



# 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 FXOS](#).



---

**Important** You must still read the release notes, which can contain additional critical and version-specific information. For example, new and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. Or, known issues (open bugs) can affect upgrade.

---

- [Minimum Version to Upgrade, on page 1](#)
- [Upgrade Guidelines for Version 7.1, on page 2](#)
- [Unresponsive Upgrades, on page 3](#)
- [Traffic Flow and Inspection for FTD Upgrades, on page 3](#)
- [Time and Disk Space Tests, on page 4](#)

## Minimum Version to Upgrade

### Minimum Version to Upgrade

You can upgrade directly to Version 7.1, including maintenance releases, as follows.

*Table 1: Minimum Version to Upgrade to Version 7.1*

Platform	Minimum Version
FTD	6.5  FXOS 2.11.1.154 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 <a href="#">Cisco Firepower 4100/9300 FXOS Release Notes, 2.11(1)</a> .

**Minimum Version to Patch**

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

# Upgrade Guidelines for Version 7.1

These checklists provide new and/or previously published upgrade guidelines that may apply to you.

**Table 2: Upgrade Guidelines for FTD with FDM Version 7.1**

✓	Guideline	Platforms	Upgrading From	Directly To
	<a href="#">Cisco Secure Firewall Device Manager New Features by Release</a> , for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	<a href="#">Cisco Firepower Release Notes</a> , in the <i>Open and Resolved Bugs</i> chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	<a href="#">Minimum Version to Upgrade, on page 1</a>	Any	Any	Any
	<a href="#">Upgrade Guidelines for FXOS</a>	Firepower 4100/9300	Any	Any
	<a href="#">Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 2</a>	Any	7.0.4+	7.1.0 only
	<a href="#">Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 3</a>	Firepower 1010	6.4.0 through 6.6.x	6.7+

## Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0

**Deployments:** Any

**Upgrading from:** Version 7.0.4 or later maintenance release

**Directly to:** Version 7.1.0 only

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+.

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

**Deployments:** Firepower 1010

**Upgrading from:** Version 6.4 through 6.6

**Directly to:** Version 6.7+

For the Firepower 1010, FTD upgrades to Version 6.7+ will fail if you configured switch ports with a VLAN ID in the 3968–4047 range. These IDs are for internal use only.

## Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down during upgrade. You could place the system in an unusable state and require a reimage.

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



---

**Note** By default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to manually cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Auto-cancel is not supported for patches. In a high availability deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

This feature is not supported for patches or for upgrades from Version 6.6 and earlier.

---

## Traffic Flow and Inspection for FTD Upgrades

### Software Upgrades

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

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

### Software Revert (Major/Maintenance Releases)

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

### Deploying Configuration Changes

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

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

## Time and Disk Space Tests

For reference purposes, we provide reports of in-house time and disk space tests for software upgrades.

### Time Tests

We report the *slowest* tested time of all software upgrades tested on a particular platform/series. Your upgrade will likely take longer than the provided times for multiple reasons, as explained in the following table. We recommend you track and record your own upgrade times so you can use them as future benchmarks.



**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 Upgrades, on page 3](#).

**Table 3: Time Test Conditions for Software Upgrades**

Condition	Details
Deployment	Times for device upgrades are from tests in a FMC deployments. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
Versions	For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version. Upgrade time usually increases if your upgrade skips versions.
Models	In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.
Virtual appliances	We test with the default settings for memory and resources. However, note that upgrade time in virtual deployments is highly hardware dependent.
High availability/scalability	Unless otherwise noted, we test on standalone devices. 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	We test on appliances with minimal configurations and traffic load. Upgrade time can increase with the complexity of your configurations and whether/how those things 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.

Condition	Details
Components	We report times for the software upgrade itself and the subsequent reboot <i>only</i> . This does not include time for operating system upgrades, transferring upgrade packages, readiness checks, VDB and intrusion rule (SRU/LSP) updates, or deploying configurations.

### Disk Space Tests

We report the *most* disk space used of all software upgrades tested on a particular platform/series. This includes the space needed to copy the upgrade package to the device.

We also report the space needed on the FMC (in either /Volume or /var) for the device upgrade package. If you are using FDM, ignore those values.

When we report disk space estimates for a particular location (for example, /var or /ngfw), we are reporting the disk space estimate for the partition mounted in that location. On some platforms, these locations may be on the same partition.

Without enough free disk space, the upgrade fails.

To check disk space, use the **show disk** CLI command.

## Time and Disk Space for Version 7.1.0.3

Table 4: Time and Disk Space for Version 7.1.0.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 1000 series	—	3.2 GB in /ngfw	1.0 GB	9 min	13 min
Firepower 2100 series	—	3.2 GB in /ngfw	1.1 GB	7 min	14 min
Secure Firewall 3100 series	—	3.5 GB in /ngfw	1.1 GB	4 min	15 min
Firepower 4100 series	—	2.8 GB in /ngfw	780 MB	5 min	7 min
Firepower 9300	—	2.3 GB in /ngfw	780 MB	5 min	10 min
ISA 3000	1.7 GB in /ngfw/var	270 MB in /ngfw/bin	780 MB	11 min	14 min
FTDv: VMware	2.1 GB in /ngfw/var	270 MB in /ngfw/bin	350 MB	5 min	6 min

## Time and Disk Space for Version 7.1.0.2

Table 5: Time and Disk Space for Version 7.1.0.2

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Secure Firewall 3100 series	—	3.2 GB in /ngfw		4 min	46 min

## Time and Disk Space for Version 7.1.0.1

Table 6: Time and Disk Space for Version 7.1.0.1

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 1000 series	—	5.6 GB in /ngfw	430 MB	10 min	11 min
Firepower 2100 series	—	5.6 GB in /ngfw	420 MB	10 min	10 min
Firepower 4100 series	—	5.6 GB in /ngfw	430 MB	7 min	7 min
Firepower 9300	—	5.1 GB in /ngfw	430 MB	7 min	8 min
ISA 3000	2.0 GB in /ngfw/var	240 MB in /ngfw/bin	430 MB	4 min	13 min
FTDv: VMware	1.5 GB in /ngfw/var	240 MN in /ngfw/bin	430 MB	4 min	4 min

## Time and Disk Space for Version 7.1.0

Table 7: Time and Disk Space for Version 7.1.0

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time	
Firepower 1000 series	—	8.2 GB in /ngfw	930 MB	16 min	11 min	
Firepower 2100 series	—	8.3 GB in /ngfw	1 GB	13 min	13 min	
Firepower 4100 series	—	8.6 GB in /ngfw	870 MB	15 min	9 min	
Firepower 9300	—	11.2 GB in /ngfw	870 MB	11 min	12 min	
ISA 3000	from Version 6.5–6.6	9.3 GB in /home	256 KB in /ngfw	1 GB	8 min	
	from Version 6.7	9.3 GB in /ngfw/Volume				
	from Version 7.0	9.2 GB in /ngfw/var				260 KB in /ngfw/bin
FTDv: VMware	from Version 6.5–6.6	4.6 GB in /home	925 KB in /ngfw	1 GB	11 min	
	from Version 6.7	4.4 GB in /ngfw/Volume				210 KB in /ngfw
	from Version 7.0	5.3 GB in /ngfw/var				220 KB in /ngfw/bin