CONTENTS

CHAPTER 1 Getting Started 1
Using This Guide 1
Upgrade Checklists 2
Freshly Install Firepower Software 2

PART I Prepare to Upgrade 5

CHAPTER 2 Assess Your Deployment 7
Deployment Assessment Questions 7
Find Current Version Information 7

CHAPTER 3 Plan Your Upgrade Path 9
About Upgrade Paths: Can I Upgrade? 9
Is Direct Upgrade Possible? 10
Can I Maintain FMC-Device Version Compatibility? 10
Where Do I Begin? 11
Major Upgrades vs Patches 12
Identify Preinstallation Packages 13
Identify When to Add New Devices 14
Identify Interruptions in Traffic Flow and Inspection 15
Identify Other Major Tasks 15

CHAPTER 4 Obtain Upgrade Packages 17
About Upgrade Packages 17
Guidelines and Limitations for Managing Upgrade Packages 19
Downloading Upgrade Packages 19
Download Patches Directly from Cisco
Upload Upgrade Packages to the FMC
Get FTD Upgrade Packages from an Internal Server
Push Upgrade Packages to Managed Devices

Run Readiness Checks
Guidelines and Limitations for Readiness Checks
Run the Readiness Check

Other Pre-Upgrade Actions and Checks
Verify Appliance Communication and Health
Review Release Notes
Plan Configuration Changes
Check Time and Disk Space
Appliance Access During Upgrade
Check Bandwidth
Back Up Configurations and Event Data
Verify NTP Synchronization
Schedule Maintenance Windows

Upgrade Firepower Appliances

Upgrade Firepower Management Centers
Upgrade Checklist: Firepower Management Centers
Upgrade Path: Firepower Management Centers
Upgrade a Standalone FMC
Upgrade High Availability FMCs

Upgrade Firepower Threat Defense: Firepower 4100/9300
Upgrade Checklist: FTD on Firepower 4100/9300 Chassis
Upgrade Path: FTD on Firepower 4100/9300 Chassis
Upgrade FXOS: Firepower 4100/9300 Chassis
FXOS for Firepower 4100/9300 Chassis Upgrade Packages
Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster
Upgrade an Active/Active Failover Pair Using the CLI 94
Upgrade an Active/Active Failover Pair Using ASDM 97
Upgrade an ASA Cluster 98
Upgrade an ASA Cluster Using the CLI 98
Upgrade an ASA Cluster Using ASDM 103
Upgrade an ASA FirePOWER Module 106

PART III
Reference 109

CHAPTER 12
Compatibility 111
Firepower Management Centers 111
   About Firepower Management Centers 111
   Firepower Management Centers: Physical 112
   Firepower Management Centers: Virtual 113
   BIOS and Firmware for FMCs 114
Firepower Devices 115
   About Firepower Devices 115
   Firepower 1000/2100 Series with FTD 116
   Firepower 4100/9300 with FTD 116
   ASA 5500-X Series and ISA 3000 with FTD 118
   Firepower Threat Defense Virtual 119
   Firepower 7000/8000 Series and Legacy Devices 119
   ASA 5500-X Series and ISA 3000 with FirePOWER Services 120
   NGIPSv 121
Bundled Components 122

CHAPTER 13
Example Upgrade Paths 127
   Example: Upgrading High Availability FMCs 127
   Example: Upgrading Firepower 4100/9300 High Availability Pairs 128
   Example: Upgrading Firepower 4100/9300 Intra-Chassis Clusters 129
   Example: Upgrading Firepower 4100/9300 Inter-Chassis Clusters 130
   Example: Upgrading Other FTD Devices 131
   Example: Upgrading FMCv/NGIPSv Deployments 132
   Example: Upgrading ASA with FirePOWER Services 132
CHAPTER 14

Upgrade Guidelines and Warnings by Version  137

 Deprecated Features  137

 Deprecated FlexConfig Commands  145

 Multiversion Guidelines  147

 EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic  147

 Upgrade Failure: Insufficient Disk Space on Container Instances  147

 Patch/Hotfix for Dynamic Analysis CA Certificates  147

 Version 6.6.0 Guidelines  148

 FMCv Requires 28 GB RAM for Upgrade  150

 FTDv for VMware e1000 Interfaces Prevent Upgrade  151

 Events Temporarily Unavailable After FMC Upgrade  151

 Version 6.5.0 Guidelines  152

 Firepower 1000 Series Devices Require Post-Upgrade Power Cycle  153

 Disable Egress Optimization for Version 6.5.0  153

 Upgrade Assigns Deployment to North America Cisco Cloud  154

 Cisco Threat Intelligence Director (TID) Behavior Changes  154

 New URL Categories and Reputations  155

 Pre-Upgrade Actions for URL Categories and Reputations  156

 Post-Upgrade Actions for URL Categories and Reputations  157

 Guidelines for Rules with Merged URL Categories  158

 Version 6.4.0.x Guidelines  161

 Versions 6.4.0.1 and 6.4.0.2 Not Supported on Firepower 1000 Series  161

 Version 6.4.0 Guidelines  161

 Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12  163

 TLS Crypto Acceleration Enabled/Cannot Disable  163

 Firepower 4100/9300 Requires Version 6.2.0 for Upgrade  164

 Version 6.3.0.x Guidelines  164

 Version 6.3.0 Guidelines  164

 Renamed Upgrade and Installation Packages  166

 Reimaging to Version 6.3+ Disables LOM on Most Appliances  167

 Timeouts for the URL Filtering Cache Can Change  168

 Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv  168

 RA VPN Default Setting Change Can Block VPN Traffic  168
TLS/SSL Hardware Acceleration Enabled on Upgrade 169
Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER 169
Updated Security for Appliance Access 169
Security Intelligence Enables Application Identification 170
Update VDB after Upgrade to Enable CIP Detection 170
Invalid Intrusion Variable Sets Can Cause Deploy Failure 170
Syslog Behavior Changes for Connection and Intrusion Events 171
Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade 171
Version 6.2.3.x Guidelines 172
Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure 172
Version 6.2.3.3 FTD Device Cannot Switch to Local Management 173
Hotfix Before Upgrading Version 6.2.3-88 FMCs 173
Version 6.2.3 Guidelines 173
Sharing Data with Cisco 174
Edit/Resave Access Control Policies After Upgrade 174
Changes to Result Limits in Reports 174
Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade 175
Version 6.2.2.x Guidelines 175
Cannot Upgrade Firepower 2100 Series HA Pair from Version 6.2.2 to 6.2.2.4 176
Version 6.2.2 Guidelines 176
Security Enhancement: Signed Upgrade Packages 176
Version 6.2.2.1+ Required for 8000 Series Security Certs Compliance 177
Version 6.2.0.x Guidelines 177
Apply Hotfix BH to Version 6.2.0.3 FMCs 177
Version 6.2.0 Guidelines 177
Access Control Can Get Latency-Based Performance Settings from SRUs 178
'Snort Fail Open' Replaces 'Failsafe' on FTD 178
IAB 'All Applications' Option Removed on Upgrade 179
URL Filtering Sub-site Lookups for Low-Memory Devices Disabled on Upgrade 180
Version 6.1.0 Guidelines 180
Version 6.0.0 Guidelines 181

CHAPTER 15

Time Tests and Disk Space Requirements 185

About Time Tests 186
About Disk Space Requirements 187
Version 6.6.0 Time and Disk Space 188
Version 6.5.0.4 Time and Disk Space 188
Version 6.5.0.3 Time and Disk Space 189
Version 6.5.0.2 Time and Disk Space 189
Version 6.5.0.1 Time and Disk Space 190
Version 6.5.0 Time and Disk Space 190
Version 6.4.0.8 Time and Disk Space 190
Version 6.4.0.7 Time and Disk Space 191
Version 6.4.0.6 Time and Disk Space 191
Version 6.4.0.5 Time and Disk Space 192
Version 6.4.0.4 Time and Disk Space 192
Version 6.4.0.3 Time and Disk Space 193
Version 6.4.0.2 Time and Disk Space 193
Version 6.4.0.1 Time and Disk Space 194
Version 6.4.0 Time and Disk Space 194
Version 6.3.0.5 Time and Disk Space 195
Version 6.3.0.4 Time and Disk Space 195
Version 6.3.0.3 Time and Disk Space 196
Version 6.3.0.2 Time and Disk Space 197
Version 6.3.0.1 Time and Disk Space 197
Version 6.3.0 Time and Disk Space 198
Version 6.2.3.15 Time and Disk Space 198
Version 6.2.3.14 Time and Disk Space 199
Version 6.2.3.13 Time and Disk Space 199
Version 6.2.3.12 Time and Disk Space 200
Version 6.2.3.11 Time and Disk Space 200
Version 6.2.3.10 Time and Disk Space 201
Version 6.2.3.9 Time and Disk Space 201
Version 6.2.3.8 Time and Disk Space 202
Version 6.2.3.7 Time and Disk Space 202
Version 6.2.3.6 Time and Disk Space 202
Version 6.2.3.5 Time and Disk Space 203
Version 6.2.3.4 Time and Disk Space 203
Version 6.2.3.3 Time and Disk Space 204
Version 6.2.3.2 Time and Disk Space 204
Version 6.2.3.1 Time and Disk Space 205
Version 6.2.3 Time and Disk Space 206
Version 6.2.2.5 Time and Disk Space 207
Version 6.2.2.4 Time and Disk Space 207
Version 6.2.2.3 Time and Disk Space 208
Version 6.2.2.2 Time and Disk Space 209
Version 6.2.2.1 Time and Disk Space 209
Version 6.2.2 Time and Disk Space 210
Version 6.2.0.6 Time and Disk Space 210
Version 6.2.0.5 Time and Disk Space 211
Version 6.2.0.4 Time and Disk Space 211
Version 6.2.0.3 Time and Disk Space 212
Version 6.2.0.2 Time and Disk Space 213
Version 6.2.0.1 Time and Disk Space 213
Version 6.2.0 Time and Disk Space 214
Version 6.1.0.7 Time and Disk Space 214
Version 6.1.0.6 Time and Disk Space 215
Version 6.1.0.5 Time and Disk Space 215
Version 6.1.0.4 Time and Disk Space 216
Version 6.1.0.3 Time and Disk Space 216
Version 6.1.0.2 Time and Disk Space 217
Version 6.1.0.1 Time and Disk Space 217
Version 6.1.0 Time and Disk Space 218
Version 6.0.1.4 Time and Disk Space 218
Version 6.0.1.3 Time and Disk Space 219
Version 6.0.1.2 Time and Disk Space 219
Version 6.0.1.1 Time and Disk Space 220
Version 6.0.1 Time and Disk Space 220
Version 6.0.0.1 Time and Disk Space 221
Version 6.0 Time and Disk Space 221

CHAPTER 16
Traffic Flow, Inspection, and Device Behavior 223
FTD Upgrade Behavior: Firepower 4100/9300 Chassis  223
FTD Upgrade Behavior: Other Devices  226
Firepower 7000/8000 Series Upgrade Behavior  228
ASA FirePOWER Upgrade Behavior  230
NGIPSv Upgrade Behavior  230
Getting Started

Welcome to the Firepower Management Center upgrade guide. This guide explains how to prepare for and complete a successful upgrade of an FMC deployment where all appliances are running at least Firepower Version 5.4.0.2/5.4.1.1.

This guide does not contain upgrade information for locally managed (FDM/ASDM) devices. Instead, see the Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager or the Cisco ASA Upgrade Guide.

Upgrading an FMC deployment can be complex process. Careful planning and preparation can help you avoid missteps. You should consider planning and preparation as much a part of the upgrade process as actually performing the mechanical steps that invoke the upgrade scripts.

- Using This Guide, on page 1
- Upgrade Checklists, on page 2
- Freshly Install Firepower Software, on page 2

Using This Guide

This guide has three main parts:

- Prepare to Upgrade, on page 5: Deployment assessment, upgrade path planning, obtaining upgrade packages, and so on.

- Upgrade Firepower Appliances, on page 31: Describes the actual process of upgrading Firepower appliances, including operating system upgrades where necessary. Includes checklists (see the next topic) and upgrade paths.

- Reference, on page 109: Reference information that helps you plan and execute Firepower upgrades. If you are already familiar with the upgrade procedures, this allows you to quickly answer your most frequently asked questions.
# Upgrade Checklists

This guide provides upgrade checklists for Firepower platforms. These checklists walk you through the upgrade process, including planning and preparation. Complete the checklist every time you upgrade. Skipping steps can result in an unsuccessful upgrade.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Checklist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Management Center, including FMCv and FMCv 300.</td>
<td>Upgrade Checklist: Firepower Management Centers, on page 33</td>
</tr>
</tbody>
</table>
| Firepower Threat Defense:  
• Firepower 4100 series  
• Firepower 9300 | Upgrade Checklist: FTD on Firepower 4100/9300 Chassis, on page 41 |
| Firepower Threat Defense:  
• Firepower 1000 series  
• Firepower 2100 series  
• ASA 5500-X series  
• ISA 3000  
• Firepower Threat Defense Virtual | Upgrade Checklist: Other FTD Devices, on page 67 |
| NGIPS software:  
• Firepower 7000/8000 series  
• NGIPSv | Upgrade Checklist: Firepower 7000/8000 Series and NGIPSv, on page 73 |
| ASA with FirePOWER Services:  
• ASA 5500-X series  
• ISA 3000 | Upgrade Checklist: ASA with FirePOWER Services, on page 79 |

## Freshly Install Firepower Software

If you are unable to upgrade a Firepower appliance, or are disinclined to follow the required upgrade path, you can freshly install major Firepower releases. This is also called reimagining. To run a particular patch, install the major version, then upgrade.

If you think you might need to reimage, see the Cisco Firepower Release Notes for your version and review the fresh install chapter. Make sure you understand:

- Scenarios where you need to reimage.
• Important guidelines and limitations, including making backups, ensuring appliance access, addressing licensing concerns, and so on.

• Where to find installation instructions.
Freshly Install Firepower Software
Prepare to Upgrade

- Assess Your Deployment, on page 7
- Plan Your Upgrade Path, on page 9
- Obtain Upgrade Packages, on page 17
- Run Readiness Checks, on page 25
- Other Pre-Upgrade Actions and Checks, on page 27
Assess Your Deployment

Before you upgrade any Firepower appliance, determine the current state of your deployment. Understanding where you are determines how you get to where you want to go.

- Deployment Assessment Questions, on page 7
- Find Current Version Information, on page 7

Deployment Assessment Questions

- What appliances do you have, and what Firepower version are they running? What version do you want them to run, and can they run that version?
- Do any of your appliances require a separate operating system upgrade? Or, do you want to upgrade only the operating system?
- Do you have virtual appliances that require a hosting environment upgrade? Or, do you want to upgrade only the hosting environment?
- Are you using a standalone Firepower Management Center, or do you have a pair of high availability Firepower Management Centers?
- Are your devices standalone, or do you have clusters, stacks, and high availability pairs of devices?
- Are your devices deployed passively, as an IPS, as a firewall?
- Are you replacing an appliance or adding a new one to your deployment?

Find Current Version Information

This table lists where you can find information on the currently running versions of the upgradeable components of your Firepower deployment.
### Table 1: Finding the Current Firepower Version

<table>
<thead>
<tr>
<th>Component</th>
<th>Platform</th>
<th>Version Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower software</td>
<td>Firepower Management Center</td>
<td>On the FMC, choose Help &gt; About.</td>
</tr>
<tr>
<td>Device managed by an FMC</td>
<td></td>
<td>On the FMC, choose Devices &gt; Device Management.</td>
</tr>
<tr>
<td>FXOS</td>
<td>Firepower 4100/9300 chassis</td>
<td>On the FXOS CLI, use the <code>show version</code> command.</td>
</tr>
<tr>
<td>ASA OS</td>
<td>ASA with FirePOWER Services</td>
<td>On the ASA CLI, use the <code>show version</code> command.</td>
</tr>
<tr>
<td>Virtual hosting environment</td>
<td>Firepower virtual appliance</td>
<td>See the documentation for your virtual hosting environment.</td>
</tr>
</tbody>
</table>
Plan Your Upgrade Path

Use these guidelines to help you build your upgrade path.

• About Upgrade Paths: Can I Upgrade?, on page 9
• Major Upgrades vs Patches, on page 12
• Identify Preinstallation Packages, on page 13
• Identify When to Add New Devices, on page 14
• Identify Interruptions in Traffic Flow and Inspection, on page 15
• Identify Other Major Tasks, on page 15

About Upgrade Paths: Can I Upgrade?

Your upgrade path is a detailed plan for what you will upgrade and when. In general, you upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first. If you have assessed your deployment—that is, you know what you have and what you want—you are ready to build your upgrade path.

Tip

Especially in larger deployments where you must alternate FMC and device upgrades, upgrade paths that require intermediate versions can be time consuming. To save time, you can reimage older devices instead of upgrading. First, remove the devices from the FMC. Then, upgrade the FMC, reimage the devices, and re-add them to the FMC.

Answer ‘Yes’ to Two Important Questions

You must answer ‘yes’ to both of these questions, every time you upgrade either an FMC or a device:

• Is Direct Upgrade Possible?, on page 10
• Can I Maintain FMC-Device Version Compatibility?, on page 10

If the answer to either question is 'no,' your upgrade path is invalid.
Is Direct Upgrade Possible?

If a direct upgrade from your current to your target version is not possible, your upgrade path must include either intermediate versions, or strategic reimaging. To patch Firepower, you must be running the base major version. You cannot upgrade directly to a patch from an previous major version.

For major upgrades, this table summarizes upgrade capabilities for Firepower Management Centers and their managed devices. Find your current major version in the first column, then read across to determine if a direct upgrade is possible to your target version. For upgrade paths for each appliance type see the upgrade chapters: Upgrade Firepower Appliances, on page 31.

Table 2: Firepower Direct Upgrade Support

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Target Version: Direct Upgrade Supported</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>to 6.6.0</td>
</tr>
<tr>
<td>from 6.5.0</td>
<td>Yes</td>
</tr>
<tr>
<td>6.4.0</td>
<td>Yes</td>
</tr>
<tr>
<td>6.3.0</td>
<td>Yes</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Yes</td>
</tr>
<tr>
<td>6.2.2</td>
<td>—</td>
</tr>
<tr>
<td>6.2.1</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0</td>
<td>—</td>
</tr>
<tr>
<td>6.0.1</td>
<td>—</td>
</tr>
<tr>
<td>6.0.0</td>
<td>—</td>
</tr>
<tr>
<td>5.4.x</td>
<td>—</td>
</tr>
</tbody>
</table>

* You must be running at least Version 5.4.0.2/5.4.1.1 to upgrade to Version 6.0.
† You cannot upgrade a Firepower 4100/9300 series device from Version 6.1 directly to Version 6.4. We recommend you use Version 6.2.3 as an intermediate version.

Can I Maintain FMC-Device Version Compatibility?

Before you upgrade the Firepower Management Center, make sure the upgraded FMC will be able to manage its current devices. If it will not be able to, upgrade the devices first. You cannot upgrade a device past the FMC’s own major version.

Note that you can patch a device without patching the FMC, and vice versa. However, we strongly recommend you upgrade both. This allows you to take advantage of new features and bug fixes.
This table lists major FMC versions, and the major versions of devices they can manage. Find your current major version in the first column, then read across to determine which devices you can manage.

### Table 3: FMC-Device Version Compatibility

<table>
<thead>
<tr>
<th>FMC Version</th>
<th>Device Version</th>
<th>6.6.0</th>
<th>6.5.0</th>
<th>6.4.0</th>
<th>6.3.0</th>
<th>6.2.3</th>
<th>6.2.2</th>
<th>6.2.1</th>
<th>6.2.0</th>
<th>6.1.0</th>
<th>6.0.1</th>
<th>6.0.0</th>
<th>5.4.1</th>
<th>5.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.5.0</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.0.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.0.0</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>5.4.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>5.4.0</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* A device must be running at least Version 5.4.0.2/5.4.1.1 to be managed by a Version 6.0, 6.0.1, or 6.1 FMC.

### Where Do I Begin?

If you are not sure how to start planning your upgrade path, refer to your deployment assessment and find your platforms in this table.

### Table 4: Beginning a Firepower Upgrade Based on Current Major Version

<table>
<thead>
<tr>
<th>FMC Version</th>
<th>Devices</th>
<th>First Upgrade</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.0</td>
<td>6.2.3 through 6.5.0</td>
<td>FMC → 6.6.0</td>
<td>A Version 6.6.0 FMC can manage devices back to Version 6.2.3.</td>
</tr>
</tbody>
</table>
## Major Upgrades vs Patches

Major upgrades are more complex and take more time than patches.

<table>
<thead>
<tr>
<th>FMC</th>
<th>Devices</th>
<th>First Upgrade</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.0</td>
<td>6.2.3 through 6.4.0</td>
<td>FMC → 6.5.0 or 6.6.0</td>
<td>These FMCs can manage devices back to Version 6.2.3.</td>
</tr>
<tr>
<td></td>
<td>6.1.0 through 6.2.2</td>
<td>Devices → 6.2.0 or 6.2.2 or 6.2.3 or 6.3.0 or 6.4.0</td>
<td>Upgrade devices to Version 6.2.3+ if you plan to upgrade the FMC to Version 6.6.0.</td>
</tr>
<tr>
<td>6.3.0</td>
<td>6.2.3 through 6.3.0</td>
<td>FMC → 6.4.0 or 6.5.0 or 6.6.0</td>
<td>These FMCs can manage devices back to Version 6.2.3.</td>
</tr>
<tr>
<td></td>
<td>6.1.0 through 6.2.2</td>
<td>Devices → 6.2.0 or 6.2.2 or 6.2.3 or 6.3.0</td>
<td>Upgrade devices to Version 6.2.3+ if you plan to upgrade the FMC to Version 6.6.0.</td>
</tr>
<tr>
<td>6.2.3</td>
<td>6.2.3</td>
<td>FMC → 6.3.0 or 6.4.0 or 6.5.0 or 6.6.0</td>
<td>These FMCs can manage devices back to Version 6.2.3.</td>
</tr>
<tr>
<td></td>
<td>6.1.0 through 6.2.2</td>
<td>Devices → 6.2.0 or 6.2.2 or 6.2.3</td>
<td>Upgrade devices to Version 6.2.3 if you plan to upgrade the FMC to 6.6.0.</td>
</tr>
<tr>
<td>6.2.2</td>
<td>6.1.0 through 6.2.2</td>
<td>FMC → 6.2.3 or 6.3.0 or 6.4.0</td>
<td>These FMCs can manage devices back to Version 6.1.0.</td>
</tr>
<tr>
<td>6.2.1</td>
<td>6.1.0 through 6.2.1</td>
<td>FMC → 6.2.2 or 6.2.3 or 6.3.0 or 6.4.0</td>
<td>These FMCs can manage devices back to Version 6.1.0.</td>
</tr>
<tr>
<td>6.2.0</td>
<td>6.1.0 through 6.2.0</td>
<td>FMC → 6.2.2 or 6.2.3 or 6.4.0</td>
<td>These FMCs can manage devices back to Version 6.1.0.</td>
</tr>
<tr>
<td>6.1.0</td>
<td>6.1.0</td>
<td>FMC → 6.2.0 or 6.2.3 or 6.3.0 or 6.4.0</td>
<td>These FMCs can manage devices back to Version 6.1.0.</td>
</tr>
<tr>
<td></td>
<td>5.4.0 through 6.0.1</td>
<td>Devices → 6.1.0</td>
<td>You must upgrade devices to Version 6.1.0 if you plan to upgrade the FMC past Version 6.1.0.</td>
</tr>
<tr>
<td>6.0.1</td>
<td>5.4.0 through 6.0.1</td>
<td>FMC → 6.1.0</td>
<td>A Version 6.1.0 FMC can manage devices back to Version 5.4.0.</td>
</tr>
<tr>
<td>6.0.0</td>
<td>5.4.0 through 6.0.0</td>
<td>FMC → 6.0.1</td>
<td>A Version 6.0.1 FMC can manage devices back to Version 5.4.0.</td>
</tr>
<tr>
<td>5.4.x</td>
<td>5.4.x</td>
<td>FMC → 6.0.0</td>
<td>A Version 6.0.0 FMC can manage Version 5.4.x devices.</td>
</tr>
</tbody>
</table>
Although we recommend you upgrade your entire deployment, you can patch a device without patching the FMC, and vice versa. Just keep in mind that you cannot fully take advantage of new features and bug fixes until you patch both.

**Table 5: Characteristics of Major Upgrades vs Patches**

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Major Upgrades</th>
<th>Patches</th>
</tr>
</thead>
<tbody>
<tr>
<td>New features and functionality</td>
<td>Include new features and functionality, and may entail large-scale changes to the product.</td>
<td>Contains a limited range of fixes. Minor feature and functionality updates only — often none at all.</td>
</tr>
<tr>
<td>Upgrade Requirements</td>
<td>You can always upgrade to the next major version. You do not have to be running the latest patch to upgrade. Often, you can skip major versions when upgrading. For details, refer to the supported upgrade path for your platform.</td>
<td>You can only patch within a major version sequence. For example:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Yes: 6.4.0 → 6.4.0.5</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• No: 6.2.3 → 6.4.0.5</td>
</tr>
<tr>
<td>OS upgrades</td>
<td>Likely to have companion operating system upgrades, for devices where you upgrade the OS separately.</td>
<td>Usually do not have companion operating system upgrades, although often you can patch the OS to resolve minor issues.</td>
</tr>
<tr>
<td>Freshly Installing</td>
<td>Can be freshly installed/restored. If you are unable to upgrade a Firepower appliance, or are disinclined to follow the required upgrade path, you can freshly install major Firepower releases.</td>
<td>Cannot be freshly installed. Cisco does not provide installation packages for patches. To run a particular patch, install the major version, then apply the patch.</td>
</tr>
<tr>
<td>Uninstalling</td>
<td>Cannot be uninstalled. If you need to revert to an earlier version, you must freshly install.</td>
<td>Can be uninstalled. When you uninstall, either you:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Return to the previously released patch, regardless of where you upgraded from: Versions 5.4.x to 6.2.2.x.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Return to the previously installed patch, that is, the patch you actually upgraded from: Version 6.2.3+.</td>
</tr>
</tbody>
</table>

**Identify Preinstallation Packages**

For some upgrades on some platforms, we provide a preinstallation package or hotfix that optimizes the upgrade, enables specific upgrade functions, or fixes upgrade issues.

Preinstallation packages and hotfixes are available on the Cisco Support & Download site in the same location as the upgrade and installation packages. Just as with regular upgrade packages, use the System > Updates page on the FMC to run a preinstall or hotfix. We recommend you do this just before you upgrade.
## Identify When to Add New Devices

If your upgrade path includes adding a new device, when you add it depends on the device type:

- **Physical device**: Determine which Firepower version the device is currently running. Add the device as soon as you can, then use the Firepower Management Center to upgrade the new device with the rest of your deployment. Do not upgrade your FMC past the point where it can no longer manage the out-of-the-box device.

- **Virtual device**: Create after you upgrade the FMC to its target version. When you add a new virtual device, you should never have to perform a major upgrade, only patches.

### Table 6: Firepower Preinstallation Packages

<table>
<thead>
<tr>
<th>Target Version</th>
<th>Platforms</th>
<th>Severity</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1</td>
<td>FMC &amp; FMCv</td>
<td>Optional</td>
<td>Allows readiness checks for the Version 6.1 upgrade. After Version 6.1, the readiness check is included with upgrade packages. See: Firepower System Release Notes Version 6.1.0 Preinstallation Package</td>
</tr>
<tr>
<td></td>
<td>All devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1</td>
<td>FTD devices in HA pairs</td>
<td>Optional</td>
<td>Allows hitless upgrades of FTD HA pairs. Without the preinstall, you must break high availability before you upgrade to Version 6.1. See: Firepower System Release Notes Version 6.1.0 Preinstallation Package</td>
</tr>
<tr>
<td>6.0.1</td>
<td>FMC &amp; FMCv</td>
<td>Required</td>
<td>Optimizes the upgrade. See: Firepower System Release Notes Version 6.0.1 Preinstallation</td>
</tr>
<tr>
<td>6.0</td>
<td>FMC &amp; FMCv</td>
<td>Required from:</td>
<td>Optimizes the upgrade. Allows you to upgrade appliances in STIG mode. See: FireSIGHT System Release Notes Version 6.0.0 Preinstallation</td>
</tr>
<tr>
<td></td>
<td>All devices</td>
<td>• 5.4.0.2 through 5.4.0.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 5.4.1.1 through 5.4.1.5</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Recommended from:</td>
<td>• 5.4.0.7+</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• 5.4.1.6+</td>
</tr>
</tbody>
</table>
Identify Interruptions in Traffic Flow and Inspection

You must identify potential interruptions in traffic flow and inspection during the upgrade. This can occur:

- When a device is rebooted.
- When you upgrade the operating system or virtual hosting environment on a device.
- When you upgrade the Firepower software on a device, or uninstall a patch.
- When you deploy configuration changes as part of the upgrade or uninstall process (Snort process restarts).

Device type, deployment type (standalone, high availability, clustered), and interface configurations (passive, IPS, firewall, and so on) determine the nature of the interruptions. We strongly recommend performing any upgrade or uninstall in a maintenance window or at a time when any interruption will have the least impact on your deployment.

For more information, see Traffic Flow, Inspection, and Device Behavior, on page 223.

Identify Other Major Tasks

Many steps in the upgrade process can take a significant amount of time. You should explicitly include these steps in your plan. These can include, but are not limited to:

- Backups—Back Up Configurations and Event Data, on page 28
- Downloads and pushes—Obtain Upgrade Packages, on page 17
- Readiness checks—Run Readiness Checks, on page 25
- Pre- and post-upgrade configuration changes—Plan Configuration Changes, on page 27
Identify Other Major Tasks
Obtain Upgrade Packages

To upgrade a Firepower appliance, the upgrade package must be on the appliance. For more information, see:

- About Upgrade Packages, on page 17
- Guidelines and Limitations for Managing Upgrade Packages, on page 19
- Downloading Upgrade Packages, on page 19
- Upload Upgrade Packages to the FMC, on page 21
- Get FTD Upgrade Packages from an Internal Server, on page 22
- Push Upgrade Packages to Managed Devices, on page 23

About Upgrade Packages

To upgrade a Firepower appliance (or perform a readiness check), the upgrade package must be on the appliance.

In Version 6.5.0 and earlier, devices get their upgrade packages from the FMC. This means you must upload both FMC and device upgrade packages onto the FMC. Version 6.6.0 adds the ability to use your own internal web server instead of the FMC as the source for FTD upgrade packages. This means that FTD upgrade packages no longer have to 'go through' the FMC.

This table explains how to get upgrade packages onto the FMC.

**Table 7: Getting Upgrade Packages onto the FMC**

<table>
<thead>
<tr>
<th>Method</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual</td>
<td>Download from the Cisco Support &amp; Download site, then upload to the FMC.</td>
</tr>
<tr>
<td>Direct from Cisco</td>
<td>Use the FMC to get patches, hotfixes, and VDB updates directly from Cisco.</td>
</tr>
</tbody>
</table>

This table explains how to get upgrade packages onto managed devices.
### Table 8: Getting Upgrade Packages onto Managed Devices

<table>
<thead>
<tr>
<th>Method</th>
<th>Source</th>
<th>Details</th>
<th>Advantages</th>
<th>Supported Versions/Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy packages as part of upgrade. When you start a device upgrade, the system copies the upgrade package to the device as the first task.</td>
<td>FMC</td>
<td>Upload device upgrade packages to the FMC before you upgrade the devices. See the previous table.</td>
<td>—</td>
<td>Any. If your FMC is Version 6.2.2 or earlier, this is your only choice.</td>
</tr>
<tr>
<td>Copy (push) packages before upgrade.</td>
<td>FMC</td>
<td>Upload device upgrade packages to the FMC, but choose when to copy them to devices. See Push Upgrade Packages to Managed Devices, on page 23.</td>
<td>Reduces the length of your upgrade maintenance window.</td>
<td>Version 6.2.3 FMC</td>
</tr>
<tr>
<td>Internal web server</td>
<td>Internal web server</td>
<td>Upload device upgrade packages to an internal web server. Then, configure your FTD devices to get upgrade packages from the server instead of the FMC. See Get FTD Upgrade Packages from an Internal Server, on page 22.</td>
<td>Useful if you have limited bandwidth between the FMC and its devices. Saves space on the FMC.</td>
<td>Version 6.6.0+ FTD devices</td>
</tr>
<tr>
<td></td>
<td>Internal web server</td>
<td>Configure an internal web server instead of the FMC as the source for FTD upgrade packages, and choose when to copy the packages to devices. See Get FTD Upgrade Packages from an Internal Server, on page 22 and Push Upgrade Packages to Managed Devices, on page 23.</td>
<td>Reduces the length of your upgrade maintenance window. Useful if you have limited bandwidth between the FMC and its devices. Saves space on the FMC.</td>
<td>Version 6.6.0+ FTD devices</td>
</tr>
</tbody>
</table>
Guidelines and Limitations for Managing Upgrade Packages

The following guidelines and limitations apply to obtaining and managing upgrade packages.

**High Availability FMCs**

In a FMC high availability deployment, you must transfer upgrades packages to both the active/primary FMC and the standby/secondary FMC. Additionally, you must pause synchronization before you transfer the package to the standby FMC.

To limit interruptions to HA synchronization during the upgrade process, we recommend that you:

- Active FMC: Transfer the package during the preparation stage of the upgrade.
- Standby FMC: Transfer the package as part of the actual upgrade process, after you pause synchronization.

For more information, see Upgrade High Availability FMCs, on page 38.

**Push Firepower Upgrade Package Before FXOS Upgrade**

For Firepower 4100/9300 with FTD, best practice is to push the Firepower upgrade package before you begin the required companion FXOS upgrade.

*Note*

For upgrades from Version 6.1.0 directly to Version 6.3.0 or 6.4.0, a push from the FMC is required. You must push before you upgrade FXOS.

**Check Bandwidth**

Firepower upgrade package sizes vary. Make sure your management network has the bandwidth to perform large data transfers. For more information, see Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).

**Downloading Upgrade Packages**

Upgrade packages are available on the Cisco Support & Download site:

- Firepower Management Center, including FMCv: https://www.cisco.com/go/firepower-software
- Firepower Threat Defense (all other models, including FTDv): https://www.cisco.com/go/ftd-software
- Firepower 7000 series: https://www.cisco.com/go/7000series-software
- Firepower 8000 series: https://www.cisco.com/go/8000series-software
- NGIPSv: https://www.cisco.com/go/ngipsv-software
To find an upgrade package, select or search for your Firepower appliance model, then browse to the Firepower software download page for your current version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads.

You use the same upgrade package for all Firepower models in a family or series. Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and Firepower version. For example:

- **Package:** Cisco_Firepower_Mgmt_Center_Upgrade-6.5.0-120.sh.REL.tar
- **Platform:** Firepower Management Center
- **Package type:** Upgrade
- **Version and build:** 6.5.0-120
- **File extension:** sh.REL.tar

Upgrade packages from Version 6.2.1+ are signed tar archives (.tar). Do not untar. Do not transfer upgrade packages by email.

### Table 9: Upgrade Package Naming Schemes

<table>
<thead>
<tr>
<th>Platform</th>
<th>Versions</th>
<th>Platform Naming Scheme</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC/FMCv</td>
<td>6.3.0+</td>
<td>Cisco_Firepower_Mgmt_Center</td>
</tr>
<tr>
<td></td>
<td>5.4.0 to 6.2.3</td>
<td>Sourcefire_3D_Defense_Center_S3</td>
</tr>
<tr>
<td>Firepower 1000 series</td>
<td>Any</td>
<td>Cisco_FTD_SSP-FP1K</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>Any</td>
<td>Cisco_FTD_SSP-FP2K</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>Any</td>
<td>Cisco_FTD_SSP</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>Any</td>
<td>Cisco_FTD</td>
</tr>
<tr>
<td>ISA 3000 with FTD</td>
<td>Any</td>
<td>Cisco_FTD</td>
</tr>
<tr>
<td>FTDv</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower 7000/8000 series AMP models</td>
<td>6.3.0 to 6.4.0</td>
<td>Cisco_Firepower_NGIPS_Appliance</td>
</tr>
<tr>
<td></td>
<td>5.4.0 to 6.2.3</td>
<td>Sourcefire_3D_Device_S3</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>Any</td>
<td>Cisco_Network_Sensor</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>6.3.0+</td>
<td>Cisco_Firepower_NGIPS_Virtual</td>
</tr>
<tr>
<td></td>
<td>6.2.2 to 6.2.3</td>
<td>Sourcefire_3D_Device_VMware</td>
</tr>
<tr>
<td></td>
<td>5.4.0 to 6.2.0</td>
<td>Sourcefire_3D_Device_Virtual64_VMware</td>
</tr>
</tbody>
</table>

### Operating System Upgrade Packages

For information on operating system upgrade packages, see:
Download Patches Directly from Cisco

An FMC with internet access can get patches, hotfixes, and VDB updates directly from Cisco. Direct download is not supported for major upgrades or to managed devices. See Downloading Upgrade Packages, on page 19.

Before you begin

If you are using the standby FMC in a high availability pair, pause synchronization. See Guidelines and Limitations for Managing Upgrade Packages, on page 19.

Step 1
On the FMC web interface, choose System > Updates.

Step 2
Click Download Updates.

The number of upgrade packages retrieved, and therefore the time to retrieve them, depends on:

- How up-to-date your current deployment is: The FMC downloads a package for each patch and hotfix associated with the version your appliances are currently running, as well as the latest VDB if needed.
- How many different device types you have: The FMC downloads a different package for each device type. If your deployment includes multiple devices of the same type (for example, ten Firepower 2100 series devices), the FMC downloads a single package to upgrade them all.

What to do next

Refer to your plan. Optionally but recommended, copy upgrade packages to managed devices. See Push Upgrade Packages to Managed Devices, on page 23.

Upload Upgrade Packages to the FMC

Use the following procedure to manually upload upgrade packages to the FMC, for itself and the devices it manages.

Before you begin

- Download the appropriate upgrade package from the Cisco Support & Download site. See Downloading Upgrade Packages, on page 19.
- If you are using the standby FMC in a high availability pair, pause synchronization. See Guidelines and Limitations for Managing Upgrade Packages, on page 19.

Step 1
On the FMC web interface, choose System > Updates.
Step 2  Click Upload Update.
Step 3  (Version 6.6.0+) For the Action, click the Upload local software update package radio button.
Step 4  Click Choose File.
Step 5  Browse to the package and click Upload.

---

**What to do next**

Refer to your plan. Optionally but recommended, copy device upgrade packages to managed devices. See Push Upgrade Packages to Managed Devices, on page 23.

---

**Get FTD Upgrade Packages from an Internal Server**

Starting with Version 6.6.0, Firepower Threat Defense devices can get upgrade packages from an internal web server, rather than from the FMC. This is especially useful if you have limited bandwidth between the FMC and its devices. It also saves space on the FMC.

---

**Note**

This feature is supported only for FTD devices running Version 6.6.0+. It is not supported for upgrades to Version 6.6.0, nor is it supported for the FMC or Classic devices.

To configure this feature, you save a pointer (URL) to an upgrade package's location on the web server. The upgrade process will then get the upgrade package from the web server instead of the FMC. Or, you can use the push feature on the FMC to copy the package before you upgrade.

Repeat this procedure for each FTD upgrade package. You can configure only one location per upgrade package.

---

**Before you begin**

- Download the appropriate upgrade packages from the Cisco Support & Download site. See Downloading Upgrade Packages, on page 19.
- Copy the upgrade packages to an internal web server that your FTD devices can access.
- For secure web servers (HTTPS), obtain the server's digital certificate (PEM format). You should be able to obtain the certificate from the server's administrator. You may also be able to use your browser, or a tool like OpenSSL, to view the server's certificate details and export or copy the certificate.

---

Step 1  On the FMC web interface, choose System > Updates.
Step 2  Click Upload Update.
Choose this option even though you will not upload anything. The next page will prompt you for a URL.
Step 3  For the Action, click the Specify software update source radio button.
Step 4  Enter a Source URL for the upgrade package.
Provide the protocol (HTTP/HTTPS) and full path, for example:

https://internal_web_server/upgrade_package.sh.REL.tar
Upgrade package file names reflect the platform, package type (upgrade, patch, hotfix), and the Firepower version you are upgrading to. Make sure you enter the correct file name.

**Step 5**
For HTTPS servers, provide a **CA Certificate**.
This is the server's digital certificate you obtained earlier. Copy and paste the entire block of text, including the BEGIN CERTIFICATE and END CERTIFICATE lines.

**Step 6**
Click **Save**.
You are returned to the Product Updates page. Uploaded upgrade packages and upgrade package URLs are listed together, but are labeled distinctly.

---

**What to do next**

Refer to your plan. Optionally but recommended, copy device upgrade packages to devices. This helps reduce the length of your upgrade maintenance window and allows you to run readiness checks. See [Push Upgrade Packages to Managed Devices](#), on page 23.

---

### Push Upgrade Packages to Managed Devices

Starting with Version 6.2.3, you can copy (or push) upgrade packages from the FMC before the upgrade. This helps reduce the length of your upgrade maintenance window. Version 6.6.0 adds the ability to use an internal web server instead of the FMC as the source for FTD upgrade packages.

When you push, each device gets the upgrade package individually from the source — the system does not copy upgrade packages between cluster, stack, or HA member units.

If you do not push before upgrade, the device gets the upgrade package as the first step in the upgrade process.

**Before you begin**

Firepower upgrade package sizes vary. Make sure your management network has the bandwidth to perform large data transfers. For more information, see [Guidelines for Downloading Data from the Firepower Management Center to Managed Devices](#) (Troubleshooting TechNote).

---

**Step 1**
On the FMC web interface, choose **System > Updates**.
**Step 2**
Put the upgrade package where the device can get it. Choose:

- **FMC**
  
  Manually upload or directly retrieve the package to the FMC. See [Upload Upgrade Packages to the FMC](#), on page 21 or [Download Patches Directly from Cisco](#), on page 21.

- **Internal web server (FTD Version 6.6.0+)**
  
  Upload to an internal web server and configure FTD devices to get the package from that server. See [Get FTD Upgrade Packages from an Internal Server](#), on page 22.

**Step 3**
Click the **Push** (Version 6.5.0 and earlier) or **Push or Stage update** (Version 6.6.0+) icon next to the upgrade package you want to push, then choose destination devices.

If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.
Step 4  Push the package. For:
  • FMCs, click Push.
  • Internal web servers, click Download Update to Device from Source.

What to do next
After the file transfer to the device completes, you can proceed with readiness checks and/or the actual upgrade. Refer to your plan.
Run Readiness Checks

Readiness checks assess an appliance's preparedness for a Firepower upgrade. They identify issues including database integrity, version inconsistencies, and device registration. Readiness checks are included in upgrade packages after Version 6.1.

- Guidelines and Limitations for Readiness Checks, on page 25
- Run the Readiness Check, on page 26

Guidelines and Limitations for Readiness Checks

These guidelines and limitations apply to Firepower readiness checks.

Evaluates Firepower Software Readiness Only

The readiness check is for Firepower software readiness only. It does not assess preparedness for intrusion rule, VDB, or GeoDB updates.

Requires Version 6.1+

The readiness check was introduced in Version 6.1. If you are:

- Upgrading to Version 6.1: Install the Version 6.1 preinstallation package before you run the readiness check.
- Upgrading to any later version, including Version 6.1 patches: Readiness check is built in.

FMC and Standalone Devices Only

You can use the Firepower Management Center to perform the readiness check on itself and its standalone managed devices only.

Note

For clustered devices, stacked devices, and devices in high availability pairs, you can run the readiness check from the Linux shell, also called expert mode. To run the check, you must first push or copy the upgrade package to the correct location on each device, then use this command: `sudo install_update.pl --detach --readiness-check /var/sf/updates/upgrade_package_name`. For detailed instructions, contact Cisco TAC.
**Time Requirements**

The time required to run the readiness check varies depending on appliance model and database size. You may find it expedient to forgo readiness checks if your deployment is large.

---

**Tip**

You can reduce the amount of time it takes to run device readiness checks by pushing upgrade packages to devices before you begin. Requires an FMC running Version 6.2.3+.

---

**During The Check/Failed Checks**

Do not manually reboot, or shut down an appliance running readiness checks. If your appliance fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, do not begin the upgrade. Instead, contact Cisco TAC.

---

**Run the Readiness Check**

Use this procedure to perform readiness checks on the FMC and its standalone managed devices.

**Before you begin**

- Upload the upgrade packages for the appliances whose readiness you want to check to the FMC. Readiness checks are included in upgrade packages.
- (Optional, Version 6.2.3+) Push upgrade packages to managed devices. This can reduce the time required to run the check.
- Deploy configurations to managed devices whose configurations are out of date. Otherwise, the readiness check may fail.

---

**Step 1**

On the FMC web interface, choose **System > Updates**.

**Step 2**

Click the Install icon next to the appropriate upgrade package.

**Step 3**

Click **Launch Readiness Check**.

**Step 4**

Monitor the progress of the readiness check in the Message Center. When the readiness check completes, the system reports success or failure on the Readiness Check Status page.
CHAPTER 6

Other Pre-Upgrade Actions and Checks

The following pre-upgrade actions and checks are also essential to a successful upgrade.

• Verify Appliance Communication and Health, on page 27
• Review Release Notes, on page 27
• Plan Configuration Changes, on page 27
• Check Time and Disk Space, on page 28
• Appliance Access During Upgrade, on page 28
• Check Bandwidth, on page 28
• Back Up Configurations and Event Data, on page 28
• Verify NTP Synchronization, on page 29
• Schedule Maintenance Windows, on page 29

Verify Appliance Communication and Health

At all times during the upgrade process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor. Resolve minor issues before they become major.

Review Release Notes

Always read the release notes for critical and release-specific information:

• Firepower Release Notes
• ASA Release Notes
• FXOS Release Notes

Plan Configuration Changes

Especially with major upgrades, upgrading may cause or require significant configuration changes that you must address.
For example, Version 6.0 removes support for Firepower Management Center high availability. You must break any pairs before you begin the upgrade. As another example, Version 6.2.3 limits the number of results you can use or include in a report section. The upgrade process can lower your results limits and disable PDF reports, depending on your pre-upgrade configurations. Post upgrade, you may want to adjust your report templates to accommodate the new limits and reenable PDF reports.

For more information on pre- and post-upgrade configuration changes, see the release notes as well as Upgrade Guidelines and Warnings by Version, on page 137.

Check Time and Disk Space

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. You must also have enough time to perform the upgrade. Depending on your deployment, upgrades may take longer than the provided estimates. For example, lower-memory appliances and appliances under heavy load may take longer to upgrade.

For lists of time and disk space per release, see Time Tests and Disk Space Requirements, on page 185.

Appliance Access During Upgrade

Firepower devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade a Firepower device, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In Firepower Management Center deployments, you should also be able to access the FMC management interface without traversing the device.

Check Bandwidth

Firepower upgrade package sizes vary. Make sure your management network has the bandwidth to perform large data transfers. For more information, see:

- Obtain Upgrade Packages, on page 17
- Time Tests and Disk Space Requirements, on page 185
- Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote)

Back Up Configurations and Event Data

Back up Firepower appliances both before and after upgrade:

- **Before upgrade**: Sometimes if an upgrade fails catastrophically, you must reimage and restore. Reimaging returns most settings to factory defaults, including the system password. If you have a recent backup, you can return to normal operations more quickly.

- **After upgrade**: Back up after you upgrade, so you have a snapshot of your freshly upgraded deployment. We recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.
We strongly recommend you back up Firepower appliances to a secure remote location and verify transfer success. Backups left on an appliance may be deleted, either manually or by the upgrade process, which purges locally stored backups.

Especially because backup files are unencrypted, do not allow unauthorized access. If backup files are modified, the restore process will fail. Keep in mind that anyone with the Admin/Maint role can access the Backup Management page, where they can move and delete files from remote storage.

This table summarizes Firepower backup capabilities. For requirements, guidelines, limitations, best practices, and procedures, see the Firepower Management Center Configuration Guide.

Table 10: Firepower Backup Capabilities

<table>
<thead>
<tr>
<th>Platform</th>
<th>Current Version</th>
<th>Method</th>
<th>Backed Up Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Management Center</td>
<td>Any</td>
<td>FMC</td>
<td>Configurations and events</td>
</tr>
<tr>
<td>7000/8000 series</td>
<td>Any</td>
<td>FMC or device GUI</td>
<td>Configurations</td>
</tr>
<tr>
<td>FTD: physical platforms</td>
<td>6.3+</td>
<td>FMC</td>
<td>Configurations</td>
</tr>
<tr>
<td>FTDv: VMware</td>
<td>6.0.1 to 6.2.3</td>
<td></td>
<td>You cannot create individual configuration and event backup files for these devices.</td>
</tr>
<tr>
<td>FTDv: KVM, AWS, Azure NGIPSv</td>
<td>Any</td>
<td></td>
<td>You cannot create individual configuration and event backup files for these devices.</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Verify NTP Synchronization

Before you upgrade, make sure Firepower appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In FMC deployments, the Time Synchronization Status health module does alert if clocks are out of sync by more than 10 seconds, but you should still check manually.

To check time:

- FMC: Choose System > Configuration > Time.
- Devices: Use the show time CLI command.

Schedule Maintenance Windows

When you schedule a maintenance window, consider the upgrade's effect on traffic flow and inspection, and how long the upgrade is likely to take. Also consider the tasks you must perform in the window, and those you can perform ahead of time. Minimize disruption with careful planning and preparation. Do not wait until
Schedule Maintenance Windows

the maintenance window to obtaining and push upgrade packages, running readiness checks, create backups, and so on.
PART II

Upgrade Firepower Appliances

• Upgrade Firepower Management Centers, on page 33
• Upgrade Firepower Threat Defense: Firepower 4100/9300, on page 41
• Upgrade Firepower Threat Defense: Other FTD Devices, on page 67
• Upgrade Firepower 7000/8000 Series and NGIPSv, on page 73
• Upgrade ASA with FirePOWER Services, on page 79
Upgrade Firepower Management Centers

Upgrade Checklist: Firepower Management Centers

Use this checklist to upgrade Firepower Management Centers, including FMCv. If you are upgrading FMCs in a high availability pair, complete the checklist for each peer.

Complete the checklist every time you upgrade. Skipping steps can result in an unsuccessful upgrade. At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Plan the Upgrade

Maintain deployment compatibility at all times by correctly planning and following an upgrade path.

<table>
<thead>
<tr>
<th>✓ Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Verify Upgrade Path</strong></td>
<td>Upgrade Path: Firepower Management Centers, on page 35</td>
</tr>
<tr>
<td>Check your place in your upgrade path. Know which upgrade you just performed and which you are performing next.</td>
<td></td>
</tr>
<tr>
<td><strong>Check Versions</strong></td>
<td>Firepower Management Centers, on page 111</td>
</tr>
<tr>
<td>Check current and target versions on the FMC:</td>
<td></td>
</tr>
<tr>
<td>• Firepower software</td>
<td></td>
</tr>
<tr>
<td>• Virtual hosting environment (FMCv)</td>
<td></td>
</tr>
<tr>
<td><strong>Check FMC Compatibility</strong></td>
<td>Can I Maintain FMC-Device Version Compatibility?, on page 10</td>
</tr>
<tr>
<td>Check if the FMC will be able to manage the devices after it upgrades. If not, revise your upgrade path so you upgrade the devices first.</td>
<td></td>
</tr>
</tbody>
</table>
Read Release Notes
Read the release notes for the next upgrade/set of upgrades, paying special attention to version-specific warnings and guidelines.

Pre-Upgrade Actions and Checks
Minimize disruption by performing prechecks outside the maintenance window.

<table>
<thead>
<tr>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make Required Configuration Changes</td>
<td>Firepower Release Notes</td>
</tr>
<tr>
<td>Check Disk Space</td>
<td>Time Tests and Disk Space Requirements, on page 185</td>
</tr>
<tr>
<td>Get Upgrade Package</td>
<td>Obtain Upgrade Packages, on page 17</td>
</tr>
<tr>
<td>Run Readiness Check</td>
<td>Run Readiness Checks, on page 25</td>
</tr>
<tr>
<td>Back Up Events &amp; Configurations</td>
<td>Firepower Management Center Configuration Guide</td>
</tr>
<tr>
<td>Schedule Maintenance Window</td>
<td>Time Tests and Disk Space Requirements, on page 185</td>
</tr>
</tbody>
</table>

Upgrade the Firepower Management Center
Perform the upgrade in a maintenance window.

<table>
<thead>
<tr>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Hosting</td>
<td>See the documentation for your hosting environment.</td>
</tr>
</tbody>
</table>
Upgrade Firepower Appliances

Upgrade Path: Firepower Management Centers

This table provides upgrade paths for Firepower Management Centers, including FMCv. If you cannot perform a direct upgrade from your current to the target version, your upgrade path must include intermediate versions as noted.

Note

Upgrading to Version 6.0.0 and Version 6.0.1 requires a preinstallation package. For more information, see Identify Preinstallation Packages, on page 13.

Table 11: Recommended Upgrade Paths: Firepower Management Centers

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Target Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.6.0</td>
</tr>
<tr>
<td>6.5.0</td>
<td>Direct</td>
</tr>
<tr>
<td>6.4.0</td>
<td>Direct</td>
</tr>
<tr>
<td>Last support for FMC 750, 1500, and 3500.</td>
<td>Direct</td>
</tr>
<tr>
<td>6.3.0</td>
<td>Direct</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Direct</td>
</tr>
<tr>
<td>6.2.2</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.2.1</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.2.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.1.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
</tbody>
</table>

✓ | Action/Check | Details
|——|----------------|-----------------------------------|
|   | Upgrade Firepower Software | Upgrade a Standalone FMC, on page 36 or Upgrade High Availability FMCs, on page 38

Upgrade the Firepower software.
Upgrade a Standalone FMC

Use this procedure to upgrade a standalone Firepower Management Center, including Firepower Management Center Virtual.

⚠️ Caution

Do *not* deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do *not* restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

**Before you begin**

Check your place in the upgrade path, including hosting environment and managed device upgrades. Make sure you have fully planned and prepared for this step.

**Step 1**

Deploy to managed devices whose configurations are out of date.

On the FMC menu bar, click **Deploy**. Choose devices, then click **Deploy** again. Deploying before you upgrade reduces the chance of failure.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device...
handles traffic, may interrupt traffic until the restart completes. For more information, see Traffic Flow, Inspection, and Device Behavior, on page 223.

**Step 2** Perform final preupgrade checks.

- Check health: Use the Message Center (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

- Running tasks: Also in the Message Center, make sure essential tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

- Check disk space: Perform a final disk space check. Without enough free disk space, the upgrade fails. For disk space requirements, see Time Tests and Disk Space Requirements, on page 185.

**Step 3** Choose System > Updates.

**Step 4** Click the Install icon next to the upgrade package you want to use, then choose the FMC.

**Step 5** Click Install to begin the upgrade.

Confirm that you want to upgrade and reboot the FMC.

**Step 6** Monitor precheck progress in the Message Center until you are logged out.

Do not make configuration changes or deploy to any device while the FMC is upgrading. Even if the Message Center shows no progress for several minutes or indicates that the upgrade has failed, do not restart the upgrade or reboot the FMC. Instead, contact Cisco TAC.

**Step 7** Log back into the FMC when you can.

- Minor upgrades (patches and hotfixes): You can log in after the upgrade completes and the FMC reboots.

- Major upgrades: You can log in before the upgrade completes. The FMC displays a page you can use to monitor the upgrade's progress and view the upgrade log and any error messages. You are logged out again when the upgrade completes and the FMC reboots. After the reboot, log back in again.

**Step 8** If prompted, review and accept the End User License Agreement (EULA).

**Step 9** Verify upgrade success.

If the FMC does not notify you of the upgrade's success when you log in, choose Help > About to display current software version information.

**Step 10** Use the Message Center to recheck deployment health.

**Step 11** Update intrusion rules (SRU) and the vulnerability database (VDB).

If the SRU or the VDB available on the Cisco Support & Downloads site is newer than the version currently running, install the newer version. For more information, see the Firepower Management Center Configuration Guide. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

**Step 12** Complete any post-upgrade configuration changes described in the release notes.

**Step 13** Redeploy configurations.

Redeploy to all managed devices. If you do not deploy to a device, its eventual upgrade may fail and you may have to reimagine it.
Upgrade High Availability FMCs

Use this procedure to upgrade the Firepower software on Firepower Management Centers in a high availability pair.

You upgrade peers one at a time. With synchronization paused, first upgrade the standby, then the active. When the standby FMC starts prechecks, its status switches from standby to active, so that both peers are active. This temporary state is called **split-brain** and is not supported except during upgrade. Do not make or deploy configuration changes while the pair is split-brain. Your changes will be lost after you restart synchronization.

---

**Caution**

Do not deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

---

**Before you begin**

Check your place in the upgrade path, including managed device upgrades. Make sure you have fully planned and prepared for this step.

---

**Step 1**

On the active FMC, deploy to managed devices whose configurations are out of date.

On the FMC menu bar, click **Deploy**. Choose devices, then click **Deploy** again. Deploying before you upgrade reduces the chance of failure.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. For more information, see Traffic Flow, Inspection, and Device Behavior, on page 223.

**Step 2**

Use the Message Center to check deployment health before you pause synchronization.

Click the System Status icon on the FMC menu bar to display the Message Center. Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Step 3**

Pause synchronization.

a) Choose **System > Integration**.

b) On the **High Availability** tab, click **Pause Synchronization**.

**Step 4**

Upgrade the FMCs one at a time—first the standby, then the active.

Follow the instructions in Upgrade a Standalone FMC, on page 36, but omit the initial deploy, and stop after you verify update success on each FMC. In summary, for each FMC:

a) Perform final preupgrade checks (health, running tasks, disk space).

b) On the **System > Updates** page, install the upgrade.

c) Monitor progress until you are logged out, then log back in when you can (this happens twice for major upgrades).

d) Verify upgrade success.

Do not make or deploy configuration changes while the pair is split-brain.
Step 5  On the FMC you want to make the active peer, restart synchronization.
   a) Choose **System > Integration**.
   b) On the **High Availability** tab, click **Make-Me-Active**.
   c) Wait until synchronization restarts and the other FMC switches to standby mode.

Step 6  Use the Message Center to recheck deployment health.

Step 7  Update intrusion rules (SRU) and the vulnerability database (VDB).

   If the SRU or the VDB available on the Cisco Support & Downloads site is newer than the version currently running, install the newer version. For more information, see the Firepower Management Center Configuration Guide. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 8  Complete any post-upgrade configuration changes described in the release notes.

Step 9  Redeploy configurations.

   Redeploy to all managed devices. If you do not deploy to a device, its eventual upgrade may fail and you may have to reimagine it.
Upgrade High Availability FMCs
Upgrade Firepower Threat Defense: Firepower 4100/9300

**Upgrade Checklist: FTD on Firepower 4100/9300 Chassis**

Use this checklist to upgrade Firepower 4100/9300 chassis with FTD. Complete the checklist every time you upgrade. Skipping steps can result in an unsuccessful upgrade. At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Plan the Upgrade**

Maintain deployment compatibility at all times by correctly planning and following an upgrade path.

<table>
<thead>
<tr>
<th>✓</th>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Verify Upgrade Path</td>
<td>Upgrade Path: FTD on Firepower 4100/9300 Chassis, on page 43</td>
</tr>
<tr>
<td></td>
<td>Check your place in your upgrade path. Know which upgrade you just performed and which you are performing next.</td>
<td>Upgrade Path: FTD on Firepower 4100/9300 Chassis, on page 43</td>
</tr>
<tr>
<td></td>
<td>Check Versions</td>
<td>Firepower 4100/9300 with FTD, on page 116</td>
</tr>
<tr>
<td></td>
<td>Check current and target versions on the devices:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Firepower software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• FXOS</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Check FMC Compatibility</td>
<td>Can I Maintain FMC-Device Version Compatibility?, on page 10</td>
</tr>
<tr>
<td></td>
<td>Check if the FMC will be able to manage the devices after you upgrade them. If not, revise your upgrade path so you upgrade the FMC first.</td>
<td></td>
</tr>
</tbody>
</table>
### Pre-Upgrade Actions and Checks
Minimize disruption by performing prechecks outside the maintenance window.

<table>
<thead>
<tr>
<th>✓ Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Read Release Notes</strong></td>
<td>Read the release notes for the next upgrade/set of upgrades, paying special attention to version-specific warnings and guidelines.</td>
</tr>
<tr>
<td><strong>Make Required Configuration Changes</strong></td>
<td>Make required pre-upgrade configuration changes, and be prepared to make required post-upgrade configuration changes.</td>
</tr>
<tr>
<td><strong>Check Disk Space</strong></td>
<td>Run a preliminary disk space check for the Firepower software upgrade.</td>
</tr>
<tr>
<td><strong>Get Upgrade Package</strong></td>
<td>Obtain the correct upgrade package and upload it to the FMC. Do not untar signed (.tar) packages.</td>
</tr>
<tr>
<td><strong>Check Bandwidth</strong></td>
<td>Make sure you have the bandwidth to perform a large data transfer from the FMC to the devices.</td>
</tr>
<tr>
<td><strong>Push Upgrade Package</strong></td>
<td>Push the upgrade package to the devices. We strongly recommend (and sometimes require) you push before you begin the required companion FXOS upgrade. Requires Version 6.2.3+.</td>
</tr>
<tr>
<td><strong>Run Readiness Check</strong></td>
<td>Run a readiness check. Requires Version 6.1+.</td>
</tr>
<tr>
<td><strong>Back Up Devices</strong></td>
<td>Use the FMC to back up configuration data for physical FTD devices and FTDv: VMware. Back up to an external location and verify transfer success. No support for other FTDv implementations. Requires Version 6.3+.</td>
</tr>
<tr>
<td><strong>Verify Appliance Access</strong></td>
<td>Make sure your computer can connect to the FMC’s management interface and to the device’s management interface, both without traversing the device itself.</td>
</tr>
</tbody>
</table>
Details

✓ Action/Check

Schedule Maintenance Window
Schedule a maintenance window when it will have the least impact, considering the tasks you must perform, the upgrade's effect on traffic flow and inspection, and the time the upgrade is likely to take.

Details

✓ Action/Check

Schedule Maintenance Window
Schedule a maintenance window when it will have the least impact, considering the tasks you must perform, the upgrade's effect on traffic flow and inspection, and the time the upgrade is likely to take.

Details

✓ Action/Check

Schedule Maintenance Window
Schedule a maintenance window when it will have the least impact, considering the tasks you must perform, the upgrade's effect on traffic flow and inspection, and the time the upgrade is likely to take.

Details

✓ Action/Check

Schedule Maintenance Window
Schedule a maintenance window when it will have the least impact, considering the tasks you must perform, the upgrade's effect on traffic flow and inspection, and the time the upgrade is likely to take.

Details

✓ Action/Check

Schedule Maintenance Window
Schedule a maintenance window when it will have the least impact, considering the tasks you must perform, the upgrade's effect on traffic flow and inspection, and the time the upgrade is likely to take.

Details
Upgrade Path: FTD on Firepower 4100/9300 Chassis

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Target Version &amp; Recommended FXOS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.0</td>
<td>FXOS 2.8.1</td>
</tr>
<tr>
<td>6.2.2</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.2.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.1.0</td>
<td>→ 6.2.3</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.0.1</td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.2.3</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
</tbody>
</table>

Upgrading FXOS

Although you upgrade the Firepower software on a device clusters or high availability pair as a unit, you upgrade FXOS on each chassis independently. This table outlines FXOS upgrade order for standalone and HA/scalability deployments. For more information, see Upgrade FXOS: Firepower 4100/9300 Chassis, on page 45.

Table 13: FXOS + FTD Upgrade Order

<table>
<thead>
<tr>
<th>FTD Deployment</th>
<th>Upgrade Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone device</td>
<td>1. Upgrade FXOS.</td>
</tr>
<tr>
<td></td>
<td>2. Upgrade Firepower software.</td>
</tr>
<tr>
<td>High availability</td>
<td>To minimize disruption, always upgrade the standby.</td>
</tr>
<tr>
<td></td>
<td>1. Upgrade FXOS on the standby.</td>
</tr>
<tr>
<td></td>
<td>2. Switch roles.</td>
</tr>
<tr>
<td></td>
<td>3. Upgrade FXOS on the new standby.</td>
</tr>
<tr>
<td></td>
<td>4. Upgrade the Firepower software.</td>
</tr>
<tr>
<td>Intra-chassis cluster (Firepower 9300 only)</td>
<td>1. Upgrade FXOS.</td>
</tr>
<tr>
<td></td>
<td>2. Upgrade Firepower software.</td>
</tr>
</tbody>
</table>
Upgrade Firepower Appliances

Upgrade FXOS: Firepower 4100/9300 Chassis

<table>
<thead>
<tr>
<th>FTD Deployment</th>
<th>Upgrade Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inter-chassis cluster</td>
<td>To minimize disruption, always upgrade an all-slave chassis. For example, for a</td>
</tr>
<tr>
<td>(6.2+)</td>
<td>two-chassis cluster:</td>
</tr>
<tr>
<td></td>
<td>1. Upgrade FXOS on the all-slave chassis.</td>
</tr>
<tr>
<td></td>
<td>2. Switch the master module to the chassis you just upgraded.</td>
</tr>
<tr>
<td></td>
<td>3. Upgrade FXOS on the new all-slave chassis.</td>
</tr>
<tr>
<td></td>
<td>4. Upgrade Firepower software.</td>
</tr>
</tbody>
</table>

High Availability and Clustering Hitless Upgrade Requirements

Performing hitless upgrades have the following additional requirements.

Flow Offload: Due to bug fixes in the flow offload feature, some combinations of FXOS and FTD do not support flow offload; see the Cisco Firepower Compatibility Guide. To perform a hitless upgrade in a high availability or clustered deployment, you must make sure you are always running a compatible combination.

If your upgrade path includes upgrading FXOS to 2.2.2.91, 2.3.1.130, or later (including FXOS 2.4.1.x, 2.6.1.x, and so on) use this path:

1. Upgrade FTD to 6.2.2.2 or later.
2. Upgrade FXOS to 2.2.2.91, 2.3.1.130, or later.
3. Upgrade FTD to your final version.

For example, if you are running FXOS 2.2.2.17/FTD 6.2.2.0, and you want to upgrade to FXOS 2.6.1/FTD 6.4.0, then you can:

1. Upgrade FTD to 6.2.2.5.
2. Upgrade FXOS to 2.6.1.
3. Upgrade FTD to 6.4.0.

Version 6.1.0 Upgrades: Performing a hitless upgrade of an FTD high availability pair to Version 6.1.0 requires a preinstallation package. For more information, see Firepower System Release Notes Version 6.1.0 Preinstallation Package.

Upgrade FXOS: Firepower 4100/9300 Chassis

On the Firepower 4100/9300 chassis, you upgrade the FXOS operating system separately from the Firepower software. You upgrade FXOS on each chassis independently, even if you have Firepower inter-chassis clustering or high availability pairs configured.

Major Firepower versions have a companion FXOS version. You must be running that companion version of FXOS before you upgrade the Firepower software on the Firepower 4100/9300 chassis.

Upgrading FXOS reboots the chassis. Depending on your deployment, traffic can either drop or traverse the network without inspection; see FTD Upgrade Behavior: Firepower 4100/9300 Chassis, on page 223.
FXOS for Firepower 4100/9300 Chassis Upgrade Packages

For FXOS upgrade packages for the Firepower 4100/9300 chassis, browse to:

- Firepower 4100 series: http://www.cisco.com/go/firepower4100-software
- Firepower 9300: http://www.cisco.com/go/firepower9300-software

Choose your model > Firepower Extensible Operating System > version.

Table 14: FXOS Upgrade Packages

<table>
<thead>
<tr>
<th>Package Type</th>
<th>Package Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>FXOS image</td>
<td>fxos-k9.version.SPA</td>
</tr>
<tr>
<td>Recovery (kickstart)</td>
<td>fxos-k9-kickstart.version.SPA</td>
</tr>
<tr>
<td>Recovery (manager)</td>
<td>fxos-k9-manager.version.SPA</td>
</tr>
<tr>
<td>Recovery (system)</td>
<td>fxos-k9-system.version.SPA</td>
</tr>
<tr>
<td>MIBs</td>
<td>fxos-mibs-fp9k-fp4k.version.zip</td>
</tr>
<tr>
<td>Firmware: Firepower 4100 series</td>
<td>fxos-k9-fpr4k-firmware.version.SPA</td>
</tr>
<tr>
<td>Firmware: Firepower 9300</td>
<td>fxos-k9-fpr9k-firmware.version.SPA</td>
</tr>
</tbody>
</table>

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster

Use the FXOS CLI or Firepower Chassis Manager to upgrade the FXOS platform bundle on a Firepower 4100/9300 Series security appliance that has standalone or intra-chassis clustered Firepower Threat Defense logical devices installed on the appliance.

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using Firepower Chassis Manager

This section describes how to upgrade the FXOS platform bundle for a standalone Firepower 4100/9300 chassis.

The section describes the upgrade process for the following types of devices:

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with one or more standalone FTD logical devices that are not part of a failover pair or inter-chassis cluster.
- A Firepower 9300 chassis that is configured with FTD logical devices in an intra-chassis cluster.
Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading (see FXOS for Firepower 4100/9300 Chassis Upgrade Packages, on page 46).

- Back up your FXOS and FTD configurations.

Note

The upgrade process typically takes between 20 and 30 minutes. Traffic will not traverse through the device while it is upgrading.

---

**Step 1**

In Firepower Chassis Manager, choose **System > Updates**.

The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

**Step 2**

Upload the new platform bundle image:

a) Click **Upload Image** to open the Upload Image dialog box.

b) Click **Choose File** to navigate to and select the image that you want to upload.

c) Click **Upload**.

The selected image is uploaded to the Firepower 4100/9300 chassis.

d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.

**Step 3**

After the new platform bundle image has been successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

**Step 4**

Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

**Step 5**

Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter **scope system**.

b) Enter **show firmware monitor**.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show **Upgrade-Status: Ready**.

**Note** After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

**Example:**

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FP9300-A/FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready
```
Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Step 6  After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:
  a) Enter `top`.
  b) Enter `scope ssa`.
  c) Enter `show slot`.
  d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
  e) Enter `show app-instance`.
  f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using the FXOS CLI

This section describes how to upgrade the FXOS platform bundle for a standalone Firepower 4100/9300 chassis.

The section describes the FXOS upgrade process for the following types of devices:
  • A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair or inter-chassis cluster.
  • A Firepower 9300 chassis that is configured with one or more standalone FTD devices that are not part of a failover pair or inter-chassis cluster.
  • A Firepower 9300 chassis that is configured with FTD logical devices in an intra-chassis cluster.

Before you begin

Before beginning your upgrade, make sure that you have already done the following:
  • Download the FXOS platform bundle software package to which you are upgrading (see FXOS for Firepower 4100/9300 Chassis Upgrade Packages, on page 46).
  • Back up your FXOS and FTD configurations.
  • Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
    • IP address and authentication credentials for the server from which you are copying the image.
    • Fully qualified name of the image file.
The upgrade process typically takes between 20 and 30 minutes. Traffic will not traverse through the device while it is upgrading.

**Step 1**
Connect to the FXOS CLI.

**Step 2**
Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:
   ```bash
   Firepower-chassis-a # scope firmware
   ```

b) Download the FXOS platform bundle software image:
   ```bash
   Firepower-chassis-a /firmware # download image URL
   ```

Specify the URL for the file being imported using one of the following syntax:

- `ftp://username@hostname/path/image_name`
- `scp://username@hostname/path/image_name`
- `sftp://username@hostname/path/image_name`
- `tftp://hostname:port-num/path/image_name`

c) To monitor the download process:
   ```bash
   Firepower-chassis-a /firmware # scope download-task image_name
   ```
   ```bash
   Firepower-chassis-a /firmware/download-task # show detail
   ```

**Example:**
The following example copies an image using the SCP protocol:

```bash
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
```

**Download task:**
- **File Name:** fxos-k9.2.3.1.58.SPA
- **Protocol:** scp
- **Server:** 192.168.1.1
- **Userid:**
- **Path:**
- **Downloaded Image Size (KB):** 853688
- **State:** Downloading
- **Current Task:** downloading image fxos-k9.2.3.1.58.SPA from 192.168.1.1(FSM-STAGE: sam:dme:FirmwareDownloaderDownload:Local)

**Step 3**
If necessary, return to firmware mode:
```bash
Firepower-chassis-a /firmware/download-task # up
``` 

**Step 4**
Enter auto-install mode:
```bash
Firepower-chassis-a /firmware # scope auto-install
```
Step 5  Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # install platform-platform-vers version_number

*version_number* is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

Step 6  The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter yes to confirm that you want to proceed with verification.

Step 7  Enter yes to confirm that you want to proceed with installation, or enter no to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.

Step 8  To monitor the upgrade process:

a) Enter scope system.

b) Enter show firmware monitor.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show Upgrade-Status: Ready.

**Note** After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

**Example:**

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FP9300-A /system #
```

Step 9  After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter top.

b) Enter scope ssa.

c) Enter show slot.

d) Verify that the Admin State is Ok and the Oper State is Online for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

e) Enter show app-instance.

f) Verify that the Oper State is Online for any logical devices installed on the chassis.
Upgrade FXOS on a Firepower Threat Defense High Availability Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade the FXOS platform bundle on Firepower 4100/9300 Series security appliances with Firepower Threat Defense logical devices configured as a high availability pair.

Upgrade FXOS on a FTD High Availability Pair Using Firepower Chassis Manager

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as a high availability pair, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin

Before beginning your upgrade, make sure that you have already done the following:

• Download the FXOS platform bundle software package to which you are upgrading (see FXOS for Firepower 4100/9300 Chassis Upgrade Packages, on page 46).

• Back up your FXOS and FTD configurations.

Note

The upgrade process typically takes between 20 and 30 minutes per chassis.

---

Step 1
Connect to Firepower Chassis Manager on the Firepower security appliance that contains the standby Firepower Threat Defense logical device:

Step 2
In Firepower Chassis Manager, choose System > Updates.
The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

Step 3
Upload the new platform bundle image:

a) Click Upload Image to open the Upload Image dialog box.
b) Click Choose File to navigate to and select the image that you want to upload.
c) Click Upload.
   The selected image is uploaded to the Firepower 4100/9300 chassis.
d) For certain software images you will be presented with an end-user license agreement after uploading the image.
   Follow the system prompts to accept the end-user license agreement.

Step 4
After the new platform bundle image has successfully uploaded, click Upgrade for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Step 5
Click Yes to confirm that you want to proceed with installation, or click No to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.
Step 6 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter `scope system`.
b) Enter `show firmware monitor`.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
   Package-Vers: 2.3(1.58)
   Upgrade-Status: Ready

Fabric Interconnect A:
   Package-Vers: 2.3(1.58)
   Upgrade-Status: Ready

Chassis 1:
   Server 1:
      Package-Vers: 2.3(1.58)
      Upgrade-Status: Ready
   Server 2:
      Package-Vers: 2.3(1.58)
      Upgrade-Status: Ready
```

Step 7 After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter `top`.
b) Enter `scope ssa`.
c) Enter `show slot`.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter `show app-instance`.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 8 Make the unit that you just upgraded the active unit so that traffic flows to the upgraded unit:

a) Connect to Firepower Management Center.
b) Choose `Devices > Device Management`.

c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon.
d) Click `Yes` to immediately make the standby device the active device in the high availability pair.

Step 9 Connect to Firepower Chassis Manager on the Firepower security appliance that contains the new standby Firepower Threat Defense logical device:

Step 10 In Firepower Chassis Manager, choose `System > Updates`.
The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

Step 11 Upload the new platform bundle image:

a) Click `Upload Image` to open the Upload Image dialog box.
b) Click **Choose File** to navigate to and select the image that you want to upload.

c) Click **Upload**.
   
   The selected image is uploaded to the Firepower 4100/9300 chassis.

d) For certain software images you will be presented with an end-user license agreement after uploading the image.
   
   Follow the system prompts to accept the end-user license agreement.

**Step 12**

After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.

The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

**Step 13**

Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

**Step 14**

Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter `scope system`.

b) Enter `show firmware monitor`.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show **Upgrade-Status: Ready**.

   **Note** After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

**Example:**

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
   Package-Vers: 2.3(1.58)
   Upgrade-Status: Ready

Fabric Interconnect A:
   Package-Vers: 2.3(1.58)
   Upgrade-Status: Ready

Chassis 1:
   Server 1:
      Package-Vers: 2.3(1.58)
      Upgrade-Status: Ready
   Server 2:
      Package-Vers: 2.3(1.58)
      Upgrade-Status: Ready
```

**Step 15**

After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter `top`.

b) Enter `scope ssa`.

c) Enter `show slot`.

d) Verify that the Admin State is **Ok** and the Oper State is **Online** for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

e) Enter `show app-instance`.
f) Verify that the Oper State is Online for any logical devices installed on the chassis.

Step 16
Make the unit that you just upgraded the active unit as it was before the upgrade:

a) Connect to Firepower Management Center.

b) Choose Devices > Device Management.

c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ( ).

d) Click Yes to immediately make the standby device the active device in the high availability pair.

Upgrade FXOS on a FTD High Availability Pair Using the FXOS CLI

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as a high availability pair, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

Before you begin
Before beginning your upgrade, make sure that you have already done the following:

• Download the FXOS platform bundle software package to which you are upgrading (see FXOS for Firepower 4100/9300 Chassis Upgrade Packages, on page 46).

• Back up your FXOS and FTD configurations.

• Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
  • IP address and authentication credentials for the server from which you are copying the image.
  • Fully qualified name of the image file.

Note The upgrade process typically takes between 20 and 30 minutes per chassis.

Step 1
Connect to FXOS CLI on the Firepower security appliance that contains the standby Firepower Threat Defense logical device:

Step 2
Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

   Firepower-chassis-a # scope firmware

b) Download the FXOS platform bundle software image:

   Firepower-chassis-a /firmware # download image URL

Specify the URL for the file being imported using one of the following syntax:

• ftp://username@hostname/path/image_name

• scp://username@hostname/path/image_name

• sftp://username@hostname/path/image_name
• *tftp://hostname:port-num/path/image_name*

c) To monitor the download process:

Firepower-chassis-a /firmware # **scope download-task** image_name

Firepower-chassis-a /firmware/download-task # **show detail**

**Example:**

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
```

Download task:
- File Name: fxos-k9.2.3.1.58.SPA
- Protocol: scp
- Server: 192.168.1.1
- Userid: 
- Path: 
- Downloaded Image Size (KB): 853688
- State: Downloading
- Current Task: downloading image fxos-k9.2.3.1.58.SPA from 192.168.1.1(FSM-STAGE:fw:fw:FirmwareDownloaderDownload:Local)

**Step 3**  If necessary, return to firmware mode:

Firepower-chassis-a /firmware/download-task # **up**

**Step 4**  Enter auto-install mode:

Firepower-chassis-a /firmware # **scope auto-install**

**Step 5**  Install the FXOS platform bundle:

Firepower-chassis-a /firmware/auto-install # **install platform platform-vers** version_number

`version_number` is the version number of the FXOS platform bundle you are installing—for example, 2.3(1.58).

**Step 6**  The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter `yes` to confirm that you want to proceed with verification.

**Step 7**  Enter `yes` to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.

**Step 8**  To monitor the upgrade process:

a) Enter **scope system**.

b) Enter **show firmware monitor**.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show **Upgrade-Status: Ready**.

**Note**  After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.
Example:

FP9300-A# scope system
FP9300-A /system # show firmware monitor

FPM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Step 9
After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter `top`.
b) Enter `scope ssa`.
c) Enter `show slot`.
d) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter `show app-instance`.
f) Verify that the Oper State is `Online` for any logical devices installed on the chassis.

Step 10
Make the unit that you just upgraded the `active` unit so that traffic flows to the upgraded unit:

a) Connect to Firepower Management Center.
b) Choose `Devices` > `Device Management`.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon (🔗).
d) Click `Yes` to immediately make the standby device the active device in the high availability pair.

Step 11
Connect to FXOS CLI on the Firepower security appliance that contains the `new standby` Firepower Threat Defense logical device:

Step 12
Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter firmware mode:

```
Firepower-chassis-a # scope firmware
```

b) Download the FXOS platform bundle software image:

```
Firepower-chassis-a /firmware # download image URL
```

Specify the URL for the file being imported using one of the following syntax:

- `ftp://username@hostname/path/image_name`
- `scp://username@hostname/path/image_name`
- `sftp://username@hostname/path/image_name`
Example:
The following example copies an image using the SCP protocol:

Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail

Download task:
  File Name: fxos-k9.2.3.1.58.SPA
  Protocol: scp
  Server: 192.168.1.1
  Userid: 
  Path: 
  Downloaded Image Size (KB): 853688
  State: Downloading
  Current Task: downloading image fxos-k9.2.3.1.58.SPA from 192.168.1.1 (FSM-STAGE: sam:dme:FirmwareDownloaderDownload:Local)

Step 13 If necessary, return to firmware mode:
Firepower-chassis-a /firmware/download-task # up

Step 14 Enter auto-install mode:
Firepower-chassis-a /firmware # scope auto-install

Step 15 Install the FXOS platform bundle:
Firepower-chassis-a /firmware/auto-install # install platform platform-vers version_number

version_number is the version number of the FXOS platform bundle you are installing--for example, 2.3(1.58).

Step 16 The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

Enter yes to confirm that you want to proceed with verification.

Step 17 Enter yes to confirm that you want to proceed with installation, or enter no to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.

Step 18 To monitor the upgrade process:
  a) Enter scope system.
  b) Enter show firmware monitor.
  c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show Upgrade-Status: Ready.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.
Example:

FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Step 19
After all components have successfully upgraded, enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter `top`.
b) Enter `scope ssa`.
c) Enter `show slot`.
d) Verify that the Admin State is Ok and the Oper State is Online for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter `show app-instance`.
f) Verify that the Oper State is Online for any logical devices installed on the chassis.

Step 20
Make the unit that you just upgraded the active unit as it was before the upgrade:

a) Connect to Firepower Management Center.
b) Choose Devices > Device Management.
c) Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon (��).
d) Click Yes to immediately make the standby device the active device in the high availability pair.

---

Upgrade FXOS on a Firepower Threat Defense Inter-chassis Cluster

Use the FXOS CLI or Firepower Chassis Manager to upgrade the FXOS platform bundle on Firepower 4100/9300 Series security appliances with Firepower Threat Defense logical devices configured as an inter-chassis cluster.

Upgrade FXOS on a FTD Inter-chassis Cluster Using Firepower Chassis Manager

If you have Firepower 9300 or Firepower 4100 series security appliances that have FTD logical devices configured as an inter-chassis cluster, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:
Before you begin

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading (see FXOS for Firepower 4100/9300 Chassis Upgrade Packages, on page 46).
- Back up your FXOS and FTD configurations.

Note

The upgrade process typically takes between 20 and 30 minutes per chassis.

Step 1

Enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the Primary unit).

b) Enter `top`.

c) Enter `scope ssa`.

d) Enter `show slot`.

e) Verify that the Admin State is `Ok` and the Oper State is `Online` for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

f) Enter `show app-instance`.

g) Verify that the Oper State is `Online` and that the Cluster State is `In Cluster` for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

Note

Verify that the Primary unit is not on this chassis. There should not be any Firepower Threat Defense instance with Cluster Role set to `Master`.

h) For any security modules installed on a Firepower 9300 appliance or for the security engine on a Firepower 4100 series appliance, verify that the FXOS version is correct:

   `scope server 1/slot_id`, where `slot_id` is 1 for a Firepower 4100 series security engine.

   `show version`.

Step 2

Connect to Firepower Chassis Manager on Chassis #2 (this should be a chassis that does not have the Primary unit).

Step 3

In Firepower Chassis Manager, choose `System > Updates`. The Available Updates page shows a list of the Firepower eXtensible Operating System platform bundle images and application images that are available on the chassis.

Step 4

Upload the new platform bundle image:

a) Click `Upload Image` to open the Upload Image dialog box.

b) Click `Choose File` to navigate to and select the image that you want to upload.

c) Click `Upload`.

   The selected image is uploaded to the Firepower 4100/9300 chassis.

d) For certain software images you will be presented with an end-user license agreement after uploading the image.

   Follow the system prompts to accept the end-user license agreement.

Step 5

After the new platform bundle image has successfully uploaded, click `Upgrade` for the FXOS platform bundle to which you want to upgrade.
The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.

**Step 6**

Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.

The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components. The upgrade process can take up to 30 minutes to complete.

**Step 7**

Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:

a) Enter `scope system`.

b) Enter `show firmware monitor`.

c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status: Ready`.

   **Note**  
   After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

d) Enter `top`.

e) Enter `scope ssa`.

f) Enter `show slot`.

g) Verify that the Admin State is **Ok** and the Oper State is **Online** for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.

h) Enter `show app-instance`.

i) Verify that the Oper State is **Online**, that the Cluster State is **In Cluster** and that the Cluster Role is **Slave** for any logical devices installed on the chassis.

**Example:**

```
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Fabric Interconnect A:
  Package-Vers: 2.3(1.58)
  Upgrade-Status: Ready

Chassis 1:
  Server 1:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready
  Server 2:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

FP9300-A /system #
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
  Slot ID Log Level Admin State Oper State
    -------- --------- ------------ ----------
  1        Info   Ok       Online
  2        Info   Ok       Online
  3        Info   Ok       Not Available
```

Cisco Firepower Management Center Upgrade Guide
Upgrade FXOS on a FTD Inter-chassis Cluster Using the FXOS CLI

If you have Firepower 9300 or Firepower 4100 series security appliances with FTD logical devices configured as an inter-chassis cluster, use the following procedure to update the FXOS platform bundle on your Firepower 9300 or Firepower 4100 series security appliances:

**Before you begin**

Before beginning your upgrade, make sure that you have already done the following:

- Download the FXOS platform bundle software package to which you are upgrading (see FXOS for Firepower 4100/9300 Chassis Upgrade Packages, on page 46).
- Back up your FXOS and FTD configurations.
- Collect the following information that you will need to download the software image to the Firepower 4100/9300 chassis:
  - IP address and authentication credentials for the server from which you are copying the image.
  - Fully qualified name of the image file.

**Note**
The upgrade process typically takes between 20 and 30 minutes per chassis.

---

**Step 1**
Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the Primary unit).

**Step 2**
Enter the following commands to verify the status of the security modules/security engine and any installed applications:

a) Enter `top`.

b) Enter `scope ssa`.
c) Enter `show slot`.
d) Verify that the Admin State is Ok and the Oper State is Online for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
e) Enter `show app-instance`.
f) Verify that the Oper State is Online and that the Cluster State is In Cluster for any logical devices installed on the chassis. Also verify that the correct FTD software version is shown as the Running Version.

**Note** Verify that the Primary unit is not on this chassis. There should not be any Firepower Threat Defense instance with Cluster Role set to Master.

g) For any security modules installed on a Firepower 9300 appliance or for the security engine on a Firepower 4100 series appliance, verify that the FXOS version is correct:

```
scope server 1/slot_id, where slot_id is 1 for a Firepower 4100 series security engine.
show version.
```

**Step 3**

Download the new platform bundle image to the Firepower 4100/9300 chassis:

a) Enter `top`.

b) Enter firmware mode:

```
Firepower-chassis-a # scope firmware
```

c) Download the FXOS platform bundle software image:

```
Firepower-chassis-a /firmware # download image URL
```

Specify the URL for the file being imported using one of the following syntax:

- `ftp://username@hostname/path/image_name`
- `scp://username@hostname/path/image_name`
- `sftp://username@hostname/path/image_name`
- `tftp://hostname:port-num/path/image_name`

d) To monitor the download process:

```
Firepower-chassis-a /firmware # scope download-task image_name
Firepower-chassis-a /firmware/download-task # show detail
```

**Example:**

The following example copies an image using the SCP protocol:

```
Firepower-chassis-a # scope firmware
Firepower-chassis-a /firmware # download image scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis-a /firmware/download-task # show detail
```

Download task:

- File Name: fxos-k9.2.3.1.58.SPA
- Protocol: scp
- Server: 192.168.1.1
- Userid: 
- Path: 
- Downloaded Image Size (KB): 853688
- State: Downloading
- Current Task: downloading image fxos-k9.2.3.1.58.SPA from
Step 4
If necessary, return to firmware mode:
Firepower-chassis-a /firmware/download-task # up

Step 5
Enter auto-install mode:
Firepower-chassis /firmware # scope auto-install

Step 6
Install the FXOS platform bundle:
Firepower-chassis /firmware/auto-install # install platform platform-vers version_number

version_number is the version number of the FXOS platform bundle you are installing—for example, 2.3(1.58).

Step 7
The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.
Enter yes to confirm that you want to proceed with verification.

Step 8
Enter yes to confirm that you want to proceed with installation, or enter no to cancel the installation.
The Firepower eXtensible Operating System unpacks the bundle and upgrades/reloads the components.

Step 9
To monitor the upgrade process:

a) Enter scope system.
b) Enter show firmware monitor.
c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show Upgrade-Status: Ready.

Note After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

d) Enter top.
e) Enter scope ssa.
f) Enter show slot.
g) Verify that the Admin State is Ok and the Oper State is Online for the security engine on a Firepower 4100 series appliance or for any security modules installed on a Firepower 9300 appliance.
h) Enter show app-instance.
i) Verify that the Oper State is Online, that the Cluster State is In Cluster and that the Cluster Role is Slave for any logical devices installed on the chassis.

Example:
FP9300-A# scope system
FP9300-A /system # show firmware monitor
FPRM:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Fabric Interconnect A:
    Package-Vers: 2.3(1.58)
    Upgrade-Status: Ready

Chassis 1:
    Server 1:
        Package-Vers: 2.3(1.58)
Upgrade Status: Ready
Server 2:
Package-Vers: 2.3(1.58)
Upgrade Status: Ready

FP9300-A /system#
FP9300-A /system # top
FP9300-A# scope ssa
FP9300-A /ssa # show slot

Slot:
<table>
<thead>
<tr>
<th>Slot ID</th>
<th>Log Level</th>
<th>Admin State</th>
<th>Oper State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Info</td>
<td>Ok</td>
<td>Online</td>
</tr>
<tr>
<td>2</td>
<td>Info</td>
<td>Ok</td>
<td>Online</td>
</tr>
<tr>
<td>3</td>
<td>Info</td>
<td>Ok</td>
<td>Not Available</td>
</tr>
</tbody>
</table>

FP9300-A /ssa#

FP9300-A /ssa # show app-instance
App Name Slot ID Admin State Oper State Running Version Startup Version Profile Name Cluster State Cluster Role
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>-----------------</td>
<td>-----------</td>
<td>-------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>---------------</td>
<td>-----------------</td>
<td>---------------</td>
</tr>
<tr>
<td>ftd 1</td>
<td>Enabled</td>
<td>Online</td>
<td>6.2.2.81</td>
<td>6.2.2.81</td>
<td>In</td>
<td>Cluster Slave</td>
<td></td>
</tr>
<tr>
<td>ftd 2</td>
<td>Enabled</td>
<td>Online</td>
<td>6.2.2.81</td>
<td>6.2.2.81</td>
<td>In</td>
<td>Cluster Slave</td>
<td></td>
</tr>
<tr>
<td>ftd 3</td>
<td>Disabled</td>
<td>Not Available</td>
<td>6.2.2.81</td>
<td>Not Applicable</td>
<td>None</td>
<td>Cluster Slave</td>
<td></td>
</tr>
</tbody>
</table>

FP9300-A /ssa#

**Step 10**
Set one of the security modules on Chassis #2 as Primary.
After setting one of the security modules on Chassis #2 to Primary, Chassis #1 no longer contains the Primary unit and can now be upgraded.

**Step 11**
Repeat Steps 1-9 for all other Chassis in the cluster.

**Step 12**
To return the Primary role to Chassis #1, set one of the security modules on Chassis #1 as Primary.

---

**Upgrade FTD Software: Firepower 4100/9300 Chassis**

Use this procedure to upgrade the FTD software on the Firepower 4100/9300 chassis. You can upgrade multiple devices at once. You must upgrade the members of device clusters and high availability pairs at the same time.

**Caution**
Do not deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.
Before you begin

Check your place in the upgrade path, including FXOS and FMC upgrades. Make sure you have fully planned and prepared for this step.

---

**Step 1**
Deploy configurations to the devices you are about to upgrade.

On the FMC menu bar, click **Deploy**. Choose devices, then click **Deploy** again. Deploying before you upgrade reduces the chance of failure.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. For more information, see FTD Upgrade Behavior: Firepower 4100/9300 Chassis, on page 223.

---

**Step 2**
Perform final preupgrade checks.

- **Check health**: Use the Message Center (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

- **Running tasks**: Also in the Message Center, make sure essential tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

- **Check disk space**: Perform a final disk space check. Without enough free disk space, the upgrade fails. For disk space requirements, see Time Tests and Disk Space Requirements, on page 185.

---

**Step 3**
(Optional, high availability only) Switch the active/standby roles of your high availability device pairs.

The standby device in a high availability pair upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices’ roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

Choose **Devices > Device Management**, click the **Switch Active Peer** icon next to the pair, and confirm your choice.

---

**Step 4**
Choose **System > Updates**.

**Step 5**
Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

**Note**  We strongly recommend upgrading no more than five devices simultaneously. The FMC does not allow you to stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

---

**Step 6**
Click **Install**, then confirm that you want to upgrade and reboot the devices.

Some devices may reboot twice during the upgrade; this is expected behavior.

Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see FTD Upgrade Behavior: Firepower 4100/9300 Chassis, on page 223.

---

**Step 7**
Monitor upgrade progress in the Message Center.

Do not deploy configurations to the device while it is upgrading. Even if the Message Center shows no progress for several minutes or indicates that the upgrade has failed, do not restart the upgrade or reboot the device. Instead, contact Cisco TAC.
Step 8  Verify success.
After the upgrade completes, choose **Devices > Device Management** and confirm that the devices you upgraded have the correct software version.

Step 9  Use the Message Center to recheck deployment health.

Step 10  Update intrusion rules (SRU) and the vulnerability database (VDB).
If the SRU or the VDB available on the Cisco Support & Downloads site is newer than the version currently running, install the newer version. For more information, see the Firepower Management Center Configuration Guide. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 11  Complete any post-upgrade configuration changes described in the release notes.

Step 12  Redeploy configurations to the devices you just upgraded.
CHAPTER 9

Upgrade Firepower Threat Defense: Other FTD Devices

- Upgrade Checklist: Other FTD Devices, on page 67
- Upgrade Path: Other FTD Devices, on page 69
- Upgrade FTD Software: Other FTD Devices, on page 70

Upgrade Checklist: Other FTD Devices

Use this checklist to upgrade Firepower 1000/2100 series, ASA 5500-X series, ISA 3000, and FTDv devices. Complete the checklist every time you upgrade. Skipping steps can result in an unsuccessful upgrade. At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

Plan the Upgrade

Maintain deployment compatibility at all times by correctly planning and following an upgrade path.

<table>
<thead>
<tr>
<th>✓ Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Upgrade Path</td>
<td>Upgrade Path: Other FTD Devices, on page 69</td>
</tr>
<tr>
<td>Check your place in your upgrade path. Know which upgrade you just performed and which you are performing next.</td>
<td></td>
</tr>
<tr>
<td>Check Versions</td>
<td>Firepower Devices, on page 115</td>
</tr>
<tr>
<td>Check current and target versions on the devices:</td>
<td></td>
</tr>
<tr>
<td>• Firepower Threat Defense software</td>
<td></td>
</tr>
<tr>
<td>• Virtual hosting environment (FTDv)</td>
<td></td>
</tr>
<tr>
<td>Check FMC Compatibility</td>
<td>Can I Maintain FMC-Device Version Compatibility?, on page 10</td>
</tr>
<tr>
<td>Check if the FMC will be able to manage the devices after you upgrade them. If not, revise your upgrade path so you upgrade the FMC first.</td>
<td></td>
</tr>
</tbody>
</table>
## Pre-Upgrade Actions and Checks

Minimize disruption by performing prechecks outside the maintenance window.

<table>
<thead>
<tr>
<th>✓</th>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td><strong>Read Release Notes</strong></td>
<td>Firepower Release Notes</td>
</tr>
<tr>
<td></td>
<td>Read the release notes for the next upgrade/set of upgrades, paying special attention to version-specific warnings and guidelines.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Make Required Configuration Changes</strong></td>
<td>Firepower Release Notes</td>
</tr>
<tr>
<td></td>
<td>Make required pre-upgrade configuration changes, and be prepared to make required post-upgrade configuration changes.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Check Disk Space</strong></td>
<td>Time Tests and Disk Space Requirements, on page 185</td>
</tr>
<tr>
<td></td>
<td>Run a preliminary disk space check for the Firepower software upgrade.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Get Upgrade Package</strong></td>
<td>Obtain Upgrade Packages, on page 17</td>
</tr>
<tr>
<td></td>
<td>Obtain the correct upgrade package and upload it to the FMC. Do not untar signed (.tar) packages.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Check Bandwidth</strong></td>
<td>Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote)</td>
</tr>
<tr>
<td></td>
<td>Make sure you have the bandwidth to perform a large data transfer from the FMC to the devices.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Push Upgrade Package</strong></td>
<td>Push Upgrade Packages to Managed Devices, on page 23</td>
</tr>
<tr>
<td></td>
<td>Push the upgrade package to the devices. Requires Version 6.2.3+.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Run Readiness Check</strong></td>
<td>Run Readiness Checks, on page 25</td>
</tr>
<tr>
<td>✓</td>
<td><strong>Back Up Devices</strong></td>
<td>Firepower Management Center Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>Use the FMC to back up configuration data for physical FTD devices and FTDv: VMware. Back up to an external location and verify transfer success. No support for other FTDv implementations. Requires Version 6.3+.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Verify Appliance Access</strong></td>
<td>Appliance Access During Upgrade, on page 28</td>
</tr>
<tr>
<td></td>
<td>Make sure your computer can connect to the FMC’s management interface and to the device’s management interface, both without traversing the device itself.</td>
<td></td>
</tr>
</tbody>
</table>
Upgrade the Devices

Because upgrades can cause interruptions in traffic flow or inspection, perform them in a maintenance window.

<table>
<thead>
<tr>
<th>✓</th>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Schedule Maintenance Window</td>
<td>FTD Upgrade Behavior: Other Devices, on page 226</td>
</tr>
<tr>
<td></td>
<td>Schedule a maintenance window when it will have</td>
<td>and</td>
</tr>
<tr>
<td></td>
<td>the least impact, considering the tasks you must</td>
<td>Time Tests and Disk Space</td>
</tr>
<tr>
<td></td>
<td>perform, the upgrade's effect on traffic flow and</td>
<td>Requirements, on page 185</td>
</tr>
<tr>
<td></td>
<td>inspection, and the time the upgrade is likely to</td>
<td></td>
</tr>
<tr>
<td></td>
<td>take.</td>
<td></td>
</tr>
</tbody>
</table>

Upgrade Path: Other FTD Devices

This table provides upgrade paths for Firepower Threat Defense devices with bundled operating systems, managed by a Firepower Management Center: Firepower 1000 series, Firepower 2100 series, ASA 5500-X series, ISA 3000, and FTDv. If you cannot perform a direct upgrade from your current to the target version, your upgrade path must include intermediate versions as noted.

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Target Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.6.0</td>
</tr>
<tr>
<td>6.5.0</td>
<td>Direct</td>
</tr>
<tr>
<td>6.4.0</td>
<td>Direct</td>
</tr>
<tr>
<td>6.3.0</td>
<td>Direct</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Direct</td>
</tr>
<tr>
<td>6.2.2</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
</tbody>
</table>

Note: Performing a hitless upgrade of an FTD high availability pair to Version 6.1.0 requires a preinstallation package. For more information, see Firepower System Release Notes Version 6.1.0 Preinstallation Package.
Upgrade FTD Software: Other FTD Devices

Use this procedure to upgrade Firepower 1000/2100 series, ASA 5500-X series, ISA 3000, and FTDv devices. You can upgrade multiple devices at once if they use the same upgrade package. You must upgrade the members of high availability pairs at the same time.

Caution
Do not deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Before you begin
Check your place in the upgrade path, including virtual hosting environment and FMC upgrades. Make sure you have fully planned and prepared for this step.

Step 1
Deploy configurations to the devices you are about to upgrade.

On the FMC menu bar, click Deploy. Choose devices, then click Deploy again. Deploying before you upgrade reduces the chance of failure.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. For more information, see FTD Upgrade Behavior: Other Devices, on page 226.

Step 2
Perform final preupgrade checks.
• Check health: Use the Message Center (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

• Running tasks: Also in the Message Center, make sure essential tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

• Check disk space: Perform a final disk space check. Without enough free disk space, the upgrade fails. For disk space requirements, see Time Tests and Disk Space Requirements, on page 185.

Step 3
(Optional, high availability only) Switch the active/standby roles of your high availability device pairs.

The standby device in a high availability pair upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

Choose Devices > Device Management, click the Switch Active Peer icon next to the pair, and confirm your choice.

Step 4
Choose System > Updates.

Step 5
Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

**Note** We *strongly* recommend upgrading no more than five devices simultaneously. The FMC does not allow you to stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 6
Click Install, then confirm that you want to upgrade and reboot the devices.

Some devices may reboot twice during the upgrade; this is expected behavior.

Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see FTD Upgrade Behavior: Other Devices, on page 226.

Step 7
Monitor upgrade progress in the Message Center.

Do not deploy configurations to the device while it is upgrading. Even if the Message Center shows no progress for several minutes or indicates that the upgrade has failed, do not restart the upgrade or reboot the device. Instead, contact Cisco TAC.

Step 8
Verify success.

After the upgrade completes, choose Devices > Device Management and confirm that the devices you upgraded have the correct software version.

Step 9
Use the Message Center to recheck deployment health.

Step 10
Update intrusion rules (SRU) and the vulnerability database (VDB).

If the SRU or the VDB available on the Cisco Support & Downloads site is newer than the version currently running, install the newer version. For more information, see the Firepower Management Center Configuration Guide. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 11
Complete any post-upgrade configuration changes described in the release notes.

Step 12
Redeploy configurations to the devices you just upgraded.
Upgrade FTD Software: Other FTD Devices
Upgrade Firepower 7000/8000 Series and NGIPSv

Use this checklist to upgrade Firepower 7000/8000 series and NGIPSv devices.

Complete the checklist every time you upgrade. Skipping steps can result in an unsuccessful upgrade. At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

**Plan the Upgrade**

Maintain deployment compatibility at all times by correctly planning and following an upgrade path.

<table>
<thead>
<tr>
<th>✓</th>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td><strong>Verify Upgrade Path</strong></td>
<td>Upgrade Path: Firepower 7000/8000 Series and NGIPSv, on page 75</td>
</tr>
<tr>
<td></td>
<td>Check your place in your upgrade path. Know which upgrade you just performed and which you are performing next.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Check Versions</strong></td>
<td>Firepower 7000/8000 Series and Legacy Devices, on page 119 or NGIPSv, on page 121</td>
</tr>
<tr>
<td></td>
<td>Check current and target versions on the devices:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Firepower software</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Virtual hosting environment (NGIPSv)</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td><strong>Check FMC Compatibility</strong></td>
<td>Can I Maintain FMC-Device Version Compatibility?, on page 10</td>
</tr>
<tr>
<td></td>
<td>Check if the FMC will be able to manage the devices after you upgrade them.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If not, revise your upgrade path so you upgrade the FMC first.</td>
<td></td>
</tr>
</tbody>
</table>
Pre-Upgrade Actions and Checks

Minimize disruption by performing prechecks outside the maintenance window.

<table>
<thead>
<tr>
<th>✓</th>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Read Release Notes</td>
<td>Firepower Release Notes</td>
</tr>
<tr>
<td></td>
<td>Read the release notes for the next upgrade/set of upgrades, paying special attention to version-specific warnings and guidelines.</td>
<td></td>
</tr>
</tbody>
</table>

**Pre-Upgrade Actions and Checks**

Minimize disruption by performing prechecks outside the maintenance window.

<table>
<thead>
<tr>
<th>✓</th>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Make Required Configuration Changes</td>
<td>Firepower Release Notes</td>
</tr>
<tr>
<td></td>
<td>Make required pre-upgrade configuration changes, and be prepared to make required post-upgrade configuration changes.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Check Disk Space</td>
<td>Time Tests and Disk Space Requirements, on page 185</td>
</tr>
<tr>
<td></td>
<td>Run a preliminary disk space check for the Firepower software upgrade.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Get Upgrade Package</td>
<td>Obtain Upgrade Packages, on page 17</td>
</tr>
<tr>
<td></td>
<td>Obtain the correct upgrade package and upload it to the FMC. Do not untar signed (.tar) packages.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Check Bandwidth</td>
<td>Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote)</td>
</tr>
<tr>
<td></td>
<td>Make sure you have the bandwidth to perform a large data transfer from the FMC to the devices.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Push Upgrade Package</td>
<td>Push Upgrade Packages to Managed Devices, on page 23</td>
</tr>
<tr>
<td></td>
<td>Push the upgrade package to the devices. Requires Version 6.2.3+.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Run Readiness Check</td>
<td>Run Readiness Checks, on page 25</td>
</tr>
<tr>
<td>✓</td>
<td>Back Up Devices</td>
<td>Firepower Management Center Configuration Guide</td>
</tr>
<tr>
<td></td>
<td>Use the FMC to back up configuration data for 7000/8000 series devices. Back up to an external location and verify transfer success. Not supported for NGIPSv.</td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Verify Appliance Access</td>
<td>Appliance Access During Upgrade, on page 28</td>
</tr>
<tr>
<td></td>
<td>Make sure your computer can connect to the FMC’s management interface and to the device’s management interface, both without traversing the device itself.</td>
<td></td>
</tr>
</tbody>
</table>
Schedule Maintenance Window
Schedule a maintenance window when it will have the least impact, considering the tasks you must perform, the upgrade's effect on traffic flow and inspection, and the time the upgrade is likely to take.

 Upgrade the Devices
Because upgrades can cause interruptions in traffic flow or inspection, perform them in a maintenance window.

 Upgrade Path: Firepower 7000/8000 Series and NGIPSv
This table provides upgrade paths for 7000/8000 series and NGIPSv devices, managed by a Firepower Management Center. If you cannot perform a direct upgrade from your current to the target version, your upgrade path must include intermediate versions as noted.

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Target Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.6.0</td>
</tr>
<tr>
<td>6.5.0</td>
<td>Direct</td>
</tr>
<tr>
<td>6.4.0</td>
<td>Direct</td>
</tr>
</tbody>
</table>

Note
Upgrading to Version 6.0 requires a preinstallation package. For more information, see FireSIGHT System Release Notes Version 6.0.0 Preinstallation.

Table 16: Recommended Upgrade Paths: Firepower 7000/8000 Series and NGIPSv with FMC
## Upgrade Firepower 7000/8000 Series and NGIPSv

Use this procedure to upgrade Firepower 7000/8000 series and NGIPSv devices. You can upgrade multiple devices at once if they use the same upgrade package. You must upgrade the members of device stacks and high availability pairs at the same time.

*You must be running at least Version 5.4.0.2 to upgrade to Version 6.0.0.*

### Upgrade Firepower Appliances

<table>
<thead>
<tr>
<th>Current Version</th>
<th>Target Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.6.0</td>
</tr>
<tr>
<td>6.3.0</td>
<td>Direct</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Direct</td>
</tr>
<tr>
<td>6.2.2</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td>6.2.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td>6.1.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td>6.0.1</td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td>6.0.0</td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td>5.4.x*</td>
<td>→ 6.0.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.0.1</td>
</tr>
<tr>
<td></td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
</tbody>
</table>
Caution
Do not deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Before you begin
Check your place in the upgrade path, including virtual hosting environment and FMC upgrades. Make sure you have fully planned and prepared for this step.

Step 1
Deploy configurations to the devices you are about to upgrade.
On the FMC menu bar, click Deploy. Choose devices, then click Deploy again. Deploying before you upgrade reduces the chance of failure.
When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. For more information, see Firepower 7000/8000 Series Upgrade Behavior, on page 228 or NGIPSv Upgrade Behavior, on page 230.

Step 2
Perform final preupgrade checks.
• Check health: Use the Message Center (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.
• Running tasks: Also in the Message Center, make sure essential tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.
• Check disk space: Perform a final disk space check. Without enough free disk space, the upgrade fails. For disk space requirements, see Time Tests and Disk Space Requirements, on page 185.

Step 3
(Optional, high availability only) Switch the active/standby roles of your high availability device pairs that perform switching/routing.
If your high availability pairs are deployed to perform access control only, the active upgrades first. When the upgrade completes, the active and standby maintain their old roles.
However, in a routed or switched deployment, the standby upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.
Choose Devices > Device Management, click the Switch Active Peer icon next to the pair, and confirm your choice.

Step 4
Choose System > Updates.

Step 5
Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.
If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

Note
We strongly recommend upgrading no more than five devices simultaneously. The FMC does not allow you stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 6
Click Install, then confirm that you want to upgrade and reboot the devices.
Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see Firepower 7000/8000 Series Upgrade Behavior, on page 228 or NGIPSv Upgrade Behavior, on page 230.

**Step 7**
Monitor upgrade progress in the Message Center.

Do not deploy configurations to the device while it is upgrading. Even if the Message Center shows no progress for several minutes or indicates that the upgrade has failed, do not restart the upgrade or reboot the device. Instead, contact Cisco TAC.

**Step 8**
Verify success.

After the upgrade completes, choose **Devices > Device Management** and confirm that the devices you upgraded have the correct software version.

**Step 9**
Use the Message Center to recheck deployment health.

**Step 10**
Update intrusion rules (SRU) and the vulnerability database (VDB).

If the SRU or the VDB available on the Cisco Support & Downloads site is newer than the version currently running, install the newer version. For more information, see the Firepower Management Center Configuration Guide. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

**Step 11**
Complete any post-upgrade configuration changes described in the release notes.

**Step 12**
Redeploy configurations to the devices you just upgraded.
## Upgrade ASA with FirePOWER Services

- Upgrade Checklist: ASA with FirePOWER Services, on page 79
- Upgrade Path: ASA FirePOWER, on page 81
- Upgrade the ASA, on page 85
- Upgrade an ASA FirePOWER Module, on page 106

### Upgrade Checklist: ASA with FirePOWER Services

Use this checklist to upgrade ASA with FirePOWER Services.

Complete the checklist every time you upgrade. Skipping steps can result in an unsuccessful upgrade. At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

#### Plan the Upgrade

Maintain deployment compatibility at all times by correctly planning and following an upgrade path.

<table>
<thead>
<tr>
<th>✓ Action/Check</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Upgrade Path</td>
<td>Upgrade Path: ASA FirePOWER, on page 81</td>
</tr>
<tr>
<td>Check Versions</td>
<td>ASA 5500-X Series and ISA 3000 with FirePOWER Services, on page 120</td>
</tr>
<tr>
<td>Check FMC Compatibility</td>
<td>Can I Maintain FMC-Device Version Compatibility?, on page 10</td>
</tr>
</tbody>
</table>
Read Release Notes
Read the release notes for the next upgrade/set of upgrades, paying special attention to version-specific warnings and guidelines.

Pre-Upgrade Actions and Checks
Minimize disruption by performing prechecks outside the maintenance window.

Make Required Configuration Changes
Make required pre-upgrade configuration changes, and be prepared to make required post-upgrade configuration changes.

Check Disk Space
Run a preliminary disk space check for the Firepower software upgrade.

Get Upgrade Package
Obtain the correct upgrade package and upload it to the FMC. Do not untar signed (.tar) packages.

Check Bandwidth
Make sure you have the bandwidth to perform a large data transfer from the FMC to the devices.

Push Upgrade Package
Push the upgrade package to the devices. Requires Version 6.2.3+.

Run Readiness Check

Verify Appliance Access
Make sure your computer can connect to the FMC’s management interface and to the device’s management interface, both without traversing the device itself.

Schedule Maintenance Window
Schedule a maintenance window when it will have the least impact, considering the tasks you must perform, the upgrade's effect on traffic flow and inspection, and the time the upgrade is likely to take.
Upgrade ASA and ASA with FirePOWER Services

Because upgrades can cause interruptions in traffic flow or inspection, perform them in a maintenance window.

<table>
<thead>
<tr>
<th>✓</th>
<th>Action/Check</th>
<th>Details</th>
</tr>
</thead>
</table>
| ✓ | Upgrade Standalone ASA Devices | Upgrade a Standalone Unit, on page 85
| | | and Upgrade an ASA FirePOWER Module, on page 106 |
| | Upgrade the ASA FirePOWER module on standalone ASA devices. | |
| | If you are also upgrading ASA, use the FMC to upgrade the ASA FirePOWER module just *after* you upgrade ASA and reload. | |
| | Upgrade ASA Clusters & Failover Pairs | One of:
| | Upgrade an Active/Standby Failover Pair, on page 90
| | Upgrade an Active/Active Failover Pair, on page 94
| | Upgrade an ASA Cluster, on page 98
| | and Upgrade an ASA FirePOWER Module, on page 106 |
| | Upgrade the ASA FirePOWER module on ASA devices in clusters and failover pairs. | |
| | To avoid interruptions in traffic flow and inspection, fully upgrade these devices *one at a time*. If you are also upgrading ASA, use the FMC to upgrade the ASA FirePOWER module just *before* you reload each unit to upgrade ASA. | |

Upgrade Path: ASA FirePOWER

This table provides upgrade paths for ASA FirePOWER modules, managed by a Firepower Management Center. If you cannot perform a direct upgrade from your current to the target version, your upgrade path must include intermediate versions as noted.

**Note**

Upgrading to Version 6.0.0 requires a preinstallation package. For more information, see FireSIGHT System Release Notes Version 6.0.0 Preinstallation

| Table 17: Recommended Upgrade Paths: ASA FirePOWER with FMC |
|---|---|---|---|---|---|---|---|---|---|
| Current Version | Target Version | 6.6.0 | 6.5.0 | 6.4.0 | 6.3.0 | 6.2.3 | 6.2.2 | 6.2.0 | 6.1.0 | 6.0.1 | 6.0.0 |
| 6.5.0 | Direct | — | — | — | — | — | — | — | — | — |
| 6.4.0 | Last Firepower support for ASA 5585-X series and ASA 5515-X. | Direct | Direct | — | — | — | — | — | — | — | — |

Cisco Firepower Management Center Upgrade Guide
<table>
<thead>
<tr>
<th>Current Version</th>
<th>Target Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.6.0</td>
</tr>
<tr>
<td>6.3.0</td>
<td>Direct</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Direct</td>
</tr>
<tr>
<td></td>
<td><em>Last Firepower support for ASA 5506-X series and ASA 5512-X.</em></td>
</tr>
<tr>
<td>6.2.2</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.2.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.1.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.0.1</td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>6.0.0</td>
<td>→ 6.0.1</td>
</tr>
<tr>
<td></td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>5.4.x*</td>
<td>→ 6.0.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.0.1</td>
</tr>
<tr>
<td></td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.6.0</td>
</tr>
<tr>
<td>Current Version</td>
<td>Target Version</td>
</tr>
<tr>
<td>----------------</td>
<td>---------------</td>
</tr>
<tr>
<td></td>
<td>6.5.0</td>
</tr>
<tr>
<td>6.4.0</td>
<td>Direct</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3.0</td>
<td>Direct</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.3</td>
<td>Direct</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.2</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.5.0</td>
</tr>
<tr>
<td>6.2.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.5.0</td>
</tr>
<tr>
<td>6.1.0</td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.5.0</td>
</tr>
<tr>
<td>6.0.1</td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.5.0</td>
</tr>
<tr>
<td>6.0.0</td>
<td>→ 6.0.1</td>
</tr>
<tr>
<td></td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.5.0</td>
</tr>
<tr>
<td>5.4.x*</td>
<td>→ 6.0.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.0.1</td>
</tr>
<tr>
<td></td>
<td>→ 6.1.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.4.0</td>
</tr>
<tr>
<td></td>
<td>→ 6.5.0</td>
</tr>
</tbody>
</table>

* You must be running at least Version 5.4.0.2/5.4.1.1 to upgrade to Version 6.0.0.
**Upgrading ASA**

There is wide compatibility between ASA and ASA FirePOWER versions. However, even if an ASA upgrade is not strictly required, resolving issues may require an upgrade to the latest supported version. For detailed compatibility information, see ASA 5500-X Series and ISA 3000 with FirePOWER Services, on page 120.

You upgrade ASA on each device independently, even if you have ASA clustering or failover pairs configured. Exactly when you upgrade the ASA FirePOWER module (before or after ASA reload) depends on your deployment. This table outlines ASA upgrade order for standalone and HA/scalability deployments. For detailed instructions, see Upgrade the ASA, on page 85.

**Table 19: ASA + ASA FirePOWER Upgrade Order**

<table>
<thead>
<tr>
<th>ASA Deployment</th>
<th>Upgrade Order</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone device</td>
<td>1. Upgrade ASA, including reload.</td>
</tr>
<tr>
<td></td>
<td>2. Upgrade ASA FirePOWER.</td>
</tr>
<tr>
<td>ASA failover: active/standby</td>
<td>Always upgrade the standby.</td>
</tr>
<tr>
<td></td>
<td>1. Upgrade ASA on the standby, but do not reload.</td>
</tr>
<tr>
<td></td>
<td>2. Upgrade ASA FirePOWER on the standby.</td>
</tr>
<tr>
<td></td>
<td>3. Reload ASA on the standby.</td>
</tr>
<tr>
<td></td>
<td>4. Fail over.</td>
</tr>
<tr>
<td></td>
<td>5. Upgrade ASA on the new standby.</td>
</tr>
<tr>
<td></td>
<td>6. Upgrade ASA FirePOWER on the new standby.</td>
</tr>
<tr>
<td></td>
<td>7. Reload ASA on the new standby.</td>
</tr>
<tr>
<td>ASA failover: active/active</td>
<td>Make both failover groups active on the unit you are not upgrading.</td>
</tr>
<tr>
<td></td>
<td>1. Make both failover groups active on the primary.</td>
</tr>
<tr>
<td></td>
<td>2. Upgrade ASA on the secondary, but do not reload.</td>
</tr>
<tr>
<td></td>
<td>3. Upgrade ASA FirePOWER on the secondary.</td>
</tr>
<tr>
<td></td>
<td>4. Reload ASA on the secondary.</td>
</tr>
<tr>
<td></td>
<td>5. Make both failover groups active on the secondary.</td>
</tr>
<tr>
<td></td>
<td>6. Upgrade ASA on the primary, but do not reload.</td>
</tr>
<tr>
<td></td>
<td>7. Upgrade ASA FirePOWER on the primary.</td>
</tr>
<tr>
<td></td>
<td>8. Reload ASA on the primary.</td>
</tr>
</tbody>
</table>
Upgrade the ASA

Use the procedures in this section to upgrade ASA and ASDM for standalone, failover, or clustering deployments.

Upgrade a Standalone Unit

Use the CLI or ASDM to upgrade the standalone unit.

Upgrade a Standalone Unit Using the CLI

This section describes how to install the ASDM and ASA images, and also when to upgrade the ASA FirePOWER module.

Before you begin

This procedure uses FTP. For TFTP, HTTP, or other server types, see the copy command in the ASA command reference.

Step 1

In privileged EXEC mode, copy the ASA software to flash memory.

```
copy ftp://[[user[:password]@]server[/path]/asa_image_name disk0:[/path]/asa_image_name
```

Example:

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asa-9-12-1-smp-k8.bin disk0:/asa-9-12-1-smp-k8.bin
```
Step 2  Copy the ASDM image to flash memory.

```
copy ftp://[[user[:password]@]server[/path]/asdm_image_name diskn:[/path]/asdm_image_name
```

**Example:**

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-7121.bin disk0:/asdm-7121.bin
```

Step 3  Access global configuration mode.

```
configure terminal
```

**Example:**

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Step 4  Show the current boot images configured (up to 4):

```
show running-config boot system
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

**Example:**

```
ciscoasa(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

Step 5  Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

```
no boot system diskn:[/path]/asa_image_name
```

**Example:**

```
ciscoasa(config)# no boot system disk0:/cdisk.bin
```
```
ciscoasa(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 6  Set the ASA image to boot (the one you just uploaded):

```
boot system diskn:[/path]/asa_image_name
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

**Example:**

```
ciscoasa(config)# boot system disk0:/asa-9-12-1-smp-k8.bin
```

Step 7  Set the ASDM image to use (the one you just uploaded):

```
asdm image diskn:[/path]/asdm_image_name
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.
Example:

ciscoasa(config)# asdm image disk0:/asdm-7121.bin

Step 8
Save the new settings to the startup configuration:
write memory

Step 9
Reload the ASA:
reload

Step 10
If you are upgrading the ASA FirePOWER module, disable the ASA REST API or else the upgrade will fail.
no rest-api agent
You can reenable it after the upgrade:
rest-api agent

Note: The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 11
Upgrade the ASA FirePOWER module.

Upgrade a Standalone Unit from Your Local Computer Using ASDM

The Upgrade Software from Local Computer tool lets you upload an image file from your computer to the flash file system to upgrade the ASA.

Step 1
In the main ASDM application window, choose Tools > Upgrade Software from Local Computer. The Upgrade Software dialog box appears.

Step 2
From the Image to Upload drop-down list, choose ASDM.

Step 3
In the Local File Path field, click Browse Local Files to find the file on your PC.

Step 4
In the Flash File System Path field, click Browse Flash to find the directory or file in the flash file system.

Step 5
Click Upload Image.

The uploading process might take a few minutes.

Step 6
You are prompted to set this image as the ASDM image. Click Yes.

Step 7
You are reminded to exit ASDM and save the configuration. Click OK.

You exit the Upgrade tool. Note: You will save the configuration and exit and reconnect to ASDM after you upgrade the ASA software.

Step 8
Repeat these steps, choosing ASA from the Image to Upload drop-down list. You can also use this procedure to upload other file types.

Step 9
Choose Tools > System Reload to reload the ASA.

A new window appears that asks you to verify the details of the reload.

a) Click the Save the running configuration at the time of reload radio button (the default).
b) Choose a time to reload (for example, **Now**, the default).

c) Click **Schedule Reload**.

Once the reload is in progress, a **Reload Status** window appears that indicates that a reload is being performed. An option to exit ASDM is also provided.

**Step 10**

After the ASA reloads, restart ASDM.

You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.

**Step 11**

If you are upgrading an ASA FirePOWER module, disable the ASA REST API by choosing **Tools > Command Line Interface**, and entering **no rest-api agent**.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail. You can reenable it after the upgrade:

```
rest-api agent
```

**Note** The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

**Step 12**

Upgrade the ASA FirePOWER module.

---

**Upgrade a Standalone Unit Using the ASDM Cisco.com Wizard**

The **Upgrade Software from Cisco.com Wizard** lets you automatically upgrade the ASDM and ASA to more current versions.

In this wizard, you can do the following:

- Choose an ASA image file and/or ASDM image file to upgrade.

*Note* ASDM downloads the latest image version, which includes the build number. For example, if you are downloading 9.9(1), the download might be 9.9(1.2). This behavior is expected, so you can proceed with the planned upgrade.

- Review the upgrade changes that you have made.
- Download the image or images and install them.
- Review the status of the installation.
- If the installation completed successfully, reload the ASA to save the configuration and complete the upgrade.

**Before you begin**

Due to an internal change, the wizard is only supported using ASDM 7.10(1) and later; also, due to an image naming change, you must use ASDM 7.12(1) or later to upgrade to ASA 9.10(1) and later. Because ASDM is backwards compatible with earlier ASA releases, you can upgrade ASDM no matter which ASA version you are running.
Step 1  Choose Tools > Check for ASA/ASDM Updates.  
In multiple context mode, access this menu from the System.  
The Cisco.com Authentication dialog box appears.  

Step 2  Enter your Cisco.com username and password, and then click Login.  
The Cisco.com Upgrade Wizard appears.  
Note  If there is no upgrade available, a dialog box appears. Click OK to exit the wizard.  

Step 3  Click Next to display the Select Software screen.  
The current ASA version and ASDM version appear.  

Step 4  To upgrade the ASA version and ASDM version, perform the following steps:  
a) In the ASA area, check the Upgrade to check box, and then choose an ASA version to which you want to upgrade from the drop-down list.  
b) In the ASDM area, check the Upgrade to check box, and then choose an ASDM version to which you want to upgrade from the drop-down list.  

Step 5  Click Next to display the Review Changes screen.  

Step 6  Verify the following items:  
• The ASA image file and/or ASDM image file that you have downloaded are the correct ones.  
• The ASA image file and/or ASDM image file that you want to upload are the correct ones.  
• The correct ASA boot image has been selected.  

Step 7  Click Next to start the upgrade installation.  
You can then view the status of the upgrade installation as it progresses.  
The Results screen appears, which provides additional details, such as the upgrade installation status (success or failure).  

Step 8  If the upgrade installation succeeded, for the upgrade versions to take effect, check the Save configuration and reload device now check box to restart the ASA, and restart ASDM.  

Step 9  Click Finish to exit the wizard and save the configuration changes that you have made.  
Note  To upgrade to the next higher version, if any, you must restart the wizard.  

Step 10  After the ASA reloads, restart ASDM.  
You can check the reload status from a console port, or you can wait a few minutes and try to connect using ASDM until you are successful.  

Step 11  If you are upgrading an ASA FirePOWER module, disable the ASA REST API by choosing Tools > Command Line Interface, and entering no rest-api agent.  
If you do not disable the REST API, the ASA FirePOWER module upgrade will fail. You can reenable it after the upgrade:  
rest-api agent
The ASA 5506-X series does not support the ASA REST API if you are running the FirePOWER module Version 6.0 or later.

Step 12 Upgrade the ASA FirePOWER module.

Upgrade an Active/Standby Failover Pair

Use the CLI or ASDM to upgrade the Active/Standby failover pair for a zero downtime upgrade.

Upgrade an Active/Standby Failover Pair Using the CLI

To upgrade the Active/Standby failover pair, perform the following steps.

Before you begin

- Perform these steps on the active unit. For SSH access, connect to the active IP address; the active unit always owns this IP address. When you connect to the CLI, determine the failover status by looking at the ASA prompt; you can configure the ASA prompt to show the failover status and priority (primary or secondary), which is useful to determine which unit you are connected to. See the `prompt` command. Alternatively, enter the `show failover` command to view this unit’s status and priority (primary or secondary).
- This procedure uses FTP. For TFTP, HTTP, or other server types, see the `copy` command in the ASA command reference.

Step 1

On the active unit in privileged EXEC mode, copy the ASA software to the active unit flash memory:

`copy ftp://[user[:password]@]server[/path]asa_image_name disk:n:[/path]asa_image_name`

Example:

`asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin`

Step 2

Copy the software to the standby unit; be sure to specify the same path as for the active unit:

`failover exec mate copy /noconfirm ftp://[user[:password]@]server[/path]asa_image_name diskn:[/path]asa_image_name`

Example:

`asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin`

Step 3

Copy the ASDM image to the active unit flash memory:

`copy ftp://[user[:password]@]server[/path]asdm_image_name diskn:[/path]asdm_image_name`

Example:

`asa/act# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin disk0:/asdm-77178271417151.bin`
Step 4  Copy the ASDM image to the standby unit; be sure to specify the same path as for the active unit:

```
failover exec mate copy /noconfirm ftp://[user:[password]@]server[/path]asdm_image_name
diskn:[/path]asdm_image_name
```

Example:

```
asa/act# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.bin
```

Step 5  If you are not already in global configuration mode, access global configuration mode:

```
configure terminal
```

Step 6  Show the current boot images configured (up to 4):

```
show running-config boot system
```

Example:

```
asa/act(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 7  Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

```
no boot system diskn:[/path]asa_image_name
```

Example:

```
asa/act(config)# no boot system disk0:/cdisk.bin
asa/act(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 8  Set the ASA image to boot (the one you just uploaded):

```
boot system diskn:[/path]asa_image_name
```

Example:

```
asa/act(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 9  Set the ASDM image to use (the one you just uploaded):

```
asdm image diskn:[/path]asdm_image_name
```

Example:
You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 10
Save the new settings to the startup configuration:
```
write memory
```
These configuration changes are automatically saved on the standby unit.

Step 11
If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the upgrade will fail.
```
no rest-api agent
```

Step 12
Upgrade the ASA FirePOWER module on the standby unit.
For an ASA FirePOWER module managed by ASDM, connect ASDM to the `standby` management IP address. Wait for the upgrade to complete.

Step 13
Reload the standby unit to boot the new image:
```
failover reload-standby
```
Wait for the standby unit to finish loading. Use the `show failover` command to verify that the standby unit is in the Standby Ready state.

Step 14
Force the active unit to fail over to the standby unit.
```
no failover active
```
If you are disconnected from your SSH session, reconnect to the main IP address, now on the new active/former standby unit.

Step 15
Upgrade the ASA FirePOWER module on the former active unit.
For an ASA FirePOWER module managed by ASDM, connect ASDM to the `standby` management IP address. Wait for the upgrade to complete.

Step 16
From the new active unit, reload the former active unit (now the new standby unit).
```
failover reload-standby
```

Example:
```
asa/act# failover reload-standby
```

Note
If you are connected to the former active unit console port, you should instead enter the `reload` command to reload the former active unit.

---

**Upgrade an Active/Standby Failover Pair Using ASDM**

To upgrade the Active/Standby failover pair, perform the following steps.
Before you begin

Place the ASA and ASDM images on your local management computer.

Step 1
Launch ASDM on the standby unit by connecting to the standby IP address.

Step 2
In the main ASDM application window, choose Tools > Upgrade Software from Local Computer. The Upgrade Software dialog box appears.

Step 3
From the Image to Upload drop-down list, choose ASDM.

Step 4
In the Local File Path field, enter the local path to the file on your computer or click Browse Local Files to find the file on your PC.

Step 5
In the Flash File System Path field, enter the path to the flash file system or click Browse Flash to find the directory or file in the flash file system.

Step 6
Click Upload Image. The uploading process might take a few minutes.

When you are prompted to set this image as the ASDM image, click No. You exit the Upgrade tool.

Step 7
Repeat these steps, choosing ASA from the Image to Upload drop-down list.

When you are prompted to set this image as the ASA image, click No. You exit the Upgrade tool.

Step 8
Connect ASDM to the active unit by connecting to the main IP address, and upload the ASDM software, using the same file location you used on the standby unit.

Step 9
When you are prompted to set the image as the ASDM image, click Yes.

You are reminded to exit ASDM and save the configuration. Click OK. You exit the Upgrade tool. Note: You will save the configuration and reload ASDM after you upgrade the ASA software.

Step 10
Upload the ASA software, using the same file location you used for the standby unit.

Step 11
When you are prompted to set the image as the ASA image, click Yes.

You are reminded to reload the ASA to use the new image. Click OK. You exit the Upgrade tool.

Step 12
Click the Save icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the standby unit.

Step 13
If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing Tools > Command Line Interface, and entering no rest-api enable.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14
Upgrade the ASA FirePOWER module on the standby unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the standby management IP address. Wait for the upgrade to complete, and then connect ASDM back to the active unit.

Step 15
Reload the standby unit by choosing Monitoring > Properties > Failover > Status, and clicking Reload Standby.

Stay on the System pane to monitor when the standby unit reloads.

Step 16
After the standby unit reloads, force the active unit to fail over to the standby unit by choosing Monitoring > Properties > Failover > Status, and clicking Make Standby.

ASDM will automatically reconnect to the new active unit.
Step 17

Upgrade the ASA FirePOWER module on the former active unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the standby management IP address. Wait for the upgrade to complete, and then connect ASDM back to the active unit.

Step 18

Reload the (new) standby unit by choosing Monitoring > Properties > Failover > Status, and clicking Reload Standby.

---

Upgrade an Active/Active Failover Pair

Use the CLI or ASDM to upgrade the Active/Active failover pair for a zero downtime upgrade.

Upgrade an Active/Active Failover Pair Using the CLI

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Before you begin

- Perform these steps on the primary unit.
- Perform these steps in the system execution space.
- This procedure uses FTP. For TFTP, HTTP, or other server types, see the copy command in the ASA command reference.

Step 1

On the primary unit in privileged EXEC mode, copy the ASA software to flash memory:

```plaintext
copy ftp://[user:password@]server[/path]/asa_image_name diskn:[/path]/asa_image_name
```

Example:

```plaintext
asa/act/pri# copy ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
disk0:/asa9829-15-1-smp-k8.bin
```

Step 2

Copy the software to the secondary unit; be sure to specify the same path as for the primary unit:

```plaintext
failover exec mate copy /noconfirm ftp://[user:password@]server[/path]/asa_image_name diskn:[/path]/asa_image_name
```

Example:

```plaintext
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin
disk0:/asa9829-15-1-smp-k8.bin
```

Step 3

Copy the ASDM image to the primary unit flash memory:

```plaintext
copy ftp://[user:password@]server[/path]/asdm_image_name diskn:[/path]/asdm_image_name
```

Example:

```plaintext
asa/act/pri# ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
```
Step 4  Copy the ASDM image to the secondary unit; be sure to specify the same path as for the primary unit:

```
failover exec mate copy /noconfirm ftp://[user:password@]server[/path]/asdm_image_name
disk[n][/path]/asdm_image_name
```

Example:

```
asa/act/pri# failover exec mate copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.bin
```

Step 5  If you are not already in global configuration mode, access global configuration mode:

```
configure terminal
```

Step 6  Show the current boot images configured (up to 4):

```
show running-config boot system
```

Example:

```
asa/act/pri(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

Step 7  Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

```
no boot system disk[n][/path]/asa_image_name
```

Example:

```
asa/act/pri(config)# no boot system disk0:/cdisk.bin
asa/act/pri(config)# no boot system disk0:/asa931-smp-k8.bin
```

Step 8  Set the ASA image to boot (the one you just uploaded):

```
boot system disk[n][/path]/asa_image_name
```

Example:

```
asa/act/pri(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 9  Set the ASDM image to use (the one you just uploaded):

```
asdm image disk[n][/path]/asdm_image_name
```

Example:
You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

**Step 10**
Save the new settings to the startup configuration:

```
write memory
```

These configuration changes are automatically saved on the secondary unit.

**Step 11**
If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the upgrade will fail.

```
no rest-api agent
```

**Step 12**
Make both failover groups active on the primary unit:

```
failover active group 1
failover active group 2
```

*Example:*

```
asa/act/pri(config)# failover active group 1
asa/act/pri(config)# failover active group 2
```

**Step 13**
Upgrade the ASA FirePOWER module on the secondary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 `standby` management IP address. Wait for the upgrade to complete.

**Step 14**
Reload the secondary unit to boot the new image:

```
failover reload-standby
```

Wait for the secondary unit to finish loading. Use the `show failover` command to verify that both failover groups are in the Standby Ready state.

**Step 15**
Force both failover groups to become active on the secondary unit:

```
no failover active group 1
no failover active group 2
```

*Example:*

```
asa/act/pri(config)# no failover active group 1
asa/act/pri(config)# no failover active group 2
asa/stby/pri(config)#
```

If you are disconnected from your SSH session, reconnect to the failover group 1 IP address, now on the secondary unit.

**Step 16**
Upgrade the ASA FirePOWER module on the primary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 `standby` management IP address. Wait for the upgrade to complete.

**Step 17**
Reload the primary unit:
failover reload-standby

Example:

asa/act/sec# failover reload-standby

Note  If you are connected to the primary unit console port, you should instead enter the reload command to reload the primary unit.

You may be disconnected from your SSH session.

Step 18  If the failover groups are configured with the preempt command, they automatically become active on their designated unit after the preempt delay has passed.

Upgrade an Active/Active Failover Pair Using ASDM

To upgrade two units in an Active/Active failover configuration, perform the following steps.

Before you begin

• Perform these steps in the system execution space.
• Place the ASA and ASDM images on your local management computer.

Step 1  Launch ASDM on the secondary unit by connecting to the management address in failover group 2.

Step 2  In the main ASDM application window, choose Tools > Upgrade Software from Local Computer.

The Upgrade Software dialog box appears.

Step 3  From the Image to Upload drop-down list, choose ASDM.

Step 4  In the Local File Path field, enter the local path to the file on your computer or click Browse Local Files to find the file on your PC.

Step 5  In the Flash File System Path field, enter the path to the flash file system or click Browse Flash to find the directory or file in the flash file system.

Step 6  Click Upload Image. The uploading process might take a few minutes.

When you are prompted to set this image as the ASDM image, click No. You exit the Upgrade tool.

Step 7  Repeat these steps, choosing ASA from the Image to Upload drop-down list.

When you are prompted to set this image as the ASA image, click No. You exit the Upgrade tool.

Step 8  Connect ASDM to the primary unit by connecting to the management IP address in failover group 1, and upload the ASDM software, using the same file location you used on the secondary unit.

Step 9  When you are prompted to set the image as the ASDM image, click Yes.

You are reminded to exit ASDM and save the configuration. Click OK. You exit the Upgrade tool. Note: You will save the configuration and reload ASDM after you upgrade the ASA software.

Step 10  Upload the ASA software, using the same file location you used for the secondary unit.

Step 11  When you are prompted to set the image as the ASA image, click Yes.
You are reminded to reload the ASA to use the new image. Click OK. You exit the Upgrade tool.

**Step 12**
Click the Save icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the secondary unit.

**Step 13**
If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing Tools > Command Line Interface, and entering no rest-api enable.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

**Step 14**
Make both failover groups active on the primary unit by choosing Monitoring > Failover > Failover Group #, where # is the number of the failover group you want to move to the primary unit, and clicking Make Active.

**Step 15**
Upgrade the ASA FirePOWER module on the secondary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 standby management IP address. Wait for the upgrade to complete, and then connect ASDM back to the primary unit.

**Step 16**
Reload the secondary unit by choosing Monitoring > Failover > System, and clicking Reload Standby.

Stay on the System pane to monitor when the secondary unit reloads.

**Step 17**
After the secondary unit comes up, make both failover groups active on the secondary unit by choosing Monitoring > Failover > Failover Group #, where # is the number of the failover group you want to move to the secondary unit, and clicking Make Standby.

ASDM will automatically reconnect to the failover group 1 IP address on the secondary unit.

**Step 18**
Upgrade the ASA FirePOWER module on the primary unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the failover group 1 or 2 standby management IP address. Wait for the upgrade to complete, and then connect ASDM back to the secondary unit.

**Step 19**
Reload the primary unit by choosing Monitoring > Failover > System, and clicking Reload Standby.

**Step 20**
If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. ASDM will automatically reconnect to the failover group 1 IP address on the primary unit.

---

**Upgrade an ASA Cluster**

Use the CLI or ASDM to upgrade the ASA Cluster for a zero downtime upgrade.

**Upgrade an ASA Cluster Using the CLI**

To upgrade all units in an ASA cluster, perform the following steps. This procedure uses FTP. For TFTP, HTTP, or other server types, see the copy command in the ASA command reference.

**Before you begin**

- Perform these steps on the master unit. If you are also upgrading the ASA FirePOWER module, then you need console or ASDM access on each slave unit. You can configure the ASA prompt to show the cluster unit and state (master or slave), which is useful to determine which unit you are connected to. See the prompt command. Alternatively, enter the show cluster info command to view each unit's role.
You must use the console port; you cannot enable or disable clustering from a remote CLI connection.

Perform these steps in the system execution space for multiple context mode.

---

**Step 1**

On the master unit in privileged EXEC mode, copy the ASA software to all units in the cluster.

```
cluster exec copy /noconfirm ftp://[user[:password]@]server[/path]/asa_image_name diskn:[/path]/asa_image_name
```

**Example:**

```
asa/unit1/master# cluster exec copy /noconfirm
ftp://jcrichton:aeryn@10.1.1.1/asa9829-15-1-smp-k8.bin disk0:/asa9829-15-1-smp-k8.bin
```

**Step 2**

Copy the ASDM image to all units in the cluster:

```
cluster exec copy /noconfirm ftp://[user[:password]@]server[/path]/asdm_image_name
diskn:[/path]/asdm_image_name
```

**Example:**

```
asa/unit1/master# cluster exec copy /noconfirm ftp://jcrichton:aeryn@10.1.1.1/asdm-77178271417151.bin
disk0:/asdm-77178271417151.bin
```

**Step 3**

If you are not already in global configuration mode, access it now.

```
configure terminal
```

**Example:**

```
asa/unit1/master# configure terminal
asa/unit1/master(config)#
```

**Step 4**

Show the current boot images configured (up to 4).

```
show running-config boot system
```

**Example:**

```
asa/unit1/master(config)# show running-config boot system
boot system disk0:/cdisk.bin
boot system disk0:/asa931-smp-k8.bin
```

The ASA uses the images in the order listed; if the first image is unavailable, the next image is used, and so on. You cannot insert a new image URL at the top of the list; to specify the new image to be first, you must remove any existing entries, and enter the image URLs in the order desired, according to the next steps.

**Step 5**

Remove any existing boot image configurations so that you can enter the new boot image as your first choice:

```
no boot system diskn:[/path]/asa_image_name
```

**Example:**

```
asa/unit1/master(config)# no boot system disk0:/cdisk.bin
asa/unit1/master(config)# no boot system disk0:/asa931-smp-k8.bin
```
Step 6  Set the ASA image to boot (the one you just uploaded):

```
boot system disk:n:[path]/asa_image_name
```

**Example:**

```bash
asa/unit1/master(config)# boot system disk0://asa9829-15-1-smp-k8.bin
```

Repeat this command for any backup images that you want to use in case this image is unavailable. For example, you can re-enter the images that you previously removed.

Step 7  Set the ASDM image to use (the one you just uploaded):

```
asdm image disk:n:[path]/asdm_image_name
```

**Example:**

```bash
asa/unit1/master(config)# asdm image disk0:/asdm-77178271417151.bin
```

You can only configure one ASDM image to use, so you do not need to first remove the existing configuration.

Step 8  Save the new settings to the startup configuration:

```
write memory
```

These configuration changes are automatically saved on the slave units.

Step 9  If you are upgrading ASA FirePOWER modules, disable the ASA REST API or else the ASA FirePOWER module upgrade will fail.

```
no rest-api agent
```

Step 10 If you are upgrading ASA FirePOWER modules that are managed by ASDM, you will need to connect ASDM to the individual management IP addresses, so you need to note the IP addresses for each unit.

```
show running-config interface management_interface_id
```

Note the `cluster-pool poolname` used.

```
show ip[v6] local pool poolname
```

Note the cluster unit IP addresses.

**Example:**

```bash
asa/unit2/slave# show running-config interface gigabitethernet0/0
!
interface GigabitEthernet0/0
  management-only
  nameif inside
  security-level 100
  ip address 10.86.118.1 255.255.252.0 cluster-pool inside-pool
asa/unit2/slave# show ip local pool inside-pool
Begin   End     Mask     Free Held In use
10.86.118.16 10.86.118.17 255.255.252.0 0 0 2

Cluster Unit   IP Address Allocated
unit2          10.86.118.16
unit1          10.86.118.17
asa1/unit2/slave#
```
Step 11 Upgrade the slave units.

Choose the procedure below depending on whether you are also upgrading ASA FirePOWER modules. The ASA FirePOWER procedures minimize the number of ASA reloads when also upgrading the ASA FirePOWER module. You can choose to use the slave Console or ASDM for these procedures. You may want to use ASDM instead of the Console if you do not have ready access to all of the console ports but can reach ASDM over the network.

**Note** During the upgrade process, never use the `cluster master unit` command to force a slave unit to become master; you can cause network connectivity and cluster stability-related problems. You must upgrade and reload all slave units first, and then continue with this procedure to ensure a smooth transition from the current master unit to a new master unit.

**If you do not have ASA FirePOWER module upgrades:**

a) On the master unit, to view member names, enter `cluster exec unit ?`, or enter the `show cluster info` command.

b) Reload a slave unit.

   ```
   cluster exec unit slave-unit reload noconfirm
   ```

   **Example:**

   ```
   asa/unit1/master# cluster exec unit unit2 reload noconfirm
   ```

c) Repeat for each slave unit.

   To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, enter `show cluster info`.

**If you also have ASA FirePOWER module upgrades (using the slave Console):**

a) Connect to the console port of a slave unit, and enter global configuration mode.

   ```
   enable
   configure terminal
   ```

   **Example:**

   ```
   asa/unit2/slave> enable
   Password:
   asa/unit2/slave# configure terminal
   asa/unit2/slave(config)#
   ```

b) Disable clustering.

   ```
   cluster group name
   no enable
   ```

   Do not save this configuration; you want clustering to be enabled when you reload. You need to disable clustering to avoid multiple failures and rejoins during the upgrade process; this unit should only rejoin after all of the upgrading and reloading is complete.

   **Example:**

   ```
   asa/unit2/slave(config)# cluster group cluster1
   asa/unit2/slave(cfg-cluster)# no enable
   Cluster disable is performing cleanup..done.
   ```
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.

Cluster unit unit2 transitioned from SLAVE to DISABLED
asa/unit2/ClusterDisabled(cfg-cluster)#

c) Upgrade the ASA FirePOWER module on this slave unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the individual management IP address that you noted earlier. Wait for the upgrade to complete.

d) Reload the slave unit.
   
   reload noconfirm

e) Repeat for each slave unit.
   
   To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, enter show cluster info.

If you also have ASA FirePOWER module upgrades (using ASDM):

a) Connect ASDM to the individual management IP address of this slave unit that you noted earlier.

b) Choose Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Configuration > .

c) Uncheck the Participate in ASA cluster check box.
   
   You need to disable clustering to avoid multiple failures and rejoins during the upgrade process; this unit should only rejoin after all of the upgrading and reloading is complete.
   
   Do not uncheck the Configure ASA cluster settings check box; this action clears all cluster configuration, and also shuts down all interfaces including the management interface to which ASDM is connected. To restore connectivity in this case, you need to access the CLI at the console port.

   
   Note Some older versions of ASDM do not support disabling the cluster on this screen; in this case, use the Tools > Command Line Interface tool, click the Multiple Line radio button, and enter cluster group name and no enable. You can view the cluster group name in the Home > Device Dashboard > Device Information > ASA Cluster area.

d) Click Apply.

   
   e) You are prompted to exit ASDM. Reconnect ASDM to the same IP address.

   
   f) Upgrade the ASA FirePOWER module.

   Wait for the upgrade to complete.

   
   g) In ASDM, choose Tools > System Reload.

   
   h) Click the Reload without saving the running configuration radio button.

   
   You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.

   
   i) Click Schedule Reload.

   
   j) Click Yes to continue the reload.

   
   k) Repeat for each slave unit.
To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the **Monitoring > ASA Cluster > Cluster Summary** pane on the master unit.

**Step 12** Upgrade the master unit.

a) Disable clustering.

```
cluster group name
no enable
```

Wait for 5 minutes for a new master unit to be selected and traffic to stabilize.

Do not save this configuration; you want clustering to be enabled when you reload.

We recommend manually disabling cluster on the master unit if possible so that a new master unit can be elected as quickly and cleanly as possible.

**Example:**

```
asa/unit1/master(config)# cluster group cluster1
asa/unit1/master(cfg-cluster)# no enable
Cluster disable is performing cleanup..done.
All data interfaces have been shutdown due to clustering being disabled. To recover either enable clustering or remove cluster group configuration.
Cluster unit unit1 transitioned from MASTER to DISABLED
asa/unit1/ClusterDisabled(cfg-cluster)#
```

b) Upgrade the ASA FirePOWER module on this unit.

For an ASA FirePOWER module managed by ASDM, connect ASDM to the individual management IP address that you noted earlier. The main cluster IP address now belongs to the new master unit; this former master unit is still accessible on its individual management IP address.

Wait for the upgrade to complete.

c) Reload this unit.

```
reload noconfirm
```

When the former master unit rejoins the cluster, it will be a slave unit.

---

**Upgrade an ASA Cluster Using ASDM**

To upgrade all units in an ASA cluster, perform the following steps.

**Before you begin**

- Perform these steps on the master unit. If you are also upgrading the ASA FirePOWER module, then you need ASDM access to each slave unit.
- Perform these steps in the system execution space for multiple context mode.
- Place the ASA and ASDM images on your local management computer.
Step 1  Launch ASDM on the master unit by connecting to the main cluster IP address. This IP address always stays with the master unit.

Step 2  In the main ASDM application window, choose Tools > Upgrade Software from Local Computer. The Upgrade Software from Local Computer dialog box appears.

Step 3  Click the All devices in the cluster radio button. The Upgrade Software dialog box appears.

Step 4  From the Image to Upload drop-down list, choose ASDM.

Step 5  In the Local File Path field, click Browse Local Files to find the file on your computer.

Step 6  (Optional) In the Flash File System Path field, enter the path to the flash file system or click Browse Flash to find the directory or file in the flash file system. By default, this field is prepopulated with the following path: disk0:filename.

Step 7  Click Upload Image. The uploading process might take a few minutes.

Step 8  You are prompted to set this image as the ASDM image. Click Yes.

Step 9  You are reminded to exit ASDM and save the configuration. Click OK.

You exit the Upgrade tool. Note: You will save the configuration and reload ASDM after you upgrade the ASA software.

Step 10  Repeat these steps, choosing ASA from the Image to Upload drop-down list.

Step 11  Click the Save icon on the toolbar to save your configuration changes.

These configuration changes are automatically saved on the slave units.

Step 12  Take note of the individual management IP addresses for each unit on Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Members so that you can connect ASDM directly to slave units later.

Step 13  If you are upgrading ASA FirePOWER modules, disable the ASA REST API by choosing Tools > Command Line Interface, and entering no rest-api enable.

If you do not disable the REST API, the ASA FirePOWER module upgrade will fail.

Step 14  Upgrade the slave units.

Choose the procedure below depending on whether you are also upgrading ASA FirePOWER modules. The ASA FirePOWER procedure minimizes the number of ASA reloads when also upgrading the ASA FirePOWER module.

Note During the upgrade process, never use the Monitoring > ASA Cluster > Cluster Summary > Change Master To drop-down list to force a slave unit to become master; you can cause network connectivity and cluster stability-related problems. You must reload all slave units first, and then continue with this procedure to ensure a smooth transition from the current master unit to a new master unit.

If you do not have ASA FirePOWER module upgrades:

a) On the master unit, choose Tools > System Reload.
b) Choose a slave unit name from the Device drop-down list.
c) Click Schedule Reload.
d) Click Yes to continue the reload.
e) Repeat for each slave unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the Monitoring > ASA Cluster > Cluster Summary pane.

If you also have ASA FirePOWER module upgrades:

a) On the master unit, choose Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Members.
b) Select the slave unit that you want to upgrade, and click Delete.
c) Click Apply.
d) Exit ASDM, and connect ASDM to the slave unit by connecting to its individual management IP address that you noted earlier.
e) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.
f) In ASDM, choose Tools > System Reload.
g) Click the Reload without saving the running configuration radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.
h) Click Schedule Reload.
i) Click Yes to continue the reload.
j) Repeat for each slave unit.

To avoid connection loss and allow traffic to stabilize, wait for each unit to come back up and rejoin the cluster (approximately 5 minutes) before repeating these steps for the next unit. To view when a unit rejoins the cluster, see the Monitoring > ASA Cluster > Cluster Summary pane.

Step 15

Upgrade the master unit.

a) In ASDM on the master unit, choose Configuration > Device Management > High Availability and Scalability > ASA Cluster > Cluster Configuration pane.
b) Uncheck the Participate in ASA cluster check box, and click Apply.

You are prompted to exit ASDM.
c) Wait for up to 5 minutes for a new master unit to be selected and traffic to stabilize.

When the former master unit rejoins the cluster, it will be a slave unit.
d) Re-connect ASDM to the former master unit by connecting to its individual management IP address that you noted earlier.

The main cluster IP address now belongs to the new master unit; this former master unit is still accessible on its individual management IP address.
e) Upgrade the ASA FirePOWER module.

Wait for the upgrade to complete.
f) Choose Tools > System Reload.
g) Click the Reload without saving the running configuration radio button.

You do not want to save the configuration; when this unit reloads, you want clustering to be enabled on it.
h) Click Schedule Reload.
Upgrade an ASA FirePOWER Module

Use this procedure to upgrade an ASA FirePOWER module managed by an FMC. When you upgrade the module depends on whether you are upgrading ASA, and on your ASA deployment.

- Upgrading standalone ASA devices: If you are also upgrading ASA, use the FMC to upgrade the ASA FirePOWER module just after you upgrade ASA and reload.
- Upgrading ASA clusters and failover pairs: To avoid interruptions in traffic flow and inspection, fully upgrade these devices one at a time. If you are also upgrading ASA, use the FMC to upgrade the ASA FirePOWER module just before you reload each unit to upgrade ASA.

For more information, see Upgrade Path: ASA FirePOWER, on page 81 and the ASA upgrade procedures.

Caution

Do not deploy changes to or from, manually reboot, or shut down an upgrading appliance. Do not restart an upgrade in progress. The upgrade process may appear inactive during prechecks; this is expected. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, contact Cisco TAC.

Before you begin

Check your place in the upgrade path, including ASA and FMC upgrades. Make sure you have fully planned and prepared for this step.

Step 1

Deploy configurations to the devices you are about to upgrade.

On the FMC menu bar, click Deploy. Choose devices, then click Deploy again. Deploying before you upgrade reduces the chance of failure.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, deploying some configurations restarts Snort, which interrupts traffic inspection and, depending on how your device handles traffic, may interrupt traffic until the restart completes. For more information, see ASA FirePOWER Upgrade Behavior, on page 230.

Step 2

(Upgrading to Version 6.1+) Disable the ASA REST API.

If you do not disable the REST API, the upgrade will fail. Note that ASA 5506-X series devices do not support the ASA REST API if you are also running Version 6.0+ of the ASA FirePOWER module.

Use the CLI on the ASA to disable the REST API:

no rest-api agent

You can reenable it after the upgrade:

rest-api agent
Step 3  Perform final preupgrade checks.

- Check health: Use the Message Center (click the System Status icon on the menu bar). Make sure the appliances in your deployment are successfully communicating and that there are no issues reported by the health monitor.

- Running tasks: Also in the Message Center, make sure essential tasks are complete. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. You can manually delete failed status messages later.

- Check disk space: Perform a final disk space check. Without enough free disk space, the upgrade fails. For disk space requirements, see Time Tests and Disk Space Requirements, on page 185.

Step 4  Choose System > Updates.

Step 5  Click the Install icon next to the upgrade package you want to use and choose the devices to upgrade.

If the devices you want to upgrade are not listed, you chose the wrong upgrade package.

Note  We strongly recommend upgrading no more than five devices simultaneously. The FMC does not allow you to stop the upgrade until all selected devices complete the process. If there is an issue with any one device upgrade, all devices must finish upgrading before you can resolve the issue.

Step 6  Click Install, then confirm that you want to upgrade and reboot the devices.

Traffic either drops throughout the upgrade or traverses the network without inspection depending on how your devices are configured and deployed. For more information, see ASA FirePOWER Upgrade Behavior, on page 230.

Step 7  Monitor upgrade progress in the Message Center.

Do not deploy configurations to the device while it is upgrading. Even if the Message Center shows no progress for several minutes or indicates that the upgrade has failed, do not restart the upgrade or reboot the device. Instead, contact Cisco TAC.

Step 8  Verify success.

After the upgrade completes, choose Devices > Device Management and confirm that the devices you upgraded have the correct software version.

Step 9  Use the Message Center to recheck deployment health.

Step 10  Update intrusion rules (SRU) and the vulnerability database (VDB).

If the SRU or the VDB available on the Cisco Support & Downloads site is newer than the version currently running, install the newer version. For more information, see the Firepower Management Center Configuration Guide. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 11  Complete any post-upgrade configuration changes described in the release notes.

Step 12  Redeploy configurations to the devices you just upgraded.
Upgrade an ASA FirePOWER Module
PART III

Reference

- Compatibility, on page 111
- Example Upgrade Paths, on page 127
- Upgrade Guidelines and Warnings by Version, on page 137
- Time Tests and Disk Space Requirements, on page 185
- Traffic Flow, Inspection, and Device Behavior, on page 223
Compatibility

The following topics provide Cisco Firepower software and hardware compatibility, including operating system and hosting environment requirements, for each supported Firepower version.

**Note**
This guide provides compatibility information relevant to the upgrade process. For additional information, see the Cisco Firepower Compatibility Guide.

- Firepower Management Centers, on page 111
- Firepower Devices, on page 115
- Bundled Components, on page 122

Firepower Management Centers

About Firepower Management Centers

With an FMC, you can manage devices running:

- The *same major version* as the FMC, including patches.

  Although you can manage a patched device with an unpatched FMC, new features and resolved issues often require the latest patch on both the FMC and its managed devices. We *strongly* recommend that you patch your entire deployment.

- *Some older major versions* and patches to those major versions.

  Although you can manage an older device with a newer FMC, you cannot fully take advantage of new features and bug fixes until you upgrade both.

This table lists major FMC versions, and the major versions of devices they can manage. Find your current major version in the first column, then read across to determine which devices you can manage.
### Table 20: FMC-Device Version Compatibility

<table>
<thead>
<tr>
<th>FMC Version</th>
<th>Device Version</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.6.0</td>
</tr>
<tr>
<td>6.6.0</td>
<td>Yes</td>
</tr>
<tr>
<td>6.5.0</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2</td>
<td>—</td>
</tr>
<tr>
<td>6.2.1</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0</td>
<td>—</td>
</tr>
<tr>
<td>6.0.1</td>
<td>—</td>
</tr>
<tr>
<td>6.0.0</td>
<td>—</td>
</tr>
<tr>
<td>5.4.1</td>
<td>—</td>
</tr>
<tr>
<td>5.4.0</td>
<td>—</td>
</tr>
</tbody>
</table>

* A device must be running at least Version 5.4.0.2/5.4.1.1 to be managed by a Version 6.0, 6.0.1, or 6.1 FMC.

### Firepower Management Centers: Physical

### Table 21: Firepower Management Center Compatibility

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>FMC 1600</th>
<th>FMC 2600</th>
<th>FMC 1000</th>
<th>FMC 2500</th>
<th>FMC 4600</th>
<th>FMC 3500</th>
<th>FMC 4500</th>
<th>FMC 2000</th>
<th>FMC 1500</th>
<th>FMC 4000</th>
<th>DC 500</th>
<th>DC 1000</th>
<th>DC 3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.5.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
### Firepower Management Centers: Virtual

These tables lists Firepower compatibility and virtual hosting environment requirements for FMCv. Note that support for FMCv 300 on VMware begins in Version 6.5.0.

**Table 22: Firepower Management Center Virtual Compatibility: Version 6.0+**

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>VMware vSphere/VMware ESXi</th>
<th>Amazon Web Services (AWS)</th>
<th>Kernel-Based Virtual Machine (KVM)</th>
<th>Microsoft Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.0</td>
<td>Yes Yes Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.5.0</td>
<td>Yes Yes Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.4.0</td>
<td>— Yes Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.3.0</td>
<td>— Yes Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3</td>
<td>— Yes Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2</td>
<td>— — Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.2.1</td>
<td>— — Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>— — Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0</td>
<td>— — Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>FMC 1600 FMC 2600 FMC 4600</th>
<th>FMC 1000 FMC 2500 FMC 4500</th>
<th>FMC 2000 FMC 4000</th>
<th>FMC 750 FMC 1500 FMC 3500</th>
<th>DC 500 DC 1000 DC 3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>— Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>6.2.0</td>
<td>— Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>6.1.0</td>
<td>— —</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>6.0.1</td>
<td>— —</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>6.0.0</td>
<td>— —</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td></td>
</tr>
<tr>
<td>5.4.1</td>
<td>— —</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td>5.4.0</td>
<td>5.4.0 only; use 5.4.1.x Defense Centers to manage 5.4.x devices.</td>
<td>— —</td>
<td>Yes</td>
<td>Yes</td>
<td></td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>FMC 2000 FMC 4000</th>
<th>FMC 750 FMC 1500 FMC 3500</th>
<th>DC 500 DC 1000 DC 3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>— Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>— Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0</td>
<td>— —</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.0.1</td>
<td>— —</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.0.0</td>
<td>— —</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>5.4.1</td>
<td>— —</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>5.4.0</td>
<td>5.4.0 only; use 5.4.1.x Defense Centers to manage 5.4.x devices.</td>
<td>— —</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>DC 500 DC 1000 DC 3000</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.1</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0</td>
<td>—</td>
</tr>
</tbody>
</table>

---

Note: Firepower Management Centers: Virtual

Reference
Table 23: FireSIGHT Defense Center Virtual Compatibility: Version 5.4

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>VMware vSphere/VMware ESXi</th>
<th>Amazon Web Services (AWS)</th>
<th>Kernel-Based Virtual Machine (KVM)</th>
<th>Microsoft Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.0.1</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.0.0</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
</tbody>
</table>

Table 24: BIOS and Firmware Minimum Requirements

<table>
<thead>
<tr>
<th>Platform</th>
<th>Firepower Version</th>
<th>BIOS</th>
<th>RAID Controller Firmware</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC 1000, 2500, 4500</td>
<td>6.2.3+</td>
<td>C220M4.4.0.2d.0</td>
<td>24.12.1-0433</td>
</tr>
<tr>
<td>FMC 2000, 4000</td>
<td>6.2.3+</td>
<td>C220M3.2.0.8.0</td>
<td>23.33.0-0049</td>
</tr>
</tbody>
</table>

To determine the current versions on an FMC, run these commands from the Linux shell/expert mode:

- BIOS: `sudo dmidecode -t bios -q`
- RAID controller firmware (FMC 4500): `sudo MegaCLI -AdpAllInfo -aALL | grep "FW Package"`
- RAID controller firmware (all other models): `sudo storcli /c0 show | grep "FW Package"`

If the FMC does not meet the minimum requirements, apply Firepower Management Center BIOS Update Hotfix CJ. Applying the hotfix is the only way to update the BIOS and RAID controller firmware. Upgrading the Firepower software does not accomplish this task, nor does reimaging.

Note that Hotfix CJ also updates the CIMC firmware. Although we do not support changing configurations on the FMC using CIMC, if you have concerns, apply the hotfix. If the FMC is already up to date, the hotfix has no effect.
The hotfix is available on the Cisco Support & Download site, in the same location as the upgrade and installation packages for your current major version. Use the regular upgrade page (System > Updates) to apply the hotfix. For hotfix release notes, see Cisco Firepower Hotfix Release Notes.

Regardless of the FMC’s current Firepower version and which Hotfix CJ package you upload, the FMC web interface lists it as Hotfix CJ Version 6.7.0. This is expected behavior and the hotfix is safe to apply to all Version 6.2.3+ FMCs.

Firepower Devices

About Firepower Devices

A Firepower device can run either Firepower Threat Defense or NGIPS software. Note that you can deploy some ASA models as either FTD or NGIPS (ASA FirePOWER).

Table 25: Device Software Types

<table>
<thead>
<tr>
<th>Device Software</th>
<th>Firepower Version</th>
<th>Implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower Threat Defense</td>
<td>Version 6.0.1+ with FMC</td>
<td>Physical or virtual device</td>
</tr>
<tr>
<td></td>
<td>Version 6.1.0+ with FDM</td>
<td></td>
</tr>
<tr>
<td>NGIPS: Firepower (classic/legacy)</td>
<td>Any</td>
<td>Physical or virtual device</td>
</tr>
<tr>
<td>NGIPS: ASA FirePOWER</td>
<td>Any</td>
<td>A separately installed module on an ASA device. Traffic is sent to the module after ASA firewall policies are applied. You cannot use an FMC to manage ASA firewall functions.</td>
</tr>
</tbody>
</table>

You can manage a Firepower device either locally (FDM/ASDM) or remotely (FMC). You can use only one management method for a device at a time.

Table 26: Device Management Methods

<table>
<thead>
<tr>
<th>To Manage...</th>
<th>Use...</th>
<th>Compatibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multiple devices running FTD, NGIPS, or both.</td>
<td>Firepower Management Center</td>
<td>The FMC must be running at least the same major version as its devices. For more information, see About Firepower Management Centers, on page 111.</td>
</tr>
<tr>
<td>One FTD device</td>
<td>Firepower Device Manager (Version 6.1.0+)</td>
<td>FDM is built into Firepower Threat Defense. There is no concept of manager-device compatibility in this type of deployment.</td>
</tr>
</tbody>
</table>
Firepower 1000/2100 Series with FTD

Firepower 1000 and Firepower 2100 series devices use the FXOS operating system. Upgrading Firepower Threat Defense automatically upgrades FXOS. For information on the FXOS version bundled with each Firepower version, see Bundled Components, on page 122.

These devices can also run ASA instead of FTD. For more information, see Cisco ASA Compatibility.

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>Firepower 2110</th>
<th>Firepower 2120</th>
<th>Firepower 2130</th>
<th>Firepower 2140</th>
<th>Firepower 1010</th>
<th>Firepower 1120</th>
<th>Firepower 1140</th>
<th>Firepower 1150</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.0</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.5.0</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.1</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

Firepower 4100/9300 with FTD

For the Firepower 4100/9300 chassis, major Firepower versions have a specially qualified and recommended companion FXOS version, listed below in bold. Use these combinations whenever possible, because we perform enhanced testing for them.

These devices can also run ASA instead of FTD. With ASA 9.12+ and FTD 6.4+, you can run both ASA and FTD on separate modules in the same Firepower 9300 chassis. For more information, see Cisco Firepower 4100/9300 FXOS Compatibility.
To perform flow offload in the following major version sequences, you must be running a specific combination of Firepower and FXOS:

- Version 6.2.2.x: Version 6.2.2.2+ on FXOS 2.3.1.130+
- Version 6.2.0.x: Version 6.2.0.3+ on either FXOS 2.2.1.x or FXOS 2.2.2, builds 17-86

### Table 28: Firepower 4100/9300 Compatibility

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>FXOS Version</th>
<th>Firepower 9300</th>
<th>Firepower 4100 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>SM-26</td>
<td>SM-36</td>
</tr>
<tr>
<td>6.6.0</td>
<td>2.8.1.105+</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.5.0</td>
<td>2.7.1.92+</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>2.8.1.105+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.4.0</td>
<td>2.6.1.157+</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>2.7.1.92+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.8.1.105+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.3.0</td>
<td>2.4.1.214+</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>2.6.1.157+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.7.1.92+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.8.1.105+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.3</td>
<td>2.3.1.73+</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>2.4.1.214+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.6.1.157+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.7.1.92+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.8.1.105+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.2</td>
<td>2.2.2.x</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>2.3.1.73+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.4.1.214+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.6.1.157+</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2.7.1.92+</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
ASA 5500-X Series and ISA 3000 with FTD

ASA 5500-X series and ISA 3000 devices use the ASA operating system. Upgrading Firepower Threat Defense automatically upgrades ASA. For information on the ASA version bundled with each Firepower version, see Bundled Components, on page 122.

Table 29: ASA 5500-X Series and ISA 3000 Compatibility

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>FXOS Version</th>
<th>Firepower 9300</th>
<th>Firepower 4100 Series</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>SM-26 SM-36 SM-44</td>
<td>SM-40 SM-48 SM-56</td>
</tr>
<tr>
<td>6.2.0</td>
<td>2.1.1.x, 2.2.1.x, 2.2.2.x 2.3.1.73+ 2.4.1.214+ 2.6.1.157+</td>
<td>Yes —</td>
<td>Yes Yes</td>
</tr>
<tr>
<td>6.1.0</td>
<td>2.0.1.x 2.1.1.x 2.3.1.73+</td>
<td>Yes —</td>
<td>Yes Yes</td>
</tr>
<tr>
<td>6.0.1</td>
<td>1.1.4.x 2.0.1.x</td>
<td>Yes —</td>
<td>Yes —</td>
</tr>
</tbody>
</table>

ASA 5500-X Series and ISA 3000 with FTD

ASA 5500-X series and ISA 3000 devices use the ASA operating system. Upgrading Firepower Threat Defense automatically upgrades ASA. For information on the ASA version bundled with each Firepower version, see Bundled Components, on page 122.

Table 29: ASA 5500-X Series and ISA 3000 Compatibility

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>ASA 5508-X</th>
<th>ISA 3000</th>
<th>ASA 5515-X</th>
<th>ASA 5506-X</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>ASA 5516-X</td>
<td></td>
<td>ASA 5525-X</td>
<td>ASA 5545-X</td>
</tr>
<tr>
<td></td>
<td>ASA 5555-X</td>
<td></td>
<td>ASA 5515-X</td>
<td>ASA 5506-H-X</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ASA 5506W-X</td>
<td>ASA 5512-X</td>
</tr>
<tr>
<td>6.6.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.5.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.3.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.2.3</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.2.2</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.2.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>Yes</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Firepower Threat Defense Virtual

This table lists Firepower compatibility and virtual hosting environment requirements for FTDv.

Table 30: Firepower Threat Defense Virtual Compatibility

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>VMware vSphere/VMware ESXi</th>
<th>Amazon Web Services (AWS)</th>
<th>Kernel-Based Virtual Machine (KVM)</th>
<th>Microsoft Azure</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.7</td>
<td>6.5</td>
<td>6.0</td>
<td>5.5</td>
</tr>
<tr>
<td></td>
<td>6.5.0</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>6.4.0</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>6.3.0</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>6.2.3</td>
<td>—</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>6.2.2</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>6.2.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>6.2.0</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>6.1.0</td>
<td>—</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>6.0.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

Firepower 7000/8000 Series and Legacy Devices

This table lists Firepower compatibility with 7000/8000 series devices, AMP models, and legacy device platforms.

Table 31: Firepower 7000/8000 Series Compatibility

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>7000/8000 Series (Includes AMP)</th>
<th>Series 2 (Legacy)</th>
<th>Cisco NGIPS for Blue Coat X-Series (Legacy)</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.4.0</td>
<td>Yes</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>
ASA 5500-X Series and ISA 3000 with FirePOWER Services

The ASA FirePOWER module runs on the separately upgraded ASA operating system. There is wide compatibility between ASA and ASA FirePOWER versions. However, even if an ASA upgrade is not strictly required, resolving issues may require an upgrade to the latest supported version.

Note

If you are running Firepower 5.4.0 through 6.0.1, due to CSCuc91730, we recommend you upgrade to ASA 9.2(4.5)+, 9.3(3.8)+, 9.4(2)+, or later major version.

This table lists ASA FirePOWER compatibility with ASA device models, ASA OS versions, and ASDM. If you are using an FMC to manage your ASA FirePOWER modules, you can ignore the ASDM requirements. Note that the Firepower captive portal feature requires at least ASA FirePOWER Version 6.0.0 on ASA 9.5(2).

Table 32: ASA with FirePOWER Services Compatibility

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>Min. ASDM Version</th>
<th>ASA Model and Supported ASA Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.0</td>
<td>7.14(1)</td>
<td>9.5(2)+</td>
</tr>
<tr>
<td>6.5.0</td>
<td>7.13(1)</td>
<td>9.5(2)+</td>
</tr>
<tr>
<td>6.4.0</td>
<td>7.12(1)</td>
<td>9.5(2)+</td>
</tr>
</tbody>
</table>
# ASA Model and Supported ASA Versions

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6.3.0</td>
<td>7.10(1)</td>
<td>9.5(2)+</td>
<td>9.5(2)+</td>
<td>9.5(2)+</td>
<td>9.5(2) to 9.12(x)</td>
<td>—</td>
<td>—</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.3</td>
<td>7.9(2)</td>
<td>—</td>
<td>9.5(2)+</td>
<td>9.5(2)+</td>
<td>9.5(2) to 9.12(x)</td>
<td>9.5(2) to 9.9(x)</td>
<td>9.6(x) to 9.9(x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.2</td>
<td>7.8(2)</td>
<td>—</td>
<td>9.5(2)+</td>
<td>9.5(2)+</td>
<td>9.5(2) to 9.12(x)</td>
<td>9.5(2) to 9.9(x)</td>
<td>9.6(x) to 9.9(x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.2.0</td>
<td>7.7(1)</td>
<td>—</td>
<td>9.5(2)+</td>
<td>9.5(2)+</td>
<td>9.5(2) to 9.12(x)</td>
<td>9.5(2) to 9.9(x)</td>
<td>9.6(x) to 9.9(x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.0</td>
<td>7.6(2)</td>
<td>—</td>
<td>9.5(2)+</td>
<td>9.5(2)+</td>
<td>9.5(2) to 9.12(x)</td>
<td>9.5(2) to 9.9(x)</td>
<td>9.6(x) to 9.9(x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.0.1</td>
<td>7.6(1) req. ASA 9.5(1.5)+</td>
<td>—</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
</tr>
<tr>
<td>6.0.0</td>
<td>7.5(1.112) req. ASA 9.5(1.5)+</td>
<td>—</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td>9.5(1.5) to 9.6(x)</td>
<td></td>
</tr>
<tr>
<td>5.4.1</td>
<td>7.5(1.112) 9.5(1.5)+ 9.4(1.225)+</td>
<td>9.5(1.5)+ 9.4(x)</td>
<td>9.5(1.5)+ 9.4(x)</td>
<td>—</td>
<td>—</td>
<td>9.5(1.5) to 9.9(x)</td>
<td>9.3(2) to 9.9(x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7.4(1)</td>
<td>—</td>
<td>9.5(1.5)+ 9.4(x)</td>
<td>—</td>
<td>—</td>
<td>9.5(1.5) to 9.9(x)</td>
<td>9.3(2) to 9.9(x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>7.3(3)</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>9.5(1.5) to 9.9(x)</td>
<td>9.3(2) to 9.9(x)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.4.0.2+</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>9.5(1.5)+ 9.3(2) to 9.4(x)</td>
<td>9.5(1.5) to 9.12(x)</td>
<td>9.5(1.5) to 9.9(x)</td>
<td>9.5(1.5) to 9.9(x)</td>
<td>9.3(2) to 9.4(x)</td>
<td></td>
</tr>
<tr>
<td>5.4.0 only</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>9.2(2.4), 9.2(3), 9.2(4)</td>
<td>9.2(2.4), 9.2(3), 9.2(4)</td>
<td>9.2(2.4), 9.2(3), 9.2(4)</td>
<td>—</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**NGIPSv**

This table lists Firepower compatibility and virtual hosting environment requirements for NGIPSv (virtual NGIPS devices running on VMware).
### Table 33: NGIPSv Compatibility

<table>
<thead>
<tr>
<th>Firepower Version</th>
<th>VMware vSphere/VMware ESXi</th>
<th>VMware vCloud Director</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>6.7</td>
<td>6.5</td>
</tr>
<tr>
<td>6.6.0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.5.0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>6.4.0</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>6.3.0</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>6.2.3</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>6.2.2</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.1</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.0.1</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.0.0</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>5.4.0</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

### Bundled Components

This table lists the versions of various components bundled with Firepower releases. Use this information to identify open or resolved caveats in bundled components that may affect your Firepower deployment.

### Table 34: Bundled Components

<table>
<thead>
<tr>
<th>Firepower</th>
<th>ASA (ASA 5500-X Series with FTD)</th>
<th>FXOS (Firepower 1000/2100 Series with FTD)</th>
<th>Snort</th>
<th>GeoDB</th>
<th>VDB</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6.0</td>
<td>9.14(1.1)</td>
<td>2.8.1.105</td>
<td>2.9.16-140</td>
<td>2019-06-03-002</td>
<td>4.5.0-328</td>
</tr>
<tr>
<td>6.5.0.4</td>
<td>9.13(1.5)</td>
<td>2.7.1.117</td>
<td>2.9.15-15201</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.5.0.3</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.5.0.2</td>
<td>9.13(1.151)</td>
<td>2.7.1.115</td>
<td>2.9.15-15101</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.5.0.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.5.0</td>
<td>9.13(1)</td>
<td>2.7.1.107</td>
<td>2.9.15-7</td>
<td>2019-06-03-002</td>
<td>4.5.0-309</td>
</tr>
<tr>
<td>Firepower</td>
<td>ASA (ASA 5500-X Series with FTD)</td>
<td>FXOS (Firepower 1000/2100 Series with FTD)</td>
<td>Snort</td>
<td>GeoDB</td>
<td>VDB</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------------------------</td>
<td>-------------------------------------------</td>
<td>-------</td>
<td>-------</td>
<td>-----</td>
</tr>
<tr>
<td>6.4.0.8</td>
<td>9.12(2.18)</td>
<td>2.6.1.166</td>
<td>2.9.14-15707</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0.7</td>
<td>9.12(2.151)</td>
<td>2.6.1.156</td>
<td>2.9.14-15605</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0.6</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0.5</td>
<td>9.12(2.4)</td>
<td>2.6.1.144</td>
<td>2.9.14-15507</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0.4</td>
<td>9.12(2.4)</td>
<td>2.6.1.144</td>
<td>2.9.12-15301</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0.3</td>
<td>9.12(1.12)</td>
<td>2.6.1.133</td>
<td>2.9.14-15301</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0.2</td>
<td>9.12(1.10)</td>
<td>2.6.1.133</td>
<td>2.9.14-15209</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0.1</td>
<td>9.12(1.7)</td>
<td>2.6.1.133</td>
<td>2.9.14-15100</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.4.0</td>
<td>9.12(1.6)</td>
<td>2.6.1.133</td>
<td>2.9.14-15003</td>
<td>2018-07-09-002</td>
<td>4.5.0-309</td>
</tr>
<tr>
<td>6.3.0.5</td>
<td>9.10(1.31)</td>
<td>2.4.1.255</td>
<td>2.9.13-15503</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0.4</td>
<td>9.10(1.28)</td>
<td>2.4.1.248</td>
<td>2.9.13-15409</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0.3</td>
<td>9.10(1.18)</td>
<td>2.4.1.237</td>
<td>2.9.13-15307</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0.2</td>
<td>9.10(1.12)</td>
<td>2.4.1.237</td>
<td>2.9.13-15211</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0.1</td>
<td>9.10(1.8)</td>
<td>2.4.1.222</td>
<td>2.9.13-15101</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.3.0</td>
<td>9.10(1.3)</td>
<td>2.4.1.216</td>
<td>2.9.13-15013</td>
<td>2018-07-09-002</td>
<td>4.5.0-299</td>
</tr>
<tr>
<td>6.2.3.15</td>
<td>9.9(2.60)</td>
<td>2.3.1.167</td>
<td>2.9.12-1513</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.14</td>
<td>9.9(2.55)</td>
<td>2.3.1.151</td>
<td>2.9.12-1401</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.13</td>
<td>9.9(2.51)</td>
<td>2.3.1.144</td>
<td>2.9.12-1306</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.12</td>
<td>9.9(2.48)</td>
<td>2.3.1.144</td>
<td>2.9.12-1207</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.11</td>
<td>9.9(2.43)</td>
<td>2.3.1.132</td>
<td>2.9.12-1102</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.10</td>
<td>9.9(2.41)</td>
<td>2.3.1.131</td>
<td>2.9.12-902</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.9</td>
<td>9.9(2.37)</td>
<td>2.3.1.122</td>
<td>2.9.12-806</td>
<td>2017-12-12-002</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.8</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.7</td>
<td>9.9(2.32)</td>
<td>2.3.1.118</td>
<td>2.9.12-704</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.6</td>
<td>9.9(2.26)</td>
<td>2.3.1.115</td>
<td>2.9.12-607</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.5</td>
<td>9.9(2.245)</td>
<td>2.3.1.108</td>
<td>2.9.12-506</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.4</td>
<td>9.9(2.15)</td>
<td>2.3.1.108</td>
<td>2.9.12-383</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Firepower</td>
<td>ASA (ASA 5500-X Series with FTD)</td>
<td>FXOS (Firepower 1000/2100 Series with FTD)</td>
<td>Snort</td>
<td>GeoDB</td>
<td>VDB</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------</td>
<td>-------------------------------------------</td>
<td>-------</td>
<td>-------</td>
<td>-----</td>
</tr>
<tr>
<td>6.2.3.3</td>
<td>9.9(2.13)</td>
<td>2.3.1.104</td>
<td>2.9.12-325</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.2</td>
<td>9.9(2.8)</td>
<td>2.3.1.85</td>
<td>2.9.12-270</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3.1</td>
<td>9.9(2.4)</td>
<td>2.3.1.84</td>
<td>2.9.12-204</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.3</td>
<td>9.9(2)</td>
<td>2.3.1.84</td>
<td>2.9.12-136</td>
<td>2017-01-17-002</td>
<td>4.5.0-290</td>
</tr>
<tr>
<td>6.2.2.5</td>
<td>9.8(2.44)</td>
<td>2.2.2.107</td>
<td>2.9.11-430</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2.4</td>
<td>9.8(2.36)</td>
<td>2.2.2.86</td>
<td>2.9.11-371</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2.3</td>
<td>9.8(2.30)</td>
<td>2.2.2.79</td>
<td>2.9.11-303</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2.2</td>
<td>9.8(2.22)</td>
<td>2.2.2.75</td>
<td>2.9.11-273</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2.1</td>
<td>9.8(2.10)</td>
<td>2.2.2.63</td>
<td>2.9.11-207</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.2</td>
<td>9.8(2.3)</td>
<td>2.2.2.52</td>
<td>2.9.11-125</td>
<td>2017-01-17-002</td>
<td>4.5.0-271</td>
</tr>
<tr>
<td>6.2.1</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0.6</td>
<td>9.7(1.25)</td>
<td>2.1.1.97</td>
<td>2.9.10-301</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0.5</td>
<td>9.7(1.23)</td>
<td>Not supported</td>
<td>2.9.10-255</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0.4</td>
<td>9.7(1.19)</td>
<td>Not supported</td>
<td>2.9.10-205</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0.3</td>
<td>9.7(1.15)</td>
<td>Not supported</td>
<td>2.9.10-160</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0.2</td>
<td>9.7(1.10)</td>
<td>Not supported</td>
<td>2.9.10-126</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0.1</td>
<td>9.7(1.7)</td>
<td>Not supported</td>
<td>2.9.10-98</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.2.0</td>
<td>9.7(1.4)</td>
<td>Not supported</td>
<td>2.9.10-42</td>
<td>2015-10-12-001</td>
<td>4.5.0-271</td>
</tr>
<tr>
<td>6.1.0.7</td>
<td>9.6(4.12)</td>
<td>Not supported</td>
<td>2.9.9-312</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0.6</td>
<td>9.6(3.23)</td>
<td>Not supported</td>
<td>2.9.9-258</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0.5</td>
<td>9.6(2.21)</td>
<td>Not supported</td>
<td>2.9.9-225</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0.4</td>
<td>9.6(2.16)</td>
<td>Not supported</td>
<td>2.9.9-191</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0.3</td>
<td>9.6(2.16)</td>
<td>Not supported</td>
<td>2.9.9-159</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0.2</td>
<td>9.6(2.4)</td>
<td>Not supported</td>
<td>2.9.9-125</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0.1</td>
<td>9.6(2.4)</td>
<td>Not supported</td>
<td>2.9.9-92</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.1.0</td>
<td>9.6(2)</td>
<td>Not supported</td>
<td>2.9.9-330</td>
<td>2015-10-12-001</td>
<td>4.5.0-270</td>
</tr>
<tr>
<td>6.0.1.4</td>
<td>9.6(1.19)</td>
<td>Not supported</td>
<td>2.9.8-490</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Firepower</td>
<td>ASA (ASA 5500-X Series with FTD)</td>
<td>FXOS (Firepower 1000/2100 Series with FTD)</td>
<td>Snort</td>
<td>GeoDB</td>
<td>VDB</td>
</tr>
<tr>
<td>-----------</td>
<td>---------------------------------</td>
<td>------------------------------------------</td>
<td>-------</td>
<td>-------</td>
<td>-----</td>
</tr>
<tr>
<td>6.0.1.3</td>
<td>9.6(1.12)</td>
<td>Not supported</td>
<td>2.9.8-461</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.0.1.2</td>
<td>9.6(1.11)</td>
<td>Not supported</td>
<td>2.9.8-426</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.0.1.1</td>
<td>9.6(1)</td>
<td>Not supported</td>
<td>2.9.8-383</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.0.1</td>
<td>9.6(1)</td>
<td>Not supported</td>
<td>2.9.8-224</td>
<td>2015-10-12-001</td>
<td>4.5.0-259</td>
</tr>
<tr>
<td>6.0.0.1</td>
<td>9.6(1)</td>
<td>Not supported</td>
<td>2.9.8-235</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>6.0.0</td>
<td>9.6(1)</td>
<td>Not supported</td>
<td>2.9.8-229</td>
<td>2015-10-12-001</td>
<td>4.5.0-252</td>
</tr>
</tbody>
</table>
Example Upgrade Paths

The following topics provide example upgrade paths for Firepower appliances.

- Example: Upgrading High Availability FMCs, on page 127
- Example: Upgrading Firepower 4100/9300 High Availability Pairs, on page 128
- Example: Upgrading Firepower 4100/9300 Intra-Chassis Clusters, on page 129
- Example: Upgrading Firepower 4100/9300 Inter-Chassis Clusters, on page 130
- Example: Upgrading Other FTD Devices, on page 131
- Example: Upgrading FMCv/NGIPSv Deployments, on page 132
- Example: Upgrading ASA with FirePOWER Services, on page 132

Example: Upgrading High Availability FMCs

You upgrade high availability Firepower Management Centers one at a time, manually. With synchronization paused, first upgrade the standby FMC, then the active.

Note
While Firepower 5.4.x supports FMC HA, Version 6.0 discontinues support. To upgrade your deployment from Version 5.4.x to Version 6.0, you must break—not just pause—HA. FMC HA support returns in Version 6.1. After you reconfigure HA, you do not need to break it for subsequent upgrades.

This example includes Firepower 7000/8000 series devices, which are legacy NGIPS devices. You can configure them as standalone devices, high availability pairs, and stacks.

Deployment

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Current</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 7000/8000 series devices:</td>
<td>Firepower 5.4.0.x (various)</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td>• Standalone devices</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• High availability pairs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Stacks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Example: Upgrading Firepower 4100/9300 High Availability Pairs

Firepower 6.0.1 introduces Firepower Threat Defense on Firepower 4100/9300 chassis. Upgrade FXOS on each chassis independently, always upgrading the standby.
Deployment

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Current Platform</th>
<th>Target Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 6.2.3</td>
<td>Firepower 6.0.1</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td>FXOS 2.3.1</td>
<td>FXOS 1.1.4</td>
<td>FXOS 2.3.1</td>
</tr>
<tr>
<td>Firepower 6.0.1</td>
<td>Firepower 6.0.1</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td>Firepower Management Center</td>
<td>Firepower 6.0.1</td>
<td>Firepower 6.2.3</td>
</tr>
</tbody>
</table>

Upgrade Path

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade</td>
<td>FMC</td>
<td>Firepower Preinstall → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade FXOS</td>
<td>Device B (standby)</td>
<td>FXOS 1.1.4 → 2.0.1</td>
</tr>
<tr>
<td>3</td>
<td>Switch roles</td>
<td>Device HA pair</td>
<td>Always upgrade the standby.</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade FXOS</td>
<td>Device A (new standby)</td>
<td>FXOS 1.1.4 → 2.0.1</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade Firepower software</td>
<td>Device HA pair</td>
<td>Firepower 6.0.1 → Preinstall → 6.1</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade</td>
<td>FMC</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>7</td>
<td>Upgrade FXOS</td>
<td>Device A (standby)</td>
<td>FXOS 2.0.1 → 2.3.1</td>
</tr>
<tr>
<td>8</td>
<td>Switch roles</td>
<td>Device HA pair</td>
<td>Always upgrade the standby.</td>
</tr>
<tr>
<td>9</td>
<td>Upgrade FXOS</td>
<td>Device B (new standby)</td>
<td>FXOS 2.0.1 → 2.3.1</td>
</tr>
<tr>
<td>10</td>
<td>Upgrade Firepower software</td>
<td>Device HA pair</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
</tbody>
</table>

Example: Upgrading Firepower 4100/9300 Intra-Chassis Clusters

Firepower 6.0.1 introduces Firepower Threat Defense on Firepower 4100/9300 chassis. Upgrade FXOS on each chassis independently.

Deployment

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Current Platform</th>
<th>Target Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 9300 intra-chassis cluster with three security modules</td>
<td>Firepower 6.0.1</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td></td>
<td>FXOS 1.1.4</td>
<td>FXOS 2.3.1</td>
</tr>
</tbody>
</table>
### Example: Upgrading Firepower 4100/9300 Inter-Chassis Clusters

Firepower 6.2 introduces Firepower Threat Defense inter-chassis clustering on Firepower 4100/9300 chassis. Upgrade FXOS on each chassis independently, always upgrading an all-slave chassis.

#### Deployment

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Current</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 9300 inter-chassis cluster with two chassis:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• A (three modules, including the master)</td>
<td>Firepower 6.2</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td>• B (three modules, all slaves)</td>
<td>FXOS 2.1.1</td>
<td>FXOS 2.3.1</td>
</tr>
<tr>
<td>Firepower Management Center</td>
<td>Firepower 6.2</td>
<td>Firepower 6.2.3</td>
</tr>
</tbody>
</table>

---

### Upgrade Path

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade FMC</td>
<td>Firepower 6.0.1</td>
<td>Firepower Preinstall → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade FXOS</td>
<td>Firepower 9300</td>
<td>FXOS 1.1.4 → 2.0.1</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade FXOS</td>
<td>Firepower 4100 series</td>
<td>FXOS 1.1.4 → 2.0.1</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade Firepower software</td>
<td>Both devices</td>
<td>Firepower 6.0.1 → 6.1</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade FMC</td>
<td>Firepower 6.1</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade FXOS</td>
<td>Firepower 9300</td>
<td>FXOS 2.0.1 → 2.3.1</td>
</tr>
<tr>
<td>7</td>
<td>Upgrade FXOS</td>
<td>Firepower 4100 series</td>
<td>FXOS 2.0.1 → 2.3.1</td>
</tr>
<tr>
<td>8</td>
<td>Upgrade Firepower software</td>
<td>Both devices</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
</tbody>
</table>
Example: Upgrading Other FTD Devices

Firepower 6.0.1 introduces Firepower Threat Defense. On many platforms, including ASA 5500-X series (ASA OS), ISA 3000 (ASA OS), and Firepower 1000/2100 series (FXOS), upgrading the Firepower software automatically upgrades the operating system. You do not need to perform these tasks separately.

Deployment

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Current</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>Firepower 6.0.1</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td>Firepower 2100 series with FTD</td>
<td>Firepower 6.2.1 (new in box)</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td>ISA 3000 with FTD</td>
<td>Firepower 6.2.3 (new in box)</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td>Firepower Management Center</td>
<td>Firepower 6.0.1</td>
<td>Firepower 6.2.3</td>
</tr>
</tbody>
</table>

Upgrade Path

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade</td>
<td>FMC</td>
<td>Firepower Preinstall → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade</td>
<td>ASA 5500-X series</td>
<td>Firepower 6.0.1 → 6.1</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade</td>
<td>FMC</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade</td>
<td>ASA 5500-X series</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>5</td>
<td>Add to the deployment</td>
<td>Firepower 2100 series</td>
<td>First opportunity to add the device.</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade</td>
<td>Firepower 2100 series</td>
<td>Firepower 6.2.1 → 6.2.3</td>
</tr>
</tbody>
</table>
Example: Upgrading FMCv/NGIPSv Deployments

In virtual deployments, make sure the hosting environment is compatible with the target version of the virtual appliance.

Deployment

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Current</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGIPSv</td>
<td>5.4.0.x (various)</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td></td>
<td>VMware ESXi 5.0</td>
<td>VMware ESXi 6.5</td>
</tr>
<tr>
<td>Firepower Management Center Virtual</td>
<td>Firepower 6.0</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td></td>
<td>VMware ESXi 5.5</td>
<td>VMware ESXi 6.5</td>
</tr>
</tbody>
</table>

Upgrade Path

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade Firepower software</td>
<td>FMCv</td>
<td>Firepower 6.0 → Preinstall → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade VMware ESXi</td>
<td>NGIPSv</td>
<td>ESXi 5.0 → 5.5</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade Firepower software</td>
<td>NGIPSv</td>
<td>Firepower 5.4.0.x → Preinstall → 6.0 → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade Firepower software</td>
<td>FMCv</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade Firepower software</td>
<td>NGIPSv</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade VMware ESXi</td>
<td>NGIPSv</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>7</td>
<td>Upgrade VMware ESXi</td>
<td>NGIPSv</td>
<td>ESXi 5.5 → 6.5</td>
</tr>
</tbody>
</table>

Example: Upgrading ASA with FirePOWER Services

Upgrade ASA on each chassis independently. On clustered or failover ASA devices, upgrade ASA FirePOWER modules one at a time, even when you are not upgrading ASA. You can avoid traffic loss by performing a failover or by disabling clustering on a unit before you upgrade the module.
The ASA 5506-X series and the ASA 5512-X do not support the ASA FirePOWER module running ASA 9.10(1) with any Firepower version.

### Deployment

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Current</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA FirePOWER running on various ASA 5500-X series models:</td>
<td>Firepower 5.4.x (various)</td>
<td>Firepower 6.2.3</td>
</tr>
<tr>
<td>A &amp; B (standalone)</td>
<td>ASA 9.3(2)</td>
<td>ASA 9.10(1)</td>
</tr>
<tr>
<td>C &amp; D (active/standby failover pair)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E &amp; F (active/active failover pair)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>G, H, I (master/slave/slave cluster)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firepower Management Center</td>
<td>Firepower 6.1</td>
<td>Firepower 6.2.3</td>
</tr>
</tbody>
</table>

### Upgrade Path: ASA and ASA FirePOWER on Standalone Devices (A & B)

Upgrade ASA and the ASA FirePOWER module as far as you can. Upgrade the ASA FirePOWER module after you upgrade and reload ASA.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade ASA</td>
<td>Device A (standalone)</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade ASA</td>
<td>Device B (standalone)</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade ASA FirePOWER</td>
<td>Devices A &amp; B</td>
<td>Firepower 5.4.x → Preinstall → 6.0 → 6.0.1 → 6.1</td>
</tr>
</tbody>
</table>

### Upgrade Path: ASA and ASA FirePOWER on Active/Standby Failover Pairs (C & D)

Upgrade ASA and the ASA FirePOWER module as far as you can. Upgrade the ASA FirePOWER module as you are upgrading ASA, just before you reload.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade ASA</td>
<td>Device D (standby in active/standby pair)</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade ASA FirePOWER</td>
<td>Device D</td>
<td>Firepower 5.4.x → Preinstall → 6.0 → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>3</td>
<td>Fail over</td>
<td>Device C &amp; D pair</td>
<td>Always upgrade the standby.</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade ASA</td>
<td>Device C (new standby)</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
</tbody>
</table>
### Upgrade Path: ASA and ASA FirePOWER on Active/Active Failover Pairs (E & F)

Upgrade ASA and the ASA FirePOWER module as far as you can. Upgrade the ASA FirePOWER module as you are upgrading ASA, just before you reload.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Make both failover groups active on the primary</td>
<td>Device E (primary in active/active pair)</td>
<td>Avoid traffic interruptions.</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade ASA</td>
<td>Device F (secondary in active/active pair)</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade ASA FirePOWER</td>
<td>Device F</td>
<td>Firepower 5.4.x → Preinstall → 6.0 → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>4</td>
<td>Make both failover groups active on the secondary</td>
<td>Device F</td>
<td>Avoid traffic interruptions.</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade ASA</td>
<td>Device E</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade ASA FirePOWER</td>
<td>Device E</td>
<td>Firepower 5.4.x → Preinstall → 6.0 → 6.0.1 → 6.1</td>
</tr>
</tbody>
</table>

### Upgrade Path: ASA and ASA FirePOWER on ASA Clusters (H, G, & I)

Upgrade ASA and the ASA FirePOWER module as far as you can. Upgrade the ASA FirePOWER module as you are upgrading ASA, just before you reload.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Remove from the cluster</td>
<td>Device I (slave)</td>
<td>Avoid traffic interruptions.</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade ASA</td>
<td>Device I</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade ASA FirePOWER</td>
<td>Device I</td>
<td>Firepower 5.4.x → Preinstall → 6.0 → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>4</td>
<td>Return to the cluster</td>
<td>Device I</td>
<td>Resume handling traffic.</td>
</tr>
<tr>
<td>5</td>
<td>Remove from the cluster</td>
<td>Device H (slave)</td>
<td>Avoid traffic interruptions.</td>
</tr>
<tr>
<td>6</td>
<td>Upgrade ASA</td>
<td>Device H</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
<tr>
<td>7</td>
<td>Upgrade ASA FirePOWER</td>
<td>Device H</td>
<td>Firepower 5.4.x → Preinstall → 6.0 → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>Step</td>
<td>Action</td>
<td>Platforms</td>
<td>Details</td>
</tr>
<tr>
<td>------</td>
<td>--------</td>
<td>-----------</td>
<td>---------</td>
</tr>
<tr>
<td>8</td>
<td>Return to the cluster</td>
<td>Device H</td>
<td>Resume handling traffic.</td>
</tr>
<tr>
<td>9</td>
<td>Remove from the cluster</td>
<td>Device G (master)</td>
<td>Avoid traffic interruptions.</td>
</tr>
<tr>
<td>10</td>
<td>Upgrade ASA</td>
<td>Device G</td>
<td>ASA 9.3(2) → 9.10(1)</td>
</tr>
<tr>
<td>11</td>
<td>Upgrade ASA FirePOWER</td>
<td>Device G</td>
<td>Firepower 5.4.x → Preinstall → 6.0 → 6.0.1 → 6.1</td>
</tr>
<tr>
<td>12</td>
<td>Return to the cluster</td>
<td>Device G</td>
<td>Resume handling traffic. Device G returns as a slave unit.</td>
</tr>
</tbody>
</table>

**Upgrade Path: Upgrade ASA FirePOWER Only**

At this point:

- The ASA devices are all running ASA 9.10(1)
- The FMC and all ASA FirePOWER modules are running Firepower 6.1

Because ASA is at its target version, you just need to upgrade the ASA FirePOWER modules. On clustered or failover ASA devices, even though you can upgrade them all together, best practice is still to upgrade ASA FirePOWER modules one at a time.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Platforms</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Upgrade</td>
<td>FMC</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>2</td>
<td>Upgrade ASA FirePOWER</td>
<td>Devices A &amp; B (standalone devices) Upgrade together, using the same package.</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade ASA FirePOWER</td>
<td>Devices C &amp; D (active/standby failover pair) Upgrade one at a time. First the standby, fail over, then the new standby.</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>4</td>
<td>Upgrade ASA FirePOWER</td>
<td>Devices E &amp; F (active/active failover pair) Upgrade one at a time. First, make both failover groups active on the primary, and upgrade the secondary. Then, make both failover groups active on the secondary, and upgrade the primary.</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
<tr>
<td>5</td>
<td>Upgrade ASA FirePOWER</td>
<td>Devices G, H, I (master/slave/slave cluster) Upgrade one at a time. Remove each device from the cluster, upgrade, then return to the cluster. Upgrade master last.</td>
<td>Firepower 6.1 → 6.2.3</td>
</tr>
</tbody>
</table>
Example: Upgrading ASA with FirePOWER Services
CHAPTER 14

Upgrade Guidelines and Warnings by Version

This chapter provides critical and release-specific information for Firepower software upgrades.

If your upgrade path skips one or more major versions—that is, you are not upgrading from the last major version or one of its patches—you must review the warnings and guidelines for intermediate releases. You can find that information in this chapter and in the Firepower Release Notes.

• Deprecated Features, on page 137
• Deprecated FlexConfig Commands, on page 145
• Multiversion Guidelines, on page 147
• Version 6.6.0 Guidelines, on page 148
• Version 6.5.0 Guidelines, on page 152
• Version 6.4.0.x Guidelines, on page 161
• Version 6.4.0 Guidelines, on page 161
• Version 6.3.0.x Guidelines, on page 164
• Version 6.3.0 Guidelines, on page 164
• Version 6.2.3.x Guidelines, on page 172
• Version 6.2.3 Guidelines, on page 173
• Version 6.2.2.x Guidelines, on page 175
• Version 6.2.2 Guidelines, on page 176
• Version 6.2.0.x Guidelines, on page 177
• Version 6.2.0 Guidelines, on page 177
• Version 6.1.0 Guidelines, on page 180
• Version 6.0.0 Guidelines, on page 181

Deprecated Features

This topic lists deprecated features and platforms by Firepower version. If your upgrade path skips one or more major versions, you must review the information for intermediate releases.

For detailed compatibility information for all supported Firepower versions, including links to end-of-sale and end-of-life announcements for deprecated platforms, see the Cisco Firepower Compatibility Guide.
Version 6.6.0 is the last major Firepower version that supports the Cisco Firepower User Agent software as an identity source. You should switch to Cisco Identity Services Engine/Passive Identity Connector (ISE/ISE-PIC) now. This will also allow you to take advantage of features that are not available with the user agent. To convert your license, contact Sales.

For more information, see the appropriate *Cisco Firepower User Agent Configuration Guide* on the Cisco Firepower Management Center Configuration Guides page.

### Version 6.6.0 Deprecated Features

These features were deprecated in Version 6.6.0.

**Table 35: Version 6.6.0 Deprecated Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lower-memory instances for cloud-based FMCv deployments</td>
<td>For performance reasons, the following FMCv instances are no longer supported:</td>
</tr>
<tr>
<td></td>
<td>• c3.xlarge on AWS</td>
</tr>
<tr>
<td></td>
<td>• c3.2xlarge on AWS</td>
</tr>
<tr>
<td></td>
<td>• c4.xlarge on AWS</td>
</tr>
<tr>
<td></td>
<td>• c4.2xlarge on AWS</td>
</tr>
<tr>
<td></td>
<td>• Standard_D3_v2 on Azure</td>
</tr>
<tr>
<td></td>
<td>You must resize before you upgrade to Version 6.6.0+. For more information, see <em>FMCv Requires 28 GB RAM for Upgrade</em>, on page 150.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments are fully deprecated. You cannot create new FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances.</td>
</tr>
<tr>
<td></td>
<td>Affected platforms: FMCv on AWS or Azure</td>
</tr>
<tr>
<td>e1000 Interfaces on FTDv for VMware</td>
<td>Version 6.6.0 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the <em>Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide</em>.</td>
</tr>
<tr>
<td></td>
<td>Affected platforms: FTDv for VMware</td>
</tr>
</tbody>
</table>
Custom tables for connection events

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Version 6.6.0 ends support for custom tables for connection and Security Intelligence events. After you upgrade, existing custom tables for those events are still 'available' but return no results. We recommend you delete them. There is no change to other types of custom tables. | Deprecated options:  
  - Analysis > Advanced > Custom Tables > click Create Custom Table > Tables drop-down list > Connection Events and Security Intelligence Events  
  Affected platforms: FMC |
| Ability to delete connection events from the event viewer | Version 6.6.0 ends support for deleting connection and Security Intelligence events from the event viewer. To purge the database, select System > Tools > Data Purge.  
  Deprecated options:  
  - Analysis > Connections > Events > Delete and Delete All  
  - Analysis > Connections > Security Intelligence Events > Delete and Delete All  
  Affected platforms: FMC |

**Version 6.5.0.x Deprecated Features**

These features were deprecated in Version 6.5.0.x patches.

**Table 36: Version 6.5.0.x Deprecated Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
</table>
| Version 6.5.0.3 no longer available | 6.5.0.3 | Version 6.5.0.3 was removed from the Cisco Support & Download site on 2019-02-04 (for FMCs) and 2020-03-02 (for devices). If you are running this version, it is safe to continue.  
  Related bugs: CSCvs86257  
  Affected platforms: All |
Patching an FTD device to Version 6.5.0.2+ turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled.

**Note** We recommend you patch to Version 6.5.0.2+. 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`.

For more information, see the software advisory: FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature.

Related bugs: CSCvq34340

Affected platforms: FTD

### Version 6.5.0 Deprecated Features

These features were deprecated in Version 6.5.0.

**Table 37: Version 6.5.0 Deprecated Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ability to disable the FMC CLI</td>
<td>Version 6.3.0 introduced the FMC CLI, which you had to explicitly enable. In Version 6.5.0, the FMC CLI is automatically enabled, for both new and upgraded deployments. If you want to access the Linux shell (also called <code>expert mode</code>), you must log in to the CLI and then use the <code>expert</code> command. <strong>Caution</strong> We recommend you do not access Firepower appliances using the shell, unless directed by Cisco TAC.</td>
<td>Deprecated options: System &gt; Configuration &gt; Console Configuration &gt; Enable CLI access check box</td>
</tr>
<tr>
<td>Feature</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
<td></td>
</tr>
</tbody>
</table>
| TLS 1.0 & 1.1 | To enhance security:  
| | • Captive portal (active authentication) has removed support for TLS 1.0.  
| | • Host input has removed support for TLS 1.0 and TLS 1.1.  
| | If your client fails to connect with a Firepower appliance, we recommend you upgrade your client to support TLS 1.2.  
| | Affected platforms: FMC |
| TLS crypto acceleration FXOS CLI commands for Firepower 4100/9300 | As part of allowing TLS crypto acceleration for multiple container instances on Firepower 4100/9300, we removed the following FXOS CLI commands:  
| | • show hwCrypto  
| | • config hwCrypto  
| | And this FTD CLI command:  
| | • show crypto accelerator status  
| | For information on their replacements, see the new feature documentation.  
| | Affected platforms: Firepower 4100/9300 |
| | Deprecated screens/options:  
| | • System > Integration > Packet Analyzer  
| | • Analysis > Advanced > Packet Analyzer Queries  
| | • Query Packet Analyzer when right-clicking on an event in the dashboard or event viewer  
| | Affected platforms: FMC |
| Firepower Management Center models FMC 750, 1500, 3500 | You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower Management Center software on the MC750, MC1500, and MC3500 models. You cannot manage Version 6.5.0+ devices with these FMCs. |
| ASA 5515-X and ASA 5585-X series devices with Firepower software | You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software (both FTD and ASA FirePOWER) on these models:  
| | • ASA 5515-X  
| | • ASA 5585-X-SSP-10, -20, -40, -60  
| | You can, however, manage older devices (Version 6.2.3 through 6.4.x) with a Version 6.5.0 or 6.6.0 FMC. |
**Deprecation Features**

You cannot upgrade to or freshly install Version 6.5.0+ of the Firepower software on Firepower 7000/8000 series devices, including AMP models. You can, however, manage older devices (Version 6.2.3 through 6.4.x) with a Version 6.5.0 or 6.6.0 FMC.

### Version 6.4.0.x Deprecated Features

These features were deprecated in Version 6.4.0.x patches.

#### Table 38: Version 6.4.0.x Deprecated Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egress optimization</td>
<td>6.4.0.7</td>
<td>To mitigate CSCvq34340, patching an FTD device to Version 6.4.0.7 turns off egress optimization processing. This happens regardless of whether the egress optimization feature is enabled or disabled. <strong>Note</strong> Upgrading to Version 6.5.0 will turn egress optimization back on, if you left the feature 'enabled.' We recommend you patch to Version 6.5.0.2+. If you remain at Version 6.5.0 or 6.5.0.1, you should manually disable egress optimization from the FTD CLI: <code>no asp inspect-dp egress-optimization</code>. For more information, see the software advisory: <a href="#">FTD traffic outage due to 9344 block size depletion caused by the egress optimization feature</a>. Affected platforms: FTD</td>
</tr>
<tr>
<td>Version 6.4.0.6 no longer available</td>
<td>6.4.0.6</td>
<td>Version 6.4.0.6 was removed from the Cisco Support &amp; Download site on 2019-12-19. If you are running this version, we recommend you upgrade. If you upgrade from Version 6.4.0.6 to a later patch, and then uninstall that patch, you return to Version 6.4.0.6. At that point, you should either immediately upgrade, or uninstall Version 6.4.0.6. Do not remain at Version 6.4.0.6. Affected platforms: All</td>
</tr>
</tbody>
</table>

### Version 6.4.0 Deprecated Features

These features were deprecated in Version 6.4.0.
### Table 39: Version 6.4.0 Deprecated Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL hardware acceleration FTD CLI commands</td>
<td>As part of the TLS crypto acceleration feature, we removed the following FTD CLI commands:</td>
</tr>
<tr>
<td></td>
<td>• system support ssl-hw-accel enable</td>
</tr>
<tr>
<td></td>
<td>• system support ssl-hw-accel disable</td>
</tr>
<tr>
<td></td>
<td>• system support ssl-hw-status</td>
</tr>
<tr>
<td></td>
<td>For information on their replacements, see the new feature documentation.</td>
</tr>
<tr>
<td></td>
<td>Affected platforms: FTD</td>
</tr>
</tbody>
</table>

### Version 6.3.0 Deprecated Features

These features were deprecated in Version 6.3.0.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMS extension support for decryption</td>
<td>Version 6.3.0 discontinues EMS extension support, which was introduced in Version 6.2.3.8/6.2.3.9. This means that the Decrypt-Resign and Decrypt-Known Key SSL policy actions no longer support the EMS extension during ClientHello negotiation, which would enable more secure communications. The EMS extension is defined by RFC 7627.</td>
</tr>
<tr>
<td></td>
<td>In FMC deployments, this feature depends on the device version. Upgrading the FMC to Version 6.3.0 does not discontinue support, as long as the device is running a supported version. However, upgrading the device to Version 6.3.0 does discontinue support.</td>
</tr>
<tr>
<td></td>
<td>Support is reintroduced in Version 6.3.0.1.</td>
</tr>
<tr>
<td></td>
<td>Affected platforms: Any</td>
</tr>
<tr>
<td>Decryption on passive and inline tap Interfaces</td>
<td>Version 6.3.0 ends support for decrypting traffic on interfaces in passive or inline tap mode, even though the GUI allows you to configure it. Any inspection of encrypted traffic is necessarily limited.</td>
</tr>
<tr>
<td>VMware 5.5 hosting</td>
<td>Version 6.3.0+ virtual deployments have not been tested on VMware vSphere/VMware ESXi 5.5. We recommend you upgrade the hosting environment before you upgrade the Firepower software.</td>
</tr>
<tr>
<td></td>
<td>Affected platforms: FMCv, FTDv, and NGIPSv for VMware</td>
</tr>
</tbody>
</table>
## Deprecated Features

ASA 5506-X series and ASA 5512-X devices with Firepower software

You cannot upgrade to or freshly install Version 6.3.0+ of the Firepower software (both FTD and ASA FirePOWER) on these models:

- ASA 5506-X, 5506H-X, 5506W-X
- ASA 5512-X

You can, however, manage older devices (Version 6.1.0 through 6.2.3.x) with a Version 6.3.0 FMC.

### Version 6.2.3.x Deprecated Features

These features were deprecated in Version 6.2.3.x patches.

**Table 41: Version 6.2.3.x Deprecated Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
</table>
| Version 6.2.3.8 no longer available | 6.2.3.8 | Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. If you are running this version, we strongly recommend you upgrade. Devices running Version 6.2.3.8 may stop passing traffic after a certain amount of time.  
If you upgrade from Version 6.2.3.8 to a later patch, and then uninstall that patch, you return to Version 6.2.3.8. At that point, you should either immediately upgrade, or uninstall Version 6.2.3.8. Do not remain at Version 6.2.3.8.  
Related bugs: CSCvn82378  
Affected platforms: All |

### Version 6.2.1 Deprecated Features

These features were deprecated in Version 6.2.1.

**Table 42: Version 6.2.1 Deprecated Features**

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
</table>
| Verizon 6.2.1 no longer available | Version 6.2.1 was removed from the Cisco Support & Download site on 2017-11-17. This version is replaced by Version 6.2.2, which offers the same functionality and supports the full set of Firepower platforms.  
If you are running Version 6.2.1, we strongly recommend you upgrade.  
Affected platforms: FMC, Firepower 2100 series |

### Version 6.2.0 Deprecated Features

These features were deprecated in Version 6.2.0.
Table 43: Version 6.2.0 Deprecated Features

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nested correlation rules</td>
<td>Version 6.2.0 ends support for nested correlation rules. A correlation rule is nested if it serves as a trigger for another correlation rule. For example, if you create Rule A and Rule B, which both trigger on an intrusion event, you can use 'Rule A is true' as a constraint for Rule B. In this configuration, Rule A is nested inside Rule B.</td>
</tr>
</tbody>
</table>

**Automatic Configuration Changes**

The upgrade process "flattens" certain nested correlation rules by copying settings from the nested rule (Rule A) to the nesting rule (Rule B), then deleting the nested rule. The upgrade also copies the host profile/user qualifications and the snooze/inactive periods from the nested rule to the nesting rule.

For all of these settings except inactive periods, the system can copy the settings from the nested rule to the nesting rule only if the settings are absent from the nesting rule. When the system copies inactive periods from the nested rule to the nesting rule, it retains inactive periods from the nesting rule, so that the resulting rule uses settings from both rules originally involved in the nesting configuration.

**Avoiding Upgrade Failure**

Before you upgrade, make sure that any nested correlation rules can be "flattened." Otherwise, the upgrade will fail. Note that the upgrade cannot flatten nested rules if the nested and nesting rule have specific conflicts. To avoid upgrade failure, modify your correlation rules before the upgrade:

- Remove the host profile qualification, user qualification, and snooze period settings from either the nested rule or the nesting rule, so that only one rule in the nested configuration specifies these settings.
- Remove connection trackers from any nested rules.
- Remove host profile qualifications, user qualifications, snooze periods, and inactive periods from nested rules that do not have to be true; that is, remove those elements from nested rules that are linked to other rule conditions using the OR operator, within the nesting rule.

Affected platforms: FMC

---

**Deprecated FlexConfig Commands**

Some Firepower Threat Defense features are configured using ASA configuration commands. Beginning with Version 6.2 (FMC deployments), you can use Smart CLI or FlexConfig to manually configure various ASA features that are not otherwise supported in the web interface.
FTD upgrades can add GUI or Smart CLI support for features that you previously configured using FlexConfig. This can deprecate FlexConfig commands that you are currently using. Although your existing configurations continue to work and you can still deploy, you cannot assign or create FlexConfig objects using the newly deprecated commands.

After the upgrade, examine your FlexConfig policies and objects. If any contain commands that are now deprecated, messages indicate the problem. We recommend you redo your configuration. After you are satisfied with the new configuration, you can delete the problematic FlexConfig objects or commands.

**FTD with Firepower Management Center**

This table lists deprecated FlexConfig objects and their associated text objects. For a full list of predefined objects, see the Firepower Management Center Configuration Guide.

*Table 44: FTD with FMC: Deprecated FlexConfig Objects*

<table>
<thead>
<tr>
<th>Deprecated</th>
<th>Objects</th>
<th>Details</th>
<th>New Location</th>
</tr>
</thead>
</table>
| 6.3.0+     | FlexConfig Objects:  
• Default_DNS_Configure  
Associated Text Objects:  
• defaultDNSNameServerList  
• defaultDNSParameters | Configure the Default DNS group, which defines the DNS servers that can be used when resolving fully-qualified domain names on the data interfaces. This allowed you to use commands in the CLI, such as ping, using host names rather than IP addresses. | Configure DNS for the data interfaces in the FTD platform settings policy. |
| 6.3.0+     | FlexConfig Objects:  
• TCP_Embryonic_Conn_Limit  
• TCP_Embryonic_Conn_Timeout  
Associated Text Objects:  
• tcp_conn_misc  
• tcp_conn_limit  
• tcp_conn_timeout | Configure embryonic connection limits and timeouts to protect against SYN Flood Denial of Service (DoS) attacks. | Configure these features in the FTD service policy, which you can find on the Advanced tab of the access control policy assigned to the device. |

This table lists CLI commands that were newly deprecated for FTD with FDM, in Version 6.2.3+. For a full list of deprecated commands, including those deprecated when the feature was introduced in Version 6.2.0, see the Firepower Management Center Configuration Guide.

*Table 45: FTD with FMC: Deprecated CLI Commands*

<table>
<thead>
<tr>
<th>Deprecated</th>
<th>Command</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.3+</td>
<td>pager</td>
<td>Configuration blocked.</td>
</tr>
</tbody>
</table>
Multiversion Guidelines

These important guidelines and warnings apply to multiple Firepower major versions, or to a major version and multiple patches.

Table 46: Multiversion Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Affected Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic, on page 147</td>
<td>Firepower 1010</td>
<td>6.4.0 through 6.4.0.4</td>
</tr>
<tr>
<td></td>
<td>Upgrade Failure: Insufficient Disk Space on Container Instances, on page 147</td>
<td>Firepower 4100/9300</td>
<td>6.3.0.1 through 6.5.0</td>
</tr>
<tr>
<td></td>
<td>Patch/Hotfix for Dynamic Analysis CA Certificates, on page 147</td>
<td>Any</td>
<td>6.0.0 through 6.2.3.x</td>
</tr>
</tbody>
</table>

EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic

**Deployments:** Firepower 1010 with FTD

**Affected Versions:** Version 6.4.0 to 6.4.0.5

**Related Bug:** CSCvq81354

We strongly recommend you do not configure EtherChannels on Firepower 1010 devices running FTD Version 6.4.0 to Version 6.4.0.5. (Note that Versions 6.4.0.1 and 6.4.0.2 are not supported on this model.)

Due to an internal traffic hashing issue, some EtherChannels on Firepower 1010 devices may blackhole some egress traffic. The hashing is based on source/destination IP address so the behavior will be consistent for a given source/destination IP pair. That is, some traffic consistently works and some consistently fails.

We will fix this issue in an upcoming 6.4.0.x patch. It is also fixed in Version 6.5.0.

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.

Patch/Hotfix for Dynamic Analysis CA Certificates

**Deployments:** AMP for Networks (malware detection) deployments where you submit files for dynamic analysis
**Affected Versions:** Version 6.0+

**Resolves:** CSCvj07038

On June 15, 2018, some Firepower deployments stopped being able to submit files for dynamic analysis. This occurred due to an expired CA certificate that was required for communications with the AMP Threat Grid cloud. Version 6.3.0 is the first major version with the new certificate.

If you do not want to upgrade to Version 6.3.0+, you must patch or hotfix to obtain the new certificate and reenable dynamic analysis. However, subsequently upgrading a patched or hotfixed deployment to either Version 6.2.0 or Version 6.2.3 reverts to the old certificate and you must patch or hotfix again.

If this is your first time installing the patch or hotfix, make sure your firewall allows outbound connections to `fmc.api.threatgrid.com` (replacing `panacea.threatgrid.com`) from both the FMC and its managed devices. Managed devices submit files to the cloud for dynamic analysis; the FMC queries for results.

The following table lists the versions with the old certificates, as well as the patches and hotfixes that contain the new certificates, for each major version sequence and platform. Patches and hotfixes are available on the Cisco Support & Download site. For release notes, see Firepower Release Notes.

**Table 47: Patches and Hotfixes with New CA Certificates**

<table>
<thead>
<tr>
<th>Versions with Old Cert</th>
<th>First Patch with New Cert</th>
<th>Hotfix with New Cert</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.2.3 through 6.2.3.3</td>
<td>6.2.3.4</td>
<td>Hotfix G</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FTD devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hotfix H</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FMC, NGIPS devices</td>
</tr>
<tr>
<td>6.2.2 through 6.2.2.3</td>
<td>6.2.2.4</td>
<td>Hotfix BN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All platforms</td>
</tr>
<tr>
<td>6.2.1</td>
<td>None. You must upgrade.</td>
<td>None. You must upgrade.</td>
</tr>
<tr>
<td>6.2.0 through 6.2.0.5</td>
<td>6.2.0.6</td>
<td>Hotfix BX</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FTD devices</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hotfix BW</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FMC, NGIPS devices</td>
</tr>
<tr>
<td>6.1.0 through 6.1.0.6</td>
<td>6.1.0.7</td>
<td>Hotfix EM</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All platforms</td>
</tr>
<tr>
<td>6.0.x</td>
<td>None. You must upgrade.</td>
<td>None. You must upgrade.</td>
</tr>
</tbody>
</table>

---

**Version 6.6.0 Guidelines**

This checklist contains important upgrade guidelines and warnings that are *new* for this major version.

**Table 48: Version 6.6.0 New Guidelines**

<table>
<thead>
<tr>
<th>✓ Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMCv Requires 28 GB RAM for Upgrade, on page 150</td>
<td>FMCv for VMware</td>
<td>6.2.3 through 6.5.0.x</td>
<td>6.6.0+</td>
</tr>
</tbody>
</table>
These previously published guidelines and warnings apply to intermediate releases. Review this checklist if your upgrade path skips major versions.

Table 49: Version 6.6.0 Previously Published Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>FTDv for VMware e1000 Interfaces Prevent Upgrade, on page 151</td>
<td>FTDv for VMware</td>
<td>6.2.3 through 6.5.0.x</td>
<td>6.6.0+</td>
</tr>
<tr>
<td>✓</td>
<td>Events Temporarily Unavailable After FMC Upgrade, on page 151</td>
<td>FMC</td>
<td>6.2.3 through 6.5.0.x</td>
<td>6.6.0+</td>
</tr>
</tbody>
</table>
FMCv Requires 28 GB RAM for Upgrade

**Deployments:** FMCv

**Upgrading from:** Version 6.2.3 through 6.5.0.x

**Directly to:** Version 6.6.0+

**Related bug:** CSCvr67542

All FMCv implementations now have the same RAM requirements: 32 GB recommended, 28 GB required (64 GB for FMCv 300). Upgrades to Version 6.6.0+ 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 on FMCv memory requirements, see the Cisco Firepower Management Center Virtual Getting Started Guide.

---

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 FMCv instances using them, even for earlier Firepower versions. You can continue running existing instances.

This table summarizes pre-upgrade requirements for lower-memory FMCv deployments.

**Table 50: FMCv Memory Requirements for Version 6.6.0+ Upgrades**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Pre-Upgrade Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware</td>
<td>Allocate 28 GB minimum/32 GB recommended.</td>
<td>Power off the virtual machine first. For instructions, see the VMware documentation.</td>
</tr>
<tr>
<td>KVM</td>
<td>Allocate 28 GB minimum/32 GB recommended.</td>
<td>For instructions, see the documentation for your KVM environment.</td>
</tr>
</tbody>
</table>
### Pre-Upgrade Action

<table>
<thead>
<tr>
<th>Platform</th>
<th>Pre-Upgrade Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>Resize instances:</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- From c3.xlarge to c3.4xlarge.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- From c3.2.xlarge to c3.4xlarge.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- From c4.xlarge to c4.4xlarge.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- From c4.2xlarge to c4.4xlarge.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>We also offer a c5.4xlarge instance for new deployments.</td>
<td></td>
</tr>
<tr>
<td>Azure</td>
<td>Resize instances:</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>- From Standard_D3_v2 to Standard_D4_v2.</td>
<td></td>
</tr>
</tbody>
</table>

### FTDv for VMware e1000 Interfaces Prevent Upgrade

**Deployments:** FTDv for VMware

**Upgrading from:** Version 6.2.3 through 6.5.0.x

**Directly to:** Version 6.6.0+

Version 6.6.0 ends support for e1000 interfaces on FTDv for VMware. You cannot upgrade until you switch to vmxnet3 or ixgbe interfaces. Or, you can deploy a new device.

For more information, see the Cisco Firepower Threat Defense Virtual for VMware Getting Started Guide.

### Events Temporarily Unavailable After FMC Upgrade

**Deployments:** FMC

**Upgrading from:** Version 6.2.3 through 6.5.0.x

**Directly to:** Version 6.6.0+

Version 6.6.0 uses a new datastore for connection and Security Intelligence events.

After the upgrade finishes and the FMC reboots, historical connection and Security Intelligence events are migrated in the background, resource constrained. Depending on FMC model, system load, and how many events you have stored, this can take from a few hours up to a day.

Historical events are migrated by age, newest events first. Events that have not been migrated do not appear in query results or dashboards. If you reach the connection event database limit before the migration completes, for example, because of post-upgrade events, the oldest historical events are not migrated.
Version 6.5.0 Guidelines

This checklist contains important upgrade guidelines and warnings that are new for this major version.

Table 51: Version 6.5.0 New Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Firepower 1000 Series Devices Require Post-Upgrade Power Cycle, on page 153</td>
<td>Firepower 1000 series</td>
<td>6.4.0.x</td>
<td>6.5.0+</td>
</tr>
<tr>
<td>✓</td>
<td>Disable Egress Optimization for Version 6.5.0, on page 153</td>
<td>FTD</td>
<td>6.2.3 through 6.4.0.x</td>
<td>6.5.0 only</td>
</tr>
<tr>
<td>✓</td>
<td>Upgrade Assigns Deployment to North America Cisco Cloud, on page 154</td>
<td>Any</td>
<td>6.2.3 through 6.4.0.x</td>
<td>6.5.0+</td>
</tr>
<tr>
<td>✓</td>
<td>Cisco Threat Intelligence Director (TID) Behavior Changes, on page 154</td>
<td>FMC</td>
<td>6.2.3 through 6.4.0.x</td>
<td>6.5.0+</td>
</tr>
<tr>
<td>✓</td>
<td>New URL Categories and Reputations, on page 155</td>
<td>Any</td>
<td>6.2.3 through 6.4.0.x</td>
<td>6.5.0+</td>
</tr>
</tbody>
</table>

These previously published guidelines and warnings apply to intermediate releases. Review this checklist if your upgrade path skips major versions.

Table 52: Version 6.5.0 Previously Published Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Upgrade Failure: Insufficient Disk Space on Container Instances, on page 147</td>
<td>Firepower 4100/9300</td>
<td>6.3.0 through 6.4.0.x</td>
<td>6.3.0.1 through 6.5.0</td>
</tr>
<tr>
<td>✓</td>
<td>TLS Crypto Acceleration Enabled/Cannot Disable, on page 163</td>
<td>Firepower 2100 series</td>
<td>6.2.3 through 6.3.0.x</td>
<td>6.4.0+</td>
</tr>
<tr>
<td>✓</td>
<td>Firepower 4100/9300</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>✓</td>
<td>Timeouts for the URL Filtering Cache Can Change, on page 168</td>
<td>Any</td>
<td>6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td>✓</td>
<td>Guideline</td>
<td>Platforms</td>
<td>Upgrading From</td>
<td>Directly To</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------</td>
<td>-----------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 168</td>
<td>FMC Firepower 7000/8000 series NGIPSv</td>
<td>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</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>RA VPN Default Setting Change Can Block VPN Traffic, on page 168</td>
<td>FTD with FMC</td>
<td>6.2.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Updated Security for Appliance Access, on page 169</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Security Intelligence Enables Application Identification, on page 170</td>
<td>FMC deployments</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Update VDB after Upgrade to Enable CIP Detection, on page 170</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 170</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Syslog Behavior Changes for Connection and Intrusion Events, on page 171</td>
<td>FMC</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
</tbody>
</table>

**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.

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.

Upgrade Assigns Deployment to North America Cisco Cloud

**Deployments:** Any

**Upgrading from:** Version 6.2.3 through 6.4.x

**Directly to:** Version 6.5.0+

We have now introduced Cisco Cloud Services regions. Your deployment's regional cloud is used for the following features: Cisco Defense Orchestrator, Cisco Threat Response, Cisco Success Network, and Cisco Support Diagnostics.

For FMC deployments, by default, the upgrade assigns you to the US (North America) region. You can change your region on the **System > Integration > Cloud Services** page.

Cisco Threat Intelligence Director (TID) Behavior Changes

**Deployments:** FMC

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

**Directly to:** Version 6.5.0+

In Version 6.5.0+, TID blocking/monitoring observable actions now have priority over blocking/monitoring with Security Intelligence blacklists.

If you configure the **Block** TID observable action, even if the traffic also matches a Security Intelligence blacklist set to **Block**:  

- The Security Intelligence category in the connection event is a variant of **TID Block**.
- The system generates a TID incident with an action taken of **Blocked**.
If you configure the **Monitor** TID observable action, even if the traffic also matches a Security Intelligence blacklist set to **Monitor**:

- The Security Intelligence category in the connection event is a variant of TID Monitor
- The system generates a TID incident with an action taken of **Monitored**.

Previously, in each of these cases, the system reported the category by analysis and did not generate a TID incident.

---

**Note**

The system still effectively handles traffic as before. Traffic that was blocked before is still blocked, and monitored traffic is still monitored. This simply changes which component gets the 'credit.' You may also see more TID incidents generated.

For complete information on system behavior when you enable both Security Intelligence and TID, see the *TID-Firepower Management Center Action Prioritization* information in the Firepower Management Center Configuration Guide.

### New URL Categories and Reputations

**Deployments:** Any

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

**Directly to:** Version 6.5.0+

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

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

- **Uncategorized URLs** can have a Questionable, Neutral, Favorable, or Trusted reputation.
  
  You can filter **Uncategorized** URLs but you cannot further constrain by reputation. These rules will match all uncategorized URLs, regardless of reputation.

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

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

The following table summarizes the changes on upgrade. Although they are designed for minimal impact and will not prevent post-upgrade deploy for most customers, we *strongly* recommend you review these release notes and your current URL filtering configuration. Careful planning and preparation can help you avoid missteps, as well as reduce the time you spend troubleshooting post-upgrade.
## Table 53: Deployment Changes on Upgrade

<table>
<thead>
<tr>
<th>Change</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modifies URL rule categories.</td>
<td>The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies:</td>
</tr>
<tr>
<td></td>
<td>• Access control</td>
</tr>
<tr>
<td></td>
<td>• SSL</td>
</tr>
<tr>
<td></td>
<td>• QoS (FMC only)</td>
</tr>
<tr>
<td></td>
<td>• Correlation (FMC only)</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Renames URL rule reputations.</td>
<td>The upgrade modifies URL rules to use the new reputation names:</td>
</tr>
<tr>
<td></td>
<td>1. Untrusted (was High Risk)</td>
</tr>
<tr>
<td></td>
<td>2. Questionable (was Suspicious sites)</td>
</tr>
<tr>
<td></td>
<td>3. Neutral (was Benign sites with security risks)</td>
</tr>
<tr>
<td></td>
<td>4. Favorable (was Benign sites)</td>
</tr>
<tr>
<td></td>
<td>5. Trusted (was Well Known)</td>
</tr>
<tr>
<td>Clears the URL cache.</td>
<td>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.</td>
</tr>
<tr>
<td>Labels 'legacy' events.</td>
<td>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.</td>
</tr>
</tbody>
</table>

## Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.
Table 54: Pre-Upgrade Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
</table>
| Make sure your appliances can reach Talos resources. | The system must be able to communicate with the following Cisco resources after the upgrade:  
  - 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:ffe::/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 (报告图标) 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 55: Post-Upgrade Actions

<table>
<thead>
<tr>
<th>Action</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remove deprecated categories from rules. Required.</td>
<td>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.</td>
</tr>
<tr>
<td>Create or modify rules to include the new categories.</td>
<td>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.</td>
</tr>
<tr>
<td>Evaluate rules changed as a result of merged categories.</td>
<td>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 158. 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.</td>
</tr>
<tr>
<td>Evaluate rules changed as a result of split categories.</td>
<td>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.</td>
</tr>
<tr>
<td>Understand which categories were renamed or are unchanged.</td>
<td>Although no action is required, you should be aware of these changes. These changes are not marked.</td>
</tr>
<tr>
<td>Evaluate how you handle uncategorized and reputationless URLs.</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 56: Guidelines for Rules with Merged URL Categories

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rule Order Determines Which Rule Matches Traffic</td>
<td>When considering rules that include the same category, remember that traffic matches the first rule in the list that includes the condition.</td>
</tr>
<tr>
<td>Categories in the Same Rule vs Categories in Different Rules</td>
<td>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.</td>
</tr>
<tr>
<td>Associated Action</td>
<td>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.</td>
</tr>
<tr>
<td>Associated Reputation Level</td>
<td>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.</td>
</tr>
<tr>
<td>Duplicate and Redundant Categories and Rules</td>
<td>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.</td>
</tr>
<tr>
<td>Other URL Categories in a Rule</td>
<td>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.</td>
</tr>
</tbody>
</table>
Guidelines for Rules with Merged URL Categories

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-URL Conditions in a Rule</td>
<td>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.</td>
</tr>
</tbody>
</table>

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 57: Examples of Rules with Merged URL Categories**

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Before Upgrade</th>
<th>After Upgrade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Merged categories in the same rule</td>
<td>Rule 1 has Category A and Category B.</td>
<td>Rule 1 has Category AB.</td>
</tr>
<tr>
<td>Merged categories in different rules</td>
<td>Rule 1 has Category A.</td>
<td>Rule 1 has Category AB.</td>
</tr>
<tr>
<td></td>
<td>Rule 2 has Category B.</td>
<td>Rule 2 has Category AB.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Merged categories in different rules have different actions</td>
<td>Rule 1 has Category A set to Allow.</td>
<td>Rule 1 has Category AB set to Allow.</td>
</tr>
<tr>
<td>(Reputation is the same)</td>
<td>Rule 2 has Category B set to Block.</td>
<td>Rule 2 has Category AB set to Block.</td>
</tr>
<tr>
<td></td>
<td>(Reputation is the same)</td>
<td>Rule 1 will match all traffic for this category.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Merged categories in the same rule have different reputation levels</td>
<td>Rule 1 includes: Category A with Reputation Any</td>
<td>Rule 1 includes Category AB with Reputation Any.</td>
</tr>
<tr>
<td></td>
<td>Category B with Reputation 1-3</td>
<td></td>
</tr>
<tr>
<td>Merged categories in different rules have different reputation levels</td>
<td>Rule 1 includes Category A with Reputation Any.</td>
<td>Rule 1 includes Category AB with Reputation Any.</td>
</tr>
<tr>
<td></td>
<td>Rule 2 includes Category B with Reputation 1-3</td>
<td>Rule 2 includes Category AB with Reputation 1-3.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rule 1 will match all traffic for this category.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Rule 2 will never match traffic, but you will not see a warning indicator because the reputations are not identical.</td>
</tr>
</tbody>
</table>
Version 6.4.0.x Guidelines

Table 58: Version 6.4.0.x Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Upgrade Failure: Insufficient Disk Space on Container Instances, on page 147</td>
<td>Firepower 4100/9300</td>
<td>6.4.0.x</td>
<td>Later patches 6.5.0</td>
</tr>
<tr>
<td></td>
<td>EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic, on page 147</td>
<td>Firepower 1010</td>
<td>6.4.0 only</td>
<td>6.4.0.3 through 6.4.0.5</td>
</tr>
<tr>
<td></td>
<td>Versions 6.4.0.1 and 6.4.0.2 Not Supported on Firepower 1000 Series, on page 161</td>
<td>Firepower 1000 series</td>
<td>6.4.0 only</td>
<td>6.4.0.1 or 6.4.0.2</td>
</tr>
</tbody>
</table>

Versions 6.4.0.1 and 6.4.0.2 Not Supported on Firepower 1000 Series

**Deployments:** Firepower 1000 series

**Upgrading from:** Version 6.4.0

**Directly to:** Version 6.4.0.1 or 6.4.0.2

You cannot upgrade a Firepower 1000 series device to Version 6.4.0.1 or 6.4.0.2.

Version 6.4.0 Guidelines

This checklist contains important upgrade guidelines and warnings that are *new* for this major version.

Table 59: Version 6.4.0 New Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic, on page 147</td>
<td>Firepower 1010</td>
<td>6.4.0</td>
<td>6.4.0.3 through 6.4.0.5</td>
</tr>
<tr>
<td></td>
<td>Upgrade Failure: Insufficient Disk Space on Container Instances, on page 147</td>
<td>Firepower 4100/9300</td>
<td>6.3.0 through 6.4.0.x</td>
<td>6.3.0.1 through 6.5.0</td>
</tr>
<tr>
<td></td>
<td>Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12, on page 163</td>
<td>Firepower 7000/8000 series ASA FirePOWER NGIPSv</td>
<td>6.2.3 through 6.3.0.x</td>
<td>6.4.0 only</td>
</tr>
<tr>
<td>✓</td>
<td>Guideline</td>
<td>Platforms</td>
<td>Upgrading From</td>
<td>Directly To</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------</td>
<td>-------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>TLS Crypto Acceleration Enabled/Cannot Disable, on page 163</td>
<td>Firepower 2100 series</td>
<td>6.1.0 through 6.3.0.x</td>
<td>6.4.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firepower 4100/9300</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Firepower 4100/9300 Requires Version 6.2.0 for Upgrade, on page 164</td>
<td>Firepower 4100/9300</td>
<td>6.1.0.x</td>
<td>6.4.0 only</td>
</tr>
</tbody>
</table>

These previously published guidelines and warnings apply to intermediate releases. Review this checklist if your upgrade path skips major versions.

Table 60: Version 6.4.0 Previously Published Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Timeouts for the URL Filtering Cache Can Change, on page 168</td>
<td>Any</td>
<td>6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 168</td>
<td>FMC Firepower 7000/8000 series NGIPSv</td>
<td>6.1.0 through 6.1.0.6</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6.2.0 through 6.2.2.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RA VPN Default Setting Change Can Block VPN Traffic, on page 168</td>
<td>FTD with FMC</td>
<td>6.2.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Updated Security for Appliance Access, on page 169</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Security Intelligence Enables Application Identification, on page 170</td>
<td>FMC deployments</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Update VDB after Upgrade to Enable CIP Detection, on page 170</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 170</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Syslog Behavior Changes for Connection and Intrusion Events, on page 171</td>
<td>FMC</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Changes to Result Limits in Reports, on page 174</td>
<td>FMC</td>
<td>6.1.0 through 6.2.2.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
<tr>
<td>✓</td>
<td>Guideline</td>
<td>Platforms</td>
<td>Upgrading From</td>
<td>Directly To</td>
</tr>
<tr>
<td>---</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------</td>
<td>----------------</td>
<td>--------------</td>
</tr>
<tr>
<td></td>
<td>Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page</td>
<td>FTD clusters</td>
<td>6.1.0.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>175</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Access Control Can Get Latency-Based Performance Settings from SRUs, on</td>
<td>FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>page 178</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 178</td>
<td>FTD with FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
</tbody>
</table>

**Upgrade Failure: NGIPS Devices Previously at Version 6.2.3.12**

**Deployments:** 7000/8000 series, ASA FirePOWER, NGIPSv

**Related bug:** CSCvp42398

**Upgrading from:** Version 6.2.3 through 6.3.0.x

**Directly to:** Version 6.4.0 only

You cannot upgrade an NGIPS device to Version 6.4.0 if:

- The device previously ran Version 6.2.3.12, and then
- You uninstalled the Version 6.2.3.12 patch, or upgraded to Version 6.3.0.x.

This also includes scenarios where you uninstalled the Version 6.2.3.12 patch and then upgraded to Version 6.3.0.x.

If this is your current situation, 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 \texttt{config hwCrypto enable} CLI command.

**Firepower 4100/9300 Requires Version 6.2.0 for Upgrade**

**Deployments:** Firepower 4100/9300 with FTD  
**Upgrading from:** Version 6.1.x  
**Directly to:** Version 6.4.0 only

Unlike other FMC-managed devices, you cannot upgrade the Firepower Threat Defense software directly from Version 6.1 $\rightarrow$ 6.4 on a Firepower 4100/9300 series device. This is because FXOS 2.6.1 is incompatible with FTD Version 6.1, but required for Version 6.4.

We recommend Version 6.2.3 on FXOS 2.3.1 as the intermediate version—and remember to upgrade FXOS first. Do not use Version 6.3 as an intermediate release; see the guidelines and warnings in the Firepower Release Notes, Version 6.3.0.

**Version 6.3.0.x Guidelines**

<table>
<thead>
<tr>
<th>✓ Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upgrade Failure: Insufficient Disk Space on Container Instances, on page 147</td>
<td>Firepower 4100/9300</td>
<td>6.3.0.x</td>
<td>Later patches 6.4.0 and 6.5.0</td>
</tr>
</tbody>
</table>

**Version 6.3.0 Guidelines**

This checklist contains important upgrade guidelines and warnings that are \textit{new} for this major version.

<table>
<thead>
<tr>
<th>✓ Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
</table>
| Renamed Upgrade and Installation Packages, on page 166 | FMC  
Firepower 7000/8000 series  
NGIPSv | Any | 6.3.0+ |
| Reimaging to Version 6.3+ Disables LOM on Most Appliances, on page 167 | FMC (physical)  
Firepower 7000/8000 series | Any | 6.3.0+ |
<p>| Timeouts for the URL Filtering Cache Can Change, on page 168 | Any | 6.2.3.x | 6.3.0+ |</p>
<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv, on page 168</td>
<td>FMC</td>
<td>6.2.3 through 6.2.3.4</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firepower 7000/8000 series</td>
<td>6.2.2 through 6.2.2.4</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NGIPSv</td>
<td>6.2.1</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6.2.0 through 6.2.0.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6.1.0 through 6.1.0.6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RA VPN Default Setting Change Can Block VPN Traffic, on page 168</td>
<td>FTD with FMC</td>
<td>6.2.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>TLS/SSL Hardware Acceleration Enabled on Upgrade, on page 169</td>
<td>Firepower 2100 series</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0 only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Firepower 4100/9300</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER, on page 169</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FMC</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0 only</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ASA FirePOWER with ASDM</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Updated Security for Appliance Access, on page 169</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Security Intelligence Enables Application Identification, on page 170</td>
<td>FMC deployments</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Update VDB after Upgrade to Enable CIP Detection, on page 170</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 170</td>
<td>Any</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Syslog Behavior Changes for Connection and Intrusion Events, on page 171</td>
<td>FMC</td>
<td>6.1.0 through 6.2.3.x</td>
<td>6.3.0+</td>
</tr>
<tr>
<td></td>
<td>Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade, on page 171</td>
<td>Firepower 4100/9300</td>
<td>6.1.0.x</td>
<td>6.3.0 only</td>
</tr>
</tbody>
</table>

These previously published guidelines and warnings apply to intermediate releases. Review this checklist if your upgrade path skips major versions.
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 63: Version 6.3.0 Previously Published Guidelines**

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Changes to Result Limits in Reports, on page 174</td>
<td>FMC</td>
<td>6.1.0 through 6.2.2.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
<tr>
<td>✓</td>
<td>Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 175</td>
<td>FTD clusters</td>
<td>6.1.0.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
<tr>
<td>✓</td>
<td>Access Control Can Get Latency-Based Performance Settings from SRUs, on page 178</td>
<td>FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
<tr>
<td>✓</td>
<td>'Snort Fail Open' Replaces 'Failsafe' on FTD, on page 178</td>
<td>FTD with FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
</tbody>
</table>

---

**Table 64: Naming Schemes: Upgrade, Patch, and Hotfix Packages**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Naming Schemes</th>
</tr>
</thead>
</table>
| FMC      | New: Cisco_Firepower_Mgmt_Center  
           | Old: Sourcefire_3D_Defense_Center_S3 |
| Firepower 7000/8000 series | New: Cisco_Firepower_NGIPS_Appliance  
                             | Old: Sourcefire_3D_Device_S3 |
| NGIPSv   | New: Cisco_Firepower_NGIPS_Virtual  
           | Old: Sourcefire_3D_Device_VMware  
           | Old: Sourcefire_3D_Device_Virtual64_VMware |
Table 65: Naming Schemes: Installation Packages

<table>
<thead>
<tr>
<th>Platform</th>
<th>Naming Schemes</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC (physical)</td>
<td><strong>New:</strong> Cisco_Firepower_Mgmt_Center</td>
</tr>
<tr>
<td></td>
<td><strong>Old:</strong> Sourcefire_Defense_Center_M4</td>
</tr>
<tr>
<td></td>
<td><strong>Old:</strong> Sourcefire_Defense_Center_S3</td>
</tr>
<tr>
<td>FMCv: VMware</td>
<td><strong>New:</strong> Cisco_Firepower_Mgmt_Center_Virtual_VMware</td>
</tr>
<tr>
<td></td>
<td><strong>Old:</strong> Cisco_Firepower_Management_Center_Virtual_VMware</td>
</tr>
<tr>
<td>FMCv: KVM</td>
<td><strong>New:</strong> Cisco_Firepower_Mgmt_Center_Virtual_KVM</td>
</tr>
<tr>
<td></td>
<td><strong>Old:</strong> Cisco_Firepower_Management_Center_Virtual_KVM</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td><strong>New:</strong> Cisco_Firepower_NGIPS_Appliance</td>
</tr>
<tr>
<td></td>
<td><strong>Old:</strong> Sourcefire_3D_Device_S3</td>
</tr>
<tr>
<td>NGIPSv</td>
<td><strong>New:</strong> Cisco_Firepower_NGIPSv_VMware</td>
</tr>
<tr>
<td></td>
<td><strong>Old:</strong> Cisco_Firepower_NGIPS_Virtual</td>
</tr>
</tbody>
</table>

Reimaging to Version 6.3+ Disables LOM on Most Appliances

**Deployments:** Physical FMCs, 7000/8000 series devices

**Reimaging from:** Version 6.0+

**Directly to:** Version 6.3+

Freshly installing Version 6.3+ now automatically deletes Lights-Out Management (LOM) settings on most appliances, for security reasons. On a few older FMC models, you have the option of retaining LOM settings along with your management network settings.

If you delete network settings during a Version 6.3+ reimage, you must make sure you have physical access to the appliance to perform the initial configuration. You cannot use LOM. After you perform the initial configuration, you can reenable LOM and LOM users.

Table 66: Reimage Effect on LOM Settings

<table>
<thead>
<tr>
<th>Platform</th>
<th>Reimage to Version 6.2.3 or earlier</th>
<th>Reimage to Version 6.3+</th>
</tr>
</thead>
<tbody>
<tr>
<td>MC1600, 2600, 4600</td>
<td>Never deleted</td>
<td>Always deleted</td>
</tr>
<tr>
<td>MC1000, 2500, 4500</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MC2000, 4000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MC750, 1500, 3500</td>
<td>Deleted if you delete network settings</td>
<td>Deleted if you delete network settings</td>
</tr>
<tr>
<td>7000/8000 series</td>
<td>Always deleted</td>
<td>Always deleted</td>
</tr>
</tbody>
</table>
Timeouts for the URL Filtering Cache Can Change

Deployments: Any

Upgrading from: Version 6.2.3.x

Directly to: Version 6.3.0+

New for Version 6.3.0, the GUI allows you configure a timeout value for the URL filtering cache. To minimize instances of URLs matching on stale data, you can set URLs in the cache to expire. If you worked with Cisco TAC to specify a timeout value for the URL filtering cache, the upgrade may change that value.

After the upgrade completes:

- FMC: Choose System > Integration, click the Cisco CSI tab, and evaluate the Cached URLs Expire setting.
- FDM: Choose System Settings > Traffic Settings > URL Filtering Preferences and evaluate the URL Time to Live setting.

Readiness Check May Fail on FMC, 7000/8000 Series, NGIPSv

Deployments: FMC, 7000/8000 series devices, 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 67: Patches with Readiness Checks for Version 6.3.0+

<table>
<thead>
<tr>
<th>Readiness Check Not Supported</th>
<th>First Patch with Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1.0 through 6.1.0.6</td>
<td>6.1.0.7</td>
</tr>
<tr>
<td>6.2.0 through 6.2.0.6</td>
<td>6.2.0.7</td>
</tr>
<tr>
<td>6.2.1</td>
<td>None. Upgrade to Version 6.2.3.5+.</td>
</tr>
<tr>
<td>6.2.2 through 6.2.2.4</td>
<td>6.2.2.5</td>
</tr>
<tr>
<td>6.2.3 through 6.2.3.4</td>
<td>6.2.3.5</td>
</tr>
</tbody>
</table>

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.

### TLS/SSL Hardware Acceleration Enabled on Upgrade

**Deployments:** Firepower 2100 series, Firepower 4100/9300 chassis

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

**Directly to:** Version 6.3.0 only

The upgrade process automatically enables TLS/SSL hardware acceleration (sometimes called TLS crypto acceleration) on eligible devices. When it was introduced in Version 6.2.3, this feature was disabled by default on Firepower 4100/9300 chassis, and was not available on Firepower 2100 series devices.

Using TLS/SSL hardware acceleration on a managed device that is not decrypting traffic can affect performance. In Version 6.3.0.x, we recommend you disable this feature on devices that are not decrypting traffic.

To disable, use this CLI command:

```
system support ssl-hw-offload disable
```

### Upgrade Failure: Version 6.3.0-83 Upgrades to FMC and ASA FirePOWER

**Deployments:** Firepower Management Center, ASA FirePOWER (locally managed)

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

**Directly to:** Version 6.3.0-83

Some Firepower Management Centers and locally (ASDM) managed ASA FirePOWER modules experienced upgrade failures with Version 6.3.0, build 83. This issue was limited to a subset of customers who upgraded from Version 5.4.x. For more information, see CSCvn62123 in the Cisco Bug Search Tool.

A new upgrade package is now available. If you downloaded the Version 6.3.0-83 upgrade package, do not use it. If you already experienced an upgrade failure due to this issue, contact Cisco TAC.

### Updated Security for Appliance Access

**Deployments:** Any

**Upgrading from:** Version 6.1 through 6.2.3.x

**Directly to:** Version 6.3+
To enhance security, in Version 6.3 we updated the list of supported ciphers and cryptographic algorithms for secure SSH access. If your SSH client fails to connect with a Firepower appliance due to a cipher error, update your client to the latest version.

**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.
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.

**Syslog Behavior Changes for Connection and Intrusion Events**

**Deployments:** Firepower Management Center

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

**Directly to:** Version 6.3.0+

Version 6.3.0 changes and centralizes the way the system logs connection and intrusion events via syslog. You can access these settings on the new Logging tab in the access control policy.

The upgrade does not change your existing settings for connection event logging. However, you may suddenly start receiving intrusion events you did not "expect" via syslog. This is because after you upgrade to Version 6.3.0+, the intrusion policy sends syslog events to the destination on the new Logging tab. (Before Version 6.3.0, you could configure syslog alerting in an intrusion policy to send events to the syslog on the managed device itself rather than to an external host.)

Also, messages sent from NGIPS devices (7000/8000 series, ASA FirePOWER, NGIPSv) now use the ISO 8601 timestamp format as specified in RFC 5425.

**Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade**

**Deployments:** Firepower 4100/9300 with FTD

**Upgrading from:** Version 6.1.x on FXOS 2.0.1, 2.1.1, or 2.3.1

**Directly to:** Version 6.3.0 on FXOS 2.4.1

If your Firepower Management Center is running Version 6.2.3+, we strongly recommend you push (copy) Firepower upgrade packages to managed devices before you upgrade. This helps reduce the length of your upgrade maintenance window.

For Firepower 4100/9300 with FTD, best practice is to push before you begin the required companion FXOS upgrade. And, if you are upgrading from Version 6.1 directly to Version 6.3, this push is required. You must push before you upgrade FXOS.

This is because upgrading FXOS to Version 2.4.1 while still running Firepower 6.1 causes the device management port to flap, which in turn causes intermittent communication problems between the device and the FMC. You may see 'sftunnel daemon exited' alarms, and any task that involves sustained communications—such as pushing a large upgrade package—may fail.

To upgrade Firepower 4100/9300 with FTD, always follow this sequence:

<table>
<thead>
<tr>
<th>Valid</th>
<th>Invalid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include: 10.0.0.0/8</td>
<td>Include: 10.1.0.0/16</td>
</tr>
<tr>
<td>Exclude: 10.1.0.0/16</td>
<td>Exclude: 172.16.0.0/12</td>
</tr>
<tr>
<td></td>
<td>Exclude: 10.0.0.0/8</td>
</tr>
</tbody>
</table>
1. Upgrade the FMC to the target version.
2. Obtain the device upgrade package from the Cisco Support & Download site and upload it to the FMC.
3. Use the FMC to push the upgrade package to the device.
4. After the push completes, upgrade FXOS to the target version.
5. Immediately, use the FMC to upgrade the Firepower software on the device.

Remember, until you upgrade the Firepower software, you may continue to experience management port flaps.

**Version 6.2.3.x Guidelines**

<table>
<thead>
<tr>
<th>✓ Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch/Hotfix for Dynamic Analysis CA Certificates, on page 147</td>
<td>Any</td>
<td>6.2.3.x</td>
<td>Later patches</td>
</tr>
<tr>
<td>Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure, on page 172</td>
<td>FTD</td>
<td>6.2.3 through 6.2.3.9</td>
<td>6.2.3.10 only</td>
</tr>
<tr>
<td>Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 173</td>
<td>FTD with FMC</td>
<td>6.2.3 through 6.2.3.2</td>
<td>6.2.3.3</td>
</tr>
<tr>
<td>Hotfix Before Upgrading Version 6.2.3-88 FMCs, on page 173</td>
<td>FMC</td>
<td>6.2.3-88</td>
<td>6.2.3.1 through 6.2.3.3</td>
</tr>
</tbody>
</table>

**Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure**

**Deployments:** Firepower Threat Defense

**Upgrading from:** Version 6.2.3 through 6.2.3.9

**Directly to:** Version 6.2.3.10 only

**Known issue:** CSCvo39052

Upgrading an FTD device to Version 6.2.3.10 with CC mode enabled causes a FSIC (file system integrity check) failure when the device reboots.

**Caution**

If security certifications compliance is enabled and the FSIC fails, Firepower software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.

If your FTD deployment requires security certifications compliance (CC mode), we recommend you upgrade directly to Version 6.2.3.13+. For Firepower 4100/9300 devices, we also recommend that you upgrade to FXOS 2.3.1.130+. 
Version 6.2.3.3 FTD Device Cannot Switch to Local Management

**Deployments:** FTD wth FMC

**Upgrading from:** Version 6.2.3 through Version 6.2.3.2

**Directly to:** Version 6.2.3.3 only

In Version 6.2.3.3, you cannot switch Firepower Threat Defense device management from FMC to FDM. This happens even if you uninstall the Version 6.2.3.3 patch. If you want to switch to local management at that point, either freshly install Version 6.2.3, or contact Cisco TAC.

As a workaround, switch management before you upgrade to Version 6.2.3.3. Or, upgrade to the latest patch. Keep in mind that you lose device configurations when you switch management.

Note that you can switch management from FDM to FMC in Version 6.2.3.3.

Hotfix Before Upgrading Version 6.2.3-88 FMCs

**Deployments:** FMC

**Upgrading from:** Version 6.2.3-88

**Directly to:** Version 6.2.3.1, Version 6.2.3.2, or Version 6.2.3.3

Sometimes Cisco releases updated builds of Firepower upgrade packages. Version 6.2.3-88 has been replaced by a later build. If you upgrade an FMC running Version 6.2.3-88 to Version 6.2.3.1, Version 6.2.3.2, or Version 6.2.3.3, the SSE cloud connection continuously drops and generates errors. Uninstalling the patch does not resolve the issue.

If you are running Version 6.2.3-88, install Hotfix T before you upgrade.

Version 6.2.3 Guidelines

This checklist contains important upgrade guidelines and warnings that are *new* for this major version.

*Table 69: Version 6.2.3 New Guidelines*

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Sharing Data with Cisco, on page 174</td>
<td>Any</td>
<td>Any</td>
<td>6.2.3+</td>
</tr>
<tr>
<td></td>
<td>Edit/Resave Access Control Policies After Upgrade, on page 174</td>
<td>Any</td>
<td>6.1.0 through 6.2.2.x</td>
<td>6.2.3 only</td>
</tr>
<tr>
<td></td>
<td>Changes to Result Limits in Reports, on page 174</td>
<td>FMC</td>
<td>6.1.0 through 6.2.2.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 175</td>
<td>FTD clusters</td>
<td>6.1.0.x</td>
<td>6.2.3 through 6.4.0</td>
</tr>
</tbody>
</table>

These previously published guidelines and warnings apply to intermediate releases. Review this checklist if your upgrade path skips major versions.
Table 7: Version 6.2.3 Previously Published Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Access Control Can Get Latency-Based Performance Settings from SRUs, on page 178</td>
<td>FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
<tr>
<td>✓</td>
<td>'Snort Fail Open' Replaces 'Failsafe' on FTD, on page 178</td>
<td>FTD with FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
<tr>
<td>✓</td>
<td>Patch/Hotfix for Dynamic Analysis CA Certificates, on page 147</td>
<td>Any</td>
<td>6.1.0 through 6.2.3</td>
<td>Later versions</td>
</tr>
</tbody>
</table>

Sharing Data with Cisco

**Deployments:** Any

**Upgrading from:** Version 6.1.0+

**Directly to:** Version 6.2.3+

Various features involve sharing data with Cisco:

- In 6.2.3+, *Cisco Success Network* sends usage information and statistics to Cisco, which are essential to provide you with technical support.

- In 6.2.3+, *Web analytics tracking* sends non-personally-identifiable usage data to Cisco, including but not limited to page interactions, browser versions, product versions, user location, and management IP addresses or hostnames of your FMCs.

- In 6.5.0+, *Cisco Support Diagnostics* (sometimes called *Cisco Proactive Support*) sends configuration and operational health data to Cisco, and processes that data through our automated problem detection system, allowing us to proactively notify you of issues. This feature also allows Cisco TAC to collect essential information from your devices during the course of a TAC case.

These features may be automatically enabled. For information on accepting or declining participation, see the configuration guide.

Edit/Resave Access Control Policies After Upgrade

**Deployments:** Any

**Upgrading from:** Version 6.1 through 6.2.2.x

**Directly to:** Version 6.2.3 only

If you configured network or port objects that are used only in intrusion policy variable sets, deploying associated access control policies after the upgrade fails. If this happens, edit the access control policy, make a change (such as editing the description), save, and redeploy.

Changes to Result Limits in Reports

**Deployments:** Firepower Management Center
Upgrading from: Version 6.1.0 through 6.2.2.x

Directly to: Version 6.2.3 through 6.4.0

Version 6.2.3 limits the number of results you can use or include in a report section, as follows. For table and detail views, you can include fewer records in a PDF report than in an HTML/CSV report.

Table 71: New Result Limits in Reports

<table>
<thead>
<tr>
<th>Report Section Type</th>
<th>Max Records: HTML/CSV Report Section</th>
<th>Max Records: PDF Report Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bar chart</td>
<td>100 (top or bottom)</td>
<td>100 (top or bottom)</td>
</tr>
<tr>
<td>Pie chart</td>
<td>100 (top or bottom)</td>
<td></td>
</tr>
<tr>
<td>Table view</td>
<td>400,000</td>
<td>100,000</td>
</tr>
<tr>
<td>Detail view</td>
<td>1,000</td>
<td>500</td>
</tr>
</tbody>
</table>

If, before you upgrade a Firepower Management Center, a section in a report template specifies a larger number of results than the HTML/CSV maximum, the upgrade process lowers the setting to the new maximum value.

For report templates that generate PDF reports, if you exceed the PDF limit in any template section, the upgrade process changes the output format to HTML. To continue generating PDFs, lower the results limit to the PDF maximum. If you do this after the upgrade, set the output format back to PDF.

Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade

Deployments: Firepower Threat Defense clusters

Upgrading from: Version 6.1.x

Directly to: Version 6.2.3 through 6.4.0

Firepower Threat Defense Version 6.1.x clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in Version 6.2.0).

If you deployed or redeployed a Version 6.1.x cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, remove the site ID (set to 0) on each unit in FXOS before you upgrade. Otherwise, the units cannot rejoin the cluster after the upgrade.

If you already upgraded, remove the site ID from each unit, then reestablish the cluster. To view or change the site ID, see the Cisco FXOS CLI Configuration Guide.

Version 6.2.2.x Guidelines

Table 72: Version 6.2.2.x Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Patch/Hotfix for Dynamic Analysis CA Certificates, on page 147</td>
<td>Any</td>
<td>6.2.2.x</td>
<td>Later patches</td>
</tr>
</tbody>
</table>
Cannot Upgrade Firepower 2100 Series HA Pair from Version 6.2.2 to 6.2.2.4

**Deployments**: Firepower 2100 series devices configured as an FTD high availability pair

**Upgrading from**: Version 6.2.2 only

**Directly to**: Version 6.2.2.4 only

The upgrade from Version 6.2.2 to Version 6.2.2.4 fails for Firepower 2100 devices in high availability. If you are running Version 6.2.2 and really need to be at Version 6.2.2.4, upgrade to Version 6.2.2.1 first. Otherwise, we recommend you skip this version.

If you already started the upgrade and it has failed, we recommend you reimage.

Version 6.2.2 Guidelines

This checklist contains important upgrade guidelines and warnings that are new for this major version.

**Table 73: Version 6.2.2 New Guidelines**

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Security Enhancement: Signed Upgrade Packages, on page 176</td>
<td>Any</td>
<td>Any</td>
<td>6.2.2+</td>
</tr>
<tr>
<td></td>
<td>Version 6.2.2.1+ Required for 8000 Series Security Certs Compliance, on</td>
<td>Firepower 8000</td>
<td>6.2.0.x</td>
<td>6.2.2 only</td>
</tr>
<tr>
<td></td>
<td>page 177</td>
<td>series</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Security Enhancement: Signed Upgrade Packages

**Deployments**: Any

**Upgrading from**: Version 6.2.1+

**Directly to**: Version 6.2.2+

So that Firepower can verify that you are using the correct files, upgrade packages from (and hotfixes to) Version 6.2.1+ are signed tar archives (.tar). Upgrades from earlier versions continue to use unsigned packages.

When you manually download upgrade packages from the Cisco Support & Download site—for example, for a major upgrade or in an air-gapped deployment—make sure you download the correct package. Do not untar signed (.tar) packages.
After you upload a signed upgrade package, the GUI can take several minutes to load as the system verifies the package. Remove signed packages after you no longer need them to speed up the display.

**Version 6.2.2.1+ Required for 8000 Series Security Certs Compliance**

**Deployments:** Firepower 8000 series devices

**Upgrading from:** Version 6.2.0.x

**Directly to:** Version 6.2.2 only

Enabling security certifications compliance (CC/UCAPL mode) on 8000 series devices running Version 6.2.2 can cause a FSIC (file system integrity check) failure. Wait until you upgrade the device to Version 6.2.2.1+

**Caution**

Because the FSIC fails, Firepower software does not start, remote SSH access is disabled, and you can access the appliance only via local console. If this happens, contact Cisco TAC.

**Version 6.2.0.x Guidelines**

**Table 74: Version 6.2.0.x Guidelines**

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Patch/Hotfix for Dynamic Analysis CA Certificates, on page 147</td>
<td>Any</td>
<td>6.2.0.x</td>
<td>Later patches</td>
</tr>
<tr>
<td></td>
<td>Apply Hotfix BH to Version 6.2.0.3 FMCs, on page 177</td>
<td>FMC</td>
<td>6.2.0 through 6.2.0.2</td>
<td>6.2.0.3 only</td>
</tr>
</tbody>
</table>

**Apply Hotfix BH to Version 6.2.0.3 FMCs**

**Deployments:** FMC

**Upgrading from:** Version 6.2 through 6.2.0.2

**Directly to:** Version 6.2.0.3 only

**Resolves:** CSCvg32885

After you upgrade to Version 6.2.0.3, you must apply Hotfix BH. If you do not apply Hotfix BH, you cannot edit access control rules or deploy configuration changes.

For more information, see the Firepower Hotfix Release Notes.

**Version 6.2.0 Guidelines**

This checklist contains important upgrade guidelines and warnings that are new for this major version.
Table 75: Version 6.2.0 New Guidelines

<table>
<thead>
<tr>
<th>✓</th>
<th>Guideline</th>
<th>Platforms</th>
<th>Upgrading From</th>
<th>Directly To</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>Access Control Can Get Latency-Based Performance Settings from SRUs, on page 178</td>
<td>FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>'Snort Fail Open' Replaces 'Failsafe' on FTD, on page 178</td>
<td>FTD with FMC</td>
<td>6.1.0.x</td>
<td>6.2.0 through 6.4.0</td>
</tr>
<tr>
<td></td>
<td>IAB 'All Applications' Option Removed on Upgrade, on page 179</td>
<td>FMC, ASA FirePOWER with ASDM</td>
<td>6.1.0.3 or later patch</td>
<td>6.2.0 only</td>
</tr>
<tr>
<td></td>
<td>URL Filtering Sub-site Lookups for Low-Memory Devices Disabled on Upgrade, on page 180</td>
<td>Any</td>
<td>6.1.0.1 or later patch</td>
<td>6.2.0 only</td>
</tr>
</tbody>
</table>

Access Control Can Get Latency-Based Performance Settings from SRUs

**Deployments:** FMC

**Upgrading from:** 6.1.x

**Directly to:** 6.2.0+

New access control policies in Version 6.2.0+ by default get their latency-based performance settings from the latest intrusion rule update (SRU). This behavior is controlled by a new **Apply Settings From** option. To configure this option, edit or create an access control policy, click **Advanced**, and edit the Latency-Based Performance Settings.

When you upgrade to Version 6.2.0+, the new option is set according to your current (Version 6.1.x) configuration. If your current settings are:

- **Default:** The new option is set to **Installed Rule Update**. When you deploy after the upgrade, the system uses the latency-based performance settings from the latest SRU. It is possible that traffic handling could change, depending on what the latest SRU specifies.
- **Custom:** The new option is set to **Custom**. The system retains its current performance settings. There should be no behavior change due to this option.

We recommend you review your configurations before you upgrade. From the Version 6.1.x FMC web interface, view your policies' Latency-Based Performance Settings as described earlier, and see whether the **Revert to Defaults** button is dimmed. If the button is dimmed, you are using the default settings. If it is active, you have configured custom settings.

'Snort Fail Open' Replaces 'Failsafe' on FTD

**Deployments:** FTD with FMC

**Upgrading from:** Version 6.1.x

**Directly to:** Version 6.2+
In Version 6.2, the Snort Fail Open configuration replaces the Failsafe option on FMC-managed Firepower Threat Defense devices. While Failsafe allows you to drop traffic when Snort is busy, traffic automatically passes without inspection when Snort is down. Snort Fail Open allows you to drop this traffic.

When you upgrade an FTD device, its new Snort Fail Open setting depends on its old Failsafe setting, as follows. Although the new configuration should not change traffic handling, we still recommend that you consider whether to enable or disable Failsafe before you upgrade.

Table 76: Migrating Failsafe to Snort Fail Open

<table>
<thead>
<tr>
<th>Version 6.1 Failsafe</th>
<th>Version 6.2 Snort Fail Open</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled (default behavior)</td>
<td>Busy: Disabled Down: Enabled</td>
<td>New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down.</td>
</tr>
<tr>
<td>Enabled</td>
<td>Busy: Enabled Down: Enabled</td>
<td>New and existing connections pass without inspection when the Snort process is busy or down.</td>
</tr>
</tbody>
</table>

Note that Snort Fail Open requires Version 6.2 on the device. If you are managing a Version 6.1.x device, the FMC web interface displays the Failsafe option.

**IAB 'All Applications' Option Removed on Upgrade**

**Deployments:** FMC, ASA FirePOWER with ASDM

**Upgrading from:** 6.1.0.3 or later patch

**Directly to:** 6.2.0 only

The Intelligent Application Bypass (IAB) option 'All applications including unidentified applications' trusts any application that exceeds any flow bypass threshold, regardless of application type, if one of the IAB inspection performance thresholds is met. The option is available in the following versions:

- Version 6.0.1.4 and later patches
- Version 6.1.0.3 and later patches
- Version 6.2.0.1 and later patches
- Version 6.2.2 and all later patches and major versions

If you upgrade from a version where the option is supported to one where it is not, the option is removed. Also, if you actually enabled the option and your access control policy does not contain IAB bypassable application and filter configurations, the upgraded user interface exhibits the following unexpected behaviors:

- IAB is enabled, but the All applications including unidentified applications option is no longer present.
- The IAB configuration page displays 1 Applications/Filters, incorrectly indicating that you have configured one application or filter.
- The Selected Applications and Filters window in the applications and filters editor displays either deleted (FMC) or Any Application (ASDM). We recommend you delete this selection.

To restore the option, apply any Version 6.2.0.x patch, or upgrade to Version 6.2.2+ (recommended).
URL Filtering Sub-site Lookups for Low-Memory Devices Disabled on Upgrade

**Deployments:** Lower-memory devices performing URL filtering

**Upgrading from:** Version 6.1.0.3 or later patch

**Directly to:** Version 6.2.0 only

Due to memory limitations, some device models perform URL filtering with a smaller database of categories and reputations. This can become an issue if a URL's subsites have different URL categories and reputations than the parent site, but the device only has the parent site's data.

In Version 6.1.0.3, we changed the system's behavior so that instead of relying on the parent URL's category and reputation, the device considers these subsites to have an 'unknown' category and reputation. This forces the device to perform a cloud lookup for the subsite's data (and cache the results for next time).

Version 6.2.0 discontinues support for these subsite cloud lookups. Affected devices are:

- Firepower 7010, 7020, and 7030
- ASA 5506-X series, 5508-X, 5516-X
- ASA 5512-X, 5515-X, 5525-X

Support is reintroduced in Version 6.2.0.1.

### Version 6.1.0 Guidelines

These important warnings apply to Version 6.1.0.

**Disable the ASA REST API Before Upgrading ASA FirePOWER Modules**

**Deployments:** ASA FirePOWER

---

**Note**

This warning applies to all future releases. The upgrade procedures now explicitly include this step.

Before you upgrade an ASA FirePOWER module, use the ASA CLI to disable the ASA REST API:

```bash
don rest-api agent
```

If you do not disable the REST API, the upgrade fails. You can reenable it after the upgrade:

```bash
rest-api agent
```

ASA 5506-X series devices do not support the ASA REST API if you are also running Version 6.0+ of the ASA FirePOWER module.

**STIG Mode Changed to UCAPL Mode**

**Deployments:** Firepower Management Center

In Version 6.1, the security certifications compliance mode known as Security Technical Implementation Guide (STIG) mode is renamed to Unified Capabilities Approved Products List (UCAPL) mode. After the upgrade, a Firepower appliance that was in STIG mode will be in UCAPL mode. All of the restrictions and changes in system functionality associated with UCAPL mode will be in effect.
For more information, including information on hardening your system for UCAPL compliance, see the Security Certifications Compliance chapter of the Firepower Management Center Configuration Guide, and the guidelines for this product provided by the certifying entity.

**Restore Classic Licenses After Upgrade**

**Deployments:** Firepower Management Center

Upgrading the Firepower Management Center to Version 6.1 may delete or disable Classic licenses for managed NGIPSv, ASA FirePOWER, 7000 series, and 8000 series devices. Before you begin the update, contact Cisco TAC for a script you can run to prevent this issue.

If you do not run the pre-upgrade script, after the update:

- Check and reinstall deleted licenses: Choose **System > Licenses > Classic Licenses**.
- Edit affected devices and reenable licenses: Choose **Devices > Device Management**.

### Version 6.0.0 Guidelines

These important warnings apply to Version 6.0.0.

**Terminology and Branding**

Version 6.0 has major terminology and branding changes, including:

- FireSIGHT System → Firepower
- FireSIGHT Defense Center → Firepower Management Center (FMC)
- Series 3 device → 7000 series device or 8000 series device
- virtual managed device → NGIPSv

For more information, see the Cisco Firepower Terminology Guide.

**Version 6.0 Preinstallation Package**

For upgrades from Version 5.4.x to Version 6.0, Cisco provides a preinstallation package that optimizes the upgrade.

In some cases you **must** use the preinstallation package, as listed in the following table. And even when it is not required, we **strongly** recommend you include and use the Version 6.0 preinstallation package in your upgrade path. For more information, see FireSIGHT System Release Notes Version 6.0.0 Preinstallation.

<table>
<thead>
<tr>
<th>Platform</th>
<th>Min. Version to Upgrade</th>
<th>Package Required</th>
<th>Package Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>FireSIGHT Defense Center (FMC)</td>
<td>5.4.1.1</td>
<td>5.4.1.1 to 5.4.1.5</td>
<td>5.4.1.6+</td>
</tr>
<tr>
<td>7000/8000 series</td>
<td>5.4.0.2</td>
<td>5.4.0.2 to 5.4.0.6</td>
<td>5.4.0.7+</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>5.4.0.2</td>
<td>5.4.0.2 to 5.4.0.6</td>
<td>5.4.0.7+</td>
</tr>
<tr>
<td>ASA FirePOWER: 5.4.1.x</td>
<td>5.4.1.1</td>
<td>5.4.1.1 to 5.4.1.5</td>
<td>5.4.1.6+</td>
</tr>
<tr>
<td>Platform</td>
<td>Min. Version to Upgrade</td>
<td>Package Required</td>
<td>Package Recommended</td>
</tr>
<tr>
<td>------------------------</td>
<td>-------------------------</td>
<td>------------------------</td>
<td>----------------------</td>
</tr>
<tr>
<td>ASA FirePOWER: 5.4.0.x</td>
<td>5.4.0.2</td>
<td>5.4.0.2 to 5.4.0.6</td>
<td>5.4.0.7+</td>
</tr>
</tbody>
</table>

**Upgrade Memory for DC750, DC1500, DC3500 and Virtual Defense Center**

The following FireSIGHT Defense Center models may require additional memory to run Version 6.0:

- DC750
- DC1500
- DC3500
- Virtual Defense Center

Because the increase in memory is driven by Cisco product requirements, Cisco makes memory upgrade kits available at no cost for customers who are entitled to run Version 6.0 on a qualifying DC750 or DC1500:

- Order the kit—See Field Notice: FN - 64077 - Cisco FireSIGHT and Sourcefire Defense Center Management Appliances - Memory Upgrade Required for FirePOWER Software V6.0 and Later
- Upgrade the memory—See Memory Upgrade Instructions for Firepower Management Centers in the Firepower Management Center Installation Guide.

**Break Defense Center High Availability Pairs**

Version 6.0.x does not support high availability for Firepower Management Centers.

You cannot upgrade a Version 5.4.x high availability pair of Defense Centers to a Version 6.0 high availability pair of Firepower Management Centers. You must break the pair and upgrade each Defense Center individually. You can reestablish high availability with Version 6.1.

**Disable "Retry URL Cache Miss Lookup" Option**

Upgrading a Firepower Management Center to Version 6.0 when you are managing devices running Version 5.4.0.6, Version 5.4.1.5, or earlier may cause traffic outages and system issues.

Before you upgrade the Defense Center, disable the **Retry URL cache miss lookup** option, which you set on the Advanced tab in the access control policies deployed to your devices. Then, redeploy. You can reenable the option after you upgrade your managed devices to Version 5.4.0.7+ or Version 5.4.1.6+ (or Version 6.0).

**Update Defense Center HTTPS Certificates**

If you upgrade a Version 5.4.x Defense Center that is using one of these HTTPS certificates to a Version 6.0 Firepower Management Center, you will not be able to log in and must contact Cisco TAC:

- Certificates generated with an RSASSA-PSS signature algorithm.
  
  Before you upgrade, replace with a certificate generated with either a sha1WithRSAEncryption algorithm or sha256WithRSAEncryption algorithm, or with the Defense Center default certificate. Reboot.

- Certificates generated using a public server key larger than 2048 bits.
  
  Before you upgrade, replace with a certificate generated with a server certificate request (CSR). Reboot.
Also, do *not* upload either of these types of certificates after you upgrade. To generate a certificate on a Version 5.4.x appliance, see Using Custom HTTPS Certificates in the *FireSIGHT System User Guide*, Version 5.4.1.

**No Private AMP Cloud Support**

Version 6.0 does not support AMP for Firepower signature lookups with the private AMP cloud. In Version 6.0, the system automatically submits SHA-256 signatures to the public AMP cloud. If you have a private AMP cloud and are receiving events from endpoints, the Version 6.0 Defense Center will continue to receive those events without any additional changes to your configuration.
CHAPTER 15

Time Tests and Disk Space Requirements

To upgrade a Firepower appliance, you must have enough free disk space or the upgrade fails. When you use the Firepower Management Center to upgrade a managed device, the FMC requires additional disk space in its /Volume partition, for the device upgrade package. You must also have enough time to perform the upgrade.

We provide reports of in-house time and disk space tests for reference purposes.

- About Time Tests, on page 186
- About Disk Space Requirements, on page 187
- Version 6.6.0 Time and Disk Space, on page 188
- Version 6.5.0.4 Time and Disk Space, on page 188
- Version 6.5.0.3 Time and Disk Space, on page 189
- Version 6.5.0.2 Time and Disk Space, on page 189
- Version 6.5.0.1 Time and Disk Space, on page 190
- Version 6.5.0 Time and Disk Space, on page 190
- Version 6.4.0.8 Time and Disk Space, on page 190
- Version 6.4.0.7 Time and Disk Space, on page 191
- Version 6.4.0.6 Time and Disk Space, on page 191
- Version 6.4.0.5 Time and Disk Space, on page 192
- Version 6.4.0.4 Time and Disk Space, on page 192
- Version 6.4.0.3 Time and Disk Space, on page 193
- Version 6.4.0.2 Time and Disk Space, on page 193
- Version 6.4.0.1 Time and Disk Space, on page 194
- Version 6.4.0 Time and Disk Space, on page 194
- Version 6.3.0.5 Time and Disk Space, on page 195
- Version 6.3.0.4 Time and Disk Space, on page 195
- Version 6.3.0.3 Time and Disk Space, on page 196
- Version 6.3.0.2 Time and Disk Space, on page 197
- Version 6.3.0.1 Time and Disk Space, on page 197
- Version 6.3.0 Time and Disk Space, on page 198
- Version 6.2.3.15 Time and Disk Space, on page 198
- Version 6.2.3.14 Time and Disk Space, on page 199
- Version 6.2.3.13 Time and Disk Space, on page 199
- Version 6.2.3.12 Time and Disk Space, on page 200
- Version 6.2.3.11 Time and Disk Space, on page 200
- Version 6.2.3.10 Time and Disk Space, on page 201
About Time Tests

Time values given here are based on in-house tests.
Although we report the slowest time of all upgrades tested for a particular platform/series, your upgrade will likely take longer than the provided times for multiple reasons, provided below.

**Test Conditions**

- **Deployment**: Values are from tests in a Firepower Management Center deployment. This is because raw upgrade times for remotely and locally managed devices are similar, given similar conditions.

- **Versions**: For major upgrades, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version.

- **Models**: In most cases, we test on the lowest-end models in each series, and sometimes on multiple models in a series.

- **Virtual settings**: We test with the default settings for memory and resources.

- **High availability and scalability**: 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. Note that stacked 8000 series devices upgrade simultaneously, with the stack operating in limited, mixed-version state until all devices complete the upgrade. This should not take significantly 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.

**Time Is For Upgrade Only**

Values represent only the time it takes for the Firepower upgrade script to run on each platform. They do not include time for:

- Transferring upgrade packages to managed devices, whether before or during upgrade.

- Readiness checks.

- VDB and SRU updates.

- Deploying configurations.

- Reboots (values may be provided separately).

### About Disk Space Requirements

Space estimates are the largest reported for all upgrades. For releases after early 2020, they are:

- Not rounded up (under 1 MB).
• Rounded up to the next 1 MB (1 MB - 100 MB).
• Rounded up to the next 10 MB (100 MB - 1GB).
• Rounded up to the next 100 MB (greater than 1 GB).

Version 6.6.0 Time and Disk Space

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>
<thead>
<tr>
<th>Platform</th>
<th>Space on FMC</th>
<th>Upgrade Time</th>
<th>Reboot Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>16.5 GB</td>
<td>46 min</td>
<td>15 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>16.7 GB</td>
<td>36 min</td>
<td>7 min</td>
</tr>
<tr>
<td>Firepower 1000 series</td>
<td>410 MB</td>
<td>11.5 GB</td>
<td>1.1 GB</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>470 MB</td>
<td>10.3 GB</td>
<td>1 GB</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>61 MB</td>
<td>9.3 GB</td>
<td>980 MB</td>
</tr>
<tr>
<td>Firepower 4100 series container instance</td>
<td>46 MB</td>
<td>11.3 GB</td>
<td>980 MB</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>64 MB</td>
<td>10.5 GB</td>
<td>980 MB</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>8.7 GB</td>
<td>70 KB</td>
<td>1.2GB</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>8.7 GB</td>
<td>70 KB</td>
<td>1.2 GB</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>11.4 GB</td>
<td>63 MB</td>
<td>1.4 GB</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>6.1 GB</td>
<td>53 MB</td>
<td>860 MB</td>
</tr>
</tbody>
</table>

Version 6.5.0.4 Time and Disk Space

Table 78: Version 6.5.0.4 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 1000 series</td>
<td>500 MB</td>
<td>20 min</td>
</tr>
</tbody>
</table>
## Version 6.5.0.3 Time and Disk Space

Version 6.5.0.3 was removed from the Cisco Support & Download site on 2019-02-04 (for FMCs) and 2020-03-02 (for devices). If you are running this version, it is safe to continue.

### Version 6.5.0.3 Time and Disk Space

**Table 79: Version 6.5.0.3 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 2100 series</td>
<td>2.5 GB</td>
<td>2.5 GB</td>
<td>530 MB</td>
<td>18 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>2.5 GB</td>
<td>2.5 GB</td>
<td>360 MB</td>
<td>13 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>2.5 GB</td>
<td>2.5 GB</td>
<td>360 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.9 GB</td>
<td>110 MB</td>
<td>310 MB</td>
<td>16 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.9 GB</td>
<td>110 MB</td>
<td>310 MB</td>
<td>9 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2.6 GB</td>
<td>20 MB</td>
<td>340 MB</td>
<td>72 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>740 MB</td>
<td>20 MB</td>
<td>230 MB</td>
<td>8 min</td>
</tr>
</tbody>
</table>

## Version 6.5.0.2 Time and Disk Space

### Table 79: Version 6.5.0.2 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>2.6 GB</td>
<td>20 MB</td>
<td>—</td>
<td>42 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>2.7 GB</td>
<td>23 MB</td>
<td>—</td>
<td>34 min</td>
</tr>
<tr>
<td>Firepower 1000 series</td>
<td>2.5 GB</td>
<td>2.5 GB</td>
<td>480 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.3 GB</td>
<td>2.3 GB</td>
<td>500 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>2.3 GB</td>
<td>2.3 GB</td>
<td>340 MB</td>
<td>13 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>2.3 GB</td>
<td>2.3 GB</td>
<td>340 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.9 GB</td>
<td>110 MB</td>
<td>280 MB</td>
<td>22 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.7 GB</td>
<td>110 MB</td>
<td>280 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2.5 GB</td>
<td>20 MB</td>
<td>320 MB</td>
<td>56 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>680 MB</td>
<td>18 MB</td>
<td>210 MB</td>
<td>9 min</td>
</tr>
</tbody>
</table>
**Version 6.5.0.1 Time and Disk Space**

Version 6.5.0.1 was removed from the Cisco Support & Download site on 2019-12-19. If you are running this version, we recommend you upgrade.

**Version 6.5.0 Time and Disk Space**

Table 80: Version 6.5.0 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>18.6 GB</td>
<td>24 MB</td>
<td>—</td>
<td>47 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>18.7 GB</td>
<td>30 MB</td>
<td>—</td>
<td>35 min</td>
</tr>
<tr>
<td>Firepower 1000 series</td>
<td>1 GB</td>
<td>11.3 GB</td>
<td>1.1 GB</td>
<td>10 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1.1 GB</td>
<td>12.3 GB</td>
<td>1 GB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>20 MB</td>
<td>10.8 GB</td>
<td>990 MB</td>
<td>8 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>23 MB</td>
<td>10.9 GB</td>
<td>990 MB</td>
<td>8 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>10.4 GB</td>
<td>120 KB</td>
<td>1.1 GB</td>
<td>17 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>10 GB</td>
<td>120 KB</td>
<td>1.1 GB</td>
<td>10 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>12.2 GB</td>
<td>26 MB</td>
<td>1.3 GB</td>
<td>81 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>6.6 GB</td>
<td>22 MB</td>
<td>870 MB</td>
<td>9 min</td>
</tr>
</tbody>
</table>

**Version 6.4.0.8 Time and Disk Space**

Table 81: Version 6.4.0.8 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>5 GB</td>
<td>170 MB</td>
<td>—</td>
<td>44 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>5.1 GB</td>
<td>170 MB</td>
<td>—</td>
<td>32 min</td>
</tr>
<tr>
<td>Firepower 1000 series</td>
<td>3 GB</td>
<td>3 GB</td>
<td>530 MB</td>
<td>18 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.5 GB</td>
<td>2.5 GB</td>
<td>510 MB</td>
<td>18 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.8 GB</td>
<td>1.8 GB</td>
<td>310 MB</td>
<td>14 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>2 GB</td>
<td>2 GB</td>
<td>310 MB</td>
<td>11 min</td>
</tr>
</tbody>
</table>
## Version 6.4.0.7 Time and Disk Space

Table 82: Version 6.4.0.7 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.8 GB</td>
<td>110 MB</td>
<td>290 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.9 GB</td>
<td>110 MB</td>
<td>290 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.7 GB</td>
<td>190 MB</td>
<td>650 MB</td>
<td>25 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2.2 GB</td>
<td>110 MB</td>
<td>590 MB</td>
<td>16 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.1 GB</td>
<td>150 MB</td>
<td>450 MB</td>
<td>9 min</td>
</tr>
</tbody>
</table>

## Version 6.4.0.6 Time and Disk Space

Version 6.4.0.6 was removed from the Cisco Support & Download site on 2019-12-19. If you are running this version, we recommend you upgrade.
# Version 6.4.0.5 Time and Disk Space

**Table 83: Version 6.4.0.5 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>5 GB</td>
<td>170 MB</td>
<td>—</td>
<td>39 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>3.7 GB</td>
<td>170 MB</td>
<td>—</td>
<td>27 min</td>
</tr>
<tr>
<td>Firepower 1000 series</td>
<td>2.9 GB</td>
<td>2.9 GB</td>
<td>530 MB</td>
<td>26 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.5 GB</td>
<td>2.5 GB</td>
<td>500 MB</td>
<td>16 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.8 GB</td>
<td>1.8 GB</td>
<td>310 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.8 GB</td>
<td>1.8 GB</td>
<td>310 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.8 GB</td>
<td>110 MB</td>
<td>290 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.8 GB</td>
<td>110 MB</td>
<td>290 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.6 GB</td>
<td>170 MB</td>
<td>650 MB</td>
<td>26 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>4.1 GB</td>
<td>36 MB</td>
<td>590 MB</td>
<td>45 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.1 GB</td>
<td>150 MB</td>
<td>450 MB</td>
<td>10 min</td>
</tr>
</tbody>
</table>

# Version 6.4.0.4 Time and Disk Space

**Table 84: Version 6.4.0.4 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>4.4 GB</td>
<td>170 MB</td>
<td>—</td>
<td>35 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>4.8 GB</td>
<td>170 MB</td>
<td>—</td>
<td>31 min</td>
</tr>
<tr>
<td>Firepower 1000 series</td>
<td>2.9 GB</td>
<td>2.9 GB</td>
<td>520 MB</td>
<td>28 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.4 GB</td>
<td>2.4 GB</td>
<td>500 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>2 GB</td>
<td>2 GB</td>
<td>310 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.7 GB</td>
<td>1.7 GB</td>
<td>310 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.8 GB</td>
<td>110 MB</td>
<td>290 MB</td>
<td>29 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.8 GB</td>
<td>110 MB</td>
<td>290 MB</td>
<td>8 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.6 GB</td>
<td>170 MB</td>
<td>650 MB</td>
<td>24 min</td>
</tr>
</tbody>
</table>
### Version 6.4.0.3 Time and Disk Space

*Table 85: Version 6.4.0.3 Time and Disk Space*

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA FirePOWER</td>
<td>4.2 GB</td>
<td>36 MB</td>
<td>600 MB</td>
<td>55 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.1 GB</td>
<td>150 MB</td>
<td>550 MB</td>
<td>10 min</td>
</tr>
</tbody>
</table>

### Version 6.4.0.2 Time and Disk Space

*Table 86: Version 6.4.0.2 Time and Disk Space*

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>3.2 GB</td>
<td>24 MB</td>
<td>—</td>
<td>34 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>2.5 GB</td>
<td>23 MB</td>
<td>—</td>
<td>25 min</td>
</tr>
<tr>
<td>Firepower 1000 series</td>
<td>2.9 GB</td>
<td>2.9 GB</td>
<td>520 MB</td>
<td>22 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.4 GB</td>
<td>2.4 GB</td>
<td>500 MB</td>
<td>19 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.7 GB</td>
<td>1.7 GB</td>
<td>310 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.7 GB</td>
<td>1.7 GB</td>
<td>310 MB</td>
<td>14 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.8 GB</td>
<td>110 MB</td>
<td>290 MB</td>
<td>18 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.8 GB</td>
<td>110 MB</td>
<td>290 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>1.9 GB</td>
<td>21 MB</td>
<td>370 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2.5 GB</td>
<td>2.5 GB</td>
<td>320 MB</td>
<td>28 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>690 MB</td>
<td>21 MB</td>
<td>210 MB</td>
<td>8 min</td>
</tr>
</tbody>
</table>
### Version 6.4.0.1 Time and Disk Space

**Table 87: Version 6.4.0.1 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.8 GB</td>
<td>110 MB</td>
<td>270 MB</td>
<td>21 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.2 GB</td>
<td>110 MB</td>
<td>270 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>1.9 GB</td>
<td>36 MB</td>
<td>350 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2 GB</td>
<td>21 MB</td>
<td>300 MB</td>
<td>34 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>630 MB</td>
<td>21 MB</td>
<td>190 MB</td>
<td>10 min</td>
</tr>
</tbody>
</table>

### Version 6.4.0 Time and Disk Space

**Table 88: Version 6.4.0 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.4.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>1.8 GB</td>
<td>24 MB</td>
<td>—</td>
<td>50 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>1.8 GB</td>
<td>23 MB</td>
<td>—</td>
<td>20 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1.4 GB</td>
<td>1.4 GB</td>
<td>300 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.1 GB</td>
<td>1.1 GB</td>
<td>95 MB</td>
<td>9 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.1 GB</td>
<td>1.1 GB</td>
<td>95 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>550 MB</td>
<td>110 MB</td>
<td>76 MB</td>
<td>16 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>550 MB</td>
<td>110 MB</td>
<td>76 MB</td>
<td>15 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>59 MB</td>
<td>21 MB</td>
<td>2 MB</td>
<td>14 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>85 MB</td>
<td>20 MB</td>
<td>2 MB</td>
<td>30 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>45 MB</td>
<td>21 MB</td>
<td>2 MB</td>
<td>10 min</td>
</tr>
</tbody>
</table>

---

**Cisco Firepower Management Center Upgrade Guide**

194
### Version 6.3.0.5 Time and Disk Space

**Table 89: Version 6.3.0.5 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 4100 series</td>
<td>10 MB</td>
<td>7.5 GB</td>
<td>920 MB</td>
<td>6 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>10 MB</td>
<td>7.7 GB</td>
<td>920 MB</td>
<td>7 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>9 GB</td>
<td>110 KB</td>
<td>1.1 GB</td>
<td>24 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>7.5 GB</td>
<td>100 KB</td>
<td>1.1 GB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>7.7 GB</td>
<td>19 MB</td>
<td>980 MB</td>
<td>34 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>11.5 GB</td>
<td>22 MB</td>
<td>1.3 GB</td>
<td>66 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>6.5 GB</td>
<td>19 MB</td>
<td>840 MB</td>
<td>16 min</td>
</tr>
</tbody>
</table>

### Version 6.3.0.4 Time and Disk Space

**Table 90: Version 6.3.0.4 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>4.9 GB</td>
<td>200 MB</td>
<td>—</td>
<td>46 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>4.5 GB</td>
<td>180 MB</td>
<td>—</td>
<td>41 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.3 GB</td>
<td>2.3 GB</td>
<td>480 MB</td>
<td>21 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.6 GB</td>
<td>1.6 GB</td>
<td>280 MB</td>
<td>13 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.6 GB</td>
<td>1.6 GB</td>
<td>280 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.7 GB</td>
<td>110 MB</td>
<td>270 MB</td>
<td>26 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.7 GB</td>
<td>110 MB</td>
<td>270 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>2.6 GB</td>
<td>210 MB</td>
<td>600 MB</td>
<td>23 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3.6 GB</td>
<td>47 MB</td>
<td>540 MB</td>
<td>74 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.1 GB</td>
<td>160 MB</td>
<td>440 MB</td>
<td>17 min</td>
</tr>
</tbody>
</table>
### Version 6.3.0.3 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /Zone</th>
<th>Space on FMC</th>
<th>Time from 6.3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMCv: VMware 6.0</td>
<td>4.4 GB</td>
<td>180 MB</td>
<td>—</td>
<td>38 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.3 GB</td>
<td>2.3 GB</td>
<td>480 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.6 GB</td>
<td>1.6 GB</td>
<td>280 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.8 GB</td>
<td>1.8 GB</td>
<td>280 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.7 GB</td>
<td>110 MB</td>
<td>270 MB</td>
<td>23 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>1.7 GB</td>
<td>110 MB</td>
<td>270 MB</td>
<td>18 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.3 GB</td>
<td>170 MB</td>
<td>600 MB</td>
<td>21 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3.5 GB</td>
<td>31 MB</td>
<td>530 MB</td>
<td>48 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.1 GB</td>
<td>160 MB</td>
<td>430 MB</td>
<td>16 min</td>
</tr>
</tbody>
</table>

**Table 91: Version 6.3.0.3 Time and Disk Space**
## Version 6.3.0.2 Time and Disk Space

Table 92: Version 6.3.0.2 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>3.5 GB</td>
<td>180 MB</td>
<td>—</td>
<td>53 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>3.2 GB</td>
<td>180 MB</td>
<td>—</td>
<td>28 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1.2 GB</td>
<td>1.2 GB</td>
<td>100 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>970 MB</td>
<td>970 MB</td>
<td>100 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>970 MB</td>
<td>970 MB</td>
<td>100 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>570 MB</td>
<td>110 MB</td>
<td>80 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>600 MB</td>
<td>110 MB</td>
<td>80 MV</td>
<td>10 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>2.5 GB</td>
<td>170 MB</td>
<td>400 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3 GB</td>
<td>30 MB</td>
<td>340 MB</td>
<td>45 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>1.5 GB</td>
<td>160 MB</td>
<td>250 MB</td>
<td>10 min</td>
</tr>
</tbody>
</table>

## Version 6.3.0.1 Time and Disk Space

Table 93: Version 6.3.0.1 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.3.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>3 GB</td>
<td>170 MB</td>
<td>—</td>
<td>31 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>2.4 GB</td>
<td>170 MB</td>
<td>—</td>
<td>25 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1.2 GB</td>
<td>1.2 GB</td>
<td>290 MB</td>
<td>18 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>740 MB</td>
<td>740 MB</td>
<td>100 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>740 MB</td>
<td>740 MB</td>
<td>100 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>400 MB</td>
<td>150 MB</td>
<td>72 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>400 MB</td>
<td>150 MB</td>
<td>72 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>2.1 GB</td>
<td>170 MB</td>
<td>350 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2.4 GB</td>
<td>28 MB</td>
<td>270 MB</td>
<td>44 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>1.5 GB</td>
<td>150 MB</td>
<td>350 MB</td>
<td>10 min</td>
</tr>
</tbody>
</table>
## Version 6.3.0 Time and Disk Space

### Table 94: Version 6.3.0 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>12.7 GB</td>
<td>29 MB</td>
<td>—</td>
<td>47 min</td>
</tr>
<tr>
<td>FMCv on: VMware 6.0</td>
<td>12.7 GB</td>
<td>29 MB</td>
<td>—</td>
<td>29 min</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>13 MB</td>
<td>8.8 GB</td>
<td>930 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>10 MB</td>
<td>7.6 GB</td>
<td>930 MB</td>
<td>6 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>7.9 GB</td>
<td>100 KB</td>
<td>1.1 GB</td>
<td>25 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>7.3 GB</td>
<td>100 KB</td>
<td>1.1 GB</td>
<td>12 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>7.0 GB</td>
<td>19 MB</td>
<td>920 MB</td>
<td>32 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>11.3 GB</td>
<td>22 MB</td>
<td>1.2 GB</td>
<td>63 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>5.7 GB</td>
<td>19 MB</td>
<td>810 MB</td>
<td>16 min</td>
</tr>
</tbody>
</table>

## Version 6.2.3.15 Time and Disk Space

### Table 95: Version 6.2.3.15 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>4.7 GB</td>
<td>260 MB</td>
<td>—</td>
<td>50 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>4.7 GB</td>
<td>210 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.3 GB</td>
<td>2.3 GB</td>
<td>590 MB</td>
<td>27 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.7 GB</td>
<td>1.7 GB</td>
<td>390 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>2.4 GB</td>
<td>2.4 GB</td>
<td>390 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>2 GB</td>
<td>190 MB</td>
<td>410 MB</td>
<td>38 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>2.4 GB</td>
<td>190 MB</td>
<td>410 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.5 GB</td>
<td>210 MB</td>
<td>640 MB</td>
<td>19 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3.9 GB</td>
<td>56 MB</td>
<td>580 MB</td>
<td>100 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.7 GB</td>
<td>180 MB</td>
<td>470 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
# Version 6.2.3.14 Time and Disk Space

## Table 96: Version 6.2.3.14 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>4.5 GB</td>
<td>260 MB</td>
<td>—</td>
<td>58 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>4.7 GB</td>
<td>190 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1.9 GB</td>
<td>1.9 GB</td>
<td>590 MB</td>
<td>23 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.7 GB</td>
<td>1.7 GB</td>
<td>390 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.7 GB</td>
<td>1.7 GB</td>
<td>390 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>2 GB</td>
<td>200 MB</td>
<td>410 MB</td>
<td>32 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>2.4 GB</td>
<td>190 MB</td>
<td>410 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.4 GB</td>
<td>200 MB</td>
<td>630 MB</td>
<td>19 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3.7 GB</td>
<td>53 MB</td>
<td>560 MB</td>
<td>106 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.6 GB</td>
<td>190 MB</td>
<td>470 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

# Version 6.2.3.13 Time and Disk Space

## Table 97: Version 6.2.3.13 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>4.7 GB</td>
<td>290 MB</td>
<td>—</td>
<td>50 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>4.6 GB</td>
<td>190 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.6 GB</td>
<td>2.6 GB</td>
<td>590 MB</td>
<td>25 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>1.7 GB</td>
<td>1.7 GB</td>
<td>390 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.8 GB</td>
<td>1.8 GB</td>
<td>390 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>2.4 GB</td>
<td>190 MB</td>
<td>410 MB</td>
<td>32 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>2.3 GB</td>
<td>190 MB</td>
<td>410 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.8 GB</td>
<td>190 MB</td>
<td>620 MB</td>
<td>18 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3.7 GB</td>
<td>51 MB</td>
<td>560 MB</td>
<td>105 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.6 GB</td>
<td>180 MB</td>
<td>470 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
## Version 6.2.3.12 Time and Disk Space

**Table 98: Version 6.2.3.12 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>3.9 GB</td>
<td>220 MB</td>
<td>—</td>
<td>49 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>4.6 GB</td>
<td>160 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1.9 GB</td>
<td>1.9 GB</td>
<td>390 MB</td>
<td>21 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>970 MB</td>
<td>970 MB</td>
<td>190 MB</td>
<td>14 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.7 GB</td>
<td>1.7 GB</td>
<td>190 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.4 GB</td>
<td>96 MB</td>
<td>210 MB</td>
<td>30 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>2.4 GB</td>
<td>200 MB</td>
<td>210 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.6 GB</td>
<td>160 MB</td>
<td>540 MB</td>
<td>19 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3.5 GB</td>
<td>31 MB</td>
<td>480 MB</td>
<td>104 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.6 GB</td>
<td>130 MB</td>
<td>400 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

## Version 6.2.3.11 Time and Disk Space

**Table 99: Version 6.2.3.11 Time and Disk Space**

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>4.5 GB</td>
<td>250 MB</td>
<td>—</td>
<td>39 min</td>
</tr>
<tr>
<td>FMCv: VMware 6.0</td>
<td>4.6 GB</td>
<td>35 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2.8 GB</td>
<td>2.8 GB</td>
<td>590 MB</td>
<td>40 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>2 GB</td>
<td>2 GB</td>
<td>380 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1.6 GB</td>
<td>1.6 GB</td>
<td>380 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.8 GB</td>
<td>230 MB</td>
<td>410 MB</td>
<td>33 min</td>
</tr>
<tr>
<td>FTDv: VMware 6.0</td>
<td>2.2 GB</td>
<td>230 MB</td>
<td>410 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.3 GB</td>
<td>170 MB</td>
<td>600 MB</td>
<td>23 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3.6 GB</td>
<td>50 MB</td>
<td>530 MB</td>
<td>110 min</td>
</tr>
<tr>
<td>NGIPSv: VMware 6.0</td>
<td>2.6 GB</td>
<td>130 MB</td>
<td>450 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
Version 6.2.3.10 Time and Disk Space

Table 100: Version 6.2.3.10 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>4.2 GB</td>
<td>200 MB</td>
<td>—</td>
<td>40 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>4.5 GB</td>
<td>230 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1.8 GB</td>
<td>1.8 GB</td>
<td>390 MB</td>
<td>21 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>1.3 GB</td>
<td>1.3 GB</td>
<td>190 MB</td>
<td>11 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1.3 GB</td>
<td>140 MB</td>
<td>210 MB</td>
<td>25 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>1.6 GB</td>
<td>140 MB</td>
<td>210 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3.2 GB</td>
<td>190 MB</td>
<td>560 MB</td>
<td>25 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3.4 GB</td>
<td>31 MB</td>
<td>480 MB</td>
<td>100 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>2.1 GB</td>
<td>160 MB</td>
<td>400 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

Version 6.2.3.9 Time and Disk Space

Table 101: Version 6.2.3.9 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>3630 MB</td>
<td>190 MB</td>
<td>—</td>
<td>35 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>3596 MB</td>
<td>172 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1677 MB</td>
<td>1677 MB</td>
<td>385 MB</td>
<td>21 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>779 MB</td>
<td>779 MB</td>
<td>184 MB</td>
<td>9 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1105 MB</td>
<td>130 MB</td>
<td>206 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>ISA 3000 with FTD</td>
<td>1071 MB</td>
<td>130 MB</td>
<td>206 MB</td>
<td>25 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>1094 MB</td>
<td>130 MB</td>
<td>206 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>2975 MB</td>
<td>161 MB</td>
<td>538 MB</td>
<td>30 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3211 MB</td>
<td>27 MB</td>
<td>462 MB</td>
<td>38 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>1883 MB</td>
<td>146 MB</td>
<td>378 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
Version 6.2.3.8 Time and Disk Space

Version 6.2.3.8 was removed from the Cisco Support & Download site on 2019-01-07. If you are running this version, we recommend you upgrade.

Version 6.2.3.7 Time and Disk Space

Table 102: Version 6.2.3.7 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Time from 6.2.3</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>25 min</td>
<td>2909 MB</td>
<td>137 MB</td>
<td>—</td>
</tr>
<tr>
<td>FMCv</td>
<td>20 min</td>
<td>3972 MB</td>
<td>211 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>19 min</td>
<td>1668 MB</td>
<td>1668 MB</td>
<td>384 MB</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>8 min</td>
<td>795 MB</td>
<td>795 MB</td>
<td>183 MB</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>9 min</td>
<td>1067 MB</td>
<td>130 MB</td>
<td>205 MB</td>
</tr>
<tr>
<td>ISA 3000 with FTD</td>
<td>20 min</td>
<td>1080 MB</td>
<td>130 MB</td>
<td>205 MB</td>
</tr>
<tr>
<td>FTDv</td>
<td>Hardware dependent</td>
<td>1146 MB</td>
<td>130 MB</td>
<td>205 MB</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>20 min</td>
<td>3300 MB</td>
<td>136 MB</td>
<td>477 MB</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>80 min</td>
<td>2291 MB</td>
<td>26 MB</td>
<td>411 MB</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>Hardware dependent</td>
<td>1588 MB</td>
<td>121 MB</td>
<td>327 MB</td>
</tr>
</tbody>
</table>

Version 6.2.3.6 Time and Disk Space

Table 103: Version 6.2.3.6 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Time from 6.2.3</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>30 min</td>
<td>2524 MB</td>
<td>47 MB</td>
<td>—</td>
</tr>
<tr>
<td>FMCv</td>
<td>Hardware dependent</td>
<td>2315 MB</td>
<td>101 MB</td>
<td>—</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>10 min</td>
<td>1673 MB</td>
<td>1673 MB</td>
<td>383 MB</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>17 min</td>
<td>790 MB</td>
<td>790 MB</td>
<td>182 MB</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>21 min</td>
<td>1220 MB</td>
<td>130 MB</td>
<td>205 MB</td>
</tr>
<tr>
<td>ISA 3000 with FTD</td>
<td>21 min</td>
<td>1087 MB</td>
<td>130 MB</td>
<td>205 MB</td>
</tr>
</tbody>
</table>
## Version 6.2.3.5 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTDv</td>
<td>1133 MB</td>
<td>130 MB</td>
<td>205 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>1196 MB</td>
<td>17 MB</td>
<td>204 MB</td>
<td>30 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>1844 MB</td>
<td>16 MB</td>
<td>226 MB</td>
<td>106 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>364 MB</td>
<td>17 MB</td>
<td>142 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

## Version 6.2.3.4 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>1566 MB</td>
<td>24 MB</td>
<td>—</td>
<td>28 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>2266 MB</td>
<td>80 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1001 MB</td>
<td>1001 MB</td>
<td>257 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>370 MB</td>
<td>370 MB</td>
<td>56 MB</td>
<td>7 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>587 MB</td>
<td>130 MB</td>
<td>78 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>ISA 3000 with FTD</td>
<td>379 MB</td>
<td>130 MB</td>
<td>78 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>806 MB</td>
<td>17 MB</td>
<td>78 MB</td>
<td>22 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>1465 MB</td>
<td>15 MB</td>
<td>100 MB</td>
<td>70 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>120 MB</td>
<td>17 MB</td>
<td>16 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
### Version 6.2.3.3 Time and Disk Space

#### Table 106: Version 6.2.3.3 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISA 3000 with FTD</td>
<td>393 MB</td>
<td>128 MB</td>
<td>82 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>411 MB</td>
<td>128 MB</td>
<td>82 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>800 MB</td>
<td>17 MB</td>
<td>82 MB</td>
<td>23 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>1385 MB</td>
<td>15 MB</td>
<td>103 MB</td>
<td>25 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>191 MB</td>
<td>17 MB</td>
<td>20 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.2.3.2 Time and Disk Space

#### Table 107: Version 6.2.3.2 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>1879 MB</td>
<td>88 MB</td>
<td>—</td>
<td>26 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>2093 MB</td>
<td>90 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>987 MB</td>
<td>987 MB</td>
<td>255 MB</td>
<td>15 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>313 MB</td>
<td>313 MB</td>
<td>54 MB</td>
<td>5 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>553 MB</td>
<td>128 MB</td>
<td>77 MB</td>
<td>16 min</td>
</tr>
<tr>
<td>ISA 3000 with FTD</td>
<td>307 MB</td>
<td>90 MB</td>
<td>77 MB</td>
<td>15 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>307 MB</td>
<td>90 MB</td>
<td>77 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>825 MB</td>
<td>17 MB</td>
<td>77 MB</td>
<td>15 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>634 MB</td>
<td>16 MB</td>
<td>98 MB</td>
<td>40 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>102 MB</td>
<td>17 MB</td>
<td>77 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
## Version 6.2.3.1 Time and Disk Space

*Table 108: Version 6.2.3.1 Time and Disk Space*

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>374 MB</td>
<td>374 MB</td>
<td>51 MB</td>
<td>4 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>585 MB</td>
<td>126 MB</td>
<td>73 MB</td>
<td>16 min</td>
</tr>
<tr>
<td>ISA 3000 with FTD</td>
<td>676 MB</td>
<td>126 MB</td>
<td>73 MB</td>
<td>17 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>585 MB</td>
<td>126 MB</td>
<td>73 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>688 MB</td>
<td>11 MB</td>
<td>76 MB</td>
<td>13 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>1440 MB</td>
<td>15 MB</td>
<td>98 MB</td>
<td>40 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>96 MB</td>
<td>17 MB</td>
<td>14 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

**Cisco Firepower Management Center Upgrade Guide**

205
# Version 6.2.3 Time and Disk Space

## Table 109: Version 6.2.3 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>From 6.1.0: 7415 MB</td>
<td>From 6.1.0: 17 MB</td>
<td>—</td>
<td>From 6.1.0: 38 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.0: 8863 MB</td>
<td>From 6.2.0: 24 MB</td>
<td>—</td>
<td>From 6.2.0: 43 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.1: 8263 MB</td>
<td>From 6.2.1: 23 MB</td>
<td>—</td>
<td>From 6.2.1: 37 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 11860 MB</td>
<td>From 6.2.2: 24 MB</td>
<td>—</td>
<td>From 6.2.2: 37 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>From 6.1.0: 7993 MB</td>
<td>From 6.1.0: 23 MB</td>
<td>Hardware dependent</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>From 6.2.0: 9320 MB</td>
<td>From 6.2.0: 28 MB</td>
<td>Hardware dependent</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>From 6.2.1: 11571 MB</td>
<td>From 6.2.1: 24 MB</td>
<td>Hardware dependent</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 11487 MB</td>
<td>From 6.2.2: 24 MB</td>
<td>Hardware dependent</td>
<td>—</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>From 6.2.1: 7356 MB</td>
<td>From 6.2.1: 7356 MB</td>
<td>1000 MB</td>
<td>From 6.2.1: 15 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 11356 MB</td>
<td>From 6.2.2: 11356 MB</td>
<td>1000 MB</td>
<td>From 6.2.2: 15 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>From 6.1.0: 5593 MB</td>
<td>From 6.1.0: 5593 MB</td>
<td>795 MB</td>
<td>From 6.1.0: 10 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.0: 5122 MB</td>
<td>From 6.2.0: 5122 MB</td>
<td>795 MB</td>
<td>From 6.2.0: 12 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 7498 MB</td>
<td>From 6.2.2: 7498 MB</td>
<td>795 MB</td>
<td>From 6.2.2: 15 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>From 6.1.0: 4322 MB</td>
<td>From 6.1.0: .088 MB</td>
<td>1000 MB</td>
<td>From 6.1.0: 54 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.0: 6421 MB</td>
<td>From 6.2.0: .092 MB</td>
<td>1000 MB</td>
<td>From 6.2.0: 53 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 6450 MB</td>
<td>From 6.2.2: .088 MB</td>
<td>1000 MB</td>
<td>From 6.2.2: 50 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>From 6.1.0: 4225 MB</td>
<td>From 6.1.0: .076 MB</td>
<td>Hardware dependent</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>From 6.2.0: 5179 MB</td>
<td>From 6.2.0: .092 MB</td>
<td>Hardware dependent</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 6450 MB</td>
<td>From 6.2.2: .092 MB</td>
<td>Hardware dependent</td>
<td>—</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>From 6.1.0: 5145 MB</td>
<td>From 6.1.0: 18 MB</td>
<td>840 MB</td>
<td>From 6.1.0: 29 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.0: 5732 MB</td>
<td>From 6.2.0: 18 MB</td>
<td>840 MB</td>
<td>From 6.2.0: 31 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 6752 MB</td>
<td>From 6.2.2: 18 MB</td>
<td>840 MB</td>
<td>From 6.2.2: 31 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>From 6.1.0: 7286 MB</td>
<td>From 6.1.0: 16 MB</td>
<td>From 6.1.0: 1200 MB</td>
<td>From 6.1.0: 94 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.0: 7286 MB</td>
<td>From 6.2.0: 16 MB</td>
<td>From 6.2.0: 1200 MB</td>
<td>From 6.2.0: 104 min</td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 10748 MB</td>
<td>From 6.2.2: 16 MB</td>
<td>From 6.2.2: 104 MB</td>
<td>From 6.2.2: 96 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>From 6.1.0: 4115 MB</td>
<td>From 6.1.0: 18 MB</td>
<td>741 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td></td>
<td>From 6.2.0: 5505 MB</td>
<td>From 6.2.0: 18 MB</td>
<td>Hardware dependent</td>
<td></td>
</tr>
<tr>
<td></td>
<td>From 6.2.2: 5871 MB</td>
<td>From 6.2.2: 19 MB</td>
<td>Hardware dependent</td>
<td></td>
</tr>
</tbody>
</table>
## Version 6.2.2.5 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>5271 MB</td>
<td>25 MB</td>
<td>—</td>
<td>From 6.2.2: 60 min From 6.2.2.4: 42 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>5292 MB</td>
<td>33 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>9113 MB</td>
<td>9113 MB</td>
<td>2 GB</td>
<td>From 6.2.2: 87 min From 6.2.2.4: 32 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>3325 MB</td>
<td>3325 MB</td>
<td>612 MB</td>
<td>From 6.2.2: 28 min From 6.2.2.4: 12 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>3809 MB</td>
<td>226 MB</td>
<td>724 MB</td>
<td>From 6.2.2: 49 min From 6.2.2.4: 25 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>3809 MB</td>
<td>226 MB</td>
<td>724 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>566 MB</td>
<td>28 MB</td>
<td>419 MB</td>
<td>From 6.2.2: 54 min From 6.2.2.4: 12 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3714 MB</td>
<td>28 MB</td>
<td>432 MB</td>
<td>From 6.2.2: 215 min From 6.2.2.4: 105 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>3799 MB</td>
<td>24 MB</td>
<td>98 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

## Version 6.2.2.4 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>4435 MB</td>
<td>217 MB</td>
<td>—</td>
<td>From 6.2.2: 85 min From 6.2.2.3: 42 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>3691 MB</td>
<td>48 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>6965 MB</td>
<td>6965 MB</td>
<td>1 GB</td>
<td>From 6.2.2: 58 min From 6.2.2.3: 34 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>1676 MB</td>
<td>1676 MB</td>
<td>339 MB</td>
<td>From 6.2.2: 24 min From 6.2.2.3: 13 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1695 MB</td>
<td>225 MB</td>
<td>427 MB</td>
<td>From 6.2.2: 142 min From 6.2.2.3: 68 min</td>
</tr>
</tbody>
</table>
## Version 6.2.2.3 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTDv</td>
<td>1695 MB</td>
<td>225 MB</td>
<td>427 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3343 MB</td>
<td>36 MB</td>
<td>414 MB</td>
<td>From 6.2.2: 45 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.3: 19 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3192 MB</td>
<td>27 MB</td>
<td>405 MB</td>
<td>From 6.2.2: 182 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.3: 80 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>444 MB</td>
<td>28 MB</td>
<td>94 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>FMC</td>
<td>3766.6 MB</td>
<td>205 MB</td>
<td>—</td>
<td>From 6.2.2: 66 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.2: 41 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>3485 MB</td>
<td>17.5 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>4486.64 MB</td>
<td>4486.64 MB</td>
<td>132 MB</td>
<td>From 6.2.2: 61 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.2: 36 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>811.7 MB</td>
<td>811.7 MB</td>
<td>132 MB</td>
<td>From 6.2.2: 20 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.2: 12 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1636.6 MB</td>
<td>125.1 MB</td>
<td>199 MB</td>
<td>From 6.2.2: 35 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.2: 20 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>1810.7 MB</td>
<td>125 MB</td>
<td>199 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>2775 MB</td>
<td>17 MB</td>
<td>339 MB</td>
<td>From 6.2.2: 80 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.2: 42 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2301.5 MB</td>
<td>15.69 MB</td>
<td>308 MB</td>
<td>From 6.2.2: 184 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.2: 100 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>576.3 MB</td>
<td>17.5 MB</td>
<td>20 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
## Version 6.2.2.2 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>1656 MB</td>
<td>18 MB</td>
<td>—</td>
<td>From 6.2.2: 34 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.1: 27 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>2356 MB</td>
<td>19 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>2377 MB</td>
<td>2377 MB</td>
<td>497 MB</td>
<td>From 6.2.2: 41 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.1: 20 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>561 MB</td>
<td>561 MB</td>
<td>41 MB</td>
<td>From 6.2.2: 21 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.1: 13 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>984 MB</td>
<td>122 MB</td>
<td>136 MB</td>
<td>From 6.2.2: 110 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.1: 70 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>984 MB</td>
<td>122 MB</td>
<td>136 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>1706 MB</td>
<td>16 MB</td>
<td>310 MB</td>
<td>From 6.2.2: 56 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.1: 40 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>1602 MB</td>
<td>15 MB</td>
<td>190 MB</td>
<td>From 6.2.2: 113 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.2.1: 80 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>170 MB</td>
<td>17 MB</td>
<td>16 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

## Version 6.2.2.1 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>480 MB</td>
<td>18 MB</td>
<td>—</td>
<td>52 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>775 MB</td>
<td>30 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 2100 series</td>
<td>1003 MB</td>
<td>1003 MB</td>
<td>47 MB</td>
<td>28 min</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>299 MB</td>
<td>299 MB</td>
<td>47 MB</td>
<td>35 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>674 MB</td>
<td>121 MB</td>
<td>69 MB</td>
<td>72 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>674 MB</td>
<td>121 MB</td>
<td>69 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>664 MB</td>
<td>14 MB</td>
<td>61 MB</td>
<td>33 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>758 MB</td>
<td>15 MB</td>
<td>83 MB</td>
<td>90 min</td>
</tr>
</tbody>
</table>
### Version 6.2.2 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>NGIPSv</td>
<td>106 MB</td>
<td>17 MB</td>
<td>10 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.2.0.6 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>8547 MB</td>
<td>104 MB</td>
<td>—</td>
<td>From 6.2.0: 97 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.5: 36 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>8543 MB</td>
<td>30 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>4085 MB</td>
<td>4085 MB</td>
<td>789 MB</td>
<td>From 6.2.0: 23 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.5: 13 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>4526 MB</td>
<td>226 MB</td>
<td>918 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>4960 MB</td>
<td>227 MB</td>
<td>918 MB</td>
<td>From 6.2.0: 56 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.5:27 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>7464 MB</td>
<td>29 MB</td>
<td>944 MB</td>
<td>From 6.2.0: 60 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.5: 24 min</td>
</tr>
</tbody>
</table>
### Version 6.2.0.5 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA FirePOWER</td>
<td>7191 MB</td>
<td>28 MB</td>
<td>878 MB</td>
<td>From 6.2.0: 75 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.5: 49 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>1658 MB</td>
<td>29 MB</td>
<td>284 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.2.0.4 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>6009 MB</td>
<td>180 MB</td>
<td>—</td>
<td>From 6.2.0: 72 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.4: 34 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>6943 MB</td>
<td>20 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>3009 MB</td>
<td>3009 MB</td>
<td>441 MB</td>
<td>From 6.2.0: 28 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.4: 16 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>2805 MB</td>
<td>135 MB</td>
<td>548 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>4316 MB</td>
<td>135 MB</td>
<td>548 MB</td>
<td>From 6.2.0: 46 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.4: 22 min</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>5806 MB</td>
<td>18 MB</td>
<td>693 MB</td>
<td>From 6.2.0: 51 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.4: 18 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>5945 MB</td>
<td>16 MB</td>
<td>703 MB</td>
<td>From 6.2.0: 66 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.4: 27 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>1301 MB</td>
<td>18 MB</td>
<td>211 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
## Version 6.2.0.3 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>3593 MB</td>
<td>134 MB</td>
<td>448 MB</td>
<td>From 6.2.0: 2 hr 28 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.3: 69 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>275 MB</td>
<td>136 MB</td>
<td>448 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>4614 MB</td>
<td>18 MB</td>
<td>608 MB</td>
<td>From 6.2.0: 45 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.3: 17 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>4585 MB</td>
<td>16 MB</td>
<td>597 MB</td>
<td>From 6.2.0: 3 hr 34 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.3: 83 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>1067 MB</td>
<td>18 MB</td>
<td>208 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

## Version 6.2.0.3 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>3352 MB</td>
<td>18 MB</td>
<td>—</td>
<td>From 6.2.0: 75 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.2: 37 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>3342 MB</td>
<td>19 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>—</td>
<td>1355 MB</td>
<td>319 MB</td>
<td>From 6.2.0: 18 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.2: 12 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>131 MB</td>
<td>2302 MB</td>
<td>384 MB</td>
<td>From 6.2.0: 118 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.2: 76 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>842 MB</td>
<td>17 MB</td>
<td>384 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3526 MB</td>
<td>17 MB</td>
<td>554 MB</td>
<td>From 6.2.0: 38 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.2: 19 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>15 MB</td>
<td>3361 MB</td>
<td>521 MB</td>
<td>From 6.2.0: 3 hr</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.2: 97 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>842 MB</td>
<td>17 MB</td>
<td>202 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
### Version 6.2.0.2 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>1665 MB</td>
<td>35 MB</td>
<td>—</td>
<td>From 6.2.0: 36 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.1: 30 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>2834 MB</td>
<td>21 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>1060 MB</td>
<td>1060 MB</td>
<td>274 MB</td>
<td>From 6.2.0: 12 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.1: 9 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1808 MB</td>
<td>144 MB</td>
<td>295 MB</td>
<td>From 6.2.0: 95 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.1: 59 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>998 MB</td>
<td>143 MB</td>
<td>295 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>2110 MB</td>
<td>17 MB</td>
<td>458 MB</td>
<td>From 6.2.0: 54 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.1: 35 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2014 MB</td>
<td>17 MB</td>
<td>383 MB</td>
<td>From 6.2.0: 40 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.2.0.1: 80 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>612 MB</td>
<td>19 MB</td>
<td>195 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.2.0.1 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.2.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>1237 MB</td>
<td>50 MB</td>
<td>—</td>
<td>28 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>1488 MB</td>
<td>23 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>524 MB</td>
<td>524 MB</td>
<td>137 MB</td>
<td>12 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>945 MB</td>
<td>144 MB</td>
<td>159 MB</td>
<td>62 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>144 MB</td>
<td>10 MB</td>
<td>159 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>1134 MB</td>
<td>18 MB</td>
<td>186 MB</td>
<td>22 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>97 MB</td>
<td>17 MB</td>
<td>206 MB</td>
<td>69 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>721 MB</td>
<td>19 MB</td>
<td>98 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
### Version 6.2.0 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>10207 MB</td>
<td>17 MB</td>
<td>—</td>
<td>57 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>10207 MB</td>
<td>17 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>5234 MB</td>
<td>5234 MB</td>
<td>734 MB</td>
<td>21 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>5213 MB</td>
<td>.096 MB</td>
<td>938 MB</td>
<td>83 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>5663 MB</td>
<td>1 MB</td>
<td>936 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>6129 MB</td>
<td>17 MB</td>
<td>1200 MB</td>
<td>27 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>6619 MB</td>
<td>16 MB</td>
<td>1100 MB</td>
<td>165 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>7028 MB</td>
<td>18 MB</td>
<td>1300 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.1.0.7 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>1941 MB</td>
<td>187 MB</td>
<td>—</td>
<td>From 6.1.0: 111 min From 6.1.0.5: 41 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>12435 MB</td>
<td>218 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>9881 MB</td>
<td>9881 MB</td>
<td>1400 MB</td>
<td>From 6.1.0: 43 min From 6.1.0.5: 13 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>8846 MB</td>
<td>1033 MB</td>
<td>1480 MB</td>
<td>From 6.1.0: 251 min From 6.1.0.5: 75 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>1339 MB</td>
<td>185 MB</td>
<td>1480 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>5896 MB</td>
<td>33 MB</td>
<td>159 MB</td>
<td>From 6.1.0: 39 min From 6.1.0.5: 25 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>13061 MB</td>
<td>45 MB</td>
<td>1390 MB</td>
<td>From 6.1.0: 156 min From 6.1.0.5: 28 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>5477 MB</td>
<td>185 MB</td>
<td>717 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
# Version 6.1.0.6 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>10503 MB</td>
<td>215 MB</td>
<td>—</td>
<td>From 6.1.0: 66 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.5: 27 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>1367 MB</td>
<td>196 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>8140 MB</td>
<td>8140 MB</td>
<td>1126 MB</td>
<td>From 6.1.0: 270 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.5: 75 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>8540 MB</td>
<td>1034 MB</td>
<td>1229 MB</td>
<td>From 6.1.0: 40 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.5: 15 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>7414 MB</td>
<td>1033 MB</td>
<td>1229 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>12725 MB</td>
<td>237 MB</td>
<td>1434 MB</td>
<td>From 6.1.0: 136 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.5: 34 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>11189 MB</td>
<td>31 MB</td>
<td>1131 MB</td>
<td>From 6.1.0: 257 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.5: 60 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>4606 MB</td>
<td>196 MB</td>
<td>644 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

# Version 6.1.0.5 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>7673 MB</td>
<td>46 MB</td>
<td>—</td>
<td>From 6.1.0: 56 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.4: 28 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>10790 MB</td>
<td>216 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>7680 MB</td>
<td>7680 MB</td>
<td>1060 MB</td>
<td>From 6.1.0: 30 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.4: 10 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>7952 MB</td>
<td>137 MB</td>
<td>1141 MB</td>
<td>From 6.1.0: 186 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.4: 70 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>7453 MB</td>
<td>1140 MB</td>
<td>1141 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>11877 MB</td>
<td>259 MB</td>
<td>1403 MB</td>
<td>From 6.1.0: 115 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.4: 25 min</td>
</tr>
</tbody>
</table>
## Version 6.1.0.4 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA FirePOWER</td>
<td>8955 MB</td>
<td>34 MB</td>
<td>1217 MB</td>
<td>From 6.1.0: 208 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.4: 105 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>4298 MB</td>
<td>215 MB</td>
<td>640 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

## Version 6.1.0.3 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>6739516 MB</td>
<td>218808 MB</td>
<td>—</td>
<td>From 6.1.0: 65 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.3: 30 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>675984 MB</td>
<td>200748 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>6010092 MB</td>
<td>6010092 MB</td>
<td>1020 MB</td>
<td>From 6.1.0: 26 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.3: 10 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>6155828 MB</td>
<td>1058968 MB</td>
<td>1100 MB</td>
<td>From 6.1.0: 49 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.3: 20 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>1059632 MB</td>
<td>1059632 MB</td>
<td>1100 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>8713068 MB</td>
<td>240940 MB</td>
<td>1200 MB</td>
<td>From 6.1.0: 48 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.3: 17 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>7442808 MB</td>
<td>31740 MB</td>
<td>1100 MB</td>
<td>From 6.1.0: 63 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.3: 45 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>3367536 MB</td>
<td>20120 MB</td>
<td>636 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

---

---
### Version 6.1.0.2 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>ASA 5000-X series with FTD</td>
<td>1057776 MB</td>
<td>1057776 MB</td>
<td>1000 MB</td>
<td>From 6.1.0: 40 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.2: 23 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>1059932 MB</td>
<td>1059932 MB</td>
<td>1000 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>7357340 MB</td>
<td>228728 MB</td>
<td>1100 MB</td>
<td>From 6.1.0: 43 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.2: 25 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>4782384 MB</td>
<td>31792 MB</td>
<td>1000 MB</td>
<td>From 6.1.0: 160 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.2: 80 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>2710540 MB</td>
<td>200896 MB</td>
<td>635 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.1.0.1 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>3872 MB</td>
<td>235 MB</td>
<td>—</td>
<td>44 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.1: 22 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>3871 MB</td>
<td>219 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>4046 MB</td>
<td>4046 MB</td>
<td>886 MB</td>
<td>From 6.1.0: 20 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.1: 14 min</td>
</tr>
<tr>
<td>ASA 5000-X series with FTD</td>
<td>2291 MB</td>
<td>96 MB</td>
<td>918 MB</td>
<td>From 6.1.0: 74 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.1: 106 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>2797 MB</td>
<td>1137 MB</td>
<td>918 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>4130 MB</td>
<td>260 MB</td>
<td>965 MB</td>
<td>From 6.1.0: 62 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.1: 24 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>4549 MB</td>
<td>40 MB</td>
<td>816 MB</td>
<td>From 6.1.0: 139 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.1.0.1: 34 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>2710540 MB</td>
<td>200896 MB</td>
<td>635 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.1.0 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>1893 MB</td>
<td>140 MB</td>
<td>—</td>
<td>23 min</td>
</tr>
</tbody>
</table>
### Version 6.1.0 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.1.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMCv</td>
<td>2144 MB</td>
<td>207 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>2580 MB</td>
<td>580 MB</td>
<td>600 MB</td>
<td>15 min</td>
</tr>
<tr>
<td>Firepower 9300</td>
<td>1877 MB</td>
<td>1877 MB</td>
<td>600 MB</td>
<td>20 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>1377 MB</td>
<td>846 MB</td>
<td>600 MB</td>
<td>10 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>1377 MB</td>
<td>846 MB</td>
<td>600 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>2094 MB</td>
<td>156 MB</td>
<td>513 MB</td>
<td>47 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>1728 MB</td>
<td>34 MB</td>
<td>433 MB</td>
<td>76 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>793 MB</td>
<td>130 MB</td>
<td>295 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.0.1.4 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.0.1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>10722 MB</td>
<td>18 MB</td>
<td>—</td>
<td>47 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>10128 MB</td>
<td>17 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>5213 MB</td>
<td>.096 MB</td>
<td>914 MB</td>
<td>21 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>5403 MB</td>
<td>.096 MB</td>
<td>914 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>7108 MB</td>
<td>61 MB</td>
<td>1740 MB</td>
<td>39 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>8392 MB</td>
<td>47 MB</td>
<td>1300 MB</td>
<td>59 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>6368 MB</td>
<td>54 MB</td>
<td>1229 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.0.1.4 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.0.0: 92 min</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>3428 MB</td>
<td>201 MB</td>
<td>—</td>
<td>From 6.0.0: 92 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>3108 MB</td>
<td>95 MB</td>
<td>—</td>
<td>From 6.0.1.3: 39 min</td>
</tr>
<tr>
<td>Firepower 4100 series</td>
<td>5237 MB</td>
<td>5237 MB</td>
<td>1000 MB</td>
<td>From 6.0.0: 30 min</td>
</tr>
</tbody>
</table>

From 6.0.1.3: 18 min
## Version 6.0.1.3 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firepower 9300</td>
<td>1360 MB</td>
<td>5434 MB</td>
<td>1000 MB</td>
<td>From 6.0.0: 26 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.0.1.3: 14 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>3416 MB</td>
<td>1017 MB</td>
<td>1000 MB</td>
<td>From 6.0.0: 26 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.0.1.3: 14 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>3619 MB</td>
<td>1020 MB</td>
<td>1000 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>7891 MB</td>
<td>222 MB</td>
<td>1270 MB</td>
<td>From 6.0.0: 47 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.0.1.3: 23 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>6049 MB</td>
<td>45 MB</td>
<td>990 MB</td>
<td>From 6.0.0: 95 min</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>From 6.0.1.3: 43 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>2916 MB</td>
<td>192 MB</td>
<td>990 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

## Version 6.0.1.2 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>2419 MB</td>
<td>110 MB</td>
<td>—</td>
<td>58 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>2419 MB</td>
<td>101 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>2781 MB</td>
<td>2781 MB</td>
<td>473 MB</td>
<td>22 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>2641 MB</td>
<td>813 MB</td>
<td>473 MB</td>
<td>24 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>2651 MB</td>
<td>813 MB</td>
<td>473 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>4757 MB</td>
<td>125 MB</td>
<td>926 MB</td>
<td>55 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>3883 MB</td>
<td>58 MB</td>
<td>685 MB</td>
<td>184 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>1695 MB</td>
<td>107 MB</td>
<td>430 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
### Version 6.0.1.1 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.0.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>14 MB</td>
<td>54 MB</td>
<td>—</td>
<td>23 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>14 MB</td>
<td>54 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 4100/9300 chassis</td>
<td>54 MB</td>
<td>54 MB</td>
<td>2 MB</td>
<td>6 min</td>
</tr>
<tr>
<td>ASA 5500-X series with FTD</td>
<td>54 MB</td>
<td>54 MB</td>
<td>2 MB</td>
<td>7 min</td>
</tr>
<tr>
<td>FTDv</td>
<td>14 MB</td>
<td>54 MB</td>
<td>2 MB</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>944 MB</td>
<td>61 MB</td>
<td>166 MB</td>
<td>39 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>824 MB</td>
<td>54 MB</td>
<td>84 MB</td>
<td>46 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>54 MB</td>
<td>56 MB</td>
<td>1 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

### Version 6.0.1 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>8959 MB</td>
<td>18 MB</td>
<td>—</td>
<td>66 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>—</td>
<td>—</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>3683 MB</td>
<td>227 MB</td>
<td>614 MB</td>
<td>30 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>2966 MB</td>
<td>54 MB</td>
<td>429 MB</td>
<td>91 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>2090 MB</td>
<td>196 MB</td>
<td>3050 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
## Version 6.0.0.1 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time from 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>976 MB</td>
<td>120 MB</td>
<td>—</td>
<td>25 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>969 MB</td>
<td>119 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>1568 MB</td>
<td>134 MB</td>
<td>273 MB</td>
<td>25 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>1101 MB</td>
<td>56 MB</td>
<td>181 MB</td>
<td>56 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>929 MB</td>
<td>26 MB</td>
<td>174 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>

## Version 6.0 Time and Disk Space

<table>
<thead>
<tr>
<th>Platform</th>
<th>Space on /Volume</th>
<th>Space on /</th>
<th>Space on FMC</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>FMC</td>
<td>8022 MB</td>
<td>16 MB</td>
<td>—</td>
<td>58 min</td>
</tr>
<tr>
<td>FMCv</td>
<td>8022 MB</td>
<td>16 MB</td>
<td>—</td>
<td>Hardware dependent</td>
</tr>
<tr>
<td>Firepower 7000/8000 series</td>
<td>6496 MB</td>
<td>16 MB</td>
<td>1200 MB</td>
<td>94 min</td>
</tr>
<tr>
<td>ASA FirePOWER</td>
<td>7644 MB</td>
<td>32 MB</td>
<td>1200 MB</td>
<td>41 min</td>
</tr>
<tr>
<td>NGIPSv</td>
<td>6046 MB</td>
<td>17 MB</td>
<td>102000 MB</td>
<td>Hardware dependent</td>
</tr>
</tbody>
</table>
CHAPTER 16

Traffic Flow, Inspection, and Device Behavior

You must identify potential interruptions in traffic flow and inspection during the upgrade. This can occur:

- When a device is rebooted.
- When you upgrade the operating system or virtual hosting environment on a device.
- When you upgrade the Firepower software on a device, or uninstall a patch.
- When you deploy configuration changes as part of the upgrade or uninstall process (Snort process restarts).

Device type, deployment type (standalone, high availability, clustered), and interface configurations (passive, IPS, firewall, and so on) determine the nature of the interruptions. We strongly recommend performing any upgrade or uninstall in a maintenance window or at a time when any interruption will have the least impact on your deployment.

- FTD Upgrade Behavior: Firepower 4100/9300 Chassis, on page 223
- FTD Upgrade Behavior: Other Devices, on page 226
- Firepower 7000/8000 Series Upgrade Behavior, on page 228
- ASA FirePOWER Upgrade Behavior, on page 230
- NGIPSv Upgrade Behavior, on page 230

FTD Upgrade Behavior: Firepower 4100/9300 Chassis

This section describes device and traffic behavior when you upgrade a Firepower 4100/9300 chassis with FTD.

Firepower 4100/9300 Chassis: FXOS Upgrade

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

**Standalone FTD Device: Firepower Software Upgrade**

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

*Table 111: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device*

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall interfaces</td>
<td>Routef or switched including EtherChannel, redundant, subinterfaces Switched interfaces are also known as bridge group or transparent interfaces.</td>
</tr>
</tbody>
</table>
| IPS-only interfaces              | Inline set, fail-to-wire enabled: Bypass: Standby or Bypass-Force (6.1+) | Either:  
  • Dropped (6.1 through 6.2.2.x)  
  • Passed without inspection (6.2.3+) |
|                                  | Inline set, fail-to-wire disabled: Bypass: Disabled (6.1+)               | Dropped                        |
|                                  | Inline set, no fail-to-wire module                                      | Dropped                        |
|                                  | Inline set, tap mode                                                    | Egress packet immediately, copy not inspected |
|                                  | Passive, ERSPAN passive                                                 | Uninterrupted, not inspected    |
High Availability Pairs: Firepower Software Upgrade

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

The standby device upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices’ roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

Clusters: Firepower Software Upgrade

You should not experience interruptions in traffic flow or inspection while upgrading the Firepower software on devices in Firepower Threat Defense clusters. To ensure continuity of operations, they upgrade one at a time. Devices operate in maintenance mode while they upgrade.

The slave security module or modules upgrade first, then the master. Security modules operate in maintenance mode while they upgrade.

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

Note

Upgrading an inter-chassis cluster from Version 6.2.0, 6.2.0.1, or 6.2.0.2 causes a 2-3 second traffic interruption in traffic inspection when each module is removed from the cluster. Whether traffic drops during this interruption or passes without further inspection depends on how the device handles traffic.

High Availability and Clustering Hitless Upgrade Requirements

Performing hitless upgrades have the following additional requirements.

Flow Offload: Due to bug fixes in the flow offload feature, some combinations of FXOS and FTD do not support flow offload; see the Cisco Firepower Compatibility Guide. To perform a hitless upgrade in a high availability or clustered deployment, you must make sure you are always running a compatible combination.

If your upgrade path includes upgrading FXOS to 2.2.2.91, 2.3.1.130, or later (including FXOS 2.4.1.x, 2.6.1.x, and so on) use this path:

1. Upgrade FTD to 6.2.2.2 or later.
2. Upgrade FXOS to 2.2.2.91, 2.3.1.130, or later.
3. Upgrade FTD to your final version.

For example, if you are running FXOS 2.2.2.17/FTD 6.2.2.0, and you want to upgrade to FXOS 2.6.1/FTD 6.4.0, then you can:

1. Upgrade FTD to 6.2.2.5.
2. Upgrade FXOS to 2.6.1.
3. Upgrade FTD to 6.4.0.
**Version 6.1.0 Upgrades:** Performing a hitless upgrade of an FTD high availability pair to Version 6.1.0 requires a preinstallation package. For more information, see Firepower System Release Notes Version 6.1.0 Preinstallation Package.

**Traffic Behavior During Deployment**

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see Configurations that Restart the Snort Process when Deployed or Activated in the Firepower Management Center Configuration Guide.

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

**Table 112: Traffic Behavior During FTD Deployment**

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall interfaces</td>
<td>Routed or switched including EtherChannel, redundant, subinterfaces</td>
</tr>
<tr>
<td></td>
<td>Switched interfaces are also known as bridge group or transparent interfaces.</td>
</tr>
<tr>
<td></td>
<td>Dropped</td>
</tr>
<tr>
<td>IPS-only interfaces</td>
<td>Inline set, Failsafe enabled or disabled (6.0.1 - 6.1.0.x)</td>
</tr>
<tr>
<td></td>
<td>Passed without inspection</td>
</tr>
<tr>
<td></td>
<td>A few packets might drop if Failsafe is disabled and Snort is busy but not down.</td>
</tr>
<tr>
<td>Inline set, Snort Fail Open: Down: disabled (6.2+)</td>
<td>Dropped</td>
</tr>
<tr>
<td>Inline set, Snort Fail Open: Down: enabled (6.2+)</td>
<td>Passed without inspection</td>
</tr>
<tr>
<td>Inline set, tap mode</td>
<td>Egress packet immediately, copy not inspected</td>
</tr>
<tr>
<td>Passive, ERSPAN passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
</tbody>
</table>

**FTD Upgrade Behavior: Other Devices**

This section describes device and traffic behavior when you upgrade Firepower Threat Defense on Firepower 1000/2100 series, ASA 5500-X series, ISA 3000, and FTDv.

**Standalone FTD Device: Firepower Software Upgrade**

Interface configurations determine how a standalone device handles traffic during the upgrade.
Table 113: Traffic Behavior During Firepower Software Upgrade: Standalone FTD Device

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall interfaces</td>
<td>Routed or switched including EtherChannel, redundant, subinterfaces Switched interfaces are also known as bridge group or transparent interfaces.</td>
</tr>
</tbody>
</table>

IPS-only interfaces

<table>
<thead>
<tr>
<th>Inline set, fail-to-wire enabled: Bypass: Standby or Bypass-Force (6.1+)</th>
<th>Either:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Dropped (6.1 through 6.2.2.x)</td>
<td></td>
</tr>
<tr>
<td>• Passed without inspection (6.2.3+)</td>
<td></td>
</tr>
</tbody>
</table>

| Inline set, fail-to-wire disabled: Bypass: Disabled (6.1+) | Dropped |
| In-line set, no fail-to-wire module | Dropped |
| Inline set, tap mode | Egress packet immediately, copy not inspected |
| Passive, ERSPAN passive | Uninterrupted, not inspected |

High Availability Pairs: Firepower Software Upgrade

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

The standby device upgrades first. The devices switch roles, then the new standby upgrades. When the upgrade completes, the devices' roles remain switched. If you want to preserve the active/standby roles, manually switch the roles before you upgrade. That way, the upgrade process switches them back.

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see Configurations that Restart the Snort Process when Deployed or Activated in the Firepower Management Center Configuration Guide.

When you deploy, resource demands may result in a small number of packets dropping without inspection. Additionally, restarting the Snort process interrupts traffic inspection on all Firepower devices, including those configured for HA/scalability. Interface configurations determine whether traffic drops or passes without inspection during the interruption.
Table 114: Traffic Behavior During FTD Deployment

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall interfaces</td>
<td></td>
</tr>
<tr>
<td>Routed or switched including EtherChannel, redundant, subinterfaces Switched interfaces are also known as bridge group or transparent interfaces.</td>
<td>Dropped</td>
</tr>
<tr>
<td>IPS-only interfaces</td>
<td></td>
</tr>
<tr>
<td>Inline set, <strong>Failsafe</strong> enabled or disabled (6.0.1 - 6.1.0.x)</td>
<td>Passed without inspection A few packets might drop if <strong>Failsafe</strong> is disabled and Snort is busy but not down.</td>
</tr>
<tr>
<td>Inline set, <strong>Snort Fail Open: Down</strong> disabled (6.2+)</td>
<td>Dropped</td>
</tr>
<tr>
<td>Inline set, <strong>Snort Fail Open: Down</strong> enabled (6.2+)</td>
<td>Passed without inspection</td>
</tr>
<tr>
<td>Inline set, tap mode</td>
<td>Egress packet immediately, copy not inspected</td>
</tr>
<tr>
<td>Passive, ERSPAN passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
</tbody>
</table>

Firepower 7000/8000 Series Upgrade Behavior

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

**Standalone 7000/8000 Series: Firepower Software Upgrade**

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

Table 115: Traffic Behavior During Upgrade: Standalone 7000/8000 Series

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
</table>
| Inline, hardware bypass enabled (Bypass Mode: Bypass) | Passed without inspection, although traffic is interrupted briefly at two points:  
  - At the beginning of the upgrade process as link goes down and up (flaps) and the network card switches into hardware bypass.  
  - After the upgrade finishes as link flaps and the network card switches out of bypass. Inspection resumes after the endpoints reconnect and reestablish link with the device interfaces. |
| Inline, no hardware bypass module, or hardware bypass disabled (Bypass Mode: Non-Bypass) | Dropped |
7000/8000 Series High Availability Pairs: Firepower Software Upgrade

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

Which peer upgrades first depends on your deployment:

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

- Access control only: Active upgrades first. When the upgrade completes, the active and standby maintain their old roles.

8000 Series Stacks: Firepower Software Upgrade

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

Traffic Behavior During Deployment

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see Configurations that Restart the Snort Process when Deployed or Activated in the Firepower Management Center Configuration Guide.

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

Table 116: Traffic Behavior During Deployment: 7000/8000 Series

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline, tap mode</td>
<td>Egress packet immediately, copy not inspected</td>
</tr>
<tr>
<td>Passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
<tr>
<td>Routed, switched</td>
<td>Dropped</td>
</tr>
</tbody>
</table>

Table 116: Traffic Behavior During Deployment: 7000/8000 Series

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline, <strong>Failsafe</strong> enabled or disabled</td>
<td>Passed without inspection&lt;br&gt;A few packets might drop if <strong>Failsafe</strong> is disabled and Snort is busy but not down.</td>
</tr>
<tr>
<td>Inline, tap mode</td>
<td>Egress packet immediately, copy bypasses Snort</td>
</tr>
<tr>
<td>Passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
<tr>
<td>Routed, switched</td>
<td>Dropped</td>
</tr>
</tbody>
</table>
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 117: Traffic Behavior During ASA FirePOWER Upgrade

<table>
<thead>
<tr>
<th>Traffic Redirection Policy</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fail open (sfr fail-open)</td>
<td>Passed without inspection</td>
</tr>
<tr>
<td>Fail closed (sfr fail-close)</td>
<td>Dropped</td>
</tr>
<tr>
<td>Monitor only (sfr {fail-close}</td>
<td>{fail-open} monitor-only)</td>
</tr>
</tbody>
</table>

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 118: Traffic Behavior During NGIPSv Upgrade

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline</td>
<td>Dropped</td>
</tr>
<tr>
<td>Inline, tap mode</td>
<td>Egress packet immediately, copy not inspected</td>
</tr>
<tr>
<td>Passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
</tbody>
</table>
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 119: Traffic Behavior During NGIPSv Deployment

<table>
<thead>
<tr>
<th>Interface Configuration</th>
<th>Traffic Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inline, <strong>Failsafe</strong> enabled or disabled</td>
<td>Passed without inspection</td>
</tr>
<tr>
<td></td>
<td>A few packets might drop if <strong>Failsafe</strong> is disabled and Snort is busy but not down.</td>
</tr>
<tr>
<td>Inline, tap mode</td>
<td>Egress packet immediately, copy bypasses Snort</td>
</tr>
<tr>
<td>Passive</td>
<td>Uninterrupted, not inspected</td>
</tr>
</tbody>
</table>