Cisco FXOS Release Notes, 2.2(1)

First Published: May 15, 2017
Last Revised: December 19, 2017

This document contains release information for Cisco Firepower eXtensible Operating System 2.2(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 2.2.1.70

Cisco Firepower eXtensible Operating System 2.2.1.70 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.2.1.70, page 17).

New Features in FXOS 2.2.1.66

Cisco Firepower eXtensible Operating System 2.2.1.66 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 2.2.1.66, you might receive a critical fault asking you to update the firmware for your security module adapters. For instructions, see Adapter Bootloader Upgrade, page 4.
- Fixes for various problems (see Resolved Bugs in FXOS 2.2.1.66, page 17).

New Features in FXOS 2.2.1.63

Cisco Firepower eXtensible Operating System 2.2.1.63 introduces the following new features:

- Support for ASA 9.8(1).
- Adds the ability to upgrade the firmware on Network Modules installed in the Firepower chassis.
- You can now examine the maximum failed login attempts lockout status of a user and clear the user's locked out state.
- Provides a new CLI command that consolidates output of different environmental monitoring variables for Firepower security appliances.
- Adds the ability to separately configure the absolute session timeout and idle session timeout for serial console sessions. This allows for disabling the serial console absolute session timeout for debugging needs while maintaining the timeout for other forms of access.
- 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, 2.2(1)* or *Cisco FXOS Firepower Chassis Manager Configuration Guide, 2.2(1)* (http://www.cisco.com/go/firepower9300-config).
- Support for Certificate Revocation List (CRL) checks for HTTPS connections.
- The Flow Offload feature has been improved to support offloading of up to 4 million uni-directional flows or 2 million bi-directional flows per security module.
- Fixes for various problems (see Resolved Bugs in FXOS 2.2.1.63, page 17).

Software Download

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

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

For information about the applications that are supported on a specific version 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

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

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

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

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

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

  For instructions on how to verify your firmware package version and to upgrade the firmware if necessary, see the "Firmware Upgrade" topic in the *Cisco FXOS CLI Configuration Guide, 2.2(1)* or *Cisco FXOS Firepower Chassis Manager Configuration Guide, 2.2(1)* (http://www.cisco.com/go/firepower9300-config).

- 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 2.2.1.66 and later adds additional testing to verify the security module adapters on your security appliance. After installing FXOS 2.2.1.66 or later, you might receive the following critical fault on your security appliance indicating that you should update the firmware for your security module adapter:

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

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

1. Connect to the FXOS CLI on your Firepower security appliance. For instructions, see the "Accessing the FXOS CLI" topic in the *Cisco FXOS CLI Configuration Guide* or the *Cisco FXOS Firepower Chassis Manager Configuration Guide* (see Related Documentation, page 18).
2. Enter the adapter mode for the adapter whose boot image you are updating:

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

3. 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: 5.2(1.2)
    Package-Vers: 2.2(1.66)
    Update-Status: Ready
    Activate-Status: Ready
    Bootloader-Update-Status: Ready
    Startup-Vers: 5.2(1.2)
    Backup-Vers: 5.0(1.2)
    Bootloader-Vers: 4.0(1.62)
```

System Requirements

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

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

Testing on FXOS 2.2(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

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

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

Current Version	Upgrade Path		
FXOS 2.2(1.x) FTD 6.2.0.x	→ FXOS 2.2(1.70) FTD 6.2.0.x		
FXOS 2.1(1.x) FTD 6.2.0.x	→ FXOS 2.2(1.70) FTD 6.2.0.x		
FXOS 2.0(1.x) FTD 6.1.0.x	→ FXOS 2.1(1.64) FTD 6.2.0.x	→ FXOS 2.2(1.70) 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(1.64) FTD 6.2.0.x	→ FXOS 2.2(1.70) FTD 6.2.0.x

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

Current Version	Upgrade Path		
FXOS 2.2(1.x) ASA 9.8(1)	→ FXOS 2.2(1.70) ASA 9.8(1)		
FXOS 2.1(1.x) ASA 9.7(1)	→ FXOS 2.2(1.70) ASA 9.8(1)		
FXOS 2.0(1.x) ASA 9.6(2)/9.6(3)	→ FXOS 2.1(1.64) ASA 9.7(1)	→ FXOS 2.2(1.70) ASA 9.8(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(1.64) ASA 9.7(1)	→ FXOS 2.2(1.70) ASA 9.8(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 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	Upgrading a Firepower Security Appliance with No Logical Devices Configured, page 7
Firepower security appliance that is running standalone Firepower Threat Defense logical devices or a Firepower Threat Defense intra-chassis cluster	Upgrading a Firepower Security Appliance Running Standalone Firepower Threat Defense Logical Devices or a Firepower Threat Defense Intra-Chassis Cluster, page 7
Firepower security appliances with Firepower Threat Defense logical devices in a failover configuration	Upgrading Firepower Security Appliances with Firepower Threat Defense Logical Devices in a Failover Configuration, page 8
Two or more Firepower security appliances that are configured as a Firepower Threat Defense inter-chassis cluster	Upgrading Firepower Security Appliances Configured as a Firepower Threat Defense Inter-Chassis Cluster, page 9
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 10
Firepower security appliances with ASA logical devices in a failover configuration	Upgrading Firepower Security Appliances with ASA Logical Devices in a Failover Configuration, page 11
Two or more Firepower security appliances that are configured as an ASA inter-chassis cluster	Upgrading Firepower Security Appliances Configured as an ASA Inter-Chassis Cluster, page 13

Upgrading a Firepower Security Appliance with No Logical Devices Configured

If your Firepower security appliance is not yet configured with any logical devices, perform the following steps to update your system to 2.2(1):

1. Download the FXOS 2.2(1) image to your local machine (see Software Download).
2. Upload the FXOS 2.2(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 18).
3. Upgrade your Firepower security appliance using the FXOS 2.2(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*.

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

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

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

1. Download the FXOS 2.2(1) image to your local machine (see Software Download).
2. Upload the FXOS 2.2(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 18).
3. Upgrade your Firepower security appliance using the FXOS 2.2(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*.

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

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

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

1. Download the FXOS 2.2(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*** Firepower Threat Defense logical device:
   a. Upload the FXOS 2.2(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 18).
   b. Upgrade your Firepower security appliance using the FXOS 2.2(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. 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 2.2(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 18).
   b. Upgrade your Firepower security appliance using the FXOS 2.2(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. 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".
7. If desired, you can now make the unit that you just upgraded the *active* unit as it was before the upgrade.

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

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

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

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* (see Related Documentation, page 18).
2. Verify that all installed security modules are online:

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

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

   scope ssa
   show app-instance

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

Procedure

1. Download the FXOS 2.2(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* (see Related Documentation, page 18).
3. Upgrade the Firepower eXtensible Operating System bundle on Chassis #2:
   a. Upload the FXOS 2.2(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 18).

b. Upgrade your Firepower security appliance using the FXOS 2.2(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 18).

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 applications are currently online:

      scope ssa
      show app-instance

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

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

      Verify that the cluster role is "Slave" for all applications in the chassis.

5. Set one of the security modules on Chassis #2 as Primary.

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

6. Repeat the Pre-Upgrade Checklist and Steps 2-4 for Chassis #1.

7. If there are any additional chassis included in the cluster, repeat the Pre-Upgrade Checklist and Steps 2-4 for those chassis.

8. To return the Primary role to Chassis #1, set one of the security modules on Chassis #1 as Primary.

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 2.2(1) image to your local machine (see Software Download).

2. Upload the FXOS 2.2(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 18).

3. Upgrade your Firepower security appliance using the FXOS 2.2(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 Firepower Security Appliances with ASA Logical Devices in a Failover Configuration

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

1. Download the FXOS 2.2(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 2.2(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 18).
   b. Upgrade your Firepower security appliance using the FXOS 2.2(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 18).
   b. Upgrade your logical device image using the ASA CSP image:

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

      scope app-instance vdp
      set startup-version *<version>*
      exit
   d. Commit the configuration:

      commit-buffer
   e. If there are multiple failover peers (with or without Radware DefensePro decorator) configured on the Firepower security appliance, upgrade them using **Steps b-d**.

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

   scope ssa
   show app-instance

6. Make the unit that you just upgraded the *active* unit so that traffic flows to the upgraded unit:
   a. Connect to the ASA console on the Firepower security appliance that contains the ***standby*** ASA logical device.
   b. Make this unit active:

      failover active

   c. Save the configuration:

      write memory

   d. Verify that the unit is *active*:

      show failover

7. Upgrade the Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the ***new standby*** ASA logical device:
   a. Upload the FXOS 2.2(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 18).
   b. Upgrade your Firepower security appliance using the FXOS 2.2(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 18).

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

      top (set the scope to the top level in the mode hierarchy)
      scope ssa
      scope slot *x* (where *x* is the slot ID on which the ASA logical device is configured)
      scope app-instance asa
      set startup-version *<version>*
      exit

c. If Radware DefensePro is configured as a decorator for this ASA application, upgrade the vDP image:

scope app-instance vdp
set startup-version *<version>*
exit

d. Commit the configuration:

commit-buffer

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

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

scope ssa
show app-instance

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

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

b. Make this unit active:

failover active

c. Save the configuration:

write memory

d. Verify that the unit is *active*:

show failover

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

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

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 18).
2. Verify that all installed security modules are online:

scope ssa
show slot

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

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

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

   scope ssa
   show app-instance

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

   connect module *x* **console**
   show cluster info

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

   scope ssa
   show app-instance

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

Procedure

1. Download the FXOS 2.2(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 18).
3. Upgrade the Firepower eXtensible Operating System bundle on Chassis #2:
   a. Upload the FXOS 2.2(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 18).
   b. Upgrade your Firepower security appliance using the FXOS 2.2(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 18).
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 18).
   b. Upgrade your logical device image using the ASA CSP image:

      top (set the scope to the top level in the mode hierarchy)
      scope ssa
      scope slot *x* (where *x* is the slot ID on which the ASA logical device is configured)

scope app-instance asa
set startup-version *<version>*
exit

c. If Radware DefensePro is configured as a decorator for this ASA application, upgrade the vDP image:

scope app-instance vdp
set startup-version *<version>*
exit

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

e. Commit the configuration:

commit-buffer

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

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 2.2(1) are listed in the following table:

Table 4 Open Bugs Affecting FXOS 2.2(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
CSCux37821	Platform settings auth the order field shows only lowest-available
CSCux63101	All memory(s) under Memory array shows as unknown in operable column
CSCux76704	Mysterious “>>” box under logical device save box with no pull-down info
CSCux77947	Pcap file size not updated properly when data sent at high rate
CSCux98517	Un-decorating data port for VDP should be allowed from Chassis Manager
CSCuy21573	Chassis Manager: Sorting Broken in Updates Page
CSCuy31784	Images are not listed after a delete when filter is used
CSCuy98317	Unable to soft dissociate intf from LD, if LD name has -
CSCuz93180	AAA LDAP configuration does not preserve information if validation fails
CSCva86452	link flap on switch connected to 10G and 40G SR FTW card on power off
CSCvb52076	Link flap on link partner with Watford 1G-Copper FTW module during boot up
CSCvb65011	EntityPhysical MIB has the Sup serial number for the chassis
CSCvc03494	Radware vDP cannot be added into APSolute Vision. As a workaround, you must manually download the device driver and install it into Vision.
CSCvc14775	App-instance stuck at Not Responding if downgraded from FXOS 2.0.1.86 + ASA 9.6.2 to FXOS 1.1.4.140
CSCvc16980	For CSP image integrity, the Validation State for the FXOS images should be shown as “None” initially
CSCvc22039	BS/QP: Descrepancies seen in the snmpwalk output
CSCvc44522	Log Capacity on Management controller Server1/1 is very low Warning
CSCvd05138	Attack traffic in transparent mode is detected earlier than routed mode
CSCvd25253	Bootup MIO with ASA running but FTW pairs in bypass mode
CSCvd32155	FPR Network Modules returning the wrong vendorequipmenttype
CSCvd34042	MIO has rebooted while testing the packet capture with 92.2.1.1821
CSCvd35471	App stuck in "Installing" after MIO reboot due to time is set back for 7hr
CSCvd48719	FTD logical device not allowing user to provide FMC hostname instead of ip
CSCvd63389	FXOS may show thermal condition due to loss of connectivity with blade
CSCvd70434	Validation error in chassis manager upon assigning a data intf to ASA that was earlier mgmt intf
CSCvd75663	Help files not loading when we click on ? mark
CSCvd81250	FP9300 FXOS 2.1.1.64 port-channel goes down after multiple shut and no shut on the link from N7K

Table 4 Open Bugs Affecting FXOS 2.2(1)

Identifier	Description
CSCvd90177	Blade went to fault state after doing a MIO reload on QP-D with FXOS 2.2.1.57
CSCvd91049	Image loading taking more time when downgrading
CSCvd98034	Seeing error message in the output for STS ethanlayzer testcase in clapton image 92.2.1.2016

Resolved Bugs in FXOS 2.2.1.70

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.2.1.70:

Table 5 Resolved Bugs in FXOS 2.2.1.70

Identifier	Description
CSCuw92801	Waiting for Cruz link. Link flaps.
CSCvd58911	Chassis reboots while copying large (5GB) files to /bootflash
CSCvd89895	FP4100 FXOS 2.1.1.73 ecmp-groups to " del" state intermittently after link shut/unshut
CSCvd94904	If the browser is other than English setting, the setting cannot be changed correctly on the FCM
CSCve14981	FPR4100: insufficient max memory for appAG
CSCvf07255	Application is not coming up after powering the chassis " off" and then " on"
CSCvf12326	SL: Port agent version 1.6.14 to FXOS
CSCvf14733	NTP server status does not show correctly for IPv6

Resolved Bugs in FXOS 2.2.1.66

The following table lists the defects that were resolved in Firepower eXtensible Operating System 2.2.1.66:

Table 6 Resolved Bugs in FXOS 2.2.1.66

Identifier	Description
CSCvd88338	Switch configuration failed - Error: unknown - delete lpmc ipmc-group 5
CSCve28609	build cruz-uboot into platform bundle
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 2.2.1.63

The following table lists the previously release-noted and customer-found defects that were resolved in Firepower eXtensible Operating System 2.2.1.63:

Table 7 Resolved Bugs in FXOS 2.2.1.63

Identifier	Description
CSCuw89854	Error message when creating session above or around 5GB
CSCux85255	Pkt Capture session creation fails if the session name has 'port'
CSCvb29020	Syslog message %KERN-3-SYSTEM_MSG on FP9300
CSCvb48642	Evaluation of ssp for Openssl September 2016
CSCvb85629	Evaluation of ssp for CVE-2016-5195 (DIRTY CoW)
CSCvb87967	Logical Device installation fails with error SdLduProvisionLDU

Table 7 Resolved Bugs in FXOS 2.2.1.63

Identifier	Description
CSCvb91501	SFP checksum error when swapping SFP module types
CSCvb97771	Add signal number to fxos core dump file name
CSCvc07229	SSH host key-string input is different than ssh user key-string
CSCvc19428	FCM:Not able to create app-port on eventing events
CSCvc33064	CISCO-FIREPOWER-MIB.MY does not contain traps definition
CSCvc44777	FP4100 - " Add Device" under LD menu goes ungrey after several minutes despite there is one installed
CSCvc52435	Packet Capture:IPv6 packet capture filter issue
CSCvc54102	Nodes left cluster due to Master sent invite with invalid checksum after node reboot
CSCvc60078	BootCLI show tech support should not paginate by default
CSCvc61010	MIO crashed after running clustering scripts and deleting the LD
CSCvc65400	BS/QP: blades should not be reset twice when the chassis is powered on
CSCvc69958	ASA 9.6.1 and FTD 6.0.1 not coming online with FXOS 2.0.1.129
CSCvc70139	App-instance does not come online Error Msg: CPU_Verification_Error
CSCvc70696	FXOS 'Int Mac Tx (errors)' constantly increasing for port-channel interfaces
CSCvc79560	Multiple faults for blades 2 and 3 on FPR9300 chassis with only 1 SSP installed
CSCvc91208	Remove faults generated by manager for DIMMs not in catalog
CSCvd13036	FXOS - Unable to register/unregister smart licensing via Chassis Manager GUI
CSCvd21762	ASA HA: Secondary Standby Unit conn count and CPU keeps increasing for http CPS traffic flow
CSCvd33287	Is Firepower 9300 affected by a MITM described in CVE-2016-5387
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
CSCvd60406	In ethanalyzer while capturing packet for inbound-hi interface output showing malformed packet
CSCvd70247	Chassis manager accepts special characters for registration key
CSCvd86756	License Manager slow memory leak causes licmgr crash and chassis reloads
CSCvd90400	SSP MIO - fix memory leak in cmc
CSCvd97962	IP-Blocks are not getting cleared after erase samdb

Related Documentation

For additional information on the Firepower 9300 or 4100 Series security appliance and the Firepower eXtensible Operating System, see Navigating the Cisco Firepower 9300 Documentation.

Obtain Documentation and Submit a Service Request

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

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