Cisco Firepower 4100/9300 FXOS Release Notes, 2.0(1)

First Published: June 23, 2016
Last Revised: June 3, 2019

This document contains release information for Cisco Firepower eXtensible Operating System 2.0(1).

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

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 2.0.1.206

Cisco Firepower eXtensible Operating System 2.0.1.206 introduces the following new features in addition to the features included in earlier releases:

Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.206, page 25).

New Features in FXOS 2.0.1.204

Cisco Firepower eXtensible Operating System 2.0.1.204 introduces the following new features in addition to the features included in earlier releases:

Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.204, page 25).

New Features in FXOS 2.0.1.203

Cisco Firepower eXtensible Operating System 2.0.1.203 introduces the following new features in addition to the features included in earlier releases:

Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.203, page 25).

New Features in FXOS 2.0.1.201

Cisco Firepower eXtensible Operating System 2.0.1.201 introduces the following new features in addition to the features included in earlier releases:

Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.201, page 25).

New Features in FXOS 2.0.1.188

Cisco Firepower eXtensible Operating System 2.0.1.188 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.188, page 26).

New Features in FXOS 2.0.1.159

Cisco Firepower eXtensible Operating System 2.0.1.159 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.159, page 26).

New Features in FXOS 2.0.1.153

Cisco Firepower eXtensible Operating System 2.0.1.153 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.153, page 27).

New Features in FXOS 2.0.1.149

Cisco Firepower eXtensible Operating System 2.0.1.149 introduces the following new features in addition to the features included in earlier releases:

- Adds additional support for verifying security module adapters and provides CLI commands for viewing and updating the boot image for the adapter.

  Note: After installing FXOS 2.0.1.149, you might receive a critical fault asking you to update the firmware for your security module adapters. For instructions, see Adapter Bootloader Upgrade, page 7.

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.149, page 27).

New Features in FXOS 2.0.1.148

Cisco Firepower eXtensible Operating System 2.0.1.148 introduces the following new features in addition to the features included in earlier releases:

- Secure Unlock, also called Cisco Interactive Debug, is a new serviceability feature that implements a secure way of accessing a Linux prompt on the Supervisor Module on Firepower 9300 and Firepower 4100 Series security appliances.

  Note: Before you can use the Secure Unlock feature, the security appliance must have Firmware package 1.0.12 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, 2.0(1)* or *Cisco FXOS Firepower Chassis Manager Configuration Guide, 2.0(1)* (http://www.cisco.com/go/firepower9300-config).

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.148, page 28).

New Features in FXOS 2.0.1.144

Cisco Firepower eXtensible Operating System 2.0.1.144 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.144, page 28).

New Features in FXOS 2.0.1.141

Cisco Firepower eXtensible Operating System 2.0.1.141 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.141, page 29).

New Features in FXOS 2.0.1.135

Cisco Firepower eXtensible Operating System 2.0.1.135 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.135, page 29).

New Features in FXOS 2.0.1.129

Cisco Firepower eXtensible Operating System 2.0.1.129 introduces the following new features in addition to the features included in earlier releases:

Note: FXOS 2.0.1.129 does not support ASA 9.6(1) or FTD 6.0.1.x. If you are running either of these applications on your Firepower security appliance, you must upgrade to FXOS 2.0.1.135 to enable the following features. If you are running ASA 9.6(2) or FTD 6.1, you do not need to upgrade from FXOS 2.0.1.129 to 2.0.1.135 unless you desire the bug fixes included in the newer build.

Note: FXOS 2.0.1.129 is no longer available on Cisco.com and has been superseded by FXOS 2.0.1.135.

- Provides required foundation for future Zero Downtime Upgrade on Firepower security appliance and ASA logical devices in a failover or clustered configuration.
- Added the option to configure the certificate revocation check mode to be either strict or relaxed for IPSec and Secure LDAP connections.
- Added the option to configure enforcement of matching cryptographic key strength between IKE and SA connections for IPSec.
- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.129, page 29).

New Features in FXOS 2.0.1.86

Cisco Firepower eXtensible Operating System 2.0.1.86 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.86, page 30).

New Features in FXOS 2.0.1.68

Cisco Firepower eXtensible Operating System 2.0.1.68 introduces the following new features in addition to the features included in earlier releases:

- Support for ASA 9.6.1.10.
- Increased maximum possible MTU value to 9216 for Jumbo Frame support on logical devices.
- Fixes for various problems (see Resolved Bugs in FXOS 2.0.1.68, page 30).

New Features in FXOS 2.0.1.37

Cisco Firepower eXtensible Operating System 2.0.1.37 introduces the following new features:

- FXOS 2.0(1) contains several new features and numerous enhancements to support achieving compliance with the following certifications: FIPS (Federal Information Processing Standard) 140-2, Common Criteria, UC-APL (Unified Capabilities Approved Product List), and USGv6 (United States Government IPv6).
- You can now perform graceful shutdown for Firepower Threat Defense running on a Firepower 9300 or Firepower 4100 Series security appliance.

- You can now view the latest status for time synchronization with an NTP server.
- You can now schedule when you would like to have configuration settings exported.
- You can now customize the login banners for FXOS.
- Two new user roles are now available: Operations and AAA Administrator.
- Beginning with FXOS 2.0(1), the range of possible values for the maximum number of failed login attempts before a user is locked out of the chassis is now 0-10 (0 means no limit). Also, all types of user accounts (including account type 'admin') are locked out of the system after exceeding the maximum number of login attempts.
- Beginning with FXOS 2.0(1), the session timeout and refresh-period ranges have been changed to 0-600 seconds with a default value of 600 seconds.
- FXOS now supports pulling of log information from Security Modules.
- Information about inline pairs is now propagated from Firepower Threat Defense to FXOS.

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 FXOS, refer to 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

- Firmware Upgrade—We recommend upgrading your Firepower 4100/9300 security appliance with the latest firmware. For information about how to install a firmware update and the fixes included in each update, see https://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/firmware-upgrade/fxos-firmware-upgrade.html.
- If you are running FXOS 2.0(1) and have an ASA logical device that is running 9.6(2), the logical device will go offline if you downgrade FXOS to 1.1(4). To continue using your logical device, you must downgrade the ASA to 9.6(1) which will bring your logical device back online. You can then upgrade the ASA back to 9.6(2).
- Beginning with FXOS 1.1(3), the behavior for port-channels was changed. In FXOS 1.1(3) and later releases, when a port-channel is created, it is now configured as lacp cluster-detach by default and its status will show as down even if the physical link is up. The port-channel will be brought out of cluster-detach mode in the following situations:
  - The port-channel's port-type is set to either cluster or mgmt
  - The port-channel is added as a data port for a logical device that is part of a cluster and at least one security module has joined the cluster

  If the port-channel is removed from the logical device or the logical device is deleted, the port-channel will revert to cluster-detach mode.

Adapter Bootloader Upgrade

FXOS 2.0.1.149 and later adds additional testing to verify the security module adapters on your security appliance. After installing FXOS 2.0.1.149 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 31).
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. Use the **show image** command 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. Use the **update boot-loader** command 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. Use the **show boot-update status** command 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
   ```

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

Testing on FXOS 2.0(1) was performed using Mozilla Firefox version 42 and Google Chrome version 47. 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

Refer to the FXOS Compatibility guide for release version compatibility information. Use older compatible versions of the application only in the context of upgrades. Note that for upgrade-compatible versions, you may be prompted that the application version is not compatible with the new FXOS version; in this case, indicate Yes to continue with the upgrade. You are expected to upgrade the application version as soon as possible.

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

Current Version		Upgrade Path
FXOS 2.0(1.x) FTD 6.1.0.x	→	FXOS 2.0(1.206) FTD 6.1.0.x
FXOS 1.1(4.x) FTD 6.0.1.x	→	FXOS 2.0(1.206) FTD 6.1.0.x

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

Current Version		Upgrade Path						
FXOS 2.0(1.x) ASA 9.6(2)/9.6(3)	→	FXOS 2.0(1.206) ASA 9.6(2)/9.6(3)						
FXOS 1.1(4.x) ASA 9.6(1)	→	FXOS 2.0(1.206) ASA 9.6(2)/9.6(3)						
FXOS 1.1(3.x) ASA 9.5(x)	→	FXOS 1.1(4.179) ASA 9.6(1)	→	FXOS 2.0(1.206) ASA 9.6(2)/9.6(3)				
FXOS 1.1(2.x) ASA 9.4(1)/9.4(2)	→	FXOS 1.1(3.97) ASA 9.5(x)	→	FXOS 1.1(4.179) ASA 9.6(1)	→	FXOS 2.0(1.206) ASA 9.6(2)/9.6(3)		
FXOS 1.1(1.x) ASA 9.4(1)	→	FXOS 1.1(2.178) ASA 9.4(1)/9.4(2)	→	FXOS 1.1(3.97) ASA 9.5(x)	→	FXOS 1.1(4.179) ASA 9.6(1)	→	FXOS 2.0(1.206) ASA 9.6(2)/9.6(3)

Installation Notes

- FXOS 2.0(1.129) does not support ASA 9.6(1) or FTD 6.0.1.x and is no longer available for download. If you are running either of these applications on your Firepower security appliance and have already upgraded to FXOS 2.0(1.129), you must downgrade to FXOS 2.0(1.86) and then upgrade to FXOS 2.0(1.135).
- 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

Refer to the upgrade instructions that apply 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 9
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 10
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 10
Firepower security appliance that is running standalone ASA logical devices or an ASA intra-chassis cluster	Upgrading a Firepower Security Appliance Running Standalone ASA Logical Devices or an ASA Intra-Chassis Cluster, page 11
Firepower security appliances with ASA logical devices in a failover configuration	For instructions on how to upgrade from FXOS 2.0(1.135) or later to a newer version, see Upgrading an ASA Failover Pair Using the Enhanced Zero Downtime Process, page 11. For instructions on how to upgrade from FXOS 2.0(1.86) or earlier to FXOS 2.0(1.135) or later, see Upgrading an ASA Failover Pair, page 14.
Two or more Firepower security appliances that are configured as an ASA inter-chassis cluster	For instructions on how to upgrade from FXOS 2.0(1.135) or later to a newer version, see Upgrading an ASA Inter-chassis Cluster Using the Enhanced Zero Downtime Process, page 18. For instructions on how to upgrade from FXOS 2.0(1.86) or earlier to FXOS 2.0(1.135) or later, see Upgrading an ASA Inter-chassis Cluster, page 21.

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 2.0(1):

1. Download the FXOS 2.0(1) image to your local computer (see Software Download).
2. Upload the FXOS 2.0(1) 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 31).
3. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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 2.0(1) image to your local computer (see Software Download).
2. Upload the FXOS 2.0(1) 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 31).
3. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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 2.0(1) image to your local computer (see Software Download).
2. Upgrade the Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the *standby* Firepower Threat Defense logical device:
   a. Upload the FXOS 2.0(1) 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 31).
   b. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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 Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the *new standby* Firepower Threat Defense logical device:
   a. Upload the FXOS 2.0(1) 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 31).
   b. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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.

Upgrading 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 2.0(1) image to your local machine (see Software Download).
2. Upload the FXOS 2.0(1) 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 31).
3. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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*.

Upgrading an ASA Failover Pair Using the Enhanced Zero Downtime Process

Note: This process is only supported when upgrading from FXOS 2.0(1.135) or later to a newer version. If you are upgrading from FXOS 2.0(1.86) or earlier, see Upgrading an ASA Failover Pair, page 14.

1. Download the FXOS 2.0(1) image to your local machine (see Software Download).
2. Upgrade the Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the ***standby*** ASA logical device:

a. Upload the FXOS 2.0(1) 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 31).

b. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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. Use the **show firmware monitor** command under **scope system** to monitor the upgrade process.

b. After the upgrade process finishes, use the **show slot** command under **scope ssa** to verify that the slots have come "Online."

c. Use the **show app-instance** command under **scope ssa** to verify that the applications have come "online".

4. Upgrade the ASA and vDP logical device images:

a. Upload the ASA 9.6.2.x 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 31).

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 Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the ***new standby*** ASA logical device:

a. Upload the FXOS 2.0(1) 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 31).

b. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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. Use the **show firmware monitor** command under **scope system** to monitor the upgrade process.

b. After the upgrade process finishes, use the **show slot** command under **scope ssa** to verify that the slots have come "Online."

c. Use the **show app-instance** command under **scope ssa** to verify that the applications have come "online".

9. Upgrade the ASA and vDP logical device images:

a. Upload the ASA 9.6.2.x 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 31).

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

Upgrading an ASA Failover Pair

Note: This process is only supported when upgrading from FXOS 2.0(1.86) or earlier to FXOS 2.0(1.135) or later. If you are upgrading from FXOS 2.0(1.135) or later, see Upgrading an ASA Failover Pair Using the Enhanced Zero Downtime Process, page 11.

1. Download the FXOS 2.0(1) image to your local machine (see Software Download).
2. Disable applications on the ***standby*** ASA logical device:
    a. Connect to the FXOS CLI on the Firepower security appliance that contains the ***standby*** ASA logical device. 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 31).
    b. Turn off the ASA application:

       scope ssa
       scope slot *x* (where *x* is the slot ID on which the ASA logical device is configured)
       scope app-instance asa
       disable
       exit

    c. If Radware DefensePro is configured as a decorator for this ASA application, disable it. If not, proceed to **Step d**.

       scope app-instance vdp
       disable
       exit

    d. Commit the configuration:

       commit-buffer

    e. Verify that the applications are offline:

       show app-instance

    Note: It may take 2-5 minutes before all applications are "Offline," as vDP begins stopping only after the security module reboots following the ASA stop. If any of the stop jobs fail, please repeat **Steps b-d**.

    f. If there are multiple failover peers (with or without Radware DefensePro decorator) configured on the Firepower security appliance, disable them and verify using **Steps b-e**.

3. Upgrade the Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the ***standby*** ASA logical device:
   a. Upload the FXOS 2.0(1) 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 31).
   b. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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. Wait for the chassis to reboot and upgrade successfully:
   a. Use the **show firmware monitor** command under **scope system** to monitor the upgrade process.
   b. After the upgrade process finishes, use the **show slot** command under **scope ssa** to verify that the slots have come "Online."
5. Upgrade the ASA and vDP logical device images:
   a. Upload the ASA 9.6.2.x 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 31).
   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**.
6. After the upgrade process finishes, re-enable applications on the ***standby*** ASA logical device:
   a. Use the **show slot** command under **scope ssa** to verify that every slot is "Online."
   b. Use the **show app-instance** command under **scope ssa** to verify that the application has successfully completed upgrade and is now "Offline."
   c. Turn on the ASA application:

      scope ssa
      scope slot *x* (where *x* is the slot ID on which the ASA logical device is configured)
      scope app-instance asa
      enable
      exit

d. If Radware DefensePro is configured as a decorator for this ASA application, enable it. If not, proceed to **Step e**.

scope app-instance vdp
enable
exit

e. Commit the configuration:

commit-buffer

f. Verify that the applications are online:

show app-instance

g. If there are multiple failover peers (with or without Radware DefensePro decorator) configured on the Firepower security appliance, enable them and verify using **Steps a-f**.

7. 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. Enable failover and make active:

failover

failover active

c. Save the configuration:

write memory

d. Verify that the unit is *active*:

show failover

8. Disable applications on the ***new standby*** ASA logical device:

a. Connect to the FXOS CLI on the Firepower security appliance that contains the ***new standby*** ASA logical device. 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 31).

b. Turn off the ASA application:

scope ssa
scope slot *x* (where *x* is the slot ID on which the ASA logical device is configured)
scope app-instance asa
disable
exit

c. If Radware DefensePro is configured as a decorator for this ASA application, disable it. If not, proceed to **Step d**.

scope app-instance vdp
disable
exit

d. Commit the configuration:

commit-buffer

e. Verify that the applications are offline:

show app-instance

Note: It may take 2–5 minutes before all applications are "Offline," as vDP begins stopping only after the security module reboots following the ASA stop. If any of the stop jobs fail, please repeat **Steps b–d**.

f. If there are multiple failover peers (with or without Radware DefensePro decorator) configured on the Firepower security appliance, disable them and verify using **Steps b–e**.

9. Upgrade the Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the ***new standby*** ASA logical device:

a. Upload the FXOS 2.0(1) 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 31).

b. Upgrade your Firepower security appliance using the FXOS 2.0(1) Platform Bundle image. For instructions, see the "Upgrading the Firepower eXtensible Operating System Platform Bundle" topic in the *Cisco Firepower Chassis Manager Configuration Guide*.

10. Wait for the chassis to reboot and upgrade successfully:

a. Use the **show firmware monitor** command under **scope system** to monitor the upgrade process.

b. After the upgrade process finishes, use the **show slot** command under **scope ssa** to verify that the slots have come "Online."

11. Upgrade the ASA and vDP logical device images:

a. Upload the ASA 9.6.2.x 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 31).

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**.

12. After the upgrade process finishes, re-enable applications on the ***new standby*** ASA logical device:
    a. Use the **show slot** command under **scope ssa** to verify that every slot is "Online."
    b. Use the **show app-instance** command under **scope ssa** to verify that the application has successfully completed upgrade and is now "Offline."
    c. Turn on the ASA application:

       scope ssa
       scope slot *x* (where *x* is the slot ID on which the ASA logical device is configured)
       scope app-instance asa
       enable
       exit

    d. If Radware DefensePro is configured as a decorator for this ASA application, enable it. If not, proceed to **Step e**.

       scope app-instance vdp
       enable
       exit

    e. Commit the configuration:

       commit-buffer

    f. Verify that the applications are online:

       show app-instance

    g. If there are multiple failover peers (with or without Radware DefensePro decorator) configured on the Firepower security appliance, enable them and verify using **Steps a-f**.
13. 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. Enable failover and make active:

       failover
       failover active

    c. Save the configuration:

       write memory

    d. Verify that the unit is *active*:

       show failover

Upgrading an ASA Inter-chassis Cluster Using the Enhanced Zero Downtime Process

Note: This process is only supported when upgrading from FXOS 2.0(1.135) or later to a newer version. If you are upgrading from FXOS 2.0(1.86) or earlier, see Upgrading an ASA Inter-chassis Cluster, page 21.

Pre-Upgrade 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 31).
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 2.0(1) image to your local machine (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 31).
3. Upgrade the Firepower eXtensible Operating System bundle on Chassis #2:
   a. Upload the FXOS 2.0(1) 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 31).
   b. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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 31).
4. Wait for the chassis to reboot and upgrade successfully (approximately 15-20 minutes):
   a. Use the **show firmware monitor** command 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 9.6.2.x 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 31).

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

6. 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.

7. 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.

8. Repeat the Pre-Upgrade Checklist and Steps 1-6 for Chassis #1.

9. If there are any additional chassis included in the cluster, repeat the Pre-Upgrade Checklist and Steps 1-6 for those chassis.

10. 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

Upgrading an ASA Inter-chassis Cluster

Note: This process is only supported when upgrading from FXOS 2.0(1.86) or earlier to FXOS 2.0(1.135) or later. If you are upgrading from FXOS 2.0(1.135) or later, see Upgrading an ASA Inter-chassis Cluster Using the Enhanced Zero Downtime Process, page 18.

Pre-Upgrade 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 31).
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 2.0(1) image to your local machine (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 31).
3. Turn off all applications on Chassis #2:
   a. Turn off the ASA application:

      scope ssa
      scope slot *x* (where *x* is the slot ID on which the ASA logical device is configured)
      scope app-instance asa
      disable
      exit

b. If Radware DefensePro is configured as a decorator for this ASA application, disable it. If not, proceed to **Step c**.

scope app-instance vdp
disable
exit

c. Repeat **Steps a-b** for all slots of the logical device installed on this security appliance.

d. Commit the configuration:

commit-buffer

e. Verify that the applications are offline:

top (set the scope to the top level in the mode hierarchy)
scope ssa
show app-instance

Note: It may take 2-5 minutes before all applications are "Offline." If any of the stop jobs fail, please repeat **Steps a-d**.

4. Upgrade the Firepower eXtensible Operating System bundle on Chassis #2:

a. Upload the FXOS 2.0(1) 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 31).

b. Upgrade your Firepower security appliance using the FXOS 2.0(1) 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 31).

5. Wait for the chassis to reboot and upgrade successfully (approximately 15-20 minutes).

Use the **show firmware monitor** command under **scope system** to monitor the upgrade process. Every component should show "Upgrade-Status: Ready."

6. Upgrade the ASA and vDP logical device images:

a. Upload the ASA 9.6.2.x 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 31).

b. Verify that all installed security modules are online:

scope ssa
show slot

c. Verify that all ASA applications are currently offline:

scope ssa
show app-instance

d. 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

e. 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

f. Repeat **Steps d-e** for all slots of the logical device installed on this security appliance.

g. Commit the configuration:

commit-buffer

7. After the upgrade process finishes, re-enable applications on Chassis #2:

a. Use the **show slot** command under **scope ssa** to verify that every slot is "Online."

b. Use the **show app-instance** command under **scope ssa** to verify that all the applications have successfully completed upgrade and are now "Offline."

c. Turn on the ASA application:

scope ssa
scope slot *x* (where *x* is the slot ID on which the ASA logical device is configured)
scope app-instance asa
enable
exit

d. If Radware DefensePro is configured as a decorator for this ASA application, enable it. If not, proceed to **Step e**.

scope app-instance vdp
enable
exit

e. Repeat **Steps c-d** for all slots of the logical device installed on this security appliance.

f. Commit the configuration:

commit-buffer

ASA nodes will automatically rejoin the existing cluster after successful upgrade and re-enabling.

g. Verify that the applications are online:

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.

8. 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.

9. Repeat the Pre-Upgrade Checklist and Steps 1-7 for Chassis #1.

10. If there are any additional chassis included in the cluster, repeat the Pre-Upgrade Checklist and Steps 1-7 for those chassis.

11. 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

Open bugs severity 3 and higher for Firepower eXtensible Operating System 2.0(1) are listed in the following table:

Table 4 Open Bugs Affecting FXOS 2.0(1)

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
CSCuw65954	vDP: mgmt-ip is not updated in vDP after Change management boot strap
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
CSCux85969	QP: Show the PSU as empty if its not present
CSCux98517	Un-decorating data port for VDP should be allowed from Chassis Manager
CSCuy21573	Chassis Manager: Sorting Broken in Updates Page
CSCuy31784	Images are not listed after a delete when filter is used
CSCuy34708	SSP MIO - Kernel spin lock seen on MIO during MIO boot
CSCuy38842	ARP issues when using Flow-offload, ASA transparent LD, HSRP/VRRP
CSCuy58732	Increased Latency in Data traffic in ASA + VDP Cluster with Flow-offload
CSCuy73153	QP 4110: Bad Fixed Port 1-4 on P2D beta unit
CSCuz54858	FTW-Cluster: No Traffic continuity after starting fxos upgrade
CSCuz62795	POST cert requests has invalid error message
CSCuz69280	MIO to blade comms fails. Cannot send heartbeat update messages.
CSCuz81832	During FTD intra-cluster config in CM, the interface info tab is messy
CSCuz93180	AAA LDAP configuration does not preserve information if validation fails

Table 4 Open Bugs Affecting FXOS 2.0(1)

Identifier	Description
CSCva05729	MIO has crashed with FXOS 2.0.1.24 at aclmgr
CSCva11473	Slot occasionally get into Not Responding state after upgrade
CSCva46249	Traffic is not bypassed for 1-2 min after changing bootstrap setting.
CSCva86452	link flap on switch connected to 10G and 40G SR FTW card on power off

Resolved Bugs in FXOS 2.0.1.206

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.206:

Table 5 Resolved Bugs in FXOS 2.0.1.206

Identifier	Description
CSCvi47523	SSP-NTP: ssp-ntp script monitoring script enhancements for XRU, KP

Resolved Bugs in FXOS 2.0.1.204

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.204:

Table 6 Resolved Bugs in FXOS 2.0.1.204

Identifier	Description
CSCvm81014	FP9300/FP4100 Smart Licensing - Unable to register FXOS devices Smart Licensing

Resolved Bugs in FXOS 2.0.1.203

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.203:

Table 7 Resolved Bugs in FXOS 2.0.1.203

Identifier	Description
CSCuy98806	QP Fan LED behavior should include failed condition

Resolved Bugs in FXOS 2.0.1.201

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.201:

Table 8 Resolved Bugs in FXOS 2.0.1.201

Identifier	Description
CSCvf79289	FCM Export Configuration doesn't download XML file on IE11
CSCvf81997	QP backplane went down after repeating cluster bundle/de-bundle
CSCvg02469	Prevent potential Assertion core for empty CRL filename
CSCvg81822	FXOS NTP Client chooses IPv4 over Ipv6 when Dual Stack Server Resolution is returned.
CSCvg87518	Ethanalyzer command on FX-OS prompts for password when tacacs authentication is enabled
CSCvg91754	FXOS NTP Server Corruption Caused by Deleting DNS Server Entry for Resolution

Table 8 Resolved Bugs in FXOS 2.0.1.201

Identifier	Description
CSCvh51597	Option to include domain name / FQDN in system name when queried by SNMP
CSCvh60428	FXOS upgrade from 2.2.1.66 to 2.2.2 or 2.3.1 hangs at fabric-interconnect Failed until reboot.
CSCvh91287	Adjust minimum fan PWM on thermal policy
CSCvh96609	BGP peering flaps during cluster upgrade
CSCvi05189	FPR4100/9300:Adapter uplink interface on security module showing link state unavailable
CSCvi41789	FXOS might crash in \" fcpc hap reset\" service

Resolved Bugs in FXOS 2.0.1.188

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.188:

Table 9 Resolved Bugs in FXOS 2.0.1.188

Identifier	Description
CSCvf63171	SNMP walk not working FXOS Software Version2.2.1.66
CSCvg19034	A Firepower 9300 chassis may unexpectedly reload with the reason of " pfma" hap
CSCvg24820	ASA app-instance running 9.6.1 is disabled when upgrading from 2.0(1.37) to 2.0(1.149)
CSCvg34848	NTP Server information not loading when using FQDN for ipv6
CSCvg53646	FXOS: Memory leak on appAG process
CSCvg59491	Etherchannel between FXOS chassis may get stuck in " Suspended" state after reloading simultaneously
CSCvc70696	FXOS 'Int Mac Tx (errors)' constantly increasing for port-channel interfaces
CSCvd27726	FPR4100 Chassis Manager and CLI still shows the presence of SSD even after removal
CSCvd66066	FXOS inconsistent behaviour when setting the hostname
CSCvd70434	Validation error in chassis manager when assigning data int to logical device that was a mgmt int
CSCvf70505	FPR Chassis manager continues contacting previous TACACS server configured after it is deleted.
CSCvf95185	FXOS - Unable to clear SSH host key in local-mgmt CLI
CSCvg12566	Inconsistent reporting on Management Interface for SNMP Queries
CSCvc38482	ENH: Chassis Manager UI needs message re: setting NTP for SSP FTDs

Resolved Bugs in FXOS 2.0.1.159

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.159:

Table 10 Resolved Bugs in FXOS 2.0.1.159

Identifier	Description
CSCva32541	SSP - Need to support CIMC (BMC) upgrade
CSCvd05201	Blade upgrade de-bundle notification delayed
CSCvd25253	Bootup MIO with ASA running but FTW pairs in bypass mode
CSCvd35471	App stuck in “Installing” after MIO reboot due to time is set back for 7hr

Table 10 Resolved Bugs in FXOS 2.0.1.159

Identifier	Description
CSCvd63389	FXOS may show thermal condition due to loss of connectivity with blade
CSCvd65202	Unable to ping linux machines from ASA
CSCvd88338	Switch configuration failed - Error: unknown - delete lpmc ipmc-group 5
CSCvf14733	NTP server status does not show correctly for IPv6
CSCvf65919	FP9300 chassis running fxos 2.1.1.73 reloaded due to license manager service.
CSCvf72423	CSP image download fails while trying via FTP
CSCvf73138	SL: Port smart agent fix for CSCvf40307

Resolved Bugs in FXOS 2.0.1.153

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.153:

Table 11 Resolved Bugs in FXOS 2.0.1.153

Identifier	Description
CSCuz84989	Thermal fault reported when any logical device is installed on FPR 9300
CSCva50255	SRTS-ChassisManager PLR - undefined error on clicking 'Generate Button'
CSCva70726	MIO crashed after doing reload with SNMP
CSCva82729	Add space before colon in license manager messages.
CSCvc22039	BS/QP: Remove UCSB Info from DME Data Model
CSCvd89895	FP4100 FXOS 2.1.1.73 ecmp-groups to " del" state intermittently after link shut/unshut
CSCve02820	Damaged EPM resistor causes chassis reboot after SFP/QSFP OIR
CSCve14981	QP: insufficient max memory for appAG
CSCve31871	FXOS: unable to collect module tech-support if blade in FTD prompt
CSCve40673	the delivery of cruz core files to MIO was delayed for hours or days
CSCvf12326	SL: Port agent version 1.6.14 to FXOS

Resolved Bugs in FXOS 2.0.1.149

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.149:

Table 12 Resolved Bugs in FXOS 2.0.1.149

Identifier	Description
CSCve28609	build cruz-uboot into platform bundle
CSCve32694	cruz uboot upgrade and serial# fault
CSCve33457	FCM: PLR issue in showing License Status and Return Code

Resolved Bugs in FXOS 2.0.1.148

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.148:

Table 13 Resolved Bugs in FXOS 2.0.1.148

Identifier	Description
CSCuw92801	Waiting for Cruz link. Link flaps.
CSCuy37194	SNM log file incorrectly displaying time
CSCva32099	SSP: Module in chassis can leave the cluster due to chassis hc failure
CSCva42606	SSP: stats client crash seen
CSCva62672	FxOS:Chassis manager accepts special characters for registration key
CSCva67548	STS:BS - Cluster is disabled because chassis-blade out-of-sync detected
CSCvb83067	FXOS didn't perform firmware upgrade if there is only one firmware change
CSCvc33064	CISCO-FIREPOWER-MIB.MY does not contain traps definition
CSCvc58687	Add secure unlock support
CSCvc72840	syslog for secure unlock
CSCvc74860	SSP3RU Cluster broke after out-of-sync error message on Lina
CSCvc77412	Error seen when we issue show version in FXOS
CSCvc79927	Upgrading ROMMON, FPGA and EPM FPGA failed
CSCvc91000	remove catalog dependency for memory, disk, CPU on blade
CSCvc96198	Dist-S2S: Coredump file not generated for actual/forced crash as its stuck in Transient_Core_Files
CSCvc98978	BS SSD Operability as N/A and Drive State, Power State, and Link Speed are shown as Unknown
CSCvd24987	SNM trace log should be in the show tech-support
CSCvd43857	svc_sam_bladeAG_log core seen with fxos 92.2.1.1953 + ASA 98.1.1.96
CSCvd48060	FPR 9300 Chassis Manager sending message: WARNING: possible memory leak is detected
CSCvd56418	FP 9300: Blades status under "show firmware monitor" still shows as Upgrading
CSCvd58911	Chassis reboots while copying large (5GB) files to /bootflash
CSCvd85149	Getting error when we click on Permanent License in r201 build
CSCvd86756	License Manager slow memory leak causes licmgr crash and chassis reloads
CSCvd90400	SSP MIO - fix memory leak in cmc
CSCve07152	CRL must be signed by certificate containing cRLSign key usage

Resolved Bugs in FXOS 2.0.1.144

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.144:

Table 14 Resolved Bugs in FXOS 2.0.1.144

Identifier	Description
CSCva42606	SSP: stats client crash seen
CSCvb91501	SFP checksum error when swapping SFP module types
CSCvc54102	Nodes left cluster due to Master sent invite with invalid checksum after node reboot

Table 14 Resolved Bugs in FXOS 2.0.1.144

Identifier	Description
CSCvd36898	FXOS may allocate a CPU core to both control and dataplane which may cause system instability
CSCvd51116	FXOS - Unable to delete partially generated files from workspace folder
CSCvd66415	CC: HTTPS connection failures must be logged to syslog

Resolved Bugs in FXOS 2.0.1.141

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.141:

Table 15 Resolved Bugs in FXOS 2.0.1.141

Identifier	Description
CSCva25230	Platform *SHOULD* return SUCCESS if app already in right status
CSCvb16766	500 Internal Server Error when uploading images with external auth
CSCvb33687	Add tooltip for Red button in Security Engine tab in FCM GUI to indicate what is powered off
CSCvc01835	Interfaces show down and not associated on MIO
CSCvc30488	SSP MIO CLI Copyright still displays 2015
CSCvc55585	IPSec only apply CRL constraint in peer cert in strict mode
CSCvc64787	While enabling FIPS mode- SYSMGR-2-SERVICE_CRASHED: Service “snmpd”
CSCvc88408	Unable to read SSD information at FST
CSCvc91208	Remove faults generated by manager for DIMMs not in catalog
CSCvc98489	Unable to find 9.6.1 ASA app using chassis manager running 2.0.1.136
CSCvc98499	ASA app-instance does not come online after doing an upgrade from 1.1.4.95 to 2.0.1.136

Resolved Bugs in FXOS 2.0.1.135

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.135:

Table 16 Resolved Bugs in FXOS 2.0.1.135

Identifier	Description
CSCvc59936	MIO appAG crashed after running packet capture and deleting the LD
CSCvc69958	ASA 9.6.1 and FTD 6.0.1 not coming online with FXOS 2.0.1.129

Resolved Bugs in FXOS 2.0.1.129

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.129:

Table 17 Resolved Bugs in FXOS 2.0.1.129

Identifier	Description
CSCuz66945	Inter-chassis Graceful upgrade is failing-Master surrendered it's role
CSCvb12835	Check needed on 961 image support for QP-D - FP9K-SM-44
CSCvb58168	SSP fault shows invalid FRU for DIMMs on latest version 2.0.1(68)
CSCvb68332	collecting blade logs from MIO failed
CSCvb73538	help files remain in htdocs folder even after moving them to private_htdocs

Table 17 Resolved Bugs in FXOS 2.0.1.129

Identifier	Description
CSCvb73658	IBM AppScan: api/sys/license/register/status.$$$ temp file download
CSCvb73662	IBM AppScan: Cacheable SSL Page Found api/sys/chassis
CSCvb87098	LDAP: CRL is not obtained from Certificate Distribution Point per RFC 5280
CSCvb87106	IPSec: CRL checking is hard coded to relaxed
CSCvb93522	Error: Timed out communicating with DME after downgrade from r211 to r114
CSCvb94704	CC: Syslogs need to be generated when SSH configuration changes are made.
CSCvb96209	CC: FIPS/CC mode must be logged in audit log
CSCvc25846	ASA Blade goes unresponsive after NTP configuration on FXOS
CSCvc32575	Syslog : syslog messages show unrelated home directory info
CSCvc44443	LDAP-crl: Syslogs do not have info related to ldap auth failure

Resolved Bugs in FXOS 2.0.1.86

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.86:

Table 18 Resolved Bugs in FXOS 2.0.1.86

Identifier	Description
CSCva84501	FTD mode not getting applied from chassis manager to FTD
CSCvb29020	Syslog message %KERN-3-SYSTEM_MSG on FP9300
CSCvb48642	Evaluation of ssp for Openssl September 2016
CSCvb59511	FP9300 unexpected reload due to service "lldp" hap failure
CSCvb61656	FIPS required 2048-bit or higher

Resolved Bugs in FXOS 2.0.1.68

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.0.1.68:

Table 19 Resolved Bugs in FXOS 2.0.1.68

Identifier	Description
CSCuy79646	SSP: UCSM should not mark blades with correctable errors as degraded
CSCuz67201	SSP: LLDP HAP Reset
CSCuz71155	FTW bypass to standby switchover time over 10 sec with N5K switch
CSCuz99280	MIO has crashed after disabling the Telnet services FXOS 2.0.1.24
CSCva32529	Increase BCM TD2 MTU
CSCva32531	Increase vNIC MTU
CSCva37119	Increase maximum possible vNIC MTU in Cruz Firmware
CSCva37130	Increase maximum possible eNIC MTU
CSCva48653	FP9300 chassis reload with reason "Kernel Panic"

Resolved Bugs in FXOS 2.0.1.37

The following table lists the previously release-noted and customer-found defects that were resolved in Firepower eXtensible Operating System 2.0.1.37:

Table 20 Resolved Bugs in FXOS 2.0.1.37

Identifier	Description
CSCuv76823	1G Copper and Fiber blink on Network Module. Should stay Solid Green
CSCuv99740	Error message is not shown when the session memory usage is full
CSCux83883	9.6.1/QP - Traceback in appagent_async_client_send_thread
CSCuy38586	Breakout ports are not deleted after swapping the 40G EPM w/ 10G EPM

Related Documentation

For additional information on the Firepower 9300 security appliance and the Firepower eXtensible Operating System, see Navigating the Cisco Firepower 9300 Documentation.

Communications, Services, and Additional Information

- To receive timely, relevant information from Cisco, sign up at Cisco Profile Manager.
- To get the business impact you're looking for with the technologies that matter, visit Cisco Services.
- To submit a service request, visit Cisco Support.
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit Cisco Marketplace.
- To obtain general networking, training, and certification titles, visit Cisco Press.
- To find warranty information for a specific product or product family, access Cisco Warranty Finder.

Cisco Bug Search Tool

Cisco Bug Search Tool (BST) is a web-based tool that acts as a gateway to the Cisco bug tracking system that maintains a comprehensive list of defects and vulnerabilities in Cisco products and software. BST provides you with detailed defect information about your products and software.