

Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager, Version 7.2

First Published: 2022-06-06

Last Modified: 2026-09-03

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

© 2022–2026 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 4

For Assistance 4

CHAPTER 2 **System Requirements** 7

Firewall Threat Defense Platforms 7

Firewall Threat Defense Management 9

CHAPTER 3 **Software Upgrade Guidelines** 11

Minimum Version to Upgrade 11

Upgrade Guidelines for Version 7.2 12

Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs 12

Unresponsive Upgrades 13

Traffic Flow and Inspection for Firewall Threat Defense Upgrades 13

Traffic Flow and Inspection when Deploying Configurations 14

Time and Disk Space 14

CHAPTER 4 **Upgrade the Chassis on the Firepower 4100/9300** 17

Upgrade Packages for FXOS 17

Upgrade Guidelines for the Firepower 4100/9300 Chassis 17

Traffic Flow and Inspection for Chassis Upgrades 18

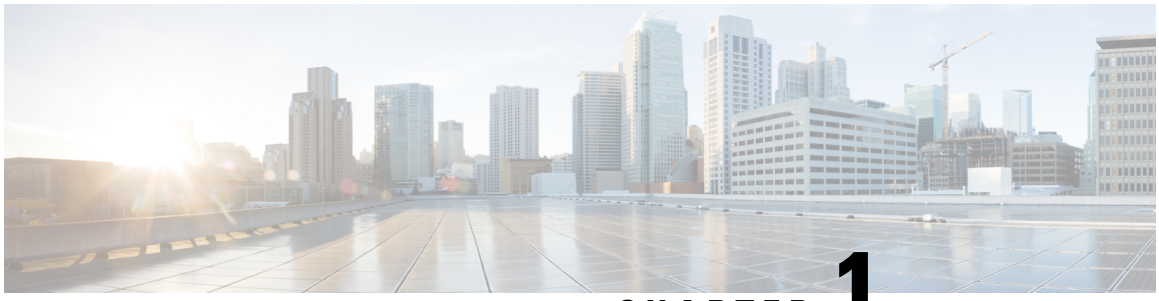
Upgrade Paths for FXOS 19

Upgrade Path for FXOS with Firewall Threat Defense 19

Upgrade Path for FXOS with Firewall Threat Defense and ASA 21

Upgrade Order for FXOS with Firewall Threat Defense High Availability 23
Upgrade FXOS with Firewall Chassis Manager 23
Upgrade FXOS for Standalone FTD Logical Devices Using Firepower Chassis Manager 23
Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager 25
Upgrade FXOS with the CLI 28
Upgrade FXOS for Standalone FTD Logical Devices Using the FXOS CLI 28
Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI 31

CHAPTER 5 **Upgrade Firewall Threat Defense** 37
Upgrade Checklist for Firewall Threat Defense 37
Upgrade Paths for Firewall Threat Defense 40
Upgrade Path for Firewall Threat Defense with FXOS 41
Upgrade Path for Firewall Threat Defense without FXOS 43
Upgrade Packages for Firewall Threat Defense 45
Upgrade Readiness Checks for Firewall Threat Defense 46
Upgrade Firewall Threat Defense 47
Upgrade Standalone Firewall Threat Defense 47
Upgrade High Availability Firewall Threat Defense 48
Monitor Firewall Threat Defense Upgrades 50
Cancel or Retry Firewall Threat Defense Upgrades 51
Revert Firewall Threat Defense 51
Troubleshooting Threat Defense Upgrades 52



CHAPTER 1

Getting Started

- Is this Guide for You?, on page 1
- Planning Your Upgrade, on page 3
- Upgrade Feature History, on page 4
- For Assistance, on page 4

Is this Guide for You?

This guide explains how to prepare for and complete a successful upgrade of **Secure Firewall Threat Defense** with **Secure Firewall Device Manager** currently running **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 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	Release Notes for Cisco Secure Firewall Threat Defense and Firepower Hotfixes
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 5: 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 the software. 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 6: Device Upgrade Feature History

Feature	Minimum Threat Defense	Details
Pre-upgrade readiness check.	7.0.0	You can run a readiness check before upgrade. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations. A link to run the upgrade readiness check was added to the **System Upgrade** section of the **Device** > **Updates** page.
Cancel and revert a failed upgrade.	6.7.0	If a major software upgrade fails or is otherwise not functioning correctly, you can revert to the state of the device as it was when you installed the upgrade. We added the ability to revert the upgrade to the System Upgrade panel in FDM. During an upgrade, the FDM login screen shows the upgrade status and gives you the option to cancel or revert in case of upgrade failure. In the Firewall Threat Defense API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources. In the Firewall Threat Defense CLI, we added the following commands: **show last-upgrade status**, **show upgrade status**, **show upgrade revert-info**, **upgrade cancel**, **upgrade revert**, **upgrade cleanup-revert**, **upgrade retry**.
Upgrade with Firewall Device Manager.	6.2.0	You can install software upgrades through Firewall Device Manager. Select **Device** > **Updates**.

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 7: Upgrade Guides

Platform	Upgrade Guide	Link
Firewall Management Center	Firewall Management Center version you are *currently* running.	https://cisco.com/go/fmc-upgrade

Platform	Upgrade Guide	Link
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 8: 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

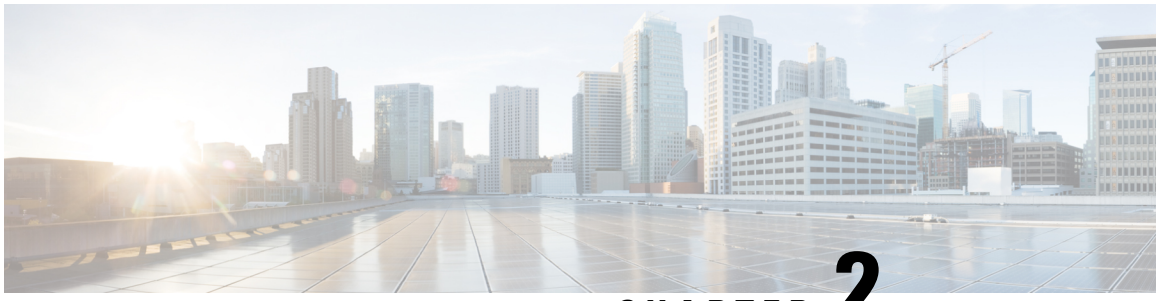
- Cisco Support & Download site: https://cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://cisco.com/cisco/support/notifications.html

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 Threat Defense Platforms, on page 7
- Firewall Threat Defense Management, on page 9

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 9. 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 9: 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+.
Firepower 2110, 2120, 2130, 2140	YES	YES	YES	YES	—
Secure Firewall3110, 3120, 3130, 3140	YES	YES	YES	YES	—

Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility		Notes
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO	
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 10: Version 7.2 Firewall Threat Defense Virtual Platforms

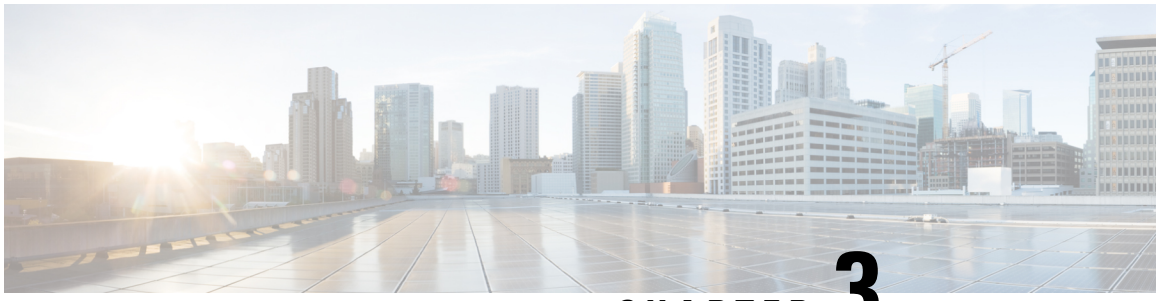
Device Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility	
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	YES	YES	YES
Microsoft Azure	YES	YES	YES	YES
Google Cloud Platform (GCP)	YES	YES	YES	YES
Oracle Cloud Infrastructure (OCI)	YES	YES	—	—
Private Cloud				

Device Platform	Firewall Management Center Compatibility		Firewall Device Manager Compatibility	
	Customer Deployed	Cloud Delivered	Firewall Device Manager Only	Firewall Device Manager + CDO
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

You can use Firewall Device Manager to locally manage a single Firewall Threat Defense device. Most models suppport local management.

Optionally, add Security Cloud Control to remotely manage multiple Firewall Threat Defense devices, as an alternative to the Firewall Management Center. Although some configurations still require Firewall Device Manager, Security Cloud Control allows you to establish and maintain consistent security policies across your Firewall Threat Defense deployment.



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 17.

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 11
- Upgrade Guidelines for Version 7.2, on page 12
- Unresponsive Upgrades, on page 13
- Traffic Flow and Inspection for Firewall Threat Defense Upgrades, on page 13
- Traffic Flow and Inspection when Deploying Configurations, on page 14
- Time and Disk Space, on page 14

Minimum Version to Upgrade

Minimum Version to Upgrade

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

Table 11: Minimum Version to Upgrade to Version 7.2

Platform	Minimum Version
Firewall Threat Defense	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.

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 12: Upgrade Guidelines for Firewall Threat Defense with Firewall Device Manager Version 7.2

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 11	Any	Any	Any
	Cisco Secure Firewall Device Manager 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
	Release Notes for Secure Firewall Threat Defense, 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 the Firepower 4100/9300 Chassis, on page 17	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 12	Firepower 1010	6.4.0 through 6.6.x	6.7+

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.

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.

For major and maintenance upgrades, you can manually cancel failed or in-progress upgrades, and retry failed upgrades. Use the System Upgrade panel or the Firewall Threat Defense CLI. Note that this feature is only supported for upgrades *from* (not to) Version 6.7.0 or later.

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 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

Traffic is dropped while you upgrade. In a high availability deployment, you can minimize disruption by upgrading devices one at a time.

For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

Software Revert (Major/Maintenance Releases)

Traffic is dropped while you revert. In a high availability deployment, revert is more successful when you revert both units simultaneously. Traffic flow and inspection resume when the first unit comes back online.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability. 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.

Traffic Flow and Inspection when Deploying Configurations

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability. 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.

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.

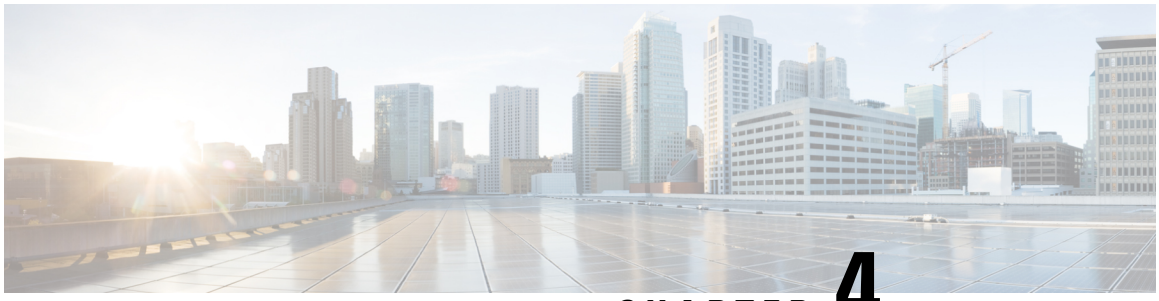
Caution Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see Troubleshooting Threat Defense Upgrades, on page 52.

Table 13: 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	In a high availability 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, therefore, takes longer than upgrading a standalone device.
Configurations	Upgrade time can increase with the complexity of your configurations and whether/how they are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.
Components	You may need additional time to perform operating system or virtual hosting upgrades, upgrade package transfers, readiness checks, VDB and intrusion rule (SRU/LSP) updates, configuration deployment, and other related tasks.

Disk Space to Upgrade

To upgrade, the upgrade package must be on the device. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails. To check disk space, use the **show disk** CLI command.



CHAPTER 4

Upgrade the Chassis on the Firepower 4100/9300

Cisco Firepower 4100/9300 FXOS Release Notes, 2.12

- Upgrade Packages for FXOS, on page 17
- Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 17
- Upgrade Paths for FXOS, on page 19
- Upgrade FXOS with Firewall Chassis Manager, on page 23
- Upgrade FXOS with the CLI, on page 28

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 14: 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 18.
Chassis upgrade order with Firewall Threat Defense high availability/scalability.	In high availability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade FXOS one chassis at a time. You must also upgrade the Firewall Threat Defense devices one at a time. For more information, see Upgrade Order for FXOS with Firewall Threat Defense High Availability, on page 23.
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 21. 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 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, on page 23.

Table 15: Traffic Flow and Inspection: FXOS Upgrades

Firewall Threat Defense Deployment	Traffic Behavior	Method
Standalone	Dropped.	—

Firewall Threat Defense Deployment	Traffic Behavior	Method
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.

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 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. For minimum builds and other detailed compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Table 16: 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

Current Versions	Target Versions
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
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

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 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). 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 17: 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

Upgrade Order for FXOS with Firewall Threat Defense High Availability

In high availability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade FXOS one chassis at a time. You must also upgrade the Firewall Threat Defense devices one at a time.

Table 18:

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. In the following scenario, Device A is the original active device and Device B is the original standby. **1.** Upgrade FXOS on the chassis with the standby device (B). **2.** Switch roles. **3.** Upgrade FXOS on the chassis with the new standby device (A). **4.** Upgrade Firewall Threat Defense on the new standby device (A). **5.** Switch roles again. **6.** Upgrade Firewall Threat Defense on the original standby device (B).

Upgrade FXOS with Firewall Chassis Manager

Upgrade FXOS for Standalone FTD Logical Devices 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.
- A Firepower 9300 chassis that is configured with one or more standalone FTD logical devices that are not part of a failover pair.

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

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 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

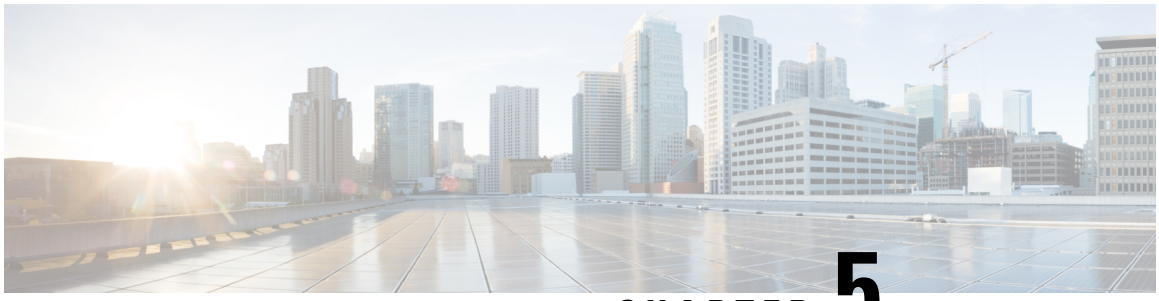
FP9300-A /system #
```

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 5

Upgrade Firewall Threat Defense

- Upgrade Checklist for Firewall Threat Defense, on page 37
- Upgrade Paths for Firewall Threat Defense, on page 40
- Upgrade Packages for Firewall Threat Defense, on page 45
- Upgrade Readiness Checks for Firewall Threat Defense, on page 46
- Upgrade Firewall Threat Defense, on page 47
- Monitor Firewall Threat Defense Upgrades, on page 50
- Cancel or Retry Firewall Threat Defense Upgrades, on page 51
- Revert Firewall Threat Defense, on page 51
- Troubleshooting Threat Defense Upgrades, on page 52

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.
	Plan your upgrade path.	This is especially important for high availability 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 Paths for Firewall Threat Defense, on page 40 • Upgrade Paths for FXOS, on page 19

✓	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 11, for critical and release-specific upgrade guidelines. • *Cisco Secure Firewall Device Manager New Features by Release*, for new and deprecated features that have upgrade impact. Check all versions between your current and target version. • Release Notes for Secure Firewall Threat Defense, 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 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.
	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. See Guidelines for Downloading Data from the Firepower Managemen t Center to Managed Devices (Troubleshooting TechNote).
	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 Firewall Threat Defense Upgrades, on page 13 • Traffic Flow and Inspection for Chassis Upgrades, on page 18 • Time and Disk Space, on page 14

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.

✓	Action/Check	Details
	Back up Firewall Threat Defense.	To back up Firewall Threat Defense configurations, see the *System Management* chapter in the *Cisco Secure Firewall Device Manager Configuration 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 the upgrade package from Cisco and upload it to the device.	Upgrade packages are available on the Cisco Support & Download site: Upgrade Packages for Firewall Threat Defense, on page 45. For Firewall Threat Defense high availability, you must upload the upgrade package to both units.

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*.

✓	Action/Check	Details
	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 one chassis at a time. See Upgrade the Chassis on the Firepower 4100/9300, on page 17.

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. Being out of sync can cause upgrade failure. To check time, 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 13.
	Run readiness checks.	Passing readiness checks reduces the chance of upgrade failure. See Upgrade Readiness Checks for Firewall Threat Defense, on page 46.
	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 device, use the **show disk** CLI command.
	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. We also recommend you 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 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 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. For minimum builds and other detailed compatibility information, see the *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Table 19: 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

Current Versions	Target Versions
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
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

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 Firepower 1000/2100 series, ASA-5500-X series, and the ISA 3000.

Note that if your current Firewall Threat Defense 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 20: 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 Packages for 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 21: 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

Platform	Upgrade Package
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

Upgrade Readiness Checks for Firewall Threat Defense

Before the system installs an upgrade, it runs a readiness check to ensure the upgrade is valid for the system, and to check other items that sometimes prevent a successful upgrade. If the readiness check fails, you should fix the problems before trying the installation again. If the check has failed, you will be prompted about the failure the next time you try the installation, and you are given the option to force the installation if you want to.

You can also manually run the readiness check prior to initiating the upgrade, as described in this procedure.

Before you begin

Upload the upgrade package you want to check.

Procedure

Step 1 Select **Device**, then click **View Configuration** in the Updates summary.

The **System Upgrade** section shows the currently running software version and any update that you have already uploaded.

Step 2 Look at the **Readiness Check** section.

- If the upgrade check has not been performed yet, click the **Run Upgrade Readiness Check** link. The progress of the check is shown in this area. It should take about 20 seconds to complete the process.
- If the upgrade check has already been run, this section indicates whether the check succeeded or failed. For failed checks, click **See Details** to view more information about the readiness check. After fixing problems, run the check again.

Step 3 If the readiness check fails, you should resolve the issues before you install the upgrade. The detailed information includes help on how to fix indicated problems. For a failed script, click the **Show Recovery Message** link to see the information.

Following are some typical problems:

- FXOS version incompatibility—On systems where you install FXOS upgrades separately, such as the Firepower 4100/9300, an upgrade package might require a different minimum FXOS version than the Firewall Threat Defense software version you are currently running. In this case, you must first upgrade FXOS before you can upgrade the Firewall Threat Defense software.
- Unsupported device model—The upgrade package cannot be installed on this device. You might have uploaded the wrong package, or the device is an older model that is simply no longer supported in the new Firewall Threat Defense software version. Please check device compatibility and upload a supported package, if one is available.

- Insufficient disk space—If not enough space is available, try deleting unneeded files, such as system backups. Delete only those files you have created.

Upgrade Firewall Threat Defense

Upgrade Standalone Firewall Threat Defense

Use this procedure to upgrade a standalone Firewall Threat Defense device. If you need to update FXOS, do that first. To upgrade high availability threat defense, see Upgrade High Availability Firewall Threat Defense, on page 48.

Caution Traffic is dropped while you upgrade. Even if the system appears inactive or unresponsive, do not manually reboot or shut down during upgrade; you could place the system in an unusable state and require a reimage. You can manually cancel failed or in-progress major and maintenance upgrades, and retry failed upgrades. If you continue to have issues, contact Cisco TAC.

For details on these and other issues you may encounter during upgrade, see Troubleshooting Threat Defense Upgrades, on page 52.

Before you begin

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

Procedure

Step 1 Select **Device**, then click **View Configuration** in the Updates panel.
The System Upgrade panel shows the currently running software version and any upgrade package that you have already uploaded.

Step 2 Upload the upgrade package.

You can upload one package only. If you upload a new package, it replaces the old one. Make sure you have the correct package for your target version and device model. Click **Browse** or **Replace File** to begin the upload.

When the upload completes, the system displays a confirmation dialog box. Before you click **OK**, optionally select **Run Upgrade Immediately** to choose rollback options and upgrade now. If you upgrade now, it is especially important to have completed as much of the pre-upgrade checklist as possible (see the next step).

Step 3 Perform final pre-upgrade checks, including the readiness check.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks. If you do not run the readiness check manually, it runs when you initiate the upgrade. If the readiness check fails, the upgrade is canceled. For more information, see Upgrade Readiness Checks for Firewall Threat Defense, on page 46.

Step 4 Click **Upgrade Now** to start the upgrade.

a) Choose rollback options.

You can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon major or maintenance upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade.

b) Click **Continue** to upgrade and reboot the device.

You are automatically logged off and taken to a status page where you can monitor the upgrade until the device reboots. The page also includes an option to cancel the in-progress installation. If you disabled automatic rollback and the upgrade fails, you can manually cancel or retry the upgrade.

Traffic is dropped while you upgrade. For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

Step 5 Log back in when you can and verify upgrade success.

The Device Summary page shows the currently running software version.

Step 6 Complete post-upgrade tasks.

a) Update system databases. If you do not have automatic updates configured for intrusion rules, VDB, and GeoDB, update them now.
b) Complete any other required post-upgrade configuration changes.
c) Deploy.

What to do next

- For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for the 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 a snapshot of your freshly upgraded device.

Upgrade High Availability Firewall Threat Defense

Use this procedure to upgrade high availability devices. Upgrade them one at a time. To minimize disruption, always upgrade the standby. That is, upgrade the current standby, switch roles, then upgrade the new standby. If you need to update FXOS, do that on both chassis before you upgrade Firewall Threat Defense on either. Again, always upgrade the standby.

Caution Do not make or deploy configuration changes on one unit while the other is upgrading, or to a mixed version pair. 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. You can manually cancel failed or in-progress major and maintenance upgrades, and retry failed upgrades. If you continue to have issues, contact Cisco TAC.

For details on these and other issues you may encounter during upgrade, see Troubleshooting Threat Defense Upgrades, on page 52.

Before you begin

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

Procedure

Step 1 Log into the standby unit.

Step 2 Select **Device**, then click **View Configuration** in the Updates panel.
The System Upgrade panel shows the currently running software version and any upgrade package that you have already uploaded.

Step 3 Upload the upgrade package.

You can upload one package only. If you upload a new package, it replaces the old one. Make sure you have the correct package for your target version and device model. Click **Browse** or **Replace File** to begin the upload.

When the upload completes, the system displays a confirmation dialog box. Before you click **OK**, optionally select **Run Upgrade Immediately** to choose rollback options and upgrade now. If you upgrade now, it is especially important to have completed as much of the pre-upgrade checklist as possible (see the next step).

Step 4 Perform final pre-upgrade checks, including the readiness check.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks. If you do not run the readiness check manually, it runs when you initiate the upgrade. If the readiness check fails, the upgrade is canceled. For more information, see Upgrade Readiness Checks for Firewall Threat Defense, on page 46.

Step 5 Click **Upgrade Now** to start the upgrade.

a) Choose rollback options.

You can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon major or maintenance upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade.

b) Click **Continue** to upgrade and reboot the device.

You are automatically logged off and taken to a status page where you can monitor the upgrade until the device reboots. The page also includes an option to cancel the in-progress installation. If you disabled automatic rollback and the upgrade fails, you can manually cancel or retry the upgrade.

Traffic is dropped while you upgrade. For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

Step 6 Log back in when you can and verify upgrade success.

The Device Summary page shows the currently running software version and high availability status. Do not proceed until you have verified success *and* high availability has resumed. If high availability remains suspended after successful upgrade, see Troubleshooting Threat Defense Upgrades, on page 52.

Step 7 Upgrade the second unit.

a) Switch roles, making this device active: Select **Device** > **High Availability**, then select **Switch Mode** from the gear menu ( ). Wait for the unit's status to change to active and confirm that traffic is flowing normally. Log out.

b) Upgrade: Repeat the previous steps to log into the new standby, upload the package, upgrade the device, monitor progress, and verify success.

Step 8 Examine device roles.

If you have preferred roles for specific devices, make those changes now.

Step 9 Log into the active unit.

Step 10 Complete post-upgrade tasks.

a) Update system databases. If you do not have automatic updates configured for intrusion rules, VDB, and GeoDB, update them now.

b) Complete any other required post-upgrade configuration changes.

c) Deploy.

What to do next

- For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for the upgraded logical devices. 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 a 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 a snapshot of your freshly upgraded deployment.

Monitor Firewall Threat Defense Upgrades

When you start the Firewall Threat Defense upgrade, you are automatically logged off and taken to a status page where you can monitor overall upgrade progress. The page also includes an option to cancel the in-progress installation. If you disabled automatic rollback and the upgrade fails, the page allows you to manually cancel or retry the upgrade.

You can also SSH to the device and use the CLI: **show upgrade status**. Add the **continuous** keyword to view log entries as they are made, and **detail** to see detailed information. Add both keywords to get continuous detailed information.

After the upgrade completes, you lose access to the status page and the CLI when the device reboots.

Cancel or Retry Firewall Threat Defense Upgrades

Use the upgrade status page or the CLI to manually cancel failed or in-progress major or maintenance upgrades, and to retry failed upgrades:

- Upgrade status page: Click **Cancel Upgrade** to cancel an in-process upgrade. If the upgrade fails, you can click **Cancel Upgrade** to stop the job and to return to the state of the device prior to the upgrade, or click **Continue** to retry the upgrade.
- CLI: Use **upgrade cancel** to cancel an in-process upgrade. If the upgrade fails, you can use **upgrade cancel** to stop the job and to return to the state of the device prior to the upgrade, or use **upgrade retry** to retry the upgrade.



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. In a high availability deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

Cancel and retry are not supported for patches. For information on reverting a successful upgrade, see Revert Firewall Threat Defense, on page 51.

Revert Firewall Threat Defense

If an upgrade succeeds but the system does not function to your expectations, you may be able to revert. Reverting Firewall Threat Defense returns the software to its state just before the last upgrade; post-upgrade configuration changes are not retained. Reverting after patching (fourth-digit upgrades) necessarily removes patches as well. You cannot revert individual patches or hotfixes.

The following procedure explains how to revert from Firewall Device Manager. If you cannot get into Firewall Device Manager, you can revert from the Firewall Threat Defense command line in an SSH session using the **upgrade revert** command. You can use the **show upgrade revert-info** command to see what version the system will revert to.

Before you begin

If the unit is part of a high availability pair, you must revert both units. Ideally, initiate the revert on both units at the same time so that the configuration can be reverted without failover issues. Open sessions with both units and verify that revert will be possible on each, then start the processes. Note that traffic will be interrupted during the revert, so do this at off hours if at all possible.

For the Firepower 4100/9300 chassis, major Firewall Threat Defense versions have a specially qualified and recommended companion FXOS version. This means that after you revert the Firewall Threat Defense software, you might be running a non-recommended version of FXOS (too new). Although newer versions of FXOS are backwards compatible with older the Firewall Threat Defense versions, we do perform enhanced testing for the recommended combinations. You cannot downgrade FXOS, so if you find yourself in this situation, and you want to run a recommended combination, you will need to reimage the device.

Procedure

Step 1 Select **Device**, then click **View Configuration** in the **Updates** summary.

Step 2 In the **System Upgrade** section, click the **Revert Upgrade** link.

You are presented with a confirmation dialog box that shows the current version and the version to which the system will revert. If there is no available version to revert to, there will not be a **Revert Upgrade** link.

Step 3 If you are comfortable with the target version (and one is available), click **Revert**.

What to do next

- Re-register the device with the Smart Software Manager.
- For the Firepower 4100/9300, set a new Firewall Threat Defense startup version for the reverted 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 a post-revert backup, the backup and startup versions match. For more information, see the *Image Management* chapter in the *Cisco Firepower 4100/9300 FXOS Secure Firewall Chassis Manager Configuration Guide*, or the *Cisco Firepower 4100/9300 FXOS Command Reference*.

Troubleshooting Threat Defense Upgrades

General Upgrade Troubleshooting

These issues can occur when you are upgrading any device, whether standalone or in a high availability pair.

Upgrade package errors.

To find the correct upgrade package, select or search for your model on the Cisco Support & Download site, then browse to the software download page for the appropriate version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), software version, and build.

Upgrade packages from Version 6.2.1+ are signed, and terminate in .sh.REL.tar. If you are upgrading from an older version, download the package that terminates in .sh instead. The Cisco Support & Download site indicates the correct package for your version. Do not untar signed upgrade packages. Do not rename upgrade packages or transfer them by email.

Cannot reach the device at all during upgrade.

Devices 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.

Device appears inactive or is unresponsive during upgrade.

You can manually cancel in-progress major and maintenance upgrades; see Cancel or Retry Firewall Threat Defense Upgrades, on page 51. If the device is unresponsive, or if you cannot cancel the upgrade, contact Cisco TAC.

Caution 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.

Upgrade is successful but the system does not function to your expectations.

First, make sure that cached information gets refreshed. Do not simply refresh the browser window to log back in. Instead, delete any "extra" path from the URL and reconnect to the home page; for example, http://threat-defense.example.com/.

If you continue to have issues and need to return to an earlier major or maintenance release, you may be able to revert; see Revert Firewall Threat Defense, on page 51. If you cannot revert, you must reimage.

Upgrade fails.

When you initiate a major or maintenance upgrade, you use the **Automatically cancel on upgrade failure...** (auto-cancel) option to choose what happens if upgrade fails, as follows:

- Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. Correct any issues and try again later.
- Auto-cancel disabled: If upgrade fails, the device remains as it is. Correct the issues and retry immediately, or manually cancel the upgrade and try again later.

For more information, see Cancel or Retry Firewall Threat Defense Upgrades, on page 51. If you cannot retry or cancel, or if you continue to have issues, contact Cisco TAC.

High Availability Upgrade Troubleshooting

These issues are specific to high availability upgrades.

Upgrade will not begin without deploying uncommitted changes.

If you get an error message stating that you must deploy all uncommitted changes even though there are none, log into the active unit (remember, you should be upgrading the standby), create some minor change, and deploy. Then, undo the change, redeploy, and try the upgrade again on the standby.

If this does not work, and the units are running different software versions against recommendations, switch roles to make the standby unit active, then suspend high availability. Deploy from the active/suspended unit, resume high availability, then switch roles to make the active unit the standby again. Upgrade should then work.

Deployment from active unit fails during standby upgrade, or causes an application synchronization error.

This can happen if you deploy from the active unit while the standby is upgrading, which is not supported. Proceed with the upgrade despite the error. After you upgrade both units, make any required configuration changes and deploy from the active unit. The error should resolve.

To avoid these issues, do not make or deploy configuration changes on one unit while the other is upgrading, or to a mixed version pair.

Configuration changes made during upgrade are lost.

If you absolutely must make and deploy changes to a mixed version pair, you must make the changes to both units or they will be lost after you upgrade the down-level active unit.

High availability is suspended after upgrade.

After the post-upgrade reboot, high availability is briefly suspended while the system performs some final automated tasks, such as updating libraries and restarting Snort. You are most likely to notice this if you log into the CLI *very* shortly after upgrade. If high availability does not resume on its own after the upgrade fully completes and Firewall Device Manager is available, do it manually:

1. Log into both the active device and the standby device and check the task lists. Wait until all tasks are finished running on both devices. If you resume high availability too soon, you may have a future issue where failover causes an outage.
2. Select **Device** > **High Availability**, then select **Resume HA** from the gear menu ( ).

Failover does not occur with a mixed version pair.

Although an advantage of high availability is that you can upgrade your deployment without traffic or inspection interruptions, failover is disabled during the entire upgrade process. That is, not only is failover necessarily disabled when one device is offline (because there is nothing to fail over to—you are essentially already failed over), but failover is also disabled with mixed version pairs. During upgrade is the only time where mixed version pairs are (temporarily) allowed. Schedule upgrades during maintenance windows when they will have the least impact if something goes wrong, and make sure you have enough time to upgrade both devices in that window.

Upgrade failed on only one device, or one device was reverted. The pair is now running mixed versions.

Mixed version pairs are not supported for general operations. Either upgrade the down-version device or revert the higher version device. For patches, because revert is not supported, if you cannot successfully upgrade the down-version device you must break high availability, reimage one or both devices, then re-establish high availability.