Cisco Firepower 4100/9300 FXOS Release Notes, 2.14(3)

First Published: 2025-09-16

Last Modified: 2026-11-04

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.14.3.

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.
- Firewall 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 2.14.3.3018

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.14.3.3018, on page 4)

New Features in FXOS 2.14.3.125

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.14.3.125, on page 5)

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 Firewall 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 2.14.3 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
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 register for an account.

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

Resolved bugs in FXOS 2.14.3.3018

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.14.3.3018:

Identifier	Headline
CSCwo90678	ASA: MAC address of the port-channel interface changes leading to ping failure
CSCwt88545	Remove diffie-hellman-group14-sha1 from ssh/sshd configuration
CSCwr59870	ASAv on Hyper-v encountering boot loop issues when running netvsc driver
CSCwt24371	Boot loop due to AFM process stuck causing a BootTimerFail reset.
CSCwc40735	Fixes for vulnerabilities mentioned in CVE-2019-17567
CSCwq24140	Security module reboot triggered by a CIMC reset.
CSCwt62145	ARP requests are not forwarded to all threat defenses on the chassis in multi-instance deployment
CSCwu11083	cseSysMemoryUtilization (1.3.6.1.4.1.9.9.305.1.1.2) returns incorrect memory metrics post-FXOS 2.14.1.187 upgrade
CSCwu27874	Evaluate Cisco FXOS for CVE-2026-31431
CSCws51772	Deployment failing with ERR-http-initializing
CSCws65684	10G_T_X SFP interfaces are not coming up in 10G speed.
CSCwu32444	CVE-2026-43284: linux-kernel: In the Linux kernel, the following vul...
CSCwj31475	F1758 FXOS Fault Observed in ASA Appliances Following FXOS Upgrade
CSCwr36159	FXOS:ASA SSH login fails at the first attempt when it is integrated with DUO
CSCwt09824	FTD should not honour a huge time jump from NTP
CSCwt55803	FPR4225 losing communication with netmod

Identifier	Headline
CSCwt61597	Continued Evolution of Persistence Mechanism Against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense
CSCwi76642	FXOS capture in Container mode behaves erratically
CSCwu06269	Firepower 1100 Copper SFP Ports Show Link Up with GLC-TE/GLC-T Despite No Cable
CSCwt28479	PortAG memory leak causing traceback while threat defense instance is offline
CSCws01587	Device entering failsafe mode and not exiting even though the app launches
CSCws68206	ASA on hyper-v couldn't configure VLAN after upgrade
CSCwq99801	System calls may be delayed due to printing of ECC errors on console

Resolved bugs in FXOS 2.14.3.125

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.14.3.125:

Identifier	Headline
CSCwq74986	Threat defense instance stuck in Boot Loop
CSCwq96870	Interfaces are coming up when the Firepower is shutting down
CSCws46901	Management center M6 direct install kernel crash and device struck during baseline
CSCwr01482	Secure Firewall 4215 "Not supported" alarm occurred, when insert the SFPs
CSCwq44834	Multicast and broadcast packets do not reach all multi-instance firewalls via shared interface on 3100/4200
CSCwo91436	Secure Firewall 4125 Multi instance High Snort and System Core CPU Usage (100%) Triggering FMC Critical Alerts
CSCwq70133	Password Expiry Age does not reset after password change
CSCwq23394	Threat defense may drop traffic in the Azure cloud at mlx5 driver level.
CSCwq60586	Threat defense upgrade failed due to bundle image existence verification failure
CSCwq36466	Expat/xml FW rebooted itself and no crashinfo generated
CSCws33462	Faults generated during first boot on 6.x can't be cleared
CSCwq26863	Firepower 2110 - ntpd process constantly crashing
CSCwq72989	Vulnerabilities mentioned in CVE-2024-3447
CSCwo87551	Vulnerabilities mentioned in CVE-2025-21959
CSCwq13032	3100/4200 1G management interface flapping after upgrade

Identifier	Headline
CSCwq31342	Secure Firewall 4200 | 3100 multi instance chassis deeployment failed in DNS configuration
CSCwd92327	On Firepower 2100 platform, external authentication fails for users starting with number
CSCwp89969	Prolonged delays in firewall restart/reboot completion
CSCwr88733	Collecting `show tech-support fprm` results in corefile in TAR process
CSCwr24999	Secure Firewall 3140 threat defense HA upgrade getting stuck
CSCwo55957	Vulnerabilities mentioned in CVE-2024-26687
CSCwp60896	ASA Clock reverts to UTC after device reload
CSCwo74009	Cisco FXOS and UCS manager software command injection vulnerability
CSCwq65955	Secure Firewall 4200 HA link arp packets getting dropped, internal uplink linkChange counters incrementing
CSCwq52255	SSH login to threat defense management IP address lands in FXOS shell instead of threat defense CLISH due to missing /mnt/boot/application/*.def file
CSCws37370	Threat defense, dcosAG continuously crashing
CSCwq73002	Vulnerabilities mentioned in CVE-2024-6505
CSCwr83390	Secure Firewall 4200 Port-channel flaps while generating chassis FPRM
CSCwo56025	Vulnerabilities mentioned in CVE-2024-40945
CSCwr59870	ASAv on Hyper-v encountering boot loop issues when running netvsc driver
CSCwk87700	Multiple core.svc_sam_statsAG on FxOS platforms
CSCws25638	Secure Firewall 3110 MI (shared subinterface) - Traffic outage when disabling multicast routing on one firewall instance
CSCwq73009	Vulnerabilities mentioned in CVE-2024-8088
CSCwr31136	SNMP OID polling for chassis temperature not giving response
CSCwq85986	Secure Firewall 4225 Interface with SFP - 10/25G_LR_S (or CSR_S) is not coming up after reboot of peer side.
CSCwn92248	Firepower 2100 & Firepower 1100 Port-channel interfaces flap with LACP
CSCwp33410	dmesg and kern.log file flooded with Tx Queue=0 logs
CSCwq92373	Secure Firewall 4200 MI two apps went to Not Responding state with reason Error in App Instance ftd. sma reported fault Instance xxx is disabled due to restart loop. Please consider reinstalling this app-instance.
CSCwo55715	Vulnerabilities mentioned in CVE-2022-49219

Identifier	Headline
CSCwn95347	Vulnerabilities mentioned in CVE-2024-56739
CSCwn71596	Intf Link down (Init, mac-link-down) seen - EtherChannel Membership in Down/Down/Down state after unplug/replug of the cable
CSCwr22508	Device doesn't boot and gets stuck after a successful upgrade
CSCwq88796	Firepower SSH access lost after timezone change in platform mode
CSCwq31988	Errors on all interface of FPR1010 | line protocol is down (not associated with supervisor)
CSCwq66716	Vulnerabilities mentioned in CVE-2025-27363
CSCwr83527	Secure Firewall 2110 Critical fault alerts for remote users
CSCwo75483	SNMP polling to chassis is unsuccessful with FTD Multi-instance in HA used as SNMP agent
CSCws91179	Warning about the usage of failsafe-exit
CSCwp22743	Secure Firewall 4200 - 1gsx link remains up on wpk but on switch side it shows as not connected
CSCwp83219	Secure Firewall 3100 (aldrin/aldrin2, CPSS 4.3.5) Intf Tx MAC stuck issue when peer reloads/flaps.
CSCwq95241	Reboots on FP2130 due to missing heimdall PID
CSCwp65952	Secure Firewall 4200/3100 EPM FPGA upgrade chooses incorrect bundle

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://bst.cloudapps.cisco.com/bugsearch/search
- 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.