# Cisco Firepower 4100/9300 FXOS Release Notes, 2.9(1)

**First Published:** 2020-11-02

**Last Modified:** 2021-05-17

## Cisco Firepower 4100/9300 FXOS Release Notes, 2.9(1)

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.9(1).

Use these Release Notes 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

Cisco FXOS 2.9.1 introduces the following:

### New Features in FXOS 2.9.1.150

Fixes for various problems (see Resolved bugs in FXOS 2.9.1.150).

### New Features in FXOS 2.9.1.143

Fixes for various problems (see Resolved bugs in FXOS 2.9.1.143).

### New Features in FXOS 2.9.1.135

Fixes for various problems (see Resolved bugs in FXOS 2.9.1.135).

### New Features in FXOS 2.9.1.131

Cisco FXOS 2.9.1.131 introduces the following new features:

| Feature | Description |
|---|---|
| Support for Firepower Threat Defense 6.7 | For more information about Firepower 6.7, see the Cisco Firepower Release Notes, Version 6.7.0. |
| Support for ASA 9.15(1) | For more information about ASA 9.15(1), see the Release Notes for the Cisco ASA Series, 9.15(1). |
| Enhancements to the upgrade process | Various improvements to the Firepower 4100/9300 FXOS upgrade process, including:<br>• Hardening of FXOS upgrade scripts<br>In instances where FTD is running on Firepower 9300 or 4100, FMC now displays FXOS compatibility information required for upgrade. If the device is not running a required FXOS version, the upgrade is not allowed, and the FMC indicates that the FXOS version must be upgraded prior to FTD upgrade. |
| FTD synchronization between operational and physical link state | The FTD application can now synchronize the operational link state with the physical link state for data interfaces by using a new state, Service State. Currently, data interfaces can transition to an Up state physically before the FTD application has completely come online, or can stay Up for a period of time after you initiate an FTD shutdown.For example, for inline sets a premature Up state can result in dropped packets because external routers may start sending traffic to the FTD before the FTD can handle it.<br>**Note** This feature is disabled by default, and can be enabled per logical device in FXOS. This feature is not supported for clustering, container instances, or an FTD with a Radware vDP decorator. It is also not supported for ASA.<br>New/Modified Firepower Chassis Manager screens: **Logical Devices > Enable Link State**<br>New/Modified FXOS commands: **set link-state-sync enabled**, **show interface expand detail** |

## 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

- In FXOS 2.4(1) or later, if you are using an IPSec secure channel in FIPS mode, the IPSec peer entity must support RFC 7427.
- 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** 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 you upgrade 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.

## 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 2.9(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 use one of the tested versions.

# Upgrade Instructions

You can upgrade your Firepower 9300 or Firepower 4100 series security appliance directly to FXOS 2.9(1) if it is currently running FXOS version 2.2(2) or later. Before you upgrade your Firepower 9300 or Firepower 4100 series security appliance to FXOS 2.9(1), first upgrade to FXOS 2.2(2), or verify that you are currently running FXOS 2.2(2).

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

### Installation Notes

- An upgrade to FXOS 2.9(1) can take up to 45 minutes. 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.

# Resolved and Open Bugs

The resolved and open 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.

## Resolved bugs in FXOS 2.9.1.158

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.9.1.158:

***Table 1:***

| Caveat ID Number | Description |
|---|---|
| CSCvv10396 | Some VIF interfaces may be reported as down in FXOS faults after software upgrade |
| CSCvx04995 | Fault F0736 should not be generated due to unreacheable default gateway |
| CSCvy48764 | SSH access with public key authentication requires user password |
| CSCvy59868 | ENH: Include output of 'show card detail expand' and 'show card-config' in chassis show-tech |

| Caveat ID Number | Description |
|---|---|
| CSCvy67759 | FXOS chassis/blade show-tech file generation failure in chassis manager |
| CSCvy72185 | FXOS Apache HTTP Server Multiple Vulnerabilities (CVE-2020-11993) and (CVE-2020-9490) |
| CSCvy80380 | Disk utilization increasing /var/tmp in FPR4150-ASA chassis |
| CSCvy83696 | ENH: FPR 4100/9300 bcm_usd process logs to support possible RCA |
| CSCvy90746 | ENH: Include output of 'show cc-mode' and 'show fips-mode' in chassis show-tech |
| CSCvy95497 | Chassis SSD firmware upgrade may be prevented improperly |
| CSCvv35531 | core svc_sam_appAG seen on 2.6.1.207 |
| CSCvy89766 | 7.0.0.1-14 9300 FTD node failed to join the cluster after the upgrade |
| CSCvz91266 | FXOS A crafted request uri-path can cause mod_proxy to forward the request to an origin server |
| CSCvx17543 | FPR-NM-4X40G EPM card aggregate interfaces are down after non-graceful OIR |
| CSCvx32797 | MIO should handle CIMC IPMI restarts gracefully |
| CSCvy09807 | Increase Blade Tech support collection timeout |
| CSCvy23328 | Send PnuOS logs from blade to MIO |
| CSCvy32270 | Display message “nothing to update” if the SSD installed is not applicable for the firmware update |
| CSCvy35746 | svc_sam_statsAG_log core file found while setting the admin state to offline in card 3 |
| CSCvy51624 | Chassis Reset reason shows different dates |
| CSCvz38489 | ENH: Add failure reason in Fault messages |
| CSCwa03285 | Upgrade to 2.10.1.166 causes degraded SM - Unrecognized Firmware format |
| CSCvz46420 | BootCLI commands user messages to be more clear |
| CSCvv90988 | Crashes on SMP platforms produce incomplete/corrupt tracebacks |
| CSCvx85964 | Fix dpdk bbappend warnings seen on mips-le builds in FXOS |
| CSCvp07518 | Verify MIO FPGA minimum version and recommend upgrades if needed |
| CSCvw89570 | FXOS: FPGA minimum version does not get cleared after upgrade to version 2.00 |
| CSCvz03480 | LINA not up for QW FTD LD running 6.6.0 and FXOS upgraded to 2.11.1.64 |

## Open Bugs in FXOS 2.9.1.158

There are no disclosed open defects at this time.

## Resolved bugs in FXOS 2.9.1.150

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.9.1.150:

***Table 2: Resolved Bugs in FXOS 2.9.1.150***

| Identifier | Description |
|---|---|
| CSCvu84127 | Firepower may reboot for no apparent reason |
| CSCvw58736 | FP9300 2.8.1.105 chassis reboots after adding 16th Instance in SM-56 |
| CSCvw62255 | "Link not connected" error when using WSP-Q40GLR4L transceiver and Arista switch |
| CSCvw72260 | ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found" |
| CSCvw74660 | Syslog-ng not starting up while CC mode due to possble bad syslog-ng patch |
| CSCvw79465 | FXOS upgrade does not do proper compatibility check for FTD image |
| CSCvx16700 | FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC" |
| CSCvx25336 | ENH: add a way to disable the FQDN check |
| CSCvx33904 | Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privile |
| CSCvx82705 | Evaluation of ssp for OpenSSL March 2021 vulnerabilities |
| CSCvy03357 | 6.6.4-56: KP and WM serial console prompt a process ID every 2 seconds which made CLI unusable |
| CSCvy04959 | 'Memory leak' may casue appAG process traceback and reload |
| CSCvy08798 | WR6, WR8 and LTS18 commit id update in CCM layer(sprint 110, seq 10) |
| CSCvy34333 | When ASA upgrade fails, version status is desynched between platform and application |
| CSCvt03244 | Can't Generate FPRM Logs - Fails when custom user with admin priviledge tries |
| CSCvt18178 | FP93K // 2.3.1.144 // SSH sessions not clearing. More than 32 FPRM CLI sessions are not allowed |
| CSCvu47574 | PortAG Core file detected while testing UUT Image 92.10.1.212 |
| CSCvv89821 | "show hardware internal bcm-usd info driver-info" returns error |
| CSCvv98629 | QAT: Upgrade QAT driver from 4.2 to 4.11 in FXOS |
| CSCvw05392 | Message appearing constantly on diagnostic-cli |

| Identifier | Description |
|---|---|
| CSCvw05590 | Placeholder ddts to checkin mibs in global mibs branch |
| CSCvw33536 | 4100/9300: Cannot associate port channel / interface to App |
| CSCvw67974 | SSH access with public key authentication fails after FXOS upgrade |
| CSCvw77924 | Radius Key with the ASCII character " configured on FXOS does not work after chassis reload. |
| CSCvw95181 | FXOS upgrade fails with error "does not support application instances of deployment type container" |
| CSCvw98315 | FXOS reporting old FTD version after FTD upgrade to 6.7.0 |
| CSCvx13328 | enhance debug prints in switch_driver code |
| CSCvx14602 | Firepower memory leak in svc_sam_dcosAG |
| CSCvx38047 | FXOS show fault warning code F4526902 |
| CSCvx43226 | LTP FXOS PEM File Change for Backend Certificates |
| CSCvx66329 | FTD Hotfix Cisco_FTD_SSP_FP2K_Hotfix_O installation fails on script 000_start/125_verify_bundle.sh |
| CSCvx89827 | Not able to set Bangkok time zone in FPR 2110 |
| CSCvy25035 | Enable log rotation of rsc* logfiles that can grow large due to bug CSCvy13543 |
| CSCvy39791 | Lina traceback and core file size is beyond 40G and compression fails. |
| CSCvy66942 | FPR4100/9300 IPv6 config cannot be applied using Rest API LTP on 9300/4100 Supervisor |
| CSCvy68403 | NTP script generates "binary operator expected" syntax error |
| CSCvy83657 | FXOS process core pruned/deleted from system files (no validation) |
| CSCvs29015 | Enhancement to make link down/flap reasons from CSCvo90987 user readable |
| CSCvt93959 | Increase log levels related to app-instance state change to 'not-responding' |
| CSCvw37088 | FTD requires glib-2.0 update |
| CSCvr94911 | FXOS: some interface transition logs have no reason |
| CSCvp79990 | decommission blade should be blocked when disk format in progress |
| CSCvu53810 | TD2 does not load balance MPLS across backplane interfaces and sends it all to first interface |
| CSCvw21766 | Need to include AAA logs/debugs in FPRM tar bundle |
| CSCvw81976 | Rename status BYPASS-FAIL for fail-to-wire inline pairs |

| Identifier | Description |
|---|---|
| CSCvx13557 | Need more bcm-usd output in tech-support |
| CSCvx66494 | Handle CIMC Watchdog reset in MIO |
| CSCvx86058 | BCM SDK patch 6.5.8 - Parity error in TDM Calendar memories causes traffic drop after SER correction |
| CSCvy13341 | CLI to enable/disable SDK logs |
| CSCvy23328 | Send PnuOS logs from blade to MIO |
| CSCvy29668 | Add Server environment detail to techsupport |
| CSCvy59639 | Drop counter statistics for BCM |
| CSCvy65802 | AppAgent Heartbeat enhancement |
| CSCvy67487 | 9300/4100 Enable Blade Console logs for Release images |

## Resolved bugs in FXOS 2.9.1.143

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.9.1.143:

***Table 3: Resolved Bugs in FXOS 2.9.1.143***

| Identifier | Description |
|---|---|
| CSCvx90804 | MIO SSD upgraded to wrong firmware version. |
| CSCvx29429 | ma_ctx*.log consuming high diskspace on FPR4100/FPR9300 despite the fix for CSCvx07389 |
| CSCvy23422 | QW:4112:FXOS traceback and reload after upgrade to 2.8.1.143 |
| CSCvv05277 | Need to support firmware upgrade for SSD in FXOS |
| CSCvx13861 | QuoVadis root CA decommission on Firepower 9300/4100 Supervisor |
| CSCvw84884 | Integrate kenton micron ssd firmware script from FTD hotfix |
| CSCvu70493 | FXOS - AAA/RADIUS - NAS-IP Field set to 127.0.01 |
| CSCvx01786 | Pre-login-banner not showing on FCM WebUI |

## Resolved bugs in FXOS 2.9.1.135

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.9.1.135:

| Caveat ID Number | Description |
|---|---|
| CSCvu70493 | FXOS - AAA/RADIUS - NAS-IP Field set to 127.0.01 |

| Caveat ID Number | Description |
|---|---|
| CSCvv36393 | StatsAG memory leak |
| CSCvv58480 | FXOS: Voltage on DC PSU displayed with wrong values from the 'show stats' |
| CSCvv84358 | VIC adapter kernel crash at boot |
| CSCvv85742 | Upgrade : FSM status can show incorrect value after upgrade |
| CSCvw13348 | WR6, WR8 and LTS18 commit id update in CCM layer (sprint 98, seq 2) |
| CSCvw19401 | Memory leak : DME process may traceback generating core on Firepower 4100/9300 (M5 series only) |
| CSCvw22435 | Error "No such file or directory" happended when using "copy ftp: wrokspace:" in FXOS 2.8.1 |
| CSCvw48829 | Timezone in "show clock" is different from which in "show run clock" |
| CSCvw53494 | CRUZ paloview is not accessible on release build |

### Open Bugs in FXOS 2.9.1.150

There are no disclosed open defects at this time.

### Open Bugs in FXOS 2.9.1.143

There are no disclosed open defects at this time.

### Open Bugs in FXOS 2.9.1.135

There are no disclosed open defects at this time.

### Open Bugs in FXOS 2.9.1.131

There are no disclosed open defects at this time.

## 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.