

Software Upgrade Guidelines

For your convenience, this document duplicates the critical and release-specific software upgrade guidelines published in the Firewall Threat Defense release notes. For FXOS upgrade guidelines for the Firepower 4100/9300, see Upgrade Guidelines for the Firepower 4100/9300 Chassis.

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 7.2, on page 2
- Upgrade Guidelines for Cloud-Delivered Firewall Management Center, on page 4
- Unresponsive Upgrades, on page 4
- Traffic Flow and Inspection for Firewall Threat Defense Upgrades, on page 5
- Traffic Flow and Inspection when Deploying Configurations, on page 7
- Time and Disk Space, on page 8

Minimum Version to Upgrade

Minimum Version to Upgrade

You can upgrade directly to Version 7.2, including maintenance releases, as follows.

Table 1: Minimum Version to Upgrade to Version 7.2

Platform	Minimum Version
Firewall Management Center	6.6
Firewall Threat Defense (except Threat Defense Virtual with GCP)	6.6 FXOS 2.12.1.95 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, 2.12.

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. The mininum version to upgrade to a Version 7.2.x maintenance release is Version 7.2.0.

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 7.2

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

Table 2: Upgrade Guidelines for Firewall Threat Defense with Firewall Management Center Version 7.2

✓	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
	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	Firewall Threat Defense	Any	Any
	Upgrade Guidelines for the Firepower 4100/9300 Chassis	Firepower 4100/9300	Any	Any
ADDITIONAL GUIDELINES FOR SPECIFIC DEPLOYMENTS				
	Extended Post-Upgrade Deploy to Version 7.2.4–7.2.5 for Large Configurations, on page 3	Firewall Management Center	6.6.0+	7.2.4 through 7.2.5

✓	Guideline	Platforms	Upgrading From	Directly To
	Reconnect with Cisco Secure Malware Analytics for High Availability Firewall Management Centers, on page 3	Firewall Management Center	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+

Extended Post-Upgrade Deploy to Version 7.2.4–7.2.5 for Large Configurations

Deployment: Firewall Management Center

Upgrading from: Any deployment where object optimization is disabled.

Directly to: Version 7.2.4-7.2.5

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 Firewall 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 Firewall 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.

Reconnect with Cisco Secure Malware Analytics for High Availability Firewall Management Centers

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 Firewall Management Center:

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, Firewall Threat Defense 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.

Upgrade Guidelines for Cloud-Delivered Firewall Management Center

You do not upgrade the Cloud-Delivered Firewall Management Center. We take care of feature updates. To upgrade Firewall Threat Defense with the Cloud-Delivered Firewall Management Center, see the Secure Firewall Threat Defense upgrade guides for Cloud-Delivered Firewall Management Center.

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 Firewall 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 Firewall Threat Defense Upgrade

For major and maintenance upgrades, you can manually cancel failed or in-progress upgrades, and retry failed upgrades. On the Firewall 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 Firewall Threat Defense CLI.

Note By default, Firewall 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 Firewall 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.

Traffic Flow and Inspection when Deploying Configurations

Snort typically restarts during the first deployment immediately after upgrade. This means that for Firewall Management Center upgrades, Snort could restart on all managed devices. Snort does not restart after subsequent deployments unless, before deploying, you modify specific policy or device configurations.

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.

Table 6: 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.

Interface Configuration		Traffic Behavior
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

Time to Upgrade

We recommend you track and record your own upgrade times so you can use them as future benchmarks. The following table lists some things that can affect upgrade time.

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 7: Upgrade Time Considerations

Consideration	Details
Versions	Upgrade time usually increases if your upgrade skips versions.
Models	Upgrade time usually increases with lower-end models.
Virtual appliances	Upgrade time in virtual deployments is highly hardware dependent.
High availability and clustering	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	Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how they 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.

Consideration	Details
Components	You may need additional time to perform operating system or virtual hosting upgrades, upgrade package transfers, readiness checks, VDB and intrusion rule (SRU/LSP) updates, configuration deployment, and other related tasks.

Disk Space to Upgrade

To upgrade, the upgrade package must be on the appliance. For device upgrades, you must also have enough space on the Firewall Management Center (in either /Volume or /var) for the device upgrade package. Or, you can use an internal server to store them. Readiness checks should indicate whether you have enough disk space to perform the upgrade. Without enough free disk space, the upgrade fails.