



# Upgrade Guidelines

This document provides critical and release-specific upgrade guidelines for Version 6.6.

- [Planning Your Upgrade, on page 1](#)
- [Minimum Version to Upgrade, on page 2](#)
- [Upgrade Guidelines for Version 6.6, on page 3](#)
- [Upgrade Guidelines for FXOS, on page 17](#)
- [Unresponsive Upgrades, on page 18](#)
- [Uninstall a Patch, on page 18](#)
- [Traffic Flow and Inspection, on page 20](#)
- [Time and Disk Space Tests, on page 25](#)

## 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 appropriate upgrade or configuration guide: <http://www.cisco.com/go/threatdefense-66-docs>.

**Table 1: Upgrade Planning Phases**

Planning Phase	Includes
Planning and Feasibility	Assess your deployment. Plan your upgrade path. Read <i>all</i> 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 firmware on the Firepower 4100/9300. Upgrade FXOS on the Firepower 4100/9300. Upgrade ASA for ASA FirePOWER.
Final Checks	Check configurations. Check NTP synchronization. Deploy configurations. Run readiness checks. Check disk space. Check running tasks. Check deployment health and communications.

## Minimum Version to Upgrade

### Minimum Version to Upgrade

You can upgrade directly to Version 6.6, including maintenance releases, as follows.

*Table 2: Minimum Version to Upgrade to Version 6.6*

Platform	Minimum Version
FMC	6.2.3
FTD	6.2.3 FXOS 2.8.1.15 is required for the Firepower 4100/9300. In most cases, we recommend you use the latest FXOS build in each major version. To help you decide, see the <a href="#">Cisco Firepower 4100/9300 FXOS Release Notes, 2.8(1)</a> .
ASA with FirePOWER Services	6.2.3 See <a href="#">Device Platforms</a> for ASA requirements for your model. Although there is wide compatibility between ASA and ASA FirePOWER versions, upgrading allows you to take advantage of new features and resolved issues. To help you decide, see the <a href="#">Cisco Secure Firewall ASA Release Notes</a> .
NGIPSv	6.2.3

### Minimum Version to Patch

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

## Upgrade Guidelines for Version 6.6

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

**Table 3: Upgrade Guidelines for FTD with FMC Version 6.6**

✓	Guideline	Platforms	Upgrading From	Directly To
	<a href="#">Cisco Secure Firewall Management Center New Features by Release</a> , for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	<a href="#">Open and Resolved Bugs</a> , for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any
	<a href="#">Minimum Version to Upgrade</a> , on page 2	Any	Any	Any
	<a href="#">Upgrade Guidelines for FXOS</a> , on page 17	Firepower 4100/9300	Any	Any
	<a href="#">Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0</a> , on page 6	FMC	6.6.5 or later 6.6.x release	6.7.0 only
	<a href="#">Upgrade Failure: FMC with Email Alerting for Intrusion Events</a> , on page 6	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.
	<a href="#">FMCv Requires 28 GB RAM for Upgrade</a> , on page 7	FMCv	6.2.3 through 6.5.0.x	6.6+
	<a href="#">Firepower 1000 Series Devices Require Post-Upgrade Power Cycle</a> , on page 8	Firepower 1000 series	6.4.0.x	6.5+
	<a href="#">New URL Categories and Reputations</a> , on page 8	Any	6.2.3 through 6.4.0.x	6.5+

✓	Guideline	Platforms	Upgrading From	Directly To
	<a href="#">TLS Crypto Acceleration Enabled/Cannot Disable, on page 14</a>	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4+
	<a href="#">Renamed Upgrade and Installation Packages, on page 14</a>	FMC Firepower 7000/8000 series NGIPSv	Any	6.3+
	<a href="#">Readiness Check May Fail on FMC, NGIPSv, on page 15</a>	FMC Firepower 7000/8000 series 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+
	<a href="#">RA VPN Default Setting Change Can Block VPN Traffic, on page 15</a>	FTD	6.2.0 through 6.2.3.x	6.3+
	<a href="#">Security Intelligence Enables Application Identification, on page 16</a>	FMC deployments	6.1.0 through 6.2.3.x	6.3+
	<a href="#">Update VDB after Upgrade to Enable CIP Detection, on page 16</a>	Any	6.1.0 through 6.2.3.x	6.3+
	<a href="#">Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 17</a>	Any	6.1.0 through 6.2.3.x	6.3+

**Table 4: Upgrade Guidelines for FTD with FDM Version 6.6**

✓	Guideline	Platforms	Upgrading From	Directly To
	<a href="#">Cisco Secure Firewall Device Manager New Features by Release</a> , for new and deprecated features that have upgrade impact. Check all versions between your current and target version.	Any	Any	Any
	<a href="#">Open and Resolved Bugs</a> , for bugs that have upgrade impact. Check all versions of the release notes between your current and target version.	Any	Any	Any

✓	Guideline	Platforms	Upgrading From	Directly To
	<a href="#">Minimum Version to Upgrade, on page 2</a>	Any	Any	Any
	<a href="#">Upgrade Guidelines for FXOS, on page 17</a>	Firepower 4100/9300	Any	Any
	<a href="#">Version 6.6.0.1 FTD Upgrade with FDM Suspends HA, on page 5</a>	Any	6.6.0	6.6.0.1
	<a href="#">Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 8</a>	Firepower 1000 series	6.4.0.x	6.5+
	<a href="#">Historical Data Removed During FTD Upgrade with FDM, on page 8</a>	Any	6.2.3 through 6.4.0.x	6.5+
	<a href="#">New URL Categories and Reputations, on page 8</a>	Any	6.2.3 through 6.4.0.x	6.5+
	<a href="#">TLS Crypto Acceleration Enabled/Cannot Disable, on page 14</a>	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4+
	<a href="#">Update VDB after Upgrade to Enable CIP Detection, on page 16</a>	Any	6.1.0 through 6.2.3.x	6.3+
	<a href="#">Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 17</a>	Any	6.1.0 through 6.2.3.x	6.3+

## Version 6.6.0.1 FTD Upgrade with FDM Suspends HA

**Deployments:** FTD with FDM, configured as a high availability pair

**Upgrading from:** Version 6.6.0

**Directly to:** Version 6.6.0.1

**Related bug:** [CSCvv45500](#)

After you upgrade an FDM-managed FTD device in high availability (HA) to Version 6.6.0.1, the device enters Suspended mode after the post-upgrade reboot. You must manually resume HA.

FMC deployments are not affected.

To upgrade an FDM-managed FTD HA pair to Version 6.6.0.1:

1. Upgrade the standby device.
2. When the upgrade completes and the device reboots, manually resume HA. You can use FDM or the CLI:
  - FDM: Click **Device** > **High Availability**, then select **Resume HA** from the gear menu (⚙️).
  - CLI: **configure high-availability resume**

The HA status of the freshly upgraded device should return to normal, as the standby unit, after the unit negotiates with the peer.

3. Switch the active and standby peers (force failover) so the freshly upgraded device is now the active peer.
4. Repeat this procedure for the new standby peer.

For more information on configuring and managing high availability with FDM, see the [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#).

## 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: 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 5: 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: <ul style="list-style-type: none"> <li>• <b>From</b> c3.xlarge <b>to</b> c3.4xlarge.</li> <li>• <b>From</b> c3.2.xlarge <b>to</b> c3.4xlarge.</li> <li>• <b>From</b> c4.xlarge <b>to</b> c4.4xlarge.</li> <li>• <b>From</b> c4.2xlarge <b>to</b> c4.4xlarge.</li> </ul> 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.

Platform	Pre-Upgrade Action	Details
Azure	Resize instances: <ul style="list-style-type: none"> <li>• <b>From</b> Standard_D3_v2 to Standard_D4_v2.</li> </ul>	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 Upgrade with FDM

**Deployments:** FTD with FDM

**Upgrading from:** Version 6.2.3 through 6.4.0.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+

Talos Intelligence Group 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 6: Deployment Changes on Upgrade**

Change	Details
Modifies URL rule categories.	<p>The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies:</p> <ul style="list-style-type: none"> <li>• Access control</li> <li>• SSL</li> <li>• QoS (FMC only)</li> <li>• Correlation (FMC only)</li> </ul> <p>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.</p>
Renames URL rule reputations.	<p>The upgrade modifies URL rules to use the new reputation names:</p> <ol style="list-style-type: none"> <li>1. Untrusted (was <i>High Risk</i>)</li> <li>2. Questionable (was <i>Suspicious sites</i>)</li> <li>3. Neutral (was <i>Benign sites with security risks</i>)</li> <li>4. Favorable (was <i>Benign sites</i>)</li> <li>5. Trusted (was <i>Well Known</i>)</li> </ol>
Clears the URL cache.	<p>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.</p>
Labels 'legacy' events.	<p>For already-logged events, the upgrade labels any associated URL category and reputation information as <code>Legacy</code>. These legacy events will age out of the database over time.</p>

## Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 7: Pre-Upgrade Actions

Action	Details
<p>Make sure your appliances can reach Talos resources.</p>	<p>The system must be able to communicate with the following Cisco resources after the upgrade:</p> <ul style="list-style-type: none"> <li>• <a href="https://regsvc.sco.cisco.com/">https://regsvc.sco.cisco.com/</a> — Registration</li> <li>• <a href="https://est.sco.cisco.com/">https://est.sco.cisco.com/</a> — Obtain certificates for secure communications</li> <li>• <a href="https://updates-talos.sco.cisco.com/">https://updates-talos.sco.cisco.com/</a> — Obtain client/server manifests</li> <li>• <a href="http://updates.ironport.com/">http://updates.ironport.com/</a> — Download database (note: uses port 80)</li> <li>• <a href="https://v3.sds.cisco.com/">https://v3.sds.cisco.com/</a> — Cloud queries</li> </ul> <p>The cloud query service also uses the following IP address blocks:</p> <ul style="list-style-type: none"> <li>• IPv4 cloud queries: <ul style="list-style-type: none"> <li>• 146.112.62.0/24</li> <li>• 146.112.63.0/24</li> <li>• 146.112.255.0/24</li> <li>• 146.112.59.0/24</li> </ul> </li> <li>• IPv6 cloud queries: <ul style="list-style-type: none"> <li>• 2a04:e4c7:fff::/48</li> <li>• 2a04:e4c7:ffe::/48</li> </ul> </li> </ul>
<p>Identify potential rule issues.</p>	<p>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).</p> <p><b>Note</b> You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade.</p> <p>In FMC deployments, we recommend you generate an <i>access control policy report</i>, 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 <b>Policies &gt; Access Control</b>, then click the report icon () next to the appropriate policy.</p>

## 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 8: Post-Upgrade Actions**

Action	Details
Remove <b>deprecated categories</b> from rules. Required.	<p>The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy.</p> <p>On the FMC, these rules are marked.</p>
Create or modify rules to include the <b>new categories</b> .	<p>Most of the new categories identify threats. We strongly recommend you use them.</p> <p>On the FMC, these new categories are not marked after <i>this</i> upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.</p>
Evaluate rules changed as a result of <b>merged categories</b> .	<p>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 <a href="#">Guidelines for Rules with Merged URL Categories, on page 11</a>.</p> <p>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.</p>
Evaluate rules changed as a result of <b>split categories</b> .	<p>The upgrade replaces each old, single category in URL rules with <i>all</i> 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.</p> <p>These changes are not marked.</p>
Understand which categories were <b>renamed</b> or are <b>unchanged</b> .	<p>Although no action is required, you should be aware of these changes.</p> <p>These changes are not marked.</p>
Evaluate how you handle <b>uncategorized</b> and <b>reputationless</b> URLs.	<p>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.</p> <p>Make sure that rules that filter by the <b>Uncategorized</b> category, or by <b>Any</b> reputation, will behave as you expect.</p>

## 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 9: 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	<p>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.</p> <p>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.</p>
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 <b>Any reputation</b> and Category B was associated in the same rule with reputation level <b>3 - Benign sites with security risks</b> , then after merge Category AB in that rule will be associated with <b>Any reputation</b> .
Duplicate and Redundant Categories and Rules	<p>After merge, different rules may have the same category associated with different actions and reputation levels.</p> <p>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.</p> <p>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.</p> <p>Caution: Consider all conditions in the rule when determining how to resolve duplicate or redundant categories.</p>
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 10: 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.

## 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.

## Renamed Upgrade and Installation Packages

**Deployments:** FMC, 7000/8000 series, NGIPSv

**Upgrading from:** Version 6.1.0 through 6.2.3.x

**Directly to:** Version 6.3+

The naming scheme (that is, the first part of the name) for upgrade, patch, hotfix, and installation packages changed starting with Version 6.3.0, on select platforms.



**Note** This change causes issues with reimaging older *physical* appliances: DC750, 1500, 2000, 3500, and 4000, as well as 7000/8000 series devices and AMP models. If you are currently running Version 5.x and need to freshly install Version 6.3.0 or 6.4.0 on one of these appliances, rename the installation package to the "old" name after you download it from the Cisco Support & Download site. You cannot reimage these appliances to Version 6.5+.

**Table 11: Naming Schemes: Upgrade, Patch, and Hotfix Packages**

Platform	Naming Schemes
FMC	<b>New:</b> Cisco_Firepower_Mgmt_Center <b>Old:</b> Sourcefire_3D_Defense_Center_S3
NGIPSv	<b>New:</b> Cisco_Firepower_NGIPS_Virtual <b>Old:</b> Sourcefire_3D_Device_VMware <b>Old:</b> Sourcefire_3D_Device_Virtual64_VMware

Table 12: Naming Schemes: Installation Packages

Platform	Naming Schemes
FMC (physical)	<b>New:</b> Cisco_Firepower_Mgmt_Center <b>Old:</b> Sourcefire_Defense_Center_M4 <b>Old:</b> Sourcefire_Defense_Center_S3
FMCv: VMware	<b>New:</b> Cisco_Firepower_Mgmt_Center_Virtual_VMware <b>Old:</b> Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	<b>New:</b> Cisco_Firepower_Mgmt_Center_Virtual_KVM <b>Old:</b> Cisco_Firepower_Management_Center_Virtual
Firepower 7000/8000 series	<b>New:</b> Cisco_Firepower_NGIPS_Appliance <b>Old:</b> Sourcefire_3D_Device_S3
NGIPSv	<b>New:</b> Cisco_Firepower_NGIPSv_VMware <b>Old:</b> Cisco_Firepower_NGIPS_VMware

## 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 13: 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.

## Upgrade Guidelines for FXOS

For the Firepower 4100/9300, major FTD upgrades also require an FXOS upgrade.

Major FTD versions have a specially qualified and recommended companion FXOS version. Use these combinations whenever possible because we perform enhanced testing for them. Maintenance release and patches rarely require FXOS upgrades, but you may still want to upgrade to the latest FXOS build to take advantage of resolved issues.

We also recommend the latest firmware; see the [Cisco Firepower 4100/9300 FXOS Firmware Upgrade Guide](#).

For critical and release-specific upgrade guidelines, new and deprecated features, and open and resolved bugs, see the [Cisco Firepower 4100/9300 FXOS Release Notes](#).

### Minimum FXOS Version to Upgrade FTD

The minimum FXOS version to run Version 6.6 is FXOS 2.8.1.15.

### Minimum FXOS Version to Upgrade FXOS

You can upgrade to any later FXOS version from as far back as FXOS 2.2.2.

### Time to Upgrade FXOS

An FXOS upgrade can take up to 45 minutes and can affect traffic flow and inspection. For more information, see [Traffic Flow and Inspection for FXOS Upgrades, on page 20](#).

## 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. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

## Uninstall a Patch

In FMC and ASDM deployments, you can uninstall most patches. If you need to return to an earlier major or maintenance release, you must reimage. For guidelines, limitations, and procedures, see [Uninstall a Patch](#) in the FMC upgrade guide or [Uninstall ASA FirePOWER Patches with ASDM, on page 18](#) in these release notes.

## Uninstall ASA FirePOWER Patches with ASDM

Use the Linux shell (*expert mode*) to uninstall device patches. You must have access to the device shell as the `admin` user for the device, or as another local user with CLI configuration access. If you disabled shell access, contact Cisco TAC to reverse the lockdown.

For ASA failover pairs and clusters, minimize disruption by uninstalling from one appliance at a time. Wait until the patch has fully uninstalled from one unit before you move on to the next.

**Table 14: Uninstall Order for ASA with FirePOWER Services in ASA Failover Pairs/Clusters**

Configuration	Uninstall Order
ASA active/standby failover pair, with ASA FirePOWER	<p>Always uninstall from the standby.</p> <ol style="list-style-type: none"> <li>1. Uninstall from the ASA FirePOWER module on the standby ASA device.</li> <li>2. Fail over.</li> <li>3. Uninstall from the ASA FirePOWER module on the new standby ASA device.</li> </ol>
ASA active/active failover pair, with ASA FirePOWER	<p>Make both failover groups active on the unit you are not uninstalling.</p> <ol style="list-style-type: none"> <li>1. Make both failover groups active on the primary ASA device.</li> <li>2. Uninstall from the ASA FirePOWER module on the secondary ASA device.</li> <li>3. Make both failover groups active on the secondary ASA device.</li> <li>4. Uninstall from the ASA FirePOWER module on the primary ASA device.</li> </ol>

Configuration	Uninstall Order
ASA cluster, with ASA FirePOWER	<p>Disable clustering on each unit before you uninstall. Uninstall from one unit at a time, leaving the control unit for last.</p> <ol style="list-style-type: none"> <li>1. On a data unit, disable clustering.</li> <li>2. Uninstall from the ASA FirePOWER module on that unit.</li> <li>3. Reenable clustering. Wait for the unit to rejoin the cluster.</li> <li>4. Repeat for each data unit.</li> <li>5. On the control unit, disable clustering. Wait for a new control unit to take over.</li> <li>6. Uninstall from the ASA FirePOWER module on the former control unit.</li> <li>7. Reenable clustering.</li> </ol>

**Caution**

Do not make or deploy configuration changes during uninstall. Even if the system appears inactive, do not manually reboot, shut down, or restart an uninstall in progress. You could place the system in an unusable state and require a reimage. If you encounter issues with the uninstall, including a failed uninstall or unresponsive appliance, contact Cisco TAC.

**Before you begin**

- In ASA failover/cluster deployments, make sure you are uninstalling from the correct device.
- Make sure your deployment is healthy and successfully communicating.

**Step 1**

If the device's configurations are out of date, deploy now from ASDM.

Deploying before you uninstall reduces the chance of failure. Make sure the deployment and other essential tasks are completed. Tasks running when the uninstall begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

**Step 2**

Access the Firepower CLI on the ASA FirePOWER module. Log in as `admin` or another Firepower CLI user with configuration access.

You can either SSH to the module's management interface (hostname or IP address) or use the console. Note that the console port defaults to the ASA CLI and you must use the `session sfr` command to access the Firepower CLI.

**Step 3**

Use the `expert` command to access the Linux shell.

**Step 4**

Verify the uninstall package is in the upgrade directory.

```
ls /var/sf/updates
```

Patch uninstallers are named like upgrade packages, but have `Patch_Uninstaller` instead of `Patch` in the file name. When you patch a device, the uninstaller for that patch is automatically created in the upgrade directory. If the uninstaller is not there, contact Cisco TAC.

**Step 5** Run the uninstall command, entering your password when prompted.

```
sudo install_update.pl --detach /var/sf/updates/uninstaller_name
```

**Caution** The system does *not* ask you to confirm. Entering this command starts the uninstall, which includes a device reboot. Interruptions in traffic flow and inspection during an uninstall are the same as the interruptions that occur during an upgrade. Make sure you are ready. Note that using the `--detach` option ensures the uninstall process is not killed if your SSH session times out, which can leave the device in an unstable state.

**Step 6** Monitor the uninstall until you are logged out.

For a detached uninstall, use `tail` or `tailf` to display logs:

```
tail /ngfw/var/log/sf/update.status
```

Otherwise, monitor progress in the console or terminal.

**Step 7** Verify uninstall success.

After the uninstall completes, confirm that the module has the correct software version. Choose **Configuration > ASA FirePOWER Configurations > Device Management > Device**.

**Step 8** Redeploy configurations.

---

### What to do next

In ASA failover/cluster deployments, repeat this procedure for each unit in your planned sequence.

## Traffic Flow and Inspection

Device upgrades (software and operating system) affect traffic flow and inspection. Schedule maintenance windows when this will have the least impact.

### Traffic Flow and Inspection for FXOS Upgrades

Upgrading FXOS reboots the chassis. Even in high availability/scalability deployments, you upgrade FXOS on each chassis independently. To minimize disruption, upgrade one chassis at a time.

**Table 15: Traffic Flow and Inspection: FXOS Upgrades**

FTD Deployment	Traffic Behavior	Method
Standalone	Dropped.	—
High availability	Unaffected.	<b>Best Practice:</b> Update FXOS on the standby, switch active peers, upgrade the new standby.
	Dropped until one peer is online.	Upgrade FXOS on the active peer before the standby is finished upgrading.

FTD Deployment	Traffic Behavior	Method
Inter-chassis cluster	Unaffected.	<b>Best Practice:</b> Upgrade one chassis at a time so at least one module is always online.
	Dropped until at least one module is online.	Upgrade chassis at the same time, so all modules are down at some point.
Intra-chassis cluster (Firepower 9300 only)	Passed without inspection.	Hardware bypass enabled: <b>Bypass: Standby or Bypass-Force.</b>
	Dropped until at least one module is online.	Hardware bypass disabled: <b>Bypass: Disabled.</b>
	Dropped until at least one module is online.	No hardware bypass module.

## Traffic Flow and Inspection for FTD Upgrades with FMC

### 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 16: Traffic Flow and Inspection: Software Upgrades for Standalone Devices*

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

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: <b>Bypass: Force</b>	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: <b>Bypass: Standby</b>	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: <b>Bypass: Disabled</b>	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

### Software Upgrades for High Availability/Scalability

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

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

### Software Uninstall (Patches)

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

### Deploying Configuration Changes

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

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

Table 17: Traffic Flow and Inspection: Deploying Configuration Changes

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

## Traffic Flow and Inspection for FTD Upgrades with FDM

### Software Upgrades

Traffic is dropped while you upgrade. In a high availability deployment, you can minimize disruption by upgrading devices one at a time.

For the ISA 3000 only, if you configured hardware bypass for power failure, traffic is dropped during the upgrade but is passed without inspection while the device completes its post-upgrade reboot.

### Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection on all devices, including those configured for high availability. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

## Traffic Flow and Inspection for ASA FirePOWER Upgrades

### Software Upgrades

Your ASA service policies for redirecting traffic to the ASA FirePOWER module determine how the module handles traffic during software upgrade.

*Table 18: Traffic Flow and Inspection: ASA FirePOWER Upgrades*

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

### Software Uninstall (Patches)

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

### Deploying Configuration Changes

Restarting the Snort process briefly interrupts traffic flow and inspection. Traffic behavior while the Snort process restarts is the same as when you upgrade ASA FirePOWER. When you deploy without restarting Snort, resource demands may result in a small number of packets dropping without inspection.

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

## Traffic Flow and Inspection for NGIPSv Upgrades with FMC

### Software Upgrades

Interface configurations determine how NGIPSv handles traffic during the upgrade.

*Table 19: Traffic Flow and Inspection: NGIPSv Upgrades*

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

### Software Uninstall (Patches)

Interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade.

### Deploying Configuration Changes

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

Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations.

**Table 20: Traffic Flow and Inspection: Deploying Configuration Changes**

Interface Configuration	Traffic Behavior
Inline, <b>Failsafe</b> enabled or disabled	Passed without inspection. A few packets might drop if <b>Failsafe</b> 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 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, 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 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.
Virtual appliances	We test with the default settings for memory and resources. However, note that upgrade time in virtual deployments is highly hardware dependent.

Condition	Details
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 <i>only</i> . 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 <b>System &gt; Monitoring &gt; Statistics</b> and select the FMC. Under Disk Usage, expand the By Partition details.
FTD with FMC	Choose <b>System &gt; Monitoring &gt; Statistics</b> and select the device you want to check. Under Disk Usage, expand the By Partition details.
FTD with FDM	Use the <b>show disk</b> CLI command.

## Time and Disk Space for Version 6.6.7.1

Table 23: Time and Disk Space for Version 6.6.7.1

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.8 GB in /var	20 MB in /	—	37 min	9 min
FMCv: VMware	3.4 GB in /var	23 MB in /	—	35 min	7 min
Firepower 1000 series	—	3.8 GB in /ngfw	870 MB	9 min	7 min
Firepower 2100 series	—	2.9 GB in /ngfw	900 MB	7 min	13 min
Firepower 4100 series	—	3.1 GB in /ngfw	680 MB	6 min	8 min
Firepower 4100 series container instance	—	2.3 GB in /ngfw	680 MB	6 min	5 min
Firepower 9300	—	3.2 GB in /ngfw	680 MB	5 min	10 min
ASA 5500-X series with FTD	3.1 GB in /home	120 MB in /ngfw	630 MB	10 min	16 min
FTDv: VMware	2.5 GB in /home	120 MB in /ngfw	630 MB	7 min	6 min
ASA FirePOWER	2.9 GB in /var	21 MB in /	430 MB	22 min	6 min
NGIPSv	940 MB in /var	19 MB in /	290 MB	6 min	6 min

## Time and Disk Space for Version 6.6.7

Table 24: Time and Disk Space for Version 6.6.7

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	17.0 GB in /var	23 MB in /	—	49 min	14 min
FMCv: VMware	20.1 GB in /var	29 MB in /	—	48 min	7 min
Firepower 1000 series	—	10.4 GB in /ngfw	1.0 GB	19 min	18 min
Firepower 2100 series	—	10.3 GB in /ngfw	1.0 GB	17 min	15 min
Firepower 4100 series	—	10.1 GB in /ngfw	970 MB	10 min	11 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 4100 series container instance	—	10.4 GB in /ngfw	970 MB	10 min	8 min
Firepower 9300	—	10.2 GB in /ngfw	970 MB	14 min	10 min
ASA 5500-X series with FTD	8.6 GB in /home	752 KB in /ngfw	1.2 GB	22 min	22 min
FTDv: VMware	9.3 GB in /home	752 KB in /ngfw	1.2 GB	13 min	20 min
ASA FirePOWER	12 GB in /var	26 MB in /	1.3 GB	73 min	16 min
NGIPSv	7.4 GB in /var	21 MB in /	870 MB	12 min	7 min

## Time and Disk Space for Version 6.6.5.2

Table 25: Time and Disk Space for Version 6.6.5.2

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.8 GB in /var	20 MB in /	—	39 min	8 min
FMCv: VMware	3.4 GB in /var	23 MB in /	—	26 min	8 min
Firepower 1000 series	—	3.0 GB in /ngfw	630 MB	8 min	12 min
Firepower 2100 series	—	2.9 GB in /ngfw	660 MB	7 min	12 min
Firepower 9300	—	2.4 GB in /ngfw	430 MB	5 min	8 min
Firepower 4100 series	—	2.9 GB in /ngfw	430 MB	6 min	8 min
Firepower 4100 series container instance	—	2.5 GB in /ngfw	430 MB	5 min	6 min
ASA 5500-X series with FTD	2.2 GB in /home	120 MB in /ngfw	380 MB	10 min	15 min
FTDv: VMware	1.8 GB in /home	120 MB in /ngfw	380 MB	5 min	6 min
ASA FirePOWER	2.9 GB in /var	21 MB in /	450 MB	68 min	22 min
NGIPSv	920 MB in /var	19 MB in /	310 MB	6 min	5 min

## Time and Disk Space for Version 6.6.5.1

Table 26: Time and Disk Space for Version 6.6.5.1

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2.2 GB in /var	20 MB in /	—	34 min	8 min
FMCv: VMware	2.2 GB in /var	23 MB	—	28 min	6 min
Firepower 1000 series	—	1.5 GB in /ngfw	340 MB	8 min	12 min
Firepower 2100 series	—	1.4 GB in /ngfw	370 MB	6 min	11 min
Firepower 9300	—	770 MB in /ngfw	140 MB	5 min	8 min
Firepower 4100 series	—	790 MB in /ngfw	140 MB	5 min	8 min
Firepower 4100 series container instance	—	730 MB in /ngfw	140 MB	6 min	5 min
ASA 5500-X series with FTD	590 MB in /home	120 MB in /ngfw	85 MB	9 min	9 min
FTDv: VMware	590 MB in /home	120 MB in /ngfw	85 MB	6 min	5 min
ASA FirePOWER	1.7 GB in /var	21 MB in /	130 MB	69 min	7 min
NGIPSv	78 MB in /var	19 MB in /	16 MB	6 min	5 min

## Time and Disk Space for Version 6.6.5

Table 27: Time and Disk Space for Version 6.6.5

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	16.5 GB in /var	23 MB in /	—	55 min	14 min
FMCv: VMware	21 GB in /var	29 MB in /	—	51 min	9 min
Firepower 1000 series	9.7 GB in /ngfw/var	400 MB in /ngfw	1.1 GB	20 min	16 min
Firepower 2100 series	10.2 GB in /ngfw/var	450 MB in /ngfw	1.1 GB	17 min	15 min
Firepower 9300	10.2 GB 11 in /ngfw/var	MB in /ngfw	1.1 GB	12 min	10 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 4100 series	10.1 MB in /ngfw/var	10 MB in /ngfw	1.1 GB	10 min	11 min
Firepower 4100 series container instance	10.7 GB in /ngfw/var	11 MB in /ngfw	1.1 GB	12 min	7 min
ASA 5500-X series with FTD	8.6 GB in /ngfw/var	756 KB in /ngfw	1.3 GB	22 min	30 min
FTDv: VMware	9.1 GB in /ngfw/var	756 KB in /ngfw	1.3 GB	12 min	21 min
ASA FirePOWER	12 GB in /var	26 MB in /	1.4 GB	65 min	25 min
NGIPSv	7.4 GB 21 in /var	MB in /	910 MB	12 min	21 min

## Time and Disk Space for Version 6.6.4

Table 28: Time and Disk Space for Version 6.6.4

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	15.1 GB in /var	23 MB in /	—	60 min	28 min
FMCv: VMware	23.7 GB in /var	29 MB in /	—	43 min	8 min
Firepower 1000 series	9.7 GB in /ngfw/var	400 MB in /ngfw	1 GB	21 min	16 min
Firepower 2100 series	10.1 GB in /ngfw/var	450 MB in /ngfw	1 GB	21 min	13 min
Firepower 9300	10.1 GB in /ngfw/var	11 MB in /ngfw	970 MB	14 min	10 min
Firepower 4100 series	8.9 GB in /ngfw/var	11 MB in /ngfw	970 MB	11 min	9 min
Firepower 4100 series container instance	10.9 GB in /ngfw/var	10 MB in /ngfw	970 MB	10 min	7 min
ASA 5500-X series with FTD	8.5 GB in /ngfw/var	756 KB in /ngfw	1.2 GB	20 min	19 min
FTDv: VMware	7.7 GB in /ngfw/var	756 KB in /ngfw	1.2 GB	19 min	12 min
ASA FirePOWER	11.4 GB in /var	26 MB in /	1.3 GB	59 min	16 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
NGIPsv	7.4 GB in /var	21 MB in /	870 MB	13 min	8 min

## Time and Disk Space for Version 6.6.3

Table 29: Time and Disk Space for Version 6.6.3

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	15.1 GB in /var	23 MB in /	—	60 min	28 min
FMCv: VMware	23.7 GB in /var	29 MB in /	—	43 min	8 min
Firepower 1000 series	9.7 GB in /ngfw/var	400 MB in /ngfw	1 GB	21 min	16 min
Firepower 2100 series	10.1 GB in /ngfw/var	450 MB in /ngfw	1 GB	21 min	13 min
Firepower 4100 series	8.9 GB in /ngfw/var	11 MB in /ngfw	970 MB	11 min	9 min
Firepower 4100 series container instance	10.9 GB in /ngfw/var	10 MB in /ngfw	970 MB	10 min	7 min
Firepower 9300	10.1 GB in /ngfw/var	11 MB in /ngfw	970 MB	14 min	10 min
ASA 5500-X series with FTD	8.5 GB in /ngfw/var	756 KB in /ngfw	1.2 GB	20 min	19 min
FTDv: VMware	7.7 GB in /ngfw/var	756 KB in /ngfw	1.2 GB	19 min	12 min
ASA FirePOWER	11.4 GB in /var	26 MB in /	1.3 GB	59 min	16 min
NGIPsv	7.4 GB in /var	21 MB in /	870 MB	13 min	8 min

## Time and Disk Space for Version 6.6.1

Table 30: Time and Disk Space for Version 6.6.1

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	18.6 GB	23 MB	—	54 min	14 min
FMCv: VMware	15.8 GB	58 MB	—	56 min	13 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 1000 series	10.8 GB	400 MB	1.1 GB	20 min	17 min
Firepower 2100 series	10.9 GB	450 MB	1.1 GB	16 min	21 min
Firepower 4100 series	9.7 GB	10 MB	1 GB	15 min	14 min
Firepower 4100 series container instance	11.2 GB	9 MB	1 GB	10 min	13 min
Firepower 9300	9.8 GB	11 MB	1 GB	15 min	15 min
ASA 5500-X series with FTD	9.3 GB	1 MB	1.2 GB	21 min	24 min
FTDv: VMware	9.3 GB	1 MB	1.2 GB	18 min	19 min
ASA FirePOWER	12.3 GB	26 MB	1.4 GB	72 min	23 min
NGIPSv	7.1 GB	54 MB	860 MB	14 min	20 min

## Time and Disk Space for Version 6.6.0.1

In this table, the upgrade time includes reboot.

**Table 31: Time and Disk Space for Version 6.6.0.1**

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade + Reboot Time
FMC	31 MB	20 MB	—	22 min
FMCv: VMware	1.1 GB	23 MB	—	17 min
Firepower 1000 series	450 MB	450 MB	240 MB	21 min
Firepower 2100 series	260 MB	260 MB	270 MB	17 min
Firepower 4100 series	470 MB	470 MB	46 MB	11 min
Firepower 9300	460 MB	460 MB	46 MB	33 min
ASA 5500-X series with FTD	440 MB	120 MB	46 MB	17 min
ISA 3000 with FTD	440 MB	120 MB	46 MB	21 min

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade + Reboot Time
FTDv: VMware	430 MB	120 MB	46 MB	11 min
ASA FirePOWER	80 MB	20 MB	15 MB	18 min
NGIPSv	64 MB	28 MB	15 MB	9 min

## Time and Disk Space for Version 6.6.0



**Note** For ASA 5545-X with FirePOWER Services, if the SRU on the device is the *same as* or *newer than* the SRU in the Version 6.6.0 upgrade package (2020-01-16-001-vrt), the upgrade can take longer than expected—more than an hour longer. To determine if this will affect you, log into the Firepower CLI on the device and use the **show version** command to display the **Rules update version**.

**Table 32: Time and Disk Space for Version 6.6.0**

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	16.5 GB in /var	71 MB in /	—	46 min	15 min
FMCv: VMware	16.7 GB in /var	57 MB in /	—	36 min	7 min
Firepower 1000 series	410 MB in /ngfw/var	11.5 GB in /ngfw	1.1 GB	20 min	17 min
Firepower 2100 series	470 MB in /ngfw/var	10.3 GB in /ngfw	1 GB	14 min	14 min
Firepower 4100 series	61 MB in /ngfw/var	9.3 GB in /ngfw	980 MB	11 min	9 min
Firepower 4100 series container instance	46 MB in /ngfw/var	11.3 GB in /ngfw	980 MB	11 min	6 min
Firepower 9300	64 MB in /ngfw/var	8.7 GB in /ngfw	980 MB	15 min	12 min
ASA 5500-X series with FTD	8.7 GB in /ngfw/var	70 KB in /ngfw	1.2 GB	23 min	26 min
FTDv: VMware	8.7 GB in /ngfw/var	70 KB in /ngfw	1.2 GB	14 min	17 min
ASA FirePOWER	11.4 GB in /var	63 MB in /	1.4 GB	93 min	10 min
NGIPSv	6.1 GB in /var	53 MB in /	860 MB	10 min	5 min

