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?

The procedures in this guide are for upgrading threat defense if you are currently running Version 7.4.x–7.6.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, see Troubleshooting and Reference.

Software Upgrade Guidelines

For release-specific upgrade warnings and guidelines, as well as features and bugs with upgrade impact, see the threat defense release notes. 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 FXOS build in each major version. For release-specific FXOS upgrade warnings and guidelines, as well as features and bugs with upgrade impact, see the FXOS release notes. 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 deployments, multi-hop upgrades, and situations where you need to coordinate chassis, hosting environment or other upgrades.

Upgrading Threat Defense with Chassis Upgrade

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.

Supported Direct Upgrades

This table shows the supported direct upgrades for threat defense software. Note that although you can upgrade directly to major and maintenance 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										
	7.6	7.4	7.3	7.2	7.1	7.0	6.7	6.6	6.5	6.4	6.3
	Firepower 4100/9300 FXOS Version										
	2.16	2.14	2.13	2.12	2.11	2.10	2.9	2.8	2.7	2.6	2.4
7.6	YES	—	—	—	—	—	—	—	—	—	—
7.4	YES	YES †	—	—	—	—	—	—	—	—	—

Current Version	Target Software Version										
	7.6	7.4	7.3	7.2	7.1	7.0	6.7	6.6	6.5	6.4	6.3
	Firepower 4100/9300 FXOS Version										
	2.16	2.14	2.13	2.12	2.11	2.10	2.9	2.8	2.7	2.6	2.4
7.3	YES	YES	YES	—	—	—	—	—	—	—	—
7.2	YES	YES	YES	YES	—	—	—	—	—	—	—
7.1	YES	YES	YES	YES	YES	—	—	—	—	—	—
7.0	—	YES	YES	YES	YES	YES	—	—	—	—	—
6.7	—	—	— *	YES	YES	YES	YES	—	—	—	—
6.6	—	—	—	YES	YES	YES	YES	YES	—	—	—
6.5	—	—	—	—	YES	YES	YES	YES	—	—	—
6.4	—	—	—	—	—	YES	YES	YES	YES	—	—
6.3	—	—	—	—	—	—	YES	YES	YES	YES	—
6.2.3	—	—	—	—	—	—	—	YES	YES	YES	YES

* You cannot upgrade from Version 6.7.x to 7.3.x.

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

Upgrade Order for Threat Defense with Chassis Upgrade and High Availability

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

Table 2: Chassis Upgrade Order for the Firepower 4100/9300 with Device Manager

Threat Defense Deployment	Upgrade Order
Standalone	1. Upgrade chassis. 2. Upgrade threat defense.

Threat Defense Deployment	Upgrade Order
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 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, software version, and build. Upgrade packages are signed, and terminate in .sh.REL.tar. Do not untar or rename them.

Table 3: 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.
Secure Firewall 3100	Cisco_FTD_SSP-FP3K_Upgrade-*Version-build*.sh.REL.tar	—
Firepower 4100/9300	Cisco_FTD_SSP_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 4: 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, which typically restarts Snort); see Traffic Flow and Inspection when Deploying Configurations.

Deployment Health

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

Running and Scheduled Tasks

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

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 5: 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.