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

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
FMC	6.5
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 Cisco Firepower 4100/9300 FXOS Release Notes, 2.11(1).

Minimum Version to Patch

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

Guidelines for Cloud-delivered Firewall Management Center

You do not upgrade the cloud-delivered Firewall Management Center. It does not have a version and we take care of feature updates.

Upgrading FTD with Cloud-delivered Firewall Management Center

To upgrade FTD with the cloud-delivered Firewall Management Center, use the *latest released version* of the Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center.

Note The cloud-delivered Firewall Management Center cannot manage FTD Version 7.1. You cannot upgrade a cloud-managed device from Version 7.0 to Version 7.1 unless you unregister and disable cloud management. We recommend you upgrade the device directly to Version 7.2+.

Upgrading Co-Managed Devices

Customer-deployed FMCs running Version 7.2+ can co-manage cloud-managed FTD devices, but for event logging and analytics purposes only. You must use the cloud-delivered Firewall Management Center to manage and configure all other aspects of FTD, including upgrade.

Remember, a customer-deployed FMC must run the *same or newer* version as its managed devices—and this includes devices co-managed by the cloud-delivered Firewall Management Center. That is, you cannot use the cloud-delivered Firewall Management Center to upgrade a co-managed device past its customer-deployed FMC.

For example, consider a threat defense device with two managers:

- Device, running Version A.
- Customer-deployed FMC, running Version B.
- Cloud-delivered Firewall Management Center, no version.

In this scenario, you can use the cloud-delivered Firewall Management Center to upgrade the device to Version B (the same version as the co-manager), but not to Version C (past the co-manager).

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 FMC Version 7.1

✓	Guideline	Platforms	Upgrading From	Directly To
	Cisco Secure Firewall Management Center New Features by Release, for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	CiscoFirepower Release Notes, in the *Open and Resolved Bugs* chapter, for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	Minimum Version to Upgrade, on page 1	Any	Any	Any
	Upgrade Guidelines for FXOS	Firepower 4100/9300	Any	Any
	Upgrade Prohibited: Version 7.0.4+ to Version 7.1.0, on page 3	Any	7.0.4+	7.1.0 only
	Reconnect with Cisco Secure Malware Analytics for High Availability FMCs, on page 4	FMC	6.4.0 through 6.7.x	7.0+
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 4	Firepower 1010	6.4.0 through 6.6.x	6.7+
	FMCv Requires 28 GB RAM for Upgrade, on page 4	FMCv	6.2.3 through 6.5.0.x	6.6+

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+.

Reconnect with Cisco Secure Malware Analytics for High Availability FMCs

Deployments: High availability/AMP for Networks (malware detection) deployments where you submit files for dynamic analysis

Upgrading from: Version 6.4.0 through 6.7.x

Directly to: Version 7.0.0+

Related bug: CSCvu35704

Version 7.0.0 fixes an issue with high availability where, after failover, the system stopped submitting files for dynamic analysis. For the fix to take effect, you must reassociate with the Cisco Secure Malware Analytics public cloud.

After you upgrade the high availability pair, on the primary FMC:

1. Choose **AMP** > **Dynamic Analysis Connections**.
2. Click **Associate** in the table row corresponding to the public cloud.

   A portal window opens. You do not have to sign in. The reassociation happens in the background, within a few minutes.

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.

FMCv Requires 28 GB RAM for Upgrade

Deployments: FMCv

Upgrading from: Version 6.2.3 through 6.5

Directly to: Version 6.6+

All FMCv implementations now have the same RAM requirements: 32 GB recommended, 28 GB required (64 GB for FMCv 300). Upgrades to Version 6.6+ will fail if you allocate less than 28 GB to the virtual appliance. After upgrade, the health monitor will alert if you lower the memory allocation.

These new memory requirements enforce uniform requirements across all virtual environments, improve performance, and allow you to take advantage of new features and functionality. We recommend you do not decrease the default settings. To improve performance, you can increase a virtual appliance's memory and number of CPUs, depending on your available resources. For details, see the Cisco Secure Firewall Management Center Virtual Getting Started Guide.

Note As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments (AWS, Azure) are fully deprecated. You cannot create new instances using them, even for earlier versions. You can continue running existing instances.

This table summarizes pre-upgrade requirements for lower-memory deployments.

Table 3: FMCv Memory Requirements for Version 6.6+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 28 GB minimum/32 GB recommended.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 28 GB minimum/32 GB recommended.	For instructions, see the documentation for your KVM environment.
AWS	Resize instances: • **From** c3.xlarge **to** c3.4xlarge. • **From** c3.2.xlarge **to** c3.4xlarge. • **From** c4.xlarge **to** c4.4xlarge. • **From** c4.2xlarge **to** c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.
Azure	Resize instances: • **From** Standard_D3_v2 **to** Standard_D4_v2.	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

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.

Unresponsive FMC Upgrade

Do not restart an upgrade in progress. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Unresponsive FTD Upgrade

For major and maintenance upgrades, you can manually cancel failed or in-progress upgrades, and retry failed upgrades. On the FMC, use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center. You can also use the FTD CLI.

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 or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

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

Traffic Flow and Inspection for FTD Upgrades

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 4: Traffic Flow and Inspection: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped. For bridge group interfaces on the ISA 3000 only, you can use a FlexConfig policy to configure hardware bypass for power failure. This causes traffic to drop during software upgrades but pass without inspection while the device completes its post-upgrade reboot.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force**	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby**	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: **Bypass: Disabled**	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices. For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.

For clusters, the data security module or modules upgrade first, then the control module. During the control security module upgrade, although traffic inspection and handling continues normally, the system stops logging events. Events for traffic processed during the logging downtime appear with out-of-sync timestamps after the upgrade is completed. However, if the logging downtime is significant, the system may prune the oldest events before they can be logged.

Software Revert (Major/Maintenance Releases)

You should expect interruptions to traffic flow and inspection during revert, even in a high availability/scalability deployment. This is because revert is more successful when all units are reverted simultaneously. Simultaneous revert means that interruptions to traffic flow and inspection depend on interface configurations only, as if every device were standalone.

Software Uninstall (Patches)

For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption. 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.

Table 5: Traffic Flow and Inspection: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, **Failsafe** enabled or disabled.	Passed without inspection. A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
	Inline set, **Snort Fail Open: Down**: disabled.	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled.	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Time and Disk Space Tests

For reference purposes, we provide reports of in-house time and disk space tests for FMC and device 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 5.

Table 6: 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 or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	We test on appliances with minimal configurations and traffic load. Upgrade time can increase with the complexity of your configurations, size of event databases, 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.
Components	We report times for the software upgrade itself and the subsequent reboot *only*. 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 have an internal server for FTD upgrade packages, or 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.

Table 7: Checking Disk Space

Platform	Command
FMC	Choose **System** > **Monitoring** > **Statistics** and select the FMC. Under Disk Usage, expand the By Partition details.
FTD with FMC	Choose **System** > **Monitoring** > **Statistics** and select the device you want to check. Under Disk Usage, expand the By Partition details.

Time and Disk Space for Version 7.1.0.3

Table 8: Time and Disk Space for Version 7.1.0.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.9 GB in /var	29 MB in /	—	20 min	7 min
FMCv: VMware	4.0 GB in /var	25 MB in /	—	23 min	6 min
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 4100 series container instance	—	2.9 GB in /ngfw	780 MB	6 min	5 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 9: Time and Disk Space for Version 7.1.0.2

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.0 GB in /var	19 MB in /	—	20 min	4 min
FMCv: VMware	2.5 GB in /var	14 MB in /	—	21 min	1 min
Secure Firewall 3100 series	—	3.2 GB in /ngfw		4 min	46 min

Time and Disk Space for Version 7.1.0.1

Table 10: Time and Disk Space for Version 7.1.0.1

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.0 GB in /var	19 MB in /	—	18 min	8 min
FMCv: VMware	2.2 GB in /var	14 MB in /	—	21 min	4 min
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 4100 series container instance	—	5.6 GB in /ngfw	430 MB	6 min	4 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 11: Time and Disk Space for Version 7.1.0

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	16.9 GB in /var	43 MB in /	—	33 min	15 min
FMCv: VMware	17 GB in /var	50 MB in /	—	34 min	5 min
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 4100 series container instance	—	8.6 GB in /ngfw	870 MB	16 min	8 min
Firepower 9300	—	11.2 GB in /ngfw	870 MB	11 min	12 min

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
ISA 3000	from Version 6.5–6.6	9.3 GB in /home	256 KB in /ngfw	1 GB	21 min	8 min
	from Version 6.7	9.3 GB in /ngfw/Volume	270 KB in /ngfw			
	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	6 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			