



Cisco FXOS Release Notes, 2.2(2)

First Published: August 29, 2017

Last Revised: February 14, 2018

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.2(2).

Use this release note as a supplement with the other documents listed in the documentation roadmap:

<http://www.cisco.com/go/firepower9300-docs>

<http://www.cisco.com/go/firepower4100-docs>

Note: The online versions of the user documentation are occasionally updated after the initial release. As a result, the information contained in the documentation on Cisco.com supersedes any information contained in the context-sensitive help included with the product.

This document contains the following sections:

- [Introduction, page 2](#)
- [What's New, page 2](#)
 - [New Features in FXOS 2.2.2.28, page 2](#)
 - [New Features in FXOS 2.2.2.26, page 2](#)
 - [New Features in FXOS 2.2.2.24, page 2](#)
 - [New Features in FXOS 2.2.2.19, page 3](#)
 - [New Features in FXOS 2.2.2.17, page 3](#)
- [Software Download, page 3](#)
- [Important Notes, page 3](#)
- [Adapter Bootloader Upgrade, page 4](#)
- [System Requirements, page 5](#)
- [Upgrade Instructions, page 5](#)
 - [Installation Notes, page 6](#)
 - [Upgrade a Firepower Security Appliance with No Logical Devices Configured, page 6](#)
 - [Upgrade a Firepower Security Appliance Running Standalone Firepower Threat Defense Logical Devices or a Firepower Threat Defense Intra-Chassis Cluster, page 7](#)
 - [Upgrade Firepower Security Appliances with Firepower Threat Defense Logical Devices in a Failover Configuration, page 7](#)
 - [Upgrade Firepower Security Appliances Configured as a Firepower Threat Defense Inter-Chassis Cluster, page 8](#)
 - [Upgrade a Firepower Security Appliance Running Standalone ASA Logical Devices or an ASA Intra-Chassis Cluster, page 9](#)
 - [Upgrade Firepower Security Appliances with ASA Logical Devices in a Failover Configuration, page 10](#)

- [Upgrade Firepower Security Appliances Configured as an ASA Inter-Chassis Cluster, page 12](#)
- [Open and Resolved Bugs, page 14](#)
 - [Open Bugs, page 14](#)
 - [Resolved Bugs in FXOS 2.2.2.28](#)
 - [Resolved Bugs in FXOS 2.2.2.26, page 16](#)
 - [Resolved Bugs in FXOS 2.2.2.24, page 16](#)
 - [Resolved Bugs in FXOS 2.2.2.19, page 16](#)
 - [Resolved Bugs in FXOS 2.2.2.17, page 17](#)
- [Related Documentation, page 18](#)
- [Obtain Documentation and Submit a Service Request, page 18](#)

Introduction

The Cisco Firepower security appliance is a next-generation platform for network and content security solutions. The Firepower security appliance is part of the Cisco Application Centric Infrastructure (ACI) Security Solution and provides an agile, open, secure platform that is built for scalability, consistent control, and simplified management.

The Firepower security appliance provides the following features:

- **Modular chassis-based security system**—Provides high performance, flexible input/output configurations, and scalability.
- **Firepower Chassis Manager**—Graphical user interface provides a streamlined, visual representation of the current chassis status and allows for simplified configuration of chassis features.
- **FXOS CLI**—Provides command-based interface for configuring features, monitoring chassis status, and accessing advanced troubleshooting features.
- **FXOS REST API**—Allows users to programmatically configure and manage their chassis.

What's New

New Features in FXOS 2.2.2.28

Cisco FXOS 2.2.2.28 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see [Resolved Bugs in FXOS 2.2.2.28](#)).

New Features in FXOS 2.2.2.26

Cisco FXOS 2.2.2.26 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see [Resolved Bugs in FXOS 2.2.2.26, page 16](#)).

New Features in FXOS 2.2.2.24

Cisco FXOS 2.2.2.24 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see [Resolved Bugs in FXOS 2.2.2.24, page 16](#)).

New Features in FXOS 2.2.2.19

Cisco FXOS 2.2.2.19 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see [Resolved Bugs in FXOS 2.2.2.19, page 16](#)).

New Features in FXOS 2.2.2.17

Cisco FXOS 2.2.2.17 introduces the following new features:

- Support for FTD 6.2.2.
- Support for ASA 9.8(2).
- Fixes for various problems (see [Resolved Bugs in FXOS 2.2.2.17, page 17](#)).

Software Download

You can download software images for FXOS and supported applications from one of the following URLs:

- Firepower 9300 — <https://software.cisco.com/download/type.html?mdfid=286287252>
- Firepower 4100 — <https://software.cisco.com/download/navigator.html?mdfid=286305164>

For information about the applications that are supported on a specific version of FXOS, see the *Cisco FXOS Compatibility* guide at this URL:

<http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html>

Important Notes

- When you configure Radware DefensePro (vDP) in a service chain on a currently running Firepower Threat Defense application on a Firepower 4110 or 4120 device, the installation fails with a fault alarm. As a workaround, stop the Firepower Threat Defense application instance before installing the Radware DefensePro application. Note that this issue and workaround apply to all supported releases of Radware DefensePro service chaining with Firepower Threat Defense on Firepower 4110 and 4120 devices.

- Firmware Upgrade—We recommend upgrading your Firepower 4100/9300 security appliance with the latest firmware.

Cisco FXOS firmware package 1.0.16 provides improvements to the Supervisor FPGA and includes a fix so that the Security Engine on the Firepower 4100 series security appliance is restarted whenever the chassis is rebooted. The 1.0.16 firmware package also includes updates to the Supervisor ROMMON to support new SPI flash parts used in manufacturing Firepower 4100/9300 security appliances. All Firepower 4100/9300 security appliances using the new SPI flash will ship with updated firmware.

Before you can use the Secure Unlock feature, the security appliance must have firmware package 1.0.12 or later installed.

Before you can use a Firepower 2-port 100G Network Module (FPR9K-DNM-2X100G) with your Firepower 9300 security appliance, the security appliance must have firmware package 1.0.10 or later installed.

For instructions on how to verify your firmware package version and to upgrade the firmware if necessary, see the “Firmware Upgrade” topic in the *Cisco FXOS CLI Configuration Guide, 2.2(2)* or *Cisco FXOS Firepower Chassis Manager Configuration Guide, 2.2(2)* (<http://www.cisco.com/go/firepower9300-config>).

Adapter Bootloader Upgrade

FXOS 2.2(2) contains additional testing to verify the security module adapters on your security appliance. After installing FXOS 2.2.2.17 or later, you might receive the following critical fault on your security appliance indicating that you should update the firmware for your security module adapter:

```
Critical F1715      2017-05-11T11:43:33.121      339561 Adapter 1 on Security Module 1
requires a critical firmware upgrade. Please see Adapter Bootloader Upgrade instructions
in the FXOS Release Notes posted with this release.
```

If you receive the above message, use the following procedure to update the boot image for your adapter:

1. Connect to the FXOS CLI on your Firepower security appliance. For instructions, see the “Accessing the FXOS CLI” topic in the *Cisco FXOS CLI Configuration Guide* or the *Cisco FXOS Firepower Chassis Manager Configuration Guide* (see [Related Documentation](#), page 18).

2. Enter the adapter mode for the adapter whose boot image you are updating:

```
fxos-chassis# scope adapter 1/security_module_number/adapter_number
```

3. Enter **show image** to view the available adapter images and to verify that fxos-m83-8p40-cruzboot.4.0.1.62.bin is available to be installed:

```
fxos-chassis /chassis/server/adapter # show image
```

| Name | Type | Version |
|-------------------------------------|--------------|------------|
| ----- | ----- | ----- |
| fxos-m83-8p40-cruzboot.4.0.1.62.bin | Adapter Boot | 4.0 (1.62) |
| fxos-m83-8p40-vic.4.0.1.51.gbin | Adapter | 4.0 (1.51) |

4. Enter **update boot-loader** to update the adapter boot image to version 4.0.1.62:

```
fxos-chassis /chassis/server/adapter # update boot-loader 4.0(1.62)
```

Warning: Please DO NOT reboot blade or chassis during upgrade, otherwise, it may cause adapter to become UNUSABLE!

After upgrade has completed, blade will be power cycled automatically

```
fxos-chassis /chassis/server/adapter* # commit-buffer
```

5. Enter **show boot-update status** to monitor the update status:

```
fxos-chassis /chassis/server/adapter # show boot-update status
```

State: Updating

```
fxos-chassis /chassis/server/adapter # show boot-update status
```

State: Ready

6. Enter **show version detail** to verify that the update was successful:

Note: Your **show version detail** output might differ from the following example. However, verify that Bootloader-Update-Status is “Ready” and that Bootloader-Vers is 4.0(1.62).

```
fxos-chassis /chassis/server/adapter # show version detail
```

Adapter 1:

Running-Vers: 5.2(1.2)

Package-Vers: 2.2(2.17)

Update-Status: Ready

Activate-Status: Ready

Bootloader-Update-Status: Ready

Startup-Vers: 5.2(1.2)

Backup-Vers: 5.0(1.2)

Bootloader-Vers: 4.0(1.62)

System Requirements

You can access the Firepower Chassis Manager using the following browsers:

- Mozilla Firefox—Version 42 and later
- Google Chrome—Version 47 and later
- Microsoft Internet Explorer—Version 11 and later

We tested FXOS 2.2(2) using Mozilla Firefox version 42, Google Chrome version 47, and Internet Explorer version 11. We anticipate that future versions of these browsers will also work. However, if you experience any browser-related issues, we suggest you revert to one of the tested versions.

Upgrade Instructions

Use the following tables for guidance on the upgrade path required to move from older releases to this release. For instructions on upgrading to a specific release, see the release notes document for that release:

<http://www.cisco.com/c/en/us/support/security/firepower-9000-series/products-release-notes-list.html>

Note: If you are running a version of FXOS earlier than FXOS 1.1(4), see the *Cisco FXOS Release Notes, 1.1(4)* for information on how to upgrade your system to FXOS 1.1(4).

Table 1 Upgrade Paths for Firepower 9300/4100 with Firepower Threat Defense Logical Devices

| Current Version | Upgrade Path | | |
|--------------------------------------|--------------|---------------------------------------|---|
| FXOS 2.2(2.x) FTD 6.2.0.x/6.2.2.x | → | FXOS 2.2(2.28) FTD 6.2.0.x/6.2.2.x | |
| FXOS 2.2(1.x) FTD 6.2.0.x | → | FXOS 2.2(2.28) FTD 6.2.0.x/6.2.2.x | |
| FXOS 2.1(1.x) FTD 6.2.0.x | → | FXOS 2.2(2.28) FTD 6.2.0.x/6.2.2.x | |
| FXOS 2.0(1.x) FTD 6.1.0.x | → | FXOS 2.1(1.64) FTD 6.2.0.x | → FXOS 2.2(2.28) FTD 6.2.0.x/6.2.2.x |
| FXOS 1.1(4.x) FTD 6.0.1.x | → | FXOS 2.0(1.135) FTD 6.1.0.x | → FXOS 2.1(1.64) FTD 6.2.0.x → FXOS 2.2(2.28) FTD 6.2.0.x/6.2.2.x |

Table 2 Upgrade Paths for Firepower 9300/4100 with ASA Logical Devices

| Current Version | Upgrade Path | | | |
|------------------------------------|--------------|--------------------------------------|---|---|
| FXOS 2.2(2.x) ASA 9.8(1)/9.8(2) | → | FXOS 2.2(2.28) ASA 9.8(1)/9.8(2) | | |
| FXOS 2.2(1.x) ASA 9.8(1) | → | FXOS 2.2(2.28) ASA 9.8(1)/9.8(2) | | |
| FXOS 2.1(1.x) ASA 9.7(1) | → | FXOS 2.2(1.63) ASA 9.8(1) | → | FXOS 2.2(2.28) ASA 9.8(1)/9.8(2) |
| FXOS 2.0(1.x) ASA 9.6(2)/9.6(3) | → | FXOS 2.1(1.64) ASA 9.7(1) | → | FXOS 2.2(1.63) ASA 9.8(1) → FXOS 2.2(2.28) ASA 9.8(1)/9.8(2) |
| FXOS 1.1(4.x) ASA 9.6(1) | → | FXOS 2.0(1.135) ASA 9.6(2)/9.6(3) | → | FXOS 2.1(1.64) ASA 9.7(1) → FXOS 2.2(1.63) ASA 9.8(1) → FXOS 2.2(2.28) ASA 9.8(1)/9.8(2) |

Installation Notes

- The upgrade process typically takes between 20 and 30 minutes.

If you are upgrading a Firepower 9300 or Firepower 4100 series security appliance that is running a standalone logical device or if you are upgrading a Firepower 9300 security appliance that is running an intra-chassis cluster, traffic will not traverse through the device while it is upgrading.

If you are upgrading a Firepower 9300 or a Firepower 4100 series security appliance that is part of an inter-chassis cluster, traffic will not traverse through the device being upgraded while it is upgrading. However, the other devices in the cluster will continue to pass traffic.

- When upgrading the FXOS platform bundle software and application CSP images at the same time, do not upload the application CSP images to your security appliance until after you upgrade the FXOS platform bundle software.

Upgrade Instructions

The following table lists the upgrade instructions for your device configuration:

Table 3 Upgrade Instructions by Device Configuration

| Device Configuration | Upgrade Instructions |
|--|--|
| Firepower security appliance that currently has no logical devices configured | Upgrade a Firepower Security Appliance with No Logical Devices Configured, page 6 |
| Firepower security appliance that is running standalone Firepower Threat Defense logical devices or a Firepower Threat Defense intra-chassis cluster | Upgrade a Firepower Security Appliance Running Standalone Firepower Threat Defense Logical Devices or a Firepower Threat Defense Intra-Chassis Cluster, page 7 |
| Firepower security appliances with Firepower Threat Defense logical devices in a failover configuration | Upgrade Firepower Security Appliances with Firepower Threat Defense Logical Devices in a Failover Configuration, page 7 |
| Two or more Firepower security appliances that are configured as a Firepower Threat Defense inter-chassis cluster | Upgrade Firepower Security Appliances Configured as a Firepower Threat Defense Inter-Chassis Cluster, page 8 |
| Firepower security appliance that is running standalone ASA logical devices or an ASA intra-chassis cluster | Upgrade a Firepower Security Appliance Running Standalone ASA Logical Devices or an ASA Intra-Chassis Cluster, page 9 |
| Firepower security appliances with ASA logical devices in a failover configuration | Upgrade Firepower Security Appliances with ASA Logical Devices in a Failover Configuration, page 10 |
| Two or more Firepower security appliances that are configured as an ASA inter-chassis cluster | Upgrade Firepower Security Appliances Configured as an ASA Inter-Chassis Cluster, page 12 |

Upgrade a Firepower Security Appliance with No Logical Devices Configured

If your Firepower security appliance is not yet configured with any logical devices, perform the following steps to update your system to 2.2(2):

1. Download the FXOS 2.2(2) image to your local computer (see [Software Download](#)).
2. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
3. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.

Upgrade a Firepower Security Appliance Running Standalone Firepower Threat Defense Logical Devices or a Firepower Threat Defense Intra-Chassis Cluster

If you are upgrading a Firepower security appliance that is running standalone Firepower Threat Defense logical devices or a Firepower Threat Defense intra-chassis cluster, use the following procedure to update the FXOS version on your Firepower 9300 or Firepower 4100 series security appliance:

Note: After upgrading FXOS, you can then upgrade the Firepower Threat Defense logical devices using the Firepower Management Center. For more information, see the [Firepower System Release Notes](#).

1. Download the FXOS 2.2(2) image to your local computer (see [Software Download](#)).
2. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
3. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.

Upgrade Firepower Security Appliances with Firepower Threat Defense Logical Devices in a Failover Configuration

If you are upgrading Firepower 9300 or Firepower 4100 series security appliances that have Firepower Threat Defense logical devices configured for high availability, use the following procedure to update the FXOS version on your Firepower 9300 or Firepower 4100 series security appliances:

Note: After upgrading FXOS, you can then upgrade the Firepower Threat Defense logical devices using the Firepower Management Center. For more information, see the [Firepower System Release Notes](#).

1. Download the FXOS 2.2(2) image to your local computer (see [Software Download](#)).
2. Upgrade the FXOS bundle on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:
 - a. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
 - b. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.
3. Wait for the chassis to reboot and upgrade successfully:
 - a. Enter **show firmware monitor** under **scope system** to monitor the upgrade process.
 - b. After the upgrade process finishes, enter **show slot** under **scope ssa** to verify that the slots have come “Online.”
 - c. Enter **show app-instance** under **scope ssa** to verify that the applications have come “Online.”
4. Make the Firepower Threat Defense device that you just upgraded the *active* unit so that traffic flows to the upgraded unit. For instructions, see the “Switch the Active Peer in a Firepower Threat Defense High Availability Pair” topic in the *Firepower Management Center Configuration Guide*.

5. Upgrade the FXOS bundle on the Firepower security appliance that contains the *new standby* Firepower Threat Defense logical device:
 - a. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
 - b. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.
6. Wait for the chassis to reboot and upgrade successfully:
 - a. Enter **show firmware monitor** under **scope system** to monitor the upgrade process.
 - b. After the upgrade process finishes, enter **show slot** under **scope ssa** to verify that the slots have come “Online.”
 - c. Enter **show app-instance** under **scope ssa** to verify that the applications have come “Online.”
7. You can now make the unit that you just upgraded the *active* unit as it was before the upgrade.

Upgrade Firepower Security Appliances Configured as a Firepower Threat Defense Inter-Chassis Cluster

If you are upgrading Firepower 9300 or Firepower 4100 series security appliances that are configured as a Firepower Threat Defense inter-chassis cluster, use the following procedure to update the FXOS version on your Firepower 9300 or Firepower 4100 series security appliances.

Note: After upgrading FXOS, you can then upgrade the Firepower Threat Defense logical devices using the Firepower Management Center. For more information, see the [Firepower System Release Notes](#).

Preupgrade Checklist

1. Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the Primary unit). For instructions, see the “Accessing the FXOS CLI” topic in the *Cisco FXOS CLI Configuration Guide* (see [Related Documentation, page 18](#)).
2. Verify that all installed security modules are online:


```
scope ssa
show slot
```
3. Verify that all installed security modules have the correct FXOS version and Firepower Threat Defense version installed:


```
scope server 1/x
show version
scope ssa
show logical-device
```
4. Verify that the cluster operational state is “In-Cluster” for all security modules installed in the chassis and that the *Primary* unit is not on this chassis:


```
scope ssa
show app-instance
```

There should not be any Firepower Threat Defense instance with Cluster Role set to “Master.”

Procedure

1. Download the FXOS 2.2(2) image to your local computer (see [Software Download](#)).
2. Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the Primary unit). For instructions, see the “Accessing the FXOS CLI” topic in the *Cisco FXOS CLI Configuration Guide* (see [Related Documentation, page 18](#)).

3. Upgrade the FXOS bundle on Chassis #2:
 - a. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
 - b. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
4. Wait for the chassis to reboot and upgrade successfully (approximately 15-20 minutes):
 - a. Enter **show firmware monitor** under **scope system** to monitor the upgrade process. Every component should show “Upgrade-Status: Ready.”
 - b. After the upgrade process finishes, verify that all installed security modules are online:


```
scope ssa
show slot
```
 - c. Verify that all applications are currently online:


```
scope ssa
show app-instance
```

Verify that the operational state is “Online” for all applications in the chassis.

Verify that the cluster operational state is “In-Cluster” for all applications in the chassis.

Verify that the cluster role is “Slave” for all applications in the chassis.
5. Set one of the security modules on Chassis #2 as Primary.

After setting one of the security modules on Chassis #2 to Primary, Chassis #1 no longer contains the Primary unit and can now be upgraded.
6. Repeat the Preupgrade Checklist and Steps 2-4 for Chassis #1.
7. If there are any additional chassis included in the cluster, repeat the Preupgrade Checklist and Steps 2-4 for those chassis.
8. To return the Primary role to Chassis #1, set one of the security modules on Chassis #1 as Primary.

Upgrade a Firepower Security Appliance Running Standalone ASA Logical Devices or an ASA Intra-Chassis Cluster

If you are upgrading a Firepower security appliance that is running standalone ASA logical devices or an ASA intra-chassis cluster, use the following procedure to update the FXOS version on your Firepower 9300 or Firepower 4100 series security appliance and to update the ASA version on your logical devices:

1. Download the FXOS 2.2(2) image to your local computer (see [Software Download](#)).
2. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
3. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.
4. Upload the ASA CSP image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower Appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.
5. Upgrade any ASA logical devices (standalone or intra-chassis cluster) using the ASA CSP image. For instructions, see the “Updating the Image Version for a Logical Device” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.

Upgrade Firepower Security Appliances with ASA Logical Devices in a Failover Configuration

If you are upgrading Firepower 9300 or Firepower 4100 series security appliances that have ASA logical devices configured for high availability, use the following procedure to update the FXOS version on your Firepower 9300 or Firepower 4100 series security appliances and to update the ASA version on your logical devices:

1. Download the FXOS 2.2(2) image to your local computer (see [Software Download](#)).
2. Upgrade the FXOS bundle on the Firepower security appliance that contains the *standby* ASA logical device:
 - a. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
 - b. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.
3. Wait for the chassis to reboot and upgrade successfully:
 - a. Enter **show firmware monitor** under **scope system** to monitor the upgrade process.
 - b. After the upgrade process finishes, enter **show slot** under **scope ssa** to verify that the slots have come “Online.”
 - c. Enter **show app-instance** under **scope ssa** to verify that the applications have come “Online.”
4. Upgrade the ASA and vDP logical device images:
 - a. Upload the ASA CSP image to your Firepower security appliance. If Radware DefensePro (vDP) is configured as a decorator for this ASA application and there is an update available, upload the vDP CSP image too.

For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).

- b. Upgrade your logical device image using the ASA CSP image:


```

top (set the scope to the top level in the mode hierarchy)
scope ssa
scope slot x (where x is the slot ID on which the ASA logical device is configured)
scope app-instance asa
set startup-version version
exit
          
```
 - c. If Radware DefensePro is configured as a decorator for this ASA application, upgrade the vDP image:


```

scope app-instance vdp
set startup-version version
exit
          
```
 - d. Commit the configuration:


```

commit-buffer
          
```
 - e. If there are multiple failover peers (with or without Radware DefensePro decorator) configured on the Firepower security appliance, upgrade them using **Steps b-d**.
5. After the upgrade process finishes, verify that the applications are online:


```

scope ssa
show app-instance
      
```
6. Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:

- a. Connect to the ASA console on the Firepower security appliance that contains the *standby* ASA logical device.
 - b. Make this unit active:
failover active
 - c. Save the configuration:
write memory
 - d. Verify that the unit is *active*:
show failover
7. Upgrade the FXOS bundle on the Firepower security appliance that contains the *new standby* ASA logical device:
- a. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
 - b. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide*.
8. Wait for the chassis to reboot and upgrade successfully:
- a. Enter **show firmware monitor** under **scope system** to monitor the upgrade process.
 - b. After the upgrade process finishes, enter **show slot** under **scope ssa** to verify that the slots have come “Online.”
 - c. Enter **show app-instance** under **scope ssa** to verify that the applications have come “Online.”
9. Upgrade the ASA and vDP logical device images:
- a. Upload the ASA CSP image to your Firepower security appliance. If Radware DefensePro (vDP) is configured as a decorator for this ASA application and there is an update available, upload the vDP CSP image too.

For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
 - b. Upgrade your logical device image using the ASA CSP image:
top (set the scope to the top level in the mode hierarchy)
scope ssa
scope slot x (where *x* is the slot ID on which the ASA logical device is configured)
scope app-instance asa
set startup-version version
exit
 - c. If Radware DefensePro is configured as a decorator for this ASA application, upgrade the vDP image:
scope app-instance vdp
set startup-version version
exit
 - d. Commit the configuration:
commit-buffer
 - e. If there are multiple failover peers (with or without Radware DefensePro decorator) configured on the Firepower security appliance, upgrade them using **Steps b-d**.

10. After the upgrade process finishes, verify that the applications are online:

```
scope ssa
show app-instance
```

11. Make the unit that you just upgraded the *active* unit as it was before the upgrade:

- a. Connect to the ASA console on the Firepower security appliance that contains the *new standby* ASA logical device.

- b. Make this unit active:

```
failover active
```

- c. Save the configuration:

```
write memory
```

- d. Verify that the unit is *active*:

```
show failover
```

Upgrade Firepower Security Appliances Configured as an ASA Inter-Chassis Cluster

If you are upgrading Firepower 9300 or Firepower 4100 series security appliances that are configured as an ASA inter-chassis cluster, use the following procedure to update the FXOS version on your Firepower 9300 or Firepower 4100 series security appliances and to update the ASA version on your logical devices.

Preupgrade Checklist

1. Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the Primary unit). For instructions, see the “Accessing the FXOS CLI” topic in the *Cisco FXOS CLI Configuration Guide* or the *Cisco FXOS Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).

2. Verify that all installed security modules are online:

```
scope ssa
show slot
```

3. Verify that all installed security modules have the correct FXOS version and ASA version installed:

```
scope server 1/x
show version
scope ssa
show logical-device
```

4. Verify that the cluster operational state is “In-Cluster” for all security modules installed in the chassis:

```
scope ssa
show app-instance
```

5. Verify that all installed security modules are shown as part of the cluster:

```
connect module x console
show cluster info
```

6. Verify that the *Primary* unit is not on this chassis:

```
scope ssa
show app-instance
```

There should not be any ASA instance with Cluster Role set to “Master.”

Procedure

1. Download the FXOS 2.2(2) image to your local computer (see [Software Download](#)).
2. Connect to the FXOS CLI on Chassis #2 (this should be a chassis that does not have the Primary unit). For instructions, see the “Accessing the FXOS CLI” topic in the *Cisco FXOS CLI Configuration Guide* or the *Cisco FXOS Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
3. Upgrade the FXOS bundle on Chassis #2:
 - a. Upload the FXOS 2.2(2) Platform Bundle image to your Firepower security appliance. For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
 - b. Upgrade your Firepower security appliance using the FXOS 2.2(2) Platform Bundle image. For instructions, see the “Upgrading the Firepower eXtensible Operating System Platform Bundle” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).
4. Wait for the chassis to reboot and upgrade successfully (approximately 15-20 minutes):
 - a. Enter **show firmware monitor** under **scope system** to monitor the upgrade process. Every component should show “Upgrade-Status: Ready.”
 - b. After the upgrade process finishes, verify that all installed security modules are online:


```
scope ssa
show slot
```
 - c. Verify that all ASA applications are currently online:


```
scope ssa
show app-instance
```
5. Upgrade the ASA and vDP logical device images:
 - a. Upload the ASA CSP image to your Firepower security appliance. If Radware DefensePro (vDP) is configured as a decorator for this ASA application and there is an update available, upload the vDP CSP image too.

For instructions, see the “Uploading an Image to the Firepower appliance” topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see [Related Documentation, page 18](#)).

- b. Upgrade your logical device image using the ASA CSP image:


```
top (set the scope to the top level in the mode hierarchy)
scope ssa
scope slot x (where x is the slot ID on which the ASA logical device is configured)
scope app-instance asa
set startup-version version
exit
```
- c. If Radware DefensePro is configured as a decorator for this ASA application, upgrade the vDP image:


```
scope app-instance vdp
set startup-version version
exit
```
- d. Repeat **Steps b-c** for all slots of the logical device installed on this security appliance.
- e. Commit the configuration:


```
commit-buffer
```

- After the upgrade process finishes, verify that the applications are online:

```
scope ssa
show app-instance
```

Verify that the operational state is “Online” for all ASA and vDP applications in the chassis.

Verify that the cluster operational state is “In-Cluster” for all ASA and vDP applications in the chassis.

Verify that the cluster role is “Slave” for all ASA applications in the chassis.

- Set one of the security modules on Chassis #2 as Primary:

```
connect module x console
configure terminal
cluster master
```

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

- Repeat the Preupgrade Checklist and Steps 1-6 for Chassis #1.
- If there are any additional chassis included in the cluster, repeat the Preupgrade Checklist and Steps 1-6 for those chassis.
- To return the Primary role to Chassis #1, set one of the security modules on Chassis #1 as Primary:

```
connect module x console
configure terminal
cluster master
```

Open and Resolved Bugs

The open and resolved bugs for this release are accessible through the Cisco Bug Search Tool. This web-based tool provides you with access to the Cisco bug tracking system, which maintains information about bugs and vulnerabilities in this product and other Cisco hardware and software products.

Note: You must have a Cisco.com account to log in and access the Cisco Bug Search Tool. If you do not have one, you can [register for an account](#).

For more information about the Cisco Bug Search Tool, see the [Bug Search Tool Help & FAQ](#).

Open Bugs

Table 4 Open Bugs Affecting FXOS 2.2(2)

| Identifier | Description |
|----------------------------|--|
| CSCus73654 | ASA do not mark management-only for the mgmt interface assign by LD |
| CSCuu33739 | Physical interface speeds in port-channel are incorrect |
| CSCuu50615 | Onbox Chassis Manager: Unsupported timezones listed on Onbox |
| CSCuw31077 | Filter applied to a interface should be validated |
| CSCuw81066 | Error should be thrown while enabling a session above the disk space |
| CSCux37821 | Platform settings auth the order field shows only lowest-available |
| CSCux63101 | All memory(s) under Memory array shows as unknown in operable column |
| CSCux76704 | Mysterious “>>” box under logical device save box with no pull-down info |
| CSCux77947 | Pcap file size not updated properly when data sent at high rate |
| CSCux98517 | Un-decorating data port for VDP should be allowed from Chassis Manager |

Table 4 Open Bugs Affecting FXOS 2.2(2)

| Identifier | Description |
|----------------------------|---|
| CSCuy21573 | Chassis Manager: Sorting Broken in Updates Page |
| CSCuy31784 | Images are not listed after a delete when filter is used |
| CSCuy98317 | Unable to soft dissociate intf from LD, if LD name has - |
| CSCuz93180 | AAA LDAP configuration does not preserve information if validation fails |
| CSCva86452 | link flap on switch connected to 10G and 40G SR FTW card on power off |
| CSCvb52076 | Link flap on link partner with Watford 1G-Copper FTW module during boot up |
| CSCvb65011 | EntityPhysical MIB has the Sup serial number for the chassis |
| CSCvc03494 | Radware vDP cannot be added into APSolute Vision. As a workaround, you must manually download the device driver and install it into Vision. |
| CSCvc14775 | App-instance stuck at Not Responding if downgraded from FXOS 2.0.1.86 + ASA 9.6.2 to FXOS 1.1.4.140 |
| CSCvc16980 | For CSP image integrity, the Validation State for the FXOS images should be shown as "None" initially |
| CSCvc44522 | Log Capacity on Management controller Server1/1 is very low Warning |
| CSCvd48719 | FTD logical device not allowing user to provide FMC hostname instead of ip |
| CSCvd90177 | Blade went to fault state after doing a MIO reload on QP-D with FXOS 2.2.1.57 |

Resolved Bugs in FXOS 2.2.2.28

The following table lists the previously release-noted and customer-found defects that were resolved in FXOS 2.2.2.28:

Table 5 Resolved Bugs in FXOS 2.2.2.28

| Identifier | Description |
|----------------------------|--|
| CSCve93880 | Cisco FX-OS and NX-OS System Software CLI Command Injection Vulnerability |
| CSCvf60078 | Cisco UCS Mngr, Cisco Firepower 4100 Series NGFW, & Cisco Firepower 9300 Series Devices Cmd Inj Vuln |
| CSCvg22203 | Evaluation of pix-asa for Dnsmasq October 2017 vulnerabilities |
| CSCvg59491 | Etherchannel between FXOS chassis may get stuck in "Suspended" state after reloading simultaneously |
| CSCvg87702 | Unable to copy images using scp from switch boot |
| CSCuw44001 | Address CIAM CVE-2015-5621 in Net-SNMP Master Agent |
| CSCve17075 | Include /dev/mtd0 in fprm detail tech-support |
| CSCvf79289 | FCM Export Configuration doesn't download XML file on IE11 |
| CSCvg02469 | Prevent potential Assertion core for empty CRL filename |
| CSCvg07539 | New QP Intel SSD was not displayed properly |
| CSCvg15516 | Evaluate Red Hat Linux CVE-2017-1000253 Vulnerability |
| CSCvg15519 | Evaluate Red Hat Linux CVE-2017-1000253 Vulnerability |
| CSCvg72204 | SNMPv3 users created for noauth aren't present in FXOS CLI config, only at scope monitoring and GUI |
| CSCvg12566 | Inconsistent reporting on Management Interface for SNMP Queries |
| CSCvg87518 | Ethalyzer command on FX-OS prompts for password when tacacs authentication is enabled |
| CSCvg29876 | FXOS: Change FSM:FAILED fault severity from Critical to Info |

Resolved Bugs in FXOS 2.2.2.26

The following table lists the previously release-noted and customer-found defects that were resolved in FXOS 2.2.2.26:

Table 6 Resolved Bugs in FXOS 2.2.2.26

| Identifier | Description |
|----------------------------|--|
| CSCvg03555 | When multiple NTP servers are configured, NTP status becomes unreachable/invalid |
| CSCvg81822 | FXOS NTP Client chooses IPv4 over Ipv6 when Dual Stack Server Resolution is returned |
| CSCvg81882 | Utilizing FQDN for IPv6 NTP Server causes false "Unreachable or Invalid" state |

Resolved Bugs in FXOS 2.2.2.24

The following table lists the previously release-noted and customer-found defects that were resolved in FXOS 2.2.2.24:

Table 7 Resolved Bugs in FXOS 2.2.2.24

| Identifier | Description |
|----------------------------|--|
| CSCvd27726 | FPR4100 Chassis Manager and CLI still shows the presence of SSD even after removal |
| CSCvd63389 | FXOS may show thermal condition due to loss of connectivity with blade |
| CSCve03660 | Cisco FXOS and NX-OS Authentication, Authorization, and Accounting Denial of Service Vulnerability |
| CSCve85027 | QP-A-STC 92.3.1.2119 failed to downgrade baseline - 'Oper State: In Progress' in 'show detail' o/p |
| CSCve97137 | Apache HTTP Server ap_get_basic_auth_pw() Authentication Bypass Vulnerability |
| CSCvf60220 | Mgmt interface nameif "Diagnostic" getting removed after swapping mgmt interface from LD |
| CSCvf71673 | FP2100 Bandwidth values wrong for port-channel interface |
| CSCvf91479 | Sumitomo 100G LR4 QSFP crashed during EDVT cold corner boot cycle |
| CSCvf95185 | FXOS - Unable to clear SSH host key in local-mgmt CLI |
| CSCvg00589 | FPR4100/9300: FTW feature failing when MIO shuts down/rebooted causing packet loss. |
| CSCvg18454 | MIO does not boot from rommon during recovery process |
| CSCvg19034 | FP9300 unexpected reload due to service "pfma" hap |
| CSCvg25443 | FTD App Instance goes unresponsive after NTP synchronisation completes on FXOS |
| CSCvg27182 | Evaluation of FXOS for Apache/Struts related vulnerabilities |
| CSCvg34848 | NTP Server information not loading when using FQDN for ipv6 |
| CSCvg40142 | ASA Inter-cluster slave blades fail to come online after downgrade CSP from 9.7.1.4 to 9.6.3.1 |
| CSCvg43424 | App-Instance failed to install on BS module 1 FXOS 2.2.2.20, ASA 9.8.2.8 |
| CSCvg54622 | KP-HA:Secondary shows as "Unknown" and Deployment fails after that. |

Resolved Bugs in FXOS 2.2.2.19

The following table lists the previously release-noted and customer-found defects that were resolved in FXOS 2.2.2.19:

Table 8 Resolved Bugs in FXOS 2.2.2.19

| Identifier | Description |
|----------------------------|---|
| CSCvd06442 | Deleting SNMPv3 user should be rejected |
| CSCvd25253 | Bootup MIO with ASA running but FTW pairs in bypass mode |
| CSCvd70434 | Validation error in chassis manager when assigning data int to logical device that was a mgmt int |
| CSCve07152 | CRL must be signed by certificate containing cRLSign key usage |

Table 8 Resolved Bugs in FXOS 2.2.2.19

| Identifier | Description |
|----------------------------|---|
| CSCve26753 | Upon logging into FP with different user other than admin, some show CLI commands fail |
| CSCve56216 | SNMP sysDescr missing software type and version |
| CSCve70132 | Watford and Harlesden showing deprecated OIDs in BS/QP |
| CSCve97422 | Remote Error Code is not correct for Signature Validation failure |
| CSCvf02982 | xml file import failure occur when between Port-channel and ASA or FTD are associated. |
| CSCvf20973 | 40G LOROM 4M copper cable displayed as "QSFP 40G CR4" in show inventory expand detail |
| CSCvf31037 | ipmi is not supported for KP |
| CSCvf36828 | Service manager should support deleting mgmt. port link and re-creating it in a single transaction. |
| CSCvf46372 | Evaluation for the vulnerabilities CVE-2017-1000364 and CVE-2017-1000366 |
| CSCvf46869 | System crash with snm hap reset |
| CSCvf54485 | FXOS: FTW 1G EPM packets with frame size greater than 1554 is getting dropped. |
| CSCvf65919 | FP9300 chassis running fxos 2.1.1.73 reloaded due to license manager service. |
| CSCvf68274 | FP2100 warning message displayed when upgrading ASA bundle is incorrect |
| CSCvf70505 | FPR Chassis manager continues contacting previous TACACS server configured after it is deleted. |
| CSCvf72423 | CSP image download fails while trying via FTP |
| CSCvf73138 | SL: Port smart agent fix for smart agent race condition issue |
| CSCvf95068 | Upgrade to ASA might have a mismatch version after reboot |

Resolved Bugs in FXOS 2.2.2.17

The following table lists the previously release-noted and customer-found defects that were resolved in FXOS 2.2.2.17:

Table 9 Resolved Bugs in FXOS 2.2.2.17

| Identifier | Description |
|----------------------------|--|
| CSCvd32155 | FPR Network Modules returning the wrong vendorequipmenttype |
| CSCvd35471 | App stuck in "Installing" after MIO reboot due to time is set back for 7hr |
| CSCvd58911 | Chassis reboots while copying large (5GB) files to /bootflash |
| CSCvd66066 | FXOS inconsistent behaviour when setting the hostname |
| CSCvd75663 | Help files not loading when we click on ? mark |
| CSCvd88338 | Switch configuration failed - Error: unknown - delete Ipmc ipmc-group 5 |
| CSCvd89895 | FP4100 FXOS 2.1.1.73 ecmp-groups to "del" state intermittently after link shut/unshut |
| CSCvd91049 | Image loading taking more time when downgrading |
| CSCvd98034 | Seeing error message in the output for STS ethanalyzer testcase in clapton image 92.2.1.2016 |
| CSCve02820 | Damaged EPM resistor causes chassis reboot after SFP/QSFP OIR |
| CSCve14981 | FPR4100: insufficient max memory for appAG |
| CSCve16011 | ASA Install Failed with Error message "CSP reached max-app-limit -Install Rejected" |
| CSCve34729 | ASA interfaces may stop passing traffic after ASA reload with FIPS mode enabled |
| CSCve40222 | FCM: SSH encryption and mac algorithms change in Debden |
| CSCve58269 | NTP: change v2 to v3 |
| CSCve58356 | HA isn't working after the initial KP ASA image installation |

Table 9 Resolved Bugs in FXOS 2.2.2.17

| Identifier | Description |
|----------------------------|---|
| CSCve95234 | Unable to collect blade logs. Support send_diag_archive' command failed |
| CSCvf07255 | Application is not coming up after powering the chassis "off" and then "on" |
| CSCvf12326 | Failed Auth renewal causing Smart License to deregister unexpectedly |
| CSCvf14733 | NTP server status does not show correctly for IPv6 |
| CSCvf35263 | Port Manager Debug File portmgr.out contains incomplete Timestamps |

Related Documentation

For additional information on the Firepower 9300 or 4100 series security appliance and FXOS, see [Navigating the Cisco FXOS Documentation](#).

Obtain Documentation and Submit a Service Request

For information on obtaining documentation, using the Cisco Bug Search Tool (BST), submitting a service request, and gathering additional information, see [What's New in Cisco Product Documentation](#).

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the [What's New in Cisco Product Documentation RSS feed](#). The RSS feeds are a free service.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2017-2018 Cisco Systems, Inc. All rights reserved.