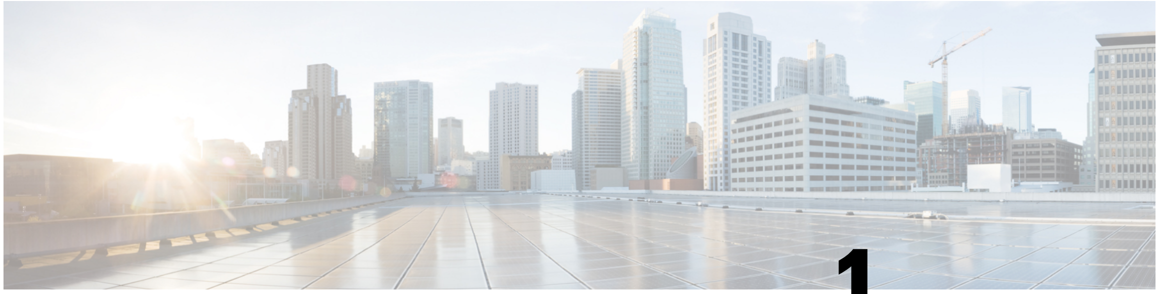
Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center, Version 7.2.0–7.2.5

First Published: 2022-06-06

Last Modified: 2024-05-29

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

CONTENTS



CHAPTER 1

Getting Started

Is this Guide for You?

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 FMC

Current FMC 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 FTD with FMC

Current FMC Version	Guide
Cloud-delivered Firewall Management Center	Cisco Secure Firewall Threat Defense Upgrade Guide for Cloud-Delivered Firewall Management Center
7.2+	Cisco Secure Firewall Threat Defense Upgrade Guide for Management Center for your version

Current FMC Version	Guide
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 FTD with FDM

Current FTD 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 CDO	Managing FDM Devices with Cisco Defense Orchestrator

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 FMC	Cisco Secure Firewall Threat Defense/Firepower Hotfix Release Notes
Latest	Firmware for the Firepower 4100/9300	Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide

Planning Your Upgrade

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 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

For Assistance

Upgrade Guides

In management center deployments, the management center must run the same or newer version as its managed devices. Upgrade the management center first, then devices. Note that you always want to use the upgrade guide for the version of management center or device manager that you are *currently* running—not your target version.

Table 6: Upgrade Guides

Platform	Upgrade Guide	Link
Management center	Management center version you are *currently* running.	https://www.cisco.com/go/fmc-upgrade
Threat defense with management center	Management center version you are *currently* running.	https://www.cisco.com/go/ftd-fmc-upgrade
Threat defense with device manager	Threat defense version you are *currently* running.	https://www.cisco.com/go/ftd-fdm-upgrade
Threat defense with cloud-delivered Firewall Management Center	Cloud-delivered Firewall Management Center.	https://www.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 threat defense version on an FXOS device, perform a full reimage—even for devices where the operating system and software are bundled.

Table 7: Install Guides

Platform	Install Guide	Link
Management center hardware	Getting started guide for your management center hardware model.	https://www.cisco.com/go/fmc-install
Management center virtual	Getting started guide for the management center virtual.	https://www.cisco.com/go/fmcv-quick
Threat defense hardware	Getting started or reimage guide for your device model.	https://www.cisco.com/go/ftd-quick
Threat defense virtual	Getting started guide for your threat defense virtual version.	https://www.cisco.com/go/ftdv-quick
FXOS for the Firepower 4100/9300	Configuration guide for your FXOS version, in the *Image Management* chapter.	https://www.cisco.com/go/firepower9300-config
FXOS for the Firepower 1000 and Secure Firewall 3100	Troubleshooting guide, in the *Reimage Procedures* chapter.	Cisco FXOS Troubleshooting Guide for the Firepower 1000/2100 and Secure Firewall 3100/4200 with Firepower 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: http://www.cisco.com/go/ftd-docs
- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.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 6.2.3.

- Device Platforms, on page 7
- Device Management, on page 8

Device Platforms

Firepower 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 Device Management, on page 8. For general compatibility information, see the Cisco Secure Firewall Threat Defense Compatibility Guide.

FTD Hardware

Version 6.2.3 FTD hardware comes in a range of throughputs, scalability capabilities, and form factors.

Table 8: Version 6.2.3 FTD Hardware

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
Firepower 4110, 4120, 4140, 4150 Firepower 9300: SM-24, SM-36, SM-44 modules	YES	—	—	—	Requires FXOS 2.3.1.73 or later build. **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+. We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.

Platform	FMC Compatibility		FDM Compatibility		Notes
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO	
ASA 5506-X, 5506H-X, 5506W-X ASA 5512-X ASA 5515-X ASA 5508-X, 5516-X ASA 5525-X, 5545-X, 5555-X	YES	—	YES	—	ASA 5506-X, 5508-X, and 5516-X devices may require a ROMMON update. See the Cisco Secure Firewall ASA and Secure Firewall Threat Defense Reimage Guide.

FTDv

Version 6.2.3 supports the following FTDv implementations. For information on supported instances, throughputs, and other hosting requirements, see the Cisco Secure Firewall Threat Defense Virtual Getting Started Guide.

Table 9: Version 6.2.3 FTDv Platforms

Device Platform	FMC Compatibility		FDM Compatibility	
	Customer Deployed	Cloud Delivered	FDM Only	FDM + CDO
Public Cloud				
Amazon Web Services (AWS)	YES	—	—	—
Microsoft Azure	YES	—	—	—
Private Cloud				
Kernel-based virtual machine (KVM)	YES	—	YES	—
VMware vSphere/VMware ESXi 5.5, 6.0, or 6.5	YES	—	YES	—

Device Management

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

CHAPTER 3

Software Upgrade Guidelines

For your convenience, this document duplicates the critical and release-specific software upgrade guidelines published in the FTD release notes. For FXOS upgrade guidelines for the Firepower 4100/9300, see Upgrade Guidelines for the Firepower 4100/9300 Chassis, on page 35.

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

Minimum Version to Upgrade

You can upgrade directly to Version 6.2.3 as follows.

Table 10: Minimum Version to Upgrade to Version 6.2.3

Platform	Minimum Version
FTD	6.1 with FMC 6.2 with FDM FXOS 2.3.1.73 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, 2.3(1). **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+.

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. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

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,.

Table 11: Upgrade Time Considerations

Consideration	Details
Versions	Upgrade time usually increases if your upgrade skips versions.
Models	Upgrade time usually increases with lower-end models.
Virtual appliances	Upgrade time in virtual deployments is highly hardware dependent.
High availability and clustering	In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how they are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.
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

CHAPTER 4

Upgrade the FMC

This chapter explains how to upgrade a customer-deployed FMC that is *currently running* Version 6.2.3.

If you are using the cloud-delivered Firewall Management Center, you do not need this chapter because we take care of FMC feature updates. Upgrade your devices using the latest released version of the Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center.

Upgrade Checklist for FMC

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 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 FTD, on page 24 • Upgrade Paths for FXOS, on page 36

✓	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 9, for critical and release-specific upgrade guidelines. • , for new and deprecated features that have upgrade impact. Check all versions between your current and target version. • Cisco Firepower Release Notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool. • Cisco Firepower 4100/9300 FXOS Release Notes, for FXOS upgrade guidelines for the Firepower 4100/9300.
	Check bandwidth.	Make sure your management network has the bandwidth to perform large data transfers. Whenever possible, upload upgrade packages ahead of time.
	Schedule maintenance windows.	Schedule maintenance windows when they will have the least impact, especially considering the time the upgrade is likely to take. Consider the tasks you must perform in the window, and those you can perform ahead of time. SeeTime and Disk Space Tests.

Backups

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

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

✓	Action/Check	Details
	Back up configurations and events.	See the *Backup and Restore* chapter in the Firepower Management Center 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 FMC.	Upgrade packages are available on the Cisco Support & Download site. You may also be able to use the FMC to perform a direct download. For FMC high availability, you must upload the FMC upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization. See Upload Upgrade Packages for FMC, on page 16.

Associated Upgrades

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

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

Final Checks

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

✓	Action/Check	Details
	Check configurations.	Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.
	Check NTP synchronization.	Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure.
	Deploy configurations.	Deploying configurations before you upgrade reduces the chance of failure. Deploying can affect traffic flow and inspection; see .
	Run readiness checks.	Passing readiness checks reduces the chance of upgrade failure. See Run Readiness Checks for FMC, on page 17.
	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 management center, choose **System** (⚙) > **Monitoring** > **Statistics** and select the FMC. Under Disk Usage, expand the By Partition details.

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

Upgrade Path for FMC

This table provides the upgrade path for customer-deployed FMCs.

The FMC must run the same or newer version as its managed devices. You cannot upgrade a device past the FMC. Even for maintenance (third-digit) releases, you must upgrade the FMC first.

Note that if your current FTD 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 12: FMC 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
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 FMC 1000, 2500, and 4500.	Any of: → 7.4.x → 7.3.x → 7.2.x → 7.1.x → Any later 7.0.x release **Note** Due to datastore incompatibilities, you cannot upgrade from Version 7.0.4+ to Version 7.1.0. We recommend you upgrade directly to Version 7.2+.
6.7	Any of: → 7.2.x → 7.1.x → 7.0.x → Any later 6.7.x release
6.6 Last support for FMC 2000 and 4000.	Any of: → 7.2.x → 7.1.x → 7.0.x → 6.7.x → Any later 6.6.x release **Note** Due to datastore incompatibilities, you cannot upgrade the FMC from Version 6.6.5+ to Version 6.7.0. We recommend you upgrade directly to Version 7.0+.
6.5	Any of: → 7.1.x → 7.0.x → 6.7.x → 6.6.x

Current Version	Target Version
6.4 Last support for FMC 750, 1500, and 3500.	Any of: → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Any of: → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3	Any of: → 6.6.x → 6.5 → 6.4 → 6.3

Upload Upgrade Packages for FMC

Use this procedure to manually upload upgrade packages to the FMC.

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

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

Before you begin

If you are upgrading the standby FMC in a high availability pair, pause synchronization.

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

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

You use the same software upgrade package for all models in a family or series. To find the correct one, select or search for your model, then browse to the software download page for the appropriate version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads.

Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), software version, and build, like this:

```
Cisco_Firepower_Mgmt_Center_Upgrade-6.2.3-999.sh.REL.tar
```

Step 2 On the FMC, choose **System** (⚙) > **Updates**.

Step 3 Click **Upload Update**.

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

Step 5 Click **Choose File**.

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

Run Readiness Checks for FMC

Use this procedure to run FMC readiness checks.

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

Before you begin

Upload the upgrade package to the FMC.

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

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

Step 3 Click **Check Readiness**.

You can monitor readiness check progress in the Message Center.

What to do next

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

Upgrade the FMC: Standalone

Use this procedure to upgrade a standalone FMC.

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

Before you begin

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

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

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

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

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

Step 4 Log back in when you can.

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

Step 5 Verify upgrade success.

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

Step 6 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

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

Step 7 Complete any required post-upgrade configuration changes.

Step 8 Redeploy configurations to all managed devices.

Upgrade the FMC: High Availability

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

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

Before you begin

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

Step 1 On the active FMC, pause synchronization.

a) Choose **System** (⚙) > **Integration**.
b) On the **High Availability** tab, click **Pause Synchronization**.

Step 2 Upload the upgrade package to the standby.

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

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

Follow the instructions in Upgrade the FMC: Standalone, on page 18, stopping after you verify update success on each peer. In summary, for each peer:

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

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

a) Choose **System** (⚙) > **Integration**.
b) On the **High Availability** tab, click **Make-Me-Active**.
c) Wait until synchronization restarts and the other FMC switches to standby mode.

Step 5 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

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

Step 6 Complete any required post-upgrade configuration changes.

Step 7 Redeploy configurations to all managed devices.

CHAPTER 5

Upgrade FTD

This chapter explains how to use a Version 6.2.3 FMC to upgrade threat defense. If your FMC is running a different version, or if you are using the cloud-delivered management center, see Is this Guide for You?, on page 1.

Upgrade Checklist for FTD

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 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 FTD, on page 24 • Upgrade Paths for FXOS, on page 36

✓	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 9, for critical and release-specific upgrade guidelines. • , for new and deprecated features that have upgrade impact. Check all versions between your current and target version. • Cisco Firepower Release Notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version. If you have a support contract, you can obtain up-to-date bug lists with the Cisco Bug Search Tool. • Cisco 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 Chassis Upgrades, on page 36 • Time and Disk Space Tests

Backups

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

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

✓	Action/Check	Details
	Back up FTD.	If you have a Firepower 9300 with FTD 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.	

Upgrade Packages

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

Associated Upgrades

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

✓	Action/Check	Details
	Upgrade virtual hosting.	If needed, upgrade the hosting environment. If this is required, it is usually because you are running an older version of VMware and are performing a major upgrade.
	Upgrade firmware on the Firepower 4100/9300.	We recommend the latest firmware. See the Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide.
	Upgrade FXOS on the Firepower 4100/9300.	Upgrading FXOS is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To minimize disruption, upgrade FXOS in FTD high availability pairs one chassis at a time. See Upgrade the Chassis on the Firepower 4100/9300, on page 35.

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.
	Deploy configurations.	Deploying configurations before you upgrade reduces the chance of failure. Deploying can affect traffic flow and inspection; see .

✓	Action/Check	Details
	Run readiness checks.	Passing readiness checks reduces the chance of upgrade failure.
	Check disk space.	Readiness checks include a disk space check. Without enough free disk space, the upgrade fails.
	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.

Upgrade Paths for FTD

Choose the upgrade path that matches your deployment.

Upgrade Path for FTD without FXOS

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

Note that if your current FTD 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 13: FTD 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.

Current Version	Target Version
7.1	Any of: → 7.4.x → 7.3.x → 7.2.x → Any later 7.1.x release
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** The cloud-delivered Firewall Management Center cannot manage FTD 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 Version 7.2+.
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

Current Version	Target Version
6.5	Any of: → 7.1.x → 7.0.x → 6.7.x → 6.6.x
6.4 Last support for ASA 5515-X.	Any of: → 7.0.x → 6.7.x → 6.6.x → 6.5
6.3	Any of: → 6.7.x → 6.6.x → 6.5 → 6.4
6.2.3 Last support for ASA 5506-X series.	Any of: → 6.6.x → 6.5 → 6.4 → 6.3

Upgrade Path for FTD with FXOS

This table provides the upgrade path for FTD on the Firepower 4100/9300.

Note that if your current FTD 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 14: FTD Direct Upgrades on the Firepower 4100/9300

Current Versions	Target Versions
FXOS 2.13 with threat defense 7.3	→ FXOS 2.13 with any later threat defense 7.3.x release
FXOS 2.12 with 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 threat defense 7.3.x → FXOS 2.12 with any later threat defense 7.2.x release
FXOS 2.11.1 with threat defense 7.1	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with any later threat defense 7.1.x release
FXOS 2.10.1 with threat defense 7.0	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with 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** The cloud-delivered Firewall Management Center cannot manage FTD 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 Version 7.2+.
FXOS 2.9.1 with threat defense 6.7	Any of: → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with any later threat defense 6.7.x release

Current Versions	Target Versions
FXOS 2.8.1 with threat defense 6.6	Any of: → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with any later threat defense 6.6.x release
FXOS 2.7.1 with threat defense 6.5	Any of: → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with threat defense 6.6.x

Upgrade Order for FTD High Availability with FXOS

Upgrade Packages for FTD

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 from Version 6.2.1+ are signed, and terminate in .sh.REL.tar, as listed in the following table. 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.

Table 15: Software Upgrade Packages

Platform	Upgrade Package
ASA 5500-X series with FTD	Cisco_FTD_Upgrade-6.2.3-999.sh.REL.tar

Upload FTD Upgrade Packages to the FMC

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

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

Step 2 Click **Upload Update**.

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

Step 4 Click **Choose File**.

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

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

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

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

b) Choose destination devices.

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

c) Click **Push**.

Upload FTD Upgrade Packages to an Internal Server

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

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

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

Before you begin

Copy the upgrade packages to an internal web server that your devices can access. For secure web servers (HTTPS), obtain the server's digital certificate (PEM format). You should be able to obtain the certificate from the server's administrator. You may also be able to use your browser, or a tool like OpenSSL, to view the server's certificate details and export or copy the certificate.

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

Step 2 Click **Upload Update**.

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

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

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

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

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

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

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

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

Step 6 Click **Save**.

The location is saved. Uploaded upgrade packages and upgrade package URLs are listed together, but are labeled distinctly.

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

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

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

b) Choose destination devices.

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

c) Click **Push**.

Upgrade FTD with the Wizard

Use this procedure to upgrade FTD using a wizard. Note that you must still use **System** (⚙) > **Updates** to manage upgrade packages and to upgrade the FMC and older Classic devices.

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

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

Note that neither your workflow nor threat defense upgrade packages are synchronized between high availability FMCs. In case of failover, you must recreate your workflow on the new active FMC, which includes uploading upgrade packages to the FMC and performing readiness checks. (Upgrade packages already copied to devices are not removed, but the FMC still must have the package or a pointer to its location.)

Note The wizard does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the workflow displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all.

To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the workflow before you click **Next**.

Before you begin

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

Begin workflow.

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

Select devices to upgrade and copy upgrade packages.

Step 2 Verify your device selection.

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

Step 3 Select the devices you want to upgrade.

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

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

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

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

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

Step 5 Verify your device selection.

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

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

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

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

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

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

Step 8 Click **Next**.

Perform compatibility, readiness, and other final checks.

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

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

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

Step 10 Perform final pre-upgrade checks.

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

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

Step 12 Click **Next**.

Upgrade devices.

Step 13 Verify your device selection and target version.

Step 14 Choose rollback options.

For major and maintenance upgrades, 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 upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

This option is not supported for patches.

Step 15 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

You can monitor overall upgrade progress in the Message Center. For detailed progress, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center. For information on traffic handling during the upgrade, see .

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

Verify success and complete post-upgrade tasks.

Step 16 Verify success.

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

Step 17 (Optional) In high availability/scalability deployments, examine device roles.

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

Step 18 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

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

Step 19 Complete any required post-upgrade configuration changes.

Step 20 Redeploy configurations to the devices you just upgraded.

What to do next

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

Upgrade FTD with System > Updates

Use this procedure to upgrade FTD using the System Updates page.

Before you begin

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

Step 1 On the FMC, choose **System** (⚙) > **Updates**.

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

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

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

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

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

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

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

Step 4 Choose the devices to upgrade.

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

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

Step 5 Choose rollback options.

For major and maintenance upgrades, 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 upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

This option is not supported for patches.

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

You can monitor upgrade progress in the Message Center. For information on traffic handling during the upgrade, see .

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

Step 7 Verify success.

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

Step 8 (Optional) In high availability/scalability deployments, examine device roles.

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

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

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

Step 10 Complete any required post-upgrade configuration changes.

Step 11 Redeploy configurations to the devices you just upgraded.

CHAPTER 6

Upgrade the Chassis on the Firepower 4100/9300

Cisco Firepower 4100/9300 FXOS Release Notes, 2.3(1)

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 FTD 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 16: Upgrade Guidelines for the Firepower 4100/9300 Chassis

Guideline	Details
FXOS upgrades.	FXOS 2.3.1.73+ is required to run threat defense Version 6.2.3 on the Firepower 4100/9300. **Note** Firepower 6.2.3.16+ requires FXOS 2.3.1.157+. 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 Cisco 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 36.

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.

Upgrade Paths for FXOS

Choose the upgrade path that matches your deployment.

Upgrade Path for FXOS with FTD

This table provides the upgrade path for FTD on the Firepower 4100/9300.

Note that if your current FTD 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 17: FTD Direct Upgrades on the Firepower 4100/9300

Current Versions	Target Versions
FXOS 2.13 with threat defense 7.3	→ FXOS 2.13 with any later threat defense 7.3.x release
FXOS 2.12 with 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 threat defense 7.3.x → FXOS 2.12 with any later threat defense 7.2.x release
FXOS 2.11.1 with threat defense 7.1	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with any later threat defense 7.1.x release
FXOS 2.10.1 with threat defense 7.0	Any of: → FXOS 2.13 with threat defense 7.3.x → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with 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** The cloud-delivered Firewall Management Center cannot manage FTD 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 Version 7.2+.
FXOS 2.9.1 with threat defense 6.7	Any of: → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with any later threat defense 6.7.x release

Current Versions	Target Versions
FXOS 2.8.1 with threat defense 6.6	Any of: → FXOS 2.12 with threat defense 7.2.x → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with any later threat defense 6.6.x release
FXOS 2.7.1 with threat defense 6.5	Any of: → FXOS 2.11.1 with threat defense 7.1.x → FXOS 2.10.1 with threat defense 7.0.x → FXOS 2.9.1 with threat defense 6.7.x → FXOS 2.8.1 with threat defense 6.6.x

Upgrade Path for FXOS with FTD and ASA

This table provides upgrade paths for the Firepower 9300 with FTD 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 FTD 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, FTD 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 18: FTD 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
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** The cloud-delivered Firewall Management Center cannot manage FTD 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 Version 7.2+.

Current Versions	Target Versions
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 FTD High Availability

Upgrade FXOS with Firepower Chassis Manager

Upgrade FXOS for Standalone FTD Logical Devices Using Firepower Chassis Manager

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

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

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

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 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.

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 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 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

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

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

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair.
- 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 9300 chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

Step 1 Connect to the FXOS CLI.

Step 2 Download the new platform bundle image to the Firepower 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 9300 chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

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

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

a) Enter firmware mode:

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

b) Download the FXOS platform bundle software image:

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

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

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

c) To monitor the download process:

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

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

Example:

The following example copies an image using the SCP protocol:

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

```
192.168.1.1(FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

Step 13 If necessary, return to firmware mode:

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

Step 14 Enter auto-install mode:

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

Step 15 Install the FXOS platform bundle:

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

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

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

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

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

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

Step 18 To monitor the upgrade process:

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

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

Example:

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

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

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

FP9300-A /system #
```

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

a) Enter **top**.

b) Enter **scope ssa**.

c) Enter **show slot**.

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

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

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

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

a) Connect to Firepower Management Center.

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

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

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

CHAPTER 7

Uninstall a Patch

You can uninstall most patches. If you need to return to an earlier major or maintenance release, you must reimage.

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

Revert Threat Defense

About Reverting FTD

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

Reverted Configurations

Configurations that are reverted include:

- Snort version.
- Device-specific configurations.

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

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

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

Configurations Not Reverted

Configurations that are not reverted include:

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

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

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

  Sync interface changes after a successful revert.

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

  If you are required to run the recommended combination of FXOS and FTD, you may need a full reimage; see Guidelines for Reverting FTD, on page 54.

Guidelines for Reverting FTD

System Requirements

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

Revert is not supported for:

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

Reverting High Availability or Clustered Devices

When you use the FMC web interface to revert FTD, you cannot select individual high availability units or clustered nodes. The system automatically reverts them simultaneously. This means that interruptions to traffic flow and inspection during revert depend on interface configurations only, as if every device were standalone.

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

Revert Does Not Downgrade FXOS

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

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

Scenarios Preventing Revert

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

Table 19: Scenarios Preventing Revert

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

Revert FTD with FMC

You must use the FMC to revert FTD. You cannot use the device CLI.

Threat Defense History:

- 7.1: Initial support.

Before you begin

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

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

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

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

Step 3 Confirm that you want to revert and reboot.

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

Step 4 Monitor revert progress.

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

Step 5 Verify revert success.

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

Step 6 (Firepower 4100/9300) Sync any interface changes you made to FTD logical devices using the Firepower Chassis Manager or the FXOS CLI.

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

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

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

Step 8 Redeploy configurations to the devices you just reverted.

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

Uninstall a Patch

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

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

Patches That Support Uninstall

Uninstalling specific patches can cause issues, *even when the uninstall itself succeeds*. These issues include:

- Inability to deploy configuration changes after uninstall.
- Incompatibilities between the operating system and the software.
- FSIC (file system integrity check) failure when the appliance reboots, if you patched with security certifications compliance enabled (CC/UCAPL mode).

Caution If security certifications compliance is enabled and the FSIC fails, the software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.

Version 6.6+ Patches That Support Uninstall

Uninstall is currently supported for all Version 6.6+ patches.

Version 6.5 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.5 patches. Uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 20: Version 6.5.0 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	ASA FirePOWER NGIPSv	FMC/FMCv
6.5.0.2+	6.5.0	6.5.0	6.5.0.1
6.5.0.1	6.5.0	6.5.0	—

Version 6.4 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.4 patches. Uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 21: Version 6.4.0 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
6.4.0.5+	6.4.0.4	6.4.0.4	6.4.0.4
6.4.0.4	—	—	—
6.4.0.3	6.4.0	—	—
6.4.0.2	6.4.0	—	—
6.4.0.1	6.4.0	6.4.0	6.4.0

Version 6.3 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.3 patches. Uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 22: Version 6.3.0 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall
6.3.0.5	—
6.3.0.1 through 6.3.0.4	6.3.0

Version 6.2.3 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.2.3 patches. Uninstalling returns you to the patch level you upgraded from. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 23: Version 6.2.3 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
6.2.3.16+	6.2.3.15	6.2.3.15	6.2.3.15
6.2.3.15	—	—	—
6.2.3.12 through 6.2.3.14	6.2.3	6.2.3.11	6.2.3.11

Current Version	Farthest Back You Should Uninstall		
	FTD/FTDv	Firepower 7000/8000 ASA FirePOWER NGIPSv	FMC/FMCv
6.2.3.11	6.2.3	—	—
6.2.3.8 through 6.2.3.10	6.2.3	6.2.3.7	6.2.3.7
6.2.3.7	6.2.3	—	—
6.2.3.1 through 6.2.3.6	6.2.3	6.2.3	6.2.3

Version 6.2.2 Patches That Support Uninstall

This table lists supported uninstall scenarios for Version 6.2.2 patches. Uninstalling returns you to the immediately preceding patch, even if you upgraded from an earlier patch. If uninstall will take you farther back than what is supported, we recommend you reimage and then upgrade to your desired patch level.

Table 24: Version 6.2.2 Patches That Support Uninstall

Current Version	Farthest Back You Should Uninstall
6.2.2.3 through 6.2.2.5	6.2.2.2
6.2.2.2	—
6.2.2.1	6.2.2

Uninstall Order for High Availability/Scalability

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

Table 25: Uninstall Order for FMC High Availability

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

Table 26: Uninstall Order for FTD High Availability and Clusters

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

Uninstall Device Patches with FMC

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

⚠

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

Before you begin

- Break FTD high availability pairs; see Uninstall Order for High Availability/Scalability, on page 59.
- Make sure your deployment is healthy and successfully communicating.

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

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

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

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

Firepower 4100/9300	`connect module slot_number console`, then `connect ftd` (first login only)

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

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

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

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

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

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

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

Step 6 Monitor the uninstall until you are logged out.

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

- FTD: `tail /ngfw/var/log/sf/update.status`
- ASA FirePOWER and NGIPSv: `tail /var/log/sf/update.status`

Otherwise, monitor progress in the console or terminal.

Step 7 Verify uninstall success.

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

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

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

Step 9 Redeploy configurations.

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

What to do next

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

Uninstall Standalone FMC Patches

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

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

Before you begin

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

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

Deploying before you uninstall reduces the chance of failure.

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

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

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

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

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

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

Step 5 Redeploy configurations to all managed devices.

Uninstall High Availability FMC Patches

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

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

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

Before you begin

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

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

Deploying before you uninstall reduces the chance of failure.

Step 2 On the active FMC, pause synchronization.

a) Choose **System** (⚙) > **Integration**.
b) On the **High Availability** tab, click **Pause Synchronization**.

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

Follow the instructions in Uninstall Standalone FMC Patches , on page 62, but omit the initial deploy, stopping after you verify uninstall success on each peer. In summary, for each peer:

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

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

a) Choose **System** (⚙) > **Integration**.
b) On the **High Availability** tab, click **Make-Me-Active**.
c) Wait until synchronization restarts and the other FMC switches to standby mode.

Step 5 Redeploy configurations to all managed devices.