



Cisco Secure Firewall Threat Defense Upgrade Guide for Device Manager, Version 7.4.1+

First Published: 2024-09-16

Last Modified: 2025-03-06

Americas Headquarters

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



CONTENTS

CHAPTER 1

Planning Your Upgrade 1

Is This Guide for You? 1

Compatibility 1

Upgrade Guidelines 1

Software Upgrade Guidelines 2

Upgrade Guidelines for the Firepower 4100/9300 Chassis 2

Upgrade Path 2

Upgrade Order 3

Upgrade Packages 4

Upgrade Readiness 5

Network and Infrastructure Checks 5

Configuration and Deployment Checks 5

Backups 6

Software Upgrade Readiness Checks 6

CHAPTER 2

Upgrade Threat Defense 7

Upgrade Readiness Checks for Threat Defense 7

Upgrade Standalone Threat Defense 8

Upgrade High Availability Threat Defense 9

Monitor Threat Defense Upgrades 11

Cancel or Retry Threat Defense Upgrades 11

Revert Threat Defense 12

CHAPTER 3

Upgrade the Firepower 4100/9300 Chassis 13

Upgrade FXOS with Chassis Manager 13

Upgrade FXOS for Standalone FTD Logical Devices Using Firepower Chassis Manager 13

Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager	15
Upgrade FXOS on the Firepower 4100/9300 with the CLI	18
Upgrade FXOS for Standalone FTD Logical Devices Using the FXOS CLI	18
Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI	20

CHAPTER 4**Troubleshooting and Reference 27**

Troubleshooting High Availability Threat Defense Upgrade	27
Unresponsive and Failed Threat Defense Upgrades	28
Traffic Flow and Inspection	29
Traffic Flow and Inspection for Threat Defense Upgrades	30
Traffic Flow and Inspection for Chassis Upgrades	30
Traffic Flow and Inspection when Deploying Configurations	30
Time and Disk Space	31
Upgrade Feature History	32



CHAPTER 1

Planning Your Upgrade

Use this guide to plan and complete threat defense upgrades. Upgrades can be major (A.x), maintenance (A.x.y), or patch (A.x.y.z) releases. We also may provide hotfixes, which are minor updates that address particular, urgent issues.

- [Is This Guide for You?, on page 1](#)
- [Compatibility, on page 1](#)
- [Upgrade Guidelines, on page 1](#)
- [Upgrade Path, on page 2](#)
- [Upgrade Order, on page 3](#)
- [Upgrade Packages, on page 4](#)
- [Upgrade Readiness, on page 5](#)

Is This Guide for You?

The procedures in this guide are for upgrading threat defense if you are currently running Version 7.4.1–7.7.x.

Compatibility

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

For compatibility information, see:

- [Cisco Secure Firewall Threat Defense Compatibility Guide](#)
- [Cisco Firepower 4100/9300 FXOS Compatibility](#)

Upgrade Guidelines

See the release notes for release-specific upgrade warnings and guidelines, and for information on features and bugs with upgrade impact. For general information on time/disk space requirements and on system

behavior during upgrade—which can include interruptions to traffic flow and inspection—see [Troubleshooting and Reference, on page 27](#).

Software Upgrade Guidelines

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

Upgrade Guidelines for the Firepower 4100/9300 Chassis

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

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

Upgrade Path

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

Supported Direct Upgrades

This table shows the supported direct upgrades for threat defense software. Note that although you can upgrade directly to maintenance (third-digit) releases, patches change the fourth digit only. You cannot upgrade directly to a patch from a previous major or maintenance release.

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

Table 1: Supported Direct Upgrades for Major and Maintenance Releases

Current Version	Target Software Version								
	to 7.7	7.6	7.4	7.3	7.2	7.1	7.0	6.6	6.4
	Firepower 4100/9300 FXOS Version for Chassis Upgrades								
	to 2.17	2.16	2.14	2.13	2.12	2.11	2.10	2.8	2.6
from 7.7	YES	—	—	—	—	—	—	—	—
7.6	YES	YES	—	—	—	—	—	—	—
7.4	YES	YES	YES *	—	—	—	—	—	—
7.3	YES	YES	YES	YES	—	—	—	—	—
7.2	YES	YES	YES	YES	YES	—	—	—	—
7.1	—	YES	YES	YES	YES	YES	—	—	—

Current Version	Target Software Version								
	to 7.7	7.6	7.4	7.3	7.2	7.1	7.0	6.6	6.4
	Firepower 4100/9300 FXOS Version for Chassis Upgrades								
	to 2.17	2.16	2.14	2.13	2.12	2.11	2.10	2.8	2.6
7.0	—	—	YES	YES	YES	YES	YES	—	—
6.6	—	—	—	—	YES	YES	YES	YES	—
6.4	—	—	—	—	—	—	YES	YES	—

* You cannot upgrade to Version 7.4.0, which is not available with device manager. Instead, upgrade to Version 7.4.1+.

Choosing a Maintenance Release



Important In most cases, we recommend you go directly to the latest maintenance release in your chosen major version.

Features, enhancements, and critical fixes included in maintenance releases (third-digit) and patches (fourth-digit) can skip future releases, depending on release date, release type (short term vs. long term), and other factors. To minimize upgrade and other impact, do not upgrade to a release that deprecates features or fixes. If you cannot go to the latest maintenance release, at least make sure your target version was released on a date after your current version. If you are running a patch, you may also want to check that the patch was also released after your target version, depending on the included fixes. For a full list of release dates including patches, see [Cisco Secure Firewall Device Manager New Features by Release](#).

If your current version is not listed next to your target version here, choose a later target.

Table 2: Released Before Version 7.7.x, by Date

Target Version		Current Version: is yours listed?				
		from 7.2	7.3	7.4	7.6	7.7
to 7.7.0	2025-03-05	7.2.0–7.2.9	7.3.0–7.3.1	7.4.0–7.4.2	7.6.0	—

Upgrade Order

Chassis Before Threat Defense

For the Firepower 4100/9300, major versions require a FXOS upgrade.

Because you upgrade the chassis first, you will briefly run a supported—but not recommended—combination, where the operating system is "ahead" of threat defense. If the chassis is already well ahead of its devices, further chassis upgrades can be blocked. In this case perform a three (or more) step upgrade: devices first,

then the chassis, then devices again. Or, perform a full reimage. In high availability deployments, upgrade one chassis at a time.

Chassis with High Availability Threat Defense

When a chassis upgrade is required in high availability deployments, upgrade one chassis at a time.

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

Threat Defense Deployment	Upgrade Order
Standalone	1. Upgrade chassis. 2. Upgrade threat defense.
High availability	Upgrade both chassis before you upgrade threat defense. To minimize disruption, always upgrade the standby. In the following scenario, Device A is the original active device and Device B is the original standby. 1. Upgrade chassis with the standby device (B). 2. Switch roles. 3. Upgrade chassis with the new standby device (A). 4. Upgrade threat defense on the new standby device (A). 5. Switch roles again. 6. Upgrade threat defense on the original standby device (B).

Upgrade Packages

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

Threat Defense Packages

You use the same upgrade package for all models in a family or series. To find the correct one, select or search for your model, then browse to the software download page for the appropriate version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads. Upgrade package file names reflect the platform, software version, and build. Upgrade packages are signed, and terminate in .sh.REL.tar. Do not untar or rename them.

Table 4: Threat Defense Packages

Platform	Package	Notes
Firepower 1000	Cisco_FTD_SSP-FP1K_Upgrade-Version-build.sh.REL.tar	—
Firepower 2100	Cisco_FTD_SSP-FP2K_Upgrade-Version-build.sh.REL.tar	Cannot upgrade past Version 7.4.x.

Platform	Package	Notes
Firepower 4100/9300	Cisco_FTD_SSP_Upgrade-Version-build.sh.REL.tar	—
Secure Firewall 1200	Cisco_Secure_FW_TD_1200-Version-build.sh.REL.tar	—
Secure Firewall 3100	Cisco_FTD_SSP-FP3K_Upgrade-Version-build.sh.REL.tar	—
Threat defense virtual	Cisco_FTD_Upgrade-Version-build.sh.REL.tar	—
ISA 3000 with FTD	Cisco_FTD_Upgrade-Version-build.sh.REL.tar	—

Chassis Packages for the Firepower 4100/9300

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

Table 5: FXOS Packages

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

Upgrade Readiness

Network and Infrastructure Checks

Appliance Access

Devices can stop passing traffic during the upgrade or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface.

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.

Configuration and Deployment Checks

Configurations

Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes. Deploy configuration changes. Note that you will need to deploy again after upgrade.

Deploying typically restarts Snort, which can affect traffic flow and inspection; see [Traffic Flow and Inspection when Deploying Configurations](#), on page 30.

Deployment Health

Make sure devices are healthy and successfully communicating. You should especially make sure you are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. To check time, use the **show time** CLI command.

Running Tasks and Scheduled Tasks

Make sure essential tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade and cancel or postpone them.

Backups

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

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

Table 6: Backups

Backup	Guide
Threat defense	Cisco Secure Firewall Device Manager Configuration Guide: System Management
Firepower 4100/9300 chassis	Cisco Firepower 4100/9300 FXOS Configuration Guide: Configuration Import/Export
ASA on a Firepower 9300 chassis	Cisco ASA Series General Operations Configuration Guide: Software and Configurations For a Firepower 9300 chassis with threat defense and ASA logical devices, use ASDM or the ASA CLI to back up ASA configurations and other critical files, especially if there is an ASA configuration migration.

Software Upgrade Readiness Checks

Besides the checks you perform yourself, the system can also check its own upgrade readiness. You can run readiness checks outside your maintenance window, otherwise it runs when you start the upgrade. Passing readiness checks is not optional. If you fail readiness checks, you cannot upgrade. The time required to run a readiness check varies depending on model and database size. Do not manually reboot or shut down during readiness checks.



CHAPTER 2

Upgrade Threat Defense

- [Upgrade Readiness Checks for Threat Defense, on page 7](#)
- [Upgrade Standalone Threat Defense, on page 8](#)
- [Upgrade High Availability Threat Defense, on page 9](#)
- [Monitor Threat Defense Upgrades, on page 11](#)
- [Cancel or Retry Threat Defense Upgrades, on page 11](#)
- [Revert Threat Defense, on page 12](#)

Upgrade Readiness Checks for Threat Defense

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

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

Before you begin

Upload the upgrade package you want to check.

Procedure

- Step 1** Select **Device**, then click **View Configuration** in the Updates summary.
- The **System Upgrade** section shows the currently running software version and any update that you have already uploaded.
- Step 2** Look at the **Readiness Check** section.
- If the upgrade check has not been performed yet, click the **Run Upgrade Readiness Check** link. The progress of the check is shown in this area. It should take about 20 seconds to complete the process.
 - If the upgrade check has already been run, this section indicates whether the check succeeded or failed. For failed checks, click **See Details** to view more information about the readiness check. After fixing problems, run the check again.

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

Following are some typical problems:

- **FXOS version incompatibility**—On systems where you install FXOS upgrades separately, such as the Firepower 4100/9300, an upgrade package might require a different minimum FXOS version than the threat defense software version you are currently running. In this case, you must first upgrade FXOS before you can upgrade the threat defense software.
- **Unsupported device model**—The upgrade package cannot be installed on this device. You might have uploaded the wrong package, or the device is an older model that is simply no longer supported in the new threat defense software version. Please check device compatibility and upload a supported package, if one is available.
- **Insufficient disk space**—If not enough space is available, try deleting unneeded files, such as system backups. Delete only those files you have created.

Upgrade Standalone Threat Defense

Use this procedure to upgrade a standalone threat defense device. If you need to update FXOS, do that first. To upgrade high availability threat defense, see [Upgrade High Availability Threat Defense, on page 9](#).



Caution

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

For details on these and other issues you may encounter during upgrade, see [Troubleshooting and Reference, on page 27](#).

Before you begin

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

Procedure

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

Step 2 Upload the upgrade package.

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

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

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

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks. If you do not run the readiness check manually, it runs when you initiate the upgrade. If the readiness check fails, the upgrade is canceled. For more information, see [Upgrade Readiness Checks for Threat Defense, on page 7](#).

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

a) Choose rollback options.

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

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

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

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

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

The Device Summary page shows the currently running software version.

Step 6 Complete post-upgrade tasks.

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

Upgrade High Availability Threat Defense

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



Caution

Do not make or deploy configuration changes on one unit while the other is upgrading, or to a mixed version pair. Even if the system appears inactive, do not manually reboot or shut down during upgrade; you could place the system in an unusable state and require a reimage. You can manually cancel failed or in-progress major and maintenance upgrades, and retry failed upgrades. If you continue to have issues, contact Cisco TAC.

For details on these and other issues you may encounter during upgrade, see [Troubleshooting and Reference, on page 27](#).

Before you begin

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

Procedure

-
- Step 1** Log into the standby unit.
- Step 2** Select **Device**, then click **View Configuration** in the Updates panel.
The System Upgrade panel shows the currently running software version and any upgrade package that you have already uploaded.
- Step 3** Upload the upgrade package.

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

When the upload completes, the system displays a confirmation dialog box. Before you click **OK**, optionally select **Run Upgrade Immediately** to choose rollback options and upgrade now. If you upgrade now, it is especially important to have completed as much of the pre-upgrade checklist as possible (see the next step).
- Step 4** Perform final pre-upgrade checks, including the readiness check.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks. If you do not run the readiness check manually, it runs when you initiate the upgrade. If the readiness check fails, the upgrade is canceled. For more information, see [Upgrade Readiness Checks for Threat Defense, on page 7](#).
- Step 5** Click **Upgrade Now** to start the upgrade.
- Choose rollback options.

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

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

Traffic is dropped while you upgrade. For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.
- Step 6** Log back in when you can and verify upgrade success.

The Device Summary page shows the currently running software version and high availability status. Do not proceed until you have verified success *and* high availability has resumed. If high availability remains suspended after successful upgrade, see [Troubleshooting High Availability Threat Defense Upgrade, on page 27](#).
- Step 7** Upgrade the second unit.
- Switch roles, making this device active: Select **Device > High Availability**, then select **Switch Mode** from the gear menu (⚙️). Wait for the unit's status to change to active and confirm that traffic is flowing normally. Log out.
 - Upgrade: Repeat the previous steps to log into the new standby, upload the package, upgrade the device, monitor progress, and verify success.

Step 8 Examine device roles.

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

Step 9 Log into the active unit.

Step 10 Complete post-upgrade tasks.

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

Monitor Threat Defense Upgrades

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

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

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

Cancel or Retry Threat Defense Upgrades

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

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



Note By default, threat defense automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to manually cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. In a high availability deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

Cancel and retry are not supported for patches. For information on reverting a successful upgrade, see [Revert Threat Defense, on page 12](#).

Revert Threat Defense

If a major or maintenance upgrade succeeds but the system does not function to your expectations, you can revert. Reverting threat defense returns the software to its state just before the last major or maintenance upgrade; post-upgrade configuration changes are not retained. Reverting after patching necessarily removes patches as well. Note that you cannot revert individual patches or hotfixes.

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

Before you begin

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

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

Procedure

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

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

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

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

After you revert, you must re-register the device with the Smart Software Manager.



CHAPTER 3

Upgrade the Firepower 4100/9300 Chassis

- [Upgrade FXOS with Chassis Manager, on page 13](#)
- [Upgrade FXOS on the Firepower 4100/9300 with the CLI, on page 18](#)

Upgrade FXOS with 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 4100/9300 chassis.

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

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair.
- A Firepower 9300 chassis that is configured with one or more standalone FTD logical devices that are not part of a failover pair.

Before you begin

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

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

Procedure

-
- | | |
|---------------|---|
| Step 1 | In Firepower Chassis Manager, choose System > Updates .
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis. |
| Step 2 | Upload the new platform bundle image: |

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

Step 3 After the new platform bundle image has been successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

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

Step 4 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

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

Step 5 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

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

Note

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

Example:

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

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

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

Step 6 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

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

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

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

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

Before you begin

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

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

Procedure

-
- Step 1** Connect to Firepower Chassis Manager on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:
- Step 2** In Firepower Chassis Manager, choose **System > Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.
- Step 3** Upload the new platform bundle image:
- a) Click **Upload Image** to open the Upload Image dialog box.
 - b) Click **Choose File** to navigate to and select the image that you want to upload.
 - c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
 - d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.
- Step 4** After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.
- Step 5** Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components.
- Step 6** Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:
- a) Enter **scope system**.
 - b) Enter **show firmware monitor**.

- c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note

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

Example:

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

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

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

- Step 7** After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:
- Enter **top**.
 - Enter **scope ssa**.
 - Enter **show slot**.
 - Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
 - Enter **show app-instance**.
 - Verify that the Oper State is `Online` for any logical devices installed on the chassis.
- Step 8** Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:
- Connect to Firepower Management Center.
 - Choose **Devices > Device Management**.
 - Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon (.
 - Click **Yes** to immediately make the standby device the active device in the high availability pair.
- Step 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:
- Click **Upload Image** to open the Upload Image dialog box.
 - Click **Choose File** to navigate to and select the image that you want to upload.
 - Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
 - For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

Step 12 After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

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

Step 13 Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The system unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

Step 14 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

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

Note

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

Example:

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

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

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

Step 15 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

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

Step 16 Make the unit that you just upgraded the *active* unit as it was before the upgrade:

- a) Connect to Firepower Management Center.
- b) Choose **Devices > Device Management**.

- c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon (.
- d) Click **Yes** to immediately make the standby device the active device in the high availability pair.

Upgrade FXOS on the Firepower 4100/9300 with the CLI

Upgrade FXOS for Standalone FTD Logical Devices Using the FXOS CLI

This section describes how to upgrade the FXOS platform bundle for a standalone Firepower 4100/9300 chassis.

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

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair.
- A Firepower 9300 chassis that is configured with one or more standalone FTD devices that are not part of a failover pair.

Before you begin

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

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.
- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
 - IP address and authentication credentials for the server from which you are copying the image.
 - Fully qualified name of the image file.

Procedure

Step 1 Connect to the FXOS CLI.

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

- a) Enter firmware mode:

```
Firepower-chassis-a # scope firmware
```

- b) Download the FXOS platform bundle software image:

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

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

- `ftp://username@hostname/path/image_name`

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

c) To monitor the download process:

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

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

Example:

The following example copies an image using the SCP protocol:

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

Step 3 If necessary, return to firmware mode:

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

Step 4 Enter auto-install mode:

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

Step 5 Install the FXOS platform bundle:

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

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

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

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

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

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

Step 8 To monitor the upgrade process:

a) Enter **scope system**.

b) Enter **show firmware monitor**.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show Upgrade-Status: Ready.

Note

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

Example:

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

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

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

FP9300-A /system #
```

Step 9

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

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

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

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

Before you begin

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

- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS and FTD configurations.
- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
 - IP address and authentication credentials for the server from which you are copying the image.

- Fully qualified name of the image file.

Procedure

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

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

a) Enter firmware mode:

```
Firepower-chassis-a # scope firmware
```

b) Download the FXOS platform bundle software image:

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

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

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

c) To monitor the download process:

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

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

Example:

The following example copies an image using the SCP protocol:

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

Step 3 If necessary, return to firmware mode:

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

Step 4 Enter auto-install mode:

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

Step 5 Install the FXOS platform bundle:

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

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

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

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

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

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

Step 8 To monitor the upgrade process:

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

Note

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

Example:

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

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

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

FP9300-A /system #
```

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

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

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

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

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

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

- a) Enter firmware mode:

```
Firepower-chassis-a # scope firmware
```

- b) Download the FXOS platform bundle software image:

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

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

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

- c) To monitor the download process:

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

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

Example:

The following example copies an image using the SCP protocol:

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

Step 13 If necessary, return to firmware mode:

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

Step 14 Enter auto-install mode:

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

Step 15 Install the FXOS platform bundle:

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

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

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

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

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

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

Step 18 To monitor the upgrade process:

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

Note

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

Example:

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

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

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

FP9300-A /system #
```

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

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

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

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



CHAPTER 4

Troubleshooting and Reference

- [Troubleshooting High Availability Threat Defense Upgrade, on page 27](#)
- [Unresponsive and Failed Threat Defense Upgrades, on page 28](#)
- [Traffic Flow and Inspection, on page 29](#)
- [Time and Disk Space, on page 31](#)
- [Upgrade Feature History, on page 32](#)

Troubleshooting High Availability Threat Defense Upgrade

Table 7: Troubleshooting High Availability Threat Defense Upgrade

Issue	Solution
Upgrade will not begin without deploying uncommitted changes.	If you get an error message stating that you must deploy all uncommitted changes even though there are none, log into the active unit (remember, you should be upgrading the standby), create some minor change, and deploy. Then, undo the change, redeploy, and try the upgrade again on the standby. If this does not work, and the units are running different software versions against recommendations, switch roles to make the standby unit active, then suspend high availability. Deploy from the active/suspended unit, resume high availability, then switch roles to make the active unit the standby again. Upgrade should then work.
Deployment from active unit fails during standby upgrade, or causes an application synchronization error.	This can happen if you deploy from the active unit while the standby is upgrading, which is not supported. Proceed with the upgrade despite the error. After you upgrade both units, make any required configuration changes and deploy from the active unit. The error should resolve. To avoid these issues, do not make or deploy configuration changes on one unit while the other is upgrading, or to a mixed version pair.
Configuration changes made during upgrade are lost.	If you absolutely must make and deploy changes to a mixed version pair, you must make the changes to both units or they will be lost after you upgrade the down-level active unit.

Issue	Solution
High availability is suspended after upgrade.	After the post-upgrade reboot, high availability is briefly suspended while the system performs some final automated tasks, such as updating libraries and restarting Snort. You are most likely to notice this if you log into the CLI <i>very</i> shortly after upgrade. If high availability does not resume on its own after the upgrade fully completes and device manager is available, do it manually: 1. Log into both the active device and the standby device and check the task lists. Wait until all tasks are finished running on both devices. If you resume high availability too soon, you may have a future issue where failover causes an outage. 2. Select Device > High Availability, then select Resume HA from the gear menu (⚙️).
Failover does not occur with a mixed version pair.	Although an advantage of high availability is that you can upgrade your deployment without traffic or inspection interruptions, failover is disabled during the entire upgrade process. That is, not only is failover necessarily disabled when one device is offline (because there is nothing to fail over to—you are essentially already failed over), but failover is also disabled with mixed version pairs. During upgrade is the only time where mixed version pairs are (temporarily) allowed. Schedule upgrades during maintenance windows when they will have the least impact if something goes wrong, and make sure you have enough time to upgrade both devices in that window.
Upgrade failed on only one device, or one device was reverted. The pair is now running mixed versions.	Mixed version pairs are not supported for general operations. Either upgrade the down-version device or revert the higher version device. For patches, because revert is not supported, if you cannot successfully upgrade the down-version device you must break high availability, reimage one or both devices, then re-establish high availability.

Unresponsive and Failed Threat Defense Upgrades



Caution

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

Table 8: Unresponsive and Failed Threat Defense Upgrades

Issue	Solution
Cannot reach the device.	Devices can stop passing traffic during the upgrade or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface.
Upgrade or patch appears hung/device appears inactive.	If device upgrade status has stopped updating but there is no report of upgrade failure, you can try canceling the upgrade; see Cancel or Retry Threat Defense Upgrades, on page 11. If you cannot cancel or canceling does not work, contact Cisco TAC.

Issue	Solution
Upgrade failed.	If an upgrade fails and: • The device reverted to its pre-upgrade state (auto-cancel is enabled), correct any issues and try again from the beginning. • The device is still in maintenance mode, correct any issues and resume the upgrade. Or, cancel and try again later. For more information, see Cancel or Retry Threat Defense Upgrades, on page 11. If you cannot retry or cancel, or if you continue to have issues, contact Cisco TAC.
Patch failed.	You cannot cancel in-progress or failed patches. However, if a patch fails early, for example, during validation stages, the device may remain up and running normally. Simply correct any issues and try again. If a patch fails after the device has entered maintenance mode, contact Cisco TAC.
I want to cancel an upgrade.	Canceling reverts the device to its pre-upgrade state. You can cancel failed and in-progress upgrades on the upgrade status page that automatically appears during upgrade. You can also use the upgrade cancel CLI command. You cannot cancel patches. If you cannot cancel or canceling does not work, contact Cisco TAC.
I want to retry (resume) a failed upgrade.	You can resume an upgrade on the upgrade status page that automatically appears during upgrade. You can also use the upgrade retry CLI command. If you continue to have issues, contact Cisco TAC.
I want to change what happens when upgrade fails.	Part of the upgrade process is choosing what happens if it fails. This is done with the Automatically cancel on upgrade failure... (auto-cancel) option: • Auto-cancel enabled (default): If upgrade fails, the upgrade cancels and the device automatically reverts to its pre-upgrade state. This returns you to normal operations as quickly as possible while you regroup and try again. • Auto-cancel disabled: If upgrade fails, the device remains as it is. This allows you to correct any issues and resume the upgrade. For high availability devices, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

Traffic Flow and Inspection

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

Traffic Flow and Inspection for Threat Defense Upgrades

Software Upgrade

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

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

Software Revert (Major/Maintenance Releases)

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

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; see [Upgrade Order, on page 3](#).

Table 9: Traffic Flow and Inspection: FXOS Upgrades

Threat Defense Deployment	Traffic Behavior	Method
Standalone	Dropped.	—
High availability	Unaffected.	Best Practice: Update FXOS on the standby, switch active peers, upgrade the new standby.
	Dropped until one peer is online.	Upgrade FXOS on the active peer before the standby is finished upgrading.

Traffic Flow and Inspection when Deploying Configurations

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

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

Time and Disk Space

Time to Upgrade

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



Caution

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see [Unresponsive and Failed Threat Defense Upgrades, on page 28](#).

Table 10: Upgrade Time Considerations

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

Disk Space to Upgrade

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

Upgrade Feature History

Table 11: Version 7.0.0 Features

Feature	Details
Upgrade readiness check for device manager-managed devices.	You can run an upgrade readiness check on an uploaded threat defense upgrade package before attempting to install it. The readiness check verifies that the upgrade is valid for the system, and that the system meets other requirements needed to install the package. Running an upgrade readiness check helps you avoid failed installations. A link to run the upgrade readiness check was added to the System Upgrade section of the Device > Updates page.

Table 12: Version 6.7.0 Features

Feature	Details
Ability to cancel a failed threat defense software upgrade and to revert to the previous release.	If an threat defense major software upgrade fails or is otherwise not functioning correctly, you can revert to the state of the device as it was when you installed the upgrade. We added the ability to revert the upgrade to the System Upgrade panel in FDM. During an upgrade, the FDM login screen shows the upgrade status and gives you the option to cancel or revert in case of upgrade failure. In the threat defense API, we added the CancelUpgrade, RevertUpgrade, RetryUpgrade, and UpgradeRevertInfo resources. In the threat defense CLI, we added the following commands: show last-upgrade status, show upgrade status, show upgrade revert-info, upgrade cancel, upgrade revert, upgrade cleanup-revert, upgrade retry.

Table 13: Version 6.2.0 Features

Feature	Details
Upgrade threat defense software through device manager.	You can install software upgrades through device manager. Select Device > Updates .