Software Upgrade Guidelines

For your convenience, this document duplicates the critical and release-specific software upgrade guidelines published in the threat defense 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 7.3, including maintenance releases, as follows.

Table 1: Minimum Version to Upgrade to Version 7.3

Platform	Minimum Version
Management Center	7.0
Threat Defense (except Threat Defense Virtual with GCP)	7.0 FXOS 2.13.0.198 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, 2.13.

Platform	Minimum Version
Threat Defense Virtual with GCP	7.2 You cannot upgrade to Version 7.2+ from Version 7.1 and earlier; you must deploy a new instance. See Threat Defense Virtual for GCP Cannot Upgrade Across Version 7.2.0, on page 3.

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 7.3

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

Table 2: Upgrade Guidelines for Threat Defense with Management Center Version 7.3

✓	Guideline	Platforms	Upgrading From	Directly To
ALWAYS CHECK				
	Minimum Version to Upgrade, on page 1	Any	Any	Any
	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
	Cisco Secure Firewall Threat Defense 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
	Upgrade Guidelines for Cloud-delivered Firewall Management Center, on page 4	Threat Defense	Any	Any
	Upgrade Guidelines for FXOS	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Extended Post-Upgrade Deploy for Large Configurations, on page 3	Management Center	6.6.0+	7.3.x

✓	Guideline	Platforms	Upgrading From	Directly To
	Threat Defense Virtual for GCP Cannot Upgrade Across Version 7.2.0, on page 3	Threat Defense Virtual for GCP	6.7.0 through 7.1.x	7.2+

Extended Post-Upgrade Deploy for Large Configurations

Deployment: Management Center

Upgrading from: Any deployment where object optimization is enabled.

Directly to: Version 7.3.x

Access control object optimization improves performance and consumes fewer device resources when you have access control rules with overlapping networks. The optimizations occur on the *managed device* on the first deploy after the feature is enabled on the management center (including if it is enabled by an upgrade). If you have a high number of rules, the system can take several minutes to an hour to evaluate your policies and perform object optimization. During this time, you may also see higher CPU use on your devices. A similar thing occurs on the first deploy after the feature is disabled (including if it is disabled by upgrade). After this feature is enabled or disabled, we recommend you deploy when it will have the least impact, such as a maintenance window or a low-traffic time.

To plan, use the following table.

Table 3: Planning Management Center Upgrades with Object Optimization

Version	Default/Reimage Setting	Upgrading	To Enable/Disable
7.0.5 and earlier	Not supported (disabled).	—	—
7.0.6 and later maint. releases	Disabled.	Respects your current setting.	Contact Cisco TAC.
7.1.0–7.2.3	Not supported (disabled).	Disables.	—
7.2.4–7.2.5	Enabled.	Enables.	Contact Cisco TAC.
7.3.x	Not supported (disabled).	Disables.	—
7.4.0	Enabled.	Enables.	Contact Cisco TAC.

Threat Defense Virtual for GCP Cannot Upgrade Across Version 7.2.0

Deployments: Threat Defense Virtual for GCP

Upgrade from: Version 6.7.0 through 7.1.x

Directly to: Version 7.2.0+

Due to interface changes required to support autoscaling, Threat Defense Virtual for GCP upgrades cannot cross Version 7.2.0. That is, you cannot upgrade to Version 7.2.0+ from Version 7.1.x and earlier. You must deploy a new instance and redo any device-specific configurations.

Upgrade 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 Threat Defense with Cloud-delivered Firewall Management Center

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

Note The cloud-delivered Firewall Management Center cannot manage threat defense 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 management centers running Version 7.2+ can co-manage cloud-managed threat defense 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 threat defense, including upgrade.

Remember, a customer-deployed management center 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 management center.

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

- Device, running Version A.
- Customer-deployed management center, 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).

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 Management Center 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 Threat Defense Upgrade

For major and maintenance upgrades, you can manually cancel failed or in-progress upgrades, and retry failed upgrades. On the management center, 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 threat defense CLI.

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. 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 Threat Defense 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.

Note that hitless upgrades are not supported for single-unit clusters. Interruptions to traffic flow and inspection depend on interface configurations of the active unit, just as with standalone devices.

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 management center 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 4.

Table 6: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for device upgrades are from tests in a management center 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 management center (in either /Volume or /var) for the device upgrade package. If you have an internal server for threat defense upgrade packages, or if you are using device manager, 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
Management Center	Choose **System** > **Monitoring** > **Statistics** and select the management center. Under Disk Usage, expand the By Partition details.
Threat Defense with management center	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 7.3.1.1

Time and disk space tests are incomplete at this time. We will update this document when test results become available.

Time and Disk Space for Version 7.3.1

Table 8: Time and Disk Space for Version 7.3.1

Platform	Space in /Volume	Space in /	Space on Mgmt Ctr	Upgrade Time	Reboot Time
Management Center	21.4 GB in /Volume	27 MB in /	—	42 min	8 min
Management Center Virtual: VMware	24.4 GB in /Volume	22 MB in /	—	34 min	6 min
Firepower 1000	—	7.8 GB in /ngfw	930 MB	17 min	18 min
Firepower 2100	—	8.1 GB in /ngfw	1.0 GB	12 min	20 min
Secure Firewall 3100	—	10.8 GB in /ngfw	1.3 GB	9 min	27 min
Firepower 4100	—	8.4 GB in /ngfw	940 MB	12 min	14 min
Firepower 4100 container instance	—	11.0 GB in /ngfw	940 MB	14 min	15 min
Firepower 9300	—	8.1 GB in /ngfw	940 MB	13 min	15 min
ISA 3000	6.3 GB in /ngfw/var	410 MB in /ngfw/bin	1.1 GB	29 min	27 min
Threat Defense Virtual: VMware	7.6 GB in /ngfw/var	380 MB in /ngfw/bin	1.1 GB	18 min	16 min

Time and Disk Space for Version 7.3.0

Table 9: Time and Disk Space for Version 7.3.0

Platform	Space in /Volume	Space in /	Space on Mgmt Ctr	Upgrade Time	Reboot Time
Management Center	19.8 GB in /Volume	49 MB in /	—	30 min	8 min
Management Center Virtual: VMware	19.7 GB in /Volume	47 MB in /	—	31 min	3 min
Firepower 1000	—	7.1 GB in /ngfw	930 MB	17 min	19 min
Firepower 2100	—	7.4 GB in /ngfw	1.0 GB	12 min	17 min
Secure Firewall 3100	—	9.8 GB in /ngfw	1.3 GB	7 min	17 min
Firepower 4100	—	8.0 GB in /ngfw	940 MB	12 min	8 min
Firepower 4100 container instance	—	8.0 GB in /ngfw	940 MB	12 min	8 min
Firepower 9300	—	11.1 GB in /ngfw	940 MB	11 min	12 min
ISA 3000	9.5 GB in /ngfw/var	270 KB in /ngfw/bin	1.1 GB	22 min	8 min
Threat Defense Virtual: VMware	400 MB in /ngfw/var	350 KB in /ngfw/bin	1.1 GB	10 min	9 min