

Upgrade Guidelines

This document provides critical and release-specific upgrade guidelines for Version 6.7.

- Planning Your Upgrade, on page 1
- Minimum Version to Upgrade, on page 2
- New Upgrade Guidelines for Version 6.7, on page 2
- Previously Published Upgrade Guidelines, on page 4
- Unresponsive Upgrades, on page 14
- Firepower Threat Defense Upgrade Behavior: Other Devices, on page 14
- Time and Disk Space Tests, on page 22
- Upgrade Instructions, on page 24

Planning Your Upgrade

Careful planning and preparation can help you avoid missteps. This table summarizes the upgrade planning process. For detailed checklists and procedures, see the the appropriate upgrade or configuration guide for full instructions: Upgrade Instructions, on page 24.

Table 1: Upgrade Planning Phases

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read *all* upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Backups	Back up the software. Back up FXOS on the Firepower 4100/9300. Back up ASA for ASA FirePOWER.

Planning Phase	Includes
Upgrade Packages	Download upgrade packages from Cisco. Upload upgrade packages to the system.
Associated Upgrades	Upgrade virtual hosting in virtual deployments. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Check disk space. Deploy configurations. Run readiness checks. Check running tasks. Check deployment health and communications.

Minimum Version to Upgrade

You can upgrade directly to Version 6.7.0 as follows. You do not need to be running any specific maintenance release or patch level.

Table 2: Minimum Version to Upgrade to Version 6.7.0/6.7.x

Platform	Minimum Version
Firepower Management Center	6.3.0 You cannot upgrade to Version 6.7.0 from Version 6.6.5 or later maintenance release. This is because the Version 6.6.5 data store is newer than the Version 6.7.0 data store. If you are running Version 6.6.5, we recommend you upgrade directly to Version 7.0.0 or later.
Firepower devices	6.3.0 FXOS 2.9.1.131 or later build required for the Firepower 4100/9300.

New Upgrade Guidelines for Version 6.7

This checklist contains upgrade guidelines that are new or specific to Version 6.7.0.

Table 3: Version 6.7.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0, on page 3	FMC	6.6.5 or later 6.6.x release	6.7.0 only
	Upgrade Failure: Firepower 1010 Switch Ports with Invalid VLAN IDs, on page 3	Firepower 1010	6.4.0 through 6.6.x	6.7.0+

Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0

Deployments: FMC

Upgrading from: Version 6.6.5 or later maintenance release

Directly to: Version 6.7.0 only

You cannot upgrade to Version 6.7.0 from Version 6.6.5 or any later 6.6.x maintenance release. This is because the Version 6.6.5 data store is newer than the Version 6.7.0 data store. If you are running Version 6.6.5+, we recommend you upgrade directly to Version 7.0.0 or later.

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 4: 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.

Previously Published Upgrade Guidelines

This checklist contains older upgrade guidelines.

Table 5: Version 6.7.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 5	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases
	FMCv Requires 28 GB RAM for Upgrade, on page 3	FMCv	6.2.3 through 6.5.0.x	6.6.0+
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 7	Firepower 1000 series	6.4.0.x	6.5.0+
	Historical Data Removed During FTD/FDM Upgrade, on page 7	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 7	Any	6.2.3 through 6.4.0.x	6.5.0+
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 13	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+

Upgrade Failure: FMC with Email Alerting for Intrusion Events

Deployments: Firepower Management Center

Upgrading from: Version 6.2.3 through 6.7.0.x

Directly to: Version 6.6.0, 6.6.1, 6.6.3, or 6.7.0, as well as any patches to these releases

Related bugs: CSCvw38870, CSCvx86231

If you configured email alerting for individual intrusion events, fully disable it before you upgrade a Firepower Management Center to any of the versions listed above. Otherwise, the upgrade will fail.

You can reenable this feature after the upgrade. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

To fully disable intrusion email alerting:

1. On the Firepower Management Center, choose **Policies** > **Actions** > **Alerts**, then click **Intrusion Email**.
2. Set the **State** to **off**.
3. Next to **Rules**, click **Email Alerting per Rule Configuration** and deselect any rules.

   Note which rules you deselected so you can reselect them after the upgrade.

Tip If reselecting rules would be too time consuming, contact Cisco TAC *before* you upgrade. They can guide you through saving your selections, so you can quickly reimplement them post-upgrade.

4. Save your configurations.

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 6: 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.

Platform	Pre-Upgrade Action	Details
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.

Firepower 1000 Series Devices Require Post-Upgrade Power Cycle

Deployments: Firepower 1000 series

Upgrading from: Version 6.4.0.x

Directly to: Version 6.5.0+

Version 6.5.0 introduces an FXOS CLI 'secure erase' feature for Firepower 1000/2100 and Firepower 4100/9300 series devices.

For Firepower 1000 series devices, you must power cycle the device after you upgrade to Version 6.5.0+ for this feature to work properly. The automatic reboot is not sufficient. Other supported devices do not require the power cycle.

Historical Data Removed During FTD/FDM Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.3 through 6.4.x

Directly to: 6.5.0+

All historical report data is removed during the upgrade due to a database schema change. After the upgrade, you cannot query historical data, nor view historical data in dashboards.

New URL Categories and Reputations

Deployments: Any

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0+

Cisco Talos Intelligence Group (Talos) has introduced new categories and renamed reputations to classify and filter URLs. For detailed lists of category changes, see the Cisco Firepower Release Notes, Version 6.5.0. For descriptions of the new URL categories, see the Talos Intelligence Categories site.

Also new are the concepts of uncategorized and reputationless URLs, although rule configuration options stay the same:

- *Uncategorized URLs* can have a Questionable, Neutral, Favorable, or Trusted reputation.

  You can filter **Uncategorized** URLs but you cannot further constrain by reputation. These rules will match all uncategorized URLs, regardless of reputation.

  Note that there is no such thing as an Untrusted rule with no category. Otherwise uncategorized URLs with an Untrusted reputation are automatically assigned to the new Malicious Sites threat category.

- *Reputationless URLs* can belong to any category.

  You cannot filter reputationless URLs. There is no option in the rule editor for 'no reputation.' However, you can filter URLs with **Any** reputation, which includes reputationless URLs. These URLs must also be constrained by category. There is no utility to an Any/Any rule.

The following table summarizes the changes on upgrade. Although they are designed for minimal impact and will not prevent post-upgrade deploy for most customers, we *strongly* recommend you review these release notes and your current URL filtering configuration. Careful planning and preparation can help you avoid missteps, as well as reduce the time you spend troubleshooting post-upgrade.

Table 7: Deployment Changes on Upgrade

Change	Details
Modifies URL rule categories.	The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies: • Access control • SSL • QoS (FMC only) • Correlation (FMC only) These changes may create redundant or preempted rules, which can slow performance. If your configuration includes merged categories, you may experience minor changes to the URLs that are allowed or blocked.
Renames URL rule reputations.	The upgrade modifies URL rules to use the new reputation names: **1.** Untrusted (was *High Risk*) **2.** Questionable (was *Suspicious sites*) **3.** Neutral (was *Benign sites with security risks*) **4.** Favorable (was *Benign sites*) **5.** Trusted (was *Well Known*)

Change	Details
Clears the URL cache.	The upgrade clears the URL cache, which contains results that the system previously looked up in the cloud. Your users may temporarily experience slightly longer access times for URLs that are not in the local data set.
Labels 'legacy' events.	For already-logged events, the upgrade labels any associated URL category and reputation information as `Legacy`. These legacy events will age out of the database over time.

Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 8: Pre-Upgrade Actions

Action	Details

Make sure your appliances can reach Talos resources.	The system must be able to communicate with the following Cisco resources after the upgrade:
	• https://regsvc.sco.cisco.com/ — Registration
	• https://est.sco.cisco.com/ — Obtain certificates for secure communications
	• https://updates-talos.sco.cisco.com/ — Obtain client/server manifests
	• http://updates.ironport.com/ — Download database (note: uses port 80)
	• https://v3.sds.cisco.com/ — Cloud queries
	The cloud query service also uses the following IP address blocks:
	• IPv4 cloud queries:
	  • 146.112.62.0/24
	  • 146.112.63.0/24
	  • 146.112.255.0/24
	  • 146.112.59.0/24
	• IPv6 cloud queries:
	  • 2a04:e4c7:ffff::/48
	  • 2a04:e4c7:fffe::/48

Action	Details
Identify potential rule issues.	Understand the upcoming changes. Examine your current URL filtering configuration and determine what post-upgrade actions you will need to take (see the next section). **Note** You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade. In FMC deployments, we recommend you generate an *access control policy report*, which provides details on the policy's current saved configuration, including access control rules and rules in subordinate policies (such as SSL). For each URL rule, you can see the current categories, reputations, and associated rule actions. On the FMC, choose **Policies** > **Access Control** , then click the report icon () next to the appropriate policy.

Post-Upgrade Actions for URL Categories and Reputations

After upgrade, you should reexamine your URL filtering configuration and take the following actions as soon as possible. Depending on deployment type and the changes made by the upgrade, some — but not all — issues may be marked in the GUI. For example, in access control policies on FMC/FDM, you can click **Show Warnings** (FMC) or **Show Problem Rules** (FDM).

Table 9: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required.	The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy. On the FMC, these rules are marked.
Create or modify rules to include the **new categories**.	Most of the new categories identify threats. We strongly recommend you use them. On the FMC, these new categories are not marked after *this* upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.
Evaluate rules changed as a result of **merged categories**.	Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 11. Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.

Action	Details
Evaluate rules changed as a result of **split categories**.	The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity. These changes are not marked.
Understand which categories were **renamed** or are **unchanged**.	Although no action is required, you should be aware of these changes. These changes are not marked.
Evaluate how you handle **uncategorized** and **reputationless** URLs.	Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs. Make sure that rules that filter by the **Uncategorized** category, or by **Any** reputation, will behave as you expect.

Guidelines for Rules with Merged URL Categories

When you examine your URL filtering configuration before the upgrade, determine which of the following scenarios and guidelines apply to you. This will ensure that your post-upgrade configuration is as you expect, and that you can take quick action to resolve any issues.

Table 10: Guidelines for Rules with Merged URL Categories

Guideline	Details
Rule Order Determines Which Rule Matches Traffic	When considering rules that include the same category, remember that traffic matches the first rule in the list that includes the condition.
Categories in the Same Rule vs Categories in Different Rules	Merging categories in a single rule will merge into a single category in the rule. For example, if Category A and Category B are merging to become Category AB, and you have a rule with both Category A and Category B, then after merge the rule will have a single Category AB. Merging categories in different rules will result in separate rules with the same category in each rule after the merge. For example, if Category A and Category B are merging to become Category AB, and you have Rule 1 with Category A and Rule 2 with Category B, then after merge Rule 1 and Rule 2 will each include Category AB. How you choose to resolve this situation depends on the rule order, on the actions and reputation levels associated with the rules, on the other URL categories included in the rule, and on the non-URL conditions that are included in the rule.
Associated Action	If merged categories in different rules were associated with different actions, then after merge you may have two or more rules with different actions for the same category.

Guideline	Details
Associated Reputation Level	If a single rule includes categories that were associated with different reputation levels before merging, the merged category will be associated with the more inclusive reputation level. For example, if Category A was associated in a particular rule with **Any reputation** and Category B was associated in the same rule with reputation level **3 - Benign sites with security risks**, then after merge Category AB in that rule will be associated with **Any reputation**.
Duplicate and Redundant Categories and Rules	After merge, different rules may have the same category associated with different actions and reputation levels. Redundant rules may not be exact duplicates, but they may no longer match traffic if another rule earlier in the rule order matches instead. For example, if you have pre-merge Rule 1 with Category A that applies to Any Reputation, and Rule 2 with Category B that applies only to Reputation 1-3, then after merge, both Rule 1 and Rule 2 will have Category AB, but Rule 2 will never match if Rule 1 is higher in the rule order. On the FMC, rules with an identical category and reputation will show a warning. However, these warnings will not indicate rules that include the same category but a different reputation. Caution: Consider all conditions in the rule when determining how to resolve duplicate or redundant categories.
Other URL Categories in a Rule	Rules with merged URLs may also include other URL categories. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.
Non-URL Conditions in a Rule	Rules with merged URL categories may also include other rule conditions, such as application conditions. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.

The examples in the following table use Category A and Category B, now merged into Category AB. In two-rule examples, Rule 1 comes before Rule 2.

Table 11: Examples of Rules with Merged URL Categories

Scenario	Before Upgrade	After Upgrade
Merged categories in the same rule	Rule 1 has Category A and Category B.	Rule 1 has Category AB.
Merged categories in different rules	Rule 1 has Category A. Rule 2 has Category B.	Rule 1 has Category AB. Rule 2 has Category AB. The specific result varies by the rules' order in the list, reputation levels, and associated actions. You should also consider all other conditions in the rule when determining how to resolve any redundancy.

Scenario	Before Upgrade	After Upgrade
Merged categories in different rules have different actions (Reputation is the same)	Rule 1 has Category A set to Allow. Rule 2 has Category B set to Block. (Reputation is the same)	Rule 1 has Category AB set to Allow. Rule 2 has Category AB set to Block. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, and will display a warning indicator if you show warnings after merge, because both category and reputation are the same.
Merged categories in the same rule have different reputation levels	Rule 1 includes: Category A with Reputation Any Category B with Reputation 1-3	Rule 1 includes Category AB with Reputation Any.
Merged categories in different rules have different reputation levels	Rule 1 includes Category A with Reputation Any. Rule 2 includes Category B with Reputation 1-3.	Rule 1 includes Category AB with Reputation Any. Rule 2 includes Category AB with Reputation 1-3. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, but you will not see a warning indicator because the reputations are not identical.

TLS Crypto Acceleration Enabled/Cannot Disable

Deployments: Firepower 2100 series, Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.3.x

Directly to: Version 6.4.0+

SSL hardware acceleration has been renamed *TLS crypto acceleration*.

Depending on the device, TLS crypto acceleration might be performed in software or in hardware. The upgrade automatically enables acceleration on all eligible devices, even if you previously disabled the feature manually. In most cases you cannot configure this feature; it is automatically enabled and you cannot disable it.

Upgrading to Version 6.4.0: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for *one* container instance per module/security engine. Acceleration is disabled for other container instances, but enabled for native instances.

Upgrading to Version 6.5.0+: If you are using the multi-instance capability of the Firepower 4100/9300 chassis, you can use the FXOS CLI to enable TLS crypto acceleration for multiple container instances (up to 16) on a Firepower 4100/9300 chassis. New instances have this feature enabled by default. However, the upgrade does *not* enable acceleration on existing instances. Instead, use the **config hwCrypto enable** CLI command.

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 or Classic Device 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:

- FMC: Use the Upgrade Status pop-up, accessible from the Upgrade tab on the Device Management page, and from the Message Center.
- FDM: Use the System Upgrade panel.

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/scalability 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.

Firepower Threat Defense Upgrade Behavior: Other Devices

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 12: Traffic Behavior: 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.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (Firepower 2100 series, 6.3+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (Firepower 2100 series, 6.3+).	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** (Firepower 2100 series, 6.3+).	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 devices.

- Firepower Threat Defense with FMC: For high availability pairs, the standby device upgrades first. The devices switch roles, then the new standby upgrades.
- Firepower Threat Defense with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: 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.
- FTD with FDM: Not supported.

Software Revert (Major/Maintenance Releases)

Reverting returns FTD to its state just before the last major or maintenance upgrade. Regardless of deployment — even for high availability/scalability — you should expect interruptions to traffic flow and inspection. 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.

Support for revert begins in Version 6.7.0 for FTD with FDM. It is not supported for FTD with FMC.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 13: Traffic Behavior: 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 (6.0.1–6.1).	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 (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

NGIPSv Upgrade Behavior

This section describes device and traffic behavior when you upgrade NGIPSv.

Firepower Software Upgrade

Interface configurations determine how NGIPSv handles traffic during the upgrade.

Table 14: Traffic Behavior During NGIPSv Upgrade

Interface Configuration	Traffic Behavior
Inline	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 15: Traffic Behavior During NGIPSv Deployment

Interface Configuration	Traffic Behavior
Inline, **Failsafe** enabled or disabled	Passed without inspection A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected

Firepower 7000/8000 Series Upgrade Behavior

The following sections describe device and traffic behavior when you upgrade Firepower 7000/8000 series devices.

Standalone 7000/8000 Series: Firepower Software Upgrade

Interface configurations determine how a standalone device handles traffic during the upgrade.

Table 16: Traffic Behavior During Upgrade: Standalone 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, hardware bypass enabled (**Bypass Mode: Bypass**)	Passed without inspection, although traffic is interrupted briefly at two points: • At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass. • After the upgrade finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces.
Inline, no hardware bypass module,or hardware bypass disabled (**Bypass Mode: Non-Bypass**)	Dropped
Inline, tap mode	Egress packet immediately, copy not inspected
Passive	Uninterrupted, not inspected

Interface Configuration	Traffic Behavior
Routed, switched	Dropped

7000/8000 Series High Availability Pairs: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading devices (or device stacks) in high availability pairs. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

Which peer upgrades first depends on your deployment:

- Routed or switched: Standby upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.
- Access control only: Active upgrades first. When the upgrade completes, the active and standby maintain their old roles.

8000 Series Stacks: Firepower Software Upgrade

In an 8000 series stack, devices upgrade simultaneously. Until the primary device completes its upgrade and the stack resumes operation, traffic is affected as if the stack were a standalone device. Until all devices complete the upgrade, the stack operates in a limited, mixed-version state.

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 17: Traffic Behavior During Deployment: 7000/8000 Series

Interface Configuration	Traffic Behavior
Inline, **Failsafe** enabled or disabled	Passed without inspection A few packets might drop if **Failsafe** is disabled and Snort is busy but not down.
Inline, tap mode	Egress packet immediately, copy bypasses Snort
Passive	Uninterrupted, not inspected
Routed, switched	Dropped

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

- Reboot a device.
- Upgrade the device software, operating system, or virtual hosting environment.
- Uninstall or revert the device software.
- Move a device between domains.
- Deploy configuration changes (Snort process restarts).

Device type, high availability/scalibility configurations, and interface configurations determine the nature of the interruptions. We *strongly* recommend performing these tasks in a maintenance window or at a time when any interruption will have the least impact on your deployment.

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

FXOS Upgrades

Upgrade FXOS on each chassis independently, even if you have inter-chassis clustering or high availability pairs configured. How you perform the upgrade determines how your devices handle traffic during the FXOS upgrade.

Table 18: Traffic Behavior: FXOS Upgrades

Deployment	Method	Traffic Behavior
Standalone	—	Dropped.
High availability	**Best Practice:** Update FXOS on the standby, switch active peers, upgrade the new standby.	Unaffected.
	Upgrade FXOS on the active peer before the standby is finished upgrading.	Dropped until one peer is online.
Inter-chassis cluster (6.2+)	**Best Practice:** Upgrade one chassis at a time so at least one module is always online.	Unaffected.
	Upgrade chassis at the same time, so all modules are down at some point.	Dropped until at least one module is online.
Intra-chassis cluster (Firepower 9300 only)	Hardware bypass enabled: **Bypass: Standby** or **Bypass-Force**. (6.1+)	Passed without inspection.
	Hardware bypass disabled: **Bypass: Disabled**. (6.1+)	Dropped until at least one module is online.
	No hardware bypass module.	Dropped until at least one module is online.

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 19: Traffic Behavior: 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.
IPS-only interfaces	Inline set, hardware bypass force-enabled: **Bypass: Force** (6.1+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: **Bypass: Standby** (6.1+).	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** (6.1+).	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.

- FTD with FMC: 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.

- FTD with FDM: For high availability pairs, upgrade the standby, manually switch roles, then upgrade the new standby.

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations.

- FTD with FMC: 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.
- FTD with FDM: Not supported.

Software Revert (Major/Maintenance Releases)

Reverting returns FTD to its state just before the last major or maintenance upgrade. Regardless of deployment — even for high availability/scalability — you should expect interruptions to traffic flow and inspection. 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.

Support for revert begins in Version 6.7.0 for FTD with FDM. It is not supported for FTD with FMC.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. 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. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.

Table 20: Traffic Behavior: 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 (6.0.1–6.1).	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 (6.2+).	Dropped.
	Inline set, **Snort Fail Open: Down**: enabled (6.2+).	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 14.

Table 21: 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.

Condition	Details
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 22: 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.
FTD with FDM	Use the **show disk** CLI command.

Time and Disk Space for Version 6.7.0

Table 23: Time and Disk Space for Version 6.7.0

Platform	Space in /var	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	13.6 GB	70 MB	—	46 min	9 min
FMCv: VMware	15.5 GB	64 MB	—	35 min	8 min
Firepower 1000 series	430 MB	11 GB	2 GB	17 min	16 min
Firepower 2100 series	500 MB	11 GB	1.1 GB	15 min	16 min
Firepower 9300	64 MB	11.1 GB	1.1 GB	13 min	12 min
Firepower 4100 series	10 MB	10 GB	1.1 GB	10 min	12 min
Firepower 4100 series container instance	8 MB	9.5 GB	1.1 GB	10 min	9 min
ASA 5500-X series with FTD	8.7 GB	96 KB	1.1 GB	26 min	13 min
FTDv: VMware	8.1 GB	26 KB	1.1 GB	14 min	18 min
ASA FirePOWER	10.3 GB	64 MB	1.3 GB	62 min	11 min
NGIPSv	5.5 GB	54 MB	840 MB	10 min	6 min

Upgrade Instructions

The release notes do not contain upgrade instructions. After you read the guidelines and warnings in these release notes, see one of the following documents.

Table 24: Firepower Upgrade Instructions

Task	Guide
Upgrade in Firepower Management Center deployments.	Cisco Firepower Management Center Upgrade Guide, Version 6.0–7.0
Upgrade Firepower Threat Defense with Firepower Device Manager.	Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager See the *System Management* chapter in the guide for the Firepower Threat Defense version you are currently running—not the version you are upgrading to.

Task	Guide
Upgrade FXOS on a Firepower 4100/9300 chassis.	Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1
Upgrade ASA FirePOWER modules with ASDM.	Cisco ASA Upgrade Guide
Upgrade the ROMMON image on the ISA 3000, ASA 5508-X, and ASA 5516-X.	Cisco ASA and Firepower Threat Defense Reimage Guide See the *Upgrade the ROMMON Image* section. You should always make sure you have the latest image.