



Cisco Firepower 4100/9300 Upgrade Guide

First Published: 2018-10-25

Last Modified: 2021-12-10

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

CHAPTER 1

Planning Your Upgrade 1

Upgrade Planning Phases 1

Current Version and Model Information 2

Upgrade Paths 2

Upgrade Path: FXOS 4

Upgrade Path: ASA Logical Devices 5

Upgrade Path: FTD Logical Devices and FMC 7

Upgrade Path: FTD Logical Devices and FDM 11

Upgrade Path: FTD and ASA Logical Devices for Firepower 9300 12

Upgrade Path: Firepower Management Centers 13

Download Upgrade Packages 15

Firepower Software Packages 16

ASA Packages 17

FXOS Packages 17

Upload Firepower Software Upgrade Packages with FMC 18

Upload to the Firepower Management Center 18

Upload to an Internal Server (Version 6.6.0+ FTD with FMC) 19

Copy to Managed Devices 20

Upload Firepower Threat Defense Upgrade Packages with FDM 21

Upload to the FTD Device (Version 6.2.0+ with FDM) 21

Upload to the FTD Device (Version 6.0.1 & 6.1.0 with FDM) 22

Firepower Software Readiness Checks with FMC 23

Run Readiness Checks with FMC (Version 7.0.0+ FTD) 23

Run Readiness Checks with FMC (Version 6.7.0+) 23

Run Readiness Checks with FMC (Version 6.0.1–6.6.x) 24

Firepower Software Readiness Checks with FDM 25

Run Readiness Checks (Version 7.0.0+ with FDM) 25

CHAPTER 2

Upgrade FXOS on the Firepower 4100/9300 27

Upgrade FXOS on a Firepower 4100/9300 Chassis Using Firepower Chassis Manager 27

Upgrade FXOS on a Firepower 4100/9300 Chassis Using the CLI 29

CHAPTER 3

Upgrade the Firepower 4100/9300 with FTD Logical Devices 33

Upgrade FXOS on a Firepower 4100/9300 with Firepower Threat Defense Logical Devices 33

Upgrade FXOS: FTD Standalone Devices and Intra-chassis Clusters 34

Upgrade FXOS for Standalone FTD Logical Devices Using Firepower Chassis Manager 34

Upgrade FXOS for Standalone FTD Logical Devices Using the FXOS CLI 35

Upgrade FXOS: FTD High Availability Pairs 38

Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager 38

Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI 42

Upgrade FXOS: FTD Inter-chassis Clusters 46

Upgrade FXOS on an FTD Inter-chassis Cluster Using Firepower Chassis Manager 46

Upgrade FXOS on an FTD Inter-chassis Cluster Using the FXOS CLI 49

Upgrade Firepower Threat Defense Logical Devices with Firepower Management Center 52

Upgrade Checklist: Firepower Threat Defense with FMC 52

Upgrade Firepower Threat Defense with FMC (Version 7.0.0) 57

Upgrade Firepower Threat Defense with FMC (Version 6.0.1–6.7.0) 60

CHAPTER 4

Upgrade the Firepower 4100/9300 with ASA Logical Devices 63

Checklist: Upgrade Firepower 4100/9300 with ASA 63

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster 64

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using Firepower Chassis Manager 64

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using the FXOS CLI 65

Upgrade FXOS and an ASA Active/Standby Failover Pair 69

Upgrade FXOS and an ASA Active/Standby Failover Pair Using Firepower Chassis Manager 69

Upgrade FXOS and an ASA Active/Standby Failover Pair Using the FXOS CLI 71

Upgrade FXOS and an ASA Active/Active Failover Pair 79

Upgrade FXOS and an ASA Active/Active Failover Pair Using Firepower Chassis Manager 79

Upgrade FXOS and an ASA Active/Active Failover Pair Using the FXOS CLI 82

Upgrade FXOS and an ASA Inter-chassis Cluster	90
Upgrade FXOS and an ASA Inter-chassis Cluster Using Firepower Chassis Manager	91
Upgrade FXOS and an ASA Inter-chassis Cluster Using the FXOS CLI	92

CHAPTER 5 Monitor Upgrade Progress and Verify Installation 99

Monitor the Upgrade Progress	99
Verify the Installation	100

PART I Reference 101

CHAPTER 6 Compatibility 103

Firepower Management Center	103
FMC-Device Compatibility	103
FMC Hardware	104
FMCv	105
BIOS and Firmware for FMC Hardware	107
Firepower 4100/9300 Compatibility with ASA and FTD	108
Radware DefensePro Compatibility	115

CHAPTER 7 Firepower Software Upgrade Guidelines 119

General Guidelines	120
Version 7.0.x Guidelines	120
Reconnect with Cisco Threat Grid for HA FMCs	121
Version 6.7.x Guidelines	121
Version 6.6.x Guidelines	122
Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0	123
Upgrade Failure: FMC with Email Alerting for Intrusion Events	124
FMCv Requires 28 GB RAM for Upgrade	124
Version 6.5.0 Guidelines	125
Disable Egress Optimization for Version 6.5.0	126
Historical Data Removed During FTD/FDM Upgrade	127
New URL Categories and Reputations	127
Pre-Upgrade Actions for URL Categories and Reputations	128
Post-Upgrade Actions for URL Categories and Reputations	129

Guidelines for Rules with Merged URL Categories	130
Version 6.4.0 Guidelines	133
EtherChannels on Firepower 1010 Devices Can Blackhole Egress Traffic	134
Upgrade Failure: Insufficient Disk Space on Container Instances	134
TLS Crypto Acceleration Enabled/Cannot Disable	134
Version 6.3.0 Guidelines	135
Renamed Upgrade and Installation Packages	136
Reimaging to Version 6.3+ Disables LOM on Most Appliances	137
Readiness Check May Fail on FMC	138
Reporting Data Removed During FTD/FDM Upgrade	138
RA VPN Default Setting Change Can Block VPN Traffic	138
TLS/SSL Hardware Acceleration Enabled on Upgrade	139
Upgrade Failure: Version 6.3.0-83 Upgrades to FMC	139
Security Intelligence Enables Application Identification	140
Update VDB after Upgrade to Enable CIP Detection	140
Invalid Intrusion Variable Sets Can Cause Deploy Failure	140
Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade	141
Version 6.2.3 Guidelines	141
Upgrade Failure: Firepower 2100 Series from Version 6.2.2.5	142
Edit/Resave Realms After FTD/FDM Upgrade	142
Upgrade Can Unregister FTD/FDM from CSSM	143
Edit/Resave Access Control Policies After Upgrade	143
Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade	143
Version 6.2.2 Guidelines	144
Security Enhancement: Signed Upgrade Packages	144
Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0	144
Version 6.2.0 Guidelines	145
Access Control Can Get Latency-Based Performance Settings from SRUs	145
'Short Fail Open' Replaces 'Failsafe' on FTD	146
IAB 'All Applications' Option Removed on Upgrade	146
URL Filtering Sub-site Lookups for Low-Memory Devices Disabled on Upgrade	147
Version 6.1.0 Guidelines	147
Patch Guidelines by Version	147
Version 6.7.x.x Guidelines	147

Version 6.6.x.x Guidelines	148
Version 6.6.0.1 FTD Upgrade with FDM Suspends HA	148
Version 6.4.0.x Guidelines	149
Version 6.3.0.x Guidelines	149
Version 6.2.3.x Guidelines	149
Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure	150
Version 6.2.3.3 FTD Device Cannot Switch to Local Management	150
Upgrade Can Unregister FTD/FDM from CSSM	150
Hotfix Before Upgrading Version 6.2.3-88 FMCs	151
Version 6.2.0.x Guidelines	151
Apply Hotfix BH to Version 6.2.0.3 FMCs	151
Date-Based Guidelines	151
Expired CA Certificates for Dynamic Analysis	152

CHAPTER 8
ASA Upgrade Guidelines 153

Version-Specific Guidelines and Migrations	153
9.16 Guidelines	153
9.15 Guidelines	154
9.14 Guidelines	156
9.13 Guidelines	156
9.12 Guidelines	159
9.10 Guidelines	160
9.9 Guidelines	160
9.8 Guidelines	160
9.7 Guidelines	160
9.6 Guidelines	160
9.5 Guidelines and Migration	161
9.4 Guidelines and Migration	162
Clustering Guidelines	163
Failover Guidelines	165
Additional Guidelines	166

CHAPTER 9
Time and Disk Space Tests 167

About Time Tests	169
------------------	-----

About Disk Space Requirements	170
Version 7.0.1 Time and Disk Space	171
Version 7.0.0.1 Time and Disk Space	171
Version 7.0.0 Time and Disk Space	172
Version 6.7.0.2 Time and Disk Space	172
Version 6.7.0.1 Time and Disk Space	173
Version 6.7.0 Time and Disk Space	174
Version 6.6.5.1 Time and Disk Space	175
Version 6.6.5 Time and Disk Space	176
Version 6.6.4 Time and Disk Space	177
Version 6.6.3 Time and Disk Space	178
Version 6.6.1 Time and Disk Space	179
Version 6.6.0.1 Time and Disk Space	179
Version 6.6.0 Time and Disk Space	180
Version 6.5.0.5 Time and Disk Space	181
Version 6.5.0.4 Time and Disk Space	181
Version 6.5.0.3 Time and Disk Space	182
Version 6.5.0.2 Time and Disk Space	182
Version 6.5.0.1 Time and Disk Space	183
Version 6.5.0 Time and Disk Space	183
Version 6.4.0.13 Time and Disk Space	183
Version 6.4.0.12 Time and Disk Space	184
Version 6.4.0.11 Time and Disk Space	185
Version 6.4.0.10 Time and Disk Space	186
Version 6.4.0.9 Time and Disk Space	186
Version 6.4.0.8 Time and Disk Space	187
Version 6.4.0.7 Time and Disk Space	188
Version 6.4.0.6 Time and Disk Space	188
Version 6.4.0.5 Time and Disk Space	188
Version 6.4.0.4 Time and Disk Space	189
Version 6.4.0.3 Time and Disk Space	189
Version 6.4.0.2 Time and Disk Space	190
Version 6.4.0.1 Time and Disk Space	191
Version 6.4.0 Time and Disk Space	191

Version 6.3.0.5 Time and Disk Space	192
Version 6.3.0.4 Time and Disk Space	192
Version 6.3.0.3 Time and Disk Space	193
Version 6.3.0.2 Time and Disk Space	193
Version 6.3.0.1 Time and Disk Space	194
Version 6.3.0 Time and Disk Space	194
Version 6.2.3.17 Time and Disk Space	195
Version 6.2.3.16 Time and Disk Space	195
Version 6.2.3.15 Time and Disk Space	196
Version 6.2.3.14 Time and Disk Space	196
Version 6.2.3.13 Time and Disk Space	197
Version 6.2.3.12 Time and Disk Space	198
Version 6.2.3.11 Time and Disk Space	198
Version 6.2.3.10 Time and Disk Space	199
Version 6.2.3.9 Time and Disk Space	199
Version 6.2.3.8 Time and Disk Space	200
Version 6.2.3.7 Time and Disk Space	200
Version 6.2.3.6 Time and Disk Space	200
Version 6.2.3.5 Time and Disk Space	201
Version 6.2.3.4 Time and Disk Space	201
Version 6.2.3.3 Time and Disk Space	202
Version 6.2.3.2 Time and Disk Space	202
Version 6.2.3.1 Time and Disk Space	203
Version 6.2.3 Time and Disk Space	203
Version 6.2.2.5 Time and Disk Space	204
Version 6.2.2.4 Time and Disk Space	205
Version 6.2.2.3 Time and Disk Space	206
Version 6.2.2.2 Time and Disk Space	206
Version 6.2.2.1 Time and Disk Space	207
Version 6.2.2 Time and Disk Space	207
Version 6.2.0.6 Time and Disk Space	208
Version 6.2.0.5 Time and Disk Space	209
Version 6.2.0.4 Time and Disk Space	209
Version 6.2.0.3 Time and Disk Space	210

Version 6.2.0.2 Time and Disk Space	210
Version 6.2.0.1 Time and Disk Space	211
Version 6.2.0 Time and Disk Space	211
Version 6.1.0.7 Time and Disk Space	212
Version 6.1.0.6 Time and Disk Space	212
Version 6.1.0.5 Time and Disk Space	213
Version 6.1.0.4 Time and Disk Space	214
Version 6.1.0.3 Time and Disk Space	214
Version 6.1.0.2 Time and Disk Space	215
Version 6.1.0.1 Time and Disk Space	215
Version 6.1.0 Time and Disk Space	216
Version 6.0.1.4 Time and Disk Space	216
Version 6.0.1.3 Time and Disk Space	217
Version 6.0.1.2 Time and Disk Space	217
Version 6.0.1.1 Time and Disk Space	218

CHAPTER 10**Traffic Flow and Inspection 219**

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300	219
--	-----



CHAPTER 1

Planning Your Upgrade

- [Upgrade Planning Phases, on page 1](#)
- [Current Version and Model Information, on page 2](#)
- [Upgrade Paths , on page 2](#)
- [Download Upgrade Packages, on page 15](#)
- [Upload Firepower Software Upgrade Packages with FMC, on page 18](#)
- [Upload Firepower Threat Defense Upgrade Packages with FDM, on page 21](#)
- [Firepower Software Readiness Checks with FMC, on page 23](#)
- [Firepower Software Readiness Checks with FDM, on page 25](#)

Upgrade Planning Phases

This table summarizes the upgrade planning process. For full checklists, see the upgrade procedures.

Table 1: Upgrade Planning Phases

Phase	Includes
Planning and Feasibility Careful planning and preparation can help you avoid missteps.	Assess your deployment. Plan your upgrade path. Read <i>all</i> upgrade guidelines and plan configuration changes. Check appliance access. Check bandwidth. Schedule maintenance windows.
Upgrade Packages Upgrade packages are available on the Cisco Support & Download site.	Download upgrade packages from Cisco. Upload upgrade packages to appliances or place them somewhere the appliances can access during the upgrade process.
Backups The ability to recover from a disaster is an essential part of any system maintenance plan.	Back up logical devices. Back up FXOS.

Phase	Includes
FXOS Upgrade Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.	Upgrade FMC virtual hosting, if needed. Upgrade FXOS.
Final Checks for FTD Logical Devices A set of final checks ensures you are ready to upgrade.	Check configurations. Check NTP synchronization. Check disk space. Deploy configurations. Run readiness checks. Check running tasks. Check deployment health and communications.

Current Version and Model Information

Use these commands to find current version and model information for your deployment,

Table 2:

Component	Information
FXOS for Firepower 4100/9300	Firepower Chassis Manager: Choose Overview . FXOS CLI: For the version, use the show version command. For the model, enter scope chassis 1 , and then show inventory .
Firepower Threat Defense logical device with FMC	On the FMC, choose Devices > Device Management .
Firepower Threat Defense logical device with FDM	In FDM, click Device to get to the Device Summary .
ASA logical device	ASDM: Choose Home > Device Dashboard > Device Information . ASA CLI: Use the show version command.
Firepower Management Center	On the FMC, choose Help > About .

Upgrade Paths

Your upgrade path is a detailed plan for what you will upgrade and when, including appliance operating systems. At all times, you must maintain hardware, software, operating system, and hosting compatibility.



Note In Firepower Management Center deployments, you upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first.

What Do I Have?

Before you upgrade any Firepower appliance, determine the current state of your deployment. In addition to current version and model information, determine if your devices are configured for high availability/scalability, and if they are deployed passively, as an IPS, as a firewall, and so on.

See [Current Version and Model Information, on page 2](#).

Where Am I Going?

Now that you know what you have, make sure you can get to where you want to go:

- Can your deployment run the target Firepower version?
- Can your deployment run the target ASA version?
- Do your appliances require a separate operating system upgrade before they can run the target Firepower version? Can your appliances run the target OS?

For answers to all these questions, see [Compatibility, on page 103](#).

How Do I Get There?

After you determine that your appliances can run the target version, make sure direct upgrade is possible:

- Is direct Firepower software upgrade possible?
- Is direct ASA software upgrade possible?
- Is direct FXOS upgrade possible?

For answers to all these questions, see the upgrade paths provided in this guide.



Tip Upgrade paths that require intermediate versions can be time consuming. Especially in larger Firepower deployments where you must alternate Firepower Management Center and device upgrades, consider reimaging older devices instead of upgrading. First, remove the devices from the Firepower Management Center. Then, upgrade the Firepower Management Center, reimage the devices, and re-add them to the Firepower Management Center.

Can I Maintain Deployment Compatibility?

At all times, you must maintain hardware, software, and operating system compatibility:

- Can I maintain Firepower version compatibility between the FMC and its managed devices: [FMC-Device Compatibility, on page 103](#)
- Can I maintain FXOS compatibility with logical devices: [Firepower 4100/9300 Compatibility with ASA and FTD, on page 108](#)

Upgrade Path: FXOS

This table provides FXOS upgrade paths for a Firepower 4100/9300 chassis without any configured logical devices.

Find your current version in the left column. You can upgrade directly to any of the versions listed in the right column. In general, we recommend the latest FXOS build in the version sequence.


Note

For early versions of FXOS, you must upgrade to all intermediate versions between the current version and the target version. Once you reach FXOS 2.2.2, your upgrade options are wider.

Table 3: Upgrade Paths: FXOS on Firepower 4100/9300

Current FXOS Version	Target FXOS Version
2.9.1	→ 2.10.1
2.8.1	Any of: → 2.10.1 → 2.9.1
2.7.1	Any of: → 2.10.1 → 2.9.1 → 2.8.1
2.6.1	Any of: → 2.10.1 → 2.9.1 → 2.8.1 → 2.7.1
2.4.1	Any of: → 2.10.1 → 2.9.1 → 2.8.1 → 2.7.1 → 2.6.1

Current FXOS Version	Target FXOS Version
2.3.1	Any of: → 2.10.1 → 2.9.1 → 2.8.1 → 2.7.1 → 2.6.1 → 2.4.1
2.2.2	Any of: → 2.10.1 → 2.9.1 → 2.8.1 → 2.7.1 → 2.6.1 → 2.4.1 → 2.3.1
2.2.1	→ 2.2.2
2.1.1	→ 2.2.1
2.0.1	→ 2.1.1
1.1.4	→ 2.0.1
1.1.3	→ 1.1.4
1.1.2	→ 1.1.3
1.1.1	→ 1.1.2

Upgrade Path: ASA Logical Devices

This table provides upgrade paths for ASA logical devices on the Firepower 4100/9300.



Note

If you are upgrading a Firepower 9300 chassis with FTD *and* ASA logical devices running on separate modules, see [Upgrade Path: FTD and ASA Logical Devices for Firepower 9300, on page 12](#).

Find your current version combination in the left column. You can upgrade to any of the version combinations listed in the right column. This is a multi-step process: first upgrade FXOS, then upgrade the logical devices.

Note that this table lists only Cisco's specially qualified version combinations. Because you must upgrade FXOS first, you will *briefly* run a supported—but not recommended—combination, where FXOS is "ahead" of the logical devices. For minimum builds and other detailed compatibility information, see [Firepower 4100/9300 Compatibility with ASA and FTD, on page 108](#).



Note For early versions of FXOS, you must upgrade to all intermediate versions between the current version and the target version. Once you reach FXOS 2.2.2, your upgrade options are wider.

Table 4: Upgrade Paths: Firepower 4100/9300 with ASA Logical Devices

Current Version	Target Version
FXOS 2.9.1 with ASA 9.15(x)	→ FXOS 2.10.1 with ASA 9.16(x)
FXOS 2.8.1 with ASA 9.14(x)	Any of: → FXOS 2.10.1 with ASA 9.16(x) → FXOS 2.9.1 with ASA 9.15(x)
FXOS 2.7.1 with ASA 9.13(x)	Any of: → FXOS 2.10.1 with ASA 9.16(x) → FXOS 2.9.1 with ASA 9.15(x) → FXOS 2.8.1 with ASA 9.14(x)
FXOS 2.6.1 with ASA 9.12(x)	Any of: → FXOS 2.10.1 with ASA 9.16(x) → FXOS 2.9.1 with ASA 9.15(x) → FXOS 2.8.1 with ASA 9.14(x) → FXOS 2.7.1 with ASA 9.13(x)
FXOS 2.4.1 with ASA 9.10(x)	Any of: → FXOS 2.10.1 with ASA 9.16(x) → FXOS 2.9.1 with ASA 9.15(x) → FXOS 2.8.1 with ASA 9.14(x) → FXOS 2.7.1 with ASA 9.13(x) → FXOS 2.6.1 with ASA 9.12(x)

Current Version	Target Version
FXOS 2.3.1 with ASA 9.9(x)	Any of: → FXOS 2.10.1 with ASA 9.16(x) → FXOS 2.9.1 with ASA 9.15(x) → FXOS 2.8.1 with ASA 9.14(x) → FXOS 2.7.1 with ASA 9.13(x) → FXOS 2.6.1 with ASA 9.12(x) → FXOS 2.4.1 with ASA 9.10(1)
FXOS 2.2.2 with ASA 9.8(x)	Any of: → FXOS 2.10.1 with ASA 9.16(x) → FXOS 2.9.1 with ASA 9.15(x) → FXOS 2.8.1 with ASA 9.14(x) → FXOS 2.7.1 with ASA 9.13(x) → FXOS 2.6.1 with ASA 9.12(x) → FXOS 2.4.1 with ASA 9.10(x) → FXOS 2.3.1 with ASA 9.9(x)
FXOS 2.2.1 with ASA 9.8(1)	→ FXOS 2.2.2 with ASA 9.8(x)
FXOS 2.1.1 with ASA 9.7(x)	→ FXOS 2.2.1 with ASA 9.8(1)
FXOS 2.0.1 with ASA 9.6(2), 9.6(3), or 9.6(4)	→ FXOS 2.1.1 with ASA 9.7(x)
FXOS 1.1.4 with ASA 9.6(1)	→ FXOS 2.0.1 with ASA 9.6(2), 9.6(3), or 9.6(4)
FXOS 1.1.3 with ASA 9.5(2) or 9.5(3)	→ FXOS 1.1.4 with ASA 9.6(1)
FXOS 1.1.2 with ASA 9.4(2)	→ FXOS 1.1.3 with ASA 9.5(2) or 9.5(3)
FXOS 1.1.1 with ASA 9.4(1)	→ FXOS 1.1.2 with ASA 9.4(2)

Note on Downgrades

Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

Upgrade Path: FTD Logical Devices and FMC

This table provides upgrade paths for the Firepower 4100/9300 with FTD logical devices, managed by a Firepower Management Center.



Note If you are upgrading a Firepower 9300 chassis with FTD *and* ASA logical devices running on separate modules, see [Upgrade Path: FTD and ASA Logical Devices for Firepower 9300, on page 12](#).

Find your current version combination in the left column. You can upgrade to any of the version combinations listed in the right column. This is a multi-step process: first upgrade FXOS, then upgrade the logical devices.

Note that this table lists only Cisco's specially qualified version combinations. Because you must upgrade FXOS first, you will *briefly* run a supported—but not recommended—combination, where FXOS is "ahead" of the logical devices. For minimum builds and other detailed compatibility information, see [Firepower 4100/9300 Compatibility with ASA and FTD, on page 108](#).



Note For early versions of FXOS, you must upgrade to all intermediate versions between the current version and the target version. Once you reach FXOS 2.2.2, your upgrade options are wider.

Table 5: Upgrade Paths: Firepower 4100/9300 with FTD Logical Devices

Current Versions	Target Versions
FXOS 2.9.1 with FTD 6.7.0/6.7.x	→ FXOS 2.10.1 with FTD 7.0.0/7.0.x
FXOS 2.8.1 with FTD 6.6.0/6.6.x	Any of: → FXOS 2.10.1 with FTD 7.0.0/7.0.x → FXOS 2.9.1 with FTD 6.7.x
FXOS 2.7.1 with FTD 6.5.0 First support for FDM & CDO management.	Any of: → FXOS 2.10.1 with FTD 7.0.0/7.0.x → FXOS 2.9.1 with FTD 6.7.0/6.7.x → FXOS 2.8.1 with FTD 6.6.0/6.6.x
FXOS 2.6.1 with FTD 6.4.0	Any of: → FXOS 2.10.1 with FTD 7.0.0/7.0.x → FXOS 2.9.1 with FTD 6.7.0/6.7.x → FXOS 2.8.1 with FTD 6.6.0/6.6.x → FXOS 2.7.1 with FTD 6.5.0
FXOS 2.4.1 with FTD 6.3.0	Any of: → FXOS 2.9.1 with FTD 6.7.0/6.7.x → FXOS 2.8.1 with FTD 6.6.0/6.6.x → FXOS 2.7.1 with FTD 6.5.0 → FXOS 2.6.1 with FTD 6.4.0

Current Versions	Target Versions
FXOS 2.3.1 with FTD 6.2.3	Any of: → FXOS 2.8.1 with FTD 6.6.0/6.6.x → FXOS 2.7.1 with FTD 6.5.0 → FXOS 2.6.1 with FTD 6.4.0 → FXOS 2.4.1 with FTD 6.3.0
FXOS 2.2.2 with FTD 6.2.2	Any of: → FXOS 2.6.1 with FTD 6.4.0 → FXOS 2.4.1 with FTD 6.3.0 → FXOS 2.3.1 with FTD 6.2.3
FXOS 2.2.2 with FTD 6.2.0	Any of: → FXOS 2.6.1 with FTD 6.4.0 → FXOS 2.4.1 with FTD 6.3.0 → FXOS 2.3.1 with FTD 6.2.3 → FXOS 2.2.2 with FTD 6.2.2
FXOS 2.2.1 with FTD 6.2.0	→ FXOS 2.2.2 with FTD 6.2.0 (upgrade <i>only</i> FXOS) Another option is to upgrade to FXOS 2.2.2 with FTD 6.2.2, which is a recommended combination. However, if you plan to further upgrade your deployment, don't bother. Now that you are running FXOS 2.2.2, you can upgrade all the way to FXOS 2.6.1 with FTD 6.4.0.
FXOS 2.1.1 with FTD 6.2.0	→ FXOS 2.2.1 with FTD 6.2.0 (upgrade <i>only</i> FXOS)
FXOS 2.0.1 with FTD 6.1.0	→ FXOS 2.1.1 with FTD 6.2.0
FXOS 1.1.4 with FTD 6.0.1	→ FXOS 2.0.1 with FTD 6.1.0

Upgrading FXOS with FTD Logical Devices in Clusters or HA Pairs

In Firepower Management Center deployments, you upgrade clustered and high availability FTD logical devices as a unit. However, you upgrade FXOS on each chassis independently.

Table 6: FXOS + FTD Upgrade Order

Deployment	Upgrade Order
Standalone device	1. Upgrade FXOS.
Cluster, units on the same chassis (Firepower 9300 only)	2. Upgrade FTD.

Deployment	Upgrade Order
High availability	<p>To minimize disruption, always upgrade the standby.</p> <ol style="list-style-type: none"> 1. Upgrade FXOS on the standby. 2. Switch roles. 3. Upgrade FXOS on the new standby. 4. Upgrade FTD.
Cluster, units on different chassis (6.2+)	<p>To minimize disruption, always upgrade an all-data unit chassis. For example, for a two-chassis cluster:</p> <ol style="list-style-type: none"> 1. Upgrade FXOS on the all-data unit chassis. 2. Switch the control module to the chassis you just upgraded. 3. Upgrade FXOS on the new all-data unit chassis. 4. Upgrade FTD.

With older versions, hitless upgrades have some additional requirements.

Table 7: Hitless Upgrades in Older Versions

Scenario	Details
<p>Upgrading high availability or clustered devices and you are currently running any of:</p> <ul style="list-style-type: none"> • FXOS 1.1.4.x through 2.2.1.x • FXOS 2.2.2.17 through FXOS 2.2.2.68 • FXOS 2.3.1.73 through FXOS 2.3.1.111 <p>With:</p> <ul style="list-style-type: none"> • FTD 6.0.1 through 6.2.2.x 	<p>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. Performing a hitless upgrade requires that you always run a compatible combination.</p> <p>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:</p> <ol style="list-style-type: none"> 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. <p>For example, if you are running FXOS 2.2.2.17 with FTD 6.2.2.0, and you want to upgrade to FXOS 2.6.1 with FTD 6.4.0, then you can:</p> <ol style="list-style-type: none"> 1. Upgrade FTD to 6.2.2.5. 2. Upgrade FXOS to 2.6.1. 3. Upgrade FTD to 6.4.0.
Upgrading high availability devices to FTD Version 6.1.0	Requires a preinstallation package. For more information, see Firepower System Release Notes Version 6.1.0 Preinstallation Package .

Note on Downgrades

Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

Upgrade Path: FTD Logical Devices and FDM

This table provides upgrade paths for the Firepower 4100/9300 with FTD logical devices, managed by Firepower Device Manager.

**Note**

If you are upgrading a Firepower 9300 chassis with FTD *and* ASA logical devices running on separate modules, see [Upgrade Path: FTD and ASA Logical Devices for Firepower 9300, on page 12](#).

Find your current version combination in the left column. You can upgrade to any of the version combinations listed in the right column. This is a multi-step process: first upgrade FXOS, then upgrade the logical devices.

Note that this table lists only Cisco's specially qualified version combinations. Because you must upgrade FXOS first, you will *briefly* run a supported—but not recommended—combination, where FXOS is "ahead" of the logical devices. For minimum builds and other detailed compatibility information, see [Firepower 4100/9300 Compatibility with ASA and FTD, on page 108](#).

Table 8: Upgrade Paths: Firepower 4100/9300 with FTD Logical Devices

Current Versions	Target Versions
FXOS 2.9.1 with FTD 6.7.0/6.7.x	→ FXOS 2.10.1 with FTD 7.0.0/7.0.x
FXOS 2.8.1 with FTD 6.6.0/6.6.x	Any of: → FXOS 2.10.1 with FTD 7.0.0/7.0.x → FXOS 2.9.1 with FTD 6.7.x
FXOS 2.7.1 with FTD 6.5.0 First support for FDM & CDO management.	Any of: → FXOS 2.10.1 with FTD 7.0.0/7.0.x → FXOS 2.9.1 with FTD 6.7.0/6.7.x → FXOS 2.8.1 with FTD 6.6.0/6.6.x

Upgrading FXOS with FTD Logical Devices in HA Pairs

In Firepower Device Manager deployments, you upgrade the members of a high availability pair separately. In the scenarios in this table, Device A is the original active device and Device B is the original standby.

Table 9: FXOS + FTD Upgrade Order

Deployment	Upgrade Order
Standalone device	<ol style="list-style-type: none"> 1. Upgrade FXOS. 2. Upgrade FTD logical device.

Deployment	Upgrade Order
High availability	<p>Upgrade FXOS on both chassis before you upgrade FTD. To minimize disruption, always upgrade the standby:</p> <ol style="list-style-type: none"> 1. Upgrade FXOS on the chassis with the standby FTD logical device (B). 2. Switch roles. 3. Upgrade FXOS on the chassis with the new standby logical device (A). 4. Upgrade the new standby FTD logical device (A). 5. Switch roles again. 6. Upgrade the original standby FTD logical device (B).

Note on Downgrades

Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

Upgrade Path: FTD and ASA Logical Devices for Firepower 9300

This table provides upgrade paths for a Firepower 9300 chassis with FTD and ASA logical devices running on separate modules.

Find your current version combination in the left column. You can upgrade to any of the version combinations listed in the right column. This is a multi-step process: first upgrade FXOS, then upgrade the logical devices.

Note that this table lists only Cisco's specially qualified version combinations. Because you must upgrade FXOS first, you will *briefly* run a supported—but not recommended—combination, where FXOS is "ahead" of the logical devices. For minimum builds and other detailed compatibility information, see [Firepower 4100/9300 Compatibility with ASA and FTD, on page 108](#).



Note

In this type of deployment, you must make sure that upgrading FXOS does not bring you out of compatibility with *either* type of logical device. If you need to skip multiple versions, FTD will usually be the limiter—FXOS and ASA can usually upgrade further in one hop than FTD can.

Table 10: Upgrade Paths: Firepower 9300 with FTD and ASA Logical Devices

Current Versions	Target Versions
FXOS 2.9.1 with: <ul style="list-style-type: none"> • FTD 6.7.0/6.7.x • ASA 9.15(x) 	→ FXOS 2.10.1 with ASA 9.16(x) and FTD 7.0.0/7.0.x

Current Versions	Target Versions
FXOS 2.8.1 with: <ul style="list-style-type: none"> • FTD 6.6.0/6.6.x • ASA 9.14(x) 	Any of: <ul style="list-style-type: none"> → FXOS 2.10.1 with ASA 9.16(x) and FTD 7.0.07.0.x → FXOS 2.9.1 with ASA 9.15(x) and FTD 6.7.0/6.7.x
FXOS 2.7.1 with: <ul style="list-style-type: none"> • FTD 6.5.0 • ASA 9.13(x) 	Any of: <ul style="list-style-type: none"> → FXOS 2.10.1 with ASA 9.16(x) and FTD 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and FTD 6.7.0/6.7.x → FXOS 2.8.1 with ASA 9.14(x) and FTD 6.6.0/6.6.x
FXOS 2.6.1 with: <ul style="list-style-type: none"> • FTD 6.4.0 • ASA 9.12(x) 	Any of: <ul style="list-style-type: none"> → FXOS 2.10.1 with ASA 9.16(x) and FTD 7.0.x → FXOS 2.9.1 with ASA 9.15(x) and FTD 6.7.0/6.7.x → FXOS 2.8.1 with ASA 9.14(x) and FTD 6.6.0/6.6.x → FXOS 2.7.1 with ASA 9.13(x) and FTD 6.5.0

Upgrade Path: Firepower Management Centers

This table provides upgrade paths for Firepower Management Centers, including FMCv.

Find your current version in the left column. You can upgrade directly to any of the versions listed in the right column.



Note

If your current version was released on a date after your target version, you *may* not be able to upgrade as listed in the table. In those cases, the upgrade quickly fails and displays an error explaining that there are data store incompatibilities between the two versions. The [Cisco Firepower Release Notes](#) for both your current and target version list any specific restrictions. The [Cisco Firepower Management Center New Features by Release](#) lists all relevant release dates.

Table 11: FMC Direct Upgrades

Current Version	Target Version
7.0.0	Any of:
7.0.x (maintenance releases)	→ Any later 7.0.x maintenance release
6.7.0	Any of:
6.7.x (maintenance releases)	→ 7.0.0 or any 7.0.x maintenance release
	→ Any later 6.7.x maintenance release

Current Version	Target Version
6.6.0 6.6.x (maintenance releases) Last support for FMC 2000 and 4000.	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → Any later 6.6.x maintenance release
6.5.0	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release
6.4.0 Last support for FMC 750, 1500, and 3500.	Any of: → 7.0.0 or any 7.0.x maintenance release → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0
6.3.0	Any of: → 6.7.0 or any 6.7.x maintenance release → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0
6.2.3	Any of: → 6.6.0 or any 6.6.x maintenance release → 6.5.0 → 6.4.0 → 6.3.0
6.2.2	Any of: → 6.4.0 → 6.3.0 → 6.2.3

Current Version	Target Version
6.2.1	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.2.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.2
6.1.0	Any of: → 6.4.0 → 6.3.0 → 6.2.3 → 6.2.0
6.0.1	Any of: → 6.1.0
6.0.0	Any of: → 6.0.1 Requires a preinstallation package: Firepower System Release Notes Version 6.0.1 Preinstallation .
5.4.1.1	Any of: → 6.0.0 Requires a preinstallation package: FireSIGHT System Release Notes Version 6.0.0 Preinstallation .

Download Upgrade Packages

Download upgrade packages from the Cisco Support & Download site before you start your upgrade. Depending on the specific upgrade, you should put the packages on either your local computer or a server that the appliance can access. The individual checklists and procedures in this guide explain your choices.



Note Downloads require a Cisco.com login and service contract.

Firepower Software Packages

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

- Firepower Management Center, including Firepower Management Center Virtual:
<https://www.cisco.com/go/firepower-software>
- Firepower Threat Defense (ISA 3000): <https://www.cisco.com/go/isa3000-software>
- Firepower Threat Defense (all other models, including Firepower Threat Defense Virtual):
<https://www.cisco.com/go/ftd-software>

To find an upgrade package, select or search for your appliance model, then browse to the software download page for your current version. Available upgrade packages are listed along with installation packages, hotfixes, and other applicable downloads.



Tip A Firepower Management Center with internet access can download select releases directly from Cisco, some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors.

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

For example:

- Package: `Cisco_Firepower_Mgmt_Center_Upgrade--999.sh.REL.tar`
- Platform: Firepower Management Center
- Package type: Upgrade
- Version and build: -999
- File extension: sh.REL.tar

So that the system can verify that you are using the correct files, upgrade packages from Version 6.2.1+ are *signed* tar archives (.tar). Do not untar signed (.tar) packages. And, do not transfer upgrade packages by email.



Note After you upload a signed upgrade package, the Firepower Management Center GUI can take several minutes to load as the system verifies the package. To speed up the display, remove these packages after you no longer need them.

Firepower Software Upgrade Packages

Table 12:

Platform	Versions	Package
FMC/FMCv	6.3.0+	Cisco_Firepower_Mgmt_Center
	5.4.0 to 6.2.3	Sourcefire_3D_Defense_Center_S3
Firepower 4100/9300	Any	Cisco_FTD_SSP

ASA Packages

ASA software for the Firepower 4100/9300 are available on the Cisco Support & Download site.

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

To find ASA software, select or search for your Firepower appliance model, browse to the appropriate download page, and select a version.



Note

When you upgrade the ASA bundle in FXOS, the ASDM image in the bundle replaces the previous ASDM bundle image on the ASA because they have the same name (**asdm.bin**). But if you manually chose a different ASDM image that you uploaded (for example, **asdm-782.bin**), then you continue to use that image even after a bundle upgrade. To make sure that you are running a compatible version of ASDM, you should either upgrade ASDM before you upgrade the bundle, or you should reconfigure the ASA to use the bundled ASDM image (**asdm.bin**) just before upgrading the ASA bundle.

Table 13: ASA Software for the Firepower 4100/9300

Download Page	Software Type	Package
Adaptive Security Appliance (ASA) Software	ASA and ASDM upgrade	cisco-asa.version.SPA.csp
Adaptive Security Appliance (ASA) Device Manager	ASDM upgrade only	asdm-version.bin
Adaptive Security Appliance REST API Plugin	ASA REST API	asa-restapi-version-lfbff-k8.SPA

FXOS Packages

FXOS packages for the Firepower 4100/9300 are available on the Cisco Support & Download site.

- Firepower 4100 series: <http://www.cisco.com/go/firepower4100-software>

- Firepower 9300: <http://www.cisco.com/go/firepower9300-software>

To find FXOS packages, select or search for your Firepower appliance model, then browse to the Firepower Extensible Operating System download page for the target version.

**Note**

If you plan to use the CLI to upgrade FXOS, copy the upgrade package to a server that the Firepower 4100/9300 can access using SCP, SFTP, TFTP, or FTP.

Table 14: FXOS Packages for the Firepower 4100/9300

Package Type	Package
FXOS image	fxos-k9.version.SPA
Recovery (kickstart)	fxos-k9-kickstart.version.SPA
Recovery (manager)	fxos-k9-manager.version.SPA
Recovery (system)	fxos-k9-system.version.SPA
MIBs	fxos-mibs-fp9k-fp4k.version.zip
Firmware: Firepower 4100 series	fxos-k9-fpr4k-firmware.version.SPA
Firmware: Firepower 9300	fxos-k9-fpr9k-firmware.version.SPA

Upload Firepower Software Upgrade Packages with FMC

To upgrade Firepower software, the software upgrade package must be on the appliance.

Upload to the Firepower Management Center

Use this procedure to manually upload Firepower software upgrade packages to the Firepower Management Center, for itself and the devices it manages.

Before you begin

If you are upgrading the standby Firepower Management Center in a high availability pair, pause synchronization.

In Firepower Management Center high availability deployments, you must upload the Firepower Management Center upgrade package to both peers, pausing synchronization before you transfer the package to the standby. To limit interruptions to HA synchronization, you can transfer the package to the active peer during the preparation stage of the upgrade, and to the standby peer as part of the actual upgrade process, after you pause synchronization.

Procedure

Step 1 On the Firepower Management Center web interface, choose **System > Updates**.

Step 2 Click **Upload Update**.

Tip Select upgrade packages become available for direct download by the Firepower Management Center some time after the release is available for manual download. The length of the delay depends on release type, release adoption, and other factors. If your Firepower Management Center has internet access, you can instead click **Download Updates** to download *all* eligible packages for your deployment, as well as the latest VDB if needed.

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**.

Upload to an Internal Server (Version 6.6.0+ FTD with FMC)

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.

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 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 and copy them 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.

Procedure

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.

Copy to Managed Devices

To upgrade Firepower software, the upgrade package must be on the device. When supported, we recommend you use this procedure to copy (*push*) packages to managed devices before you initiate the device upgrade.



Note

For the Firepower 4100/9300, we recommend (and sometimes require) you copy the Firepower Threat Defense upgrade package before you begin the required companion FXOS upgrade.

Support varies by Firepower version:

- Version 6.2.2 and earlier do not support pre-upgrade copy.

When you start a device upgrade, the system copies the upgrade package from the Firepower Management Center to the device as the first task.

- Version 6.2.3 adds the ability to manually copy upgrade packages to the device from the Firepower Management Center.

This reduces the length of your upgrade maintenance window.

- Version 6.6.0 adds the ability to manually copy upgrade packages from an internal web server to Firepower Threat Defense devices.

This is useful if you have limited bandwidth between the Firepower Management Center and its Firepower Threat Defense devices. It also saves space on the Firepower Management Center.

- Version 7.0.0 introduces a new Firepower Threat Defense upgrade workflow that prompts you to copy the upgrade package to Firepower Threat Defense devices.

If your Firepower Management Center is running Version 7.0.0+, we recommend you use the Device Upgrade page to copy the upgrade package to FTD devices; see [Upgrade Firepower Threat Defense with FMC \(Version 7.0.0\), on page 57](#). You must still use this procedure to copy upgrade packages in older deployments.

Note that when you copy manually, each device gets the upgrade package from the source—the system does not copy upgrade packages between cluster or HA member units.

Before you begin

Make sure your management network has the bandwidth to perform large data transfers. See [Guidelines for Downloading Data from the Firepower Management Center to Managed Devices](#) (Troubleshooting TechNote).

Procedure

-
- | | |
|---------------|--|
| Step 1 | On the Firepower Management Center web interface, choose System > Updates . |
| Step 2 | Put the upgrade package where the device can get it. <ul style="list-style-type: none">• Firepower Management Center: Manually upload or directly retrieve the package to the FMC.• Internal web server (Firepower Threat Defense Version 6.6.0+): Upload to an internal web server and configure Firepower Threat Defense devices to get the package from that server. |
| 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. <p>If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.</p> |
| Step 4 | Push the package <ul style="list-style-type: none">• Firepower Management Center: Click Push.• Internal web server: Click Download Update to Device from Source. |
-

Upload Firepower Threat Defense Upgrade Packages with FDM

To upgrade Firepower Threat Defense software, the software upgrade package must be on the device.

Upload to the FTD Device (Version 6.2.0+ with FDM)

Procedure

-
- | | |
|---------------|--|
| Step 1 | Select Device , then click View Configuration in the Updates summary. <p>The System Upgrade section shows the currently running software version and any update that you have already uploaded.</p> |
| Step 2 | Upload the upgrade file. |

- If you have not yet uploaded an upgrade file, click **Browse** and select the file. When the upload is complete, you can optionally select the **Run Upgrade Immediately on Upload** option to start the installation.
- If there is already an uploaded file, but you want to upload a different one, click the **Upload Another File** link. You can upload one file only. If you upload a new file, it replaces the old file.
- To remove the file, click the delete icon (🗑).

Upload to the FTD Device (Version 6.0.1 & 6.1.0 with FDM)

Procedure

- Step 1** Obtain the upgrade image and prepare it for installation.
- a) Log into Cisco.com and download the upgrade image.
 - Ensure that you obtain the appropriate upgrade file, whose file type is .sh. Do not download the system software package or the boot image.
 - Verify that you are running the required baseline image for the upgrade.
 - b) Put the image on an HTTP server that you can reach from the management IP address.
Alternatively, you can use TFTP or SCP to download the file. If you choose one of those options, place the file on a server that supports those file transfer protocols.
- Step 2** Use an SSH client to log into the management IP address using the **admin** user account and password.
Alternatively, you can connect to the Console port.
- Step 3** Enter the **expert** command to access expert mode.
- ```
> expert
admin@firepower:~$
```
- Step 4** Change the working directory (**cd**) to /var/sf/updates/.
- ```
admin@firepower:~$ cd /var/sf/updates/
admin@firepower:/var/sf/updates$
```
- Step 5** Download the upgrade file from your HTTP server.
- sudo wget url**
- For example, the following command downloads the fictitious Cisco_FTD_Upgrade-6.2.0-181.sh upgrade file from the ftd folder on the files.example.com HTTP server. Because the **sudo** command operates under root user, you see a stock warning, and you must re-enter the **admin** password before the command executes. Wait for the download to complete.

Use the **ftfp** or **scp** commands instead if you are not using an HTTP server.

Readiness checks assess a Firepower appliance's preparedness for a software upgrade. If the appliance fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, we recommend you do not begin the upgrade.

If your FMC is running Version 7.0.0+, we recommend you use the Device Upgrade page to run readiness checks on FTD devices; see [Upgrade Firepower Threat Defense with FMC \(Version 7.0.0\), on page 57](#).

This procedure is valid for FMCs *currently* running Version 6.7.0+, and their managed devices, including devices running older versions (6.3.0–6.6.x), and FTD devices in high availability and scalability deployments.

**Important**

If your FMC is running Version 7.0.0+, we recommend you use the Device Upgrade page to run readiness checks on FTD devices; see [Upgrade Firepower Threat Defense with FMC \(Version 7.0.0\)](#), on page 57. You must still use this procedure to run readiness checks on the FMC and on any Classic devices.

Before you begin

- Upgrade the FMC to at least Version 6.7.0. If your FMC is currently running an older version, see [Run Readiness Checks with FMC \(Version 6.0.1–6.6.x\)](#), on page 24.
- Upload the upgrade package to the FMC, for the appliance you want to check. If you want to check Version 6.6.0+ FTD devices, you can also specify the upgrade package location on an internal web server. This is required because readiness checks are included in upgrade packages.
- (Optional) If you are upgrading an FTD device to Version 6.3.0.1–6.6.x, copy the upgrade package to the device. This can reduce the time required to run the readiness check. If you are upgrading an FTD device to Version 6.7.0+, you can skip this step. Although we still recommend you push the upgrade package to the device before you begin the upgrade itself, you no longer have to do so before you run the readiness check.

Procedure

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

Step 2 Under Available Updates, click the **Install** icon next to the appropriate upgrade package.

The system displays a list of eligible appliances, along with their pre-upgrade compatibility check results. Starting with Version 6.7.0, FTD devices must pass certain basic checks before you can run the more complex readiness check. This pre-check catches issues that *will* cause your upgrade to fail—but we now catch them earlier and block you from proceeding.

Step 3 Select the appliances you want to check and click **Check Readiness**.

If you cannot select an otherwise eligible appliance, make sure it passed its compatibility checks. You may need to upgrade an operating system, or deploy configuration changes.

Step 4 Monitor the progress of the readiness check in the Message Center.

If the check fails, the Message Center provides failure logs.

What to do next

On the **System > Updates** page, click **Readiness Checks** to view readiness check status for your FTD deployment, including checks in progress and failed checks. You can also use this page to easily re-run checks after a failure.

Run Readiness Checks with FMC (Version 6.0.1–6.6.x)

This procedure is valid for FMCs *currently* running Version 6.0.1–6.6.x, and their standalone managed devices.



Note For clustered 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.

Before you begin

- (Version 6.0.1) If you want to run readiness checks on a Version 6.0.1 → 6.1.0 upgrade, first install the Version 6.1 preinstallation package. You must do this for the FMC and managed devices. See the [Firepower System Release Notes Version 6.1.0 Pre-Installation Package](#).
- Upload the upgrade package to the FMC, for the appliance you want to check. If you want to check Version 6.6.x FTD devices, you can also specify the upgrade package location on an internal web server. This is required because readiness checks are included in upgrade packages.
- (Optional, Version 6.2.3+) Push the upgrade package to the managed device. 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.

Procedure

- | | |
|---------------|---|
| Step 1 | On the FMC web interface, choose System > Updates . |
| Step 2 | Click the Install icon next to the appropriate upgrade package. |
| Step 3 | Select the appliances you want to check and click Launch Readiness Check . |
| Step 4 | Monitor the progress of the readiness check in the Message Center. |

Firepower Software Readiness Checks with FDM

Readiness checks assess preparedness for a Firepower Threat Defense software upgrade. If the device fails the readiness check, correct the issues and run the readiness check again. If the readiness check exposes issues that you cannot resolve, we recommend you do not begin the upgrade.

Do not manually reboot or shut down an appliance running readiness checks.

Readiness checks are supported in Firepower Device Manager Version 7.0.0+.

Run Readiness Checks (Version 7.0.0+ with FDM)

Before the system installs an upgrade, it runs a readiness check to ensure the upgrade is valid for the system, and to check other items that sometimes prevent a successful upgrade. If the readiness check fails, you should fix the problems before trying the installation again. If the check has failed, you will be prompted about the failure the next time you try the installation, and you are given the option to force the installation if you want to.

You can also manually run the readiness check prior to initiating the upgrade, as described in this procedure.

Before you begin

Upload the upgrade package you want to check.

Procedure

Step 1 Select **Device**, then click **View Configuration** in the Updates summary.

The **System Upgrade** section shows the currently running software version and any update that you have already uploaded.

Step 2 Look at the **Readiness Check** section.

- If the upgrade check has not been performed yet, click the **Run Upgrade Readiness Check** link. The progress of the check is shown in this area. It should take about 20 seconds to complete the process.
- If the upgrade check has already been run, this section indicates whether the check succeeded or failed. For failed checks, click **See Details** to view more information about the readiness check. After fixing problems, run the check again.

Step 3 If the readiness check fails, you should resolve the issues before you install the upgrade. The detailed information includes help on how to fix indicated problems. For a failed script, click the **Show Recovery Message** link to see the information.

Following are some typical problems:

- **FXOS version incompatibility**—On systems where you install FXOS upgrades separately, such as the Firepower 4100/9300, an upgrade package might require a different minimum FXOS version than the FTD software version you are currently running. In this case, you must first upgrade FXOS before you can upgrade the FTD software.
 - **Unsupported device model**—The upgrade package cannot be installed on this device. You might have uploaded the wrong package, or the device is an older model that is simply no longer supported in the new FTD software version. Please check device compatibility and upload a supported package, if one is available.
 - **Insufficient disk space**—If not enough space is available, try deleting unneeded files, such as system backups. Delete only those files you have created.
-



CHAPTER 2

Upgrade FXOS on the Firepower 4100/9300

Use these procedures to upgrade FXOS for a Firepower 4100/9300 chassis without any configured logical devices.

- [Upgrade FXOS on a Firepower 4100/9300 Chassis Using Firepower Chassis Manager, on page 27](#)
- [Upgrade FXOS on a Firepower 4100/9300 Chassis Using the CLI, on page 29](#)

Upgrade FXOS on a Firepower 4100/9300 Chassis Using Firepower Chassis Manager

This section describes how to use Firepower Chassis Manager to upgrade the FXOS platform bundle for a Firepower 4100/9300 chassis that has not yet been configured with any logical devices.



Note

If you need to upgrade the FXOS platform bundle, the application software, or both for a Firepower 4100/9300 chassis that is configured with FTD or ASA logical devices, see [Upgrade the Firepower 4100/9300 with FTD Logical Devices](#), on page 33 or [Upgrade the Firepower 4100/9300 with ASA Logical Devices](#), on page 63.

Before you begin

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

- Plan your upgrade.
- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS configuration.



Note

The upgrade process typically takes between 20 and 30 minutes.

Procedure

- 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 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 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 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 on a Firepower 4100/9300 Chassis Using the CLI

This section describes how to use the FXOS CLI to upgrade the FXOS platform bundle for a Firepower 4100/9300 chassis that has not yet been configured with any logical devices.

**Note**

If you need to upgrade the FXOS platform bundle, the application software, or both for a Firepower 4100/9300 chassis that is configured with FTD or ASA logical devices, see [Upgrade the Firepower 4100/9300 with FTD Logical Devices](#), on page 33 or [Upgrade the Firepower 4100/9300 with ASA Logical Devices](#), on page 63.

Before you begin

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

- Plan your upgrade.
- Download the FXOS platform bundle software package to which you are upgrading.
- Back up your FXOS configuration.
- 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.

Procedure

- 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:
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:sam:dme: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
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 #
```

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.
-



CHAPTER 3

Upgrade the Firepower 4100/9300 with FTD Logical Devices

Use the procedures in this section to upgrade a Firepower 4100/9300 chassis configured with Firepower Threat Defense logical devices.

Major Firepower versions have a companion FXOS version. You must be running that companion version of FXOS *before* you upgrade logical devices. You upgrade the FXOS platform bundle on each chassis independently, even if you have Firepower inter-chassis clustering or high availability pairs configured.



Note

At this time, this guide does not contain upgrade instructions for Firepower Threat Defense logical devices in Firepower Device Manager/Cloud Defense Orchestrator deployments. Use this guide to upgrade FXOS, then see one of:

- [Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager](#): See the *System Management* chapter in the guide for the FTD version you are currently running, not the version you are upgrading to.
 - [Managing FTD with Cisco Defense Orchestrator](#): See the *Device Upgrade* section.
-
- [Upgrade FXOS on a Firepower 4100/9300 with Firepower Threat Defense Logical Devices](#), on page 33
 - [Upgrade Firepower Threat Defense Logical Devices with Firepower Management Center](#), on page 52

Upgrade FXOS on a Firepower 4100/9300 with Firepower Threat Defense Logical Devices

On the Firepower 4100/9300, you upgrade FXOS on each chassis independently, even if you have Firepower inter-chassis clustering or high availability pairs configured. You can use the FXOS CLI or Firepower Chassis Manager.

Upgrading FXOS reboots the chassis. Depending on your deployment, traffic can either drop or traverse the network without inspection; see [Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300](#), on page 219.

Upgrade FXOS: FTD Standalone Devices and Intra-chassis Clusters

For a standalone Firepower Threat Defense logical device, or for an FTD intra-chassis cluster (units on the same chassis), first upgrade the FXOS platform bundle then upgrade FTD logical devices. Use the Firepower Management Center to upgrade clustered devices as a unit.

Upgrade FXOS for Standalone FTD Logical Devices 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.
- A Firepower 9300 chassis that is configured with one or more standalone FTD logical devices that are not part of a failover pair.

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.
- Back up your FXOS and FTD configurations.

Procedure

-
- Step 1** In Firepower Chassis Manager, choose **System > Updates**.
The Available Updates page shows a list of the FXOS platform bundle images and application images that are available on the chassis.
- Step 2** Upload the new platform bundle image:
- Click **Upload Image** to open the Upload Image dialog box.
 - Click **Choose File** to navigate to and select the image that you want to upload.
 - Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
 - 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 system unpacks the bundle and upgrades/reloads the components.

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
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 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.
- A Firepower 9300 chassis that is configured with one or more standalone FTD devices that are not part of a failover pair.

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.
- 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.

Procedure

-
- Step 1** Connect to the FXOS CLI.
- Step 2** Download the new platform bundle image to the Firepower 4100/9300 chassis:
- Enter firmware mode:
Firepower-chassis-a # **scope firmware**
 - 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**
 - 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:sam:dme: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 system unpacks the bundle and upgrades/reloads the components.
- Step 8** To monitor the upgrade process:
- Enter **scope system**.
 - Enter **show firmware monitor**.
 - 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

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:
- Enter **top**.
 - Enter **scope ssa**.
 - Enter **show slot**.
 - 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.
 - Enter **show app-instance**.
 - Verify that the Oper State is `Online` for any logical devices installed on the chassis.
-

Upgrade FXOS: FTD High Availability Pairs

In Firepower Threat Defense high availability deployments, upgrade the FXOS platform bundle on *both chassis* before you upgrade either FTD logical device. To minimize disruption, always upgrade the standby. In the following scenarios, Device A is the original active device and Device B is the original standby.

Firepower Management Center

In Firepower Management Center deployments, you upgrade the logical devices as a unit:

- Upgrade FXOS on the standby (B).
- Switch roles.
- Upgrade FXOS on the new standby (A).
- Upgrade FTD logical devices (A+B).

Firepower Device Manager

In Firepower Device Manager deployments, you upgrade the logical devices separately:

- Upgrade FXOS on the chassis with the standby FTD logical device (B).
- Switch roles.
- Upgrade FXOS on the chassis with the new standby logical device (A).
Both chassis now have an upgraded FXOS.
- Upgrade the new standby FTD logical device (A).
- Switch roles again.
- Upgrade the original standby FTD logical device (B).

Upgrade FXOS on an 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.
- Back up your FXOS and FTD configurations.

Procedure

-
- 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 FXOS platform bundle images and application images that are available on the chassis.
- Step 3** Upload the new platform bundle image:
- Click **Upload Image** to open the Upload Image dialog box.
 - Click **Choose File** to navigate to and select the image that you want to upload.
 - Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
 - 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 system unpacks the bundle and upgrades/reloads the components.
- Step 6** Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI:
- Enter **scope system**.
 - Enter **show firmware monitor**.
 - 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:
- Enter **top**.
 - Enter **scope ssa**.
 - Enter **show slot**.
 - 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.
 - Enter **show app-instance**.
 - 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:
- Connect to Firepower Management Center.
 - Choose **Devices > Device Management**.
 - Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon ()
 - 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 FXOS platform bundle images and application images that are available on the chassis.
- Step 11** Upload the new platform bundle image:
- Click **Upload Image** to open the Upload Image dialog box.
 - Click **Choose File** to navigate to and select the image that you want to upload.
 - Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
 - 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 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 an 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.
- 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.

Procedure

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:sam:dme: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 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
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 #

```

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:

- Enter **top**.
- Enter **scope ssa**.
- Enter **show slot**.
- 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.
- Enter **show app-instance**.
- 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:

- Connect to Firepower Management Center.
- Choose **Devices > Device Management**.
- Next to the high availability pair where you want to change the active peer, click the Switch Active Peer icon (.
- 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:

- Enter firmware mode:

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

- 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**

- 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: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 system unpacks the bundle and upgrades/reloads the components.

Step 18 To monitor the upgrade process:

- Enter **scope system**.
- Enter **show firmware monitor**.
- 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

FP9300-A /system #

```


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:

- Enter **top**.
- Enter **scope ssa**.
- Enter **show slot**.
- 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.
- Enter **show app-instance**.
- 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:

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

Upgrade FXOS: FTD Inter-chassis Clusters

For Firepower Threat Defense inter-chassis clusters (units on different chassis), upgrade the FXOS platform bundle on *all chassis* before you upgrade the FTD logical devices. To minimize disruption, always upgrade FXOS on an all-data unit chassis. Then, use the Firepower Management Center to upgrade the logical devices as a unit.

For example, for a two-chassis cluster:

- Upgrade FXOS on the all-data unit chassis.
- Switch the control module to the chassis you just upgraded.
- Upgrade FXOS on the new all-data unit chassis.
- Upgrade FTD logical devices.

Upgrade FXOS on an 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.
- Back up your FXOS and FTD configurations.

Procedure

-
- 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 control 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.
- Important** Verify that the control 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 control unit).
- Step 3** In Firepower Chassis Manager, choose **System > Updates**.
The Available Updates page shows a list of the FXOS 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 system unpacks the bundle and upgrades/reloads the components.

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
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
-----
ftd           1      Enabled    Online         6.2.2.81      6.2.2.81
              In Cluster Slave
ftd           2      Enabled    Online         6.2.2.81      6.2.2.81
              In Cluster Slave
ftd           3      Disabled   Not Available  6.2.2.81
              Not Applicable None
FP9300-A /ssa #

```

- Step 8** Set one of the security modules on Chassis #2 as control.
- After setting one of the security modules on Chassis #2 to control, Chassis #1 no longer contains the control unit and can now be upgraded.
- Step 9** Repeat Steps 1-7 for all other Chassis in the cluster.
- Step 10** To return the control role to Chassis #1, set one of the security modules on Chassis #1 as control.

Upgrade FXOS on an 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.
- 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.

Procedure

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

Important Verify that the control 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
```

```
192.168.1.1 (FSM-STAGE:sam:dme:FirmwareDownloaderDownload:Local)
```

- 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 system unpacks the bundle and upgrades/reloads the components.
- Step 9** To monitor the upgrade process:
- Enter **scope system**.
 - Enter **show firmware monitor**.
 - 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.
 - Enter **top**.
 - Enter **scope ssa**.
 - Enter **show slot**.
 - 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.
 - Enter **show app-instance**.
 - 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
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
-----
ftd           1            Enabled    Online          6.2.2.81        6.2.2.81
              In Cluster   Slave
ftd           2            Enabled    Online          6.2.2.81        6.2.2.81
              In Cluster   Slave
ftd           3            Disabled   Not Available   6.2.2.81
              Not Applicable None
FP9300-A /ssa #

```

Step 10 Set one of the security modules on Chassis #2 as control.

After setting one of the security modules on Chassis #2 to control, Chassis #1 no longer contains the control unit and can now be upgraded.

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

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

Upgrade Firepower Threat Defense Logical Devices with Firepower Management Center

In a Firepower Management Center deployment, you upgrade the Firepower Management Center first, then use the newly upgraded FMC to upgrade its managed devices. Refer to your plan. For information on upgrading the FMC itself, as well upgrading managed devices other than the Firepower 4100/9300, see the [Cisco Firepower Management Center Upgrade Guide, Versions 6.0–7.0](#).

Upgrade Checklist: Firepower Threat Defense with FMC

Complete this checklist before you upgrade Firepower Threat Defense.



Note At all times during the process, make sure you maintain deployment communication and health. And, know what to do in case of an unresponsive upgrade. See [General Guidelines, on page 120](#).

Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

Table 15:

✓	Action/Check
	<p>Plan your upgrade path.</p> <p>This is especially important for multi-appliance deployments, multi-hop upgrades, or situations where you need to upgrade operating systems or hosting environments, all while maintaining deployment compatibility. Always know which upgrade you just performed and which you are performing next.</p> <p>Note In Firepower Management Center deployments, you usually upgrade the Firepower Management Center, then its managed devices. However, in some cases you may need to upgrade devices first.</p> <p>See Upgrade Paths , on page 2.</p>
	<p>Read all upgrade guidelines and plan configuration changes.</p> <p>Especially with major upgrades, upgrading may cause or require significant configuration changes either before or after upgrade. Start with the release notes, which contain critical and release-specific information, including upgrade warnings, behavior changes, new and deprecated features, and known issues.</p>
	<p>Check appliance access.</p> <p>Devices can stop passing traffic during the upgrade (depending on interface configurations), or if the upgrade fails. Before you upgrade, make sure traffic from your location does not have to traverse the device itself to access the device's management interface. In FMC deployments, you should also be able to access the FMC management interface without traversing the device.</p>
	<p>Check bandwidth.</p> <p>Make sure your management network has the bandwidth to perform large data transfers. In Firepower Management Center deployments, if you transfer an upgrade package to a managed device at the time of upgrade, insufficient bandwidth can extend upgrade time or even cause the upgrade to time out. Whenever possible, copy upgrade packages to managed devices before you initiate the device upgrade.</p> <p>See Guidelines for Downloading Data from the Firepower Management Center to Managed Devices (Troubleshooting TechNote).</p>

✓	Action/Check
	Schedule maintenance windows. Schedule maintenance windows when they will have the least impact, considering any effect on traffic flow and inspection and the time the upgrade is likely to take. Also consider the tasks you <i>must</i> perform in the window, and those you can perform ahead of time. For example, do not wait until the maintenance window to copy upgrade packages to appliances, run readiness checks, perform backups, and so on.

Upgrade Packages

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

Table 16:

✓	Action/Check
	Upload the upgrade package to the Firepower Management Center or internal web server. In Version 6.6.0+ you can configure an internal web server instead of the Firepower Management Center as the source for FTD upgrade packages. This is useful if you have limited bandwidth between the Firepower Management Center and its devices, and saves space on the Firepower Management Center. See Upload to an Internal Server (Version 6.6.0+ FTD with FMC) , on page 19.
	Copy the upgrade package to the device. When supported, we recommend you copy (<i>push</i>) packages to managed devices before you initiate the device upgrade: <ul style="list-style-type: none"> • Version 6.2.2 and earlier do not support pre-upgrade copy. • Version 6.2.3 allows you to manually copy upgrade packages from the Firepower Management Center. • Version 6.6.0 adds the ability to manually copy upgrade packages from an internal web server. • Version 7.0.0 adds a FTD upgrade workflow that prompts you to copy upgrade packages. <p>Note For the Firepower 4100/9300, we recommend (and sometimes require) you copy the upgrade package before you begin the required companion FXOS upgrade.</p> See Copy to Managed Devices , on page 20.

Backups

The ability to recover from a disaster is an essential part of any system maintenance plan.

Backup and restore can be a complex process. You do not want to skip any steps or ignore security or licensing concerns. For detailed information on requirements, guidelines, limitations, and best practices for backup and restore, see the configuration guide for your deployment.

**Caution**

We *strongly* recommend you back up to a secure remote location and verify transfer success, both before and after upgrade.

Table 17:

✓	Action/Check
	<p>Back up Firepower Threat Defense.</p> <p>Use the Firepower Management Center to back up devices. Not all FTD platforms and configurations support backup. Requires Version 6.3.0+.</p> <p>Back up before and after upgrade:</p> <ul style="list-style-type: none"> • Before upgrade: If an upgrade fails catastrophically, you may have to 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: This creates a snapshot of your freshly upgraded deployment. In Firepower Management Center deployments, we recommend you back up the Firepower Management Center after you upgrade its managed devices, so your new Firepower Management Center backup file 'knows' that its devices have been upgraded.
	<p>Back up FXOS.</p> <p>Use the Firepower Chassis Manager or the FXOS CLI to export chassis configurations before and after upgrade, including logical device and platform configuration settings.</p>

Associated Upgrades

Because operating system and hosting environment upgrades can affect traffic flow and inspection, perform them in a maintenance window.

Table 18:

✓	Action/Check
	<p>Upgrade virtual hosting.</p> <p>If needed, upgrade the hosting environment for any virtual appliances. If this is required, it is usually because you are running an older version of VMware and are performing a major device upgrade.</p>
	<p>Upgrade FXOS.</p> <p>If needed, upgrade FXOS before you upgrade FTD. This is usually a requirement for major upgrades, but very rarely for maintenance releases and patches. To avoid interruptions in traffic flow and inspection, upgrade FXOS in FTD high availability pairs and inter-chassis clusters <i>one chassis at a time</i>.</p> <p>Note Before you upgrade FXOS, make sure you read all upgrade guidelines and plan configuration changes. Start with the FXOS release notes: Cisco Firepower 4100/9300 FXOS Release Notes.</p>

Final Checks

A set of final checks ensures you are ready to upgrade.

Table 19:

✓	Action/Check
	<p>Check configurations.</p> <p>Make sure you have made any required pre-upgrade configuration changes, and are prepared to make required post-upgrade configuration changes.</p>
	<p>Check NTP synchronization.</p> <p>Make sure all appliances are synchronized with any NTP server you are using to serve time. Being out of sync can cause upgrade failure. In Firepower Management Center deployments, the health monitor does alert if clocks are out of sync by more than 10 seconds, but you should still check manually.</p> <p>To check time:</p> <ul style="list-style-type: none"> • Firepower Management Center: Choose System > Configuration > Time. • Devices: Use the show time CLI command.
	<p>Check disk space.</p> <p>Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails.</p> <p>See Time and Disk Space Tests, on page 167.</p>
	<p>Deploy configurations.</p> <p>Deploying configurations before you upgrade reduces the chance of failure. In some deployments, you may be blocked from upgrade if you have out-of-date configurations. In Firepower Management Center high availability deployments, you only need to deploy from the active peer.</p> <p>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.</p> <p>See Traffic Flow and Inspection, on page 219.</p>
	<p>Run readiness checks.</p> <p>If your Firepower Management Center is running Version 6.1.0+, we recommend compatibility and readiness checks. These checks assess your preparedness for a software upgrade. Version 7.0.0 introduces a new FTD upgrade workflow that prompts you to complete these checks.</p> <p>See Firepower Software Readiness Checks with FMC, on page 23.</p>

✓	Action/Check
	Check running tasks. Make sure essential tasks on the device are complete before you upgrade, including the final deploy. Tasks running when the upgrade begins are stopped, become failed tasks, and cannot be resumed. We also recommend you check for tasks that are scheduled to run during the upgrade, and cancel or postpone them.

Upgrade Firepower Threat Defense with FMC (Version 7.0.0)

The FMC provides a wizard to upgrade FTD. You must still use the System Updates page (**System > Updates**) page to upload or specify the location of upgrade packages. You must also use the System Updates page to upgrade the FMC itself, as well as any older Classic devices.

The wizard walks you through important pre-upgrade stages, including selecting devices to upgrade, copying the upgrade package to the devices, and performing compatibility and readiness checks. As you proceed, the wizard displays basic information about your selected devices, as well as the current upgrade-related status. This includes any reasons why you cannot upgrade. If a device does not "pass" a stage in the wizard, it does not appear in the next stage.

If you navigate away from the wizard, your progress is preserved, although other users with Administrator access can reset, modify, or continue the workflow (unless you logged in with a CAC, in which case your progress is cleared 24 hours after you log out). Your progress is also synchronized between high availability FMCs.



Note

In Version 7.0.0/7.0.x, the Device Upgrade page does not correctly display devices in clusters or high availability pairs. Even though you must select and upgrade these devices as a unit, the workflow displays them as standalone devices. Device status and upgrade readiness are evaluated and reported on an individual basis. This means it is possible for one unit to appear to "pass" to the next stage while the other unit or units do not. However, these devices are still grouped. Running a readiness check on one, runs it on all. Starting the upgrade on one, starts it on all.

To avoid possible time-consuming upgrade failures, *manually* ensure all group members are ready to move on to the next step of the workflow before you click **Next**.



Caution

Do not make or deploy configuration changes during upgrade. Even if the system appears inactive, do not manually reboot or shut down. In most cases, do not restart an upgrade in progress. If you encounter issues with the upgrade, including a failed upgrade or unresponsive appliance, see [General Guidelines, on page 120](#).

Before you begin

Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.

Procedure

Select devices to upgrade.

Step 1 Choose **Devices > Device Management**.

Step 2 Select the devices you want to upgrade.

You can upgrade multiple devices at once. You must upgrade the members of device clusters and high availability pairs at the same time.

Important Due to performance issues, if you are upgrading a device *to* (not from) Version 6.4.0.x through 6.6.x, we *strongly* recommend upgrading no more than five devices simultaneously.

Step 3 From the **Select Action** or **Select Bulk Action** menu, select **Upgrade Firepower Software**.

The Device Upgrade page appears, indicating how many devices you selected and prompting you to select a target version. The page has two panes: Device Selection on the left, and Device Details on the right. Click a device link in the Device Selection (such as '4 devices') to show the Device Details for those devices.

Note that if there is already an upgrade workflow in process, you must first either **Merge Devices** (add the newly selected devices to the previously selected devices and continue) or **Reset** (discard the previous selections and use only the newly selected devices).

Step 4 Verify your device selection.

To select additional devices, go back to the Device Management page—your progress will not be lost. To remove devices, click **Reset** to clear your device selection and start over.

Copy upgrade packages to devices.

Step 5 From the **Upgrade to** menu, select your target version.

The system determines which of your selected devices can be upgraded to that version. If any devices are ineligible, you can click the device link to see why. You do not have to remove ineligible devices if you don't want to; they will just not be included in the next step.

Note that the choices in the **Upgrade to** menu correspond to the device upgrade packages available to the system. If your target version is not listed, go to **System > Updates** and upload or specify the location of the correct upgrade package.

Step 6 For all devices that still need an upgrade package, click **Copy Upgrade Packages**, then confirm your choice.

To upgrade FTD, the software upgrade package must be on the appliance. Copying the upgrade package before upgrade reduces the length of your upgrade maintenance window.

Perform compatibility, readiness, and other final checks.

Step 7 For all devices that need to pass the readiness check, click **Run Readiness Check**, then confirm your choice.

Although you can skip checks by disabling the **Require passing compatibility and readiness checks option**, we recommend against it. Passing all checks greatly reduces the chance of upgrade failure. Do *not* deploy changes to, manually reboot, or shut down a device while running readiness checks. If a device 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.

Note that compatibility checks are automatic. For example, the system alerts you immediately if you need to upgrade FXOS on the Firepower 4100/9300, or if you need to deploy to managed devices.

Step 8 Perform final pre-upgrade checks.

Revisit the pre-upgrade checklist. Make sure you have completed all relevant tasks, especially the final checks.

Step 9 If necessary, return to the Device Upgrade page.

Your progress should have been preserved. If it was not, someone else with Administrator access may have reset, modified, or completed the workflow.

Step 10 Click **Next**.

Upgrade.

Step 11 Verify your device selection and target version.

Step 12 Choose rollback options.

For major and maintenance upgrades, you can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

This option is not supported for patches.

Step 13 Click **Start Upgrade**, then confirm that you want to upgrade and reboot the devices.

You can monitor upgrade progress in the Message Center. For information on traffic handling during the upgrade, see [Traffic Flow and Inspection, on page 219](#).

Devices may reboot twice during the upgrade. This is expected behavior.

Verify success and complete post-upgrade tasks.

Step 14 Verify upgrade success.

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

Step 15 (Optional) In high availability/scalability deployments, examine device roles.

The upgrade process switches device roles so that it is always upgrading a standby device or data unit. It does not return devices to the roles they had before upgrade. If you have preferred roles for specific devices, make those changes now.

Step 16 Update intrusion rules (SRU/LSP) and the vulnerability database (VDB).

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. Note that when you update intrusion rules, you do not need to automatically reapply policies. You will do that later.

Step 17 Complete any post-upgrade configuration changes described in the release notes.

Step 18 Redeploy configurations to the devices you just upgraded.

What to do next

(Optional) Clear the wizard by returning to the Device Upgrade page and clicking **Finish**. Until you do this, the Device Upgrade page continues to display details about the upgrade you just performed.

Upgrade Firepower Threat Defense with FMC (Version 6.0.1–6.7.0)

Use this procedure to upgrade Firepower Threat Defense using the Firepower Management Center's System Updates page. On this page, you can upgrade multiple devices at once only if they use the same upgrade package. You must upgrade the members of device clusters and high availability pairs at the same time.

Before you begin

- Decide whether you want to use this procedure. For Firepower Threat Defense upgrades to Version 7.0.0+ we recommend you use the upgrade wizard instead; see [Upgrade Firepower Threat Defense with FMC \(Version 7.0.0\)](#), on page 57.
- Complete the pre-upgrade checklist. Make sure the appliances in your deployment are healthy and successfully communicating.
- (Optional) Switch the active/standby roles of your high availability device pairs. Choose **Devices > Device Management**, click the **Switch Active Peer** icon next to the pair, and confirm your choice.

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.

Procedure

Step 1 Choose **System > Updates**.

Step 2 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 from the System Update page. You cannot 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 3 (Version 6.7.0+) Choose rollback options.

For major and maintenance upgrades, you can **Automatically cancel on upgrade failure and roll back to the previous version**. With this option enabled, the device automatically returns to its pre-upgrade state upon upgrade failure. Disable this option if you want to be able to manually cancel or retry a failed upgrade. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted. Auto-cancel is not supported for patches.

Step 4 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 [Traffic Flow and Inspection](#), on page 219.

Step 5 Monitor upgrade progress.

Caution Do *not* deploy changes to, manually reboot, or shut down an upgrading device. In most cases, 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, there may be something you can do — see the [General Guidelines, on page 120](#).

Step 6 Verify upgrade success.

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

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

If the component available on the Cisco Support & Download site is newer than the version currently running, install the newer version. 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 to the devices you just upgraded.



CHAPTER 4

Upgrade the Firepower 4100/9300 with ASA Logical Devices

Use the procedures in this section to upgrade the FXOS platform bundle on Firepower 4100/9300 Series security appliances and the ASA software on any logical devices installed on those appliances.

- [Checklist: Upgrade Firepower 4100/9300 with ASA, on page 63](#)
- [Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster, on page 64](#)
- [Upgrade FXOS and an ASA Active/Standby Failover Pair, on page 69](#)
- [Upgrade FXOS and an ASA Active/Active Failover Pair, on page 79](#)
- [Upgrade FXOS and an ASA Inter-chassis Cluster, on page 90](#)

Checklist: Upgrade Firepower 4100/9300 with ASA

To plan your upgrade, use this checklist.

1. Current FXOS version ([Current Version and Model Information, on page 2](#)): _____
Current ASA version: _____
2. Check ASA/Firepower 4100 and 9300 compatibility ([Firepower 4100/9300 Compatibility with ASA and FTD, on page 108](#)).
Target FXOS version: _____
Target ASA version: _____
3. Check the upgrade path for FXOS ([Upgrade Path: FXOS , on page 4](#)). Are there intermediate versions required? Yes _____ No _____
If yes, intermediate FXOS versions: _____
Make sure you plan to upgrade the ASA in step with the FXOS upgrades to stay compatible.
Intermediate ASA versions required to stay compatible during the upgrade:

4. Download the target and intermediate FXOS versions ([FXOS Packages, on page 17](#)).
5. Download the target and intermediate ASA versions ([ASA Packages, on page 17](#)).



Note ASDM is included in the ASA for FXOS package.

6. Do you use the Radware DefensePro decorator application? Yes ____ No ____
If yes:
 - a. Current DefensePro version: _____
 - b. Check ASA/FXOS/DefensePro compatibility ([Radware DefensePro Compatibility, on page 115](#)).
Target DefensePro version: _____
 - c. Download the target DefensePro version.
7. Check upgrade guidelines for each operating system.
 - FXOS guidelines: see the [FXOS Release Notes](#) for each intermediate and target version.
 - [ASA Upgrade Guidelines, on page 153](#).
8. Back up your configurations. See the configuration guide for each operating system for backup methods.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and a standalone ASA device or an ASA intra-chassis cluster on a Firepower 9300.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using Firepower Chassis Manager

The upgrade process can take up to 45 minutes. Traffic will not traverse through the device while it is upgrading. Please plan your upgrade activity accordingly.

Before you begin

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

- Download the FXOS and ASA software packages to which you are upgrading: [Download Upgrade Packages, on page 15](#).
- Back up your FXOS and ASA configurations.

Procedure

Step 1

In Firepower Chassis Manager, choose **System > Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.

Step 2 Upload the new FXOS platform bundle image and ASA software image::

Note If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.

- a) Click **Upload Image**.
 - 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 chassis.

Step 3 After the new FXOS platform bundle image has successfully uploaded, click the **Upgrade** icon 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Step 4 Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

Step 5 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see [Monitor the Upgrade Progress, on page 99](#)).

Step 6 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).

Step 7 Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.

Step 8 For each ASA logical device that you want to upgrade:

- a) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
- b) For the **New Version**, choose the software version to which you want to upgrade.
- c) Click **OK**.

Step 9 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

- a) Choose **Logical Devices**.
- b) Verify the application version and operational status.

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using the FXOS CLI

The upgrade process can take up to 45 minutes. Traffic will not traverse through the device while it is upgrading. Please plan your upgrade activity accordingly.

Before you begin

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

- Download the FXOS and ASA software packages to which you are upgrading: [Download Upgrade Packages, on page 15](#).
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
 - IP address and authentication credentials for the server from which you are copying the images.
 - Fully qualified names of the image files.

Procedure

Step 1 Connect to the FXOS CLI.

Step 2 Download the new FXOS platform bundle image to the chassis:

a) Enter firmware mode:

scope firmware

b) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp://username@server/path/image_name**
- **scp://username@server/path/image_name**
- **sftp://username@server/path/image_name**
- **tftp://server:port-num/path/image_name**

c) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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** After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:
- If necessary, return to firmware mode:
up
 - Make note of the version number for the FXOS platform bundle you are installing:
show package
 - Enter auto-install mode:
scope auto-install
 - Install the FXOS platform bundle:
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).

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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

Enter **yes** to confirm that you want to proceed with verification.
 - Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.
 - To monitor the upgrade process, see [Monitor the Upgrade Progress, on page 99](#).
- Step 4** After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).
- Step 5** Download the new ASA software image to the chassis:
- Enter Security Services mode:
top
scope ssa
 - Enter Application Software mode:
scope app-software
 - Download the logical device software image:
download image *URL*

Specify the URL for the file being imported using one of the following syntax:
 - **ftp://username@server/path**
 - **scp://username@server/path**
 - **sftp://username@server/path**
 - **tftp://server:port-num/path**

- d) To monitor the download process:

show download-task

- e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:

File Name	Protocol	Server	Userid	State
cisco-asa.9.4.1.65.csp	Scp	192.168.1.1	user	Downloaded

```
Firepower-chassis /ssa/app-software # up
```

```
Firepower-chassis /ssa # show app
```

Application:

Name	Version	Description	Author	Deploy Type	CSP Type	Is Default	App
asa	9.4.1.41	N/A		Native	Application	No	
asa	9.4.1.65	N/A		Native	Application	Yes	

Step 6 For each ASA logical device that you want to upgrade:

- a) Enter Security Services mode:

top

scope ssa

- b) Set the scope to the security module you are updating:

scope slotslot_number

- c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa instance_name**

- d) Set the Startup version to the new ASA software version:

set startup-version version_number

Step 7 Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

- Step 8** To verify the status of the security modules/security engine and any installed applications, see [Verify the Installation, on page 100](#).
-

Upgrade FXOS and an ASA Active/Standby Failover Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and an ASA Active/Standby failover pair.

Upgrade FXOS and an ASA Active/Standby Failover Pair Using Firepower Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

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

- You need to determine which unit is active and which is standby: connect ASDM to the active ASA IP address. The active unit always owns the active IP address. Then choose **Monitoring > Properties > Failover > Status** to view this unit's priority (primary or secondary) so you know which unit you are connected to.
- Download the FXOS and ASA software packages to which you are upgrading: [Download Upgrade Packages, on page 15](#).
- Back up your FXOS and ASA configurations.

Procedure

- Step 1** On the Firepower security appliance that contains the *standby* ASA logical device, upload the new FXOS platform bundle image and ASA software image:
- Note** If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.
- a) In Firepower Chassis Manager, choose **System > Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
 - b) Click **Upload Image**.
 - c) Click **Choose File** to navigate to and select the image that you want to upload.
 - d) Click **Upload**.
The selected image is uploaded to the chassis.
- Step 2** After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the Firepower security appliance that contains the *standby* ASA logical device:

- a) Click the **Upgrade** icon 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.
- b) Click **Yes** to confirm that you want to proceed with installation.
FXOS unpacks the bundle and upgrades/reloads the components.

Step 3 Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see [Monitor the Upgrade Progress, on page 99](#)).

Step 4 After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).

Step 5 Upgrade the ASA logical device image:

- a) Choose **Logical Devices** to open the Logical Devices page.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
- b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
- c) For the **New Version**, choose the software version to which you want to update.
- d) Click **OK**.

Step 6 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

- a) Choose **Logical Devices**.
- b) Verify the application version and operational status.

Step 7 Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

- a) Launch ASDM on the *standby* unit by connecting to the standby ASA IP address.
- b) Force the standby unit to become active by choosing **Monitoring > Properties > Failover > Status**, and clicking **Make Active**.

Step 8 On the Firepower security appliance that contains the *new standby* ASA logical device, upload the new FXOS platform bundle image and ASA software image:

Note If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.

- a) In Firepower Chassis Manager, choose **System > Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
- b) Click **Upload Image**.
- c) Click **Choose File** to navigate to and select the image that you want to upload.
- d) Click **Upload**.
The selected image is uploaded to the chassis.

Step 9 After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the Firepower security appliance that contains the *new standby* ASA logical device:

- a) Click the **Upgrade** icon 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

- b) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

- Step 10** Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see [Monitor the Upgrade Progress, on page 99](#)).
- Step 11** After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).
- Step 12** Upgrade the ASA logical device image:
- a) Choose **Logical Devices**.
The **Logical Devices** page opens to shows a list of configured logical devices on the chassis. If no logical devices have been configured, a message stating so is shown instead.
 - b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
 - c) For the **New Version**, choose the software version to which you want to update.
 - d) Click **OK**.
- Step 13** After the upgrade process finishes, verify that the applications are online and have upgraded successfully:
- a) Choose **Logical Devices**.
 - b) Verify the application version and operational status.
- Step 14** (Optional) Make the unit that you just upgraded the *active* unit as it was before the upgrade:
- a) Launch ASDM on the *standby* unit by connecting to the standby ASA IP address.
 - b) Force the standby unit to become active by choosing **Monitoring > Properties > Failover > Status**, and clicking **Make Active**.

Upgrade FXOS and an ASA Active/Standby Failover Pair Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

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

- You need to determine which unit is active and which is standby: connect to the ASA console on the Firepower security appliance and enter the **show failover** command to view the Active/Standby status of the unit.
- Download the FXOS and ASA software packages to which you are upgrading: [Download Upgrade Packages, on page 15](#).
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
 - IP address and authentication credentials for the server from which you are copying the image.
 - Fully qualified name of the image file.

Procedure

Step 1

On the Firepower security appliance that contains the *standby* ASA logical device, download the new FXOS platform bundle image:

- a) Connect to the FXOS CLI.
- b) Enter firmware mode:

scope firmware

- c) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp://username@server/path/image_name**
- **scp://username@server/path/image_name**
- **sftp://username@server/path/image_name**
- **tftp://server:port-num/path/image_name**

- d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 2

After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

- a) If necessary, return to firmware mode:

up

- b) Make note of the version number for the FXOS platform bundle you are installing:

show package

- c) Enter auto-install mode:

scope auto-install

- d) Install the FXOS platform bundle:

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).

- e) 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

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

- f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

- g) To monitor the upgrade process, see [Monitor the Upgrade Progress, on page 99](#).

Step 3

After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).

Step 4

Download the new ASA software image to the chassis:

- a) Enter Security Services mode:

top

scope ssa

- b) Enter Application Software mode:

scope app-software

- c) Download the logical device software image:

download image *URL*

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

- **ftp**://*username@server/path*
- **scp**://*username@server/path*
- **sftp**://*username@server/path*
- **tftp**://*server:port-num/path*

- d) To monitor the download process:

show download-task

- e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:

File Name	Protocol	Server	Userid	State
cisco-asa.9.4.1.65.csp	Scp	192.168.1.1	user	Downloaded

```
Firepower-chassis /ssa/app-software # up
```

```
Firepower-chassis /ssa # show app
```

Application:

Name	Version	Description	Author	Deploy Type	CSP Type	Is Default App
asa	9.4.1.41	N/A		Native	Application	No
asa	9.4.1.65	N/A		Native	Application	Yes

Step 5

Upgrade the ASA logical device image:

- a) Enter Security Services mode:

```
top
```

```
scope ssa
```

- b) Set the scope to the security module you are updating:

```
scope slotslot_number
```

- c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa instance_name**

- d) Set the Startup version to the version you want to update:

```
set startup-version version_number
```

- e) Commit the configuration:

```
commit-buffer
```

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 6

To verify the status of the security modules/security engine and any installed applications, see [Verify the Installation, on page 100](#).

Step 7

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

- a) On the Firepower security appliance that contains the standby ASA logical device, connect to the module CLI using a console connection or a Telnet connection.

```
connect module slot_number { console | telnet }
```

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

- b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

- c) Make this unit active:

failover active

- d) Save the configuration:

write memory

- e) Verify that the unit is active:

show failover

Step 8 Exit the application console to the FXOS module CLI.
Enter **Ctrl-a, d**

Step 9 Return to the supervisor level of the FXOS CLI.

Exit the console:

- a) Enter ~

You exit to the Telnet application.

- b) To exit the Telnet application, enter:

```
telnet>quit
```

Exit the Telnet session:

- a) Enter **Ctrl-], .**

Step 10 On the Firepower security appliance that contains the *new standby* ASA logical device, download the new FXOS platform bundle image:

- a) Connect to the FXOS CLI.
- b) Enter firmware mode:

scope firmware

- c) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp://username@server/path/image_name**
- **scp://username@server/path/image_name**
- **sftp://username@server/path/image_name**
- **tftp://server:port-num/path/image_name**

- d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 11

After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

- a) If necessary, return to firmware mode:

up

- b) Make note of the version number for the FXOS platform bundle you are installing:

show package

- c) Enter auto-install mode:

scope auto-install

- d) Install the FXOS platform bundle:

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).

- e) 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

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

- f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

- g) To monitor the upgrade process, see [Monitor the Upgrade Progress, on page 99](#).

Step 12

After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).

Step 13

Download the new ASA software image to the chassis:

- a) Enter Security Services mode:

top

scope ssa

- b) Enter Application Software mode:

scope app-software

- c) Download the logical device software image:

download image *URL*

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

- **ftp://username@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) To monitor the download process:

show download-task

- e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```

Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task

Downloads for Application Software:
  File Name                Protocol  Server          Userid          State
  -----
  cisco-asa.9.4.1.65.csp   Scp      192.168.1.1     user            Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
  Name      Version    Description  Author      Deploy Type  CSP Type      Is Default App
  -----
  asa       9.4.1.41   N/A          N/A         Native       Application   No
  asa       9.4.1.65   N/A          N/A         Native       Application   Yes

```

Step 14 Upgrade the ASA logical device image:

- a) Enter Security Services mode:

top**scope ssa**

- b) Set the scope to the security module you are updating:

scope slotslot_number

- c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**For FXOS 2.4.1 and later: **scope app-instance asa instance_name**

- d) Set the Startup version to the version you want to update:

set startup-version version_number

- e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 15 To verify the status of the security modules/security engine and any installed applications, see [Verify the Installation, on page 100](#).

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

- a) On the Firepower security appliance that contains the standby ASA logical device, connect to the module CLI using a console connection or a Telnet connection.

connect module slot_number { console | telnet }

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:


```

Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>

```

- b) Connect to the application console.

connect asa

Example:

```

Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>

```

- c) Make this unit active:

failover active

- d) Save the configuration:

write memory

- e) Verify that the unit is active:

show failover

Upgrade FXOS and an ASA Active/Active Failover Pair

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and an ASA Active/Active failover pair.

Upgrade FXOS and an ASA Active/Active Failover Pair Using Firepower Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

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

- You need to determine which unit is the primary unit: connect ASDM and then choose **Monitoring > Properties > Failover > Status** to view this unit's priority (primary or secondary) so you know which unit you are connected to.
- Download the FXOS and ASA software packages to which you are upgrading.

- Back up your FXOS and ASA configurations.

Procedure

-
- Step 1** Make both failover groups active on the *primary* unit.
- Launch ASDM on the *primary* unit (or the unit with failover group 1 active) by connecting to the management address in failover group 1.
 - Choose **Monitoring > Failover > Failover Group 2**, and click **Make Active**.
 - Stay connected to ASDM on this unit for later steps.
- Step 2** On the Firepower security appliance that contains the *secondary* ASA logical device, upload the new FXOS platform bundle image and ASA software image:
- Note** If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.
- Connect to the Firepower Chassis Manager on the *secondary* unit.
 - Choose **System > Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
 - Click **Upload Image**.
 - Click **Choose File** to navigate to and select the image that you want to upload.
 - Click **Upload**.
The selected image is uploaded to the chassis.
- Step 3** After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the Firepower security appliance that contains the *secondary* ASA logical device:
- Click the **Upgrade** icon 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.
 - Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.
- Step 4** Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see [Monitor the Upgrade Progress, on page 99](#)).
- Step 5** After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).
- Step 6** Upgrade the ASA logical device image:
- Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
 - Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
 - For the **New Version**, choose the software version to which you want to update.
 - Click **OK**.

- Step 7** After the upgrade process finishes, verify that the applications are online and have upgraded successfully:
- Choose **Logical Devices**.
 - Verify the application version and operational status.
- Step 8** Make both failover groups active on the *secondary* unit.
- Launch ASDM on the *primary* unit (or the unit with failover group 1 active) by connecting to the management address in failover group 1.
 - Choose **Monitoring > Failover > Failover Group 1**, and click **Make Standby**.
 - Choose **Monitoring > Failover > Failover Group 2**, and click **Make Standby**.
- ASDM will automatically reconnect to the failover group 1 IP address on the secondary unit.
- Step 9** On the Firepower security appliance that contains the *primary* ASA logical device, upload the new FXOS platform bundle image and ASA software image:
- Note** If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.
- Connect to the Firepower Chassis Manager on the *primary* unit.
 - Choose **System > Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
 - Click **Upload Image** to open the Upload Image dialog box.
 - Click **Choose File** to navigate to and select the image that you want to upload.
 - Click **Upload**.
The selected package is uploaded to the chassis.
 - 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 10** After the new FXOS platform bundle image has successfully uploaded, upgrade the FXOS bundle on the Firepower security appliance that contains the *primary* ASA logical device:
- Click the **Upgrade** icon 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.
 - Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.
- Step 11** Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see [Monitor the Upgrade Progress, on page 99](#)).
- Step 12** After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).
- Step 13** Upgrade the ASA logical device image:
- Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
 - Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
 - For the **New Version**, choose the software version to which you want to update.

d) Click **OK**.

Step 14 After the upgrade process finishes, verify that the applications are online and have upgraded successfully:

- a) Choose **Logical Devices**.
- b) Verify the application version and operational status.

Step 15 If the failover groups are configured with Preempt Enabled, they automatically become active on their designated unit after the preempt delay has passed. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the ASDM **Monitoring > Failover > Failover Group #** pane.

Upgrade FXOS and an ASA Active/Active Failover Pair Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

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

- You need to determine which unit is primary: connect to the ASA console on the Firepower security appliance and enter the **show failover** command to view the unit's status and priority (primary or secondary).
- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
 - IP address and authentication credentials for the server from which you are copying the image.
 - Fully qualified name of the image file.

Procedure

Step 1 Connect to the FXOS CLI on the *secondary* unit, either the console port (preferred) or using SSH.

Step 2 Make both failover groups active on the primary unit.

- a) Connect to the module CLI using a console connection or a Telnet connection.

connect module *slot_number* { **console** | **telnet** }

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```

```
CISCO Serial Over LAN:
```

```
Close Network Connection to Exit  
Firepower-module1>
```

- b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa  
Connecting to asa(asa1) console... hit Ctrl + A + D to return to bootCLI  
[...]  
asa>
```

- c) Make both failover groups active on the primary unit.

enable

The enable password is blank by default.

no failover active group 1

no failover active group 2

Example:

```
asa> enable  
Password: <blank>  
asa# no failover active group 1  
asa# no failover active group 2
```

Step 3 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 4 Return to the supervisor level of the FXOS CLI.

Exit the console:

- a) Enter ~

You exit to the Telnet application.

- b) To exit the Telnet application, enter:

```
telnet>quit
```

Exit the Telnet session:

- a) Enter **Ctrl-], .**

Step 5 On the Firepower security appliance that contains the *secondary* ASA logical device, download the new FXOS platform bundle image and ASA software image:

- a) Connect to the FXOS CLI.

- b) Enter firmware mode:

scope firmware

- c) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp://username@server/path/image_name**
- **scp://username@server/path/image_name**
- **sftp://username@server/path/image_name**
- **tftp://server:port-num/path/image_name**

- d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 6

After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

- a) If necessary, return to firmware mode:

top

scope firmware

- b) Make note of the version number for the FXOS platform bundle you are installing:

show package

- c) Enter auto-install mode:

scope auto-install

- d) Install the FXOS platform bundle:

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).

- e) 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

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

- f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.
FXOS unpacks the bundle and upgrades/reloads the components.
- g) To monitor the upgrade process, see [Monitor the Upgrade Progress, on page 99](#).

Step 7

After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).

Step 8

Download the new ASA software image to the chassis:

- a) Enter Security Services mode:

top

scope ssa

- b) Enter Application Software mode:

scope app-software

- c) Download the logical device software image:

download image *URL*

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

- **ftp://username@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) To monitor the download process:

show download-task

- e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

```
Downloads for Application Software:
File Name          Protocol  Server          Userid          State
-----
cisco-asa.9.4.1.65.csp  Scp      192.168.1.1     user           Downloaded
```

```
Firepower-chassis /ssa/app-software # up
```

```
Firepower-chassis /ssa # show app
```

```
Application:
```

Name	Version	Description	Author	Deploy Type	CSP Type	Is Default	App
asa	9.4.1.41	N/A		Native	Application	No	
asa	9.4.1.65	N/A		Native	Application	Yes	

Step 9

Upgrade the ASA logical device image:

- a) Enter Security Services mode:

```
top
```

```
scope ssa
```

- b) Set the scope to the security module you are updating:

```
scope slotslot_number
```

- c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa instance_name**

- d) Set the Startup version to the version you want to update:

```
set startup-version version_number
```

- e) Commit the configuration:

```
commit-buffer
```

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 10

To verify the status of the security modules/security engine and any installed applications, see [Verify the Installation, on page 100](#).

Step 11

Make both failover groups active on the *secondary* unit.

- a) Connect to the module CLI using a console connection or a Telnet connection.

```
connect module slot_number {console | telnet}
```

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.
```



```
CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

- b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

- c) Make both failover groups active on the *secondary* unit.

enable

The enable password is blank by default.

failover active group 1

failover active group 2

Example:

```
asa> enable
Password: <blank>
asa# failover active group 1
asa# failover active group 2
```

Step 12 Exit the application console to the FXOS module CLI.

Enter **Ctrl-a, d**

Step 13 Return to the supervisor level of the FXOS CLI.

Exit the console:

- a) Enter ~

You exit to the Telnet application.

- b) To exit the Telnet application, enter:

telnet>**quit**

Exit the Telnet session:

- a) Enter **Ctrl-], .**

Step 14 On the Firepower security appliance that contains the *primary* ASA logical device, download the new FXOS platform bundle image and ASA software image:

- a) Connect to the FXOS CLI.

- b) Enter firmware mode:

scope firmware

- c) Download the FXOS platform bundle software image:

download image *URL*

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

- **ftp://username@server/path/image_name**
- **scp://username@server/path/image_name**
- **sftp://username@server/path/image_name**
- **tftp://server:port-num/path/image_name**

- d) To monitor the download process:

scope download-task *image_name*

show detail

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 15

After the new FXOS platform bundle image has successfully downloaded, upgrade the FXOS bundle:

- a) If necessary, return to firmware mode:

up

- b) Make note of the version number for the FXOS platform bundle you are installing:

show package

- c) Enter auto-install mode:

scope auto-install

- d) Install the FXOS platform bundle:

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).

- e) 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

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

- f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

- g) To monitor the upgrade process, see [Monitor the Upgrade Progress, on page 99](#).

Step 16

After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).

Step 17

Download the new ASA software image to the chassis:

- a) Enter Security Services mode:

top

scope ssa

- b) Enter Application Software mode:

scope app-software

- c) Download the logical device software image:

download image *URL*

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

- **ftp://username@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) To monitor the download process:

show download-task

- e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:

```

File Name          Protocol  Server          Userid          State
-----
cisco-asa.9.4.1.65.csp  Scp      192.168.1.1     user           Downloaded

Firepower-chassis /ssa/app-software # up

Firepower-chassis /ssa # show app

Application:
  Name      Version      Description Author      Deploy Type CSP Type      Is Default App
-----
asa        9.4.1.41     N/A                               Native      Application No
asa        9.4.1.65     N/A                               Native      Application Yes

```

Step 18 Upgrade the ASA logical device image:

- a) Enter Security Services mode:

top**scope ssa**

- b) Set the scope to the security module you are updating:

scope slot*slot_number*

- c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**For FXOS 2.4.1 and later: **scope app-instance asa** *instance_name*

- d) Set the Startup version to the version you want to update:

set startup-version *version_number*

- e) Commit the configuration:

commit-buffer

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 19 To verify the status of the security modules/security engine and any installed applications, see [Verify the Installation, on page 100](#).

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. If the failover groups are not configured with Preempt Enabled, you can return them to active status on their designated units using the ASDM **Monitoring > Failover > Failover Group #** pane.

Upgrade FXOS and an ASA Inter-chassis Cluster

Use the FXOS CLI or Firepower Chassis Manager to upgrade FXOS and ASA on all chassis in an inter-chassis cluster.

Upgrade FXOS and an ASA Inter-chassis Cluster Using Firepower Chassis Manager

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

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

- Download the FXOS and ASA software packages to which you are upgrading.
- Back up your FXOS and ASA configurations.

Procedure

-
- Step 1** Determine which chassis has the control unit. You will upgrade this chassis last:
- a) Connect to Firepower Chassis Manager.
 - b) Choose **Logical Devices**.
 - c) Click the plus sign (+) to see the attributes for the security modules included in the cluster.
 - d) Verify that the control unit is on this chassis. There should be an ASA instance with **CLUSTER-ROLE** set to "Master".
- Step 2** Connect to Firepower Chassis Manager on a chassis in the cluster that does not have the control unit.
- Step 3** Upload the new FXOS platform bundle image and ASA software image:
- Note** If you are upgrading to a version earlier than FXOS 2.3.1, do not upload the ASA CSP image to your security appliance until after you upgrade the FXOS platform bundle software.
- a) In Firepower Chassis Manager, choose **System > Updates**.
The **Available Updates** area shows a list of the packages available on the chassis.
 - b) Click **Upload Image**.
 - c) Click **Choose File** to navigate to and select the image that you want to upload.
 - d) Click **Upload**.
The selected image is uploaded to the chassis.
 - e) Wait for the images to successfully upload before continuing.
- Step 4** (FXOS 2.4.1 or earlier) Disable each app-instance for all security modules on the chassis:
Note - if you are upgrading from FXOS version 2.6.1 or later, you can skip this step.
- a) Choose **Logical Devices**.
 - b) Click the **Disable** slider for each application to disable each app-instance included in the cluster.
The **Cluster Operational Status** changes to not-in-cluster.
- Step 5** Upgrade the FXOS bundle:
- a) Choose **System > Updates**.
 - b) Click the **Upgrade** icon 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

- c) Click **Yes** to confirm that you want to proceed with installation.

FXOS unpacks the bundle and upgrades/reloads the components.

- Step 6** Firepower Chassis Manager will be unavailable during upgrade. You can monitor the upgrade process using the FXOS CLI (see [Monitor the Upgrade Progress, on page 99](#)).
- Step 7** After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).
- Step 8** Upgrade the ASA logical device image on each security module:
- a) Choose **Logical Devices**.
The **Logical Devices** page opens to show a list of configured logical devices on the chassis.
 - b) Click the **Set Version** icon for the logical device that you want to update to open the **Update Image Version** dialog box.
 - c) For the **New Version**, choose the software version to which you want to update.
 - d) Click **OK**.
- Step 9** After the upgrade process finishes, verify that the applications are online and have upgraded successfully:
- a) Choose **Logical Devices**.
 - b) Verify the application version and operational status.
- Step 10** (FXOS 2.4.1 or earlier) Re-enable clustering for all security modules on the chassis:
- Note - if you are upgrading from FXOS version 2.6.1 or later, you can skip this step.
- a) Choose **Logical Devices**.
 - b) Click the **Enable** switch for each security module included in the cluster.
The **Cluster Operational Status** changes to in-cluster.
- Step 11** Repeat steps 2-10 for all remaining chassis in the cluster that do not have the control unit.
- Step 12** After all chassis in the cluster that do not have the control unit have been upgraded, repeat steps 2-10 on the chassis with the control unit, being sure to disable clustering on the data units first, and then finally the control unit.
A new control unit will be chosen from one of the previously upgraded chassis.
- Step 13** For distributed VPN clustering mode, after the cluster has stabilized you can redistribute active sessions among all modules in the cluster using the ASA console on the control unit.

cluster redistribute vpn-sessiondb

What to do next

Set the chassis Site ID. For more information about how to set the chassis Site ID, see the Inter-Site Clustering topic in Deploying a Cluster for ASA on the Firepower 4100/9300 for Scalability and High Availability on Cisco.com.

Upgrade FXOS and an ASA Inter-chassis Cluster Using the FXOS CLI

The upgrade process can take up to 45 minutes per chassis. Please plan your upgrade activity accordingly.

Before you begin

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

- Download the FXOS and ASA software packages to which you are upgrading: [Download Upgrade Packages, on page 15](#).
- Back up your FXOS and ASA configurations.
- Collect the following information that you will need to download software images to the chassis:
 - IP address and authentication credentials for the server from which you are copying the image.
 - Fully qualified name of the image file.

Procedure

- Step 1** Determine which chassis has the control unit. You will upgrade this chassis last:
- a) Connect to the FXOS CLI.
 - b) Verify that the control unit is on this chassis. There should be an ASA instance with Cluster Role set to “Master”:

scope ssa
show app-instance
- Step 2** Connect to the FXOS CLI on a chassis in the cluster that does not have the control unit.
- Step 3** Disable each app-instance for all security modules on the chassis. For each of the ASA application(s) on the chassis, perform the following steps:
- a) Scope to the ASA application instance on a given slot:

scope slot *slot_number*
scope app-instance asa

Note To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.
 - b) Disable the ASA application:

disable
 - c) Commit the configuration:

commit-buffer
- Step 4** Download the new FXOS platform bundle image to the chassis:
- a) Enter firmware mode:

scope firmware
 - b) Download the FXOS platform bundle software image:

download image *URL*

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

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

c) To monitor the download process:

```
scope download-task image_name
show detail
```

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope firmware
Firepower-chassis /firmware # download image
scp://user@192.168.1.1/images/fxos-k9.2.3.1.58.SPA
Firepower-chassis /firmware # scope download-task fxos-k9.2.3.1.58.SPA
Firepower-chassis /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 5 Return to the supervisor level of the FXOS CLI.

Exit the console:

- a) Enter `~`
You exit to the Telnet application.
- b) To exit the Telnet application, enter:
`telnet>quit`

Exit the Telnet session:

- a) Enter `Ctrl-], .`

Step 6 Upgrade the FXOS bundle:

- a) If necessary, return to firmware mode:
`top`
`scope firmware`
- b) Make note of the version number for the FXOS platform bundle you are installing:
`show package`
- c) Enter auto-install mode:

scope auto-install

- d) Install the FXOS platform bundle:

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).

- e) 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. As long as the ASA version is listed as upgradeable in the compatibility table, you can ignore these warnings.

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

- f) Enter **yes** to confirm that you want to proceed with installation, or enter **no** to cancel the installation.

FXOS unpacks the bundle and upgrades/reloads the components.

- g) To monitor the upgrade process, see [Monitor the Upgrade Progress, on page 99](#).

Step 7

After all components have successfully upgraded, verify the status of the security modules/security engine and any installed applications before continuing (see [Verify the Installation, on page 100](#)).

Step 8

Download the new ASA software image to the chassis:

- a) Enter Security Services mode:

top

scope ssa

- b) Enter Application Software mode:

scope app-software

- c) Download the logical device software image:

download image *URL*

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

- **ftp://username@server/path**
- **scp://username@server/path**
- **sftp://username@server/path**
- **tftp://server:port-num/path**

- d) To monitor the download process:

show download-task

- e) To view the downloaded applications:

up

show app

Make note of the ASA version for the software package you downloaded. You will need to use the exact version string to enable the application in a later step.

Example:

The following example copies an image using the SCP protocol:

```
Firepower-chassis # scope ssa
Firepower-chassis /ssa # scope app-software
Firepower-chassis /ssa/app-software # download image
scp://user@192.168.1.1/images/cisco-asa.9.4.1.65.csp
Firepower-chassis /ssa/app-software # show download-task
```

Downloads for Application Software:

File Name	Protocol	Server	Userid	State
cisco-asa.9.4.1.65.csp	Scp	192.168.1.1	user	Downloaded

```
Firepower-chassis /ssa/app-software # up
```

```
Firepower-chassis /ssa # show app
```

Application:

Name	Version	Description	Author	Deploy Type	CSP Type	Is Default App
asa	9.4.1.41	N/A		Native	Application	No
asa	9.4.1.65	N/A		Native	Application	Yes

Step 9

Upgrade the ASA logical device image:

- a) Enter Security Services mode:

```
top
```

```
scope ssa
```

- b) Set the scope to the security module you are updating:

```
scope slotslot_number
```

- c) Set the scope to the ASA application:

For FXOS 2.3.1 and earlier: **scope app-instance asa**

For FXOS 2.4.1 and later: **scope app-instance asa instance_name**

- d) Set the Startup version to the version you want to update:

```
set startup-version version_number
```

- e) Commit the configuration:

```
commit-buffer
```

Commits the transaction to the system configuration. The application image is updated and the application restarts.

Step 10

To verify the status of the security modules/security engine and any installed applications, see [Verify the Installation, on page 100](#).

Step 11

After the upgraded security module come online, re-enable clustering for all security modules on the chassis:

- a) Connect to the module CLI using a console connection or a Telnet connection.

```
connect module slot_number { console | telnet }
```

To connect to the security engine of a device that does not support multiple security modules, always use **1** as the *slot_number*.

Example:

```
Firepower# connect module 1 console
Telnet escape character is '~'.
Trying 127.5.1.1...
Connected to 127.5.1.1.
Escape character is '~'.

CISCO Serial Over LAN:
Close Network Connection to Exit

Firepower-module1>
```

- b) Connect to the application console.

connect asa

Example:

```
Firepower-module1> connect asa
Connecting to asa(asal) console... hit Ctrl + A + D to return to bootCLI
[...]
asa>
```

- c) Disable clustering on one of the security modules:

cluster group *name*

enable

write memory

- d) Repeat step 12 for each security module on this chassis.

Step 12 Exit the application console to the FXOS module CLI.
Enter **Ctrl-a, d**

Step 13 Return to the supervisor level of the FXOS CLI.

Exit the console:

- a) Enter ~

You exit to the Telnet application.

- b) To exit the Telnet application, enter:

```
telnet>quit
```

Exit the Telnet session:

- a) Enter **Ctrl-], .**

Step 14 Repeat steps 2-14 for all remaining chassis in the cluster that do not have the control unit.

Step 15 After all chassis in the cluster that do not have the control unit have been upgraded, repeat steps 2-14 on the chassis with the control unit, being sure to disable clustering on the data units first, and then finally the control unit.

- Step 16** A new control unit will be chosen from one of the previously upgraded chassis.
- For distributed VPN clustering mode, after the cluster has stabilized you can redistribute active sessions among all modules in the cluster using the ASA console on the control unit.

cluster redistribute vpn-sessiondb

What to do next

Set the chassis Site ID. For more information about how to set the chassis Site ID, see the Inter-Site Clustering topic in Deploying a Cluster for ASA on the Firepower 4100/9300 for Scalability and High Availability on Cisco.com.



CHAPTER 5

Monitor Upgrade Progress and Verify Installation

- [Monitor the Upgrade Progress, on page 99](#)
- [Verify the Installation, on page 100](#)

Monitor the Upgrade Progress

You can monitor the upgrade process using the FXOS CLI:

Procedure

- | | |
|---------------|---|
| Step 1 | Connect to the FXOS CLI. |
| Step 2 | Enter scope system . |
| Step 3 | Enter show firmware monitor . |
| Step 4 | 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

```
Firepower-chassis# scope system
Firepower-chassis /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
```

Verify the Installation

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

Procedure

- Step 1** Connect to the FXOS CLI.
- Step 2** Enter **top**.
- Step 3** Enter **scope ssa**.
- Step 4** Enter **show slot**.
- Step 5** 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.

Example:

- Step 6** Enter **show app-instance**.
- Step 7** Verify that the Oper State is **Online** for any logical devices installed on the chassis and that the correct version is listed.

If this chassis is part of a cluster, verify that the cluster operational state is “In-Cluster” for all security modules installed in the chassis. Also, verify that the control unit is not on the chassis for which you are upgrading—there should not be any instance with Cluster Role set to “Master”.

Example

```
Firepower-chassis# scope ssa
Firepower-chassis /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

```
Firepower-chassis /ssa #
```

```
Firepower-chassis /ssa # show app-instance
```

App Name	Identifier	Slot ID	Admin State	Oper State	Running Version	Startup Version
asa	asa1	1	Enabled	Online	9.10.0.85	9.10.0.85
	Not Applicable	None				
asa	asa2	2	Enabled	Online	9.10.0.85	9.10.0.85
	Not Applicable	None				

```
Firepower-chassis /ssa #
```



PART I

Reference

- [Compatibility](#), on page 103
- [Firepower Software Upgrade Guidelines](#), on page 119
- [ASA Upgrade Guidelines](#), on page 153
- [Time and Disk Space Tests](#), on page 167
- [Traffic Flow and Inspection](#), on page 219



CHAPTER 6

Compatibility

For general compatibility information see:

- [Cisco Firepower Compatibility Guide](#): Detailed compatibility information for all supported versions, including versions and builds of bundled operating systems and other components, as well as links to end-of-sale and end-of-life announcements for deprecated platforms.
- [Cisco NGFW Product Line Software Release and Sustaining Bulletin](#): Support timelines for the Cisco Next Generation Firewall product line, including management platforms and operating systems.

For compatibility information relevant to the upgrade process, see:

- [Firepower Management Center, on page 103](#)
- [Firepower 4100/9300 Compatibility with ASA and FTD, on page 108](#)
- [Radware DefensePro Compatibility, on page 115](#)

Firepower Management Center

FMC-Device Compatibility

A FMC must run the *same or newer* version as its managed devices. This means:

- You *can* manage older devices with a newer FMC, usually a few major versions back.
- You *cannot* upgrade a device past the FMC.

Below, we list FMC versions and the devices they can manage. Find your current version in the first column, then read across to determine which devices you can manage. Remember, within a major version, the FMC must be running the same or newer maintenance (third-digit) release as its managed devices.

Table 20: FMC Capability: Version 6.2.3 through 7.1.x

FMC Version	Can Manage: Device Version											
	7.1.x	7.0.x	6.7.x	6.6.x	6.5.0	6.4.0	6.3.0	6.2.3	6.2.2	6.2.1	6.2.0	6.1.0
7.1.x	YES	YES	YES	YES	YES	—	—	—	—	—	—	—
7.0.x	—	YES	YES	YES	YES	YES	—	—	—	—	—	—

FMC Version	Can Manage: Device Version											
	7.1.x	7.0.x	6.7.x	6.6.x	6.5.0	6.4.0	6.3.0	6.2.3	6.2.2	6.2.1	6.2.0	6.1.0
6.7.x	—	—	YES	YES	YES	YES	YES	—	—	—	—	—
6.6.x	—	—	—	YES	YES	YES	YES	YES	—	—	—	—
6.5.0	—	—	—	—	YES	YES	YES	YES	—	—	—	—
6.4.0	—	—	—	—	—	YES	YES	YES	YES	YES	YES	YES
6.3.0	—	—	—	—	—	—	YES	YES	YES	YES	YES	YES
6.2.3	—	—	—	—	—	—	—	YES	YES	YES	YES	YES

Table 21: FMC Capability: Version 5.4.0 through 6.2.2

FMC Version	Can Manage: Device Version							
	6.2.2	6.2.1	6.2.0	6.1.0	6.0.1	6.0.0	5.4.1	5.4.0
6.2.2	YES	YES	YES	YES	—	—	—	—
6.2.1	—	YES	YES	YES	—	—	—	—
6.2.0	—	—	YES	YES	—	—	—	—
6.1.0	—	—	—	YES	YES	YES	YES *	YES *
6.0.1	—	—	—	—	YES	YES	YES *	YES *
6.0.0	—	—	—	—	—	YES	YES *	YES *
5.4.1	—	—	—	—	—	—	YES	YES
5.4.0	—	—	—	—	—	—	—	YES

* A device must be running at least Version 5.4.0.2/5.4.1.1 to be managed by a Version 6.0.0, 6.0.1, or 6.1.0 FMC.

FMC Hardware

Table 22: FMC Hardware Compatibility

FMC Version	FMC 1600 FMC 2600 FMC 4600	FMC 1000 FMC 2500 FMC 4500	FMC 2000 FMC 4000	FMC 750 FMC 1500 FMC 3500	DC 500 DC 1000 DC 3000
7.1.x	YES	—	—	—	—

FMC Version	FMC 1600	FMC 1000	FMC 2000	FMC 750	DC 500
	FMC 2600	FMC 2500	FMC 4000	FMC 1500	DC 1000
	FMC 4600	FMC 4500		FMC 3500	DC 3000
7.0.x	YES	YES	—	—	—
6.7.x	YES	YES	—	—	—
6.6.x	YES	YES	YES	—	—
6.5.0	YES	YES	YES	—	—
6.4.0	YES	YES	YES	YES	—
6.3.0	YES	YES	YES	YES	—
6.2.3	—	YES	YES	YES	—
6.2.2	—	YES	YES	YES	—
6.2.1	—	YES	YES	YES	—
6.2.0	—	YES	YES	YES	—
6.1.0	—	—	YES	YES	—
6.0.1	—	—	YES	YES	—
6.0.0	—	—	YES	YES	—
5.4.1	—	—	YES	YES	YES
5.4.0 *	—	—	YES	YES	YES

* 5.4.0 only. Use 5.4.1.x Defense Centers to manage 5.4.x devices.

FMCv

For supported FMCv instances, see the [Cisco Firepower Management Center Virtual Getting Started Guide](#).

Table 23: FMCv for VMware Compatibility: Version 6.2.3+

FMC Version	VMware vSphere/VMware ESXi					
	7.0	6.7	6.5	6.0	5.5	5.1
7.1.x	YES	YES	YES	—	—	—
7.0.x	YES	YES	YES	—	—	—
6.7.x	—	YES	YES	YES	—	—
6.6.x	—	YES	YES	YES	—	—

FMC Version	VMware vSphere/VMware ESXi					
	7.0	6.7	6.5	6.0	5.5	5.1
6.5.0	—	YES	YES	YES	—	—
6.4.0	—	—	YES	YES	—	—
6.3.0	—	—	YES	YES	—	—
6.2.3	—	—	YES	YES	YES	—

Table 24: FMCv for VMware Compatibility: Version 5.4 through 6.2.2

FMC Version	VMware vSphere/VMware ESXi				VMware vCloud Director
	6.0	5.5	5.1	5.0	
6.2.2	YES	YES	—	—	—
6.2.1	YES	YES	—	—	—
6.2.0	YES	YES	—	—	—
6.1.0	YES	YES	—	—	—
6.0.1	—	YES	YES	—	—
6.0.0	—	YES	YES	—	—
5.4.1	—	YES	YES	YES	YES
5.4.0 *	—	YES	YES	YES	YES

* 5.4.0 only; use 5.4.1.x Defense Centers to manage 5.4.x devices.

Table 25: FMCv Compatibility: Other Hypervisors

FMC Version	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Cisco HyperFlex (HyperFlex)	Kernel-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack	Oracle Cloud Infrastructure (OCI)
7.1.x	YES	YES	YES	YES	YES	YES	YES	YES
7.0.x	YES	YES	YES	YES	YES	YES	YES	YES
6.7.x	YES	YES	YES	—	YES	—	—	YES
6.6.x	YES	YES	—	—	YES	—	—	—
6.6.x	YES	YES	—	—	YES	—	—	—
6.5.0	YES	YES	—	—	YES	—	—	—

FMC Version	Amazon Web Services (AWS)	Microsoft Azure (Azure)	Google Cloud Platform (GCP)	Cisco HyperFlex (HyperFlex)	KVM-Based Virtual Machine (KVM)	Nutanix Enterprise Cloud (Nutanix)	OpenStack	Oracle Cloud Infrastructure (OCI)
6.4.0	YES	YES	—	—	YES	—	—	—
6.3.0	YES	—	—	—	YES	—	—	—
6.2.3	YES	—	—	—	YES	—	—	—
6.2.2	YES	—	—	—	YES	—	—	—
6.2.1	YES	—	—	—	YES	—	—	—
6.2.0	YES	—	—	—	YES	—	—	—
6.1.0	YES	—	—	—	YES	—	—	—
6.0.1	YES	—	—	—	—	—	—	—

BIOS and Firmware for FMC Hardware

We provide updates for BIOS and RAID controller firmware on FMC hardware. If your FMC does not meet the requirements, apply the appropriate hotfix. If your FMC model and version are not listed and you think you need to update, contact Cisco TAC.

Table 26: BIOS and Firmware Minimum Requirements

Platform	FMC	BIOS	RAID Controller Firmware	CIMC Firmware	Hotfix
FMC 1600, 2600, 4600	6.3.0 to 6.7.x	C220M5.4.1.1c.0	51.10.0-2978	4.1(1f)	BIOS Update Hotfix EI
FMC 1000, 2500, 4500	6.2.3 to 6.7.x	C22M4.4.0.2d.0	24.12.1-0433	4.0(2d)	BIOS Update Hotfix EI
FMC 2000, 4000	6.2.3 to 6.6.x	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS Update Hotfix EI
FMC 750, 1500, 3500	6.2.3 to 6.4.0	C220M3.3.0.4e.0	23.33.1-0060	3.0(4s)	BIOS Update Hotfix EI

Hotfixing is the only way to update the BIOS and RAID controller firmware. Upgrading the software does not accomplish this task, nor does reimaging to a later version. If the FMC is already up to date, the hotfix has no effect.

**Tip**

These hotfixes also update the CIMC firmware; for resolved issues see [Release Notes for Cisco UCS Rack Server Software](#). Note that in general, we do not support changing configurations on the FMC using CIMC. However, to enable logging of invalid CIMC usernames, apply Hotfix EI, then follow the instructions in the *Viewing Faults and Logs* chapter in the [Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide](#), Version 4.0 or later.

Use the regular upgrade process to apply hotfixes. For hotfix release notes, which include quicklinks to the Cisco Support & Download site, see the [Cisco Firepower Hotfix Release Notes](#).

**Note**

The FMC web interface may display these hotfixes with a version that is different from (usually later than) the current software version. This is expected behavior and the hotfixes are safe to apply.

Determining BIOS and Firmware Versions

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"**

Firepower 4100/9300 Compatibility with ASA and FTD

The following table lists compatibility between the ASA or FTD applications with the Firepower 4100/9300. The FXOS versions with (EoL) appended have reached their end of life (EoL), or end of support.

**Note**

The **bold** versions listed below are specially-qualified companion releases. You should use these software combinations whenever possible because Cisco performs enhanced testing for these combinations.

**Note**

Firepower 1000/2100 appliances utilize FXOS only as an underlying operating system that is included in the ASA and Firepower Threat Defense unified image bundles.

Table 27: ASA or FTD, and Firepower 4100/9300 Compatibility

FXOS Version	Firepower Model	ASA Version	FTD Version
Note FXOS 2.10(1.159)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.10(1.159)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	9.16(x) (recommended) 9.15(1) 9.14(x)	7.0.0 (recommended) 6.7.0 6.6.x
	Firepower 4145	9.16(x) (recommended) 9.15(1) 9.14(x) 9.13(1) 9.12(x)	7.0.0 (recommended) 6.7.0 6.6.x 6.5.0 6.4.0
	Firepower 4125		
	Firepower 4115		
	Firepower 9300 SM-56		
	Firepower 9300 SM-48	9.16(x) (recommended) 9.15(1) 9.14(x) 9.13(x) 9.12(x) 9.10(x) 9.9(x) 9.8(x)	7.0.0 (recommended) 6.7.0 6.6.x 6.5.0 6.4.0 6.3.0
	Firepower 9300 SM-40		
	Firepower 4150		
	Firepower 4140		
	Firepower 4120		
	Firepower 4110		
	Firepower 9300 SM-44		
	Firepower 9300 SM-36		
	Firepower 9300 SM-24		

FXOS Version	Firepower Model	ASA Version	FTD Version
Note FXOS 2.9(1.131)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.9(1.131)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	9.15(1) (recommended) 9.14(x)	6.7.0 (recommended) 6.6.x
	Firepower 4145	9.15(1) (recommended)	6.7.0 (recommended)
	Firepower 4125	9.14(x)	6.6.x
	Firepower 4115	9.13(1)	6.5.0
	Firepower 9300 SM-56	9.12(x)	6.4.0
	Firepower 9300 SM-48		
	Firepower 9300 SM-40		
	Firepower 4150	9.15(1) (recommended)	6.7.0 (recommended)
	Firepower 4140	9.14(x)	6.6.x
	Firepower 4120	9.13(x)	6.5.0
	Firepower 4110	9.12(x)	6.4.0
	Firepower 9300 SM-44	9.10(x)	6.3.0
	Firepower 9300 SM-36	9.9(x)	
	Firepower 9300 SM-24	9.8(x)	

FXOS Version	Firepower Model	ASA Version	FTD Version
2.8(1.105)+ Note FXOS 2.8(1.125)+ does not support ASA 9.14(1) or 9.14(1.10) for ASA SNMP polls and traps; you must use 9.14(1.15)+. Other releases that are paired with 2.8(1.125)+, such as 9.13 or 9.12, are not affected.	Firepower 4112	9.14(x)	6.6.x Note 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 4145 Firepower 4125 Firepower 4115	9.14(x) (recommended) 9.13(1) 9.12(x)	6.6.x (recommended) Note 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	Note Firepower 9300 SM-56 requires ASA 9.12(2)+	6.5.0 6.4.0
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.14(x) (recommended) 9.13(x) 9.12(x) 9.10(x)	6.6.x (recommended) Note 6.6.1+ requires FXOS 2.8(1.125)+.
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.9(x) 9.8(x) 9.6(4)	6.5.0 6.4.0 6.3.0 6.2.3 6.2.0
2.7(1.92)+	Firepower 4145 Firepower 4125 Firepower 4115	9.13(1) (recommended) 9.12(x)	6.5.0 (recommended) 6.4.0
	Firepower 9300 SM-56 Firepower 9300 SM-48 Firepower 9300 SM-40	Note Firepower 9300 SM-56 requires ASA 9.12.2+	
	Firepower 4150 Firepower 4140 Firepower 4120 Firepower 4110	9.13(1) (recommended) 9.12(x) 9.10(1) 9.9(x)	6.5.0 (recommended) 6.4.0 6.3.0 6.2.3
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	9.8(x) 9.6(4)	6.2.2 6.2.0

FXOS Version	Firepower Model	ASA Version	FTD Version	
2.6(1.157)+ Note You can now run ASA 9.12+ and FTD 6.4+ on separate modules in the same Firepower 9300 chassis	Firepower 4145	9.12(x) Note Firepower 9300 SM-56 requires ASA 9.12.2+	6.4.0	
	Firepower 4125			
	Firepower 4115			
	Firepower 9300 SM-56			
	Firepower 9300 SM-48			
	Firepower 9300 SM-40			
	Firepower 4150	9.12(x) (recommended) 9.10(1) 9.9(x) 9.8(x) 9.6(4) Note 9.7(x) is not supported.	6.4.0 (recommended) 6.3.0 6.2.3 6.2.2 6.2.0 6.1.0	
	Firepower 4140			
	Firepower 4120			
	Firepower 4110			
	Firepower 9300 SM-44			
	Firepower 9300 SM-36			
	Firepower 9300 SM-24			
2.6(1.131)				
Firepower 9300 SM-48	9.12(x)			Not supported
Firepower 9300 SM-40				
Firepower 4150	9.12(x) (recommended) 9.10(1) 9.9(x) 9.8(x) 9.6(4) Note 9.7(x) is not supported.			
Firepower 4140				
Firepower 4120				
Firepower 4110				
Firepower 9300 SM-44				
Firepower 9300 SM-36				
Firepower 9300 SM-24				
2.4(1.214)+				
Note FXOS 2.4(1.238)+ is required for hardware bypass. For more information, see the Important Notes section of the Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1) .	Firepower 4150	9.10(1) (recommended) 9.9(x) 9.8(x) 9.6(3), 9.6(4)	6.3.0 (recommended) 6.2.3 6.2.2 6.2.0 6.1.0	
	Firepower 4140			
	Firepower 4120			
	Firepower 4110			
	Firepower 9300 SM-44	Note 9.7(x) is not supported.		
	Firepower 9300 SM-36			
	Firepower 9300 SM-24			

FXOS Version	Firepower Model	ASA Version	FTD Version
2.4(1.101)	Firepower 4150	9.10(1) (recommended)	Not supported
	Firepower 4140	9.9(x)	
	Firepower 4120	9.8(x)	
	Firepower 4110	9.6(3), 9.6(4)	
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	Note 9.7(x) is not supported.	
2.3(1.73)+	Firepower 4150	9.9(x) (recommended)	6.2.3 (recommended)
	Firepower 4140	9.8(x)	Note 6.2.3.16+ requires FXOS 2.3.1.157+
	Firepower 4120	9.7(x)	6.2.2
	Firepower 4110	9.6(3), 9.6(4)	6.2.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	Note 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	6.1.0 Note 6.2.2.2+ is required for flow offload when running FXOS 2.3(1.130)+.
2.3(1.66) 2.3(1.58) 2.3(1.56) Note FXOS 2.3(1.56), which was briefly available on Cisco.com, is no longer supported. For more information, see the Cisco FXOS Release Notes, 2.3(1).	Firepower 4150	9.9(x) (recommended)	6.2.2 (recommended)
	Firepower 4140	9.8(x)	6.2.2
	Firepower 4120	9.7(x)	6.2.0
	Firepower 4110	9.6(3), 9.6(4)	6.1.0
	Firepower 9300 SM-44 Firepower 9300 SM-36 Firepower 9300 SM-24	Note 9.8(2.12)+ is required for flow offload when running FXOS 2.3(1.130)+.	Note 6.2.2.2+ is required for flow offload when running FXOS 2.3(1.130)+.

FXOS Version	Firepower Model	ASA Version	FTD Version
2.2(2)	Firepower 4150	9.8(x) (recommended)	6.2.2 (recommended) 6.2.0 Note 6.2.2+ is required for flow offload when running FXOS 2.2(2.91)+.
	Firepower 4140		
	Firepower 4120		
	Firepower 4110		
	Firepower 9300 SM-44		
	Firepower 9300 SM-36		
2.2(1)	Firepower 9300 SM-24		
	Firepower 4150	9.8(1) (recommended) 9.7(x) Note 9.7(1.15)+ is required for flow offload.	6.2.0 (recommended) Note 6.2.0.3+ is required for flow offload.
	Firepower 4140		
	Firepower 4120		
	Firepower 4110		
	Firepower 9300 SM-44		
	Firepower 9300 SM-36		
2.1(1) (EoL)	Firepower 9300 SM-24		
	Firepower 4150	9.7(x) (recommended) 9.6(2), 9.6(3), 9.6(4)	6.2.0 (recommended) 6.1.0
	Firepower 4140		
	Firepower 4120		
	Firepower 4110		
	Firepower 9300 SM-44		
	Firepower 9300 SM-36		
2.0(1)	Firepower 9300 SM-24		
	Firepower 4150	9.6(2), 9.6(3), 9.6(4) (recommended) 9.6(1)	6.1.0 (recommended) 6.0.1
	Firepower 4140		
	Firepower 4120		
	Firepower 4110		
	Firepower 9300 SM-44		
	Firepower 9300 SM-36		
	Firepower 9300 SM-24		

FXOS Version	Firepower Model	ASA Version	FTD Version
1.1(4)	Firepower 4140 Firepower 4120 Firepower 4110	9.6(1)	6.0.1 (recommended)
	Firepower 9300 SM-36 Firepower 9300 SM-24	9.6(1) (recommended) 9.5(2), 9.5(3)	
1.1(3)	Firepower 9300 SM-36 Firepower 9300 SM-24	9.5(2), 9.5(3) (recommended) 9.4(2)	Not supported
1.1(2)	Firepower 9300 SM-36 Firepower 9300 SM-24	9.4(2) (recommended) 9.4(1)	Not supported
1.1(1) (EoL)	Firepower 9300 SM-36 Firepower 9300 SM-24	9.4(1) (recommended)	Not supported

Radware DefensePro Compatibility

The following table lists the supported Radware DefensePro version for each Firepower security appliance and associated logical device.

Table 28: Radware DefensePro Compatibility

FXOS Version	ASA	Firepower Threat Defense	Radware DefensePro	Firepower Models
1.1(4)	9.6(1)	not supported	1.1(2.32-3)	9300
2.0(1)	9.6(1)	not supported	8.10.01.16-5	Firepower 9300
	9.6(2)			Firepower 4120
	9.6(3)			Firepower 4140
	9.6(4)			Firepower 4150
2.1(1)	9.6(2)	not supported	8.10.01.16-5	Firepower 9300
	9.6(3)			Firepower 4120
	9.6(4)			Firepower 4140
	9.7(1)			Firepower 4150

FXOS Version	ASA	Firepower Threat Defense	Radware DefensePro	Firepower Models
2.2(1)	9.7(1) 9.8(1)	6.2.0	8.10.01.17-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense only) Firepower 4120 Firepower 4140 Firepower 4150
2.2(2)	9.8(1) 9.8(2) 9.8(3)	6.2.0 6.2.2	8.10.01.17-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense only) Firepower 4120 Firepower 4140 Firepower 4150
2.3(1)	9.9(1) 9.9(2)	6.2.2 6.2.3	8.13.01.09-2	Firepower 9300 Firepower 4110 (Firepower Threat Defense only) Firepower 4120 Firepower 4140 Firepower 4150
2.4(1)	9.9(2) 9.10(1)	6.2.3 6.3	8.13.01.09-2	Firepower 9300 Firepower 4110 Firepower 4120 Firepower 4140 Firepower 4150
2.6(1)	9.12(1) 9.10(1)	6.4.0 6.3.0	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS Version	ASA	Firepower Threat Defense	Radware DefensePro	Firepower Models
2.7(1)	9.13(1)	6.5	8.13.01.09-3	Firepower 9300 Firepower 4110 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.8.1	9.14(1)	6.6.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150
2.9.1	9.15(1)	6.7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150

FXOS Version	ASA	Firepower Threat Defense	Radware DefensePro	Firepower Models
2.10.1	9.16(1)	7.0	8.13.01.09-3 8.22.2	Firepower 9300 Firepower 4110 Firepower 4112 Firepower 4115 Firepower 4120 Firepower 4125 Firepower 4140 Firepower 4145 Firepower 4150



CHAPTER 7

Firepower Software Upgrade Guidelines

For your convenience, this guide lists the same version-specific Firepower software upgrade guidelines as the [Cisco Firepower Release Notes](#).

If your upgrade skips versions, guidelines for intermediate releases can apply. The checklists in this chapter help you identify all applicable guidelines—just follow the cross references/links to read about them. In this chapter, upgrade guidelines appear under the version where they *first* apply.

In some cases, we may list guidelines that apply to Firepower Threat Defense platforms other than the Firepower 4100/9300. You can safely ignore these guidelines.



Important

This list of guidelines does *not* replace the release notes. You *must* read the Firepower release notes for additional critical and version-specific information. For example, new and deprecated features can require pre- or post-upgrade configuration changes, or even prevent upgrade. Or, known issues (bugs) can affect upgrade. In addition, this guide is updated less frequently.

- [General Guidelines, on page 120](#)
- [Version 7.0.x Guidelines, on page 120](#)
- [Version 6.7.x Guidelines, on page 121](#)
- [Version 6.6.x Guidelines, on page 122](#)
- [Version 6.5.0 Guidelines, on page 125](#)
- [Version 6.4.0 Guidelines, on page 133](#)
- [Version 6.3.0 Guidelines, on page 135](#)
- [Version 6.2.3 Guidelines, on page 141](#)
- [Version 6.2.2 Guidelines, on page 144](#)
- [Version 6.2.0 Guidelines, on page 145](#)
- [Version 6.1.0 Guidelines, on page 147](#)
- [Patch Guidelines by Version, on page 147](#)
- [Date-Based Guidelines, on page 151](#)

General Guidelines

Deployment Health and Communication

At all times during the process, make sure that the appliances in your deployment are successfully communicating and that there are no issues reported.

Unresponsive Upgrades

In most cases, 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, there may be something you can do.

Starting with major and maintenance FTD upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades:

- Firepower Management Center deployments: Use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center.
- Firepower Device Manager deployments: Use the System Upgrade panel.

You can also use the FTD CLI.



Note

By default, FTD automatically reverts to its pre-upgrade state upon upgrade failure ("auto-cancel"). To be able to *manually* cancel or retry a failed upgrade, disable the auto-cancel option when you initiate the upgrade. Note that auto-cancel is not supported for patches. In a high availability or clustered deployment, auto-cancel applies to each device individually. That is, if the upgrade fails on one device, only that device is reverted.

If you have exhausted all options, or if your deployment does not support cancel/retry, contact Cisco TAC.

Version 7.0.x Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 7.0.0.

Table 29: Version 7.0.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Reconnect with Cisco Threat Grid for HA FMCs, on page 121	FMC	6.4.0 through 6.7.x	7.0.0+

This checklist contains older upgrade guidelines.

Table 30: Version 7.0.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	FMCv Requires 28 GB RAM for Upgrade, on page 124	FMCv	6.2.3 through 6.5.0.x	6.6.0+

✓	Guideline	Platforms	Upgrading From	Directly To
	Historical Data Removed During FTD/FDM Upgrade, on page 127	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 127	Any	6.2.3 through 6.4.0.x	6.5.0+

Reconnect with Cisco Threat Grid for HA FMCs

Deployments: FMC high availability/AMP for Networks (malware detection) deployments where you submit files for dynamic analysis

Upgrading from: Version 6.4.0 through 6.7.x

Directly to: Version 7.0+

Related bug: [CSCvu35704](#)

Firepower Version 7.0 fixes an issue with FMC high availability where, after failover, the system stopped submitting files for dynamic analysis. For the fix to take effect, you must reassociate with the Cisco Threat Grid public cloud.

After you upgrade the HA pair, on the primary FMC:

1. Select **AMP > Dynamic Analysis Connections**.
2. Click **Associate** in the table row corresponding to the Cisco Threat Grid public cloud.

A Cisco Threat Grid portal window opens. You do not have to sign in. The reassociation happens in the background, within a few minutes.

Version 6.7.x Guidelines

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

Table 31: Version 6.7.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0, on page 123	FMC	6.6.5 or later 6.6.x release	6.7.0 only

This checklist contains older upgrade guidelines.

Table 32: Version 6.7.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 124	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases
	FMCv Requires 28 GB RAM for Upgrade, on page 124	FMCv	6.2.3 through 6.5.0.x	6.6.0+
	Historical Data Removed During FTD/FDM Upgrade, on page 127	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 127	Any	6.2.3 through 6.4.0.x	6.5.0+
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 134	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+

Version 6.6.x Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.6.x maintenance releases.

Table 33: Version 6.6.x New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0, on page 123	FMC	6.6.5 or later 6.6.x release	6.7.0 only

This checklist contains upgrade guidelines that are new or specific to Version 6.6.0.

Table 34: Version 6.6.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 124	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases
	FMCv Requires 28 GB RAM for Upgrade, on page 124	FMCv	6.2.3 through 6.5.0.x	6.6.0+

This checklist contains older upgrade guidelines.

Table 35: Version 6.6.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Historical Data Removed During FTD/FDM Upgrade, on page 127	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 127	Any	6.2.3 through 6.4.0.x	6.5.0+
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 134	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+
	Readiness Check May Fail on FMC, on page 138	FMC	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 138	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 140	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 140	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 140	Any	6.1.0 through 6.2.3.x	6.3.0+

Upgrade Prohibited: FMC Version 6.6.5+ to Version 6.7.0

Deployments: FMC

Upgrading from: Version 6.6.5 or later maintenance release.

Directly to: Version 6.7.0 only

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

Upgrade Failure: FMC with Email Alerting for Intrusion Events

Deployments: Firepower Management Center

Upgrading from: Version 6.2.3 through 6.7.0.x

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

Related bugs: [CSCvw38870](#), [CSCvx86231](#)

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

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

To fully disable intrusion email alerting:

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

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



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

4. Save your configurations.

FMCv Requires 28 GB RAM for Upgrade

Deployments: FMCv

Upgrading from: Version 6.2.3 through 6.5.0.x

Directly to: Version 6.6.0+

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](#).



Note As of the Version 6.6.0 release, lower-memory instance types for cloud-based FMCv deployments (AWS, Azure) are fully deprecated. You cannot create new 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 36: FMCv Memory Requirements for Version 6.6.0+ Upgrades

Platform	Pre-Upgrade Action	Details
VMware	Allocate 28 GB minimum/32 GB recommended.	Power off the virtual machine first. For instructions, see the VMware documentation.
KVM	Allocate 28 GB minimum/32 GB recommended.	For instructions, see the documentation for your KVM environment.
AWS	Resize instances: <ul style="list-style-type: none"> • From c3.xlarge to c3.4xlarge. • From c3.2.xlarge to c3.4xlarge. • From c4.xlarge to c4.4xlarge. • From c4.2xlarge to c4.4xlarge. We also offer a c5.4xlarge instance for new deployments.	Stop the instance before you resize. Note that when you do this, data on the instance store volume is lost, so migrate your instance store-backed instance first. Additionally, if your management interface does not have an Elastic IP address, its public IP address is released. For instructions, see the documentation on changing your instance type in the AWS user guide for Linux instances.
Azure	Resize instances: <ul style="list-style-type: none"> • From Standard_D3_v2 to Standard_D4_v2. 	Use the Azure portal or PowerShell. You do not need to stop the instance before you resize, but stopping may reveal additional sizes. Resizing restarts a running virtual machine. For instructions, see the Azure documentation on resizing a Windows VM.

Version 6.5.0 Guidelines

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

Table 37: Version 6.5.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Disable Egress Optimization for Version 6.5.0, on page 126	FTD	6.2.3 through 6.4.0.x	6.5.0 only
	Historical Data Removed During FTD/FDM Upgrade, on page 127	FTD with FDM	6.2.3 through 6.4.0.x	6.5.0+
	New URL Categories and Reputations, on page 127	Any	6.2.3 through 6.4.0.x	6.5.0+

This checklist contains older upgrade guidelines.

Table 38: Version 6.5.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 134	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 134	Firepower 2100 series Firepower 4100/9300	6.2.3 through 6.3.0.x	6.4.0+
	Readiness Check May Fail on FMC, on page 138	FMC	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 138	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 140	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 140	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 140	Any	6.1.0 through 6.2.3.x	6.3.0+

Disable Egress Optimization for Version 6.5.0

Deployments: FTD

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0 only

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

Upgrading to Version 6.5.0:

- From Version 6.2.3.x: Enables and turns on egress optimization.
- From Version 6.3.0.x: Enables and turns on egress optimization.

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



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

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

Historical Data Removed During FTD/FDM Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.3 through 6.4.x

Directly to: 6.5.0+

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

New URL Categories and Reputations

Deployments: Any

Upgrading from: Version 6.2.3 through 6.4.0.x

Directly to: Version 6.5.0+

Cisco Talos Intelligence Group (Talos) has introduced new categories and renamed reputations to classify and filter URLs. For 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 39: Deployment Changes on Upgrade

Change	Details
Modifies URL rule categories.	<p>The upgrade modifies URL rules to use the nearest equivalents in the new category set, in the following policies:</p> <ul style="list-style-type: none"> • Access control • SSL • QoS (FMC only) • Correlation (FMC only) <p>These changes may create redundant or preempted rules, which can slow performance. If your configuration includes merged categories, you may experience minor changes to the URLs that are allowed or blocked.</p>
Renames URL rule reputations.	<p>The upgrade modifies URL rules to use the new reputation names:</p> <ol style="list-style-type: none"> 1. Untrusted (was <i>High Risk</i>) 2. Questionable (was <i>Suspicious sites</i>) 3. Neutral (was <i>Benign sites with security risks</i>) 4. Favorable (was <i>Benign sites</i>) 5. Trusted (was <i>Well Known</i>)
Clears the URL cache.	<p>The upgrade clears the URL cache, which contains results that the system previously looked up in the cloud. Your users may temporarily experience slightly longer access times for URLs that are not in the local data set.</p>
Labels 'legacy' events.	<p>For already-logged events, the upgrade labels any associated URL category and reputation information as <i>Legacy</i>. These legacy events will age out of the database over time.</p>

Pre-Upgrade Actions for URL Categories and Reputations

Before upgrade, take the following actions.

Table 40: Pre-Upgrade Actions

Action	Details
Make sure your appliances can reach Talos resources.	<p>The system must be able to communicate with the following Cisco resources after the upgrade:</p> <ul style="list-style-type: none"> • https://regsvc.sco.cisco.com/ — Registration • https://est.sco.cisco.com/ — Obtain certificates for secure communications • https://updates-talos.sco.cisco.com/ — Obtain client/server manifests • http://updates.ironport.com/ — Download database (note: uses port 80) • https://v3.sds.cisco.com/ — Cloud queries <p>The cloud query service also uses the following IP address blocks:</p> <ul style="list-style-type: none"> • IPv4 cloud queries: <ul style="list-style-type: none"> • 146.112.62.0/24 • 146.112.63.0/24 • 146.112.255.0/24 • 146.112.59.0/24 • IPv6 cloud queries: <ul style="list-style-type: none"> • 2a04:e4c7:ffff::/48 • 2a04:e4c7:fffe::/48
Identify potential rule issues.	<p>Understand the upcoming changes. Examine your current URL filtering configuration and determine what post-upgrade actions you will need to take (see the next section).</p> <p>Note You may want to modify URL rules that use deprecated categories now. Otherwise, rules that use them will prevent deploy after the upgrade.</p> <p>In FMC deployments, we recommend you generate an <i>access control policy report</i>, which provides details on the policy's current saved configuration, including access control rules and rules in subordinate policies (such as SSL). For each URL rule, you can see the current categories, reputations, and associated rule actions. On the FMC, choose Policies > Access Control, then click the report icon () next to the appropriate policy.</p>

Post-Upgrade Actions for URL Categories and Reputations

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

Table 41: Post-Upgrade Actions

Action	Details
Remove deprecated categories from rules. Required.	<p>The upgrade does not modify URL rules that use deprecated categories. Rules that use them will prevent deploy.</p> <p>On the FMC, these rules are marked.</p>
Create or modify rules to include the new categories .	<p>Most of the new categories identify threats. We strongly recommend you use them.</p> <p>On the FMC, these new categories are not marked after <i>this</i> upgrade, but Talos may add additional categories in the future. When that happens, new categories are marked.</p>
Evaluate rules changed as a result of merged categories .	<p>Each rule that included any of the affected categories now include all of the affected categories. If the original categories were associated with different reputations, the new rule is associated with the broader, more inclusive reputation. To filter URLs as before, you may have to modify or delete some configurations; see Guidelines for Rules with Merged URL Categories, on page 130.</p> <p>Depending on what changed and how your platform handles rule warnings, changes may be marked. For example, the FMC marks wholly redundant and wholly preempted rules, but not rules that have partial overlap.</p>
Evaluate rules changed as a result of split categories .	<p>The upgrade replaces each old, single category in URL rules with <i>all</i> the new categories that map to the old one. This will not change the way you filter URLs, but you can modify affected rules to take advantage of the new granularity.</p> <p>These changes are not marked.</p>
Understand which categories were renamed or are unchanged .	<p>Although no action is required, you should be aware of these changes.</p> <p>These changes are not marked.</p>
Evaluate how you handle uncategorized and reputationless URLs.	<p>Even though it is now possible to have uncategorized and reputationless URLs, you cannot still cannot filter uncategorized URLs by reputation, nor can you filter reputationless URLs.</p> <p>Make sure that rules that filter by the Uncategorized category, or by Any reputation, will behave as you expect.</p>

Guidelines for Rules with Merged URL Categories

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

Table 42: Guidelines for Rules with Merged URL Categories

Guideline	Details
Rule Order Determines Which Rule Matches Traffic	When considering rules that include the same category, remember that traffic matches the first rule in the list that includes the condition.
Categories in the Same Rule vs Categories in Different Rules	<p>Merging categories in a single rule will merge into a single category in the rule. For example, if Category A and Category B are merging to become Category AB, and you have a rule with both Category A and Category B, then after merge the rule will have a single Category AB.</p> <p>Merging categories in different rules will result in separate rules with the same category in each rule after the merge. For example, if Category A and Category B are merging to become Category AB, and you have Rule 1 with Category A and Rule 2 with Category B, then after merge Rule 1 and Rule 2 will each include Category AB. How you choose to resolve this situation depends on the rule order, on the actions and reputation levels associated with the rules, on the other URL categories included in the rule, and on the non-URL conditions that are included in the rule.</p>
Associated Action	If merged categories in different rules were associated with different actions, then after merge you may have two or more rules with different actions for the same category.
Associated Reputation Level	If a single rule includes categories that were associated with different reputation levels before merging, the merged category will be associated with the more inclusive reputation level. For example, if Category A was associated in a particular rule with Any reputation and Category B was associated in the same rule with reputation level 3 - Benign sites with security risks , then after merge Category AB in that rule will be associated with Any reputation .
Duplicate and Redundant Categories and Rules	<p>After merge, different rules may have the same category associated with different actions and reputation levels.</p> <p>Redundant rules may not be exact duplicates, but they may no longer match traffic if another rule earlier in the rule order matches instead. For example, if you have pre-merge Rule 1 with Category A that applies to Any Reputation, and Rule 2 with Category B that applies only to Reputation 1-3, then after merge, both Rule 1 and Rule 2 will have Category AB, but Rule 2 will never match if Rule 1 is higher in the rule order.</p> <p>On the FMC, rules with an identical category and reputation will show a warning. However, these warnings will not indicate rules that include the same category but a different reputation.</p> <p>Caution: Consider all conditions in the rule when determining how to resolve duplicate or redundant categories.</p>
Other URL Categories in a Rule	Rules with merged URLs may also include other URL categories. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.

Guideline	Details
Non-URL Conditions in a Rule	Rules with merged URL categories may also include other rule conditions, such as application conditions. Therefore, if a particular category is duplicated after merge, you may want to modify rather than delete these rules.

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

Table 43: Examples of Rules with Merged URL Categories

Scenario	Before Upgrade	After Upgrade
Merged categories in the same rule	Rule 1 has Category A and Category B.	Rule 1 has Category AB.
Merged categories in different rules	Rule 1 has Category A. Rule 2 has Category B.	Rule 1 has Category AB. Rule 2 has Category AB. The specific result varies by the rules' order in the list, reputation levels, and associated actions. You should also consider all other conditions in the rule when determining how to resolve any redundancy.
Merged categories in different rules have different actions (Reputation is the same)	Rule 1 has Category A set to Allow. Rule 2 has Category B set to Block. (Reputation is the same)	Rule 1 has Category AB set to Allow. Rule 2 has Category AB set to Block. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, and will display a warning indicator if you show warnings after merge, because both category and reputation are the same.
Merged categories in the same rule have different reputation levels	Rule 1 includes: Category A with Reputation Any Category B with Reputation 1-3	Rule 1 includes Category AB with Reputation Any.
Merged categories in different rules have different reputation levels	Rule 1 includes Category A with Reputation Any. Rule 2 includes Category B with Reputation 1-3.	Rule 1 includes Category AB with Reputation Any. Rule 2 includes Category AB with Reputation 1-3. Rule 1 will match all traffic for this category. Rule 2 will never match traffic, but you will not see a warning indicator because the reputations are not identical.

Version 6.4.0 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.4.0.

Table 44: Version 6.4.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 134	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0
	TLS Crypto Acceleration Enabled/Cannot Disable, on page 134	Firepower 2100 series Firepower 4100/9300	6.1.0 through 6.3.0.x	6.4.0+

This checklist contains older upgrade guidelines.

Table 45: Version 6.4.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Readiness Check May Fail on FMC, on page 138	FMC	6.1.0 through 6.1.0.6 6.2.0 through 6.2.0.6 6.2.1 6.2.2 through 6.2.2.4 6.2.3 through 6.2.3.4	6.3.0+
	RA VPN Default Setting Change Can Block VPN Traffic, on page 138	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	Security Intelligence Enables Application Identification, on page 140	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 140	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 140	Any	6.1.0 through 6.2.3.x	6.3.0+
	Upgrade Can Unregister FTD/FDM from CSSM, on page 143	FTD with FDM	6.2.0 through 6.2.2.x	6.2.3 through 6.4.0

✓	Guideline	Platforms	Upgrading From	Directly To
	Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 143	FTD clusters	6.1.0.x	6.2.3 through 6.4.0
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 144	FTD with FDM	6.2.0 only	6.2.2 through 6.4.0
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 145	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD, on page 146	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0

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.

This issue is fixed in Version 6.4.0.6 and 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.

TLS Crypto Acceleration Enabled/Cannot Disable

Deployments: Firepower 4100/9300 chassis

Upgrading from: Version 6.1.0 through 6.3.x

Directly to: Version 6.4.0+

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

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

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

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

Version 6.3.0 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.3.0.

Table 46: Version 6.3.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Renamed Upgrade and Installation Packages, on page 136	FMC	Any	6.3.0+
	Reimaging to Version 6.3+ Disables LOM on Most Appliances, on page 137	FMC (physical)	Any	6.3.0+
	Readiness Check May Fail on FMC, on page 138	FMC	6.2.3 through 6.2.3.4 6.2.2 through 6.2.2.4 6.2.1 6.2.0 through 6.2.0.6 6.1.0 through 6.1.0.6	6.3.0+
	Reporting Data Removed During FTD/FDM Upgrade, on page 138	FTD with FDM	6.2.0 through 6.2.3.x	6.3.0 only
	RA VPN Default Setting Change Can Block VPN Traffic, on page 138	FTD with FMC	6.2.0 through 6.2.3.x	6.3.0+
	TLS/SSL Hardware Acceleration Enabled on Upgrade, on page 139	Firepower 2100 series Firepower 4100/9300	6.1.0 through 6.2.3.x	6.3.0 only

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Version 6.3.0-83 Upgrades to FMC, on page 139	FMC	6.1.0 through 6.2.3.x	6.3.0 only
	Security Intelligence Enables Application Identification, on page 140	FMC deployments	6.1.0 through 6.2.3.x	6.3.0+
	Update VDB after Upgrade to Enable CIP Detection, on page 140	Any	6.1.0 through 6.2.3.x	6.3.0+
	Invalid Intrusion Variable Sets Can Cause Deploy Failure, on page 140	Any	6.1.0 through 6.2.3.x	6.3.0+
	Firepower 4100/9300 Requires FTD Push Before FXOS Upgrade, on page 141	Firepower 4100/9300	6.1.0.x	6.3.0 only

This checklist contains older upgrade guidelines.

Table 47: Version 6.3.0 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Can Unregister FTD/FDM from CSSM, on page 143	FTD with FDM	6.2.0 through 6.2.2.x	6.2.3 through 6.4.0
	Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 143	FTD clusters	6.1.0.x	6.2.3 through 6.4.0
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 144	FTD with FDM	6.2.0 only	6.2.2 through 6.4.0
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 145	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD, on page 146	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0

Renamed Upgrade and Installation Packages

Deployments: FMC

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. 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 48: Naming Schemes: Upgrade, Patch, and Hotfix Packages

Platform	Naming Schemes
FMC	New: Cisco_Firepower_Mgmt_Center Old: Sourcefire_3D_Defense_Center_S3

Table 49: Naming Schemes: Installation Packages

Platform	Naming Schemes
FMC (physical)	New: Cisco_Firepower_Mgmt_Center Old: Sourcefire_Defense_Center_M4 Old: Sourcefire_Defense_Center_S3
FMCv: VMware	New: Cisco_Firepower_Mgmt_Center_Virtual_VMware Old: Cisco_Firepower_Management_Center_Virtual_VMware
FMCv: KVM	New: Cisco_Firepower_Mgmt_Center_Virtual_KVM Old: Cisco_Firepower_Management_Center_Virtual

Reimaging to Version 6.3+ Disables LOM on Most Appliances

Deployments: Physical FMCs

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 reenble LOM and LOM users.

Table 50: Reimage Effect on LOM Settings

Platform	Reimage to Version 6.2.3 or earlier	Reimage to Version 6.3+
MC1600, 2600, 4600 MC1000, 2500, 4500 MC2000, 4000	Never deleted	Always deleted
MC750, 1500, 3500	Deleted if you delete network settings	Deleted if you delete network settings

Readiness Check May Fail on FMC

Deployments: FMC

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 51: Patches with Readiness Checks for Version 6.3.0+

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

Reporting Data Removed During FTD/FDM Upgrade

Deployments: Firepower Device Manager

Upgrading from: Version 6.2.x

Directly to: Version 6.3 only

Reporting data for short time periods are removed during the Version 6.3 upgrade. After the upgrade, if you try to query short time ranges on days that fall before the upgrade, the system adjusts your query to match the available data. For example, if you query 1-3 PM for a date, and the system only has 24-hour data, the system reports on the entire day.

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 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.

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

Deployments: Firepower Management Center

Upgrading from: Version 6.1.0 through 6.2.3.x

Directly to: Version 6.3.0-83

Some Firepower Management Centers 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.

Security Intelligence Enables Application Identification

Deployments: Firepower Management Center

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3+

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

To disable discovery you must:

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

Update VDB after Upgrade to Enable CIP Detection

Deployments: Any

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

Directly to: Version 6.3.0+

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

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

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

Invalid Intrusion Variable Sets Can Cause Deploy Failure

Deployments: Any

Upgrading from: Version 6.1 through 6.2.3.x

Directly to: Version 6.3.0+

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

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

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

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

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 copy (*push*) 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 copy before you begin the required companion FXOS upgrade.



Note

We recommend that you not upgrade from Version 6.1.0 → 6.3.0. If you are running Version 6.1.0, we recommend upgrading to Version 6.2.3 on FXOS 2.3.1, and proceeding from there. If you do choose to perform this Version 6.1.0 → 6.3.0 upgrade, a push from the FMC before you upgrade FXOS is *required*.

This is because upgrading FXOS to Version 2.4.1 while still running Firepower 6.1.0 causes the device management port to flap, which in turn causes intermittent communication problems between the device and the FMC. Until you upgrade the Firepower software, you may continue to experience management port flaps. 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:

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.

Version 6.2.3 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.2.3.

Table 52: Version 6.2.3 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Edit/Resave Realms After FTD/FDM Upgrade, on page 142	FTD with FDM	6.2.0 through 6.2.2.x	6.2.3 only
	Upgrade Can Unregister FTD/FDM from CSSM, on page 143	FTD with FDM	6.2.0 through 6.2.2.x	6.2.3 through 6.4.0
	Edit/Resave Access Control Policies After Upgrade, on page 143	Any	6.1.0 through 6.2.2.x	6.2.3 only
	Remove Site IDs from Version 6.1.x FTD Clusters Before Upgrade, on page 143	FTD clusters	6.1.0.x	6.2.3 through 6.4.0

This checklist contains older upgrade guidelines.

Table 53: Version 6.2.3 Previously Published Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 144	FTD with FDM	6.2.0 only	6.2.2 through 6.4.0
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 145	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 146	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0

Upgrade Failure: Firepower 2100 Series from Version 6.2.2.5

Deployments: Firepower 2100 series with FTD, managed by FDM

Upgrading from: Version 6.2.2.5

Directly to: Version 6.2.3 only

If you change the DNS settings on a Firepower 2100 series device running Version 6.2.2.5, and then upgrade to Version 6.2.3 without an intermediate deployment, the upgrade fails. You must deploy or execute an action that triggers a deployment, such as an SRU update, before you upgrade the device.

Edit/Resave Realms After FTD/FDM Upgrade

Deployments: FTD with FDM

Upgrading from: Version 6.2.0 through Version 6.2.2.x

Directly to: Version 6.2.3 only

Before Version 6.2.3, users were not automatically logged out after 24 hours of inactivity. After you upgrade Firepower Threat Defense to Version 6.2.3 when using Firepower Device Manager, if you are using identity policies with active authentication, update your realm before you deploy configurations. Choose **Objects > Identity Realm**, edit the realm (no changes are needed), and save it. Then, deploy.

Upgrade Can Unregister FTD/FDM from CSSM

Deployments: FTD with FDM

Upgrading from: Version 6.2 through 6.2.2.x

Directly to: Version 6.2.3 through 6.4.0

Upgrading a Firepower Threat Defense device managed by Firepower Device Manager may unregister the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

Procedure

-
- | | |
|---------------|--|
| Step 1 | Click Device , then click View Configuration in the Smart License summary. |
| Step 2 | If the device is not registered, click Register Device . |
-

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.

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 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.2.2.

Table 54: Version 6.2.2 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Security Enhancement: Signed Upgrade Packages, on page 144	Any	Any	6.2.2+
	Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0, on page 144	FTD with FDM	6.2.0 only	6.2.2 through 6.4.0

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.



Note

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.

Upgrade Failure: FDM on ASA 5500-X Series from Version 6.2.0

Deployments: FTD with FDM, running on a lower-memory ASA 5500-X series device

Upgrading from: Version 6.2.0

Directly to: Version 6.2.2 through 6.4.0

If you are upgrading from Version 6.2.0, the upgrade may fail with an error of: `Uploaded file is not a valid system upgrade file`. This can occur even if you are using the correct file.

If this happens, you can try the following workarounds:

- Try again.
- Use the CLI to upgrade.
- Upgrade to 6.2.0.1 first.

Version 6.2.0 Guidelines

This checklist contains upgrade guidelines that are new or specific to Version 6.2.0.

Table 55: Version 6.2.0 New Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Access Control Can Get Latency-Based Performance Settings from SRUs, on page 145	FMC	6.1.0.x	6.2.0 through 6.4.0
	'Snort Fail Open' Replaces 'Failsafe' on FTD , on page 146	FTD with FMC	6.1.0.x	6.2.0 through 6.4.0
	IAB 'All Applications' Option Removed on Upgrade, on page 146	FMC	6.1.0.3 or later patch	6.2.0 only
	URL Filtering Sub-site Lookups for Low-Memory Devices Disabled on Upgrade , on page 147	Any	6.1.0.1 or later patch	6.2.0 only

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 56: Migrating Failsafe to Snort Fail Open

Version 6.1 Failsafe	Version 6.2 Snort Fail Open	Behavior
Disabled (default behavior)	Busy: Disabled Down: Enabled	New and existing connections drop when the Snort process is busy and pass without inspection when the Snort process is down.
Enabled	Busy: Enabled Down: Enabled	New and existing connections pass without inspection when the Snort process is busy or down.

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

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 *deleted*. 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:

- ASA 5512-X, 5515-X, 5525-X

Support is reintroduced in Version 6.2.0.1.

Version 6.1.0 Guidelines

STIG Mode Changed to UCAPL Mode

Deployments: Firepower Management Center

In Version 6.1.0, 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.

Patch Guidelines by Version

These checklists contain important upgrade guidelines and warnings for Firepower patches.

Version 6.7.x.x Guidelines

This checklist contains upgrade guidelines for Version 6.7.x patches.

Table 57: Version 6.7.x.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 124	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases

Version 6.6.x.x Guidelines

This checklist contains upgrade guidelines for Version 6.6.x patches.

Table 58: Version 6.6.x.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: FMC with Email Alerting for Intrusion Events, on page 124	FMC	6.2.3 through 6.7.0.x	6.7.0 6.6.0, 6.6.1, or 6.6.3 All patches to these releases
	Version 6.6.0.1 FTD Upgrade with FDM Suspends HA, on page 148	FTD with FDM	6.6.0	6.6.0.1

Version 6.6.0.1 FTD Upgrade with FDM Suspends HA

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

Upgrading from: Version 6.6.0

Directly to: Version 6.6.0.1

Related bug: [CSCvv45500](#)

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

FMC deployments are not affected.

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

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

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

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

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

Version 6.4.0.x Guidelines

This checklist contains upgrade guidelines for Version 6.4.0 patches.

Table 59: Version 6.4.0.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 134	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0

Version 6.3.0.x Guidelines

This checklist contains upgrade guidelines for Version 6.3.0 patches.

Table 60: Version 6.3.0.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Upgrade Failure: Insufficient Disk Space on Container Instances, on page 134	Firepower 4100/9300	6.3.0 through 6.4.0.x	6.3.0.1 through 6.5.0

Version 6.2.3.x Guidelines

This checklist contains upgrade guidelines for Version 6.2.3 patches.

Table 61: Version 6.2.3.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Version 6.2.3.10 FTD Upgrade with CC Mode Causes FSIC Failure, on page 150	FTD	6.2.3 through 6.2.3.9	6.2.3.10 only
	Version 6.2.3.3 FTD Device Cannot Switch to Local Management, on page 150	FTD with FMC	6.2.3 through 6.2.3.2	6.2.3.3
	Upgrade Can Unregister FTD/FDM from CSSM, on page 150	FTD with FDM	6.2.3 through 6.2.3.1	6.2.3.2 through 6.2.3.5

✓	Guideline	Platforms	Upgrading From	Directly To
	Hotfix Before Upgrading Version 6.2.3-88 FMCs, on page 151	FMC	6.2.3-88	6.2.3.1 through 6.2.3.3

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, the 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 with 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.

Upgrade Can Unregister FTD/FDM from CSSM

Deployments: FTD with FDM

Upgrading from: Version 6.2.3 or 6.2.3.1

Directly to: 6.2.3.2 through 6.2.3.5

Upgrading a Firepower Threat Defense device managed by Firepower Device Manager may unregister the device from the Cisco Smart Software Manager. After the upgrade completes, check your license status.

Procedure

- Step 1** Click **Device**, then click **View Configuration** in the Smart License summary.
- Step 2** If the device is not registered, click **Register Device**.

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 6.2.0.x Guidelines

This checklist contains upgrade guidelines for Version 6.2.0 patches.

Table 62: Version 6.2.0.x Guidelines

✓	Guideline	Platforms	Upgrading From	Directly To
	Apply Hotfix BH to Version 6.2.0.3 FMCs, on page 151	FMC	6.2.0 through 6.2.0.2	6.2.0.3 only

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](#).

Date-Based Guidelines

Sometimes Cisco issues date-based upgrade guidelines and warnings.

Expired CA Certificates for Dynamic Analysis

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.



Note

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.

This 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.

Table 63: Patches and Hotfixes with New CA Certificates

Versions with Old Cert	First Patch with New Cert	Hotfix with New Cert	
6.2.3 through 6.2.3.3	6.2.3.4	Hotfix G	FTD devices
		Hotfix H	FMC
6.2.2 through 6.2.2.3	6.2.2.4	Hotfix BN	All platforms
6.2.1	None. You must upgrade.	None. You must upgrade.	
6.2.0 through 6.2.0.5	6.2.0.6	Hotfix BX	FTD devices
		Hotfix BW	FMC
6.1.0 through 6.1.0.6	6.1.0.7	Hotfix EM	All platforms
6.0.x	None. You must upgrade.	None. You must upgrade.	



CHAPTER 8

ASA Upgrade Guidelines

Before you upgrade, check for migrations and any other guidelines.

- [Version-Specific Guidelines and Migrations, on page 153](#)
- [Clustering Guidelines, on page 163](#)
- [Failover Guidelines, on page 165](#)
- [Additional Guidelines, on page 166](#)

Version-Specific Guidelines and Migrations

Depending on your current version, you might experience one or more configuration migrations, and have to consider configuration guidelines for all versions between the starting version and the ending version when you upgrade.

9.16 Guidelines

- **SNMPv3 users using MD5 hashing and DES encryption are no longer supported, and the users will be removed when you upgrade to 9.16(1)**—Be sure to change any user configuration to higher security algorithms using the `snmp-server user` command before you upgrade.
- **SSH host key action required in 9.16(1)**—In addition to RSA, we added support for the EDDSA and ECDSA host keys for SSH. The ASA tries to use keys in the following order if they exist: EDDSA, ECDSA, and then RSA. When you upgrade to 9.16(1), the ASA will fall back to using the existing RSA key. However, we recommend that you generate higher-security keys as soon as possible using the **crypto key generate {eddsa | ecdsa}** command. Moreover, if you explicitly configure the ASA to use the RSA key with the **ssh key-exchange hostkey rsa** command, you must generate a key that is 2048 bits or higher. For upgrade compatibility, the ASA will use smaller RSA host keys only when the default host key setting is used. RSA support will be removed in a later release.
- **ssh version command removed in 9.16(1)**—This command has been removed. Only SSH version 2 is supported.
- **SAMLv1 feature removed in 9.16(1)**—Support for SAMLv1 was removed.
- **No support for DH groups 2, 5, and 24 in 9.16(1)**—Support has been removed for the DH groups 2, 5, and 24 in SSL DH group configuration. The `ssl dh-group` command has been updated to remove the command options **group2**, **group5**, and **group24**.

9.15 Guidelines

- **No support in ASA 9.15(1) and later for the ASA 5525-X, ASA 5545-X, and ASA 5555-X**—ASA 9.14(x) is the last supported version. For the ASA FirePOWER module, the last supported version is 6.6.
- **Cisco announces the feature deprecation for Clientless SSL VPN effective with ASA version 9.17(1)**. Limited support will continue on releases prior to 9.17(1). Further guidance will be provided regarding migration options to more robust and modern solutions (for example, remote Duo Network Gateway, AnyConnect, remote browser isolation capabilities, and so on).
- **For the Firepower 1010, invalid VLAN IDs can cause problems**—Before you upgrade to 9.15(1), make sure you are not using a VLAN for switch ports in the range 3968 to 4047. These IDs are for internal use only, and 9.15(1) includes a check to make sure you are not using these IDs. For example, if these IDs are in use after upgrading a failover pair, the failover pair will go into a suspended state. See [CSCvw33057](#) for more information.
- **SAMLv1 feature deprecation**—Support for SAMLv1 is deprecated.
- **Low-Security Cipher Removal in ASA 9.15(1)**—Support for the following less secure ciphers used by IKE and IPsec have been removed:
 - Diffie-Hellman groups: 2 and 24
 - Encryption algorithms: DES, 3DES, AES-GMAC, AES-GMAC-192, AES-GMAC-256, NULL, ESP-3DES, ESP-DES, ESP-MD5-HMAC
 - Hash algorithms: MD5



Note Low-security SSH and SSL ciphers have not yet been removed.

Before you upgrade from an earlier version of ASA to Version 9.15(1), you must update your VPN configuration to use the ciphers supported in 9.15(1), or else the old configuration will be rejected. When the configuration is rejected, one of the following actions will occur, depending on the command:

- The command will use the default cipher.
- The command will be removed.

Fixing your configuration before upgrading is especially important for clustering or failover deployments. For example, if the secondary unit is upgraded to 9.15(1), and the removed ciphers are synced to this unit from the primary, then the secondary unit will reject the configuration. This rejection might cause unexpected behavior, like failure to join the cluster.

IKEv1: The following subcommands are removed:

- **crypto ikev1 policy *priority*:**
 - **hash md5**
 - **encryption 3des**
 - **encryption des**
 - **group 2**

IKEv2: The following subcommands are removed:

- **crypto ikev2 policy *priority*:**
 - **prf md5**
 - **integrity md5**
 - **group 2**
 - **group 24**
 - **encryption 3des**
 - **encryption des**
 - **encryption null**

IPsec: The following subcommands are removed:

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
 - **protocol esp integrity md5**
 - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
 - **set pfs group2 group24**

Crypto Map: The following subcommands are removed:

- **crypto map *name sequence* set pfs group2**
- **crypto map *name sequence* set pfs group24**
- **crypto map *name sequence* set ikev1 phase1-mode aggressive group2**
- **Re-introduction of CRL Distribution Point configuration**—The static CDP URL configuration option, that was removed in 9.13(1), was re-introduced in the **match-certificate** command.
- **Restoration of bypass certificate validity checks option**—The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was restored.

The following subcommands were restored:

- **revocation-check crl none**
- **revocation-check ocsf none**
- **revocation-check crl ocsf none**
- **revocation-check ocsf crl none**

9.14 Guidelines

- **ASDM Cisco.com Upgrade Wizard failure on Firepower 1000 and 2100 in Appliance mode**—The ASDM Cisco.com Upgrade Wizard does not work for upgrading to 9.14 (**Tools > Check for ASA/ASDM Updates**). The wizard can upgrade ASDM from 7.13 to 7.14, but the ASA image upgrade is grayed out. ([CSCvt72183](#)) As a workaround, use one of the following methods:
 - Use **Tools > Upgrade Software from Local Computer** for both ASA and ASDM. Note that the ASDM image (7.14(1)) in the 9.14(1) bundle also has the bug [CSCvt72183](#); you should download the newer 7.14(1.46) image to enable correct functioning of the wizard.
 - Use **Tools > Check for ASA/ASDM Updates** to upgrade to ASDM 7.14 (the version will be 7.14(1.46)); then use the new ASDM to upgrade the ASA image. Note that you may see a **Fatal Installation Error**; in this case, click **OK**. You must then set the boot image manually on the **Configuration > Device Management > System Image/Configuration > Boot Image/Configuration** screen. Save the configuration and reload the ASA.
- **For Failover pairs in 9.14(1)+, the ASA no longer shares SNMP client engine data with its peer.**
- **No support in ASA 9.14(1)+ for cnatAddrBindNumberOfEntries and cnatAddrBindSessionCount OIDs** ([CSCvy22526](#)).
- **Downgrade issue for the Firepower 2100 in Platform mode from 9.13/9.14 to 9.12 or earlier**—For a Firepower 2100 with a fresh installation of 9.13 or 9.14 that you converted to Platform mode: If you downgrade to 9.12 or earlier, you will not be able to configure new interfaces or edit existing interfaces in FXOS (note that 9.12 and earlier only supports Platform mode). You either need to restore your version to 9.13 or later, or you need to clear your configuration using the FXOS erase configuration command. This problem does not occur if you originally upgraded to 9.13 or 9.14 from an earlier release; only fresh installations are affected, such as a new device or a re-imaged device. ([CSCvr19755](#))
- **The tls-proxy keyword, and support for SCCP/Skinny encrypted inspection, was removed** from the **inspect skinny** command.
- **ASDM Upgrade Wizard**—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. Note that ASDM 7.13 and 7.14 did not support the ASA 5512-X, 5515-X, 5585-X, or ASASM; you must upgrade to ASDM 7.13(1.101) or 7.14(1.48) to restore ASDM support.

9.13 Guidelines

- **ASAv requires 2GB memory in 9.13(1) and later**—Beginning with 9.13(1), the minimum memory requirement for the ASAv is 2GB. If your current ASAv runs with less than 2GB of memory, you cannot upgrade to 9.13(1) from an earlier version. You must adjust the memory size before upgrading. See the [ASAv Getting Started Guide](#) for information about the resource allocations (vCPU and memory) supported in version 9.13(1).
- **Downgrade issue for the Firepower 2100 in Platform mode from 9.13 to 9.12 or earlier**—For a Firepower 2100 with a fresh installation of 9.13 that you converted to Platform mode: If you downgrade to 9.12 or earlier, you will not be able to configure new interfaces or edit existing interfaces in FXOS (note that 9.12 and earlier only supports Platform mode). You either need to restore your version to 9.13, or you need to clear your configuration using the FXOS erase configuration command. This problem

does not occur if you originally upgraded to 9.13 from an earlier release; only fresh installations are affected, such as a new device or a re-imaged device. (CSCvr19755)

- **Cluster control link MTU change in 9.13(1)**—Starting in 9.13(1), many cluster control packets are larger than they were in previous releases. The recommended MTU for the cluster control link has always been 1600 or greater, and this value is appropriate. However, if you set the MTU to 1600 but then failed to match the MTU on connecting switches (for example, you left the MTU as 1500 on the switch), then you will start seeing the effects of this mismatch with dropped cluster control packets. Be sure to set all devices on the cluster control link to the same MTU, specifically 1600 or higher.
- **Beginning with 9.13(1), the ASA establishes an LDAP/SSL connection only if one of the following certification criteria is satisfied:**
 - The LDAP server certificate is trusted (exists in a trustpoint or the ASA trustpool) and is valid.
 - A CA certificate from servers issuing chain is trusted (exists in a trustpoint or the ASA trustpool) and all subordinate CA certificates in the chain are complete and valid.
- **Local CA server is removed in 9.13(1)**—When the ASA is configured as local CA server, it can issue digital certificates, publish Certificate Revocation Lists (CRLs), and securely revoke issued certificates. This feature has become obsolete and hence the **crypto ca server** command is removed.
- **Removal of CRL Distribution Point commands**—The static CDP URL configuration commands, namely **crypto-ca-trustpoint crl** and **crl url** were removed with other related logic. The CDP URL was moved to match certificate command.



Note The CDP URL configuration was enhanced to allow multiple instances of the CDP override for a single map (refer [CSCvu05216](#)).

- **Removal of bypass certificate validity checks option**—The option to bypass revocation checking due to connectivity problems with the CRL or OCSP server was removed.

The following subcommands are removed:

- **revocation-check crl none**
- **revocation-check ocsp none**
- **revocation-check crl ocsp none**
- **revocation-check ocsp crl none**

Thus, after an upgrade, any revocation-check command that is no longer supported will transition to the new behavior by ignoring the trailing none.



Note These commands were restored later (refer [CSCtb41710](#)).

- **Low-Security Cipher Deprecation**—Several encryption ciphers used by the ASA IKE, IPsec, and SSH modules are considered insecure and have been deprecated. They will be removed in a later release.

IKEv1: The following subcommands are deprecated:

- **crypto ikev1 policy *priority*:**

- **hash md5**
- **encryption 3des**
- **encryption des**
- **group 2**
- **group 5**

IKEv2: The following subcommands are deprecated:

- **crypto ikev2 policy *priority***

- **integrity md5**
- **prf md5**
- **group 2**
- **group 5**
- **group 24**
- **encryption 3des**
- **encryption des** (this command is still available when you have the DES encryption license only)
- **encryption null**

IPsec: The following commands are deprecated:

- **crypto ipsec ikev1 transform-set *name* esp-3des esp-des esp-md5-hmac**
- **crypto ipsec ikev2 ipsec-proposal *name***
 - **protocol esp integrity md5**
 - **protocol esp encryption 3des aes-gmac aes-gmac- 192 aes-gmac -256 des**
- **crypto ipsec profile *name***
 - **set pfs group2 group5 group24**

SSH: The following commands are deprecated:

- **ssh cipher integrity custom hmac-sha1-96:hmac-md5: hmac-md5-96**
- **ssh key-exchange group dh-group1-sha1**

SSL: The following commands are deprecated:

- **ssl dh-group group2**
- **ssl dh-group group5**
- **ssl dh-group group24**

Crypto Map: The following commands are deprecated:

- **crypto map name sequence set pfs group2**
- **crypto map name sequence set pfs group5**
- **crypto map name sequence set pfs group24**
- **crypto map name sequence set ikev1 phase1-mode aggressive group2**
- **crypto map name sequence set ikev1 phase1-mode aggressive group5**
- **In 9.13(1), Diffie-Hellman Group 14 is now the default** for the **group** command under **crypto ikev1 policy**, **ssl dh-group**, and **crypto ikev2 policy** for IPsec PFS using **crypto map set pfs**, **crypto ipsec profile**, **crypto dynamic-map set pfs**, and **crypto map set ikev1 phase1-mode**. The former default Diffie-Hellman group was Group 2.

When you upgrade from a pre-9.13(1) release, if you need to use the old default (Diffie-Hellman Group 2), then you must *manually* configure the DH group as **group 2** or else your tunnels will default to Group 14. Because group 2 will be removed in a future release, you should move your tunnels to group 14 as soon as possible.

9.12 Guidelines

- **ASDM Upgrade Wizard**—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.
- **SSH security improvements and new defaults in 9.12(1)**—See the following SSH security improvements:
 - SSH version 1 is no longer supported; only version 2 is supported. The **ssh version 1** command will be migrated to **ssh version 2**.
 - Diffie-Hellman Group 14 SHA256 key exchange support. This setting is now the default (**ssh key-exchange group dh-group14-sha256**). The former default was Group 1 SHA1. Make sure that your SSH client supports Diffie-Hellman Group 14 SHA256. If it does not, you may see an error such as "Couldn't agree on a key exchange algorithm." For example, OpenSSH supports Diffie-Hellman Group 14 SHA256.
 - HMAC-SHA256 integrity cipher support. The default is now the high security set of ciphers (hmac-sha1 and hmac-sha2-256 as defined by the **ssh cipher integrity high** command). The former default was the medium set.
- The NULL-SHA TLSv1 cipher is deprecated and removed in 9.12(1)—Because NULL-SHA doesn't offer encryption and is no longer considered secure against modern threats, it will be removed when listing supported ciphers for TLSv1 in the output of **tls-proxy** mode commands/options and **show ssl ciphers all**. The **ssl cipher tlsv1 all** and **ssl cipher tlsv1 custom NULL-SHA** commands will also be deprecated and removed.
- The default trustpool is removed in 9.12(1)—In order to comply with PSB requirement, SEC-AUT-DEFROOT, the "default" trusted CA bundle is removed from the ASA image. As a result, **crypto ca trustpool import default** and **crypto ca trustpool import clean default** commands are also

removed along with other related logic. However, in existing deployments, certificates that were previously imported using these command will remain in place.

- The **ssl encryption** command is removed in 9.12(1)—In 9.3(2) the deprecation was announced and replaced by **ssl cipher**. In 9.12(1), **ssl encryption** is removed and no longer supported.

9.10 Guidelines

- Due to an internal change, the ASDM Upgrade 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.

9.9 Guidelines

- ASA 5506-X memory issues with large configurations on 9.9(2) and later—If you upgrade to 9.9(2) or later, parts of a very large configuration might be rejected due to insufficient memory with the following message: "ERROR: Insufficient memory to install the rules". One option is to enter the **object-group-search access-control** command to improve memory usage for ACLs; your performance might be impacted, however. Alternatively, you can downgrade to 9.9(1).

9.8 Guidelines

- Before upgrading to 9.8(2) or later, FIPS mode requires the failover key to be at least 14 characters—Before you upgrade to 9.8(2) or later in FIPS mode, you must change the **failover key** or **failover ipsec pre-shared-key** to be at least 14 characters long. If your failover key is too short, when you upgrade the first unit, the failover key will be rejected, and both units will become active until you set the failover key to a valid value.
- Do not upgrade to 9.8(1) for ASAv on Amazon Web Services--Due to [CSCve56153](#), you should not upgrade to 9.8(1). After upgrading, the ASAv becomes unreachable. Upgrade to 9.8(1.5) or later instead.

9.7 Guidelines

- Upgrade issue with 9.7(1) to 9.7(1.x) and later for VTI and VXLAN VNI—If you configure both Virtual Tunnel Interfaces (VTIs) and VXLAN Virtual Network Identifier (VNI) interfaces, then you cannot perform a zero downtime upgrade for failover; connections on these interface types will not replicate to the standby unit until both units are on the same version. (CSCve83062)

9.6 Guidelines

- Upgrade impact when upgrading the ASA on the Firepower 9300— Due to license entitlement naming changes on the back-end, when you upgrade to ASA 9.6(1)/FXOS 1.1(4), the startup configuration may not parse correctly upon the initial reload; configuration that corresponds to add-on entitlements is rejected.

For a standalone ASA, after the unit reloads with the new version, wait until all the entitlements are processed and are in an "Authorized" state (**show license all** or **Monitoring > Properties > Smart License**), and simply reload again (**reload** or **Tools > System Reload**) *without* saving the configuration. After the reload, the startup configuration will be parsed correctly.

For a failover pair if you have any add-on entitlements, follow the upgrade procedure in the FXOS release notes, but reset failover after you reload each unit (**failover reset** or **Monitoring > Properties > Failover > Status, Monitoring > Failover > System**, or **Monitoring > Failover > Failover Group**, and then click **Reset Failover**).

For a cluster, follow the upgrade procedure in the FXOS release notes; no additional action is required.

9.5 Guidelines and Migration

- 9.5(2) New Carrier License—The new Carrier license replaces the existing GTP/GPRS license, and also includes support for SCTP and Diameter inspection. For the Firepower 9300 ASA security module, the **feature mobile-sp** command will automatically migrate to the **feature carrier** command.
- 9.5(2) E-mail proxy commands deprecated—In ASA Version 9.5(2), the e-mail proxy commands (**imap4s**, **pop3s**, **smtps**) and subcommands are no longer supported.
- 9.5(2) CSD commands deprecated or migrated—In ASA Version 9.5(2), the CSD commands (**csd image**, **show webvpn csd image**, **show webvpn csd**, **show webvpn csd hostscan**, **show webvpn csd hostscan image**) are no longer supported.

The following CSD commands will migrate: **csd enable** migrates to **hostscan enable**; **csd hostscan image** migrates to **hostscan image**.

- 9.5(2) Select AAA commands deprecated—In ASA Version 9.5(2), these AAA commands and subcommands (**override-account-disable**, **authentication crack**) are no longer supported.
- 9.5(1) We deprecated the following command: **timeout gsn**
- ASA 5508-X and 5516-X upgrade issue when upgrading to 9.5(x) or later—Before you upgrade to ASA Version 9.5(x) or later, if you never enabled jumbo frame reservation then you must check the maximum memory footprint. Due to a manufacturing defect, an incorrect software memory limit might have been applied. If you upgrade to 9.5(x) or later before performing the below fix, then your device will crash on bootup; in this case, you must downgrade to 9.4 using ROMMON ([Load an Image for the ASA 5500-X Series Using ROMMON](#)), perform the below procedure, and then upgrade again.

1. Enter the following command to check for the failure condition:

```
ciscoasa# show memory detail | include Max memory footprint
Max memory footprint      = 456384512
Max memory footprint      = 0
Max memory footprint      = 456384512
```

If a value less than **456,384,512** is returned for "Max memory footprint," then the failure condition is present, and you must complete the remaining steps before you upgrade. If the memory shown is 456,384,512 or greater, then you can skip the rest of this procedure and upgrade as normal.

2. Enter global configuration mode:

```
ciscoasa# configure terminal
```

```
ciscoasa(config)#
```

3. Temporarily enable jumbo frame reservation:

```
ciscoasa(config)# jumbo-frame reservation
WARNING: This command will take effect after the running-config
is saved and the system has been rebooted. Command accepted.
INFO: Interface MTU should be increased to avoid fragmenting
jumbo frames during transmit
```



Note Do not reload the ASA.

4. Save the configuration:

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

5. Disable jumbo frame reservation:

```
ciscoasa(config)# no jumbo-frame reservation
WARNING: This command will take effect after the running-config is saved and
the system has been rebooted. Command accepted.
```



Note Do not reload the ASA.

6. Save the configuration again:

```
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: b511ec95 6c90cadb aaf6b306 41579572
14437 bytes copied in 1.320 secs (14437 bytes/sec)
[OK]
```

7. You can now upgrade to Version 9.5(x) or later.

9.4 Guidelines and Migration

- 9.4(1) Unified Communications Phone Proxy and Intercompany Media Engine Proxy are deprecated—In ASA Version 9.4, the Phone Proxy and IME Proxy are no longer supported.

Clustering Guidelines

There are no special requirements for Zero Downtime Upgrades for ASA clustering with the following exceptions.

**Note**

Zero Downtime *Downgrades* are not officially supported with clustering.

- Firepower 4100/9300 Failover and Clustering hitless upgrade requirements for flow offload—Due to bug fixes in the flow offload feature, some combinations of FXOS and ASA do not support flow offload (see the [Firepower 4100/9300 Compatibility with ASA and FTD](#)). Flow offload is disabled by default for ASA. To perform a Failover or Clustering hitless upgrade when using flow offload, you need to follow the below upgrade paths to ensure that you are always running a compatible combination when upgrading to FXOS 2.3.1.130 or later:

1. Upgrade ASA to 9.8(3) or later
2. Upgrade FXOS to 2.3.1.130 or later
3. Upgrade ASA to your final version

For example, you are on FXOS 2.2.2.26/ASA 9.8(1), and you want to upgrade to FXOS 2.6.1/ASA 9.12(1), then you can:

1. Upgrade ASA to 9.8(4)
2. Upgrade FXOS to 2.6.1
3. Upgrade ASA to 9.12(1)

- Distributed Site-to-Site VPN—Distributed Site-to-Site VPN sessions on a failed unit require up to 30 minutes to stabilize on other units. During this time, additional unit failures might result in lost sessions. Therefore, during a cluster upgrade, to avoid traffic loss, follow these steps. Refer to the FXOS/ASA cluster upgrade procedure so you can integrate these steps into your upgrade task.

1. On the chassis *without* the control unit, disable clustering on one module using the ASA console.

cluster group *name*

no enable

If you are upgrading FXOS on the chassis as well as ASA, save the configuration so clustering will be disabled after the chassis reboots:

write memory

2. Wait for the cluster to stabilize; verify all backup sessions have been created.

show cluster vpn-sessiondb summary

3. Repeat steps 1 and 2 for each module on this chassis.
4. Upgrade FXOS on the chassis using the FXOS CLI or Firepower Chassis Manager.
5. After the chassis comes online, update the ASA image on each module using the FXOS CLI or Firepower Chassis Manager.

6. After the modules come online, re-enable clustering on each module at the ASA console.

cluster group *name*

enable

write memory

7. Repeat steps 1 through 6 on the second chassis, being sure to disable clustering on the data units first, and then finally the control unit.

A new control unit will be chosen from the upgraded chassis.

8. After the cluster has stabilized, redistribute active sessions among all modules in the cluster using the ASA console on the control unit.

cluster redistribute vpn-sessiondb

- Upgrade issue for 9.9(1) and later with clustering—9.9(1) and later includes an improvement in the backup distribution. You should perform your upgrade to 9.9(1) or later as follows to take advantage of the new backup distribution method; otherwise upgraded units will continue to use the old method.
 1. Remove all secondary units from the cluster (so the cluster consists only of the primary unit).
 2. Upgrade 1 secondary unit, and rejoin the cluster.
 3. Disable clustering on the primary unit; upgrade it, and rejoin the cluster.
 4. Upgrade the remaining secondary units, and join them back to the cluster, one at a time.
- Firepower 4100/9300 Cluster Upgrade to ASA 9.8(1) and earlier—When you disable clustering on a data unit (**no enable**), which is part of the upgrade process, traffic directed to that unit can drop for up to three seconds before traffic is redirected to a new owner [[CSCvc85008](#)].
- Zero Downtime Upgrade may not be supported when upgrading to the following releases with the fix for [CSCvb24585](#). This fix moved 3DES from the default (medium) SSL ciphers to the low cipher set. If you set a custom cipher that only includes 3DES, then you may have a mismatch if the other side of the connection uses the default (medium) ciphers that no longer include 3DES.
 - 9.1(7.12)
 - 9.2(4.18)
 - 9.4(3.12)
 - 9.4(4)
 - 9.5(3.2)
 - 9.6(2.4)
 - 9.6(3)
 - 9.7(1)
 - 9.8(1)
- Upgrade issues for fully-qualified domain name (FQDN) ACLs—Due to [CSCuv92371](#), ACLs containing FQDNs might result in incomplete ACL replication to secondary units in a cluster or failover pair. This bug is present in 9.1(7), 9.5(2), 9.6(1), and some interim releases. We suggest that you upgrade to a

version that includes the fix for CSCuy34265: 9.1(7.6) or later, 9.5(3) or later, 9.6(2) or later. However, due to the nature of configuration replication, zero downtime upgrade is not available. See [CSCuy34265](#) for more information about different methods of upgrading.

- Firepower Threat Defense Version 6.1.0 clusters do not support inter-site clustering (you can configure inter-site features using FlexConfig starting in 6.2.0). If you deployed or re-deployed a 6.1.0 cluster in FXOS 2.1.1, and you entered a value for the (unsupported) site ID, then you must remove the site ID (set it to 0) on each unit in FXOS before you upgrade to 6.2.3. Otherwise, the units will not be able to rejoin the cluster after the upgrade. If you already upgraded, change the site ID to 0 on each unit to resolve the issue. See the FXOS configuration guide to view or change the site ID
- Upgrade from 9.0(1) or 9.1(1) (CSCue72961)—Zero Downtime Upgrade is not supported.

Failover Guidelines

There are no special requirements for Zero Downtime Upgrades for failover with the following exceptions:

- For the Firepower 1010, invalid VLAN IDs can cause problems—Before you upgrade to 9.15(1), make sure you are not using a VLAN for switch ports in the range 3968 to 4047. These IDs are for internal use only, and 9.15(1) includes a check to make sure you are not using these IDs. For example, if these IDs are in use after upgrading a failover pair, the failover pair will go into a suspended state. See [CSCvw33057](#) for more information.
- Firepower 4100/9300 Failover and Clustering hitless upgrade requirements for flow offload—Due to bug fixes in the flow offload feature, some combinations of FXOS and ASA do not support flow offload (see the [Firepower 4100/9300 Compatibility with ASA and FTD](#)). Flow offload is disabled by default for ASA. To perform a Failover or Clustering hitless upgrade when using flow offload, you need to follow the below upgrade paths to ensure that you are always running a compatible combination when upgrading to FXOS 2.3.1.130 or later:
 1. Upgrade ASA to 9.8(3) or later
 2. Upgrade FXOS to 2.3.1.130 or later
 3. Upgrade ASA to your final version

For example, you are on FXOS 2.2.2.26/ASA 9.8(1), and you want to upgrade to FXOS 2.6.1/ASA 9.12(1), then you can:

1. Upgrade ASA to 9.8(4)
 2. Upgrade FXOS to 2.6.1
 3. Upgrade ASA to 9.12(1)
- Upgrade issues with 8.4(6), 9.0(2), and 9.1(2)—Due to CSCug88962, you cannot perform a Zero Downtime Upgrade to 8.4(6), 9.0(2), or 9.1(3). You should instead upgrade to 8.4(5) or 9.0(3). To upgrade 9.1(1), you cannot upgrade directly to the 9.1(3) release due to CSCuh25271, so there is no workaround for a Zero Downtime Upgrade; you must upgrade to 9.1(2) before you upgrade to 9.1(3) or later.
 - Upgrade issues for fully-qualified domain name (FQDN) ACLs—Due to [CSCuv92371](#), ACLs containing FQDNs might result in incomplete ACL replication to secondary units in a cluster or failover pair. This bug is present in 9.1(7), 9.5(2), 9.6(1), and some interim releases. We suggest that you upgrade to a version that includes the fix for CSCuy34265: 9.1(7.6) or later, 9.5(3) or later, 9.6(2) or later. However,

due to the nature of configuration replication, zero downtime upgrade is not available. See [CSCuy34265](#) for more information about different methods of upgrading.

- Upgrade issue with 9.7(1) to 9.7(1.x) and later for VTI and VXLAN VNI—If you configure both Virtual Tunnel Interfaces (VTIs) and VXLAN Virtual Network Identifier (VNI) interfaces, then you cannot perform a zero downtime upgrade for failover; connections on these interface types will not replicate to the standby unit until both units are on the same version. (CSCvc83062)
- Before upgrading to 9.8(2) or later, FIPS mode requires the failover key to be at least 14 characters—Before you upgrade to 9.8(2) or later in FIPS mode, you must change the **failover key** or **failover ipsec pre-shared-key** to be at least 14 characters long. If your failover key is too short, when you upgrade the first unit, the failover key will be rejected, and both units will become active until you set the failover key to a valid value.
- Upgrade issue with GTP inspection—There could be some downtime during the upgrade, because the GTP data structures are not replicated to the new node.

Additional Guidelines

- Cisco ASA Clientless SSL VPN Portal Customization Integrity Vulnerability—Multiple vulnerabilities have been fixed for clientless SSL VPN in ASA software, so you should upgrade your software to a fixed version. See <http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20141008-asa> for details about the vulnerability and a list of fixed ASA versions. Also, if you ever ran an earlier ASA version that had a vulnerable configuration, then regardless of the version you are currently running, you should verify that the portal customization was not compromised. If an attacker compromised a customization object in the past, then the compromised object stays persistent after you upgrade the ASA to a fixed version. Upgrading the ASA prevents this vulnerability from being exploited further, but it will not modify any customization objects that were already compromised and are still present on the system.



CHAPTER 9

Time and Disk Space Tests

You must have enough free disk space or the upgrade fails. 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 169](#)
- [About Disk Space Requirements, on page 170](#)
- [Version 7.0.1 Time and Disk Space, on page 171](#)
- [Version 7.0.0.1 Time and Disk Space, on page 171](#)
- [Version 7.0.0 Time and Disk Space, on page 172](#)
- [Version 6.7.0.2 Time and Disk Space, on page 172](#)
- [Version 6.7.0.1 Time and Disk Space, on page 173](#)
- [Version 6.7.0 Time and Disk Space, on page 174](#)
- [Version 6.6.5.1 Time and Disk Space, on page 175](#)
- [Version 6.6.5 Time and Disk Space, on page 176](#)
- [Version 6.6.4 Time and Disk Space, on page 177](#)
- [Version 6.6.3 Time and Disk Space, on page 178](#)
- [Version 6.6.1 Time and Disk Space, on page 179](#)
- [Version 6.6.0.1 Time and Disk Space, on page 179](#)
- [Version 6.6.0 Time and Disk Space, on page 180](#)
- [Version 6.5.0.5 Time and Disk Space, on page 181](#)
- [Version 6.5.0.4 Time and Disk Space, on page 181](#)
- [Version 6.5.0.3 Time and Disk Space, on page 182](#)
- [Version 6.5.0.2 Time and Disk Space, on page 182](#)
- [Version 6.5.0.1 Time and Disk Space, on page 183](#)
- [Version 6.5.0 Time and Disk Space, on page 183](#)
- [Version 6.4.0.13 Time and Disk Space, on page 183](#)
- [Version 6.4.0.12 Time and Disk Space, on page 184](#)
- [Version 6.4.0.11 Time and Disk Space, on page 185](#)
- [Version 6.4.0.10 Time and Disk Space, on page 186](#)
- [Version 6.4.0.9 Time and Disk Space, on page 186](#)
- [Version 6.4.0.8 Time and Disk Space, on page 187](#)
- [Version 6.4.0.7 Time and Disk Space, on page 188](#)
- [Version 6.4.0.6 Time and Disk Space, on page 188](#)
- [Version 6.4.0.5 Time and Disk Space, on page 188](#)
- [Version 6.4.0.4 Time and Disk Space, on page 189](#)

- [Version 6.4.0.3 Time and Disk Space, on page 189](#)
- [Version 6.4.0.2 Time and Disk Space, on page 190](#)
- [Version 6.4.0.1 Time and Disk Space, on page 191](#)
- [Version 6.4.0 Time and Disk Space, on page 191](#)
- [Version 6.3.0.5 Time and Disk Space, on page 192](#)
- [Version 6.3.0.4 Time and Disk Space, on page 192](#)
- [Version 6.3.0.3 Time and Disk Space, on page 193](#)
- [Version 6.3.0.2 Time and Disk Space, on page 193](#)
- [Version 6.3.0.1 Time and Disk Space, on page 194](#)
- [Version 6.3.0 Time and Disk Space, on page 194](#)
- [Version 6.2.3.17 Time and Disk Space, on page 195](#)
- [Version 6.2.3.16 Time and Disk Space, on page 195](#)
- [Version 6.2.3.15 Time and Disk Space, on page 196](#)
- [Version 6.2.3.14 Time and Disk Space, on page 196](#)
- [Version 6.2.3.13 Time and Disk Space, on page 197](#)
- [Version 6.2.3.12 Time and Disk Space, on page 198](#)
- [Version 6.2.3.11 Time and Disk Space, on page 198](#)
- [Version 6.2.3.10 Time and Disk Space, on page 199](#)
- [Version 6.2.3.9 Time and Disk Space, on page 199](#)
- [Version 6.2.3.8 Time and Disk Space, on page 200](#)
- [Version 6.2.3.7 Time and Disk Space, on page 200](#)
- [Version 6.2.3.6 Time and Disk Space, on page 200](#)
- [Version 6.2.3.5 Time and Disk Space, on page 201](#)
- [Version 6.2.3.4 Time and Disk Space, on page 201](#)
- [Version 6.2.3.3 Time and Disk Space, on page 202](#)
- [Version 6.2.3.2 Time and Disk Space, on page 202](#)
- [Version 6.2.3.1 Time and Disk Space, on page 203](#)
- [Version 6.2.3 Time and Disk Space, on page 203](#)
- [Version 6.2.2.5 Time and Disk Space, on page 204](#)
- [Version 6.2.2.4 Time and Disk Space, on page 205](#)
- [Version 6.2.2.3 Time and Disk Space, on page 206](#)
- [Version 6.2.2.2 Time and Disk Space, on page 206](#)
- [Version 6.2.2.1 Time and Disk Space, on page 207](#)
- [Version 6.2.2 Time and Disk Space, on page 207](#)
- [Version 6.2.0.6 Time and Disk Space, on page 208](#)
- [Version 6.2.0.5 Time and Disk Space, on page 209](#)
- [Version 6.2.0.4 Time and Disk Space, on page 209](#)
- [Version 6.2.0.3 Time and Disk Space, on page 210](#)
- [Version 6.2.0.2 Time and Disk Space, on page 210](#)
- [Version 6.2.0.1 Time and Disk Space, on page 211](#)
- [Version 6.2.0 Time and Disk Space, on page 211](#)
- [Version 6.1.0.7 Time and Disk Space, on page 212](#)
- [Version 6.1.0.6 Time and Disk Space, on page 212](#)
- [Version 6.1.0.5 Time and Disk Space, on page 213](#)
- [Version 6.1.0.4 Time and Disk Space, on page 214](#)
- [Version 6.1.0.3 Time and Disk Space, on page 214](#)

- [Version 6.1.0.2 Time and Disk Space, on page 215](#)
- [Version 6.1.0.1 Time and Disk Space, on page 215](#)
- [Version 6.1.0 Time and Disk Space, on page 216](#)
- [Version 6.0.1.4 Time and Disk Space, on page 216](#)
- [Version 6.0.1.3 Time and Disk Space, on page 217](#)
- [Version 6.0.1.2 Time and Disk Space, on page 217](#)
- [Version 6.0.1.1 Time and Disk Space, on page 218](#)

About Time Tests

Time values 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, as follows.

Table 64: Time Test Conditions

Condition	Details
Deployment	Values are from tests in a Firepower Management Center deployment. Raw upgrade times for remotely and locally managed devices are similar, given similar conditions.
Versions	For major and maintenance releases, we test upgrades from all eligible previous major versions. For patches, we test upgrades from the base version.
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	Unless otherwise noted, we test on standalone devices. In a high availability or clustered configuration, devices upgrade one at a time to preserve continuity of operations, with each device operating in maintenance mode while it upgrades. Upgrading a device pair or entire cluster, therefore, takes longer than upgrading a standalone device.
Configurations	We test on appliances with minimal configurations and traffic load. Upgrade time can increase with the complexity of your configurations, size of event databases, and whether/how those things are affected by the upgrade. For example, if you use a lot of access control rules and the upgrade needs to make a backend change to how those rules are stored, the upgrade can take longer.

Condition	Details
Components	<p>Values represent <i>only</i> the time it takes for the software upgrade script to run. This does not include:</p> <ul style="list-style-type: none"> • Operating system upgrades. • Transferring upgrade packages. • Readiness checks. • VDB and intrusion rule (SRU/LSP) updates. • Deploying configurations. • Reboots, although reboot time may be provided separately.

About Disk Space Requirements

Space estimates are the *largest* reported for all software 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).

Values represent *only* the space needed to upload and run the software upgrade script. They do not include values for operating system upgrades, VDB or intrusion rule (SRU/LSP) updates, and so on.



Note

When you use the Firepower Management Center to upgrade a managed device, the Firepower Management Center requires additional disk space in /Volume for the device upgrade package (unless you configure an internal web server where your devices can get the package; requires Firepower Threat Defense Version 6.6.0+) .

Checking Disk Space

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

To check disk space:

- Firepower Management Center and its managed devices: Use the **System > Monitoring > Statistics** page on the FMC. After you select the appliance you want to check, under Disk Usage, expand the By Partition details.
- Firepower Threat Defense with Firepower Device Manager: Use the **show disk** CLI command.

Version 7.0.1 Time and Disk Space

Table 65: Version 7.0.1 Time and Disk Space

Platform		Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
Firepower 1000 series		—	7 GB in /ngfw	850 MB	17 min	25 min
Firepower 2100 series		—	6.6 GB in /ngfw	900 MB	12 min	16 min
Firepower 4100 series		—	6.9 GB in /ngfw	800 MB	12 min	11 min
Firepower 9300		—	6.8 GB in /ngfw	800 MB	16 min	10 min
ASA 5500-X series with FTD	from Version 6.4.0–6.6.0	6 GB in /home	944 KB in /ngfw	1GB	17 min	18 min
	from Version 6.7.0	4 GB in /ngfw/Volume	208 KB in /ngfw			
	from Version 7.0.0	5.4 GB in /ngfw/var	320 MB in /ngfw/bin			
FTDv: VMware 6.5	from Version 6.4.0–6.6.0	5.3 GB in /home	944 KB in /ngfw	1 GB	18 min	18 min
	from Version 6.7.0	4.7 GB in /ngfw/Volume	200 KB in /ngfw			
	from Version 7.0.0	4.2 GB in /ngfw/var	175 MB in /ngfw/bin			

Version 7.0.0.1 Time and Disk Space

Table 66: Version 7.0.0.1 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time from 7.0.0	Reboot Time
Firepower 1000 series	720 MB in /ngfw	47 MB	8 min	9 min
Firepower 2100 series	710 MB in /ngfw	42 MB	6 min	10 min
Firepower 4100 series	800 MB in /ngfw	47 MB	4 min	6 min
Firepower 9300	860 MB in /ngfw	47 MB	4 min	32 min

Platform	Local Space	Space on FMC	Upgrade Time from 7.0.0	Reboot Time
ASA 5500-X series with FTD	470 MB in /ngfw/var 170 MB in /ngfw	54 MB	6 min	10 min
FTDv: VMware 6.5	490 MB in /ngfw/var 160 MB in /ngfw	54 MB	4 min	4 min

Version 7.0.0 Time and Disk Space

Table 67: Version 7.0.0 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time	Reboot Time
Firepower 1000 series	420 MB in /ngfw/var 7.6 GB	890 MB	12 min	14 min
Firepower 2100 series	480 MB in /ngfw/var 7.7 GB in /ngfw	950 MB	11 min	13 min
Firepower 4100 series	40 MB in /ngfw/var 8.4 GB in /ngfw	830 MB	8 min	9 min
Firepower 9300	45 MB in /ngfw/var 11.1 GB in /ngfw	830 MB	11 min	11 min
ASA 5500-X series with FTD	5.3 GB in /ngfw/var 95 KB in /ngfw	1.1 GB	25 min	12 min
FTDv	6.6 GB in /ngfw/var 23 KB in /ngfw	1.1 GB	11 min	6 min

Version 6.7.0.2 Time and Disk Space

Table 68: Version 6.7.0.2 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time from 6.7.0	Reboot Time
FMC	2.3 GB in /var 20 MB in /	—	35 min	7 min

Platform	Local Space		Space on FMC	Upgrade Time from 6.7.0	Reboot Time
FMCv: VMware 6.0	2.4 GB	in /var	—	28 min	2 min
	23 MB	in /			
Firepower 1000 series	3 GB	in /ngfw	610 MB	8 min	13 min
Firepower 2100 series	3GB	in /ngfw	660 MB	6 min	14 min
Firepower 9300	2.6 GB	in /ngfw	410 MB	5 min	7 min
Firepower 4100 series	2.4 GB	in /ngfw	410 MB	4 min	7 min
Firepower 4100 series container instance	2.3 GB	in /	410 MB	5 min	4 min
ASA 5500-X series with FTD	2.2 GB	in /ngfw/Volume	370 MB	10 min	7 min
	110 MB	in /ngfw			
ISA 3000 with FTD	2.3 GB	in /ngfw/Volume	370 MB	17 min	9 min
	110 MB	in /ngfw			
FTDv: VMware 6.0	2.2 GB	in /ngfw/Volume	370 MB	6 min	4 min
	110 MB	in /ngfw			
FTDv: KVM	2.2 GB	in /ngfw/Volume	370 MB	6 min	8 min
	110 MB	in /ngfw			
ASA FirePOWER	3 GB	in /var	430 MB	73 min	4 min
	21 MB	in /			
NGIPSv: VMware 6.0	930 MB	in /var	290 MB	5 min	3 min
	19 MB	in /			

Version 6.7.0.1 Time and Disk Space

Table 69: Version 6.7.0.1 Time and Disk Space

Platform	Local Space		Space on FMC	Upgrade Time from 6.7.0	Reboot Time
FMC	1.8 GB	in /var	—	32 min	7 min
	20 MB	in /			
FMCv: VMware 6.0	1.4 GB	in /var	—	28 min	5 min
	23 MB	in /			

Platform	Local Space		Space on FMC	Upgrade Time from 6.7.0	Reboot Time
Firepower 1000 series	1.4 GB	in /ngfw	340 MB	7 min	12 min
Firepower 2100 series	1.4 GB	in /ngfw	400 MB	7 min	12 min
Firepower 9300	710 MB	in /ngfw	130 MB	5 min	7 min
Firepower 4100 series	700 MB	in /ngfw	130 MB	4 min	5 min
Firepower 4100 series container instance	480 MB	in /	130 MB	5 min	2 min
ASA 5500-X series with FTD	540 MB	in /ngfw/Volume	88 MB	10 min	12 min
	110 MB	in /ngfw			
ISA 3000 with FTD	540 MB	in /ngfw/Volume	88 MB	13 min	7 min
	110 MB	in /ngfw			
FTDv: VMware 6.0	530 MB	in /ngfw/Volume	88 MB	6 min	4 min
	110 MB	in /ngfw			
FTDv: KVM	550 MB	in /ngfw/Volume	88 MB	7 min	3 min
	110 MB	in /ngfw			
ASA FirePOWER	1.2 GB	in /var	41 MB	66 min	2 min
	21 MB	in /			
NGIPSv: VMware 6.0	82 MB	in /var	9 MB	6 min	3 min
	18 MB	in /			

Version 6.7.0 Time and Disk Space

Table 70: Version 6.7.0 Time and Disk Space

Platform	Space on /var	Space on /	Space on FMC	Upgrade Time	Reboot Time
FMC	13.6 GB	70 MB	—	46 min	9 min
FMCv: VMware 6.0	15.5 GB	64 MB	—	35 min	8 min
Firepower 1000 series	430 MB	11 GB	2 GB	17 min	16 min
Firepower 2100 series	500 MB	11 GB	1.1 GB	15 min	16 min
Firepower 9300	64 MB	11.1 GB	1.1 GB	13 min	12 min

Platform	Space on /var	Space on /	Space on FMC	Upgrade Time	Reboot Time
Firepower 4100 series	10 MB	10 GB	1.1 GB	10 min	12 min
Firepower 4100 series container instance	8 MB	9.5 GB	1.1 GB	10 min	9 min
ASA 5500-X series with FTD	8.7 GB	96 KB	1.1 GB	26 min	13 min
FTDv: VMware 6.0	8.1 GB	26 KB	1.1 GB	14 min	18 min
ASA FirePOWER	10.3 GB	64 MB	1.3 GB	62 min	11 min
NGIPSv: VMware 6.0	5.5 GB	54 MB	840 MB	10 min	6 min

Version 6.6.5.1 Time and Disk Space

Table 71: Version 6.6.5.1 Time and Disk Space

Platform	Space in /Volume	Space in /	Space on FMC	Upgrade Time	Reboot Time
FMC	2,2 GB in /var	20 MB in /	—	34 min	8 min
FMCv: VMware 6.0	2.2 GB in /var	23 MB in /	—	28 min	6 min
Firepower 1000 series	—	1.5 GB in /ngfw	340 MB	8 min	12 min
Firepower 2100 series	—	1.4 GB in /ngfw	370 MB	6 min	11 min
Firepower 9300	—	770 MB in /ngfw	140 MB	5 min	8 min
Firepower 4100 series	—	790 MB in /ngfw	140 MB	5 min	8 min
Firepower 4100 series container instance	—	730 MB in /ngfw	140 MB	6 min	5 min
ASA 5500-X series with FTD	590 MB in /home	120 MB in /ngfw	85 MB	9 min	9 min
FTDv: VMware 6.0	590 MB in /home	120 MB in /ngfw	85 MB	6 min	5 min
ASA FirePOWER	1.7 GB in /var	21 MB in /	130 MB	69 min	7 min
NGIPSv: VMware 6.0	78 MB in /var	19 MB in /	16 MB	6 min	5 min

Version 6.6.5 Time and Disk Space

Table 72: Version 6.6.5 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time	Reboot Time
FMC	16.5 GB in /var 23 MB in /	—	55 min	14 min
FMCv: VMware 6.0	21 GB in /var 29 MB in /	—	51 min	9 min
Firepower 1000 series	9.7 GB in /ngfw/var 400 MB in /ngfw	1.1 GB	20 min	16 min
Firepower 2100 series	10.2 GB in /ngfw/var 450 MB in /ngfw	1.1 GB	17 min	15 min
Firepower 9300	10.2 GB in /ngfw/var 11 MB in /ngfw	1.1 GB	12 min	10 min
Firepower 4100 series	10.1 MB in /ngfw/var 10 MB in /ngfw	1.1 GB	10 min	11 min
Firepower 4100 series container instance	10.7 GB in /ngfw/var 11 MB in /ngfw	1.1 GB	12 min	7 min
ASA 5500-X series with FTD	8.6 GB in /ngfw/var 756 KB in /ngfw	1.3 GB	22 min	30 min
FTDv: VMware 6.0	9.1 GB in /ngfw/var 756 KB in /ngfw	1.3 GB	12 min	21 min
ASA FirePOWER	12 GB in /var 26 MB in /	1.4 GB	65 min	25 min
NGIPSv: VMware 6.0	7.4 GB in /var 21 MB in /	910 MB	12 min	21 min

Version 6.6.4 Time and Disk Space

Table 73: Version 6.6.4 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time	Reboot Time
FMC	15.1 GB in /var 23 MB in /	—	60 min	28 min
FMCv: VMware 6.0	23.7 GB in /var 29 MB in /	—	43 min	8 min
Firepower 1000 series	9.7 GB in /ngfw/var 400 MB in /ngfw	1 GB	21 min	16 min
Firepower 2100 series	10.1 GB in /ngfw/var 450 MB in /ngfw	1 GB	21 min	13 min
Firepower 9300	10.1 GB in /ngfw/var 11 MB in /ngfw	970 MB	14 min	10 min
Firepower 4100 series	8.9 GB in /ngfw/var 11 MB in /ngfw	970 MB	11 min	9 min
Firepower 4100 series container instance	10.9 GB in /ngfw/var 10 MB in /ngfw	970 MB	10 min	7 min
ASA 5500-X series with FTD	8.5 GB in /ngfw/var 756 KB in /ngfw	1.2 GB	20 min	19 min
FTDv: VMware 6.0	7.7 GB in /ngfw/var 756 KB in /ngfw	1.2 GB	19 min	12 min
ASA FirePOWER	11.4 GB in /var 26 MB in /	1.3 GB	59 min	16 min
NGIPSv: VMware 6.0	7.4 GB in /var 21 MB in /	870 MB	13 min	8 min

Version 6.6.3 Time and Disk Space

Table 74: Version 6.6.3 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time	Reboot Time
FMC	15.1 GB in /var 23 MB in /	—	60 min	28 min
FMCv: VMware 6.0	23.7 GB in /var 29 MB in /	—	43 min	8 min
Firepower 1000 series	9.7 GB in /ngfw/var 400 MB in /ngfw	1 GB	21 min	16 min
Firepower 2100 series	10.1 GB in /ngfw/var 450 MB in /ngfw	1 GB	21 min	13 min
Firepower 9300	10.1 GB in /ngfw/var 11 MB in /ngfw	970 MB	14 min	10 min
Firepower 4100 series	8.9 GB in /ngfw/var 11 MB in /ngfw	970 MB	11 min	9 min
Firepower 4100 series container instance	10.9 GB in /ngfw/var 10 MB in /ngfw	970 MB	10 min	7 min
ASA 5500-X series with FTD	8.5 GB in /ngfw/var 756 KB in /ngfw	1.2 GB	20 min	19 min
FTDv: VMware 6.0	7.7 GB in /ngfw/var 756 KB in /ngfw	1.2 GB	19 min	12 min
ASA FirePOWER	11.4 GB in /var 26 MB in /	1.3 GB	59 min	16 min
NGIPSv: VMware 6.0	7.4 GB in /var 21 MB in /	870 MB	13 min	8 min

Version 6.6.1 Time and Disk Space

Table 75: Version 6.6.1 Time and Disk Space

Platform	Space on /var	Space on /	Space on FMC	Upgrade Time	Reboot Time
FMC	18.6 GB	23 MB	—	54 min	14 min
FMCv: VMware 6.0	15.8 GB	58 MB	—	56 min	13 min
Firepower 1000 series	10.8 GB	400 MB	1.1 GB	20 min	17 min
Firepower 2100 series	10.9 GB	450 MB	1.1 GB	16 min	21 min
Firepower 9300	9.8 GB	11 MB	1 GB	15 min	15 min
Firepower 4100 series	9.7 GB	10 MB	1 GB	15 min	14 min
Firepower 4100 series container instance	11.2 GB	9 MB	1 GB	10 min	13 min
ASA 5500-X series with FTD	9.3 GB	1 MB	1.2 GB	21 min	24 min
FTDv: VMware 6.0	9.3 GB	1 MB	1.2 GB	18 min	19 min
ASA FirePOWER	12.3 GB	26 MB	1.4 GB	72 min	23 min
NGIPSv: VMware 6.0	7.1 GB	54 MB	860 MB	14 min	20 min

Version 6.6.0.1 Time and Disk Space

In this table, the upgrade time includes reboot.

Table 76: Version 6.6.0.1 Time and Disk Space

Platform	Space on /var	Space on /	Space on FMC	Upgrade Time from 6.6.0
FMC	31 MB	20 MB	—	22 min
FMCv: VMware 6.0	1.1 GB	23 MB	—	17 min
Firepower 1000 series	450 MB	450 MB	240 MB	21 min
Firepower 2100 series	260 MB	260 MB	270 MB	17 min
Firepower 9300	460 MB	460 MB	46 MB	33 min
Firepower 4100 series	470 MB	470 MB	46 MB	11 min
ASA 5500-X series with FTD	440 MB	120 MB	46 MB	17 min

Platform	Space on /var	Space on /	Space on FMC	Upgrade Time from 6.6.0
ISA 3000 with FTD	440 MB	120 MB	46 MB	21 min
FTDv: VMware 6.0	430 MB	120 MB	46 MB	11 min
ASA FirePOWER	80 MB	20 MB	15 MB	18 min
NGIPSv: VMware 6.0	64 MB	28 MB	15 MB	9 min

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 77: Version 6.6.0 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time	Reboot Time
FMC	16.5 GB in /var 71 MB in /	—	46 min	15 min
FMCv: VMware 6.0	16.7 GB in /var 57 MB in /	—	36 min	7 min
Firepower 1000 series	410 MB in /ngfw/var 11.5 GB in /ngfw	1.1 GB	20 min	17 min
Firepower 2100 series	470 MB in /ngfw/var 10.3 GB in /ngfw	1 GB	14 min	14 min
Firepower 9300	64 MB in /ngfw/var 8.7 GB in /ngfw	980 MB	15 min	12 min
Firepower 4100 series	61 MB in /ngfw/var 9.3 GB in /ngfw	980 MB	11 min	9 min
Firepower 4100 series container instance	46 MB in /ngfw/var 11.3 GB in /ngfw	980 MB	11 min	6 min
ASA 5500-X series with FTD	8.7 GB in /ngfw/var 70 KB in /ngfw	1.2 GB	23 min	26 min

Platform	Local Space	Space on FMC	Upgrade Time	Reboot Time
FTDv: VMware 6.0	8.7 GB in /ngfw/var 70 KB in /ngfw	1.2 GB	14 min	17 min
ASA FirePOWER	11.4 GB in /var 63 MB in /	1.4 GB	93 min	10 min
NGIPSv: VMware 6.0	6.1 GB in /var 53 MB in /	860 MB	10 min	5 min

Version 6.5.0.5 Time and Disk Space

Table 78: Version 6.5.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.5.0	Reboot Time
FMC	4.4 GB	28 MB	—	47 min	8 min
FMCv: VMware 6.0	4.2 GB	25 MB	—	36 min	4 min
Firepower 1000 series	2.6 GB	2.6 GB	510 MB	9 min	11 min
Firepower 2100 series	2.5 GB	2.5 GB	530 MB	7 min	10 min
Firepower 4100 series	2.6 GB	2.6 GB	360 MB	5 min	8 min
Firepower 9300	2.6 GB	2.6 GB	360 MB	5 min	8 min
ASA 5500-X series with FTD	1.9 GB	120 MB	310 MB	9 min	8 min
FTDv: VMware 6.0	2.2 GB	120 MB	310 MB	7 min	6 min
ASA FirePOWER	4.3 GB	32 MB	610 MB	52 min	6 min
NGIPSv: VMware 6.0	2.2 GB	420 MB	470 MB	6 min	4 min

Version 6.5.0.4 Time and Disk Space

Table 79: Version 6.5.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.5.0
Firepower 1000 series	2.6 GB	2.6 GB	500 MB	20 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.5.0
Firepower 2100 series	2.5 GB	2.5 GB	530 MB	18 min
Firepower 4100 series	2.5 GB	2.5 GB	360 MB	13 min
Firepower 9300	2.5 GB	2.5 GB	360 MB	17 min
ASA 5500-X series with FTD	1.9 GB	110 MB	310 MB	16 min
FTDv: VMware 6.0	1.9 GB	110 MB	310 MB	9 min
ASA FirePOWER	2.6 GB	20 MB	340 MB	72 min
NGIPSv: VMware 6.0	740 MB	20 MB	230 MB	8 min

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 6.5.0.2 Time and Disk Space

Table 80: Version 6.5.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.5.0
FMC	2.6 GB	20 MB	—	42 min
FMCv: VMware 6.0	2.7 GB	23 MB	—	34 min
Firepower 1000 series	2.5 GB	2.5 GB	480 MB	12 min
Firepower 2100 series	2.3 GB	2.3 GB	500 MB	17 min
Firepower 4100 series	2.3 GB	2.3 GB	340 MB	13 min
Firepower 9300	2.3 GB	2.3 GB	340 MB	17 min
ASA 5500-X series with FTD	1.9 GB	110 MB	280 MB	22 min
FTDv: VMware 6.0	1.7 GB	110 MB	280 MB	10 min
ASA FirePOWER	2.5 GB	20 MB	320 MB	56 min
NGIPSv: VMware 6.0	680 MB	18 MB	210 MB	9 min

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 81: Version 6.5.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	18.6 GB	24 MB	—	47 min
FMCv: VMware 6.0	18.7 GB	30 MB	—	35 min
Firepower 1000 series	1.0 GB	11.3 GB	1.1 GB	10 min
Firepower 2100 series	1.1 GB	12.3 GB	1.0 GB	12 min
Firepower 4100 series	20 MB	10.8 GB	990 MB	8 min
Firepower 9300	23 MB	10.9 GB	990 MB	8 min
ASA 5500-X series with FTD	10.4 GB	120 KB	1.1 GB	17 min
FTDv: VMware 6.0	10 GB	120 KB	1.1 GB	10 min
ASA FirePOWER	12.2 GB	26 MB	1.3 GB	81 min
NGIPSv: VMware 6.0	6.6 GB	22 MB	870 MB	9 min

Version 6.4.0.13 Time and Disk Space

Table 82: Version 6.4.0.13 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.8 GB in /var 170 MB in /	—	34 min	8 min
FMCv: VMware 6.0	3.9 GB in /var 170 MB in /	—	21 min	4 min
Firepower 1000 series	3.0 GB in /ngfw	540 MB	11 min	13 min
Firepower 2100 series	2.6 GB in /ngfw	510 MB	8 min	12 min

Platform	Local Space	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
Firepower 4100 series	2.5 GB in /ngfw	450 MB	4 min	9 min
Firepower 9300	2.5 GB in /ngfw	450 MB	4 min	9 min
ASA 5500-X series with FTD	2.0 GB in /home 110 MB in /ngfw	295 MB	12 min	9 min
FTDv: VMware 6.0	1.9 GB in /home 110 MB in /ngfw	295 MB	7 min	5 min
Firepower 7000/8000 series	3.7 GB in /var 170 MB in /	670 MB	11 min	14 min
ASA FirePOWER	4.2 GB in /var 38 MB in /	660 MB	43 min	8 min
NGIPSv: VMware 6.0	2.2 GB in /var 170 MB in /	460 MB	6 min	4 min

Version 6.4.0.12 Time and Disk Space

Table 83: Version 6.4.0.12 Time and Disk Space

Platform	Local Space	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.8 GB in /var 170 MB in /	—	25 min	8 min
FMCv: VMware 6.0	3.8 GB in /var 170 MB in /	—	27 min	4 min
Firepower 1000 series	2.9 GB in /ngfw	530 MB	10 min	13 min
Firepower 2100 series	2.5 GB in /ngfw	510 MB	8 min	32 min
Firepower 4100 series	2.5 GB in /ngfw	440 MB	4 min	9 min
Firepower 9300	2.5 GB in /ngfw	440 MB	4 min	8 min
ASA 5500-X series with FTD	1.9 GB in /home 110 MB in /ngfw	290 MB	12 min	40 min

Platform	Local Space	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FTDv: VMware 6.0	1.9 GB in /home 110 MB in /ngfw	290 MB	7 min	5 min
Firepower 7000/8000 series	3.7 GB in /var 170 MB in /	660 MB	10 min	15 min
ASA FirePOWER	4.2 GB in /var 37 MB in /	600 MB	47 min	51 min
NGIPSv: VMware 6.0	2.2 GB in /var 150 MB in /	460 MB	7 min	5 min

Version 6.4.0.11 Time and Disk Space

Table 84: Version 6.4.0.11 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.8 GB	170 MB	—	30 min	8 min
FMCv: VMware 6.0	4.1 GB	170 MB	—	27 min	7 min
Firepower 1000 series	3.0 GB	3.0 GB	530 MB	14 min	9 min
Firepower 2100 series	2.5 GB	2.5 GB	510 MB	9 min	6 min
Firepower 4100 series	1.8 GB	1.8 GB	310 MB	8 min	7 min
Firepower 9300	1.8 GB	1.8 GB	310 MB	9 min	9 min
ASA 5500-X series with FTD	1.6 GB	110 MB	290 MB	12 min	12 min
FTDv: VMware 6.0	4.4 GB	170 MB	290 MB	28 min	4 min
Firepower 7000/8000 series	3.6 GB	170 MB	680 MB	11 min	97 min
ASA FirePOWER	4.2 GB	36 MB	630 MB	54 min	51 min
NGIPSv: VMware 6.0	2.4 GB	150 MB	470 MB	11 min	15 min

Version 6.4.0.10 Time and Disk Space

Table 85: Version 6.4.0.10 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.8 GB	170 MB	—	30 min	8 min
FMCv: VMware 6.0	4.1 GB	170 MB	—	27 min	7 min
Firepower 1000 series	2.9 GB	2.9 GB	560 MB	11 min	14 min
Firepower 2100 series	2.5 GB	2.5 GB	530 MB	8 min	13 min
Firepower 4100 series	1.8 GB	1.8 GB	330 MB	5 min	11 min
Firepower 9300	1.8 GB	1.8 GB	330 MB	5 min	17 min
ASA 5500-X series with FTD	1.9 GB	110 MB	310 MB	12 min	31 min
FTDv: VMware 6.0	2.0 GB	110 MB	310 MB	8 min	8 min
Firepower 7000/8000 series	3.6 GB	170 MB	680 MB	11 min	97 min
ASA FirePOWER	4.2 GB	36 MB	630 MB	54 min	51 min
NGIPSv: VMware 6.0	2.4 GB	150 MB	470 MB	11 min	15 min

Version 6.4.0.9 Time and Disk Space

Table 86: Version 6.4.0.9 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
FMC	3.7 GB	170 MB	—	41 min	10 min
FMCv: VMware 6.0	3.7 GB	170 MB	—	28 min	6 min
Firepower 1000 series	2.9 GB	2.9 GB	530 MB	11 min	14 min
Firepower 2100 series	2.6 GB	2.6 GB	510 MB	10 min	13 min
Firepower 4100 series	1.8 GB	1.8 GB	310 MB	4 min	10 min
Firepower 9300	1.8 GB	1.8 GB	310 MB	4 min	10 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0	Reboot Time
ASA 5500-X series with FTD	1.9 GB	290 MB	290 MB	12 min	42 min
FTDv: VMware 6.0	1.9 GB	290 MB	290 MB	7 min	9 min
Firepower 7000/8000 series	3.7 GB	170 MB	650 MB	20 min	6 min
ASA FirePOWER	4.2 GB	36 MB	600 MB	48 min	48 min
NGIPSv: VMware 6.0	2.1 GB	150 MB	450 MB	6 min	4 min

Version 6.4.0.8 Time and Disk Space

Table 87: Version 6.4.0.8 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	5.0 GB	170 MB	—	44 min
FMCv: VMware 6.0	5.1 GB	170 MB	—	32 min
Firepower 1000 series	3.0 GB	3.0 GB	530 MB	18 min
Firepower 2100 series	2.5 GB	2.5 GB	510 MB	18 min
Firepower 4100 series	1.8 GB	1.8 GB	310 MB	14 min
Firepower 9300	2.0 GB	2.0 GB	310 MB	11 min
ASA 5500-X series with FTD	1.8 GB	110 MB	290 MB	17 min
FTDv: VMware 6.0	1.9 GB	110 MB	290 MB	12 min
Firepower 7000/8000 series	3.7 GB	190 MB	650 MB	25 min
ASA FirePOWER	2.2 GB	110 MB	590 MB	16 min
NGIPSv: VMware 6.0	2.1 GB	150 MB	450 MB	9 min

Version 6.4.0.7 Time and Disk Space

Table 88: Version 6.4.0.7 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	4.9 GB	170 MB	—	41 min
FMCv: VMware 6.0	5.1 GB	170 MB	—	32 min
Firepower 1000 series	2.9 GB	2.9 GB	530 MB	17 min
Firepower 2100 series	2.4 GB	2.4 GB	500 MB	17 min
Firepower 4100 series	1.7 GB	1.7 GB	310 MB	15 min
Firepower 9300	2.4 GB	2.4 GB	310 MB	12 min
ASA 5500-X series with FTD	1.9 GB	110 MB	290 MB	18 min
FTDv: VMware 6.0	1.8 GB	110 MB	290 MB	9 min
Firepower 7000/8000 series	3.7 GB	190 MB	650 MB	28 min
ASA FirePOWER	4.2 GB	36 MB	590 MB	54 min
NGIPSv: VMware 6.0	2.3 GB	150 MB	450 MB	9 min

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 89: Version 6.4.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	5.0 GB	170 MB	—	39 min
FMCv: VMware 6.0	3.7 GB	170 MB	—	27 min
Firepower 1000 series	2.9 GB	2.9 GB	530 MB	26 min
Firepower 2100 series	2.5 GB	2.5 GB	500 MB	16 min
Firepower 4100 series	1.8 GB	1.8 GB	310 MB	12 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
Firepower 9300	1.8 GB	1.8 GB	310 MB	11 min
ASA 5500-X series with FTD	1.8 GB	110 MB	290 MB	20 min
FTDv: VMware 6.0	1.8 GB	110 MB	290 MB	10 min
Firepower 7000/8000 series	3.6 GB	170 MB	650 MB	26 min
ASA FirePOWER	4.1 GB	36 MB	590 MB	45 min
NGIPSv: VMware 6.0	2.1 GB	150 MB	450 MB	10 min

Version 6.4.0.4 Time and Disk Space

Table 90: Version 6.4.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	4.4 GB	170 MB	—	35 min
FMCv: VMware 6.0	4.8 GB	170 MB	—	31 min
Firepower 1000 series	2.9 GB	2.9 GB	520 MB	28 min
Firepower 2100 series	2.4 GB	2.4 GB	500 MB	10 min
Firepower 4100 series	2.0 GB	2.0 GB	310 MB	12 min
Firepower 9300	1.7 GB	1.7 GB	310 MB	10 min
ASA 5500-X series with FTD	1.8 GB	110 MB	290 MB	29 min
FTDv: VMware 6.0	1.8 GB	110 MB	290 MB	8 min
Firepower 7000/8000 series	3.6 GB	170 MB	650 MB	24 min
ASA FirePOWER	4.2 GB	36 MB	600 MB	55 min
NGIPSv: VMware 6.0	2.1 GB	150 MB	550 MB	10 min

Version 6.4.0.3 Time and Disk Space

Table 91: Version 6.4.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	3.2 GB	24 MB	—	34 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMCv: VMware 6.0	2.5 GB	23 MB	—	25 min
Firepower 1000 series	2.9 GB	2.9 GB	520 MB	22 min
Firepower 2100 series	2.4 GB	2.4 GB	500 MB	19 min
Firepower 4100 series	1.7 GB	1.7 GB	310 MB	12 min
Firepower 9300	1.7 GB	1.7 GB	310 MB	14 min
ASA 5500-X series with FTD	1.8 GB	110 MB	290 MB	18 min
FTDv: VMware 6.0	1.8 GB	110 MB	290 MB	12 min
Firepower 7000/8000 series	1.9 GB	21 MB	370 MB	20 min
ASA FirePOWER	2.5 GB	2.5 GB	320 MB	28 min
NGIPSv: VMware 6.0	690 MB	21 MB	210 MB	8 min

Version 6.4.0.2 Time and Disk Space

Table 92: Version 6.4.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	3.1 GB	24 MB	—	39 min
FMCv: VMware 6.0	2.5 GB	23 MB	—	24 min
Firepower 2100 series	1.9 GB	1.9 GB	480 MB	19 min
Firepower 4100 series	2.3 GB	2.3 GB	290 MB	11 min
Firepower 9300	1.7 GB	1.7 GB	290 MB	11 min
ASA 5500-X series with FTD	1.8 GB	110 MB	270 MB	21 min
FTDv: VMware 6.0	1.2 GB	110 MB	270 MB	10 min
Firepower 7000/8000 series	1.9 GB	36 MB	350 MB	20 min
ASA FirePOWER	2.0 GB	21 MB	300 MB	34 min
NGIPSv: VMware 6.0	630 MB	21 MB	190 MB	10 min

Version 6.4.0.1 Time and Disk Space

Table 93: Version 6.4.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.4.0
FMC	1.8 GB	24 MB	—	50 min
FMCv: VMware 6.0	1.8 GB	23 MB	—	20 min
Firepower 2100 series	1.4 GB	1.4 GB	300 MB	17 min
Firepower 4100 series	1.1 GB	1.1 GB	95 MB	9 min
Firepower 9300	1.1 GB	1.1 GB	95 MB	10 min
ASA 5500-X series with FTD	550 MB	110 MB	76 MB	16 min
FTDv: VMware 6.0	550 MB	110 MB	76 MB	15 min
Firepower 7000/8000 series	59 MB	21 MB	2 MB	14 min
ASA FirePOWER	85 MB	20 MB	2 MB	30 min
NGIPSv: VMware 6.0	45 MB	21 MB	2 MB	10 min

Version 6.4.0 Time and Disk Space

Table 94: Version 6.4.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	13.3 GB	26 MB	—	41 min
FMCv: VMware 6.0	13.6 GB	29 MB	—	30 min
Firepower 2100 series	12 MB	8.9 GB	950 MB	20 min
Firepower 4100 series	10 MB	7.5 GB	920 MB	6 min
Firepower 9300	10 MB	7.7 GB	920 MB	7 min
ASA 5500-X series with FTD	9.0 GB	110 KB	1.1 GB	24 min
FTDv: VMware 6.0	7.5 GB	100 KB	1.1 GB	12 min
Firepower 7000/8000 series	7.7 GB	19 MB	980 MB	34 min
ASA FirePOWER	11.5 GB	22 MB	1.3 GB	66 min
NGIPSv: VMware 6.0	6.5 GB	19 MB	840 MB	16 min

Version 6.3.0.5 Time and Disk Space

Table 95: Version 6.3.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	4.9 GB	200 MB	—	46 min
FMCv: VMware 6.0	4.5 GB	180 MB	—	41 min
Firepower 2100 series	2.3 GB	2.3 GB	480 MB	21 min
Firepower 4100 series	1.6 GB	1.6 GB	280 MB	13 min
Firepower 9300	1.6 GB	1.6 GB	280 MB	17 min
ASA 5500-X series with FTD	1.7 GB	110 MB	270 MB	26 min
FTDv: VMware 6.0	1.7 GB	110 MB	270 MB	17 min
Firepower 7000/8000 series	2.6 GB	210 MB	600 MB	23 min
ASA FirePOWER	3.6 GB	47 MB	540 MB	74 min
NGIPSv: VMware 6.0	2.1 GB	160 MB	440 MB	17 min

Version 6.3.0.4 Time and Disk Space

Table 96: Version 6.3.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	3.4 GB	180 MB	—	34 min
FMCv: VMware 6.0	4.4 GB	180 MB	—	38 min
Firepower 2100 series	2.3 GB	2.3 GB	480 MB	17 min
Firepower 4100 series	1.6 GB	1.6 GB	280 MB	12 min
Firepower 9300	1.8 GB	1.8 GB	280 MB	12 min
ASA 5500-X series with FTD	1.7 GB	110 MB	270 MB	23 min
FTDv: VMware 6.0	1.7 GB	110 MB	270 MB	18 min
Firepower 7000/8000 series	3.3 GB	170 MB	600 MB	21 min
ASA FirePOWER	3.5 GB	31 MB	530 MB	48 min
NGIPSv: VMware 6.0	2.1 GB	160 MB	430 MB	16 min

Version 6.3.0.3 Time and Disk Space

Table 97: Version 6.3.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	3.7 GB	180 MB	—	33 min
FMCv: VMware 6.0	3.2 GB	180 MB	—	24 min
Firepower 2100 series	1.2 GB	1.2 GB	290 MB	18 min
Firepower 4100 series	990 MB	990 MB	99 MB	11 min
Firepower 9300	990 MB	990 MB	99 MB	12 min
ASA 5500-X series with FTD	620 MB	110 MB	79 MB	18 min
FTDv: VMware 6.0	240 MB	110 MB	79 MB	7 min
Firepower 7000/8000 series	2.6 GB	170 MB	400 MB	20 min
ASA FirePOWER	2.9 GB	30 MB	340 MB	45 min
NGIPSv: VMware 6.0	1.5 GB	160 MB	250 MB	4 min

Version 6.3.0.2 Time and Disk Space

Table 98: Version 6.3.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	3.5 GB	180 MB	—	53 min
FMCv: VMware 6.0	3.2 GB	180 MB	—	28 min
Firepower 2100 series	1.2 GB	1.2 GB	100 MB	17 min
Firepower 4100 series	970 MB	970 MB	100 MB	12 min
Firepower 9300	970 MB	970 MB	100 MB	11 min
ASA 5500-X series with FTD	570 MB	110 MB	80 MB	12 min
FTDv: VMware 6.0	600 MB	110 MB	80 MV	10 min
Firepower 7000/8000 series	2.5 GB	170 MB	400 MB	20 min
ASA FirePOWER	3.0 GB	30 MB	340 MB	45 min
NGIPSv: VMware 6.0	1.5 GB	160 MB	250 MB	10 min

Version 6.3.0.1 Time and Disk Space

Table 99: Version 6.3.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.3.0
FMC	3.0 GB	170 MB	—	31 min
FMCv: VMware 6.0	2.4 GB	170 MB	—	25 min
Firepower 2100 series	1.2 GB	1.2 GB	290 MB	18 min
Firepower 4100 series	740 MB	740 MB	100 MB	12 min
Firepower 9300	740 MB	740 MB	100 MB	12 min
ASA 5500-X series with FTD	400 MB	150 MB	72 MB	17 min
FTDv: VMware 6.0	400 MB	150 MB	72 MB	10 min
Firepower 7000/8000 series	2.1 GB	170 MB	350 MB	20 min
ASA FirePOWER	2.4 GB	28 MB	270 MB	44 min
NGIPSv: VMware 6.0	1.5 GB	150 MB	350 MB	10 min

Version 6.3.0 Time and Disk Space

Table 100: Version 6.3.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	12.7 GB	29 MB	—	47 min
FMCv on: VMware 6.0	12.7 GB	29 MB	—	29 min
Firepower 2100 series	13 MB	8.8 GB	930 MB	20 min
Firepower 4100/9300 chassis	10 MB	7.6 GB	930 MB	6 min
ASA 5500-X series with FTD	7.9 GB	100 KB	1.1 GB	25 min
FTDv: VMware 6.0	7.3 GB	100 KB	1.1 GB	12 min
Firepower 7000/8000 series	7.0 GB	19 MB	920 MB	32 min
ASA FirePOWER	11.3 GB	22 MB	1.2 GB	63 min
NGIPSv	5.7 GB	19 MB	810 MB	16 min

Version 6.2.3.17 Time and Disk Space

Table 101: Version 6.2.3.17 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FMC	3.4 GB	300 MB	—	32 min	7 min
FMCv: VMware 6.0	4.1 GB	230 MB	—	23 min	5 min
Firepower 2100 series	2.7 GB	2.7 GB	600 MB	12 min	12 min
Firepower 4100 series	1.7 GB	1.7 GB	390 MB	5 min	6 min
Firepower 9300	1.7 GB	1.7 GB	390 MB	5 min	7 min
ASA 5500-X series with FTD	2.1 GB	200 MB	420 MB	18 min	37 min
FTDv: VMware 6.0	2.1 GB	190 MB	420 MB	7 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	640 MB	10 min	15 min
ASA FirePOWER	3.8 GB	58 MB	580 MB	72 min	61 min
NGIPSv: VMware 6.0	2.5 GB	180 MB	480 MB	5 min	4 min

Version 6.2.3.16 Time and Disk Space

Table 102: Version 6.2.3.16 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
FMC	3.6 GB	250 MB	—	40 min	9 min
FMCv: VMware 6.0	3.3 GB	220 MB	—	25 min	4 min
Firepower 2100 series	2.6 GB	2.6 GB	620 MB	11 min	12 min
Firepower 4100 series	1.7 GB	1.7 GB	410 MB	5 min	5 min
Firepower 9300	1.8 GB	1.8 GB	410 MB	5 min	9 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3	Reboot Time
ASA 5500-X series with FTD	2.0 GB	200 MB	430 MB	18 min	33 min
FTDv: VMware 6.0	2.0 GB	190 MB	430 MB	8 min	5 min
Firepower 7000/8000 series	3.5 GB	200 MB	670 MB	31 min	14 min
ASA FirePOWER	3.8 GB	58 MB	600 MB	74 min	77 min
NGIPSv: VMware 6.0	2.3 GB	180 MB	500 MB	6 min	4 min

Version 6.2.3.15 Time and Disk Space

Table 103: Version 6.2.3.15 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.7 GB	260 MB	—	50 min
FMCv: VMware 6.0	4.7 GB	210 MB	—	Hardware dependent
Firepower 2100 series	2.3 GB	2.3 GB	590 MB	27 min
Firepower 4100 series	1.7 GB	1.7 GB	390 MB	10 min
Firepower 9300	2.4 GB	2.4 GB	390 MB	11 min
ASA 5500-X series with FTD	2.0 GB	190 MB	410 MB	38 min
FTDv: VMware 6.0	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.5 GB	210 MB	640 MB	19 min
ASA FirePOWER	3.9 GB	56 MB	580 MB	100 min
NGIPSv: VMware 6.0	2.7 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.14 Time and Disk Space

Table 104: Version 6.2.3.14 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.5 GB	260 MB	—	58 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMCv: VMware 6.0	4.7 GB	190 MB	—	Hardware dependent
Firepower 2100 series	1.9 GB	1.9 GB	590 MB	23 min
Firepower 4100 series	1.7 GB	1.7 GB	390 MB	11 min
Firepower 9300	1.7 GB	1.7 GB	390 MB	10 min
ASA 5500-X series with FTD	2.0 GB	200 MB	410 MB	32 min
FTDv: VMware 6.0	2.4 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.4 GB	200 MB	630 MB	19 min
ASA FirePOWER	3.7 GB	53 MB	560 MB	106 min
NGIPSv: VMware 6.0	2.6 GB	190 MB	470 MB	Hardware dependent

Version 6.2.3.13 Time and Disk Space

Table 105: Version 6.2.3.13 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.7 GB	290 MB	—	50 min
FMCv: VMware 6.0	4.6 GB	190 MB	—	Hardware dependent
Firepower 2100 series	2.6 GB	2.6 GB	590 MB	25 min
Firepower 4100 series	1.7 GB	1.7 GB	390 MB	11 min
Firepower 9300	1.8 GB	1.8 GB	390 MB	11 min
ASA 5500-X series with FTD	2.4 GB	190 MB	410 MB	32 min
FTDv: VMware 6.0	2.3 GB	190 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.8 GB	190 MB	620 MB	18 min
ASA FirePOWER	3.7 GB	51 MB	560 MB	105 min
NGIPSv: VMware 6.0	2.6 GB	180 MB	470 MB	Hardware dependent

Version 6.2.3.12 Time and Disk Space

Table 106: Version 6.2.3.12 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	3.9 GB	220 MB	—	49 min
FMCv: VMware 6.0	4.6 GB	160 MB	—	Hardware dependent
Firepower 2100 series	1.9 GB	1.9 GB	390 MB	21 min
Firepower 4100 series	970 MB	970 MB	190 MB	14 min
Firepower 9300	1.7 GB	1.7 GB	190 MB	11 min
ASA 5500-X series with FTD	1.4 GB	96 MB	210 MB	30 min
FTDv: VMware 6.0	2.4 GB	200 MB	210 MB	Hardware dependent
Firepower 7000/8000 series	3.6 GB	160 MB	540 MB	19 min
ASA FirePOWER	3.5 GB	31 MB	480 MB	104 min
NGIPSv: VMware 6.0	2.6 GB	130 MB	400 MB	Hardware dependent

Version 6.2.3.11 Time and Disk Space

Table 107: Version 6.2.3.11 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.5 GB	250 MB	—	39 min
FMCv: VMware 6.0	4.6 GB	35 MB	—	Hardware dependent
Firepower 2100 series	2.8 GB	2.8 GB	590 MB	40 min
Firepower 4100 series	2.0 GB	2.0 GB	380 MB	10 min
Firepower 9300	1.6 GB	1.6 GB	380 MB	11 min
ASA 5500-X series with FTD	1.8 GB	230 MB	410 MB	33 min
FTDv: VMware 6.0	2.2 GB	230 MB	410 MB	Hardware dependent
Firepower 7000/8000 series	3.3 GB	170 MB	600 MB	23 min
ASA FirePOWER	3.6 GB	50 MB	530 MB	110 min
NGIPSv: VMware 6.0	2.6 GB	130 MB	450 MB	Hardware dependent

Version 6.2.3.10 Time and Disk Space

Table 108: Version 6.2.3.10 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	4.2 GB	200 MB	—	40 min
FMCv	4.5 GB	230 MB	—	Hardware dependent
Firepower 2100 series	1.8GB	1.8 GB	390 MB	21 min
Firepower 4100/9300 chassis	1.3 GB	1.3 GB	190 MB	11 min
ASA 5500-X series with FTD	1.3 GB	140 MB	210 MB	25 min
FTDv	1.6 GB	140 MB	210 MB	Hardware dependent
Firepower 7000/8000 series	3.2 GB	190 MB	560 MB	25 min
ASA FirePOWER	3.4 GB	31 MB	480 MB	100 min
NGIPSv	2.1 GB	160 MB	400 MB	Hardware dependent

Version 6.2.3.9 Time and Disk Space

Table 109: Version 6.2.3.9 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	3630 MB	190 MB	—	35 min
FMCv	3596 MB	172 MB	—	Hardware dependent
Firepower 2100 series	1677 MB	1677 MB	385 MB	21 min
Firepower 4100/9300 chassis	779 MB	779 MB	184 MB	9 min
ASA 5500-X series with FTD	1105 MB	130 MB	206 MB	12 min
FTDv	1094 MB	130 MB	206 MB	Hardware dependent
Firepower 7000/8000 series	2975 MB	161 MB	538 MB	30 min
ASA FirePOWER	3211 MB	27 MB	462 MB	38 min
NGIPSv	1883 MB	146 MB	378 MB	Hardware dependent

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 110: Version 6.2.3.7 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2909 MB	137 MB	—	25 min
FMCv	3972 MB	211 MB	—	Hardware dependent
Firepower 2100 series	1668 MB	1668 MB	384 MB	19 min
Firepower 4100/9300 chassis	795 MB	795 MB	183 MB	8 min
ASA 5500-X series with FTD	1067 MB	130 MB	205 MB	9 min
FTDv	1146 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	3300 MB	136 MB	477 MB	20 min
ASA FirePOWER	2291 MB	26 MB	411 MB	80 min
NGIPSv	1588 MB	121 MB	327 MB	Hardware dependent

Version 6.2.3.6 Time and Disk Space

Table 111: Version 6.2.3.6 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2524 MB	47 MB	—	30 min
FMCv	2315 MB	101 MB	—	Hardware dependent
Firepower 2100 series	1673 MB	1673 MB	383 MB	10 min
Firepower 4100/9300 chassis	790 MB	790 MB	182 MB	17 min
ASA 5500-X series with FTD	1220 MB	130 MB	205 MB	21 min
FTDv	1133 MB	130 MB	205 MB	Hardware dependent
Firepower 7000/8000 series	1196 MB	17 MB	204 MB	30 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
ASA FirePOWER	1844 MB	16 MB	226 MB	106 min
NGIPSv	364 MB	17 MB	142 MB	Hardware dependent

Version 6.2.3.5 Time and Disk Space

Table 112: Version 6.2.3.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1566 MB	24 MB	—	28 min
FMCv	2266 MB	80 MB	—	Hardware dependent
Firepower 2100 series	1001 MB	1001MB	257 MB	20 min
Firepower 4100/9300 chassis	370 MB	370 MB	56 MB	7 min
ASA 5500-X series with FTD	587 MB	130 MB	78 MB	20 min
Firepower 7000/8000 series	806 MB	17 MB	78 MB	22 min
ASA FirePOWER	1465 MB	15 MB	100 MB	70 min
NGIPSv	120 MB	17 MB	16 MB	Hardware dependent

Version 6.2.3.4 Time and Disk Space

Table 113: Version 6.2.3.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	2191 MB	107 MB	—	80 min
FMCv	1760 MB	35 MB	—	Hardware dependent
Firepower 2100 series	1014 MB	1014 MB	261 MB	17 min
Firepower 4100/9300 chassis	334 MB	334 MB	59 MB	7 min
ASA 5500-X series with FTD	411 MB	128 MB	82 MB	20 min
FTDv	411 MB	128 MB	82 MB	Hardware dependent
Firepower 7000/8000 series	800 MB	17 MB	82 MB	23 min
ASA FirePOWER	1385 MB	15 MB	103 MB	25 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
NGIPSv	191 MB	17 MB	20 MB	Hardware dependent

Version 6.2.3.3 Time and Disk Space

Table 114: Version 6.2.3.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1879 MB	88 MB	—	26 min
FMCv	2093 MB	90 MB	—	Hardware dependent
Firepower 2100 series	987 MB	987 MB	255 MB	15 min
Firepower 4100/9300 chassis	313 MB	313 MB	54 MB	5 min
ASA 5500-X series with FTD	553 MB	128 MB	77 MB	16 min
FTDv	307 MB	90 MB	77 MB	Hardware dependent
Firepower 7000/8000 series	825 MB	17 MB	77 MB	15 min
ASA FirePOWER	634 MB	16 MB	98 MB	40 min
NGIPSv	102 MB	17 MB	77 MB	Hardware dependent

Version 6.2.3.2 Time and Disk Space

Table 115: Version 6.2.3.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1743 MB	27 MB	—	24 min
FMCv	1976 MB	70 MB	—	Hardware dependent
Firepower 2100 series	977 MB	977 MB	252 MB	17 min
Firepower 4100/9300 chassis	374 MB	374 MB	51 MB	4 min
ASA 5500-X series with FTD	585 MB	126 MB	73 MB	16 min
FTDv	585 MB	126 MB	73 MB	Hardware dependent
Firepower 7000/8000 series	688 MB	11 MB	76 MB	13 min
ASA FirePOWER	1440 MB	15 MB	98 MB	40 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
NGIPSv	96 MB	17 MB	14 MB	Hardware dependent

Version 6.2.3.1 Time and Disk Space

Table 116: Version 6.2.3.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.3
FMC	1361.8 MB	59.67 MB	—	25 min
FMCv	1240.8 MB	40.8 MB	—	Hardware dependent
Firepower 2100 series	948.3 MB	948.3 MB	246 MB	81 min
Firepower 4100/9300 chassis	278 MB	278 MB	45 MB	8 min
ASA 5500-X series with FTD	275.5 MB	89.9 MB	68 MB	16 min
FTDv	275.5 MB	89.9 MB	67 MB	Hardware dependent
Firepower 7000/8000 series	99.8 MB	36 MB	10 MB	19 min
ASA FirePOWER	867.9 MB	15.45 MB	32 MB	60 min
NGIPSv	101.9 MB	17.18 MB	9 MB	Hardware dependent

Version 6.2.3 Time and Disk Space

Table 117: Version 6.2.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	From 6.1.0: 7415 MB From 6.2.0: 8863 MB From 6.2.1: 8263 MB From 6.2.2: 11860 MB	From 6.1.0: 17 MB From 6.2.0: 24 MB From 6.2.1: 23 MB From 6.2.2: 24 MB	—	From 6.1.0: 38 min From 6.2.0: 43 min From 6.2.1: 37 min From 6.2.2: 37 min
FMCv	From 6.1.0: 7993 MB From 6.2.0: 9320 MB From 6.2.1: 11571 MB From 6.2.2: 11487 MB	From 6.1.0: 23 MB From 6.2.0: 28 MB From 6.2.1: 24 MB From 6.2.2: 24 MB	—	Hardware dependent

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 2100 series	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	From 6.2.1: 7356 MB From 6.2.2: 11356 MB	1000 MB	From 6.2.1: 15 min From 6.2.2: 15 min
Firepower 4100/9300 chassis	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	From 6.1.0: 5593 MB From 6.2.0: 5122 MB From 6.2.2: 7498 MB	795 MB	From 6.1.0: 10 min From 6.2.0: 12 min From 6.2.2: 15 min
ASA 5500-X series with FTD	From 6.1.0: 4322 MB From 6.2.0: 6421 MB From 6.2.2: 6450 MB	From 6.1.0: .088 MB From 6.2.0: .092 MB From 6.2.2: .088 MB	1000 MB	From 6.1.0: 54 min From 6.2.0: 53 min From 6.2.2: 50 min
FTDv	From 6.1.0: 4225 MB From 6.2.0: 5179 MB From 6.2.2: 6450 MB	From 6.1.0: .076 MB From 6.2.0: .092 MB From 6.2.2: .092 MB	1000 MB	Hardware dependent
Firepower 7000/8000 series	From 6.1.0: 5145 MB From 6.2.0: 5732 MB From 6.2.2: 6752 MB	From 6.1.0: 18 MB From 6.2.0: 18 MB From 6.2.2: 18 MB	840 MB	From 6.1.0: 29 min From 6.2.0: 31 min From 6.2.2: 31 min
ASA FirePOWER	From 6.1.0: 7286 MB From 6.2.0: 7286 MB From 6.2.2: 10748 MB	From 6.1.0: 16 MB From 6.2.0: 16 MB From 6.2.2: 16 MB	From 6.1.0: 1200 MB From 6.2.0: 1200 MB	From 6.1.0: 94 min From 6.2.0: 104 min From 6.2.2: 96 min
NGIPSv	From 6.1.0: 4115 MB From 6.2.0: 5505 MB From 6.2.2: 5871 MB	From 6.1.0: 18 MB From 6.2.0: 19 MB From 6.2.2: 19 MB	741 MB	Hardware dependent

Version 6.2.2.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	5271 MB	25 MB	—	From 6.2.2: 60 min From 6.2.2.4: 42 min
FMCv	5292 MB	33 MB	—	Hardware dependent
Firepower 2100 series	9113 MB	9113 MB	2.0 GB	From 6.2.2: 87 min From 6.2.2.4: 32 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 4100/9300	3325 MB	3325 MB	612 MB	From 6.2.2: 28 min From 6.2.2.4: 12 min
ASA 5500-X series with FTD	3809 MB	226 MB	724 MB	From 6.2.2: 49 min From 6.2.2.4: 25 min
FTDv	3809 MB	226 MB	724 MB	Hardware dependent
Firepower 7000/8000 series	566 MB	28 MB	419 MB	From 6.2.2: 54 min From 6.2.2.4: 12 min
ASA FirePOWER	3714 MB	28 MB	432 MB	From 6.2.2: 215 min From 6.2.2.4: 105 min
NGIPSv	3799 MB	24 MB	98 MB	Hardware dependent

Version 6.2.2.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	4435 MB	217 MB	—	From 6.2.2: 85 min From 6.2.2.3: 42 min
FMCv	3691 MB	48 MB	—	Hardware dependent
Firepower 2100 series	6965 MB	6965 MB	1 GB	From 6.2.2: 58 min From 6.2.2.3: 34 min
Firepower 4100/9300	1676 MB	1676 MB	339 MB	From 6.2.2: 24 min From 6.2.2.3: 13 min
ASA 5500-X series with FTD	1695 MB	225 MB	427 MB	From 6.2.2: 142 min From 6.2.2.3: 68 min
FTDv	1695 MB	225 MB	427 MB	Hardware dependent
Firepower 7000/8000 series	3343 MB	36 MB	414 MB	From 6.2.2: 45 min From 6.2.2.3: 19 min
ASA FirePOWER	3192 MB	27 MB	405 MB	From 6.2.2: 182 min From 6.2.2.3: 80 min
NGIPSv	444 MB	28 MB	94 MB	Hardware dependent

Version 6.2.2.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3766.6 MB	205 MB	—	From 6.2.2: 66 min From 6.2.2.2: 41 min
FMCv	3485 MB	17.5 MB	—	Hardware dependent
Firepower 2100 series	4486.64 MB	4486.64 MB	132 MB	From 6.2.2: 61 min From 6.2.2.2: 36 min
Firepower 4100/9300	811.7 MB	811.7 MB	132 MB	From 6.2.2: 20 min From 6.2.2.2: 12 min
ASA 5500-X series with FTD	1636.6 MB	125.1 MB	199 MB	From 6.2.2: 35 min From 6.2.2.2: 20 min
FTDv	1810.7 MB	125 MB	199 MB	Hardware dependent
Firepower 7000/8000 series	2775 MB	17 MB	339 MB	From 6.2.2: 80 min From 6.2.2.2: 42 min
ASA FirePOWER	2301.5 MB	15.69 MB	308 MB	From 6.2.2: 184 min From 6.2.2.2: 100 min
NGIPSv	576.3 MB	17.5 MB	20 MB	Hardware dependent

Version 6.2.2.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	1656 MB	18 MB	—	From 6.2.2: 34 min From 6.2.2.1: 27 min
FMCv	2356 MB	19 MB	—	Hardware dependent
Firepower 2100 series	2377 MB	2377 MB	497 MB	From 6.2.2: 41 min From 6.2.2.1: 20 min
Firepower 4100/9300	561 MB	561 MB	41 MB	From 6.2.2: 21 min From 6.2.2.1: 13 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA 5500-X series with FTD	984 MB	122 MB	136 MB	From 6.2.2: 110 min From 6.2.2.1: 70 min
FTDv	984 MB	122 MB	136 MB	Hardware dependent
Firepower 7000/8000 series	1706 MB	16 MB	310 MB	From 6.2.2: 56 min From 6.2.2.1: 40 min
ASA FirePOWER	1602 MB	15 MB	190 MB	From 6.2.2: 113 min From 6.2.2.1: 80 min
NGIPSv	170 MB	17 MB	16 MB	Hardware dependent

Version 6.2.2.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.2
FMC	480 MB	18 MB	—	52 min
FMCv	775 MB	30 MB	—	Hardware dependent
Firepower 2100 series	1003 MB	1003 MB	47 MB	28 min
Firepower 4100/9300	299 MB	299 MB	47 MB	35 min
ASA 5500-X series with FTD	674 MB	121 MB	69 MB	72 min
FTDv	674 MB	121 MB	69 MB	Hardware dependent
Firepower 7000/8000 series	664 MB	14 MB	61 MB	33 min
ASA FirePOWER	758 MB	15 MB	83 MB	90 min
NGIPSv	106 MB	17 MB	10 MB	Hardware dependent

Version 6.2.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	From 6.2.0: 6467 MB From 6.2.1: 6916 MB	From 6.2.0: 22 MB From 6.2.1: 21 MB	—	From 6.2.0: 52 min From 6.2.1: 61 min
FMCv	From 6.2.0: 6987 MB From 6.2.1: 5975 MB	From 6.2.0: 24 MB From 6.2.1: 24 MB	—	Hardware dependent

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 2100 series	5613 MB	5613 MB	925 MB	57 min
Firepower 4100/9300	4635 MB	4635 MB	743 MB	14 min
FTDv	3586 MB	.92 MB	987 MB	Hardware dependent
ASA 5500-X series with FTD	3683 MB	.16 MB	987 MB	80 min
Firepower 7000/8000 series	6745 MB	18 MB	1300 MB	27 min
ASA FirePOWER	7021 MB	16 MB	1200 MB	131 min
NGIPSv	7261 MB	18 MB	1300 MB	Hardware dependent

Version 6.2.0.6 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	8547 MB	104 MB	—	From 6.2.0: 97 min From 6.2.0.5: 36 min
FMCv	8543 MB	30 MB	—	Hardware dependent
Firepower 4100/9300	4085 MB	4085 MB	789 MB	From 6.2.0: 23 min From 6.2.0.5: 13 min
FTDv	4526 MB	226 MB	918 MB	Hardware dependent
ASA 5500-X series with FTD	4960 MB	227 MB	918 MB	From 6.2.0: 56 min From 6.2.0.5: 27 min
Firepower 7000/8000 series	7464 MB	29 MB	944 MB	From 6.2.0: 60 min From 6.2.0.5: 24 min
ASA FirePOWER	7191 MB	28 MB	878 MB	From 6.2.0: 75 min From 6.2.0.5: 49 min
NGIPSv	1658 MB	29 MB	284 MB	Hardware dependent

Version 6.2.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	6009 MB	180 MB	—	From 6.2.0: 72 min From 6.2.0.4: 34 min
FMCv	6943 MB	20 MB	—	Hardware dependent
Firepower 4100/9300	3009 MB	3009 MB	441 MB	From 6.2.0: 28 min From 6.2.0.4: 16 min
FTDv	2805 MB	135 MB	548 MB	Hardware dependent
ASA 5500-X series with FTD	4316 MB	135 MB	548 MB	From 6.2.0: 46 min From 6.2.0.4: 22 min
Firepower 7000/8000 series	5806 MB	18 MB	693 MB	From 6.2.0: 51 min From 6.2.0.4: 18 min
ASA FirePOWER	5945 MB	16 MB	703 MB	From 6.2.0: 66 min From 6.2.0.4: 27 min
NGIPSv	1301 MB	18 MB	211 MB	Hardware dependent

Version 6.2.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	5271 MB	167 MB	—	From 6.2.0: 84 min From 6.2.0.3: 50 min
FMCv	5346 MB	20 MB	—	Hardware dependent
Firepower 4100/9300	1828 MB	1828 MB	325 MB	From 6.2.0: 23 min From 6.2.0.3: 12 min
ASA 5500-X series with FTD	3593 MB	134 MB	448 MB	From 6.2.0: 2 hr 28 min From 6.2.0.3: 69 min
FTDv	275 MB	136 MB	448 MB	Hardware dependent
Firepower 7000/8000 series	4614 MB	18 MB	608 MB	From 6.2.0: 45 min From 6.2.0.3: 17 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA FirePOWER	4585 MB	16 MB	597 MB	From 6.2.0: 3 hr 34 min From 6.2.0.3: 83 min
NGIPSv	1067 MB	18 MB	208 MB	Hardware dependent

Version 6.2.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3352 MB	18 MB	—	From 6.2.0: 75 min From 6.2.0.2: 37 min
FMCv	3342 MB	19 MB	—	Hardware dependent
Firepower 4100/9300	—	1355 MB	319 MB	From 6.2.0: 18 min From 6.2.0.2: 12 min
ASA 5500-X series with FTD	131 MB	2302 MB	384 MB	From 6.2.0: 118 min From 6.2.0.2: 76 min
FTDv	842 MB	17 MB	384 MB	Hardware dependent
Firepower 7000/8000 series	3526 MB	17 MB	554 MB	From 6.2.0: 38 min From 6.2.0.2: 19 min
ASA FirePOWER	15 MB	3361 MB	521 MB	From 6.2.0: 3 hr From 6.2.0.2: 97 min
NGIPSv	842 MB	17 MB	202 MB	Hardware dependent

Version 6.2.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	1665 MB	35 MB	—	From 6.2.0: 36 min From 6.2.0.1: 30 min
FMCv	2834 MB	21 MB	—	Hardware dependent
Firepower 4100/9300	1060 MB	1060 MB	274 MB	From 6.2.0: 12 min From 6.2.0.1: 9 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA 5500-X series with FTD	1808 MB	144 MB	295 MB	From 6.2.0: 95 min From 6.2.0.1: 59 min
FTDv	998 MB	143 MB	295 MB	Hardware dependent
Firepower 7000/8000 series	2110 MB	17 MB	458 MB	From 6.2.0: 54 min From 6.2.0.1: 35 min
ASA FirePOWER	2014 MB	17 MB	383 MB	From 6.2.0: 40 min From 6.2.0.1: 80 min
NGIPSv	612 MB	19 MB	195 MB	Hardware dependent

Version 6.2.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.2.0
FMC	1237 MB	50 MB	—	28 min
FMCv	1488 MB	23 MB	—	Hardware dependent
Firepower 4100/9300	524 MB	524 MB	137 MB	12 min
ASA 5500-X series with FTD	945 MB	144 MB	159 MB	62 min
FTDv	144 MB	10 MB	159 MB	Hardware dependent
Firepower 7000/8000 series	1134 MB	18 MB	186 MB	22 min
ASA FirePOWER	97 MB	17 MB	206 MB	69 min
NGIPSv	721 MB	19 MB	98 MB	Hardware dependent

Version 6.2.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	10207 MB	17 MB	—	57 min
FMCv	10207 MB	17 MB	—	Hardware dependent
Firepower 4100/9300	5234 MB	5234 MB	734 MB	21 min
ASA 5500-X series with FTD	5213 MB	.096 MB	938 MB	83 min
FTDv	5663 MB	1 MB	936 MB	Hardware dependent

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 7000/8000 series	6129 MB	17 MB	1200 MB	27 min
ASA FirePOWER	6619 MB	16 MB	1100 MB	165 min
NGIPSv	7028 MB	18 MB	1300 MB	Hardware dependent

Version 6.1.0.7 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	1941 MB	187 MB	—	From 6.1.0: 111 min From 6.1.0.5: 41 min
FMCv	12435 MB	218 MB	—	Hardware dependent
Firepower 4100/9300	9881 MB	9881 MB	1400 MB	From 6.1.0: 43 min From 6.1.0.5: 13 min
ASA 5500-X series with FTD	8846 MB	1033 MB	1480 MB	From 6.1.0: 251 min From 6.1.0.5: 75 min
FTDv	1339 MB	185 MB	1480 MB	Hardware dependent
Firepower 7000/8000 series	5896 MB	33 MB	159 MB	From 6.1.0: 39 min From 6.1.0.5: 25 min
ASA FirePOWER	13061 MB	45 MB	1390 MB	From 6.1.0: 156 min From 6.1.0.5: 28 min
NGIPSv	5477 MB	185 MB	717 MB	Hardware dependent

Version 6.1.0.6 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	10503 MB	215 MB	—	From 6.1.0: 66 min From 6.1.0.5: 27 min
FMCv	1367 MB	196 MB	—	Hardware dependent
Firepower 4100/9300	8140 MB	8140 MB	1126 MB	From 6.1.0: 270 min From 6.1.0.5: 75 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA 5500-X series with FTD	8540 MB	1034 MB	1229 MB	From 6.1.0: 40 min From 6.1.0.5: 15 min
FTDv	7414 MB	1033 MB	1229 MB	Hardware dependent
Firepower 7000/8000 series	12725 MB	237 MB	1434 MB	From 6.1.0: 136 min From 6.1.0.5: 34 min
ASA FirePOWER	11189 MB	31 MB	1131 MB	From 6.1.0: 257 min From 6.1.0.5: 60 min
NGIPSv	4606 MB	196 MB	644 MB	Hardware dependent

Version 6.1.0.5 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	7673 MB	46 MB	—	From 6.1.0: 56 min From 6.1.0.4: 28 min
FMCv	10790 MB	216 MB	—	Hardware dependent
Firepower 4100/9300	7680 MB	7680 MB	1060 MB	From 6.1.0: 30 min From 6.1.0.4: 10 min
ASA 5500-X series with FTD	7952 MB	137 MB	1141 MB	From 6.1.0: 186 min From 6.1.0.4: 70 min
FTDv	7453 MB	1140 MB	1141 MB	Hardware dependent
Firepower 7000/8000 series	11877 MB	259 MB	1403 MB	From 6.1.0: 115 min From 6.1.0.4: 25 min
ASA FirePOWER	8955 MB	34 MB	1217 MB	From 6.1.0: 208 min From 6.1.0.4: 105 min
NGIPSv	4298 MB	215 MB	640 MB	Hardware dependent

Version 6.1.0.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	6739516 MB	218808 MB	—	From 6.1.0: 65 min From 6.1.0.3: 30 min
FMCv	675984 MB	200748 MB	—	Hardware dependent
Firepower 4100/9300	6010092 MB	6010092 MB	1020 MB	From 6.1.0: 26 min From 6.1.0.3: 10 min
ASA 5500-X series with FTD	6155828 MB	1058968 MB	1100 MB	From 6.1.0: 49 min From 6.1.0.3: 20 min
FTDv	1059632 MB	1059632 MB	1100 MB	Hardware dependent
Firepower 7000/8000 series	8713068 MB	240940 MB	1200 MB	From 6.1.0: 48 min From 6.1.0.3: 17 min
ASA FirePOWER	7442808 MB	31740 MB	1100 MB	From 6.1.0: 63 min From 6.1.0.3: 45 min
NGIPSv	3367536 MB	20120 MB	636 MB	Hardware dependent

Version 6.1.0.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	5537816 MB	218676 MB	—	From 6.1.0: 46 min From 6.1.0.2: 35 min
FMCv	6611148 MB	200904 MB	—	Hardware dependent
Firepower 4100/9300	5014020 MB	5014020 MB	929 MB	From 6.1.0: 22 min From 6.1.0.2: 13 min
ASA 5500-X series with FTD	1057776 MB	1057776 MB	1000 MB	From 6.1.0: 40 min From 6.1.0.2: 23 min
FTDv	1059932 MB	1059932 MB	1000 MB	Hardware dependent
Firepower 7000/8000 series	7357340 MB	228728 MB	1100 MB	From 6.1.0: 43 min From 6.1.0.2: 25 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
ASA FirePOWER	4782384 MB	31792 MB	1000 MB	From 6.1.0: 160 min From 6.1.0.2: 80 min
NGIPSv	2710540 MB	200896 MB	635 MB	Hardware dependent

Version 6.1.0.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3872 MB	235 MB	—	From 6.1.0: 44 min From 6.1.0.1: 22 min
FMCv	3871 MB	219 MB	—	Hardware dependent
Firepower 4100/9300	4046 MB	4046 MB	886 MB	From 6.1.0: 20 min From 6.1.0.1: 14 min
ASA 5500-X series with FTD	2291 MB	96 MB	918 MB	From 6.1.0: 74 min From 6.1.0.1: 106 min
FTDv	2797 MB	1137 MB	918 MB	Hardware dependent
Firepower 7000/8000 series	4130 MB	260 MB	965 MB	From 6.1.0: 62 min From 6.1.0.1: 24 min
ASA FirePOWER	4549 MB	40 MB	816 MB	From 6.1.0: 139 min From 6.1.0.1: 34 min
NGIPSv	2710540 MB	200896 MB	635 MB	Hardware dependent

Version 6.1.0.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.1.0
FMC	1893 MB	140 MB	—	23 min
FMCv	2144 MB	207 MB	—	Hardware dependent
Firepower 4100 series	2580 MB	580 MB	600 MB	15 min
Firepower 9300	1877 MB	1877 MB	600 MB	20 min
ASA 5500-X series with FTD	1377 MB	846 MB	600 MB	10 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.1.0
FTDv	1377 MB	846 MB	600 MB	Hardware dependent
Firepower 7000/8000 series	2094 MB	156 MB	513 MB	47 min
ASA FirePOWER	1728 MB	34 MB	433 MB	76 min
NGIPSv	793 MB	130 MB	295 MB	Hardware dependent

Version 6.1.0 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	10722 MB	18 MB	—	47 min
FMCv	10128 MB	17 MB	—	Hardware dependent
ASA 5500-X series with FTD	5213 MB	.096 MB	914 MB	21 min
FTDv	5403 MB	.096 MB	914 MB	Hardware dependent
Firepower 7000/8000 series	7108 MB	61 MB	1740 MB	39 min
ASA FirePOWER	8392 MB	47 MB	1300 MB	59 min
NGIPSv	6368 MB	54 MB	1229 MB	Hardware dependent

Version 6.0.1.4 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	3428 MB	201 MB	—	From 6.0.0: 92 min From 6.0.1.3: 39 min
FMCv	3108 MB	95 MB	—	Hardware dependent
Firepower 4100 series	5237 MB	5237 MB	1000 MB	From 6.0.0: 30 min From 6.0.1.3: 18 min
Firepower 9300	1360 MB	5434 MB	1000 MB	From 6.0.0: 26 min From 6.0.1.3: 14 min
ASA 5500-X series with FTD	3416 MB	1017 MB	1000 MB	From 6.0.0: 26 min From 6.0.1.3: 14 min
FTDv	3619 MB	1020 MB	1000 MB	Hardware dependent

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
Firepower 7000/8000 series	7891 MB	222 MB	1270 MB	From 6.0.0: 47 min From 6.0.1.3: 23 min
ASA FirePOWER	6049 MB	45 MB	990 MB	From 6.0.0: 95 min From 6.0.1.3: 43 min
NGIPSv	2916 MB	192 MB	990 MB	Hardware dependent

Version 6.0.1.3 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	2419 MB	110 MB	—	58 min
FMCv	2419 MB	101 MB	—	Hardware dependent
Firepower 4100/9300	2781 MB	2781 MB	473 MB	22 min
ASA 5500-X series with FTD	2641 MB	813 MB	473 MB	24 min
FTDv	2651 MB	813 MB	473 MB	Hardware dependent
Firepower 7000/8000 series	4757 MB	125 MB	926 MB	55 min
ASA FirePOWER	3883 MB	58 MB	685 MB	184 min
NGIPSv	1695 MB	107 MB	430 MB	Hardware dependent

Version 6.0.1.2 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
FMC	272 MB	54 MB	—	7 min
FMCv	368 MB	54 MB	—	Hardware dependent
Firepower 4100/9300	2101 MB	56 MB	302 MB	16 min
ASA 5500-X series with FTD	740 MB	807 MB	302 MB	13 min
FTDv	2101 MB	56 MB	302 MB	Hardware dependent
Firepower 7000/8000 series	3190 MB	63 MB	412 MB	17 min
ASA FirePOWER	2027 MB	54 MB	577 MB	99 min

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time
NGIPSv	602 MB	56 MB	243 MB	Hardware dependent

Version 6.0.1.1 Time and Disk Space

Platform	Space on /Volume	Space on /	Space on FMC	Upgrade Time from 6.0.1
FMC	14 MB	54 MB	—	23 min
FMCv	14 MB	54 MB	—	Hardware dependent
Firepower 4100/9300	54 MB	54 MB	2 MB	6 min
ASA 5500-X series with FTD	54 MB	54 MB	2 MB	7 min
FTDv	14 MB	54 MB	2 MB	Hardware dependent
Firepower 7000/8000 series	944 MB	61 MB	166 MB	39 min
ASA FirePOWER	824 MB	54 MB	84 MB	46 min
NGIPSv	54 MB	56 MB	1 MB	Hardware dependent



CHAPTER 10

Traffic Flow and Inspection

Interruptions in traffic flow and inspection can occur when you:

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

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

- [Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300, on page 219](#)

Firepower Threat Defense Upgrade Behavior: Firepower 4100/9300

FXOS Upgrades

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

Table 118: Traffic Behavior: FXOS Upgrades

Deployment	Method	Traffic Behavior
Standalone	—	Dropped.

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

Software Upgrades for Standalone Devices

Devices operate in maintenance mode while they upgrade. Entering maintenance mode at the beginning of the upgrade causes a 2-3 second interruption in traffic inspection. Interface configurations determine how a standalone device handles traffic both then and during the upgrade.

Table 119: Traffic Behavior: Software Upgrades for Standalone Devices

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.

Interface Configuration		Traffic Behavior
IPS-only interfaces	Inline set, hardware bypass force-enabled: Bypass: Force (6.1+).	Passed without inspection until you either disable hardware bypass, or set it back to standby mode.
	Inline set, hardware bypass standby mode: Bypass: Standby (6.1+).	Dropped during the upgrade, while the device is in maintenance mode. Then, passed without inspection while the device completes its post-upgrade reboot.
	Inline set, hardware bypass disabled: Bypass: Disabled (6.1+).	Dropped.
	Inline set, no hardware bypass module.	Dropped.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.

Software Upgrades for High Availability/Scalability

You should not experience interruptions in traffic flow or inspection while upgrading high availability or clustered devices.

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

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

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



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. Upgrading high availability or clustered devices from Version 6.0.1 through 6.2.2.x may have additional upgrade path requirements; see [Upgrade Path: FTD Logical Devices and FMC, on page 7](#).

Software Uninstall (Patches)

In Version 6.2.3 and later, uninstalling a patch returns you to the version you upgraded from, and does not change configurations. (In Version 6.2.2 and earlier, uninstalling a patch results in an appliance running the immediately preceding patch, even if you upgraded from an earlier patch.)

- Firepower Threat Defense with FMC: For standalone devices, interruptions to traffic flow and inspection during patch uninstall are the same as for upgrade. In high availability/scalability deployments, you must

explicitly plan an uninstall order that minimizes disruption. This is because you uninstall patches from devices individually, even those that you upgraded as a unit.

- Firepower Threat Defense with FDM: Not supported.

Deploying Configuration Changes

You deploy configurations multiple times during the upgrade process. Snort typically restarts during the first deployment immediately after the upgrade. It does not restart during other deployments unless, before deploying, you modify specific policy or device configurations. For more information, see *Configurations that Restart the Snort Process when Deployed or Activated* in the [Firepower Management Center Configuration Guide](#).

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

Table 120: Traffic Behavior: Deploying Configuration Changes

Interface Configuration		Traffic Behavior
Firewall interfaces	Routed or switched including EtherChannel, redundant, subinterfaces. Switched interfaces are also known as bridge group or transparent interfaces.	Dropped.
IPS-only interfaces	Inline set, Failsafe enabled or disabled (6.0.1–6.1).	Passed without inspection. A few packets might drop if Failsafe is disabled and Snort is busy but not down.
	Inline set, Snort Fail Open: Down: disabled (6.2+).	Dropped.
	Inline set, Snort Fail Open: Down: enabled (6.2+).	Passed without inspection.
	Inline set, tap mode.	Egress packet immediately, copy not inspected.
	Passive, ERSPAN passive.	Uninterrupted, not inspected.