



Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1

First Published: 2018-10-25

Last Modified: 2022-02-08

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

Getting Started 1

Is This Guide for You? 1

CHAPTER 2

Planning Your Upgrade 3

Upgrade Planning Phases 3

Current Version and Model Information 4

Upgrade Paths 4

Upgrade Path: FXOS 6

Upgrade Path: ASA Logical Devices 7

Upgrade Path: FTD Logical Devices and FMC 9

Upgrade Path: FTD Logical Devices and FDM 13

Upgrade Path: FTD and ASA Logical Devices for Firepower 9300 14

Upgrade Path: Firepower Management Centers 15

Download Upgrade Packages 17

Firepower Software Packages 18

ASA Packages 19

FXOS Packages 19

Upload Firepower Software Upgrade Packages with FMC 20

Upload to the Firepower Management Center 20

Upload to an Internal Server (Version 6.6.0+ FTD with FMC) 21

Copy to Managed Devices 22

Upload Firepower Threat Defense Upgrade Packages with FDM 23

Upload to the FTD Device (Version 6.2.0+ with FDM) 23

Upload to the FTD Device (Version 6.0.1 & 6.1.0 with FDM) 24

Firepower Software Readiness Checks with FMC 25

Run Readiness Checks with FMC (Version 7.0.0+ FTD) 25

Run Readiness Checks with FMC (Version 6.7.0+) 25

Run Readiness Checks with FMC (Version 6.0.1–6.6.x) 26

Firepower Software Readiness Checks with FDM 27

Run Readiness Checks (Version 7.0.0+ with FDM) 27

CHAPTER 3

Upgrade FXOS on the Firepower 4100/9300 29

Upgrade FXOS on a Firepower 4100/9300 Chassis Using Firepower Chassis Manager 29

Upgrade FXOS on a Firepower 4100/9300 Chassis Using the CLI 31

CHAPTER 4

Upgrade the Firepower 4100/9300 with FTD Logical Devices 35

Upgrade FXOS on a Firepower 4100/9300 with Firepower Threat Defense Logical Devices 35

Upgrade FXOS: FTD Standalone Devices and Intra-chassis Clusters 36

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using Firepower Chassis Manager 36

Upgrade FXOS for Standalone FTD Logical Devices or an FTD Intra-chassis Cluster Using the FXOS CLI 37

Upgrade FXOS: FTD High Availability Pairs 40

Upgrade FXOS on an FTD High Availability Pair Using Firepower Chassis Manager 41

Upgrade FXOS on an FTD High Availability Pair Using the FXOS CLI 44

Upgrade FXOS: FTD Inter-chassis Clusters 48

Upgrade FXOS on an FTD Inter-chassis Cluster Using Firepower Chassis Manager 49

Upgrade FXOS on an FTD Inter-chassis Cluster Using the FXOS CLI 51

Upgrade Firepower Threat Defense Logical Devices with Firepower Management Center 54

Upgrade Checklist: Firepower Threat Defense with FMC 55

Upgrade Firepower Threat Defense with FMC (Version 7.0.0) 59

Upgrade Firepower Threat Defense with FMC (Version 6.0.1–6.7.0) 62

CHAPTER 5

Upgrade the Firepower 4100/9300 with ASA Logical Devices 65

Checklist: Upgrade Firepower 4100/9300 with ASA 65

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster 66

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using Firepower Chassis Manager 66

Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster Using the FXOS CLI 67

Upgrade FXOS and an ASA Active/Standby Failover Pair 71

Upgrade FXOS and an ASA Active/Standby Failover Pair Using Firepower Chassis Manager	71
Upgrade FXOS and an ASA Active/Standby Failover Pair Using the FXOS CLI	73
Upgrade FXOS and an ASA Active/Active Failover Pair	81
Upgrade FXOS and an ASA Active/Active Failover Pair Using Firepower Chassis Manager	81
Upgrade FXOS and an ASA Active/Active Failover Pair Using the FXOS CLI	84
Upgrade FXOS and an ASA Inter-chassis Cluster	92
Upgrade FXOS and an ASA Inter-chassis Cluster Using Firepower Chassis Manager	93
Upgrade FXOS and an ASA Inter-chassis Cluster Using the FXOS CLI	94

CHAPTER 6**Monitor Upgrade Progress and Verify Installation 101**

Monitor the Upgrade Progress 101

Verify the Installation 102



CHAPTER 1

Getting Started

- [Is This Guide for You?](#), on page 1

Is This Guide for You?

This guide explains how to prepare for and complete a successful upgrade of the Firepower 4100/9300 chassis with:

- Firepower Threat Defense (FTD) logical devices managed by Firepower Management Center (FMC), **Version 6.0.1–7.0.x**
- Adaptive Security Appliance (ASA) logical devices, **Version 9.4(1)–9.16(x)**
- Firepower eXtensible Operating System (FXOS), **Version 1.1.1-2.10.1**

Additional Resources

If you are upgrading a different platform/component, or to a different version, see one of the following resources.

Upgrade	Target Version	Resource
FMC	Version 7.1.0+	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center
FTD with FMC	Version 7.1.0+	Cisco Firepower Threat Defense Upgrade Guide for Firepower Management Center
FTD with FDM	Version 7.1.0+	Cisco Firepower Threat Defense Upgrade Guide for Firepower Device Manager

Upgrade	Target Version	Resource
FTD with FDM	Version 7.0.x or earlier	<p data-bbox="922 289 1472 447">Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager, to upgrade the FTD software on any FTD device. See the <i>System Management</i> chapter for the version you are currently running.</p> <p data-bbox="922 468 1472 590">Cisco Firepower 4100/9300 Upgrade Guide, Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1 (this guide), to upgrade FXOS on the Firepower 4100/9300.</p>
ASA logical devices on the Firepower 4100/9300	ASA 9.17(x)+	Cisco ASA Upgrade Guide
BIOS and firmware for FMC	Latest	Cisco Firepower Hotfix Release Notes



CHAPTER 2

Planning Your Upgrade

- [Upgrade Planning Phases, on page 3](#)
- [Current Version and Model Information, on page 4](#)
- [Upgrade Paths, on page 4](#)
- [Download Upgrade Packages, on page 17](#)
- [Upload Firepower Software Upgrade Packages with FMC, on page 20](#)
- [Upload Firepower Threat Defense Upgrade Packages with FDM, on page 23](#)
- [Firepower Software Readiness Checks with FMC, on page 25](#)
- [Firepower Software Readiness Checks with FDM, on page 27](#)

Upgrade Planning Phases

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

Table 1: Upgrade Planning Phases

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

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

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	<p>Firepower Chassis Manager: Choose Overview.</p> <p>FXOS CLI: For the version, use the show version command. For the model, enter scope chassis 1, and then show inventory.</p>
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	<p>ASDM: Choose Home > Device Dashboard > Device Information.</p> <p>ASA CLI: Use the show version command.</p>
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.



Tip This guide covers Firepower 6.0.1–7.0.x or ASA 9.4(1)–9.16(x) with FXOS 1.1.1–2.10.1. See [Is This Guide for You?, on page 1](#)

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 4](#).

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 [Cisco Firepower 4100/9300 FXOS Compatibility](#) .

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 FMC and device upgrades, consider reimaging older devices instead of upgrading. First, remove the devices from the FMC. Then, upgrade the FMC, reimage the devices, and re-add them to the FMC.

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: [Cisco Firepower Compatibility Guide](#).
- Can I maintain FXOS compatibility with logical devices: [Cisco Firepower 4100/9300 FXOS Compatibility](#)

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 14](#).

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 [Cisco Firepower 4100/9300 FXOS Compatibility](#).



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 14](#).

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 [Cisco Firepower 4100/9300 FXOS Compatibility](#).



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	To minimize disruption, always upgrade the standby. <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+)	To minimize disruption, always upgrade an all-data unit chassis. For example, for a two-chassis cluster: <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
Upgrading high availability or clustered devices and you are currently running any of: <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 With: <ul style="list-style-type: none"> • FTD 6.0.1 through 6.2.2.x 	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>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 14](#).

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 [Cisco Firepower 4100/9300 FXOS Compatibility](#).

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	Upgrade FXOS on both chassis before you upgrade FTD. To minimize disruption, always upgrade the standby: <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 [Cisco Firepower 4100/9300 FXOS Compatibility](#).



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 the FMC, 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 later 7.0.x maintenance release
7.0.x	
Last support for FMC 1000, 2500, and 4500	

Current Version	Target Version
6.7.0 6.7.x	Any of: → 7.0.0 or any 7.0.x maintenance release → Any later 6.7.x maintenance release
6.6.0 6.6.x 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. <i>version</i> .SPA
Recovery (kickstart)	fxos-k9-kickstart. <i>version</i> .SPA
Recovery (manager)	fxos-k9-manager. <i>version</i> .SPA
Recovery (system)	fxos-k9-system. <i>version</i> .SPA
MIBs	fxos-mibs-fp9k-fp4k. <i>version</i> .zip
Firmware: Firepower 4100 series	fxos-k9-fpr4k-firmware. <i>version</i> .SPA
Firmware: Firepower 9300	fxos-k9-fpr9k-firmware. <i>version</i> .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 FMC high availability deployments, you must upload the FMC 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 59](#). 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.
- 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.
- If the devices where you want to push the upgrade package are not listed, you chose the wrong upgrade package.
- Step 4** Push the package
- 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.
- The **System Upgrade** section shows the currently running software version and any update that you have already uploaded.
- 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.

```
admin@firepower:/var/sf/updates$ sudo wget
http://files.example.com/ftd/Cisco_FTD_Upgrade-6.2.0-181.sh
```

```
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
```

```
#1) Respect the privacy of others.
```

```
#2) Think before you type.
#3) With great power comes great responsibility.
```

```
Password: (enter admin password)
Connecting to files.example.com
|*****
*****
*****
*****
*****|

...(remaining output omitted)
```

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

Firepower Software Readiness Checks with FMC

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.

The time required to run a readiness check varies depending on appliance model and database size. Later releases also have faster readiness checks.

Run Readiness Checks with FMC (Version 7.0.0+ FTD)

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 59.

See the next topics if you are:

- Running readiness checks on the FMC itself.
- Running readiness checks on managed devices, and your FMC is running Version 6.7.x.
- Running readiness checks on managed devices, and your FMC is running Version 6.6.x or earlier.

Run Readiness Checks with FMC (Version 6.7.0+)

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 59. 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 26.
- 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 3

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 29](#)
- [Upgrade FXOS on a Firepower 4100/9300 Chassis Using the CLI, on page 31](#)

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 35 or [Upgrade the Firepower 4100/9300 with ASA Logical Devices](#), on page 65.

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 35 or [Upgrade the Firepower 4100/9300 with ASA Logical Devices](#), on page 65.

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 4

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 35
 - [Upgrade Firepower Threat Defense Logical Devices with Firepower Management Center](#), on page 54

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 the [Cisco Firepower Release Notes](#) for your version.

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 or an FTD Intra-chassis Cluster Using Firepower Chassis Manager

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

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

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

Before you begin

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

- Download the FXOS platform bundle software package to which you are upgrading.
- 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 or an FTD Intra-chassis Cluster Using the FXOS CLI

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

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

- A Firepower 4100 series chassis that is configured with a FTD logical device and is not part of a failover pair or inter-chassis cluster.

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

Before you begin

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

- Download the FXOS platform bundle software package to which you are upgrading.
- 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:

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:
- 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:
- a) Click **Upload Image** to open the Upload Image dialog box.
 - b) Click **Choose File** to navigate to and select the image that you want to upload.
 - c) Click **Upload**.
The selected image is uploaded to the Firepower 4100/9300 chassis.
 - d) For certain software images you will be presented with an end-user license agreement after uploading the image. Follow the system prompts to accept the end-user license agreement.
- Step 4** After the new platform bundle image has successfully uploaded, click **Upgrade** for the FXOS platform bundle to which you want to upgrade.
- The system will first verify the software package that you want to install. It will inform you of any incompatibility between currently installed applications and the specified FXOS platform software package. It will also warn you that any existing sessions will be terminated and that the system will need to be rebooted as part of the upgrade.
- Step 5** Click **Yes** to confirm that you want to proceed with installation, or click **No** to cancel the installation.
The 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:
- a) Enter **scope system**.
 - b) Enter **show firmware monitor**.
 - c) Wait for all components (FPRM, Fabric Interconnect, and Chassis) to show `Upgrade-Status : Ready`.
- Note** After the FPRM component is upgraded, the system will reboot and then continue upgrading the other components.

Example:


```

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

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

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

```

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

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

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

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

## Upgrade FXOS: 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:

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 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:

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

- 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:

- 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 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, Version 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.

In most cases, do *not* restart an upgrade in progress. However, 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; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI. Note that 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.

### Planning and Feasibility

Careful planning and preparation can help you avoid missteps.

**Table 15:**

| ✓ | Action/Check                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p><b>Plan your upgrade path.</b></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><b>Note</b> In FMC deployments, you usually upgrade the FMC, then its managed devices. However, in some cases you may need to upgrade devices first.</p> <p>See <a href="#">Upgrade Paths, on page 4</a>.</p> |
|   | <p><b>Read <i>all</i> upgrade guidelines and plan configuration changes.</b></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><b>Check appliance access.</b></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>                                                                                                                             |

| ✓ | <b>Action/Check</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p><b>Check bandwidth.</b></p> <p>Make sure your management network has the bandwidth to perform large data transfers. In FMC 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 <a href="#">Guidelines for Downloading Data from the Firepower Management Center to Managed Devices</a> (Troubleshooting TechNote).</p> |
|   | <p><b>Schedule maintenance windows.</b></p> <p>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.</p>                                                                                        |

### Upgrade Packages

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

**Table 16:**

| ✓ | <b>Action/Check</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|---|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|   | <p><b>Upload the upgrade package to the FMC or internal web server.</b></p> <p>In Version 6.6.0+ you can configure an internal web server instead of the FMC as the source for FTD upgrade packages. This is useful if you have limited bandwidth between the FMC and its devices, and saves space on the FMC.</p> <p>See <a href="#">Upload to an Internal Server (Version 6.6.0+ FTD with FMC)</a>, on page 21.</p>                                                                                                                                                                                                                                                                                                                                                                                                                    |
|   | <p><b>Copy the upgrade package to the device.</b></p> <p>When supported, we recommend you copy (<i>push</i>) packages to managed devices before you initiate the device upgrade:</p> <ul style="list-style-type: none"> <li>• Version 6.2.2 and earlier do not support pre-upgrade copy.</li> <li>• Version 6.2.3 allows you to manually copy upgrade packages from the FMC.</li> <li>• Version 6.6.0 adds the ability to manually copy upgrade packages from an internal web server.</li> <li>• Version 7.0.0 adds a FTD upgrade workflow that prompts you to copy upgrade packages.</li> </ul> <p><b>Note</b> For the Firepower 4100/9300, we recommend (and sometimes require) you copy the upgrade package before you begin the required companion FXOS upgrade.</p> <p>See <a href="#">Copy to Managed Devices</a>, on page 22.</p> |

## 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><b>Back up FTD.</b></p> <p>Use the FMC 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"> <li>• 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.</li> <li>• After upgrade: This creates a snapshot of your freshly upgraded deployment. In FMC deployments, we recommend you back up the FMC after you upgrade its managed devices, so your new FMC backup file 'knows' that its devices have been upgraded.</li> </ul> |
|   | <p><b>Back up FXOS.</b></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><b>Upgrade virtual hosting.</b></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> |

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | <b>Action/Check</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|   | <p><b>Upgrade FXOS.</b></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><b>Note</b> Before you upgrade FXOS, make sure you read all upgrade guidelines and plan configuration changes. Start with the FXOS release notes: <a href="#">Cisco Firepower 4100/9300 FXOS Release Notes</a>.</p> |

### Final Checks

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

**Table 19:**

|   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | <b>Action/Check</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|   | <p><b>Check configurations.</b></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><b>Check NTP synchronization.</b></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 FMC 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"> <li>• FMC: Choose <b>System &gt; Configuration &gt; Time</b>.</li> <li>• Devices: Use the <b>show time</b> CLI command.</li> </ul>                                                                                                                                                                                                                                |
|   | <p><b>Check disk space.</b></p> <p>Run a disk space check for the software upgrade. Without enough free disk space, the upgrade fails.</p> <p>See the <i>Upgrade the Software</i> chapter in the <a href="#">Cisco Firepower Release Notes</a> for your target version.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|   | <p><b>Deploy configurations.</b></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 FMC 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 the <i>Upgrade the Software</i> chapter in the <a href="#">Cisco Firepower Release Notes</a> for your target version.</p> |



|   |                                                                                                                                                                                                                                                                                                                                                                                      |
|---|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ✓ | <b>Action/Check</b>                                                                                                                                                                                                                                                                                                                                                                  |
|   | <p><b>Run readiness checks.</b></p> <p>If your FMC 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 <a href="#">Firepower Software Readiness Checks with FMC</a>, on page 25.</p> |
|   | <p><b>Check running tasks.</b></p> <p>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.</p>                       |

## 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.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. However, with major and maintenance upgrades *from* Version 6.7.0, you can manually cancel failed or in-progress upgrades, and retry failed upgrades; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI.

Note that 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.

**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 the [Upgrade the Software](#) chapter in the release notes.

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 FTD using the FMC'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 FTD upgrades to Version 7.0.x we recommend you use the upgrade wizard instead; see [Upgrade Firepower Threat Defense with FMC \(Version 7.0.0\)](#), on page 59.
- 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 the *Upgrade the Software* chapter in the [Cisco Firepower Release Notes](#) for your target version.

**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. However, 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; use the Upgrade Status pop-up, accessible from the Device Management page and the Message Center, or use the FTD CLI. Note that 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.

**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 5

# 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 65](#)
- [Upgrade FXOS and an ASA Standalone Device or Intra-Chassis Cluster, on page 66](#)
- [Upgrade FXOS and an ASA Active/Standby Failover Pair, on page 71](#)
- [Upgrade FXOS and an ASA Active/Active Failover Pair, on page 81](#)
- [Upgrade FXOS and an ASA Inter-chassis Cluster, on page 92](#)

## 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 4](#)): \_\_\_\_\_  
Current ASA version: \_\_\_\_\_
2. Check ASA/Firepower 4100 and 9300 compatibility ([Cisco Firepower 4100/9300 FXOS Compatibility](#) ).  
Target FXOS version: \_\_\_\_\_  
Target ASA version: \_\_\_\_\_
3. Check the upgrade path for FXOS ([Upgrade Path: FXOS , on page 6](#)). 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 19](#)).
5. Download the target and intermediate ASA versions ([ASA Packages, on page 19](#)).




---

**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 ([Cisco Firepower 4100/9300 FXOS Compatibility](#) ).  
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 guidelines: see *Planning Your Upgrade* in the [Cisco ASA Upgrade Guide](#).
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 17](#).
- 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.
- 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, 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 101](#)).
- 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 102](#)).
- 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:
- 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 upgrade.
  - Click **OK**.
- Step 9** 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.

---

## 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 17](#).
- 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 101](#).
- 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 102](#)).
- 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 102](#).

---

## 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 17](#).
- 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 101](#)).

**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 102](#)).

**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 101](#)).
- 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 102](#)).
- Step 12** Upgrade the ASA logical device image:
- a) Choose **Logical Devices**.  
The **Logical Devices** page opens to show 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 17](#).
- 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 101](#).

**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 102](#)).

**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 N/A Native Application No
 asa 9.4.1.65 N/A 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 102](#).

**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 101](#).

**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 102](#)).

**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 102](#).

**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 101](#)).
- 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 102](#)).
- 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 101](#)).
- 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 102](#)).
- 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 101](#).

#### 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 102](#)).

#### 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 N/A Native Application No
asa 9.4.1.65 N/A 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 102](#).

**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 101](#).

### 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 102](#)).

### 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 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 19**To verify the status of the security modules/security engine and any installed applications, see [Verify the Installation, on page 102](#).**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 101](#)).

**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 102](#)).

**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 17](#).
- 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 101](#).

**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 102](#)).

**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 102](#).

**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 6

# Monitor Upgrade Progress and Verify Installation

- [Monitor the Upgrade Progress, on page 101](#)
- [Verify the Installation, on page 102](#)

## 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 #
```