Cisco Firepower 4100/9300 FXOS Release Notes, 1.1(4)

First Published: March 20, 2016
Last Revised: August 18, 2017

This document contains release information for Cisco Firepower eXtensible Operating System 1.1(4).

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

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

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

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

This document contains the following sections:

- Introduction, page 2
- What's New, page 2
  - New Features in FXOS 1.1.4.179, page 2
  - New Features in FXOS 1.1.4.178, page 2
  - New Features in FXOS 1.1.4.175, page 3
  - New Features in FXOS 1.1.4.169, page 3
  - New Features in FXOS 1.1.4.140, page 3
  - New Features in FXOS 1.1.4.117, page 3
  - New Features in FXOS 1.1.4.95, page 3
- Software Download, page 4
- Important Notes, page 4
- Adapter Bootloader Upgrade, page 4
- System Requirements, page 5
- Upgrade Instructions, page 6
  - Upgrade Paths for FXOS/ASA, page 6
  - Installation Notes, page 6
  - Upgrading a Standalone Firepower Security Appliance, page 6
  - Upgrading an ASA Failover Pair, page 7
  - Upgrading an Inter-chassis Cluster, page 10
- Open and Resolved Bugs, page 12

– Open Bugs, page 13
– Resolved Bugs in FXOS 1.1.4.179, page 14
– Resolved Bugs in FXOS 1.1.4.178, page 14
– Resolved Bugs in FXOS 1.1.4.175, page 14
– Resolved Bugs in FXOS 1.1.4.169, page 14
– Resolved Bugs in FXOS 1.1.4.140, page 15
– Resolved Bugs in FXOS 1.1.4.117, page 15
– Resolved Bugs in FXOS 1.1.4.95, page 16

- Related Documentation, page 16
- Obtain Documentation and Submit a Service Request, page 17

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 1.1.4.179

Cisco Firepower eXtensible Operating System 1.1.4.179 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 1.1.4.179, page 14).

New Features in FXOS 1.1.4.178

Cisco Firepower eXtensible Operating System 1.1.4.178 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 1.1.4.178, 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 1.1.4.178, page 14).

New Features in FXOS 1.1.4.175

Cisco Firepower eXtensible Operating System 1.1.4.175 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 1.1.4.175, page 14).

New Features in FXOS 1.1.4.169

Cisco Firepower eXtensible Operating System 1.1.4.169 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 1.1.4.169, page 14).

New Features in FXOS 1.1.4.140

Cisco Firepower eXtensible Operating System 1.1.4.140 introduces the following new features in addition to the features included in earlier releases:

- Support for DC power supply modules on Firepower 4100 Series security appliances.
- Increased maximum possible MTU value to 9216 for Jumbo Frame support on logical devices.
- Fixes for various problems (see Resolved Bugs in FXOS 1.1.4.140, page 15).

New Features in FXOS 1.1.4.117

Cisco Firepower eXtensible Operating System 1.1.4.117 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 1.1.4.117, page 15).

New Features in FXOS 1.1.4.95

Cisco Firepower eXtensible Operating System 1.1.495 introduces the following new features:

- Fixes for various problems (see Resolved Bugs in FXOS 1.1.4.95, page 16).
- Support for ASA 9.6(1).
- Support for Firepower Threat Defense 6.0.1.
- Service Chaining—The Firepower 9300 can support two services chained together on a single security module. In the current supported service chaining configuration, the Radware DefensePro (vDP) third-party application runs in front of the ASA firewall to protect customers and other applications from DDoS attacks. The Radware DefensePro application is not supported on the Firepower 4100 series security appliances, or with Firepower Threat Defense.
- You can now update the firmware on your Firepower security appliance using the CLI.
- You can now store configuration import/export settings in Firepower Chassis Manager so that they can be used for future import or export operations.
- Support for the Firepower 2-port 100G double-wide Network Module (FPR-DNM-2X100G) on the Firepower 9300 security appliance. For more information, see the *Cisco Firepower 9300 Hardware Installation Guide* (http://www.cisco.com/c/en/us/td/docs/security/firepower/9300/hw/guide/b_install_guide_9300.html).

Note: Your Firepower 9300 security appliance must have Firmware package 1.0.10 or later installed before you can use the Firepower 100G Network Module. 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, 1.1(4)* or *Cisco FXOS Firepower Chassis Manager Configuration Guide, 1.1(4)* (http://www.cisco.com/go/firepower9300-config).

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

- Before you can use a Firepower 100G Network Module 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, 1.1(4)* or *Cisco FXOS Firepower Chassis Manager Configuration Guide, 1.1(4)* (http://www.cisco.com/go/firepower9300-config).
- If you are running FXOS 2.0(1) and have an ASA logical device that is running 9.6(2), the logical device will go offline if you downgrade FXOS to 1.1(4). To continue using your logical device, you must downgrade the ASA to 9.6(1) which will bring your logical device back online. You can then upgrade the ASA back to 9.6(2).
- If you are downgrading to FXOS 1.1(4) from a higher version and you have installed any network modules that are not supported on FXOS 1.1(4), you must uninstall those network modules before downgrading to FXOS 1.1(4).
- Zero downtime upgrade is not supported when upgrading your FXOS logical devices to ASA 9.6(1).
- 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.
- To use ASDM and other strong encryption features such as VPN, after you deploy an ASA cluster you must enable the Strong Encryption (3DES) license on the master unit using the ASA CLI.

Adapter Bootloader Upgrade

FXOS 1.1.4.178 and later adds additional testing to verify the security module adapters on your security appliance. After installing FXOS 1.1.4.178 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 16).
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: 4.1(4.6)
       Package-Vers: 1.1(4.178)
       Update-Status: Ready
       Activate-Status: Ready
       Bootloader-Update-Status: Ready
       Startup-Vers: 4.1(4.6)
       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

Testing on FXOS 1.1(4) was performed using Mozilla Firefox version 42 and Google Chrome version 47. We anticipate that future versions of these browsers will also work. However, if you experience any browser-related issues, we suggest you revert to one of the tested versions.

Note: If you experience browser issues, try clearing your browser cache.

Upgrade Instructions

You can upgrade your Firepower 9300 security appliance to FXOS 1.1(4.179) if it is currently running any other FXOS 1.1(4) build. If you are running an earlier version of FXOS, refer to Upgrade Paths for FXOS/ASA, page 6 for information on how to upgrade your system to FXOS 1.1(4.95). After upgrading to FXOS 1.1(4.95), you can then upgrade to FXOS 1.1(4.179).

Upgrade Paths for FXOS/ASA

Current Version	Upgrade Path		
FXOS 1.1(3.x) and ASA 9.5.2.x	→ FXOS 1.1(4.95) and ASA 9.6.1		
FXOS 1.1(2.x) and ASA 9.4.x.x	→ FXOS 1.1(3.86) and ASA 9.5.2.2	→ FXOS 1.1(4.95) and ASA 9.6.1	
FXOS 1.1(1.x) and ASA 9.4.1.152	→ FXOS 1.1(2.178) and ASA 9.4.2.146	→ FXOS 1.1(3.86) and ASA 9.5.2.2	→ FXOS 1.1(4.95) and ASA 9.6.1

Installation Notes

- 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.
- Zero downtime upgrade is not supported when upgrading your FXOS logical devices to ASA 9.6(1).

Upgrade Instructions

Refer to the upgrade instructions that apply for your device configuration:

- For instructions on how to upgrade a standalone Firepower security appliance, see Upgrading a Standalone Firepower Security Appliance, page 6.
- For instructions on how to upgrade two Firepower security appliances that are configured as an ASA Failover Pair, see Upgrading an ASA Failover Pair, page 7.
- For instructions on how to upgrade Firepower security appliances that are configured as an inter-chassis cluster, see Upgrading an Inter-chassis Cluster, page 10.

Upgrading a Standalone Firepower Security Appliance

Perform the following steps to update your system to 1.1(4):

1. Download the required FXOS 1.1(4) image to your local machine (see Software Download).
2. Upload the FXOS 1.1(4) 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, 1.1(4)* (see Related Documentation, page 16).

Note: Do not upload the application CSP images at this time. You should only upload the application CSP images after you have successfully upgraded the chassis using the Platform Bundle image.

3. Upgrade your Firepower security appliance using the FXOS 1.1(4) Platform Bundle image. For instructions, see the "Upgrading the Firepower eXtensible Operating System Platform Bundle" topic in the *Cisco Firepower Chassis Manager Configuration Guide, 1.1(4)* (see Related Documentation, page 16).
4. Upload the application CSP images 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, 1.1(4) Beta* (see Related Documentation, page 16).

   Your system has been successfully updated.

   You can now update your existing ASA logical devices using the ASA image or you can use the ASA image when creating a new logical device.

   You can configure a new Firepower Threat Defense logical device using the Firepower Threat Defense image. For instructions, see the "Deploy Firepower Threat Defense" section in the *Cisco Firepower Threat Defense for Firepower 4100 Quick Start Guide* or the *Cisco Firepower Threat Defense for Firepower 9300 Quick Start Guide* (see Related Documentation, page 16).

   Note: If you want to install Firepower Threat Defense on a security module that currently has ASA installed, you must first delete the existing ASA logical device. For instructions, see the "Delete Existing Logical Devices and Application Configurations" topic in the *Cisco Firepower Threat Defense for Firepower 4100 Quick Start Guide* or the *Cisco Firepower Threat Defense for Firepower 9300 Quick Start Guide* (see Related Documentation, page 16).

Upgrading an ASA Failover Pair

1. Download the FXOS 1.1(4) images (see Software Download, page 4).
2. Disable failover:
   a. Connect to the ASA console on the Firepower security appliance that contains the ***primary*** ASA logical device. For instructions, see the "Connect to the Console of the Application or Decorator" topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see Related Documentation, page 16).

   b. Disable failover:

      no failover

   c. Save the configuration on both the Firepower security appliance that contains the ***primary*** ASA logical device and the Firepower security appliance that contains the ***secondary*** ASA logical device:

      write memory
3. Upgrade the Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the ***secondary*** ASA logical device:
   a. Upload the FXOS 1.1(4) 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 16).

   NOTE: Do not upload the ASA image at this time. You should only upload the ASA image after you have successfully upgraded the chassis using the FXOS 1.1(4) Platform Bundle image.

   b. Upgrade your Firepower security appliance using the FXOS 1.1(4) 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 app-instance** command under **scope ssa** to verify that the ASA application has come "Online."
5. Upgrade the ASA software on the ***secondary*** ASA logical device:
   a. Upload the ASA 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 16).
   b. Upgrade the ***secondary*** ASA logical device using the ASA image. For instructions, see the "Updating the Image Version for a Logical Device" topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see Related Documentation, page 16).
   c. Wait for the upgrade process to finish. Use the **show app-instance** command under **scope ssa** to verify that the ASA application has come "online".
6. Re-enable failover:
   a. Connect to the ASA console on the Firepower security appliance that contains the ***primary*** ASA logical device.
   b. Enable failover:

      failover
   c. Save the configuration:

      write memory
   d. Verify that the unit is active:

      show failover
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 ***secondary*** 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 failover again:
   a. Connect to the ASA console on the Firepower security appliance that contains the ***secondary*** ASA logical device (which is currently the *active* unit).
   b. Disable failover:

      no failover
   c. Save the configuration on both the Firepower security appliance that contains the ***primary*** ASA logical device and the Firepower security appliance that contains the ***secondary*** ASA logical device:

write memory

9. Upgrade the Firepower eXtensible Operating System bundle on the Firepower security appliance that contains the ***primary*** ASA logical device:
   a. Upload the FXOS 1.1(4) 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 16).

   NOTE: Do not upload the ASA image at this time. You should only upload the ASA image after you have successfully upgraded the chassis using the FXOS 1.1(4) Platform Bundle image.

   b. Upgrade your Firepower security appliance using the FXOS 1.1(4) 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 16).
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 app-instance** command under **scope ssa** to verify that the ASA application has come "online."
11. Upgrade the ASA software on the ***primary*** ASA logical device:
    a. Upload the ASA 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 16).
    b. Upgrade the ***primary*** ASA logical device using the ASA image. For instructions, see the "Updating the Image Version for a Logical Device" topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see Related Documentation, page 16).
    c. Wait for the upgrade process to finish. Use the **show app-instance** command under **scope ssa** to verify that the ASA application has come "online".
12. Re-enable failover:
    a. Connect to the ASA console on the Firepower security appliance that contains the ***secondary*** ASA logical device.
    b. Enable failover:

       failover
    c. Save the configuration:

       write memory
    d. Verify that the unit is active:

       show failover
13. Make the ***primary*** unit *active*:
    a. Connect to the ASA console on the Firepower security appliance that contains the ***primary*** 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 Inter-chassis Cluster

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 16).
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.

Procedure

1. Download the FXOS 1.1(4) 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 16).
3. For all security modules installed in Chassis #2, connect to the ASA console on each module and disable cluster:

   connect module *x* **console**

   configure terminal

   cluster group *name*

   no enable
4. Upgrade the Firepower eXtensible Operating System bundle on Chassis #2:

a. Upload the FXOS 1.1(4) 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 16).

b. Upgrade your Firepower security appliance using the FXOS 1.1(4) 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 16).

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."

   ASA nodes will automatically rejoin the existing cluster after successful upgrade.

6. After the upgrade process finishes:

   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 ASA application has come "Online."

   c. Use the **show app-instance** command under **scope ssa** to verify that the cluster operational state is "In-Cluster" for all security modules installed in the chassis.

7. Upload the ASA image to Chassis #2. For instructions, see the "Uploading an Image to the Firepower appliance" topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see Related Documentation, page 16).

8. For each security module on Chassis #2:

   a. Upgrade the ASA logical device using the ASA image. For instructions, see the "Updating the Image Version for a Logical Device" topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see Related Documentation, page 16).

   b. Wait for the upgrade process to finish.

   c. Use the **show app-instance** command under **scope ssa** to verify that the ASA application has come "online".

   d. Verify that the Cluster Operational Status for each security module is "in-cluster:"

      connect module *x* **console**

      show cluster info

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

   connect module *x* **console**

   configure terminal

   cluster master

10. Connect to the FXOS CLI on Chassis #1.

11. For all security modules in Chassis #1, connect to the ASA console on each module and disable cluster:

    connect module *x* **console**

    configure terminal

    cluster group *name*

    no enable

12. Upgrade the Firepower eXtensible Operating System bundle on Chassis #1:
    a. Upload the FXOS 1.1(4) 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 16).
    b. Upgrade your Firepower security appliance using the FXOS 1.1(4) 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 16).
13. 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."

    ASA nodes will automatically rejoin the existing cluster after successful upgrade.
14. After the upgrade process finishes:
    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 ASA application has come "Online."
    c. Use the **show app-instance** command under **scope ssa** to verify that the cluster operational state is "In-Cluster" for all security modules installed in the chassis.
15. Upload the ASA image to Chassis #1. For instructions, see the "Uploading an Image to the Firepower appliance" topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see Related Documentation, page 16).
16. For each security module on Chassis #1:
    a. Upgrade the ASA logical device using the ASA image. For instructions, see the "Updating the Image Version for a Logical Device" topic in the *Cisco Firepower Chassis Manager Configuration Guide* (see Related Documentation, page 16).
    b. Wait for the upgrade process to finish.
    c. Use the **show app-instance** command under **scope ssa** to verify that the ASA application has come "online".
    d. Verify that the Cluster Operational Status for each security module is "in-cluster:"

       connect module *x* **console**

       show cluster info
17. If there are any additional chassis included in the cluster, repeat steps 10. through 16. for those chassis.

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 1.1(4) are listed in the following table:

Table 1 Open Bugs Affecting FXOS 1.1(4)

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
CSCuv76823	1G Copper and Fiber blink on EPM. Should stay Solid Green
CSCuv99740	Error message is not shown when the session memory usage is full
CSCuw03704	FXOS SW displays incorrect Supervisor VID
CSCuw31077	Filter applied to a interface should be validated
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
CSCuw81066	Error should be thrown while enabling a session above the disk space
CSCuw89854	Error message when creating session above or around 5GB
CSCux18974	SNMP value has truncated and copyright need to update
CSCux19618	SSP: " show mem" causes tcp drop under high loaded CPU
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
CSCux94525	FXOS upgrade was allowed during Firmware upgrade.
CSCux98517	Un-decorating data port for VDP should be allowed from Chassis Manager
CSCuy05758	SSH: Local auth w/ auth-domain fails if external auth is enabled
CSCuy21573	Chassis Manager: Sorting Broken in Updates Page
CSCuy31784	Images are not listed after a delete when filter is used
CSCuy38586	Breakout ports are not deleted after swapping the 40G EPM w/ 10G EPM
CSCuy42650	Chassis manager screens get displayed even without logging in
CSCuy58732	Increased Latency in Data traffic in ASA + VDP Cluster with Flow-offload

Resolved Bugs in FXOS 1.1.4.179

The following table lists the defects that were resolved in Firepower eXtensible Operating System 1.1.4.179:

Table 2 Resolved Bugs in FXOS 1.1.4.179

Identifier	Description
CSCvd48060	FPR 9300 Chassis Manager sending message: WARNING: possible memory leak is detected
CSCvd86756	License Manager slow memory leak causes licmgr crash and chassis reloads
CSCvd90400	Unexpected reload due to memory leak on FPR4100 and 9300 FXOS platforms

Resolved Bugs in FXOS 1.1.4.178

The following table lists the defects that were resolved in Firepower eXtensible Operating System 1.1.4.178:

Table 3 Resolved Bugs in FXOS 1.1.4.178

Identifier	Description
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 1.1.4.175

The following table lists the defects that were resolved in Firepower eXtensible Operating System 1.1.4.175:

Table 4 Resolved Bugs in FXOS 1.1.4.175

Identifier	Description
CSCvc77412	Error seen when we issue show version in FXOS
CSCvd51116	FXOS - Unable to delete partially generated files from workspace folder

Resolved Bugs in FXOS 1.1.4.169

The following table lists the defects that were resolved in Firepower eXtensible Operating System 1.1.4.169:

Table 5 Resolved Bugs in FXOS 1.1.4.169

Identifier	Description
CSCuy30292	Cores files seen after running CI STS on FP9300 and FP4100
CSCuz60980	SSP fault shows invalid FRU for DIMMs installed
CSCva42606	SSP: stats client crash seen
CSCvb16766	500 Internal Server Error when uploading images with external auth
CSCvb48642	Evaluation of ssp for Openssl September 2016
CSCvb61343	Cisco Firepower 4100/9300 Command Shell Injection Vulnerability
CSCvb83067	FXOS didn't perform firmware upgrade if there is only one firmware change
CSCvb86728	Local privilege escalation through CLI command
CSCvb91501	SFP checksum error when swapping SFP module types
CSCvb93522	Error: Timed out communicating with DME after downgrade from r211 to r114
CSCvc30488	SSP MIO CLI Copyright still displays 2015

Table 5 Resolved Bugs in FXOS 1.1.4.169

Identifier	Description
CSCvc54102	Nodes left cluster due to Master sent invite with invalid checksum after node reboot
CSCvc88408	Unable to read SSD information at FST
CSCvc91000	remove catalog dependency for memory, disk, CPU on blade
CSCvc91208	Remove faults generated by manager for DIMMs not in catalog
CSCvd36898	FXOS may allocate a CPU core to both control and dataplane which may cause system instability

Resolved Bugs in FXOS 1.1.4.140

The following table lists the defects that were resolved in Firepower eXtensible Operating System 1.1.4.140:

Table 6 Resolved Bugs in FXOS 1.1.4.140

Identifier	Description
CSCuy79646	SSP: UCSM should not mark blades with correctable errors as degraded
CSCva32531	Increase vNIC MTU
CSCva47313	mac adress absent on show l2-table in fxos 1.1.4.120
CSCva48653	FP9300 chassis reload with reason " Kernel Panic"
CSCvb29020	Syslog message %KERN-3-SYSTEM_MSG on FP9300
CSCvb59511	FP9300 unexpected reload due to service " lldp" hap failure

Resolved Bugs in FXOS 1.1.4.117

The following table lists the defects that were resolved in Firepower eXtensible Operating System 1.1.4.117:

Table 7 Resolved Bugs in FXOS 1.1.4.117

Identifier	Description
CSCuu70441	Chassis Manager should support cluster hitless upgrade
CSCux32873	SSP: CCL port channel lacp suspended
CSCux83883	9.6.1/QP - Traceback in appagent_async_client_send_thread
CSCuy05579	Need to mask the error messages during MIO upgrade/reboot
CSCuy40667	QP: Chassis Manager give unknown Storage controller operability
CSCuy45358	QP: Security server disk PID/VID not shown
CSCuy66912	Ping does not pass to outside network.FXOS-1.1(4.85) + ASA-9.6.0.124
CSCuy70690	Add app_id support for feature/snm
CSCuy79839	Handle MTS_OPC_SNM_NOTIF_MSG message in portAG
CSCuy85449	R114: show fan-module shows fan in Inoperable state
CSCuy96662	QP-D: Local Disk Drive state, Power State and Link State are UNKNOWN
CSCuz01181	EC: QP FTD reboots several times, after an MIO reboot
CSCuz08655	FPR Chassis manager " Not able to fetch interface list"
CSCuz28099	Inter-chassis Master surrendered role after upgrade started on chassis 2
CSCuz64859	Power switch and shutdown implementation call FPGA power cycle command

Table 7 Resolved Bugs in FXOS 1.1.4.117

Identifier	Description
CSCuz67201	SSP: LLDP HAP Reset
CSCuz67424	Inter-chassis: Dataport bundling takes unexpected long time
CSCuz87408	Sorting on hardware & service state disappears info at Security Modules

Resolved Bugs in FXOS 1.1.4.95

The following table lists the previously release-noted and customer-found defects that were resolved in Firepower eXtensible Operating System 1.1.4.95:

Table 8 Resolved Bugs in FXOS 1.1.4.95

Identifier	Description
CSCut76730	Flow Offload : On new csp install ,offload engine not enabled
CSCuu17780	CLI allows to configure trap as " priv" even when user is set to " sha"
CSCuu18497	NTP radio button not selected even if configured
CSCuv18505	UI issues with creating port-channel (breakout port members) using CM
CSCuv97491	Message enic_get_flowtable_ctrl(): error enic_get_ft_ctrl failed!!
CSCuw61160	Warning message shown 3 times after edit cluster
CSCuw68106	after importing all configuration old user password might not work
CSCuw82080	ChassisManager: Must display port-channel operationalState
CSCuw86671	Smart License information should be included in export/import
CSCuw95062	Bad error messages when downgrading ASA from chassis manager
CSCux03547	SNMP mib object output changed.
CSCux05403	9.5.2/main: VPN-Loadbalancing with SSP shows devices as SpykerD
CSCux05661	Chassis Manager: Acknowledge Security Module refers to " blade server"
CSCux17304	blade is " not responding" but seems to be up
CSCux21401	Disabling cluster member can cause add-on license without standard lic
CSCux26822	If slave with entitlement becomes master, other slaves not synced
CSCux36990	Chassis Manager shows network module as " Empty" intermittently
CSCux37611	After fail tftp export, the export configuration remained enable state
CSCux37677	asa console slow response
CSCux37994	VLAN info not displayed in " show interface" output on SSP
CSCux44527	User should not be allowed to cancel in-progress import configuration
CSCux45823	PID value is showing empty in output for show fan-module detail
CSCux46537	Import-config failed at stage 4 importWaitForSwitch

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.