Cisco Firepower 4100/9300 FXOS Release Notes, 2.14(1)

First Published: 2023-12-13

Last Modified: 2024-09-18

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.14.1.

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 security appliance is a next-generation platform for network and content security solutions. The 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 security appliance provides the following features:

- Modular chassis-based security system—Provides high performance, flexible input/output configurations, and scalability.
- 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 2.14.1.167

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.14.1.167, on page 5)

New Features in FXOS 2.14.1.163

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.14.1.163, on page 5)

New Features in FXOS 2.14.1.143

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.14.1.143, on page 7)

New Features in FXOS 2.14.1

Cisco FXOS 2.14.1 introduces the following new features:

Feature	Description
Monitor Chassis-level health alerts in Secure Firewall Management Center	This feature allows you to monitor your chassis in the management center for chassis-level health alerts. To monitor chassis-level health alerts in the management center, you must manually configure the management center as manager on the chassis, and then register the chassis in the management center. New/modified CLI: **create device-manager** *manager_name* **hostname** {*hostname* | *ipv4_address* | *ipv6_address*} **nat-id** *nat_id*
Integrated firmware upgrade	The FXOS firmware upgrade package is now integrated with platform bundle for firmware auto-upgrade during the FXOS upgrade. Whenever you upgrade your FXOS to latetst version, the firmware package gets unpacked based on the platform and the system checks for the firmware version running on your supervisor. If the firmware version is lower than the firmware version integrated in the platform bundle, the firmware gets auto-upgraded without any user intervention. New/modified CLI: No new CLIs added. You can use the existing **show firmware monitor** command to monitor the upgrade process. Firmware Package Included: Firmware package 1.0.19
Secure Firewall chassis manager single sign-on	The chassis manager now supports single sign-on (SSO) for external users configured at any third-party SAML 2.0-compliant identity provider (IdP). New/modified pages: • **Login** > **Single Sign-On (SSO)** • **Platform Settings** > **AAA** > **Single Sign-On (SSO)**

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 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.
- From FXOS 2.13 release, the **set maxfailedlogins** command no longer works. The value can still be set, but if you try to log in a greater number of times than the already set value with an invalid password, you are not locked out. For compatibility, a similar command, **set max-login-attempts**, is available under scope security. This command also prevents logging in after a certain number of failed attempts but sets the value for all users. These commands are only available for Firepower 2100 platform mode and do not affect other platforms.

System Requirements

- You can access the 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 2.14.1 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 2.14.1 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 2.14.0, 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

- From FXOS 2.14.1, the FXOS firmware is bundled with FXOS software image. During FXOS upgrade, the system will auto-upgrade the firmware to the latest version if applicable. If the firmware is upgraded, the system will reboot 2 times and the total FXOS upgrade duration will be extended.

  Following tables lists the time taken for upgrade with or without firmaware uprade:

FXOS Upgrade With Firmware Upgrade	Duration(in mins)
Initiate FXOS Upgrade with integrated FW changes	-
First Reboot triggered by FXOS upgrade	~9

FXOS Upgrade With Firmware Upgrade	Duration(in mins)
CLI after FXOS Upgrade (before FW Upgrade)	~8
Second Reboot triggered by FW Upgrade	~1 to 20 *
CLI after FXOS Upgrade and FW Upgrade	~8
Blade to come online	~13
Application to come online	~10
Total	~49-70mins

FXOS Upgrade Without Firmware Upgrade	Duration(in mins)
Initiate FXOS Upgrade with integrated firmware changes	-
Reboot triggered by FXOS upgrade	~9
CLI after FXOS Upgrade (before firmware upgrade)	~8
Blade to come online	~13
Application to come online	~10
Total	~40 mins

- 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 Cisco.com.

For more information about the Cisco Bug Search Tool, see the Bug Search Tool Help & FAQ.

Resolved bugs in FXOS 2.14.1.167

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.14.1.167:

Identifier	Headline
CSCwc76419	Unnecessary FAN error logs needs to be removed from thermal file
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability
CSCwj69632	Default Hashing Algorithm is SHA1 for Firepower Chassis Manager Certificate on 4110
CSCwk62297	Evaluation of ssp for OpenSSH regreSSHion vulnerability
CSCwk33556	The more command is missing on FMC
CSCwj11300	TPK FTD performance down 25%
CSCwk27296	FMCv passwd command fail

Resolved bugs in FXOS 2.14.1.163

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.14.1.163:

Identifier	Headline
CSCwj08073	libuv is a multi-platform support library with a focus on asynchronous
CSCwi78370	Firpower 4100/9300 : Update CiscoSSH (Chassis Manager FXOS) to address CVE-2023-48795
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwj38928	High latency observed on FPR3120
CSCwi92914	A flaw was found in the networking subsystem of the Linux kernel withi
CSCwi92917	Linux Kernel nftables Use-After-Free Local Privilege Escalation Vulner
CSCwi84615	some stdout logs not rotated by logrotate
CSCwi24461	Device/port-channel goes down with a core generated for portmanager
CSCwi90399	FTD/ASA system clock resets to year 2023
CSCwj55081	FPR3K loses connectivity to the management center via mgmt data interface on reboot of FPR3K
CSCwj20118	FTDv reloads and generate backtrace after push EIGRP config
CSCwj49958	Crypto IPSEC Negotiation Failing At "Failed to compute a hash value"

Identifier	Headline
CSCwi24004	Out-of-bounds Read vulnerability in mod_macro of Apache HTTP Server.Th
CSCwb02701	FXOS does not retry NTP sync with servers
CSCwj42025	CCM ID LTS21-100 with RCPL21 update
CSCwi78189	It was discovered that when exec'ing from a non-leader thread, armed P
CSCwi60248	A malicious HTTP sender can use chunk extensions to cause a receiver r
CSCwh43230	Strong Encryption license is not getting applied to ASA firewalls in HA.
CSCwi59271	Suppress "End of script output before headers" syslog on FXOS
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade
CSCwh71235	A flaw was found in QEMU. The async nature of hot-unplug enables a rac
CSCwi49506	Before Go 1.20, the RSA based TLS key exchanges used the math/big libr
CSCwj16119	FP2110: When Leaving On-Box (FDM) Mode Platform API Fails
CSCwj25066	CCM ID 68 - LTS21 - CISCO_LTS21_R2160 release branch
CSCwk66252	It was discovered that a nft object or expression could reference a nf
CSCwi31480	Alert: Decommission failed, reason: Internal error is not cleared from FCM or CLI after acknowledge
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj88930	net-snmp provides various tools relating to the Simple Network Managem
CSCwj88931	net-snmp provides various tools relating to the Simple Network Managem
CSCwj88932	net-snmp provides various tools relating to the Simple Network Managem
CSCwi60256	strongSwan before 5.9.12 has a buffer overflow and possible unauthenti
CSCwi13134	Hardware bypass not working as expected in FP3140
CSCwk66253	An out-of-bounds access vulnerability involving netfilter was reported
CSCwj88929	net-snmp provides various tools relating to the Simple Network Managem
CSCwi68135	A vulnerability was found in SQLite SQLite3 up to 3.43.0 and classifie
CSCwi68133	A use-after-free vulnerability in the Linux kernel's ipv4: igmp compon
CSCwi68132	A heap out-of-bounds write vulnerability in the Linux kernel's Perform
CSCwi23964	Python 3.x through 3.10 has an open redirection vulnerability in lib/h
CSCwi78210	An out-of-bounds memory write flaw was found in the Linux kernelâs Tra

Identifier	Headline
CSCwh94201	An issue was discovered in drivers/net/ethernet/intel/igb/igb_main.c i
CSCwi92927	A use-after-free vulnerability in the Linux kernel's netfilter: nf_tab
CSCwi24032	A heap out-of-bounds write vulnerability in the Linux kernel's Linux K
CSCwi55629	ASA/FTD : Port-channels remain down on Firepower 1010 devices after upgrade
CSCwi49360	A flaw was found in the 9p passthrough filesystem (9pfs) implementatio
CSCwj48801	4200s have high UDP latency at low packet rates.
CSCwi24027	A use-after-free vulnerability was found in drivers/nvme/target/tcp.c'
CSCwh47732	Vulnerabilities in linux-kernel 5.10.79 CVE-2023-3111 and others
CSCwi24021	An issue was discovered in the Linux kernel before 6.5.9, exploitable
CSCwi53987	SSL protocol settings does not modify the FDM GUI certificate configuration or disable TLSv1.1
CSCwi46641	FTDv may traceback and reload in Thread Name 'PTHREAD-3744' when changing interface status
CSCwi78206	A vulnerability was found in GnuTLS, where a cockpit (which uses gnuTL
CSCwj30962	3140 3 MI instances upgrade failed
CSCwi85951	A use-after-free flaw was found in the __ext4_remount in fs/ext4/super
CSCwi13062	Debug messages seen on console on executing show tech-support fprm detail
CSCwj54717	Radius secret key of over 14 characters for external authentication does not get deployed (FPR3100)
CSCwj88928	net-snmp provides various tools relating to the Simple Network Managem
CSCwi04351	Threat defense upgrade failling on script 999_finish/999_zz_install_bundle.sh
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwj88925	net-snmp provides various tools relating to the Simple Network Managem
CSCwi79120	Some ssh sessions not timing out, leading to ssh and console unable to connect to the FXOS CLI

Resolved bugs in FXOS 2.14.1.143

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.14.1.143:

Identifier	Headline
CSCwh19613	ASA crashed with SAML scenarios.

Identifier	Headline
CSCwi62683	Upgrade to CiscoSSH 1.13.46 in FXOS address CVE-2023-48795.
CSCwi66007	Entropy mixing breaks NPU build.
CSCwi76630	FP2100/FP1000: ASA Smart licenses lost after reload.
CSCwj09999	FP 3100 MTU change on management interface is NOT persistent across reboots (returns to default MTU).
CSCwf61280	Failing to dowload FTD image via SAML SSO login.
CSCwh22888	FXOS: Remove enforcement of blades going into degraded state after multiple DIMM correctable errors.
CSCwh53276	Upgrade to CiscoSSL 1.1.1v.7.3.338-fips in SSP MIO.
CSCwh68167	Adding Jent library in SSP MIO.
CSCwi17589	Jent Implemention in SSP MIO.
CSCwi27924	Using entropy mixing with CiscoSSL.
CSCwi36311	Use kill tree function in SMA instead of SIGTERM.
CSCwe11124	ENH: Combine firmware bundle packages into FXOS MIO update packages.
CSCwh33196	SSP MIO: Swims token support in signing image.
CSCwf62228	Timezone not working correctly on 9300/4100 platforms.

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 FXOS 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.