Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1)

First Published: 2018-10-25

Last Modified: 2021-05-17

Cisco Firepower 4100/9300 FXOS Release Notes, 2.4(1)

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.4(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.

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 2.4.1.268

Cisco FXOS 2.4.1.268 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.268, on page 10).

New Features in FXOS 2.4.1.266

Cisco FXOS 2.4.1.266 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.266, on page 10).

New Features in FXOS 2.4.1.252

Cisco FXOS 2.4.1.252 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.252, on page 11).

New Features in FXOS 2.4.1.249

Cisco FXOS 2.4.1.249 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.249, on page 11).

New Features in FXOS 2.4.1.244

Cisco FXOS 2.4.1.244 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.244, on page 12).

New Features in FXOS 2.4.1.238

Cisco FXOS 2.4.1.238 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.238).

New Features in FXOS 2.4.1.234

Cisco FXOS 2.4.1.234 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.234).

New Features in FXOS 2.4.1.222

Cisco FXOS 2.4.1.222 introduces the following new features in addition to the features included in earlier releases:

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.222).

New Features in FXOS 2.4.1.214

Cisco FXOS 2.4.1.214 introduces the following new features in addition to the features included in earlier releases:

- Support for Firepower Threat Defense version 6.3.
- Multi-instance capability for Firepower Threat Defense (see Multi-instance capability for Firepower Threat Defense).

  Note Requires Firepower Threat Defense Version 6.3 or later.

- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.214).

New Features in FXOS 2.4.1.101

Cisco FXOS 2.4.1.101 introduces the following new features:

- Support for ASA 9.10(1).
- Support for transparent mode deployment for an ASA logical device.

  You can now specify transparent or routed mode when you deploy the ASA.

  New/Modified FXOS commands: **enter bootstrap-key FIREWALL_MODE, set value routed, set value transparent**

  New/modified Firepower Chassis Manager screens:

  Logical Devices > Add Device > Settings

  New/Modified options: **Firewall Mode drop-down list**

- Cluster control link customizable IP Address.

  By default, the cluster control link uses the 127.2.0.0/16 network. You can now set the network when you deploy the cluster in FXOS. The chassis auto-generates the cluster control link interface IP address for each unit based on the chassis ID and slot ID: 127.2.chassis_id.slot_id. However, some networking deployments do not allow 127.2.0.0/16 traffic to pass. Therefore, you can now set a custom /16 subnet for the cluster control link in FXOS except for loopback (127.0.0.0/8) and multicast (224.0.0.0/4) addresses.

  New/Modified commands: **set cluster-control-link network**

  New/modified screens:

  Logical Devices > Add Device > Cluster Information

  New/Modified options: **CCL Subnet IP field**

Note The **CCL Subnet IP field** option is supported with ASA 9.9.2 and later and Firepower Threat Defense 6.3.0 and later

- Support for data EtherChannels in On mode.

  You can now set data and data-sharing EtherChannels to either Active LACP mode or to On mode. Other types of EtherChannels only support Active mode.

  New/Modified screens:

  Interfaces > All Interfaces > Edit Port Channel > Mode

  New/Modified commands: **set port-channel-mode**
- You can now enable Radware DefensePro (vDP) with ASA on Firepower 4110 devices.
- The Radware DefensePro (vDP) application can be deployed in a standalone configuration in an inter-chassis cluster scenario.
- You now have the option to not send hostname data to Cisco Smart Licensing on Firepower 4100 series devices.
- You can now acknowledge multiple faults at one time.
- Firepower Chassis Manager now shows the upload percentage uploading images.
- Fixes for various problems (see Resolved Bugs in FXOS 2.4.1.101).

Multi-instance capability for Firepower Threat Defense

Note Requires FTD Version 6.3 or later.

You can now deploy multiple logical devices, each with a Firepower Threat Defense container instance, on a single security engine/module. Formerly, you could only deploy a single native application instance. Native instances are still also supported. For the Firepower 9300, you can use a native instance on some modules, and container instances on the other modules.

To provide flexible physical interface use, you can create VLAN subinterfaces in FXOS and also share interfaces between multiple instances. When you deploy a container instance, you must specify the number of CPU cores assigned; RAM and disk space are dynamically allocated according to the number of cores. This resource management lets you customize performance capabilities for each instance.

You can use High Availability using a container instance on two separate chassis; for example, if you have two chassis, each with ten instances, you can create ten High Availability pairs. Clustering is not supported.

Note Multi-instance capability is similar to ASA multiple context mode, although the implementation is different. Multiple context mode partitions a single application instance, while multi-instance capability allows independent container instances. Container instances allow hard resource separation, separate configuration management, separate reloads, separate software updates, and full Firepower Threat Defense feature support. Multiple context mode, due to shared resources, supports more contexts on a given platform. Multiple context mode is not available on the Firepower Threat Defense.

See the following maximum container instances per model:

- Firepower 4110—3
- Firepower 4120—3
- Firepower 4140—7
- Firepower 4150—7
- Firepower 9300 SM-24 security module—7
- Firepower 9300 SM-36 security module—11
- Firepower 9300 SM-44 security module—14

New/Modified Firepower Chassis Manager screens:

Overview > Devices

Interfaces > All Interfaces > Add New drop-down menu > Subinterface

Interfaces > All Interfaces > Type

Logical Devices > Add Device

Platform Settings > Mac Pool

Platform Settings > Resource Profiles

New/Modified FXOS commands:

connect ftd name, connect module telnet, create bootstrap-key PERMIT_EXPERT_MODE, create resource-profile, create subinterface, scope auto-macpool, set cpu-core-count, set deploy-type, set port-type data-sharing, set prefix, set resource-profile-name, set vlan, scope app-instance ftd name, show cgroups container, show interface, show mac-address, show subinterface, show tech-support module app-instance, show version

New/Modified Firepower Management Center screens:

Devices > Device Management > Edit icon > Interfaces tab

FXOS CLI Changes for ASA Applications

FXOS CLI commands used when working with ASA logical devices have been modified.

New/Modified FXOS commands:

connect asa name, create app-instance asa name, scope app-instance asa name, show app-instance asa name

Software Download

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

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

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

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

Important Notes

- If you are utilizing the hardware bypass feature, you must upgrade to FXOS 2.4.1.238. In FXOS releases prior to 2.4.1.238, ports may go to bypass state without a failure event. If this happens, you must use Firepower Management Center to bring the ports back to standby mode.
- In FXOS 2.4(1), if you are using an IPSec secure channel in FIPS mode, the IPSec peer entity must support RFC 7427.
- If you reinitialize a security module after upgrading to FXOS 2.4(1), you might receive an error message about disk partitions on that security module being incompatible if you later downgrade to an earlier FXOS release. To resolve this issue, you need to reinitialize the security module again after downgrading.
- 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.
- When upgrading a network or security module, certain faults are generated and then cleared automatically. These include a “hot swap not supported” fault or a “module removed when in online state” fault. If you have followed the appropriate procedures, as described in the Cisco Firepower 9300 Hardware Installation Guide or Cisco Firepower 4100 Series Hardware Installation Guide, the fault(s) are cleared automatically and no additional action is required.

Adapter Bootloader Upgrade

FXOS 2.4(1) contains additional testing to verify the security module adapters on your security appliance. After installing FXOS 2.4.1.101 or later, you might receive a critical fault similar to the following 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 Firepower 4100/9300 FXOS CLI Configuration Guide, 2.4(1) or Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.4(1).

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

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

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

   ```
   fxos-chassis /chassis/server/adapter # show image
   Name Type Version

   --------------------------------------------- -------------------- -------

   fxos-m83-8p40-cruzboot.4.0.1.62.bin Adapter Boot 4.0(1.62)

   fxos-m83-8p40-vic.4.0.1.51.gbin Adapter 4.0(1.51)
   ```

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

   ```
   fxos-chassis /chassis/server/adapter # update boot-loader 4.0(1.62)
   Warning: Please DO NOT reboot blade or chassis during upgrade, otherwise, it may cause
   adapter to become UNUSABLE!
   After upgrade has completed, blade will be power cycled automatically
   fxos-chassis /chassis/server/adapter* # commit-buffer
   ```

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

   ```
   fxos-chassis /chassis/server/adapter # show boot-update status
   State: Updating
   fxos-chassis /chassis/server/adapter # show boot-update status
   State: Ready
   ```

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

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

   ```
   fxos-chassis /chassis/server/adapter # show version detail
   Adapter 1:
   Running-Vers: 5.2(1.2)
   Package-Vers: 2.2(2.17)
   Update-Status: Ready
   Activate-Status: Ready
   Bootloader-Update-Status: Ready
   Startup-Vers: 5.2(1.2)
   Backup-Vers: 5.0(1.2)
   Bootloader-Vers: 4.0(1.62)
   ```

System Requirements

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

- Mozilla Firefox—Version 42 and later
- Google Chrome—Version 47 and later

- Microsoft Internet Explorer—Version 11 and later

We tested FXOS 2.4(1) using Mozilla Firefox version 42, Google Chrome version 47, and Internet Explorer version 11. Other versions of these browsers are expected to work. However, if you experience any browser-related issues, we suggest you revert to one of the tested versions.

Upgrade Instructions

You can upgrade your Firepower 9300 or Firepower 4100 series security appliance to FXOS 2.4(1.214) if it is currently running any FXOS 2.0(1) or later build.

For upgrade instructions, see the Cisco Firepower 4100/9300 Upgrade Guide.

Installation Notes

- Upgrade to FXOS 2.4(1) can take up to 45 minutes. Please plan your upgrade activity accordingly.
- 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 does 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 does not traverse through the device being upgraded while it is upgrading. However, the other devices in the cluster continue to pass traffic.
- Downgrade of FXOS images is not officially supported. The only Cisco-supported method of downgrading an image version of FXOS is to perform a complete re-image of the device.

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

The following table lists select bugs open at the time of this Release Note publication:

Table 1: Open Bugs Affecting FXOS 2.4(1)

Identifier	Description
CSCuw31077	Filter applied to a interface should be validated
CSCux63101	All memory(s) under Memory array shows as unknown in operable column
CSCux77947	Pcap file size not updated properly when data sent at high rate

Identifier	Description
CSCux98517	Un-decorating data port for VDP should be allowed from Chassis Manager
CSCuz93180	AAA LDAP configuration does not preserve information if validation fails
CSCvc03494	Radware vDP cannot be added into APSolute Vision. As a workaround, you must manually download the device driver and install it into Vision.
CSCvc44522	Log Capacity on Management controller Server1/1 is very low Warning
CSCvd90177	Blade went to fault state after doing a MIO reload on QP-D with FXOS 2.2.1.57
CSCvj96380	SAM Coupler should force FTW bypass if switch bypass enable fails
CSCvk46399	svc_sam_bladeAG_log core seen after MIO reboot
CSCvk61563	On KP ASA, /root/.ssh is not created after reboot
CSCvm66013	MIO got hung during reboot. Kernel Panic issue seen
CSCvm84592	Filter configs are lost when "Edit Session" is done for a capture session
CSCvo64240	"Service profile ssp-sprof-2 is not associated" warning alarm cannot be acknowledged.
CSCvo68997	FXOS ip-block unable to be recovered sam.configure

Resolved Bugs in FXOS 2.4.1.273

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.273:

Table 2: Resolved Bugs in FXOS 2.4.1.273

Caveat ID Number	Description
CSCvt31171	Cisco FXOS Software for Firepower 4100/9300 Series Appliances Secure Boot Bypass Vuln
CSCvt31177	Cisco ASA and FTD Software for FP 1000/2100 Series Appliances Secure Boot Bypass Vulns
CSCvt31178	Cisco ASA and FTD Software for FP 1000/2100 Series Appliances Secure Boot Bypass Vulns
CSCvv96092	Cisco FXOS and NX-OS Software UDLD DoS and Arbitrary Code Execution Vulnerability
CSCvw38984	Cisco FXOS and NX-OS Software UDLD DoS and Arbitrary Code Execution Vulnerability
CSCvx13861	QuoVadis root CA decommission on Firepower 9300/4100 Supervisor
CSCvx88998	"System does not allow more than 16 TPs" on 2.3.1.213
CSCvx90804	MIO SSD upgraded to wrong firmware version.
CSCvo14325	Make sure MIO reboot in case of firmware upgrade is graceful

Caveat ID Number	Description
CSCvv05277	Need to support firmware upgrade for SSD in FXOS

Resolved Bugs in FXOS 2.4.1.268

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.268:

Table 3: Resolved Bugs in FXOS 2.4.1.268

Identifier	Description
CSCvu27487	FXOS ASA race condition leading to cluster join failure and network outage

Resolved Bugs in FXOS 2.4.1.266

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.266:

Table 4: Resolved Bugs in FXOS 2.4.1.266

Identifier	Description
CSCvi48404	Firepower Chassis Reloads due to License Manager
CSCvj85155	Pre-login banner gets deleted on 4100 and 9300 Chassis Manager
CSCvn11962	FXOS randomly shows one NTP server as 'Unreachable Or Invalid NTP Server' once added 4 NTP servers
CSCvq12258	Storage controller firmware version is not upgraded during FXOS upgrade
CSCvr01651	Data interfaces bring up delayed after chassis reboot
CSCvr04845	DME crash after FXOS chassis reload with maximum number of https ip-blocks configured
CSCvr15083	Cisco FXOS, IOS XR, and NX-OS Software Cisco Discovery Protocol DoS Vulnerability
CSCvr24920	FPR-4110: FXOS CLI crash in feature-mgr process
CSCvr37151	Cisco FXOS and NX-OS CDP Arbitrary Code Execution and DoS Vulnerability
CSCvr40573	FPR-4100: FXOS CLI crash with fwm hap reset
CSCvs23575	BladeAG reload due to memory leak with M5 blade
CSCvs34851	Continuous link flapping leading to snm_log corefile
CSCvs90447	FXOS 8x1G FTW continuous link flap

Identifier	Description
CSCvs92044	FXOS L3 Egress Object Resource Leak due to Port-Channel Member Interface Flaps
CSCvt06091	FXOS displays a WSP-Q40GLR4L transceiver from show interface as type QSFP-40G-LR4
CSCvt34160	"Link not connected" error after reboot when using WSP-Q40GLR4L transceiver on FPR9K-NM-4X40G
CSCvt39897	FP 4120 svc_sam_dcosAG crashed with crash type:139

Resolved Bugs in FXOS 2.4.1.252

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.252:

Table 5: Resolved Bugs in FXOS 2.4.1.252

Identifier	Description
CSCvs39368	DME process crash due to memory leak on Firepower 9300/4100

Resolved Bugs in FXOS 2.4.1.249

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.249:

Table 6: Resolved Bugs in FXOS 2.4.1.249

Identifier	Description
CSCvh68895	extra "Local Disk 3" displayed on FPR9300
CSCvk70849	FCM GUI authentication fails with "Unable to Login. Authentication failed" if the password >32 chars
CSCvm76266	Lina traceback in Thread Name: cli_xml_server
CSCvm87556	Firmware auto-install state failed while upgrading 92.5(1.232)
CSCvm96265	Disable HTTP OPTIONS enabled
CSCvn24594	add NTPDATE update of blade sysclock from the supervisor before starting NTPD
CSCvn45138	FTD gets unregistered after a bootstrap change from the Chassis Manager UI
CSCvo40340	FPR4100: serial, model and vendor are black after FAN OIR
CSCvo79145	FTD is not coming up when upgraded from k9.2.4.1.222.SPA to k9.2.6.1.118.SPA (Disk quota issue)
CSCvp35769	[ciam] Apache HTTP Server URL Normalization Denial of Service Vulnerability

Identifier	Description
CSCvq17910	Multicast MAC not programmed on chassis upon app reboot or cluster rejoin
CSCvq19641	Evaluation of Firepower 4k/9k Supervisor for TCP_SACK
CSCvq33916	Linkdown between FP 4100 and switch when using 40gb bidi to 40/100 bidi

Resolved Bugs in FXOS 2.4.1.244

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.244:

Table 7: Resolved Bugs in FXOS 2.4.1.244

Identifier	Description
CSCvn77125	FXOS: copy command should allow for wildcards to transfer multiple files
CSCvo85861	Propagate link-state not shown in FTD CLI
CSCvo90987	Enhancement for debugging link down/flap issues for bcm_usd.log files on customer units
CSCvp10674	FTD may not become online after installing vDP and upgrading FXOS to version 2.4.1
CSCvp15176	Apps installed on firepower devices may report comm failure and assume itself as active/master.
CSCvp21561	Cruz Adaptor crash due to kernel patch incompatible with cruz kernel version
CSCvp40260	Prevent STP and FC frames from being sent to SUP CPU
CSCvp56801	'show tech-support module 1 app-instance <appname> <identifier>' fails when only 1x instance on 4100
CSCvp83437	serial console login using local account succeeds but immediately returns to login prompt

Resolved Bugs in FXOS 2.4.1.238

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.238:

Table 8: Resolved Bugs in FXOS 2.4.1.238

Identifier	Description
CSCvk47441	FXOS 4100/9300: icmp redirect get stuck in FXOS OOB management routing table forever
CSCvk60985	Machine Check events logged. Possible hardware issue. FXOS Blade: mcelog support
CSCvm72541	Speed is 0 in interfaceMapping message if a port-channel's status is down

Identifier	Description
CSCvn46577	Some SSH sessions to FXOS are not timed out by absolute/session timeout
CSCvn98401	Many 0-byte files in /opt/cisco/platform/logs/corruptConfigs causes LACP problems and instability
CSCvo29067	FXOS upgrade hangs and started generating DME corefiles
CSCvo31071	Traffic drops when a unit is re-joining the cluster.
CSCvo56910	ASA subinterfaces allocated to contexts will stop responding after failover intermittently
CSCvo58998	FXOS Cruz Adapter doesn't validate data sent by logical device causing dropped offloaded packets
CSCvo64091	SSP:Cluster Slave FTD Provisioning failing because "Required external ports not available"
CSCvo75349	FXOS Blade CRUZ FW coredump due to a memory corruption
CSCvo87116	MTS messages stuck in AppAG recv_q
CSCvp09791	FXOS/FTD multi-instance deployments multicast traffic outage

Resolved Bugs in FXOS 2.4.1.234

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.234:

Table 9: Resolved Bugs in FXOS 2.4.1.234

Identifier	Description
CSCvn31390	Computing Processor PortSmash Side-Channel Information Disclosure Vuln
CSCvn42582	FXOS "Reminder to trigger an export" is changed from disable to enable after reboot
CSCvn48162	NTP communication errors may cause duplicate entries in iptables resulting in HB errors
CSCvn56156	Silent packet drops may occur on FXOS platforms due to classifier table entry corruption
CSCvn77641	SSP fail to wire ports cannot recover
CSCvn78014	Graceful shutdown is not working on data port.
CSCvn90677	During FTD install, setting the disk partition size can silently fail
CSCvn90701	Errors that occur during FTD install are not logged
CSCvn93793	Failover does not occur in the event of an SSD failure
CSCvo10712	SMA creates a new file every minute if cspCfgXml is corrupted
CSCvo28623	ssp_admin_status.sh detects left over metadata json file after failed upgrade
CSCvo28634	MIO reports incorrect status to the app-instance
CSCvo30356	Port-channels are in suspended state after upgrade
CSCvo44029	Fail to wire port pair got into bypass state when the FTD was still up and running

Resolved Bugs in FXOS 2.4.1.222

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.222:

Table 10: Resolved Bugs in FXOS 2.4.1.222

Identifier	Description
CSCvm53282	FTD: Routing tables added by ICMP redirects gets stuck in routing table cache forever
CSCvn23221	Cruz ASIC crash due to ecpumgr assertion panic
CSCvn36413	upgrade-recovery corner case for specific versioning format/naming

Resolved Bugs in FXOS 2.4.1.214

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.214:

Table 11: Resolved Bugs in FXOS 2.4.1.214

Identifier	Description
CSCvg72548	Double VLAN headers observed in Maverick front and backplane packet captures
CSCvj06276	FXOS: Cannot retrieve correct disk usage value (/dev/sdaX) by snmpwalk
CSCvk09976	Packets are not captured when same filter is applied to both phy-port & app-port for same interface
CSCvm21278	Evaluation of ssp for CVE-2018-5391 (FragmentSmack)
CSCvm33545	Clock drift in the system causes ndmain to report the service down status
CSCvm73853	Firepower Chassis Reloads on License Manager running in FXOS 2.2.2.26
CSCvn02840	Port type for sdExternalPortLink is unknown when upgrading from 2.2.2 to 2.4.1
CSCvn08869	FCM: Image version fetching hang in Logical Devices page
CSCvn11768	Application CSP should not be deleted if application instance references it
CSCvn17585	FXOS: Unexpected reload due to dcosAG crash

Resolved Bugs in FXOS 2.4.1.101

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.4.1.101:

Table 12: Resolved Bugs in FXOS 2.4.1.101

Identifier	Description
CSCuy21573	Chassis Manager: Sorting Broken in Updates Page
CSCvf38144	FXOS Hostname has an "-A" appended by default
CSCvf70180	FCM is sending the DNS search domain list to ASDM instead of just one domain

Identifier	Description
CSCvg57022	Chassis Mgr:Incorrect timezone on login detail information
CSCvg57037	Chassis Mgr:Password “Set:Yes” or No appears at incorrect place (Japanese language)
CSCvg62443	Chassis Manger UI (Logical Devices page) doesn't show correct IP of FTD device
CSCvg67730	put cap on blade core files so as to avoid incomplete blade tech-support due to low disk space
CSCvg71168	asa is started even on a failed security module
CSCvg72559	Enabling packet capture with IPv6 filter failed

Related Documentation

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

Online Resources

Cisco provides online resources to download documentation, software, and tools, to query bugs, and to open service requests. Use these resources to install and configure Firepower software and to troubleshoot and resolve technical issues.

- Cisco Support & Download site: https://www.cisco.com/c/en/us/support/index.html
- Cisco Bug Search Tool: https://tools.cisco.com/bugsearch/
- Cisco Notification Service: https://www.cisco.com/cisco/support/notifications.html

Access to most tools on the Cisco Support & Download site requires a Cisco.com user ID and password.

Contact Cisco

If you cannot resolve an issue using the online resources listed above, contact Cisco TAC:

- Email Cisco TAC: tac@cisco.com
- Call Cisco TAC (North America): 1.408.526.7209 or 1.800.553.2447
- Call Cisco TAC (worldwide): Cisco Worldwide Support Contacts

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.