

Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.2.0–7.2.5

First Published: 2022-06-06

Last Modified: 2026-07-30

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

© 2022–2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1 **Getting Started** 1

Is this Guide for You? 1

Planning Your Upgrade 3

Upgrade Feature History 5

For Assistance 10

CHAPTER 2 **System Requirements** 13

Firewall Management Center Platforms 13

Firewall Threat Defense Platforms 14

Firewall Threat Defense Management 16

CHAPTER 3 **Software Upgrade Guidelines** 19

Minimum Version to Upgrade 19

Upgrade Guidelines for Version 7.2 20

Extended Post-Upgrade Deploy to Version 7.2.4–7.2.5 for Large Configurations 21

Reconnect with Cisco Secure Malware Analytics for High Availability Firewall Management Centers 21

Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs 22

Upgrade Guidelines for Cloud-Delivered Firewall Management Center 22

Unresponsive Upgrades 22

Traffic Flow and Inspection for Firewall Threat Defense Upgrades 23

Traffic Flow and Inspection when Deploying Configurations 25

Time and Disk Space 26

CHAPTER 4 **Upgrade the Firewall Management Center** 29

Upgrade Checklist for Firewall Management Center 29

Upgrade Path for Firewall Management Center 32
Upload Upgrade Packages for Firewall Management Center 35
Run Readiness Checks for Firewall Management Center 36
Upgrade the Firewall Management Center: Standalone 36
Upgrade the Firewall Management Center: High Availability 37

CHAPTER 5 **Upgrade Firewall Threat Defense** 39
Upgrade Checklist for Firewall Threat Defense 39
Upgrade Paths for Firewall Threat Defense 43
Upgrade Path for Firewall Threat Defense without FXOS 44
Upgrade Path for Firewall Threat Defense with FXOS 46
Upgrade Order for Firewall Threat Defense High Availability/Scalability with FXOS 49
Upgrade Packages for Firewall Management Center and Firewall Threat Defense 49
Upload Firewall Threat Defense Upgrade Packages to the Firewall Management Center 50
Upload Firewall Threat Defense Upgrade Packages to an Internal Server 51
Copy Firewall Threat Defense Upgrade Packages between Devices 52
Upgrade Firewall Threat Defense with the Wizard (Disable Revert) 53
Upgrade Firewall Threat Defense with System > Updates (Enable Revert) 57

CHAPTER 6 **Upgrade the Chassis on the Firepower 4100/9300** 61
Upgrade Packages for FXOS 61
Upgrade Guidelines for the Firepower 4100/9300 Chassis 61
Traffic Flow and Inspection for Chassis Upgrades 62
Upgrade Paths for FXOS 63
Upgrade Path for FXOS with Firewall Threat Defense 63
Upgrade Path for FXOS with Firewall Threat Defense and ASA 65
Upgrade Order for FXOS with Firewall Threat Defense High Availability/Scalability 68
Upgrade FXOS with Firewall Chassis Manager 69
Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using Firepower Chassis Manager 69
Upgrade FXOS on an FTD Inter-chassis Cluster Using Firepower Chassis Manager 70
Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager 73
Upgrade FXOS with the CLI 76

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using the FXOS CLI 76

Upgrade FXOS on an FTD Inter-chassis Cluster Using the FXOS CLI 78

Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI 82

CHAPTER 7 **Revert or Uninstall the Upgrade 87**

Revert Firewall Threat Defense 87

About Reverting Firewall Threat Defense 87

Guidelines for Reverting Firewall Threat Defense 88

Revert Firewall Threat Defense with Firewall Management Center 90

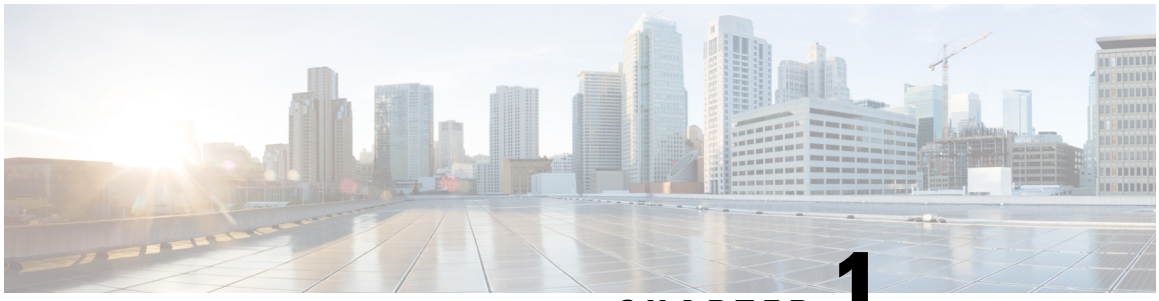
Uninstall a Patch 91

Uninstall Order for High Availability/Scalability 91

Uninstall Threat Defense Patches 92

Uninstall Standalone Firewall Management Center Patches 94

Uninstall High Availability Firewall Management Center Patches 95



CHAPTER 1

Getting Started

- Is this Guide for You?, on page 1
- Planning Your Upgrade, on page 3
- Upgrade Feature History, on page 5
- For Assistance, on page 10

Is this Guide for You?

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

- Upgrade of currently managed Firewall Threat Defense devices *as far as* Version 7.2.
- Upgrade of the Firewall Management Center to releases *after* Version 7.2.

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

Additional Resources

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

Table 1: Upgrade Guides for Firewall Management Center

Current Firewall Management Center Version	Guide
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1
7.0 or earlier	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*

Table 2: Upgrade Guides for Firewall Threat Defense with Firewall Management Center

Current Firewall Management Center Version	Guide
Cloud-Delivered Firewall Management Center	Secure Firewall Threat Defense upgrade guides for Cloud-Delivered Firewall Management Center
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version
7.1	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center, Version 7.1
7.0 or earlier	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*

Table 3: Upgrade Guides for Firewall Threat Defense with Firewall Device Manager

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

Table 4: Upgrade Guides for NGIPS

Platform	Current Manager Version	Guide
Firepower 7000/8000 series with Firewall Management Center	6.0.0–7.0.x	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*

Platform	Current Manager Version	Guide
NGIPSv with Firewall Management Center	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*
	7.2.6–7.2.x 7.4.1–7.4.x	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version
ASA FirePOWER with Firewall Management Center	6.0.0–7.1.x 7.2.0–7.2.5 7.3.x 7.4.0	*Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*
	7.2.6–7.2.x 7.4.1–7.4.x	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version
ASA FirePOWER with ASDM	Any	*Cisco Secure Firewall ASA Upgrade Guide*

Table 5: Upgrade Other Components

Version	Component	Guide
Any	ASA logical devices on the Firepower 4100/9300	*Cisco Secure Firewall ASA Upgrade Guide*
Latest	BIOS and firmware for Firewall Management Center	Secure Firewall Threat Defense/Firepower hotfix release notes
Latest	Firmware for the Firepower 4100/9300	*Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*
Latest	ROMMON image for the ISA 3000	*Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*

Planning Your Upgrade

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

Table 6: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up configurations and events. Back up FXOS on the Firepower 4100/9300.
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

Upgrade Feature History

Table 7: Device Upgrade Feature History

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 8: Firewall Management Center Upgrade Feature History

Feature	Minimum Management Center	Minimum Threat Defense	Details
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**.

Feature	Minimum Management Center	Minimum Threat Defense	Details
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.

For Assistance

Upgrade Guides

In Firewall Management Center deployments, the Firewall Management Center must run the same or newer maintenance (third-digit) release as its managed devices. Upgrade the Firewall Management Center first, then devices. Use the upgrade guide for the version you are *currently* running—not your target version.

Table 9: Upgrade Guides

Platform	Upgrade Guide	Link
Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/fmc-upgrade
Firewall Threat Defense with Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/ftd-fmc-upgrade
Firewall Threat Defense with device manager	Firewall Threat Defense version you are *currently* running.	https://cisco.com/go/ftd-fdm-upgrade
Firewall Threat Defense with Cloud-Delivered Firewall Management Center	Cloud-Delivered Firewall Management Center.	https://cisco.com/go/ftd-cdfmc-upgrade

Install Guides

If you cannot or do not want to upgrade, you can freshly install major and maintenance releases. This is also called *reimaging*. You cannot reimage to a patch. Install the appropriate major or maintenance release, then apply the patch. If you are reimaging to an earlier Firewall Threat Defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 10: Install Guides

Platform	Install Guide	Link
Firewall Management Center hardware	Getting started guide for your Firewall Management Center hardware model.	https://cisco.com/go/fmc-install
Firewall Management Center Virtual	Getting started guide for the Firewall Management Center Virtual.	https://cisco.com/go/fmcv-quick
Firewall Threat Defense hardware	Getting started or reimage guide for your device model.	https://cisco.com/go/ftd-quick
Firewall Threat Defense Virtual	Getting started guide for your Firewall Threat Defense Virtual version.	https://cisco.com/go/ftdv-quick
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://cisco.com/go/firepower9300-config
FXOS for the Firepower 1000/2100 and Secure Firewall 3100	Troubleshooting guide, in the *Reimage Procedures* chapter.	*Cisco FXOS Troubleshooting Guide for the Firewall Threat Defense*

More Online Resources

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

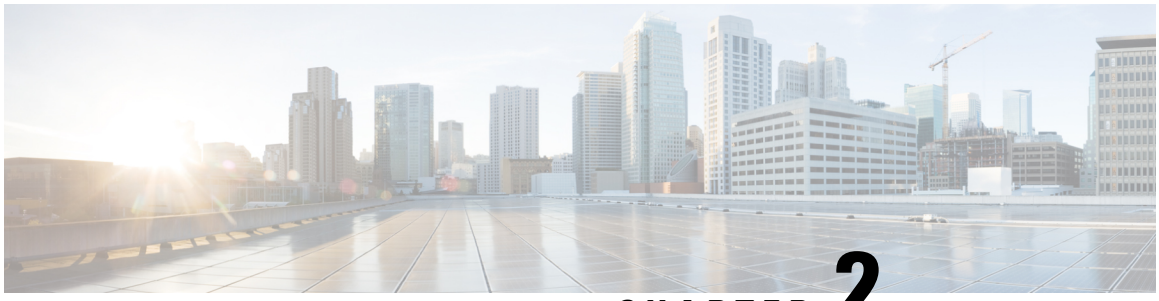
- Documentation: https://cisco.com/go/threatdefense-72-docs
- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://cisco.com/cisco/support/notifications.html

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

Contact Cisco

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

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



CHAPTER 2

System Requirements

This document includes the system requirements for Version 7.2.

- Firewall Management Center Platforms, on page 13
- Firewall Threat Defense Platforms, on page 14
- Firewall Threat Defense Management, on page 16

Firewall Management Center Platforms

The Firewall Management Center provides a centralized firewall management console. For device compatibility with the Firewall Management Center, see Firewall Threat Defense Management, on page 16. For general compatibility information, see the *Cisco Secure Firewall Management Center Compatibility Guide*.

Firewall Management Center Hardware

Version 7.2 supports the following Firewall Management Center hardware:

- Firepower Management Center 1600
- Firepower Management Center 2600
- Firepower Management Center 4600

You should also keep the BIOS and RAID controller firmware up to date; see the Secure Firewall Threat Defense/Firepower hotfix release notes.

Firewall Management Center Virtual

Version 7.2 supports Firewall Management Center Virtual deployments in both public and private clouds.

With the Firewall Management Center Virtual, you can purchase a license to manage 2, 10, or 25 devices. Some platforms support 300 devices. Note that two-device licenses do not support Firewall Management Center high availability. For full details on supported instances, see the *Cisco Secure Firewall Management Center Virtual Getting Started Guide*.

Table 11: Version 7.2 Firewall Management Center Virtual Platforms

Platform	Devices Managed		High Availability
	2, 10, 25	300	
Public Cloud			
Alibaba	YES	—	—
Amazon Web Services (AWS)	YES	YES	YES
Google Cloud Platform (GCP)	YES	—	—
Microsoft Azure	YES	—	—
Oracle Cloud Infrastructure (OCI)	YES	YES	YES
Private Cloud			
Cisco HyperFlex	YES	—	YES
Kernel-based virtual machine (KVM)	YES	—	—
Nutanix Enterprise Cloud	YES	—	—
OpenStack	YES	—	—
VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0	YES	YES	YES

Cloud-Delivered Firewall Management Center

is delivered via Security Cloud Control, which unites management across multiple Cisco security solutions. We take care of feature updates. Note that a customer-deployed Firewall Management Center is referred to as *on-prem*, even for public cloud deployments.

For up-to-date compatibility information, see the *Cisco Secure Firewall Management Center Compatibility Guide*.

Firewall Threat Defense Platforms

Threat defense devices monitor network traffic and decide whether to allow or block specific traffic based on a defined set of security rules. For details on device management methods, see Firewall Threat Defense Management, on page 16. For general compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Firewall Threat Defense Hardware

Version 7.2 Firewall Threat Defense hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 12: Version 7.2 Firewall Threat Defense Hardware

Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility		Notes
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO	
Firepower 1010E, 1010, 1120, 1140, 1150	YES	YES	YES	YES	Firepower 1010E requires Version 7.2.3+. Do not use a Version 7.2.3 or Version 7.3.0 Firewall Management Center to manage the Firepower 1010E. Instead, use a Version 7.2.3.1+ or Version 7.3.1.1+ Firewall Management Center.
Firepower 2110, 2120, 2130, 2140	YES	YES	YES	YES	—
Secure Firewall3110, 3120, 3130, 3140	YES	YES	YES	YES	—
Firepower 4110, 4120, 4140, 4150 Firepower 4112, 4115, 4125, 4145 Firepower 9300: SM-24, SM-36, SM-44 modules Firepower 9300: SM-40, SM-48, SM-56 modules	YES	YES	YES	YES	Requires FXOS 2.12.1.95 or later build. We recommend the latest firmware. See the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.
ISA 3000	YES	YES	YES	YES	May require a ROMMON update. See the *Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide*.

Firewall Threat Defense Virtual

Version 7.2 Firewall Threat Defense Virtual implementations support performance-tiered Smart Software Licensing, based on throughput requirements and remote access VPN session limits. Options run from FTDv5 (100 Mbps/50 sessions) to FTDv100 (16 Gbps/10,000 sessions). For more information on supported instances, throughputs, and other hosting requirements, see the appropriate *Getting Started Guide*.

Table 13: Version 7.2 Firewall Threat Defense Virtual Platforms

Device Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility	
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	YES	YES	YES
Microsoft Azure	YES	YES	YES	YES
Google Cloud Platform (GCP)	YES	YES	YES	YES
Oracle Cloud Infrastructure (OCI)	YES	YES	—	—
Private Cloud				
Cisco Hyperflex	YES	YES	YES	YES
Kernel-based virtual machine (KVM)	YES	YES	YES	YES
Nutanix Enterprise Cloud	YES	YES	YES	YES
OpenStack	YES	YES	—	—
VMware vSphere/VMware ESXi 6.5, 6.7, or 7.0	YES	YES	YES	YES

Firewall Threat Defense Management

Depending on device model and version, we support the following management methods.

On-Prem Firewall Management Center

All devices support remote management with a customer-deployed (*on-prem*) Firewall Management Center.

Versions are major (A.x), maintenance (A.x.y), or patch (A.x.y.z). The Firewall Management Center should run the same or newer version as its devices. New features and resolved issues often require the latest version on both the Firewall Management Center and its devices. Upgrade the Firewall Management Center first—you will still be able to manage older devices, usually a few major versions back.

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.

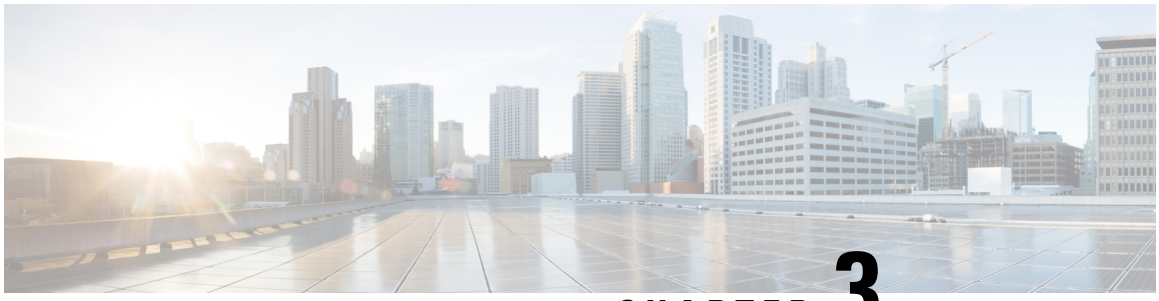
Note that in most cases you can upgrade an older device directly to the Firewall Management Center's major or maintenance version. However, sometimes you can manage an older device that you cannot directly upgrade, even though the target version is supported on the device. Rarely, there are issues with specific Firewall Management Center-device combinations. For release-specific requirements, see the release notes.

Table 14: On-Prem Firewall Management Center-Device Compatibility

Firewall Management Center Version	Oldest Device Version You Can Manage
10.x	7.3
7.7	7.2
7.6	7.1
7.4 Last support for NGIPS device management.	7.0
7.3	6.7
7.2	6.6
7.1	6.5
7.0	6.4
6.7	6.3
6.6	6.2.3
6.4	6.1
6.2.3	6.1

Cloud-Delivered Firewall Management Center

For Firewall Threat Defense compatibility with Cloud-Delivered Firewall Management Center, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.



CHAPTER 3

Software Upgrade Guidelines

For your convenience, this document duplicates the critical and release-specific software upgrade guidelines published in the Firewall Threat Defense release notes. For FXOS upgrade guidelines for the Firepower 4100/9300, see Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 61.

Important You must still read the release notes, which can contain additional critical and version-specific information. For example, new and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. Or, known issues (open bugs) can affect upgrade.

- Minimum Version to Upgrade, on page 19
- Upgrade Guidelines for Version 7.2, on page 20
- Upgrade Guidelines for Cloud-Delivered Firewall Management Center, on page 22
- Unresponsive Upgrades, on page 22
- Traffic Flow and Inspection for Firewall Threat Defense Upgrades, on page 23
- Traffic Flow and Inspection when Deploying Configurations, on page 25
- Time and Disk Space, on page 26

Minimum Version to Upgrade

Minimum Version to Upgrade

You can upgrade directly to Version 7.2, including maintenance releases, as follows.

Table 15: Minimum Version to Upgrade to Version 7.2

Platform	Minimum Version
Firewall Management Center	6.6
Firewall Threat Defense (except Threat Defense Virtual with GCP)	6.6 FXOS 2.12.1.95 is required for the Firepower 4100/9300. In most cases, we recommend you use the latest FXOS build in each major version. To help you decide, see the Cisco Firepower 4100/9300 FXOS Release Notes, 2.12.

Platform	Minimum Version
Threat Defense Virtual with GCP	7.2 You cannot upgrade to Version 7.2+ from Version 7.1 and earlier; you must deploy a new instance. The mininum version to upgrade to a Version 7.2.x maintenance release is Version 7.2.0.

Minimum Version to Patch

Patches change the fourth digit *only*. You cannot upgrade directly to a patch from a previous major or maintenance release.

Upgrade Guidelines for Version 7.2

These checklists provide new and/or previously published upgrade guidelines that may apply to you.

Table 16: Upgrade Guidelines for Firewall Threat Defense with Firewall Management Center Version 7.2

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 19	Any	Any	Any
	Cisco Secure Firewall Management Center New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	Secure Firewall Threat Defense release notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Upgrade Guidelines for Cloud-Delivered Firewall Management Center, on page 22	Firewall Threat Defense	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 61	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Extended Post-Upgrade Deploy to Version 7.2.4–7.2.5 for Large Configurations, on page 21	Firewall Management Center	6.6.0+	7.2.4 through 7.2.5

✓	Guideline	Platforms	Upgrading From	Directly To
	Reconnect with Cisco Secure Malware Analytics for High Availability Firewall Management Centers, on page 21	Firewall Management Center	6.4.0 through 6.7.x	7.0+
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 22	Firepower 1010	6.4.0 through 6.6.x	6.7+

Extended Post-Upgrade Deploy to Version 7.2.4–7.2.5 for Large Configurations

Deployment: Firewall Management Center

Upgrading from: Any deployment where object optimization is disabled.

Directly to: Version 7.2.4-7.2.5

Access control object optimization improves performance and consumes fewer device resources when you have access control rules with overlapping networks. The optimizations occur on the *managed device* on the first deploy after the feature is enabled on the Firewall Management Center (including if it is enabled by an upgrade). If you have a high number of rules, the system can take several minutes to an hour to evaluate your policies and perform object optimization. During this time, you may also see higher CPU use on your devices. A similar thing occurs on the first deploy after the feature is disabled (including if it is disabled by upgrade). After this feature is enabled or disabled, we recommend you deploy when it will have the least impact, such as a maintenance window or a low-traffic time.

To plan, use the following table.

Table 17: Planning Firewall Management Center Upgrades with Object Optimization

Version	Default/Reimage Setting	Upgrading	To Enable/Disable
7.0.5 and earlier	Not supported (disabled).	—	—
7.0.6 and later maint. releases	Disabled.	Respects your current setting.	Contact Cisco TAC.
7.1.0–7.2.3	Not supported (disabled).	Disables.	—
7.2.4–7.2.5	Enabled.	Enables.	Contact Cisco TAC.
7.3.x	Not supported (disabled).	Disables.	—
7.4.0	Enabled.	Enables.	Contact Cisco TAC.

Reconnect with Cisco Secure Malware Analytics for High Availability Firewall Management Centers

Deployments: High availability/AMP for Networks (malware detection) deployments where you submit files for dynamic analysis

Upgrading from: Version 6.4.0 through 6.7.x

Directly to: Version 7.0.0+

Related bug: CSCvu35704

Version 7.0.0 fixes an issue with high availability where, after failover, the system stopped submitting files for dynamic analysis. For the fix to take effect, you must reassociate with the Cisco Secure Malware Analytics public cloud.

After you upgrade the high availability pair, on the primary Firewall Management Center:

1. Choose **AMP** > **Dynamic Analysis Connections**.
2. Click **Associate** in the table row corresponding to the public cloud.

   A portal window opens. You do not have to sign in. The reassociation happens in the background, within a few minutes.

Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs

Deployments: Firepower 1010

Upgrading from: Version 6.4 through 6.6

Directly to: Version 6.7+

For the Firepower 1010, Firewall Threat Defense upgrades to Version 6.7+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

Upgrade Guidelines for Cloud-Delivered Firewall Management Center

You do not upgrade the Cloud-Delivered Firewall Management Center. We take care of feature updates. To upgrade Firewall Threat Defense with the Cloud-Delivered Firewall Management Center, see the Secure Firewall Threat Defense upgrade guides for Cloud-Delivered Firewall Management Center.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down during upgrade. You could place the system in an unusable state and require a reimage.

Unresponsive Firewall Management Center Upgrade

Do not restart an upgrade in progress. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Unresponsive Firewall Threat Defense Upgrade

For major and maintenance upgrades, you can manually cancel failed or in-progress upgrades, and retry failed upgrades. On the Firewall Management Center, use the Upgrade Status pop-up, accessible from the Upgrade

tab on the Device Management page, and from the Message Center. You can also use the Firewall Threat Defense CLI.

Note By default, Firewall Threat Defense automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to manually cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Auto-cancel is not supported for patches. 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.

This feature is not supported for patches or for upgrades from Version 6.6 and earlier.

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 18: 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/Scalability

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.

Deploying Configuration Changes

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.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Table 19: 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.

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 20: 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.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled.	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled.	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled.	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Time and Disk Space

Time to Upgrade

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

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades, on page 22.

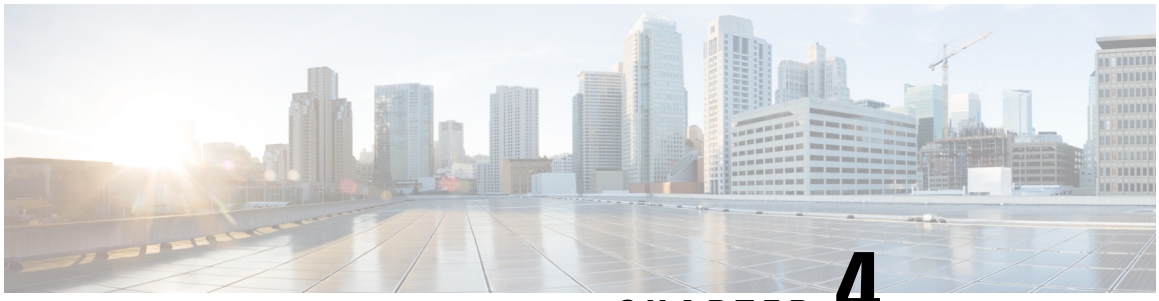
Table 21: Upgrade Time Considerations

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.
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.

Consideration	Details
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, 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.



CHAPTER 4

Upgrade the Firewall Management Center

This chapter explains how to upgrade an on-prem Firewall Management Center that is *currently running* Version 7.20–7.2.5.

- Upgrade Checklist for Firewall Management Center, on page 29
- Upgrade Path for Firewall Management Center, on page 32
- Upload Upgrade Packages for Firewall Management Center, on page 35
- Run Readiness Checks for Firewall Management Center, on page 36
- Upgrade the Firewall Management Center: Standalone, on page 36
- Upgrade the Firewall Management Center: High Availability, on page 37

Upgrade Checklist for Firewall Management Center

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

✓	Action/Check	Details
	Assess your deployment.	Understanding where you are determines how you get to where you want to go. In addition to current version and model information, determine if your deployment is configured for high availability/scalability, if your devices are deployed as an IPS or as firewalls, and so on.
	Plan your upgrade path.	This is especially important for large deployments, multi-hop upgrades, and situations where you need to upgrade operating systems or hosting environments. Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. See: • Upgrade Path for Firewall Management Center, on page 32 • Upgrade Paths for Firewall Threat Defense, on page 43 • Upgrade Paths for FXOS, on page 63

✓	Action/Check	Details
	Read upgrade guidelines and plan configuration changes.	Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with these: • Software Upgrade Guidelines, on page 19, for critical and release-specific upgrade guidelines. • *Cisco Secure Firewall Management Center New Features by Release*, for new and deprecated features that have upgrade impact. Check all versions between your current and target version. • Secure Firewall Threat Defense release notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool. • Firepower 4100/9300 FXOS release notes, for FXOS upgrade guidelines for the Firepower 4100/9300.
	Check bandwidth.	Make sure your management network has the bandwidth to perform large data transfers. Whenever possible, upload upgrade packages ahead of time.
	Schedule maintenance windows.	Schedule maintenance windows when they will have the least impact, especially considering the time the upgrade is likely to take. Consider the tasks you must perform in the window, and those you can perform ahead of time. SeeTime and Disk Space Tests.

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 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.

✓	Action/Check	Details
	Back up configurations and events.	See the *Backup/Restore* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

Upgrade Packages

Uploading upgrade packages to the system before you begin upgrade can reduce the length of your maintenance window.

✓	Action/Check	Details
	Download the upgrade package from Cisco and upload it to the Firewall Management Center.	Upgrade packages are available on the Cisco Support & Download site. You may also be able to use the Firewall Management Center to perform a direct download. For Firewall Management Center high availability, you must upload the Firewall Management Center upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization. See Upload Upgrade Packages for Firewall Management Center, on page 35.

Associated Upgrades

We recommend you perform hosting environment upgrades in a maintenance window.

✓	Action/Check	Details
	Upgrade virtual hosting.	If needed, upgrade the hosting environment. If this is required, it is usually because you are running an older version of VMware and are performing a major upgrade.

Final Checks

A set of final checks ensures you are ready to upgrade the software.

✓	Action/Check	Details
	Check configurations.	Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.
	Check NTP synchronization.	Make sure all appliances are synchronized with any NTP server you are using to serve time. Although the health monitor alerts if clocks are out of sync by more than 10 seconds, you should still check manually. Being out of sync can cause upgrade failure. To check time: • Firewall Management Center: Choose **System** (⚙) > **Configuration** > **Time**. • Firewall Threat Defense: Use the **show time** CLI command.

✓	Action/Check	Details
	Deploy configurations.	Deploying configurations before you upgrade reduces the chance of failure. Deploying can affect traffic flow and inspection; see Traffic Flow and Inspection for Firewall Threat Defense Upgrades, on page 23.
	Run readiness checks.	Passing readiness checks reduces the chance of upgrade failure. See Run Readiness Checks for Firewall Management Center, on page 36.
	Check disk space.	Readiness checks include a disk space check. Without enough free disk space, the upgrade fails. To check the disk space available on the Firewall Management Center, choose **System** (⚙) > **Monitoring** > **Statistics** and select the Firewall Management Center. Under Disk Usage, expand the By Partition details.
	Check running tasks.	Make sure essential tasks are complete, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Upgrades from Version 6.6.3+ automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. If you do not want this to happen (or if you are upgrading from an earlier version), check for tasks that are scheduled to run during the upgrade and cancel or postpone them.

Upgrade Path for Firewall Management Center

This table provides the upgrade path for customer-deployed Firewall Management Centers.

Upgrade the Firewall Management Center first. 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.

Note that if your current Firewall Threat Defense/Firewall Management Center version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

Table 22: Firewall Management Center Direct Upgrades

Current Version	Target Version
7.4	→ Any later 7.4.x release

Current Version	Target Version
7.3	Any of: → 7.4.x → Any later 7.3.x release
7.2	Any of: → 7.4.x → 7.3.x → Any later 7.2.x release
7.1	Any of: → 7.4.x → 7.3.x → 7.2.x → Any later 7.1.x release
7.0 Last support for FMC 1000, 2500, and 4500.	Any of: → 7.4.x → 7.3.x → 7.2.x → 7.1.x → Any later 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+.
6.7	Any of: → 7.2.x → 7.1.x → 7.0.x → Any later 6.7.x release

Current Version	Target Version
6.6 Last support for FMC 2000 and 4000.	Any of: → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Any later 6.6.x release **Note** Due to datastore incompatibilities, you cannot upgrade the Firewall Management Center from Version 6.6.5+ to Version 6.7.0. We recommend you upgrade directly to Version 7.0+.
6.5	Any of: → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 Last support for FMC 750, 1500, and 3500.	Any of: → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Any of: → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3	Any of: → 6.6.x → 6.5 → 6.4 → 6.3

Upload Upgrade Packages for Firewall Management Center

Use this procedure to manually upload upgrade packages to the Firewall Management Center.

Tip Select upgrade packages become available for direct download some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors. If the Firewall Management Center has internet access, you can click the **Download Updates** button to immediately download the latest VDB, latest maintenance release, and the latest critical patches for the Firewall Management Center and all managed devices.

Upgrade packages are signed tar archives (.tar). After you upload a signed package, the System Updates page on the Firewall Management Center can take extra time to load as the package is verified. To speed up the display, delete unneeded upgrade packages. Do not untar signed packages.

Before you begin

If you are upgrading the standby Firewall Management Center in a high availability pair, pause synchronization.

For Firewall Management Center high availability, you must upload the Firewall Management Center upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization.

Procedure

Step 1 Download the upgrade package from the Cisco Support & Download site: https://www.cisco.com/go/firepower-software.

You use the same software 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, package type (upgrade, patch, hotfix), software version, and build, like this:

```
Cisco_Secure_FW_Mgmt_Center_Upgrade-7.2-999.sh.REL.tar
```

Step 2 On the Firewall Management Center, choose **System** (⚙) > **Updates**.

Step 3 Click **Upload Update**.

Step 4 For the **Action**, click the **Upload local software update package** radio button.

Step 5 Click **Choose File**.

Step 6 Browse to the package and click **Upload**.

Run Readiness Checks for Firewall Management Center

Use this procedure to run Firewall Management Center readiness checks.

Readiness checks assess preparedness for major and maintenance upgrades. If you fail readiness checks, you cannot upgrade until you correct the issues. The time required to run a readiness check varies depending on model and database size. Do not manually reboot or shut down during readiness checks.

Before you begin

Upload the upgrade package to the Firewall Management Center.

Procedure

Step 1 On the Firewall Management Center, choose **System** (⚙) > **Updates**.

Step 2 Under Available Updates, click the **Install** icon next to the upgrade package, then choose the Firewall Management Center.

Step 3 Click **Check Readiness**.

You can monitor readiness check progress in the Message Center.

What to do next

On **System** (⚙) > **Updates**, click **Readiness Checks** to view readiness check status for your whole deployment, including checks in progress and failed checks. You can also use this page to easily re-run checks after a failure.

Upgrade the Firewall Management Center: Standalone

Use this procedure to upgrade a standalone Firewall Management Center.

⚠

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

Complete upgrade planning. Make sure your deployment is healthy and successfully communicating.

Procedure

Step 1 On the Firewall Management Center, choose **System** (⚙) > **Updates**.

Step 2 Under Available Updates, click the **Install** icon next to the upgrade package, then choose the Firewall Management Center.

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

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

Step 4 Log back in when you can.

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

Step 5 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 6 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.

Step 7 Complete any required post-upgrade configuration changes.

Step 8 Redeploy configurations to all managed devices.

Upgrade the Firewall Management Center: High Availability

Upgrade high availability Firewall Management Centers one at a time. With synchronization paused, upgrade the standby. When the standby upgrade completes Firewall Management Center comes back up as active, which allows you to upgrade the other Firewall Management Center. This temporary state is called *split-brain* and is not supported except during upgrade (and patch uninstall). Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after synchronization restarts; deploying could place the system in an unusable state and require a reimage.

⚠

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

Complete the pre-upgrade checklist for both peers. Make sure your deployment is healthy and successfully communicating.

Procedure

Step 1 On the active Firewall Management Center, pause synchronization.

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

Step 2 Upload the upgrade package to the standby.

For Firewall Management Center high availability, you must upload the Firewall Management Center upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization.

Step 3 Upgrade peers one at a time — first the standby, then the active.

Follow the instructions in Upgrade the Firewall Management Center: Standalone, on page 36, stopping after you verify update success on each peer. In summary, for each peer:

a) On **System** (⚙) > **Updates**, install the upgrade.
b) Monitor progress until you are logged out, then log back in when you can (this may happen twice).
c) Verify upgrade success.

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

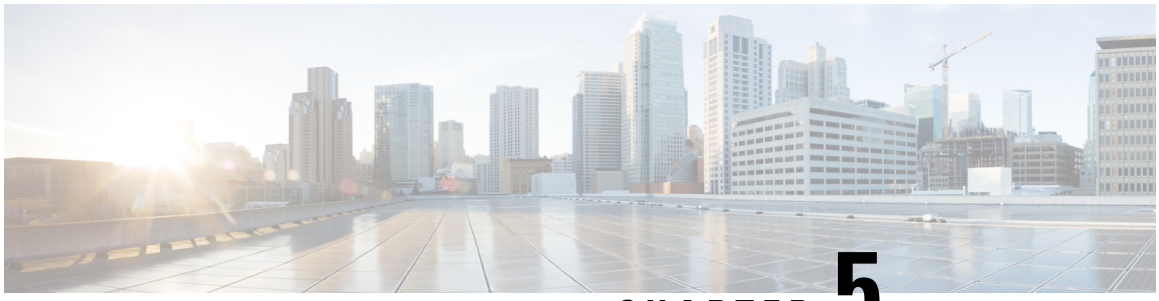
a) Choose **Integration** > **Other Integrations**.
b) On the **High Availability** tab, click **Make-Me-Active**.
c) Wait until synchronization restarts and the other Firewall Management Center switches to standby mode.

Step 5 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.

Step 6 Complete any required post-upgrade configuration changes.

Step 7 Redeploy configurations to all managed devices.



CHAPTER 5

Upgrade Firewall Threat Defense

This chapter explains how to use a Version 7.2 Firewall Management Center to upgrade Firewall Threat Defense. If your Firewall Management Center is running a different version, or if you are using the Cloud-Delivered Firewall Management Center, see Is this Guide for You?, on page 1.

- Upgrade Checklist for Firewall Threat Defense, on page 39
- Upgrade Paths for Firewall Threat Defense, on page 43
- Upgrade Packages for Firewall Management Center and Firewall Threat Defense, on page 49
- Upgrade Firewall Threat Defense with the Wizard (Disable Revert), on page 53
- Upgrade Firewall Threat Defense with System > Updates (Enable Revert), on page 57

Upgrade Checklist for Firewall Threat Defense

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

✓	Action/Check	Details
	Assess your deployment.	Understanding where you are determines how you get to where you want to go. In addition to current version and model information, determine if your deployment is configured for high availability/scalability, if your devices are deployed as an IPS or as firewalls, and so on.
	Plan your upgrade path.	This is especially important for large deployments, multi-hop upgrades, and situations where you need to upgrade operating systems or hosting environments. Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. See: • Upgrade Path for Firewall Management Center, on page 32 • Upgrade Paths for Firewall Threat Defense, on page 43 • Upgrade Paths for FXOS, on page 63

✓	Action/Check	Details
	Read upgrade guidelines and plan configuration changes.	Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with these: • Software Upgrade Guidelines, on page 19, for critical and release-specific upgrade guidelines. • *Cisco Secure Firewall Management Center New Features by Release*, for new and deprecated features that have upgrade impact. Check all versions between your current and target version. • Secure Firewall Threat Defense release notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool. • Firepower 4100/9300 FXOS release notes, for FXOS upgrade guidelines for the Firepower 4100/9300.
	Decide whether to use the wizard or System Updates page.	Some of the checklist items refer to using the Firewall Threat Defense upgrade wizard vs the System Updates page. The wizard walks you through important upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and performing compatibility and readiness checks. Upgrades performed with this wizard are faster, more reliable, and take up less disk space. We usually recommend you use the wizard to upgrade Firewall Threat Defense. But in Versions 7.1.0–7.2.5, 7.3.x, and 7.4.0, if you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates**. You must also use the System Updates page to manage upgrade packages and to upgrade the Firewall Management Center and older Classic devices.
	Check 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.
	Check bandwidth.	Make sure your management network has the bandwidth to perform large data transfers. Whenever possible, upload upgrade packages ahead of time. If you transfer an upgrade package to a device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. See Guidelines for Downloading Data from the Firepower Managemen t Center to Managed Devices (Troubleshooting TechNote).

✓	Action/Check	Details
	Schedule maintenance windows.	Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time upgrades are likely to take. Consider the tasks you must perform in the window, and those you can perform ahead of time. See: • Traffic Flow and Inspection for Chassis Upgrades, on page 62 • Time and Disk Space Tests

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 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.

✓	Action/Check	Details
	Back up Firewall Threat Defense.	Use the Firewall Management Center to back up Firewall Threat Defense configurations, when supported. See the *Backup/Restore* chapter in the *Cisco Secure Firewall Management Center Administration Guide*. If you have a Firepower 9300 with Firewall Threat Defense and ASA logical devices running on separate modules, use ASDM or the ASA CLI to back up ASA configurations and other critical files, especially if there is an ASA configuration migration. See the *Software and Configurations* chapter in the Cisco ASA Series General Operations Configuration Guide.
	Back up FXOS on the Firepower 4100/9300.	Use the Firewall Chassis Manager or the FXOS CLI to export chassis configurations, including logical device and platform configuration settings. See the *Configuration Import/Export* chapter in the Cisco Firepower 4100/9300 FXOS Configuration Guide.

Upgrade Packages

Uploading upgrade packages to the system before you begin upgrade can reduce the length of your maintenance window.

✓	Action/Check	Details
	Download upgrade packages from Cisco and upload them to the Firewall Management Center or internal web server.	Upgrade packages are available on the Cisco Support & Download site: Upgrade Packages for Firewall Management Center and Firewall Threat Defense, on page 49. You may also be able to use the Firewall Management Center to perform a direct download. Upload device upgrade packages to the Firewall Management Center, or configure devices to get them from an internal server: • Upload Firewall Threat Defense Upgrade Packages to the Firewall Management Center, on page 50 • Upload Firewall Threat Defense Upgrade Packages to an Internal Server, on page 51 For the Firepower 4100/9300, FXOS upload instructions are included in the FXOS upgrade procedures.
	Copy upgrade packages to devices.	To upgrade Firewall Threat Defense, the upgrade package must be on the device. The threat defense upgrade wizard prompts you to copy upgrade packages to devices that need them. Or, you can use the System Updates page.

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

✓	Action/Check	Details
	Upgrade virtual hosting.	If needed, upgrade the hosting environment. If this is required, it is usually because you are running an older version of VMware and are performing a major upgrade.
	Upgrade firmware on the Firepower 4100/9300.	We recommend the latest firmware. See the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.
	Upgrade FXOS on the Firepower 4100/9300.	Upgrading FXOS is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To minimize disruption, upgrade FXOS in Firewall Threat Defense high availability pairs and inter-chassis clusters one chassis at a time. See Upgrade the Chassis on the Firepower 4100/9300, on page 61.

Final Checks

A set of final checks ensures you are ready to upgrade the software.

✓	Action/Check	Details
	Check configurations.	Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.
	Check NTP synchronization.	Make sure all appliances are synchronized with any NTP server you are using to serve time. Although the health monitor alerts if clocks are out of sync by more than 10 seconds, you should still check manually. Being out of sync can cause upgrade failure. To check time: • Firewall Management Center: Choose **System** (⚙) > **Configuration** > **Time**. • Firewall Threat Defense: Use the **show time** CLI command.
	Deploy configurations.	Deploying configurations before you upgrade reduces the chance of failure. Deploying can affect traffic flow and inspection; see Traffic Flow and Inspection for Firewall Threat Defense Upgrades, on page 23.
	Run readiness checks.	Passing readiness checks reduces the chance of upgrade failure. The Firewall Threat Defense upgrade wizard prompts you to perform readiness checks. Or, you can use the System Updates page.
	Check disk space.	Readiness checks include a disk space check. Without enough free disk space, the upgrade fails. To check the disk space available on a device, choose **System** (⚙) > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.
	Check running tasks.	Make sure essential tasks are complete, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. Upgrades from Version 6.6.3+ automatically postpone scheduled tasks. Any task scheduled to begin during the upgrade will begin five minutes after the post-upgrade reboot. If you do not want this to happen (or if you are upgrading from an earlier version), check for tasks that are scheduled to run during the upgrade and cancel or postpone them.

Upgrade Paths for Firewall Threat Defense

Choose the upgrade path that matches your deployment.

Upgrade the Firewall Management Center first. 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.

Upgrade Path for Firewall Threat Defense without FXOS

This table provides the upgrade path for Firewall Threat Defense when you do not have to upgrade the operating system. This includes the Secure Firewall 3100 in appliance mode, Firepower 1000/2100 series, ASA-5500-X series, and the ISA 3000.

Note that if your current Firewall Threat Defense/Firewall Management Center version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.



Note Due to interface changes required to support autoscaling, Threat Defense Virtual for GCP upgrades cannot cross Version 7.2.0. That is, you cannot upgrade to Version 7.2.0+ from Version 7.1.x and earlier. You must deploy a new instance and redo any device-specific configurations.

Table 23: Firewall Threat Defense Direct Upgrades

Current Version	Target Version
7.4	→ Any later 7.4.x release
7.3	Any of: → 7.4.x → Any later 7.3.x release
7.2	Any of: → 7.4.x → 7.3.x → Any later 7.2.x release **Note** The Firepower 1010E, introduced in Version 7.2.3, is not supported in Version 7.3. Support returns in Version 7.4.1.
7.1	Any of: → 7.4.x → 7.3.x → 7.2.x → Any later 7.1.x release

Current Version	Target Version
7.0 Last support for ASA 5508-X and 5516-X.	Any of: → 7.4.x → 7.3.x → 7.2.x → 7.1.x → Any later 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+. **Note** cannot manage Firewall Threat Defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade directly to a later version.
6.7	Any of: → 7.2.x → 7.1.x → 7.0.x → Any later 6.7.x release
6.6 Last support for ASA 5525-X, 5545-X, and 5555-X.	Any of: → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Any later 6.6.x release
6.5	Any of: → 7.1.x → 7.0.x → 6.7.x → 6.6.x

Current Version	Target Version
6.4 Last support for ASA 5515-X.	Any of: → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Any of: → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 Last support for ASA 5506-X series.	Any of: → 6.6.x → 6.5 → 6.4 → 6.3

Upgrade Path for Firewall Threat Defense with FXOS

This table provides the upgrade path for Firewall Threat Defense on the Firepower 4100/9300.

Note that if your current Firewall Threat Defense/Firewall Management Center version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

The table lists our specially qualified version combinations. Because you upgrade FXOS first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of the device software. Make sure upgrading FXOS does not bring you out of compatibility with any logical devices or application instances. For minimum builds and other detailed compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Table 24: Firewall Threat Defense Direct Upgrades on the Firepower 4100/9300

Current Versions	Target Versions
FXOS 2.13 with Firewall Threat Defense 7.3	→ FXOS 2.13 with any later Firewall Threat Defense 7.3.x release

Current Versions	Target Versions
FXOS 2.12 with Firewall Threat Defense 7.2 Last support for Firepower 4110, 4120, 4140, 4150. Last support for the Firepower 9300 with SM-24, SM-36, or SM-44 modules.	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with any later Firewall Threat Defense 7.2.x release
FXOS 2.11.1 with Firewall Threat Defense 7.1	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with any later Firewall Threat Defense 7.1.x release
FXOS 2.10.1 with Firewall Threat Defense 7.0	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with any later Firewall Threat Defense 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+. **Note** cannot manage Firewall Threat Defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade directly to a later version.
FXOS 2.9.1 with Firewall Threat Defense 6.7	Any of: → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with any later Firewall Threat Defense 6.7.x release

Current Versions	Target Versions
FXOS 2.8.1 with Firewall Threat Defense 6.6	Any of: → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with any later Firewall Threat Defense 6.6.x release
FXOS 2.7.1 with Firewall Threat Defense 6.5	Any of: → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with Firewall Threat Defense 6.6.x
FXOS 2.6.1 with Firewall Threat Defense 6.4	Any of: → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with Firewall Threat Defense 6.6.x → FXOS 2.7.1 with Firewall Threat Defense 6.5
FXOS 2.4.1 with Firewall Threat Defense 6.3	Any of: → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with Firewall Threat Defense 6.6.x → FXOS 2.7.1 with Firewall Threat Defense 6.5 → FXOS 2.6.1 with Firewall Threat Defense 6.4
FXOS 2.3.1 with Firewall Threat Defense 6.2.3	Any of: → FXOS 2.8.1 with Firewall Threat Defense 6.6.x → FXOS 2.7.1 with Firewall Threat Defense 6.5 → FXOS 2.6.1 with Firewall Threat Defense 6.4 → FXOS 2.4.1 with Firewall Threat Defense 6.3

Upgrade Order for Firewall Threat Defense High Availability/Scalability with FXOS

Even in high availability/scalability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade FXOS one chassis at a time. For Firewall Threat Defense upgrades, the system automatically upgrades grouped devices one at a time.

Table 25: FXOS-Threat Defense Upgrade Order for the Firepower 4100/9300

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

Upgrade Packages for Firewall Management Center and Firewall Threat Defense

Upgrade packages are available on the Cisco Support & Download site: https://www.cisco.com/go/ftd-software.

You use the same upgrade package for all models in a family or series. To find the correct one, select or search for your model on the Cisco Support & Download site, then browse to the software download page for the

appropriate version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), software version, and build.

Note that upgrade packages are signed, and terminate in .sh.REL.tar. Do not untar signed upgrade packages. Do not rename upgrade packages or transfer them by email.

Table 26: Software Upgrade Packages

Platform	Upgrade Package
Firepower 1000 series	Cisco_FTD_SSP-FP1K_Upgrade-7.2-999.sh.REL.tar
Firepower 2100 series	Cisco_FTD_SSP-FP2K_Upgrade-7.2-999.sh.REL.tar
Secure Firewall 3100 series	Cisco_FTD_SSP-FP3K_Upgrade-7.2-999.sh.REL.tar
Secure Firewall 4200 series	Cisco_Secure_FW_TD_4200_Upgrade-7.2-999.sh.REL.tar
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-7.2-999.sh.REL.tar
Firewall Threat Defense Virtual	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar
ISA 3000 with FTD	Cisco_FTD_Upgrade-7.2-999.sh.REL.tar

Tip Select upgrade packages become available for direct download some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors. If the Firewall Management Center has internet access, you can click **Download Updates** on **System** (⚙) > **Updates** to immediately download the latest VDB, latest maintenance release, and the latest critical patches for the Firewall Management Center and all managed devices.

Upload Firewall Threat Defense Upgrade Packages to the Firewall Management Center

Upgrade packages are signed tar archives (.tar). After you upload a signed package, the System Updates page can take extra time to load as the package is verified. To speed up the display, delete unneeded upgrade packages. Do not untar signed packages.

Procedure

Step 1 On the Firewall Management Center, choose **System** (⚙) > **Updates**.

Step 2 Click **Upload Update**.

Step 3 For the **Action**, click the **Upload local software update package** radio button.

Step 4 Click **Choose File**.

Step 5 Browse to the package and click **Upload**.

Step 6 (Optional) Copy upgrade packages to managed devices.

If you do not need to enable revert and therefore plan to use the Firewall Threat Defense upgrade wizard, the wizard will prompt you to copy the package. If you will use the System Updates page to upgrade because you want to enable revert, we recommend you copy upgrade packages to the devices now, as follows:

a) Click the **Push or Stage Update** icon next to the upgrade package you want to copy.

b) Choose destination devices.

You can copy the package to all eligible devices now, or you can copy to a subset and then use the Firewall Threat Defense CLI to copy the upgrade package between devices; see Copy Firewall Threat Defense Upgrade Packages between Devices, on page 52.

If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.

c) Click **Push**.

Upload Firewall Threat Defense Upgrade Packages to an Internal Server

Use this procedure to configure Firewall Threat Defense devices to get upgrade packages from an internal web server, rather than from the Firewall Management Center. This is especially useful if you have limited bandwidth between the Firewall Management Center and its devices. It also saves space on the Firewall Management Center.

To configure this feature, you save a pointer (URL) to an upgrade package's location on the web server. The upgrade process will then get the upgrade package from the web server instead of the Firewall Management Center. Or, you can use the Firewall Management Center to copy the package before you upgrade.

Repeat this procedure for each upgrade package. You can configure only one location per upgrade package.

Before you begin

Copy the upgrade packages to an internal web server that your devices can access. For secure web servers (HTTPS), obtain the server's digital certificate (PEM format). 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.

Procedure

Step 1 On the Firewall Management Center, choose **System** (⚙) > **Updates**.

Step 2 Click **Upload Update**.

Choose this option even though you will not upload anything. The next page will prompt you for a URL.

Step 3 For the **Action**, click the **Specify software update source** radio button.

Step 4 Enter a **Source URL** for the upgrade package.

Provide the protocol (HTTP/HTTPS) and full path, for example:

```
https://internal_web_server/upgrade_package.sh.REL.tar
```

Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and the software version you are upgrading to. Make sure you enter the correct file name.

Step 5 For HTTPS servers, provide a **CA Certificate**.

This is the server's digital certificate you obtained earlier. Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines.

Step 6 Click **Save**.
The location is saved. Uploaded upgrade packages and upgrade package URLs are listed together, but are labeled distinctly.

Step 7 (Optional) Copy upgrade packages to managed devices.

If you do not need to enable revert and therefore plan to use the Firewall Threat Defense upgrade wizard, the wizard will prompt you to copy the package. If you will use the System Updates page to upgrade because you want to enable revert, we recommend you copy upgrade packages to the devices now, as follows:

a) Click the **Push or Stage Update** icon next to the upgrade package you want to copy.
b) Choose destination devices.

You can copy the package to all eligible devices now, or you can copy to a subset and then use the Firewall Threat Defense CLI to copy the upgrade package between devices; see Copy Firewall Threat Defense Upgrade Packages between Devices, on page 52.

If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.

c) Click **Push**.

Copy Firewall Threat Defense Upgrade Packages between Devices

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+.

Repeat the following procedure for all devices that need the upgrade package.

Before you begin

- Upload the Firewall Threat Defense upgrade package to the Firewall Management Center or to an internal server.
- Copy the upgrade package to at least one device.

Procedure

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

Step 2 Enable the feature.

configure p2psync enable

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

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

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

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

sync-from-peer *ip_address package_path*

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

Step 5 Monitor transfer status from the CLI.

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

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

Upgrade Firewall Threat Defense with the Wizard (Disable Revert)

Use this procedure to upgrade Firewall Threat Defense using a wizard.

As you proceed, the wizard displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage.

If you navigate away from the wizard, your progress is preserved and other users cannot start a new upgrade workflow. (Exception: if you are logged in with a CAC, your progress is cleared 24 hours after you log out.) If you need to reset someone else's workflow, you must have Administrator access. You can delete or deactivate the user, or update their user role so they no longer have permission to use **Devices** > **Device Upgrade** > **Threat Defense Upgrade**.

Note that neither your workflow nor 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 uploading upgrade packages to the Firewall Management Center and performing readiness checks. (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.)

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades, on page 22.

Threat Defense History:

- 7.2: Copy upgrade packages between devices.

Before you begin

- Decide whether you want to use this procedure.

  We usually recommend you use the wizard to upgrade Firewall Threat Defense. But in Versions 7.1.0–7.2.5, 7.3.x, and 7.4.0, if you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates**. You must also use the System Updates page to manage upgrade packages and to upgrade the Firewall Management Center and older Classic devices.

- Complete upgrade planning. Make sure your deployment is healthy and successfully communicating.

Procedure

Begin workflow.

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

Select devices to upgrade and copy upgrade packages.

Step 2 Verify your device selection.

To select additional devices, go back to the Device Management page—your progress will not be lost. To remove devices, click **Reset** to clear your device selection and start over.

Step 3 Select the devices you want to upgrade.

You can upgrade multiple devices at once. You must upgrade the members of device clusters and high availability pairs at the same time.

Important
Due to performance issues, if you are upgrading a device *to* (not from) Version 6.6.x or earlier, we *strongly* recommend upgrading no more than five devices simultaneously.

Step 4 From the **Select Action** or **Select Bulk Action** menu, select **Upgrade Firepower Software**.

The device upgrade wizard appears, indicating how many devices you selected and prompting you to select a target version. The page has two panes: Device Selection on the left, and Device Details on the right. Click a device link in the Device Selection pane (such as '`4 devices`') to show the Device Details for those devices.

Note that if there is already an upgrade workflow in process, you must first either **Merge Devices** (add the newly selected devices to the previously selected devices and continue) or **Reset** (discard the previous selections and use only the newly selected devices).

Step 5 Verify your device selection.

To select additional devices, go back to the Device Management page—your progress will not be lost. To remove devices, click **Reset** to clear your device selection and start over.

Step 6 From the **Upgrade to** menu, select a target version.

The system determines which of your selected devices can be upgraded to that version. If any devices are ineligible, you can click the device link to see why. You do not have to remove ineligible devices; they are automatically excluded from upgrade.

Note that the choices in the **Upgrade to** menu correspond to the device upgrade packages available to the system. If your target version is not listed, go to **System** (⚙) > **Updates** and upload or specify the location of the correct upgrade package. If you are upgrading different device models and therefore need multiple upgrade packages, do this for all necessary upgrade packages before continuing with the next step.

Step 7 For all devices that still need an upgrade package, click **Copy Upgrade Package**, then confirm your choice.

To upgrade Firewall Threat Defense, the upgrade package must be on the device. Copying the upgrade package before upgrade reduces the length of your upgrade maintenance window.

Tip
You can also use the Firewall Threat Defense CLI to copy upgrade packages from device to device. For more information, including eligibility requirements, see Copy Firewall Threat Defense Upgrade Packages between Devices, on page 52.

Step 8 Click **Next**.

Perform compatibility, readiness, and other final checks.

Step 9 For all devices that need to pass the readiness check, click **Run Readiness Check**, then confirm your choice.

Although you can skip checks by disabling the **Require passing compatibility and readiness checks** option, we recommend against it. Passing all checks greatly reduces the chance of upgrade failure. Do *not* deploy changes to, manually reboot, or shut down a device while running readiness checks. If a device fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, do not begin the upgrade. Instead, contact Cisco TAC.

Note that compatibility checks are automatic. For example, the system alerts you immediately if you need to upgrade FXOS, or if you need to deploy to managed devices.

Step 10 Perform final pre-upgrade checks.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks.

Step 11 If necessary, return to **Devices** > **Device Upgrade** > **Threat Defense Upgrade**.

Step 12 Click **Next**.

Upgrade devices.

Step 13 Verify your device selection and target version.

Step 14 (Optional) Change the upgrade order of clustered devices.

View the Device Details for the cluster and click **Change Upgrade Order**. The control unit is always upgraded last; you cannot change this.

Step 15 Choose upgrade options.

For major and maintenance upgrades, you can:

- **Automatically cancel on upgrade failure and roll back to the previous version**: The device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. 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.
- **Upgrade Snort 2 to Snort 3**: With upgrades to Version 7.2+, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations.

  For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the *Custom Snort 3 Intrusion Policies for Access Control* for your version.

These options are not supported for patches.

Step 16 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

You can monitor overall upgrade progress in the Message Center. For detailed progress, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center. For information on traffic handling during the upgrade, see Traffic Flow and Inspection for Firewall Threat Defense Upgrades, on page 23.

Devices may reboot twice during the upgrade. This is expected behavior.

Verify success and complete post-upgrade tasks.

Step 17 Verify success.

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

Step 18 (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 19 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.

Step 20 Complete any required post-upgrade configuration changes.

Step 21 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 25.

Before you deploy, you may want to review the changes made by the upgrade (as well as any changes you have made since upgrade). Choose **Deploy** > **Advanced Deploy**, select the devices you just upgraded, and click **Pending Changes Reports**. After 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 **Finish**. 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 for managed devices.
- 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 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 to create snapshots of your freshly upgraded devices.

Upgrade Firewall Threat Defense with System > Updates (Enable Revert)

Use this procedure to upgrade Firewall Threat Defense using the System Updates page.

Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Unresponsive Upgrades, on page 22.

Before you begin

- Decide whether you want to use this procedure.

  In Versions 7.1.0–7.2.5, 7.3.x, and 7.4.0, if you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates** to upgrade Firewall Threat Defense. This is the only way to set the **Enable revert after successful upgrade** option, and is in contrast to our usual recommendation to use the Firewall Threat Defense upgrade wizard.
- Complete upgrade planning. Make sure your deployment is healthy and successfully communicating.

Procedure

Step 1 On the Firewall Management Center, choose **System** (⚙) > **Updates**.

Step 2 Under Available Updates, click the **Install** icon next to the upgrade package.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

The system displays a list of eligible devices, along with pre-upgrade compatibility check results. This precheck prevents you from upgrading if there are obvious issues that will cause your upgrade to fail.

Step 3 Select the devices you want to check and click **Check Readiness**.

Readiness checks assess preparedness for major and maintenance upgrades. The time required to run a readiness check varies depending on model. Do not manually reboot or shut down during readiness checks.

Under Readiness Checks on this page, you can view check status for your whole deployment, including checks in progress and failed checks. You can also use this page to easily re-run checks after a failure. Or, monitor readiness check progress in the Message Center.

If you cannot select an otherwise eligible device, make sure it passed compatibility checks. If a device fails readiness checks, correct the issues before upgrading.

Step 4 Choose the devices to upgrade.

You can upgrade multiple devices at once only if they use the same upgrade package. You must upgrade the members of device clusters and high availability pairs at the same time.

Important
We *strongly* recommend upgrading no more than five devices simultaneously from the System Update page. You cannot stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 5 Choose upgrade options.

For major and maintenance upgrades, you can:

- **Automatically cancel on upgrade failure and roll back to the previous version**: The device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. 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.
- **Enable revert after successful upgrade**: For 30 days after a successful upgrade, you can return the device to its pre-upgrade state.
- **Upgrade Snort 2 to Snort 3**: With upgrades to Version 7.2+, eligible devices will upgrade from Snort 2 to Snort 3 when you deploy configurations.

  For devices that are ineligible because they use custom intrusion or network analysis policies, we strongly recommend you manually upgrade to Snort 3 for improved detection and performance. For migration assistance, see the *Custom Snort 3 Intrusion Policies for Access Control* for your version.

These options are not supported for patches.

Step 6 Click **Install**, then confirm that you want to upgrade and reboot the devices.

You can monitor upgrade progress in the Message Center. For information on traffic handling during the upgrade, see Traffic Flow and Inspection for Firewall Threat Defense Upgrades, on page 23.

Devices may reboot twice during the upgrade. This is expected behavior.

Step 7 Verify success.

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

Step 8 (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 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.

Step 10 Complete any required post-upgrade configuration changes.

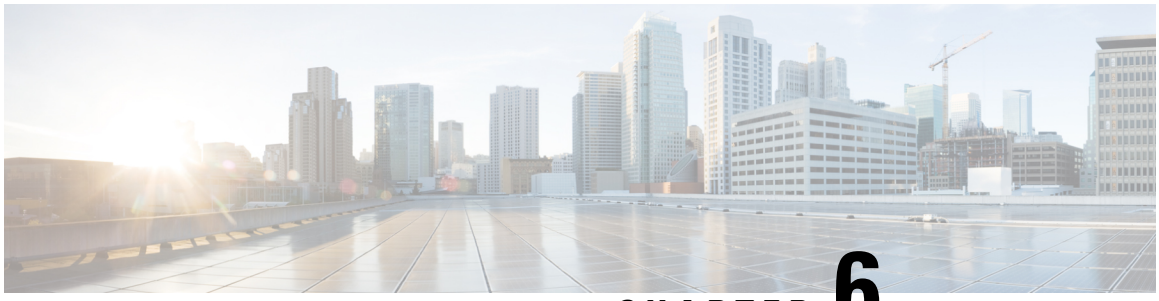
Step 11 Redeploy configurations to the devices you just upgraded.

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 25.

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

What to do next

- 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 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 to create snapshots of your freshly upgraded devices.



CHAPTER 6

Upgrade the Chassis on the Firepower 4100/9300

Cisco Firepower 4100/9300 FXOS Release Notes, 2.12

- Upgrade Packages for FXOS, on page 61
- Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 61
- Upgrade Paths for FXOS, on page 63
- Upgrade FXOS with Firewall Chassis Manager, on page 69
- Upgrade FXOS with the CLI, on page 76

Upgrade Packages for FXOS

FXOS images and firmware updates are available on the Cisco Support & Download site:

- Firepower 4100 series: http://www.cisco.com/go/firepower4100-software
- Firepower 9300: http://www.cisco.com/go/firepower9300-software

To find the correct FXOS image, select or search for your device model and browse to the *Firepower Extensible Operating System* download page for your target FXOS version and build. The FXOS image is listed along with recovery and MIB packages. If you need to upgrade the firmware, those packages are under *All Releases > Firmware*.

The packages are:

- Firepower 4100/9300 FXOS image: fxos-k9.*fxos_version*.SPA
- Firepower 4100 series firmware: fxos-k9-fpr4k-firmware.*firmware_version*.SPA
- Firepower 9300 firmware: fxos-k9-fpr9k-firmware.*firmware_version*.SPA

Upgrade Guidelines for the Firepower 4100/9300 Chassis

For the Firepower 4100/9300, major Firewall Threat Defense upgrades also require a chassis upgrade (FXOS and firmware). Maintenance release and patches rarely require this, but you may still want to upgrade to the latest build to take advantage of resolved issues.

Table 27: Upgrade Guidelines for the Firepower 4100/9300 Chassis

Guideline	Details
FXOS upgrades.	FXOS 2.12.1.95+ is required to run threat defense Version 7.2 on the Firepower 4100/9300. You can upgrade to any later FXOS version from as far back as FXOS 2.2.2. For critical and release-specific upgrade guidelines, new and deprecated features, and open and resolved bugs, see the Firepower 4100/9300 FXOS release notes.
Firmware upgrades.	FXOS 2.14.1+ upgrades include firmware. If you are upgrading to an earlier FXOS version, see the *Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide*.
Time to upgrade.	Chassis upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see Traffic Flow and Inspection for Chassis Upgrades, on page 62.
Chassis upgrade order with Firewall Threat Defense high availability/scalability.	Even in high availability/scalability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade FXOS one chassis at a time. For Firewall Threat Defense upgrades, the system automatically upgrades grouped devices one at a time. For more information, see Upgrade Order for FXOS with Firewall Threat Defense High Availability/Scalability, on page 68.
Chassis upgrade order with Firewall Threat Defense and ASA logical devices.	If you have Firewall Threat Defense *and* ASA logical devices configured on the Firepower 9300, use the procedures in this chapter to upgrade FXOS and Firewall Threat Defense. Make sure that upgrading FXOS does not bring you out of compatibility with either type of logical device; see Upgrade Path for FXOS with Firewall Threat Defense and ASA, on page 65. For ASA upgrade procedures, see the *Cisco Secure Firewall ASA Upgrade Guide*.
Chassis upgrade with no logical devices.	If you have no logical devices configured, use the procedures in this chapter for upgrading FXOS on standalone Firewall Threat Defense devices, disregarding any instructions on logical devices. Or, perform a full reimage of the chassis to the FXOS version you need.

Traffic Flow and Inspection for Chassis Upgrades

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

Even in high availability/clustered deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time. For more information, see Upgrade Order for FXOS with Firewall Threat Defense High Availability/Scalability, on page 68.

Table 28: 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.

Upgrade Paths for FXOS

Choose the upgrade path that matches your deployment.

Upgrade Path for FXOS with Firewall Threat Defense

This table provides the upgrade path for Firewall Threat Defense on the Firepower 4100/9300.

Note that if your current Firewall Threat Defense/Firewall Management Center version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

The table lists our specially qualified version combinations. Because you upgrade FXOS first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of the device software. Make sure upgrading FXOS does not bring you out of compatibility with any logical devices or application instances. For minimum builds and other detailed compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Table 29: Firewall Threat Defense Direct Upgrades on the Firepower 4100/9300

Current Versions	Target Versions
FXOS 2.13 with Firewall Threat Defense 7.3	→ FXOS 2.13 with any later Firewall Threat Defense 7.3.x release
FXOS 2.12 with Firewall Threat Defense 7.2 Last support for Firepower 4110, 4120, 4140, 4150. Last support for the Firepower 9300 with SM-24, SM-36, or SM-44 modules.	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with any later Firewall Threat Defense 7.2.x release
FXOS 2.11.1 with Firewall Threat Defense 7.1	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with any later Firewall Threat Defense 7.1.x release
FXOS 2.10.1 with Firewall Threat Defense 7.0	Any of: → FXOS 2.13 with Firewall Threat Defense 7.3.x → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with any later Firewall Threat Defense 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+. **Note** cannot manage Firewall Threat Defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade directly to a later version.
FXOS 2.9.1 with Firewall Threat Defense 6.7	Any of: → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with any later Firewall Threat Defense 6.7.x release

Current Versions	Target Versions
FXOS 2.8.1 with Firewall Threat Defense 6.6	Any of: → FXOS 2.12 with Firewall Threat Defense 7.2.x → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with any later Firewall Threat Defense 6.6.x release
FXOS 2.7.1 with Firewall Threat Defense 6.5	Any of: → FXOS 2.11.1 with Firewall Threat Defense 7.1.x → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with Firewall Threat Defense 6.6.x
FXOS 2.6.1 with Firewall Threat Defense 6.4	Any of: → FXOS 2.10.1 with Firewall Threat Defense 7.0.x → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with Firewall Threat Defense 6.6.x → FXOS 2.7.1 with Firewall Threat Defense 6.5
FXOS 2.4.1 with Firewall Threat Defense 6.3	Any of: → FXOS 2.9.1 with Firewall Threat Defense 6.7.x → FXOS 2.8.1 with Firewall Threat Defense 6.6.x → FXOS 2.7.1 with Firewall Threat Defense 6.5 → FXOS 2.6.1 with Firewall Threat Defense 6.4
FXOS 2.3.1 with Firewall Threat Defense 6.2.3	Any of: → FXOS 2.8.1 with Firewall Threat Defense 6.6.x → FXOS 2.7.1 with Firewall Threat Defense 6.5 → FXOS 2.6.1 with Firewall Threat Defense 6.4 → FXOS 2.4.1 with Firewall Threat Defense 6.3

Upgrade Path for FXOS with Firewall Threat Defense and ASA

This table provides upgrade paths for the Firepower 9300 with Firewall Threat Defense and ASA logical devices running on separate modules.

Note This document does not contain procedures for upgrading ASA logical devices. For those, see the *Cisco Secure Firewall ASA Upgrade Guide*.

Note that if your current Firewall Threat Defense/Firewall Management Center version was released on a date after your target version, you may not be able to upgrade as expected. In those cases, the upgrade quickly fails and displays an error explaining that there are datastore incompatibilities between the two versions. The release notes for both your current and target version list any specific restrictions.

The table lists our specially qualified version combinations. Because you upgrade FXOS first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of the device software. Make sure upgrading FXOS does not bring you out of compatibility with any logical devices (including ASA devices) or Firewall Threat Defense application instances. If you need to skip multiple versions, Firewall Threat Defense will usually be the limiter—FXOS and ASA can usually upgrade further in one hop. After you reach the target FXOS version, it does not matter which type of logical device you upgrade first. For minimum builds and other detailed compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*

Table 30: Firewall Threat Defense and ASA Direct Upgrades on the Firepower 9300

Current Versions	Target Versions
FXOS 2.13 with: • Threat defense 7.3 • ASA 9.19(x)	→ FXOS 2.13 with ASA 9.19(x) and any later threat defense 7.3.x release
FXOS 2.12 with: • Threat defense 7.2 • ASA 9.18(x) Last support for the Firepower 9300 with SM-24, SM-36, or SM-44 modules.	Any of: → FXOS 2.13 with ASA 9.19(x) and threat defense 7.3.x → FXOS 2.12 with ASA 9.18(x) and any later threat defense 7.2.x release
FXOS 2.11.1 with: • Threat defense 7.1 • ASA 9.17(x)	→ FXOS 2.13 with ASA 9.19(x) and threat defense 7.3.x → FXOS 2.12 with ASA 9.18(x) and threat defense 7.2.x → FXOS 2.11.1 with ASA 9.17(x) and any later threat defense 7.1.x release

Current Versions	Target Versions
FXOS 2.10.1 with: • Threat defense 7.0 • ASA 9.16(x)	Any of: → FXOS 2.13 with ASA 9.19(x) and threat defense 7.3.x → FXOS 2.12 with ASA 9.18(x) and threat defense 7.2.x → FXOS 2.11.1 with ASA 9.17(x) and threat defense 7.1.x → FXOS 2.10.1 with ASA 9.16(x) and any later threat defense 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+. **Note** cannot manage Firewall Threat Defense devices running Version 7.1, or Classic devices running any version. You cannot upgrade a cloud-managed device from Version 7.0.x to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade directly to a later version.
FXOS 2.9.1 with: • Threat defense 6.7 • ASA 9.15(x)	Any of: → FXOS 2.12 with ASA 9.18(x) and threat defense 7.2.x → FXOS 2.11.1 with ASA 9.17(x) and threat defense 7.1.x → FXOS 2.10.1 with ASA 9.16(x) and threat defense 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and any later threat defense 6.7.x release
FXOS 2.8.1 with: • Threat defense 6.6 • ASA 9.14(x)	Any of: → FXOS 2.12 with ASA 9.18(x) and threat defense 7.2.x → FXOS 2.11.1 with ASA 9.17(x) and threat defense 7.1.x → FXOS 2.10.1 with ASA 9.16(x) and threat defense 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and threat defense 6.7.x → FXOS 2.8.1 with ASA 9.14(x) and any later threat defense 6.6.x release
FXOS 2.7.1 with: • Threat defense 6.5 • ASA 9.13(x)	Any of: → FXOS 2.11.1 with ASA 9.17(x) and threat defense 7.1.x → FXOS 2.10.1 with ASA 9.16(x) and threat defense 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and threat defense 6.7.x → FXOS 2.8.1 with ASA 9.14(x) and threat defense 6.6.x

Current Versions	Target Versions
FXOS 2.6.1 with: • Threat defense 6.4 • ASA 9.12(x)	Any of: → FXOS 2.10.1 with ASA 9.16(x) and threat defense 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and threat defense 6.7.x → FXOS 2.8.1 with ASA 9.14(x) and threat defense 6.6.x → FXOS 2.7.1 with ASA 9.13(x) and threat defense 6.5

Upgrade Order for FXOS with Firewall Threat Defense High Availability/Scalability

Even in high availability/scalability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade FXOS one chassis at a time. For Firewall Threat Defense upgrades, the system automatically upgrades grouped devices one at a time.

Table 31: FXOS-Threat Defense Upgrade Order for the Firepower 4100/9300

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

Upgrade FXOS 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 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

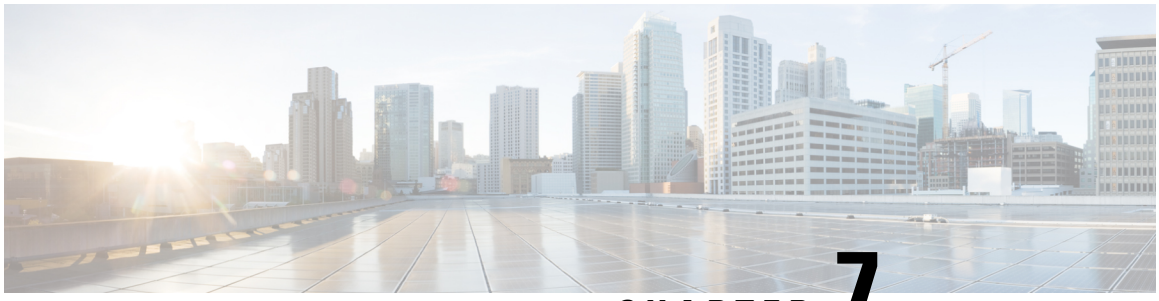
FP9300-A /system #
```

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.



CHAPTER 7

Revert or Uninstall the Upgrade

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

- Revert is supported for major and maintenance upgrades to Firewall Threat Defense Version 7.1+.
- Uninstall is supported for patches to Firewall Threat Defense and to the Firewall Management Center.

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

- Revert Firewall Threat Defense, on page 87
- Uninstall a Patch, on page 91

Revert Firewall Threat Defense

About Reverting Firewall Threat Defense

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

Reverted Configurations

Configurations that are reverted include:

- Snort version.
- Device-specific configurations.

  General device settings, routing, interfaces, inline sets, DHCP, SNMP — anything you configure on the **Devices** > **Device Management** page.
- Objects used by your device-specific configurations.

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

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

Configurations Not Reverted

Configurations that are not reverted include:

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

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

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

  Sync interface changes after a successful revert.

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

  If you are required to run the recommended combination of FXOS and Firewall Threat Defense, you may need a full reimage; see Guidelines for Reverting Firewall Threat Defense, on page 88.

Guidelines for Reverting Firewall Threat Defense

System Requirements

Revert is supported for major and maintenance upgrades to Firewall Threat Defense Version 7.1+.

Revert is not supported for:

- Upgrades to earlier versions.
- Patches and hotfixes.
- Container instances.
- Management center upgrades.

Reverting High Availability or Clustered Devices

When you use the 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 on interface configurations only, as if every device were standalone.

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

Revert Does Not Downgrade FXOS

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.

Scenarios Preventing Revert

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

Table 32: Scenarios Preventing Revert

Scenario	Solution
Revert snapshot is not available because: • You did not enable revert when you upgraded the device. • You deleted the snapshot from either the Firewall Management Center or the device, or it expired. • You upgraded the device with a different Firewall Management Center.	None. In Versions 7.1.0–7.2.5, 7.3.x, and 7.4.0, if you think you might need to revert after a successful upgrade, use **System** (⚙) > **Updates** to upgrade Firewall Threat Defense. This is the only way to set the **Enable revert after successful upgrade** option, and is in contrast to our usual recommendation to use the Firewall Threat Defense upgrade wizard. The revert snapshot is saved on the Firewall Management Center *and* the device for thirty days, after which it is automatically deleted and you can no longer revert. You can manually delete the snapshot from either appliance to save disk space, but this removes your ability to revert.
Last upgrade failed.	Return the device to its pre-upgrade state by canceling the upgrade. Or, fix the issues and try again. Revert is for situations where the upgrade succeeds, but the upgraded system does not function to your expectations. Reverting is not the same as canceling a failed or in-progress upgrade. If you cannot revert or cancel, you will have to reimage.
Management access interface changed since the upgrade.	Switch it back and try again.
Clusters where the units were upgraded from different versions.	Remove units until all match, reconcile cluster members, then revert the smaller cluster. You may also be able to revert the newly standalone units.
Clusters where one or more units were added to the cluster after upgrade.	Remove the new units, reconcile cluster members, then revert the smaller cluster. You may also be able to revert the newly standalone units.

Scenario	Solution
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.

Revert Firewall Threat Defense with Firewall Management Center

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

Caution Reverting from the CLI can cause configurations between the device and the Firewall Management Center to go out of sync, depending on what you changed post-upgrade. This can cause further communication and deployment issues.

Before you begin

- Make sure revert is supported. Read and understand the guidelines.
- Back up to a secure external location. A failed revert may require a reimage, which returns most settings to factory defaults.

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/scalability deployments, the system reverts all units simultaneously.

Step 4 Monitor revert progress.

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

Step 5 Verify revert success.

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

Step 6 (Firepower 4100/9300) Sync any interface changes you made to 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.

Uninstall a Patch

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



Note This guide describes how to uninstall Firewall Management Center and Firewall Threat Defense patches. To uninstall patches from older ASA FirePOWER or NGIPSv devices, see the *Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0*.

Uninstall Order for High Availability/Scalability

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

Table 33: Uninstall Order for Firewall Management Center High Availability

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

Table 34: Uninstall Order for Firewall Threat Defense High Availability and Clusters

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

Uninstall Threat Defense Patches

Use the Linux shell (*expert mode*) to uninstall patches. You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. You cannot use a 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

- Break Firewall Threat Defense high availability pairs; see Uninstall Order for High Availability/Scalability, on page 91.
- Make sure your deployment is healthy and successfully communicating.

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 listed in the following table.

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

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

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

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

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

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

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

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

Step 6 Monitor the uninstall until you are logged out.

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

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

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

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

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

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

Step 9 Redeploy configurations.

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

What to do next

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

Uninstall Standalone Firewall Management Center Patches

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

- If uninstalling will put the Firewall Management Center at a lower patch level than its managed devices, uninstall patches from the devices first.
- Make sure your deployment is healthy and successfully communicating.

Procedure

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

Deploying before you uninstall reduces the chance of failure.

Step 2 Under Available Updates, click the **Install** icon next to the uninstall package, then choose the Firewall Management Center.

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

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

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

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

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

Step 5 Redeploy configurations to all managed devices.

Uninstall High Availability Firewall Management Center Patches

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

- If uninstalling will put the Firewall Management Centers at a lower patch level than their managed devices, uninstall patches from the devices first.
- Make sure your deployment is healthy and successfully communicating.

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 Standalone Firewall Management Center Patches , on page 94, but omit the initial deploy, stopping after you verify uninstall success on each peer. In summary, for each peer:

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

Step 4 On the 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.