Cisco Firepower 4100/9300 FXOS Release Notes, 2.1(1)

First Published: January 23, 2017
Last Revised: June 3, 2019

This document contains release information for Cisco Firepower eXtensible Operating System 2.1(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 2.1.1.116

Cisco Firepower eXtensible Operating System 2.1.1.116 introduces the following new features in addition to the features included in earlier releases:

Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.116, page 26).

New Features in FXOS 2.1.1.115

Cisco Firepower eXtensible Operating System 2.1.1.115 introduces the following new features in addition to the features included in earlier releases:

Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.115, page 26).

New Features in FXOS 2.1.1.113

Cisco Firepower eXtensible Operating System 2.1.1.113 introduces the following new features in addition to the features included in earlier releases:

Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.113, page 27).

New Features in FXOS 2.1.1.107

Cisco Firepower eXtensible Operating System 2.1.1.107 introduces the following new features in addition to the features included in earlier releases:

Fixes for various problems (seeResolved Bugs in FXOS 2.1.1.107, page 27).

New Features in FXOS 2.1.1.106

Cisco Firepower eXtensible Operating System 2.1.1.106 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.106, page 27).

New Features in FXOS 2.1.1.97

Cisco Firepower eXtensible Operating System 2.1.1.97 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.97, page 28).

New Features in FXOS 2.1.1.86

Cisco Firepower eXtensible Operating System 2.1.1.86 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.86, page 29).

New Features in FXOS 2.1.1.85

Cisco Firepower eXtensible Operating System 2.1.1.85 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.85, page 29).

New Features in FXOS 2.1.1.83

Cisco Firepower eXtensible Operating System 2.1.1.83 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 2.1.1.83, 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.

- 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, 2.1(1)* or *Cisco FXOS Firepower Chassis Manager Configuration Guide, 2.1(1)* (http://www.cisco.com/go/firepower9300-config).

- Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.83, page 29).

New Features in FXOS 2.1.1.77

Cisco Firepower eXtensible Operating System 2.1.1.77 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.77, page 30).

New Features in FXOS 2.1.1.73

Cisco Firepower eXtensible Operating System 2.1.1.73 introduces the following new features in addition to the features included in earlier releases:

- Support for Service Chaining of Radware DefensePro (vDP) with Firepower Threat Defense on all Firepower 4100 and 9300 devices.

  Note: Radware DefensePro (vDP) with Firepower Threat Defense is supported on FXOS 2.1.1.64 and later, but requires Radware vDP version 8.10.01.17-2, which is being released at the same time as FXOS 2.1.1.73. For more information on version compatibility, see *Cisco FXOS Compatibility* (http://www.cisco.com/c/en/us/td/docs/security/firepower/fxos/compatibility/fxos-compatibility.html).

- Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.73, page 31).

New Features in FXOS 2.1.1.64

Cisco Firepower eXtensible Operating System 2.1.1.64 introduces the following new features:

- New option to remove the Call Home URL via the Firepower Chassis Manager or FXOS CLI.
- You can now configure Console authentication using the Firepower Chassis Manger.

- You can now view and configure the AAA authentication fallback method using the Firepower Chassis Manager.
- FXOS will now verify the integrity of CSP files installed on the system.
- Support for Firepower Threat Defense 6.2.
- Support for ASA 9.7(1).
- Support for Service Chaining of Radware DefensePro (vDP) with Firepower Threat Defense on all Firepower 4100 and 9300 devices.
- Support for 1GB FTW network modules on the Firepower 4100 series security appliances.
- Support high-voltage DC (HVDC) power supply modules on the Firepower 9300 security appliance.
- Support for inter-chassis clustering using Firepower Threat Defense 6.2 and later.
- Inter-site clustering improvement.
- You can now use the FXOS Chassis Manager to enable FIPs/Common Criteria mode to support achieving compliance with FIPS (Federal Information Processing Standard) 140-2 and Common Criteria security certifications.
- FXOS 2.1(1) contains several new features and numerous enhancements to support achieving compliance with the UC-APL (Unified Capabilities Approved Product List) security certification:
  - Enable/Disable FIPS/CC Mode using Firepower Chassis Manager
  - Configuring Management ACL (ip-block) via Firepower Chassis Manager
  - Configuring SSH Server – MAC Authentication via Firepower Chassis Manager
  - Configuring SSH Server – Encryption Algorithms via Firepower Chassis Manager
  - Login Notifications
  - Periodic update of CRL list
  - Client Cert authentication
- You can now enable NTP server authentication.
- FXOS now has an absolute timeout value that will close Firepower Chassis Manager sessions regardless of session use. The absolute timeout value defaults to 60 minutes and can be changed using the FXOS CLI. Refer to the FXOS CLI Configuration Guide for more information.
- Information about data port-channels inline pairs is now propagated from Firepower Threat Defense to FXOS.
- You can now use Firepower Chassis Manager to delete application instances that are not part of a logical device.
- Enhancements to the Packet Capture feature:
  - Filtering based on IPv6 addresses.
  - Specifying the snap length for a session.
  - Support for session sizes from a range of 1 MB to 2 GB. In previous releases, it was from 256 MB to 2 GB.
  - Command to delete all packet capture sessions.
- Enhancements to QoS:
  - LACP Control traffic prioritization for the configured port-channels in FXOS.
  - MIO CPU port queue settings modifications to prioritize internal Control Plane traffic.

- Licensing changes for ASA failover pairs. Only the active unit requests the license entitlements. Previously, both units requested license entitlements.
- Fixes for various problems (see Resolved Bugs in FXOS 2.1.1.64, page 31).

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 or 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

- Beginning with ASA 9.7, the behavior for smart licensing configurations for failover pairs has changed. If you are upgrading an ASA failover pair from 9.6 and earlier to 9.7 and later, you must perform the following steps to upgrade the entitlements on the devices (active unit is device A and standby unit is device B):
  a. If the current standby unit (device B) has any entitlements configured, remove the configuration from the standby unit and instead configure the same entitlements on the active unit (device A). For context count, combine the values from the active unit and standby unit and request the total number on the active unit.
  b. Upgrade the standby unit (device B) and then let it rejoin the failover pair as standby. At this point there is no smart license configuration on device B. For more information, see Upgrading an ASA Failover Pair, page 15.
  c. Upgrade the active unit (device A). During the upgrade, device A will leave the failover pair and device B will become active. All of the entitlements that were configured on device A need to be configured on device B while device A is being upgraded.
  d. After device A finishes upgrading, it will rejoin the failover pair as a standby unit. Since it is now standby, it will release all entitlements and remove the smart license configuration.

     During configuration sync from device B (active) to device A (standby), device A will receive and cache the smart license configuration from device B so that if it ever becomes the active unit, it knows what entitlements need to be requested.
- 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. 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.
- 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 2.1.1.83 and later adds additional testing to verify the security module adapters on your security appliance. After installing FXOS 2.1.1.83 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 32).
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
   ```

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

   Note: Your **show version detail** output might differ from the following example. However, please 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: 5.0(1.2)
       Package-Vers: 2.1(1.83)
   ```

```
Update-Status: Ready
Activate-Status: Ready
Bootloader-Update-Status: Ready
Startup-Vers: 5.0(1.2)
Backup-Vers: 4.0(1.55)
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

Testing on FXOS 2.1(1) was performed 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

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.

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 2.1(1.x) FTD 6.2.0.x	→ FXOS 2.1(1.116) FTD 6.2.0.x		
FXOS 2.0(1.x) FTD 6.1.0.x	→ FXOS 2.1(1.116) FTD 6.2.0.x		
FXOS 1.1(4.x) FTD 6.0.1.x	→ FXOS 2.0(1.135) FTD 6.1.0.x	→	FXOS 2.1(1.116) FTD 6.2.0.x

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

Current Version	Upgrade Path
FXOS 2.1(1.x) ASA 9.7(1)	→ FXOS 2.1(1.116) ASA 9.7(1)

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 2.1(1.116) ASA 9.7(1)		
FXOS 1.1(4.x) ASA 9.6(1)	→ FXOS 2.0(1.135) ASA 9.6(2)/9.6(3)	→ FXOS 2.1(1.116) ASA 9.7(1)	

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

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 10
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 11

Table 3 Upgrade Instructions by Device Configuration

Device Configuration	Upgrade Instructions
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 12
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 FXOS 2.1(1.64) or from FXOS 2.1(1.64) or later to FXOS 2.1(1.97), see Upgrading an ASA Failover Pair Using the Enhanced Zero Downtime Process, page 12. For instructions on how to upgrade from FXOS 2.0(1.37)-2.0(1.86) to FXOS 2.1(1.64), see Upgrading an ASA Failover Pair, page 15.
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 FXOS 2.1(1.64) or from FXOS 2.1(1.64) or later to FXOS 2.1(1.97), see Upgrading an ASA Inter-chassis Cluster Using the Enhanced Zero Downtime Process, page 19. For instructions on how to upgrade from FXOS 2.0(1.37)-2.0(1.86) to FXOS 2.1(1.64), 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 2.1(1):

1. Download the FXOS 2.1(1) image to your local computer (see Software Download).
2. Upload the FXOS 2.1(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 32).
3. Upgrade your Firepower security appliance using the FXOS 2.1(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 2.1(1) image to your local computer (see Software Download).
2. Upload the FXOS 2.1(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 32).
3. Upgrade your Firepower security appliance using the FXOS 2.1(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 2.1(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 2.1(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 32).
   b. Upgrade your Firepower security appliance using the FXOS 2.1(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 2.1(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 32).
   b. Upgrade your Firepower security appliance using the FXOS 2.1(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 2.1(1) image to your local machine (see Software Download).
2. Upload the FXOS 2.1(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 32).
3. Upgrade your Firepower security appliance using the FXOS 2.1(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

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:

Note: This process is only supported when upgrading from FXOS 2.0(1.135) or later to FXOS 2.1(1.64) or from FXOS 2.1(1.64) or later to FXOS 2.1(1.97). If you are upgrading from FXOS 2.0(1.37)-2.0(1.86) to FXOS 2.1(1.64), see Upgrading an ASA Failover Pair, page 15.

1. Download the FXOS 2.1(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 2.1(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 32).
   b. Upgrade your Firepower security appliance using the FXOS 2.1(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 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 32).
   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 2.1(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 32).
   b. Upgrade your Firepower security appliance using the FXOS 2.1(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 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 32).
   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

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:

Note: This process is only supported when upgrading from FXOS 2.0(1.37)–2.0(1.86) to FXOS 2.1(1.64). If you are upgrading from FXOS 2.0(1.135) or later to FXOS 2.1(1.64) or from FXOS 2.1(1.64) or later to FXOS 2.1(1.97), see Upgrading an ASA Failover Pair Using the Enhanced Zero Downtime Process, page 12.

1. Download the FXOS 2.1(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 32).
   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 2.1(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 32).

b. Upgrade your Firepower security appliance using the FXOS 2.1(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 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 32).

   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 32).

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 2.1(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 32).
   b. Upgrade your Firepower security appliance using the FXOS 2.1(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 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 32).
   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

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.

Note: This process is only supported when upgrading from FXOS 2.0(1.135) or later to FXOS 2.1(1.64) or from FXOS 2.1(1.64) or later to FXOS 2.1(1.97). If you are upgrading from FXOS 2.0(1.37)-2.0(1.86) to FXOS 2.1(1.64), 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 32).
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 2.1(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 32).
3. Upgrade the Firepower eXtensible Operating System bundle on Chassis #2:
   a. Upload the FXOS 2.1(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 32).
   b. Upgrade your Firepower security appliance using the FXOS 2.1(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 32).
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 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 32).

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

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.

Note: This process is only supported when upgrading from FXOS 2.0(1.37)-FXOS 2.0(1.86) to FXOS 2.1(1.64). If you are upgrading from FXOS 2.0(1.135) or later to FXOS 2.1(1.64) or from FXOS 2.1(1.64) or later to FXOS 2.1(1.97), see Upgrading an ASA Inter-chassis Cluster Using the Enhanced Zero Downtime Process, page 19.

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 32).
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 2.1(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 32).
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 2.1(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 32).

b. Upgrade your Firepower security appliance using the FXOS 2.1(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 32).

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 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 32).

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 2.1(1) are listed in the following table:

Table 4 Open Bugs Affecting FXOS 2.1(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
CSCuw81066	Error should be thrown while enabling a session above the disk space
CSCuw89854	Error message when creating session above or around 5GB
CSCux37821	Platform settings auth the order field shows only lowest-available
CSCux63101	All memory(s) under Memory array shows as unknown in operable column
CSCux65728	Remove default username/password from vDP and APsolute Vision
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
CSCux85255	Pkt Capture session creation fails if the session name has 'port'
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
CSCuy98317	Unable to soft dissociate intf from LD, if LD name has -
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
CSCva05729	MIO has crashed with FXOS 2.0.1.24 at aclmgr
CSCva11473	Slot occasionally get into Not Responding state after upgrade

Table 4 Open Bugs Affecting FXOS 2.1(1)

Identifier	Description
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
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
CSCvb87967	Logical Device installation fails with error SdLduProvisionLDU
CSCvc03494	Radware vDP cannot be added into APSolute Vision. As a workaround, you must manually download the device driver and install it into Vision.
CSCvc07229	SSH host key-string input is different than ssh user key-string
CSCvc14775	App-instance stuck at Not Responding if downgraded from FXOS 2.0.1.86 + ASA 9.6.2 to FXOX 1.1.4.140
CSCvc16980	For CSP image integrity, the Validation State for the FXOS images should be shown as " None" initially
CSCvc19428	FCM:Not able to create app-port on eventing events
CSCvc22039	BS/QP: Descrepancies seen in the snmpwalk output
CSCvc44522	Log Capacity on Management controller Server1/1 is very low Warning
CSCvc44733	FPR link flaps (err disabled) with certain link partner occasionally.
CSCvc52435	Packet Capture:IPv6 packet capture filter issue
CSCvc53082	FTD appagent pushes DONTRESOLVE in FTD configure manager add when DNS and hostname are passed
CSCvd05138	Attack traffic in transparent mode is detected earlier than routed mode
CSCvd21762	ASA HA: Secondary Standby Unit conn count and CPU keeps increasing for http CPS traffic flow

Resolved Bugs in FXOS 2.1.1.116

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.116:

Table 5 Resolved Bugs in FXOS 2.1.1.116

Identifier	Description
CSCvm05464	CVE-2018-5391 Remote denial of service via improper IP fragment handling
CSCvm81014	FP9300/FP4100 Smart Licensing - Unable to register FXOS devices Smart Licensing

Resolved Bugs in FXOS 2.1.1.115

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.115:

Table 6 Resolved Bugs in FXOS 2.1.1.115

Identifier	Description
CSCvk19056	Cruz adapter kernel panic at sock_poll
CSCvk25751	Cruz mcp crash with dcem-linkstats command
CSCvk25762	Cruz adapter doesn't recover after the crash
CSCvk27410	cruz kernel corefiles lost after transferred to MIO

Resolved Bugs in FXOS 2.1.1.113

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.113:

Table 7 Resolved Bugs in FXOS 2.1.1.113

Identifier	Description
CSCvf81997	QP backplane went down after repeating cluster bundle/de-bundle
CSCvi05189	FPR4100/9300:Adapter uplink interface on security module showing link state unavailable
CSCvi58843	Increase system resiliency when sam.config is not accessible
CSCvj66002	devcmd error messages are shown in the logs

Resolved Bugs in FXOS 2.1.1.107

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.107:

Table 8 Resolved Bugs in FXOS 2.1.1.107

Identifier	Description
CSCvh96609	BGP peering flaps during cluster upgrade

Resolved Bugs in FXOS 2.1.1.106

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.106:

Table 9 Resolved Bugs in FXOS 2.1.1.106

Identifier	Description
CSCvh12439	Transit traffic is dropped by Cluster Slave after Slave reload
CSCve85027	During bundle upgrade, after MIO reboot and come up again, under scope auto-install, "show detail" output "Oper State: In Progress" and it stuck in that state for 1-2 hours.
CSCvg18454	MIO does not boot from rommon during recovery process
CSCvg19034	FP9300 unexpected reload due to service "pfma" hap
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

Table 9 Resolved Bugs in FXOS 2.1.1.106

Identifier	Description
CSCvf91479	Sumitomo 100G LR4 QSFP crashed during EDVT cold corner boot cycle
CSCvf95185	FXOS - Unable to clear SSH host key in local-mgmt CLI
CSCvg03555	NTP status becomes Unreachable/Invalid after some time
CSCvg40142	ASA Inter-cluster slave blades fail to come online after downgrade CSP from 9.7.1.4 to 9.6.3.1
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
CSCvg87518	Ethanalyzer command on FX-OS prompts for password when tacacs authentication is enabled
CSCvg12566	Inconsistent reporting on Management Interface for SNMP Queries

Resolved Bugs in FXOS 2.1.1.97

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.97:

Table 10 Resolved Bugs in FXOS 2.1.1.97

Identifier	Description
CSCvg34848	NTP Server information not loading when using FQDN for ipv6
CSCvd63389	FXOS may show thermal condition due to loss of connectivity with blade
CSCvf01396	Cisco Cisco Adaptive Security Appliance (ASA) Software includes a version of Expat XML Parser that is affected by the vulnerabilities identified by the following Common Vulnerability and Exposures (CVE) ID: CVE-2017-9233
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.
CSCvf72423	CSP image download fails while trying via FTP
CSCvd70434	Validation error in chassis manager when assigning data int to logical device that was a mgmt int
CSCve26753	Upon logging into FP with different user other than admin, some show CLI commands fail
CSCvc57284	MIO - Upgrade to ntp-4.2.8p9 package
CSCve97422	Remote Error Code is not correct for Signature Validation failure
CSCvf36828	Service manager should support deleting mgmt. port link and re-creating it in a single transaction.
CSCvf70505	FPR Chassis manager continues contacting previous TACACS server configured after it is deleted.
CSCvf73138	SL: Port smart agent fix for smart agent race condition issue
CSCvd65202	Unable to ping linux machines from ASA

Resolved Bugs in FXOS 2.1.1.86

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.86:

Table 11 Resolved Bugs in FXOS 2.1.1.86

Identifier	Description
CSCvc70139	App-instance does not come online Error Msg: CPU_Verification_Error
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
CSCvd88338	Switch configuration failed - Error: unknown - delete lpmc ipmc-group 5
CSCve02820	Damaged EPM resistor causes chassis reboot after SFP/QSFP OIR
CSCvf01762	Evaluation for the vulnerabilities CVE-2017-1000364 and CVE-2017-1000366
CSCvf14733	NTP server status does not show correctly for IPv6

Resolved Bugs in FXOS 2.1.1.85

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.85:

Table 12 Resolved Bugs in FXOS 2.1.1.85

Identifier	Description
CSCvd94904	If the browser is other than English setting, the setting cannot be changed correctly on the FCM
CSCve22329	Cannot upgrade FXOS with Japanese FCM due to English language GUI icon
CSCvf12326	SL: Port agent version 1.6.14 to FXOS

Resolved Bugs in FXOS 2.1.1.83

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.83:

Table 13 Resolved Bugs in FXOS 2.1.1.83

Identifier	Description
CSCuw92801	Waiting for Cruz link. Link flaps.
CSCvc58687	Add secure unlock support
CSCvc72840	syslog for secure unlock
CSCvc73959	ASA App-instance start-failed with err "CSP_INSTALL_Completed"
CSCvc96198	Dist-S2S: Coredump file not generated for actual/forced crash as its stuck in Transient_Core_Files
CSCvd05201	Blade upgrade de-bundle notification delayed
CSCvd11605	QP/BS LED of Eth1/1 - 6 fixed ports are in yellow color when no SFP was plugged in
CSCvd58911	Chassis reboots while copying large (5GB) files to /bootflash
CSCvd66066	FXOS inconsistent behaviour when setting the hostname
CSCvd90400	Unexpected reload due to memory leak on FPR4100 and 9300 FXOS platforms
CSCve14981	QP: insufficient max memory for appAG
CSCve28609	build cruz-uboot into platform bundle

Table 13 Resolved Bugs in FXOS 2.1.1.83

Identifier	Description
CSCve31871	FXOS: unable to collect module tech-support if blade in FTD prompt
CSCve32694	cruz uboot upgrade and serial# fault
CSCve40673	the delivery of cruz core files to MIO was delayed for hours or days

Resolved Bugs in FXOS 2.1.1.77

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.77:

Table 14 Resolved Bugs in FXOS 2.1.1.77

Identifier	Description
CSCuy37194	SNM log file incorrectly displaying time
CSCvb83067	FXOS didn't perform firmware upgrade if there is only one firmware change
CSCvb91501	SFP checksum error when swapping SFP module types
CSCvc33064	CISCO-FIREPOWER-MIB.MY does not contain traps definition
CSCvc50397	VDP - START_FAILED, VNIC_Set_Verification_Error
CSCvc74558	Platform need to enhance the way writing to the cfg xml.
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
CSCvd00339	ipmitool install can fail to install when using sstate cache
CSCvd13036	FXOS - Unable to register/unregister smart licensing via Chassis Manager GUI
CSCvd13121	SAM related tech support does not work
CSCvd20784	Incorrect username showing up in chassis manager in case of client certificate authentication
CSCvd24987	SNM trace log should be in the show tech-support
CSCvd36898	FXOS may allocate a CPU core to both control and dataplane which may cause system instability
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
CSCvd51116	FXOS - Unable to delete partially generated files from workspace folder
CSCvd56418	FP 9300: Blades status under " show firmware monitor" still shows as Upgrading
CSCvd63042	Eventhough cluster is formed but cluster state and role shows as 'Not in Cluster'
CSCvd89895	FP4100 FXOS 2.1.1.73 ecmp-groups to " del" state intermittently after link shut/unshut
CSCvd97962	IP-Blocks are not getting cleared after erase samdb

Resolved Bugs in FXOS 2.1.1.73

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.1.1.73:

Table 15 Resolved Bugs in FXOS 2.1.1.73

Identifier	Description
CSCvc30488	SSP MIO CLI Copyright still displays 2015
CSCvc59936	MIO appAG crashed after running packet capture and deleting the LD
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
CSCvc98978	BS SSD Operability as N/A and Drive State, Power State, and Link Speed are shown as Unknown

Resolved Bugs in FXOS 2.1.1.64

The following table lists the previously release-noted and customer-found defects that were resolved in Firepower eXtensible Operating System 2.1.1.64:

Table 16 Resolved Bugs in FXOS 2.1.1.64

Identifier	Description
CSCuw03704	FXOS SW displays incorrect Supervisor VID
CSCuw37616	Deleting&adding interface in append mode has the deleted interface file
CSCuw65954	vDP: mgmt-ip is not updated in vDP after Change management boot strap
CSCux18974	SNMP value has truncated and copyright need to update
CSCux85255	Pkt Capture session creation fails if the session name has 'port'
CSCux94525	FXOS upgrade was allowed during Firmware upgrade.
CSCuy42650	Chassis manager screens get displayed even without logging in
CSCuz39085	Mgmt port in LD cannot be edited from Portchannel to mgmt Interfac 4 FTD
CSCuz41682	CM export:msg needed that On-Demand cant be created if schedule present
CSCuz41747	Onbox Manager: Disable scp/ftp/sftp require password for adding export
CSCuz60358	Chassis Manager default setting denies access for remote users
CSCuz87408	Sorting on hardware & service state disappears info at Security Modules
CSCuz92172	Error message is not right when session memory is exhausted
CSCuz99352	Not able to sort any columns on interfaces
CSCva02605	SSP: Port-channel members showing up in switch CDP neighbor list
CSCva09907	application start failure should not stop FXOS services on the blade
CSCva62672	FxOS:Chassis manager accepts special characters for registration key
CSCva98245	ASA “show inventory” command should be more specific on 9300/4100
CSCvb16766	500 Internal Server Error when uploading images with external auth
CSCvb33687	FxOS:Add tooltip for Red button in Security Engine tab in FCM GUI to indicate what is powered off
CSCvc54102	Nodes left cluster due to Master sent invite with invalid checksum after node reboot

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.