Message Center. Instead, use the Device Management page (**Devices** > **Device Management**). On the **Upgrade** tab, click **View Details** next to the device you are reverting.
Upgrade Firewall Threat Defense or chassis without a manual readiness check.	7.7.0	7.7.0	You no longer have to run time-consuming pre-upgrade readiness checks for Firewall Threat Defense or chassis upgrades. Instead, these checks are now regularly run by the system and reported in the health monitor. This allows you to preemptively fix any issues that will block upgrade. • The Database module, new for devices, manages monitors database schema and configuration data (*EO*) integrity. • The FXOS Health module, new for devices, monitors the FXOS httpd service on FXOS-based devices. • The Disk Status module is now more robust, alerting on disk health issues reported by daily running of smartctl (a Linux utility for monitoring reliability, predicting failures, and performing other self-tests). Version restrictions: This feature is supported for upgrades *from* Version 7.7+. Devices running earlier versions still require the in-upgrade readiness check.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Devices with internet access download upgrade packages from the internet.	7.6.1 7.7.0	Any	You can now begin device and chassis upgrades without the upgrade package. At the appropriate time, devices will get the package directly from the internet. This saves time and Firewall Management Center disk space. Devices without internet access can continue to get the package from the Firewall Management Center or an internal server. Note that devices try the internal server (if configured) before either the internet or the Firewall Management Center. If the internal server download fails, newer devices with internet access try the internet then the Firewall Management Center, while older devices and devices without internet access just try the Firewall Management Center. (In this context, "newer" means Firewall Threat Defense 7.6+ or chassis 7.4.1+.) Restrictions: Firewall Management Center and devices must be able to access the internet. There is no way to force a device with internet access to try the Firewall Management Center before it tries the internet. Not supported for hotfixes. Download location: https://cdo-ftd-images.s3-us-west-2.amazonaws.com/
Generate and download post-upgrade configuration change reports from the Firewall Threat Defense and chassis upgrade wizards.	7.6.0	Any	You can now generate and download post-upgrade configuration change reports from the Firewall Threat Defense and chassis upgrade wizards, as long as you have not cleared your upgrade workflow. Previously, you used the Advanced Deploy screens to generate the reports and the Message Center to download them. Note that you can still use this method, which is useful if you want to quickly generate change reports for multiple devices, or if you cleared your workflow. New/modified screens: • **Devices** > **Threat Defense Upgrade** > **Configuration Changes** • **Devices** > **Chassis Upgrade** > **Configuration Changes**
Deprecated: Copy upgrade packages ("peer-to-peer sync") from device to device.	7.6.0	7.6.0	You can no longer use the Firewall Threat Defense CLI to copy upgrade packages between devices over the management network. If you have limited bandwidth between the Firewall Management Center and its devices, configure devices to get upgrade packages directly from an internal web server. Deprecated CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
Chassis upgrade for the Secure Firewall 3100 in multi-instance mode.	7.4.1	7.4.1	For the Secure Firewall 3100 in multi-instance mode, you upgrade the operating system and the firmware (*chassis upgrade*) separately from the container instances (*Firewall Threat Defense upgrade*). New/modified screens: • Upgrade the chassis: **Devices** > **Chassis Upgrade** • Upgrade Firewall Threat Defense **Devices** > **Threat Defense Upgrade**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Firmware upgrades included in FXOS upgrades.	7.4.1	Any	**Chassis/FXOS upgrade impact. Firmware upgrades cause an extra reboot.** For the Firepower 4100/9300, FXOS upgrades to Version 2.14.1 now include 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. 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. See: *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*
Choose and direct-download upgrade packages to the Firewall Management Center.	7.3.0	Any	You can now choose which Firewall Threat Defense upgrade packages you want to direct download to the Firewall Management Center. Use the new **Download Updates** sub-tab on > **Updates** > **Product Updates**. Version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1.
Upload upgrade packages to the Firewall Management Center from the Firewall Threat Defense wizard.	7.3.0	Any	You now use the wizard to upload Firewall Threat Defense upgrade packages or specify their location. Previously (depending on version), you used **System** > **Updates** or **System** > **Product Upgrades**. Version restrictions: this feature is replaced by an improved package management system in Version 7.2.6/7.4.1.
Auto-upgrade to Snort 3 after successful Firewall Threat Defense upgrade is no longer optional.	7.3.0	Any	**Upgrade impact. All eligible devices upgrade to Snort 3 when you deploy.** When you upgrade Firewall Threat Defense to Version 7.3+, you can no longer disable the **Upgrade Snort 2 to Snort 3** option. After the software upgrade, all eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations. Although you can switch individual devices back, Snort 2 is not supported on Firewall Threat Defense 7.7+. You should stop using it now. For devices that are ineligible for auto-upgrade because they use custom intrusion or network analysis policies, manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the *Custom Snort 3 Intrusion Policies for Access Control* for your version.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Combined upgrade and install package for Secure Firewall 3100.	7.3.0	7.3.0	**Reimage Impact.** In Version 7.3, we combined the Firewall Threat Defense install and upgrade package for the Secure Firewall 3100, as follows: • Version 7.1–7.2 install package: cisco-ftd-fp3k.*version*.SPA • Version 7.1–7.2 upgrade package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar • Version 7.3+ combined package: Cisco_FTD_SSP_FP3K_Upgrade-*version-build*.sh.REL.tar Although you can upgrade Firewall Threat Defense without issue, you cannot reimage from older Firewall Threat Defense and ASA versions directly to Firewall 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. To get to Firewall Threat Defense Version 7.3+, your options are: • Upgrade from Firewall Threat Defense Version 7.1 or 7.2 — use the normal upgrade process. See the appropriate Upgrade Guide. • Reimage from Firewall Threat Defense Version 7.1 or 7.2 — reimage to ASA 9.19+ first, then reimage to Firewall Threat Defense Version 7.3+. See *Threat Defense→ASA: Firepower 1000, 2100; Secure Firewall 3100* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* 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 Firewall Threat Defense Version 7.3+. See the *Cisco Secure Firewall ASA Upgrade Guide* and then *ASA→Threat Defense: Firepower 1000, 2100 Appliance Mode; Secure Firewall 3100* in the *Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*. • Reimage from Firewall Threat Defense Version 7.3+ — use the normal reimage process. See *Reimage the System with a New Software Version* in the *Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense*.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Push packages and check readiness for older ASA FirePOWER and NGPISv devices before upgrade.	7.2.11 7.4.3	—	With the new upgrade capabilities introduced in 7.2.6 and 7.4.1, we deprecated the ability to perform a pre-upgrade package push and readiness check for ASA FirePOWER and NGPISv. These options have returned to the Classic device upgrade workflow. Version restrictions: These devices were last supported in Version 7.0, and the Version 7.4 Firewall Management Center is the last that can manage them.
Firewall Threat Defense and chassis upgrade wizards optimized for lower resolution screens.	7.2.10 7.4.3 7.6.0	Any	We optimized the Firewall Threat Defense and chassis upgrade wizards for lower resolution screens (and smaller browser windows). Text appears smaller and certain screen elements are hidden. If you change your resolution or window size mid-session, you may need to refresh the page for the web interface to adjust. Note that the minimum screen resolution to use the Firewall Management Center is 1280 x 720. New/modified screens: • **Devices** > **Threat Defense Upgrade** • **Devices** > **Chassis Upgrade**
Enable revert from the Firewall Threat Defense upgrade wizard.	7.2.6 7.4.1	Any, if upgrading to 7.1+	You can now enable revert from the Firewall Threat Defense upgrade wizard. Version restrictions: You must be upgrading Firewall Threat Defense to Version 7.1+. Not supported with Firewall Management Center Version 7.3.x or 7.4.0.
View detailed upgrade status from the Firewall Threat Defense upgrade wizard.	7.2.6 7.4.1	Any	The final page of the Firewall 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.

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

Feature	Minimum Management Center	Minimum Threat Defense	Details
Select devices to upgrade from the Firewall Threat Defense upgrade wizard.	7.2.6 7.3.0 December 13, 2022	Any	Use the wizard to select devices to upgrade. You can now use the Firewall 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.
Unattended Firewall Threat Defense upgrades.	7.2.6 7.3.0 December 13, 2022	Any	The Firewall 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.
Simultaneous Firewall Threat Defense upgrade workflows by different users.	7.2.6 7.3.0 December 13, 2022	Any	We now allow simultaneous upgrade workflows by different users, as long as you are upgrading different devices. The system prevents you from upgrading devices already in someone else's workflow. Previously, only one upgrade workflow was allowed at a time across all users.
Skip pre-upgrade troubleshoot generation for Firewall Threat Defense.	7.2.6 7.3.0 December 13, 2022	Any	You can now skip the automatic generating of troubleshooting files before major and maintenance upgrades by disabling the new **Generate troubleshooting files before upgrade begins** option. This saves time and disk space. To manually generate troubleshooting files for a Firewall Threat Defense device, choose **System**(⚙) > **Health** > **Monitor**, click the device in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Copy upgrade packages ("peer-to-peer sync") from device to device.	7.2.0	7.2.0	Instead of copying upgrade packages to each device from the Firewall Management Center or internal web server, you can use the Firewall 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 Firewall Management Center. Each device can accommodate 5 package concurrent transfers. This feature is supported for Version 7.2.x–7.4.x standalone devices managed by the same Version 7.2.x–7.4.x standalone Firewall 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 Firewall Management Centers. • Devices in different domains, or devices separated by a NAT gateway. • Devices upgrading from Version 7.1 or earlier, regardless of Firewall Management Center version. • Devices running Version 7.6+. New/modified CLI commands: **configure p2psync enable**, **configure p2psync disable**, **show peers**, **show peer details**, **sync-from-peer**, **show p2p-sync-status**
Auto-upgrade to Snort 3 after successful Firewall Threat Defense upgrade.	7.2.0	7.0.0	When you use a Version 7.2+ Firewall Management Center to upgrade Firewall Threat Defense to Version 7.2+, you can now choose whether to **Upgrade Snort 2 to Snort 3**. After the software upgrade, eligible devices upgrade from Snort 2 to Snort 3 when you deploy configurations. For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For help, see the *Custom Snort 3 Intrusion Policies for Access Control* for your version. Version restrictions: Not supported for Firewall Threat Defense upgrades to Version 7.0.x or 7.1.x.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade for single-node clusters.	7.2.0	Any	You can now use the device upgrade page (**Devices** > **Device Upgrade**) to upgrade clusters with only one active node. Any deactivated nodes are also upgraded. Previously, this type of upgrade would fail. This feature is not supported from the system updates page (**System** > **Updates**). Hitless upgrades are also not supported in this case. Interruptions to traffic flow and inspection depend on the interface configurations of the lone active unit, just as with standalone devices. Supported platforms: Firepower 4100/9300, Secure Firewall 3100
Revert a successful device upgrade.	7.1.0	7.1.0	You can now revert major and maintenance upgrades to FTD. Reverting returns the software to its state just before the last upgrade, also called a *snapshot*. If you revert an upgrade after installing a patch, you revert the patch as well as the major and/or maintenance upgrade. **Important** If you think you might need to revert, you must use **System** > **Updates** to upgrade FTD. The System Updates page is the only place you can enable the **Enable revert after successful upgrade** option, which configures the system to save a revert snapshot when you initiate the upgrade. This is in contrast to our usual recommendation to use the wizard on the **Devices** > **Device Upgrade** page. This feature is not supported for container instances. Minimum FTD: 7.1
Improvements to the upgrade workflow for clustered and high availability devices.	7.1.0	Any	We made the following improvements to the upgrade workflow for clustered and high availability devices: • The upgrade wizard now correctly displays clustered and high availability units as groups, rather than as individual devices. The system can identify, report, and preemptively require fixes for group-related issues you might have. For example, you cannot upgrade a cluster on the Firepower 4100/9300 if you have made unsynced changes on Firepower Chassis Manager. • We improved the speed and efficiency of copying upgrade packages to clusters and high availability pairs. Previously, the FMC copied the package to each group member sequentially. Now, group members can get the package from each other as part of their normal sync process. • You can now specify the upgrade order of data units in a cluster. The control unit always upgrades last.
Improved FTD upgrade performance and status reporting.	7.0.0	7.0.0	FTD upgrades are now easier faster, more reliable, and take up less disk space. A new **Upgrades** tab in the Message Center provides further enhancements to upgrade status and error reporting.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Easy-to-follow upgrade workflow for FTD devices.	7.0.0	Any	A new device upgrade page (**Devices** > **Device Upgrade**) on the FMC provides an easy-to-follow wizard for upgrading Version 6.4+ FTD devices. It walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and compatibility and readiness checks. To begin, use the new **Upgrade Firepower Software** action on the Device Management page **Devices** > **Device Management** > **Selection**. As you proceed, the system displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage. If you navigate away from wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the wizard. **Note** You must still use **System** > **Updates** to upload or specify the location of FTD upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as all non-FTD managed devices. **Note** In Version 7.0, the wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the wizard displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all. To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the wizard before you click **Next**.
Upgrade more FTD devices at once.	7.0.0	Any (source) 6.7.0 (target)	The number of devices you can upgrade at once is now limited by your management network bandwidth—not the system's ability to manage simultaneous upgrades. Previously, we recommended against upgrading more than five devices at a time. **Important** Only upgrades to FTD Version 6.7+ using the FTD upgrade wizard 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.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Upgrade different device models together.	7.0.0	Any	You can now use the FTD upgrade wizard to queue and invoke upgrades for all FTD models at the same time, as long as the system has access to the appropriate upgrade packages. Previously, you would choose an upgrade package, then choose the devices to upgrade using that package. That meant that you could upgrade multiple devices at the same time *only* if they shared an upgrade package. For example, you could upgrade two Firepower 2100 series devices at the same time, but not a Firepower 2100 series and a Firepower 1000 series.
Upgrades remove PCAP files to save disk space.	6.7.0	6.7.0	Upgrades now remove locally stored PCAP files. To upgrade, you must have enough free disk space or the upgrade fails.
Improved FTD upgrade status reporting and cancel/retry options.	6.7.0	6.7.0	You can now view the status of FTD device upgrades and readiness checks in progress on the Device Management page, as well as a 7-day history of upgrade success/failures. The Message Center also provides enhanced status and error messages. A new Upgrade Status pop-up, accessible from both Device Management and the Message Center with a single click, shows detailed upgrade information, including percentage/time remaining, specific upgrade stage, success/failure data, upgrade logs, and so on. Also on this pop-up, you can manually cancel failed or in-progress upgrades (**Cancel Upgrade**), or retry failed upgrades (**Retry Upgrade**). Canceling an upgrade reverts the device to its pre-upgrade state. **Note** To be able to manually cancel or retry a failed upgrade, you must disable the new auto-cancel option, which appears when you use the FMC to upgrade an FTD device: **Automatically cancel on upgrade failure and roll back to the previous version**. With the option enabled, the device automatically reverts to its pre-upgrade state upon upgrade failure. Auto-cancel is not supported for patches. In an HA or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. New/modified screens: • **System** > **Updates** > **Product Updates** > **Available Updates** > **Install** icon for the FTD upgrade package • **Devices** > **Device Management** > **Upgrade** • **Message Center** > **Tasks** New/modified CLI commands: **show upgrade status detail**, **show upgrade status continuous**, **show upgrade status**, **upgrade cancel**, **upgrade retry**

Feature	Minimum Management Center	Minimum Threat Defense	Details
Get FTD upgrade packages from an internal web server.	6.6.0	6.6.0	FTD devices can now get upgrade packages from your own internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC. **Note** This feature is supported only for FTD devices running Version 6.6+. It is not supported for upgrades *to* Version 6.6, nor is it supported for the FMC or Classic devices. New/modified screens: We added a **Specify software update source** option to the page where you upload upgrade packages.
Copy upgrade packages to managed devices before the upgrade.	6.2.3	Any	You can now copy (or push) an upgrade package from the FMC to a managed device before you run the actual upgrade. This is useful because you can push during times of low bandwidth use, outside of the upgrade maintenance window. When you push to high availability, clustered, or stacked devices, the system sends the upgrade package to the active/control/primary first. Then, it sends the package to the standby/data/secondary. New/modified screens: **System** > **Updates**

Table 30: Firewall Management Center Upgrade Feature History

Feature	Minimum Management Center	Minimum Threat Defense	Details
Specify how long the system retries failed upgrade package downloads.	10.0.0	Any	New global upgrade settings allow you to specify how long the system retries failed upgrade package downloads. This includes downloads from the internet to the Firewall Management Center. New/modified screens: **Administration** > **Product Upgrades** > **Global upgrade settings**
Auto-replace outdated Firewall Management Center upgrade scripts.	7.6.5 10.0.0	Any	The Firewall Management Center can get new upgrade scripts for itself from the internet, fixing late-breaking upgrade issues without replacing the whole upgrade package. If the Firewall Management Center cannot download new scripts for any reason, the upgrade proceeds as it would have without them. If you encounter issues with Firewall Management Center upgrade, including a failed upgrade or unresponsive system, contact Cisco TAC. Download location: cdo-ftd-images.s3-us-west-2.amazonaws.com

Feature	Minimum Management Center	Minimum Threat Defense	Details
Skip post-upgrade deploy for Firewall Management Center.	7.7.0	Any	In many cases, you no longer have to deploy to Snort 3 devices after you upgrade the Firewall Management Center. If deploy is required, affected devices are marked out of date (with a few exceptions). Reasons for needing to manually deploy include: • The upgrade updated the LSP and scheduled LSP updates are off. • The upgrade updated the LSP and scheduled LSP updates are on, but automatic redeploy is off. Devices may not be marked out of date in this case. Note that if automatic redeploy is on, the redeploy will take place on schedule and you do not need to do it manually. • Specific configurations changed by the upgrade require a deploy. • You need to upgrade managed devices immediately. After Firewall Management Center upgrade, you cannot upgrade managed devices until you redeploy, even if they are not marked out of date.
SRU update moved out of Firewall Management Center upgrade.	7.7.0	Any	**Upgrade impact. After Firewall Management Center upgrades to Version 7.7+, wait for SRU to install.** Instead of upgrading the SRU as part of the upgrade, the system now updates intrusion rules for Snort 2 devices (the *SRU*) after the upgrade completes and the Firewall Management Center reboots. Although this makes the upgrade itself faster, you cannot update intrusion rules, add devices, or deploy configuration changes while the SRU is updating. This occurs regardless of whether you are managing any Snort 2 devices.
Upgrade Firewall Management Center without a manual readiness check.	7.7.0	Any	You no longer have to run time-consuming pre-upgrade readiness checks for Firewall Management Center upgrades. Instead, these checks are now regularly run by the system and reported in the health monitor. This allows you to preemptively fix any issues that will block upgrade. Version restrictions: This feature is supported for upgrades *from* Version 7.7+.

Feature	Minimum Management Center	Minimum Threat Defense	Details
Improved upgrade process for high availability Firewall Management Centers.	7.6.0	Any	Upgrading high availability Firewall Management Centers is now easier: • You no longer have to manually copy the upgrade package to both peers. Depending on your setup, you can have each peer get the package from the support site, or you can copy the package between peers. • You no longer have to manually run the readiness check on both peers. Running it on one runs it on both. • If you do not have enough disk space to run the upgrade, a new **Clean Up Disk Space** option can help. • You no longer have to manually pause synchronization before upgrade, or resolve split brain after the upgrade; the system now does this automatically. Also, your original active/standby roles are preserved. Note that although you can complete most of the upgrade process from one peer (we recommend the standby), you do have to log into the second peer to actually initiate its upgrade. New/modified screens: **System** (⚙) > **Product Upgrades** Version restrictions: This feature applies to upgrades *from* Version 7.6.0 and later, not *to* 7.6.0.
Automatically generate configuration change reports after Firewall Management Center upgrade.	7.4.1	Any	You can automatically generate reports on configuration changes after major and maintenance Firewall 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. Version restrictions: Only supported for Firewall Management Center upgrades from Version 7.4.1+. Not supported for upgrades to Version 7.4.1 or any earlier version. New/modified screens: **System** > **Configuration** > **Upgrade Configuration** > **Enable Post-Upgrade Report**
Deprecated: Scheduled software upgrades.	7.3.0	Any	**Upgrade impact. Scheduled software upgrade tasks stop working.** The **Download Latest Update**, **Push Latest Update**, and **Install Latest Update** scheduled tasks are no longer supported for software updates, although the web interface allows configuration. (Exception: Version 7.3.1.2) You can still use the **Download Latest Update** and **Install Latest Update** tasks to schedule VDB updates.
Hotfix high availability Firewall Management Centers without pausing synchronization.	7.2.6 7.4.1	Any	Unless otherwise indicated by the hotfix release notes or Cisco TAC, you do not have to pause synchronization to install a hotfix on high availability Firewall Management Centers.

Feature	Minimum Management Center	Minimum Threat Defense	Details
New upgrade wizard for the Firewall Management Center.	7.2.6 7.4.1	Any	A new upgrade starting page and wizard make it easier to perform Firewall Management Center upgrades. After you use **System**(⚙) > **Product Upgrades** to get the appropriate upgrade package onto the Firewall Management Center, click **Upgrade** to begin. Version restrictions: Only supported for Firewall Management Center upgrades from Version 7.2.6+/7.4.1+. Not supported for upgrades from Version 7.3.x or 7.4.0. See: Secure Firewall Threat Defense upgrade guides for Firewall Management Center
Updated internet access requirements for direct-downloading software upgrades.	7.2.6 7.4.1	Any	**Upgrade impact. The system connects to new resources.** The Firewall Management Center has changed its direct-download location for software upgrade packages from sourcefire.com to amazonaws.com.
Improved upgrade starting page and package management.	7.2.6 7.4.1	Any	See Improved upgrade starting page and package management.
Suggested release notifications.	7.2.6 7.4.1	Any	See Suggested release notifications.
Firewall Management Center upgrade does not automatically generate troubleshooting files.	7.2.0	Any	To save time and disk space, the Firewall Management Center upgrade process no longer automatically generates troubleshooting files before the upgrade begins. Note that device upgrades are unaffected and continue to generate troubleshooting files. To manually generate troubleshooting files for the Firewall Management Center, choose **System**(⚙) > **Health** > **Monitor**, click **Firewall Management Center** in the left panel, then **View System & Troubleshoot Details**, then **Generate Troubleshooting Files**.
Upgrades postpone scheduled tasks.	6.4.0	Any	The Firewall Management Center upgrade process now postpones scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. **Note** Before you begin any upgrade, you must still make sure running tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Note that this feature is supported for all upgrades *from* a supported version. This includes Version 6.4.0.10 and later patches, Version 6.6.3 and later maintenance releases, and Version 6.7.0+. This feature is not supported for upgrades *to* a supported version from an unsupported version.