

Planning Your Upgrade

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

Note Version 10 begins a new release numbering scheme and cadence. For more information, see the *Cisco's Next Generation Firewall Product Line Software Release and Sustaining Bulletin*.

- Is This Guide for You?, on page 1
- Compatibility, on page 1
- Upgrade Guidelines, on page 2
- Upgrade Path, on page 2
- Upgrade Order, on page 4
- Manually Downloading Upgrade Packages, on page 5
- Upgrade Readiness, on page 6

Is This Guide for You?

The procedures in this guide are for upgrading Firewall Threat Defense if you are currently running Version 7.4.1–10.

Compatibility

Before you upgrade, make sure the target version is compatible with your deployment. If you cannot upgrade due to incompatibility, contact your Cisco representative or partner contact for refresh information. For compatibility, see *Cisco Secure Firewall Threat Defense Compatibility Guide*.

Upgrade Guidelines

In addition to the guidelines and resource links in the following topics, see Reference for general information on time and disk space requirements, and for details on system behavior during upgrade, which can include interruptions to traffic flow and inspection.

Software Upgrade Guidelines

For release-specific upgrade warnings and guidelines for Firewall Threat Defense, and for information on 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 Guidelines for Firewall Threat Defense Virtual

Upgrade does not change the serial number or UUID of Firewall Threat Defense Virtual instances.

Update base image and template image ID before cluster upgrade

Before you upgrade a cluster in the public cloud, copy the target version image to your cloud image repository and update the image ID in the cluster deployment template (we actually recommend replacing the existing template with a modified copy). This ensures that after the upgrade, new instances — for example, instances launched during cluster scaling — will use the correct version. If the marketplace does not have the image you need, such as when the cluster has been patched, create a custom image from a snapshot of a standalone Firewall Threat Defense Virtual instance running the correct version, with no instance-specific (day 0) configurations.

Suspend health checks before autoscaled cluster upgrade

For Firewall Threat Defense Virtual for AWS, suspend the HealthCheck and ReplaceUnhealthy processes before autoscaled cluster upgrade. This ensures that instances are not terminated by the Auto Scaling group during the post-upgrade reboot. You can resume the suspended processes afterwards. For instructions, see the Amazon EC2 Auto Scaling user guide: Suspend and resume Amazon EC2 Auto Scaling processes.

Upgrade Path

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

Choosing your upgrade target

Go **directly to the latest release possible** to minimize upgrade and other impact. This is because features, enhancements, and critical fixes can skip "future" releases that are ahead by version, but not by release date. For example, if you are up-to-date within major Version A, upgrading to dot-zero Version B can deprecate features and fixes.

If you cannot go to the latest release, at least make sure your current version was released on a date before your target version; see the Release Notes for Secure Firewall Threat Defense for your target version.

Upgrading a patched deployment

Critical fixes in patches/vulnerability (fourth-digit) releases can also skip future releases. If you depend on these critical fixes, verify that your target version contains them. For a full list of release dates, see *Cisco Secure Firewall Device Manager New Features by Release*.

Supported upgrades and downgrades

This section summarizes upgrade and downgrade capability.

Supported upgrades

This table shows the supported direct upgrades for Firewall Threat Defense software.



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

Table 1: Supported direct upgrades

Current version	Target software version							
	to 10.x	7.7	7.6	7.4	7.3	7.2	7.1	7.0
from 10.x	YES	—	—	—	—	—	—	—
from 7.7	YES	YES	—	—	—	—	—	—
from 7.6	YES	YES	YES	—	—	—	—	—
from 7.4	YES	YES	YES	YES	—	—	—	—
from 7.3	YES	YES	YES	YES	YES	—	—	—
from 7.2	—	YES	YES	YES	YES	YES	—	—
from 7.1	—	—	YES	YES	YES	YES	YES	—
from 7.0	—	—	—	YES	YES	YES	YES	YES
from 6.4	—	—	—	—	—	—	—	YES

Supported FXOS versions for Firepower 4100/9300 upgrades

For the Firepower 4100/9300, this table lists companion FXOS versions. If a chassis upgrade is required, Firewall 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 2: Supported FXOS versions for Firepower 4100/9300 upgrades

Target Firewall Threat Defense version	Minimum FXOS version
10.x	2.18.0
7.7	2.17.0
7.6	2.16.0
7.4.1–7.4.x	2.14.1
7.4.0	—
7.3	2.13.0
7.2	2.12.0
7.1	2.11.1
7.0	2.10.1
6.7	2.9.1
6.6	2.8.1
6.4	2.6.1

Supported downgrades

If an upgrade succeeds but the system does not function to your expectations, you may be able to return to a previous version; see Revert Firewall Threat Defense.

Upgrade Order

Chassis Before Firewall 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 Firewall 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 Firewall 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

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

Manually Downloading 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: Firewall 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 200		
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	—
ISA 3000 with FTD	Cisco_FTD_Upgrade-*Version-build*.sh.REL.tar	—
Threat defense virtual	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

After you check compatibility, plan your upgrade path and order, and review upgrade guidelines, you need to assess upgrade readiness. The system does some of these checks for you, but you still need to perform additional checks (and actions) yourself, like deploying configuration changes and making backups.

Use the following sections to perform last minute-tasks and confirm 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 any required pre-upgrade configuration changes, and prepare to make required post-upgrade configuration changes. Deploy configuration changes. 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.

Deployment Health

Make sure devices are healthy and successfully communicating. Because being out of sync with your NTP server can cause upgrade failure, we also recommend you check time with the **show time** CLI command.

Running Tasks and Scheduled Tasks

Make sure essential tasks are complete. Tasks running when the upgrade begins are stopped and cannot be resumed; they become failed tasks. 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
Firewall 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 Firewall 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.