Upgrade the Software

This chapter provides critical and release-specific information.

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 31.

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 6.5.0 as follows. You do not need to be running any specific patch level.

Table 2: Minimum Version to Upgrade to Version 6.5.0

Platform	Minimum Version
Firepower Management Center	6.2.3
Firepower devices	6.2.3 FXOS 2.7.1.92 or later build required for the Firepower 4100/9300.

New Upgrade Guidelines for Version 6.5.0

This checklist contains upgrade guidelines that are new or specific to Version 6.5.0.

Table 3: Version 6.5.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 3	Firepower 1000 series	6.4.0.x	6.5.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	Disable Egress Optimization for Version 6.5.0, on page 3	FTD	6.2.3 through 6.4.0.x	6.5.0 only
	Historical Data Removed During FTD/FDM Upgrade, on page 4	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 4	Any	6.2.3 through 6.4.0.x	6.5.0+

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.

Disable Egress Optimization for Version 6.5.0

Deployments: FTD

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0 only

To mitigate CSCvq34340, patching an FTD device to Version 6.4.0.7+ or Version 6.5.0.2+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled.

Upgrading to Version 6.5.0:

- From Version 6.2.3.x: Enables and turns on egress optimization.
- From Version 6.3.0.x: Enables and turns on egress optimization.
- From Version 6.4.0.x: Respects your current settings. However, if the Version 6.4.0.x patch turned off egress optimization but the feature is still enabled, the upgrade to Version 6.5.0 turns it on again.

Note We recommend you patch to Version 6.5.0.2+ or upgrade to Version 6.6.0. If you remain at Version 6.5.0 or 6.5.0.1, you should manually disable egress optimization from the FTD CLI: **no asp inspect-dp egress-optimization**.

This issue is fixed in Version 6.6.0, where egress optimization works as expected. For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature.

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 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 4: 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. For detailed lists of category changes, see URL Category Changes, on page 10.
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*)
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 5: 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

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 6: Post-Upgrade Actions

Action	Details
Remove **deprecated categories** from rules. Required. List: Deprecated Categories, on page 14.	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**. List: New Categories, on page 13.	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**. List: Merged Categories, on page 14.	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 7. 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.
Evaluate rules changed as a result of **split categories**. List: Split Categories, on page 15.	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**. Lists: Renamed Categories, on page 17 and Unchanged Categories, on page 18.	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 7: 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.
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.

Guideline	Details
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 8: 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.
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.

URL Category Changes

Use this table to determine how your URL categories changed.

Table 9: Index of Old URL Categories

Old Category	Change		Old Category	Change
Abortion	Merged Categories, on page 14		Military	Unchanged Categories, on page 18
Abused Drugs	Merged Categories, on page 14		Motor Vehicles	Renamed Categories, on page 17
Adult and Pornography	Split Categories, on page 15		Music	Renamed Categories, on page 17
Alcohol and Tobacco	Split Categories, on page 15		News and Media	Renamed Categories, on page 17
Bot Nets	Renamed Categories, on page 17		Nudity	Renamed Categories, on page 17
Business and Economy	Split Categories, on page 15		Online Greeting cards	Renamed Categories, on page 17
Cheating	Renamed Categories, on page 17		Open HTTP Proxies	Renamed Categories, on page 17
Computer and Internet Info	Split Categories, on page 15		Parked Domains	Unchanged Categories, on page 18
Computer and Internet Security	Split Categories, on page 15		Pay to Surf	Merged Categories, on page 14
Confirmed SPAM Sources	Merged Categories, on page 14		Peer to Peer	Renamed Categories, on page 17
Content Delivery Networks	Merged Categories, on page 14		Personal sites and Blogs	Split Categories, on page 15
Cult and Occult	Split Categories, on page 15		Personal Storage	Split Categories, on page 15

Old Category	Change		Old Category	Change
Dating	Unchanged Categories, on page 18		Philosophy and Political Advocacy	Renamed Categories, on page 17
Dead Sites	Renamed Categories, on page 17		Phishing and Other Frauds	Renamed Categories, on page 17
Dynamically Generated Content	Merged Categories, on page 14		Private IP Address	Deprecated Categories, on page 14
Educational Institutions	Merged Categories, on page 14		Proxy Avoidance and Anonymizers	Renamed Categories, on page 17
Entertainment and Arts	Split Categories, on page 15		Questionable	Renamed Categories, on page 17
Fashion and Beauty	Renamed Categories, on page 17		Real Estate	Unchanged Categories, on page 18
Financial Services	Renamed Categories, on page 17		Recreation and Hobbies	Merged Categories, on page 14
Food and Dining	Renamed Categories, on page 17		Reference and Research	Split Categories, on page 15
Gambling	Split Categories, on page 15		Religion	Unchanged Categories, on page 18
Games	Unchanged Categories, on page 18		Search Engines	Merged Categories, on page 14
Government	Merged Categories, on page 14		Sex Education	Merged Categories, on page 14
Gross	Merged Categories, on page 14		Shareware and Freeware	Renamed Categories, on page 17
Hacking	Merged Categories, on page 14		Shopping	Unchanged Categories, on page 18

Old Category	Change		Old Category	Change
Hate and Racism	Renamed Categories, on page 17		Social Network	Split Categories, on page 15
Health and Medicine	Renamed Categories, on page 17		Society	Split Categories, on page 15
Home and Garden	Split Categories, on page 15		SPAM URLs	Merged Categories, on page 14
Hunting and Fishing	Renamed Categories, on page 17		Sports	Merged Categories, on page 14
Illegal	Split Categories, on page 15		Spyware and Adware	Unchanged Categories, on page 18
Image and Video Search	Renamed Categories, on page 17		Streaming Media	Renamed Categories, on page 17
Individual Stock Advice and Tools	Renamed Categories, on page 17		Swimsuits and Intimate Apparel	Renamed Categories, on page 17
Internet Communications	Split Categories, on page 15		Training and Tools	Merged Categories, on page 14
Internet Portals	Merged Categories, on page 14		Travel	Unchanged Categories, on page 18
Job Search	Unchanged Categories, on page 18		Uncategorized	Deprecated Categories, on page 14
Keyloggers and Monitoring	Merged Categories, on page 14		Uncomfirmed SPAM Sources	Merged Categories, on page 14
Kids	Renamed Categories, on page 17		Violence	Merged Categories, on page 14
Legal	Merged Categories, on page 14		Weapons	Unchanged Categories, on page 18
Local Information	Renamed Categories, on page 17		Web Advertisements	Merged Categories, on page 14

Old Category	Change		Old Category	Change
Malware Sites	Unchanged Categories, on page 18		Web based email	Split Categories, on page 15
Marijuana	Merged Categories, on page 14		Web Hosting Sites	Renamed Categories, on page 17

New Categories

These tables list entirely new URL categories, most of which identify threats. We strongly recommend you create or modify URL rules to include the new threat categories. Note that some existing URL categories do identify threats; we recommend you include those also. For a list of threat categories, see the Talos Intellience Categories site.

Table 10: New Categories

New Category
Dynamic and Residential

Table 11: New Threat Categories

New Threat Category
Bogon
Cryptojacking
DNS Tunneling
Domain Generated Algorithm
Dynamic DNS
Ebanking Fraud
Exploits
High Risk Sites and Locations
Indicators of Compromise (IOC)
Linkshare
Malicious Sites
Mobile Threats
Newly Seen Domains
Open Mail Relay

New Threat Category
P2P Malware Node
Potential DNS Rebinding
TOR exit Nodes

Deprecated Categories

The upgrade does not modify URL rules that use deprecated categories. These rules will prevent deploy; you should delete or modify them.

Table 12: Deprecated Categories

Deprecated Category
Uncategorized
Private IP Address

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 7.

We also strongly recommend you create or modify URL rules to include newly designated threat categories (Spam).

Table 13: Merged Categories

Old Categories	New Merged Category
Web Advertisements	Advertisements
Pay to Surf	
Educational Institutions	Education
Training and Tools	
Violence	Extreme
Gross	
Government	Government and Law
Legal	
Abused Drugs	Illegal Drugs
Marijuana	

Old Categories	New Merged Category
Dynamically Generated Content	Infrastructure
Content Delivery Networks	
Hacking	Hacking
Keyloggers and Monitoring	
Search Engines	Search Engines and Portals
Internet Portals	
Sex Education	Sex Education
Abortion	
Confirmed SPAM Sources	Spam *(threat category)*
SPAM URLs	
Unconfirmed SPAM Sources	
Recreation and Hobbies	Sports and Recreations
Sports	

Split Categories

The upgrade replaces each old, single category in URL rules with *all* the new categories that map to the old one. After upgrade, you can modify affected rules to take advantage of the new granularity.

Table 14: Split Categories

Old Single Category	New Split Categories
Adult and Pornography	Pornography
	Adult
Alcohol and Tobacco	Alcohol
	Tobacco
Business and Economy	Business and Industry
	Mobile Phones
Computer and Internet Info	Software Updates
	Computers and Internet
	SaaS and B2B
	Online Meetings

Old Single Category	New Split Categories
Computer and Internet Security	Computer Security
	Personal VPN
Cult and Occult	Paranormal
	Astrology
Entertainment and Arts	Arts
	Entertainment
Gambling	Gambling
	Lotteries
Home and Garden	Nature
	DIY Projects
Illegal	Illegal Activities
	Child Abuse Content
	Illegal Downloads
Internet Communications	Internet Telephony
	Chat and Instant Messaging
Personal sites and Blogs	Personal Sites
	Online Communities
Personal Storage	Online Storage and Backup
	File Transfer Services
Reference and Research	Science and Technology
	Social Science
Social Network	Social Networking
	Professional Networking
Society	Society and Culture
	Non-governmental Organisation
Web based email	Web-based Email
	Organisation Email

Renamed Categories

Although no action is required, you should be aware of these changes. We do strongly recommend you create or modify URL rules to include the newly designated threat categories (Botnets, Open HTTP Proxy, Phishing).

Table 15: Renamed Categories

Old Category Name	New Category Name
Bot Nets	Botnets *(threat category)*
Cheating	Cheating and Plagiarism
Dead Sites	Not Actionable
Fashion and Beauty	Fashion
Financial Services	Finance
Food and Dining	Dining and Drinking
Hate and Racism	Hate Speech
Health and Medicine	Health and Nutrition
Hunting and Fishing	Hunting
Image and Video Search	Photo Search and Images
Individual Stock Advice and Tools	Online Trading
Kids	Safe for Kids
Local Information	Reference
Motor Vehicles	Transportation
Music	Streaming Audio
News and Media	News
Nudity	Non-sexual Nudity
Online Greeting cards	Digital Postcards
Open HTTP Proxies	Open HTTP Proxy *(threat category)*
Peer to Peer	Peer File Transfer
Philosophy and Political Advocacy	Politics
Phishing and Other Frauds	Phishing *(threat category)*
Proxy Avoidance and Anonymizers	Filter Avoidance
Questionable	Humor

Old Category Name	New Category Name
Shareware and Freeware	Freeware and Shareware
Streaming Media	Streaming Video
Swimsuits and Intimate Apparel	Lingerie and Swimsuits
Web Hosting Sites	Web Hosting

Unchanged Categories

Although no action is required, you should be aware of these changes. We do strongly recommend you create or modify URL rules to include the newly designated threat categories (Malware Sites, Spyware and Adware).

Table 16: Unchanged Categories

Unchanged Category
Dating
Games
Job Search
Military
Parked Domains
Real Estate
Religion
Shopping
Travel
Weapons

Table 17: Unchanged Threat Categories

Unchanged Threat Category
Malware Sites *(threat category)*
Spyware and Adware *(threat category)*

Previously Published Upgrade Guidelines

This checklist contains older upgrade guidelines.

Table 18: Version 6.5.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 19	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 19	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+
	Readiness Check May Fail on FMC, NGIPSv, on page 20	FMC NGIPSv	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 20	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 21	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 21	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 22	Any	6.1.0 through 6.2.3.x	6.3.0+

Upgrade Failure: Insufficient Disk Space on Container Instances

Deployments: Firepower 4100/9300 with FTD

Upgrading from: Version 6.3.0 through 6.4.0.x

Directly to: Version 6.3.0.1 through Version 6.5.0

Most often during major upgrades — but possible while patching — FTD devices configured with container instances can fail in the precheck stage with an erroneous insufficient-disk-space warning.

If this happens to you, you can try to free up more disk space. If that does not work, contact Cisco TAC.

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.

Readiness Check May Fail on FMC, NGIPSv

Deployments: FMC, NGIPSv

Upgrading from: Version 6.1.0 through 6.1.0.6, Version 6.2.0 through 6.2.0.6, Version 6.2.1, Version 6.2.2 through 6.2.2.4, and Version 6.2.3 through 6.2.3.4

Directly to: Version 6.3.0+

You cannot run the readiness check on the listed models when upgrading from one of the listed Firepower versions. This occurs because the readiness check process is incompatible with newer upgrade packages.

Table 19: Patches with Readiness Checks for Version 6.3.0+

Readiness Check Not Supported	First Patch with Fix
6.1.0 through 6.1.0.6	6.1.0.7
6.2.0 through 6.2.0.6	6.2.0.7
6.2.1	None. Upgrade to Version 6.2.3.5+.
6.2.2 through 6.2.2.4	6.2.2.5
6.2.3 through 6.2.3.4	6.2.3.5

RA VPN Default Setting Change Can Block VPN Traffic

Deployments: Firepower Threat Defense configured for remote access VPN

Upgrading from: Version 6.2.x

Directly to: Version 6.3+

Version 6.3 changes the default setting for a hidden option, **sysopt connection permit-vpn**. Upgrading can cause your remote access VPN to stop passing traffic. If this happens, use either of these techniques:

- Create a FlexConfig object that configures the **sysopt connection permit-vpn** command. The new default for this command is **no sysopt connection permit-vpn**.

  This is the more secure method to allow traffic in the VPN, because external users cannot spoof IP addresses in the remote access VPN address pool. The downside is that the VPN traffic will not be inspected, which means that intrusion and file protection, URL filtering, or other advanced features will not be applied to the traffic.

- Create access control rules to allow connections from the remote access VPN address pool.

  This method ensures that VPN traffic is inspected and advanced services can be applied to the connections. The downside is that it opens the possibility for external users to spoof IP addresses and thus gain access to your internal network.

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

In Version 6.3, Security Intelligence configurations enable application detection and identification. If you disabled discovery in your current deployment, the upgrade process may enable it again. Disabling discovery if you don't need it (for example, in an IPS-only deployment) can improve performance.

To disable discovery you must:

- Delete all rules from your network discovery policy.
- Use only simple network-based conditions to perform access control: zone, IP address, VLAN tag, and port. Do not perform any kind of application, user, URL, or geolocation control.
- **(NEW)** Disable network and URL-based Security Intelligence by deleting all whitelists and blacklists from your access control policy's Security Intelligence configuration, including the default Global lists.
- **(NEW)** Disable DNS-based Security Intelligence by deleting or disabling all rules in the associated DNS policy, including the default Global Whitelist for DNS and Global Blacklist for DNS rules.

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

Upgrading from: Version 6.1.0 through 6.2.3.x, with VDB 299+

Directly to: Version 6.3.0+

If you upgrade while using vulnerability database (VDB) 299 or later, an issue with the upgrade process prevents you from using CIP detection post-upgrade. This includes every VDB released from June 2018 to now, even the latest VDB.

Although we always recommend you update the vulnerability database (VDB) to the latest version after you upgrade, it is especially important in this case.

To check if you are affected by this issue, try to configure an access control rule with a CIP-based application condition. If you cannot find any CIP applications in the rule editor, manually update the VDB.

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

For network variables in an intrusion variable set, any IP addresses you *exclude* must be a subset of the IP addresses you *include*. This table shows you examples of valid and invalid configurations.

Valid	Invalid
Include: 10.0.0.0/8 Exclude: 10.1.0.0/16	Include: 10.1.0.0/16 Exclude: 172.16.0.0/12 Exclude: 10.0.0.0/8

Before Version 6.3.0, you could successfully save a network variable with this type of invalid configuration. Now, these configurations block deploy with the error: `Variable set has invalid excluded values`.

If this happens, identify and edit the incorrectly configured variable set, then redeploy. Note that you may have to edit network objects and groups referenced by your variable set.

Unresponsive Upgrades

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

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 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 20: 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 21: 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** (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.

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 22: 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.

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 23: 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.

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 24: 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.

ASA FirePOWER Upgrade Behavior

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during the Firepower software upgrade, including when you deploy certain configurations that restart the Snort process.

Table 25: Traffic Behavior During ASA FirePOWER Upgrade

Traffic Redirection Policy	Traffic Behavior
Fail open (**sfr fail-open**)	Passed without inspection
Fail closed (**sfr fail-close**)	Dropped
Monitor only (**sfr {fail-close}|{fail-open} monitor-only**)	Egress packet immediately, copy not inspected

Traffic Behavior During ASA FirePOWER Deployment

Traffic behavior while the Snort process restarts is the same as when you upgrade the ASA FirePOWER module.

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. Your service policies determine whether traffic drops or passes without inspection during the interruption.

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 26: 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 27: 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

Time and Disk Space Tests

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

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 Even if the system appears inactive, do not manually reboot, shut down, or 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, contact Cisco TAC.

Table 28: Time Test Conditions for Software Upgrades

Condition	Details
Deployment	Times for FTD 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 /var) for the device upgrade package. If you are using FDM, ignore those values.

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

Table 29: 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.

Version 6.5.0 Time and Disk Space

Table 30: Version 6.5.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	18.6 GB	24 MB	—	47 min
FMCv: VMware	18.7 GB	30 MB	—	35 min
Firepower 1000 series	1.0 GB	11.3 GB	1.1 GB	10 min
Firepower 2100 series	1.1 GB	12.3 GB	1.0 GB	12 min
Firepower 4100 series	20 MB	10.8 GB	990 MB	8 min
Firepower 9300	23 MB	10.9 GB	990 MB	8 min
ASA 5500-X series with FTD	10.4 GB	120 KB	1.1 GB	17 min
FTDv: VMware	10 GB	120 KB	1.1 GB	10 min
ASA FirePOWER	12.2 GB	26 MB	1.3 GB	81 min
NGIPSv	6.6 GB	22 MB	870 MB	

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 31: 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.
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.