Cisco Firepower 4100/9300 FXOS Release Notes, 2.14(2)

First Published: 2025-09-16

Last Modified: 2025-09-15

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.14.2.

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 2.14.2.137

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.14.2.137, on page 4)

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 2.14.2 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 firamware 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 2.14.2.137

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.14.2.137:

Identifier	Headline
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
CSCwe48399	The public API function BIO_new_NDEF is a helper function used for str
CSCwf04460	The fxos directory disappears after cancelling show tech fprm detail command with Ctr+c is executed.
CSCwh81366	[Multi-Instance] Second Hard Drive (FPR-MSP-SSD) not in use
CSCwi13134	Hardware bypass not working as expected in Secure Firewall 3140
CSCwi22296	ASA: The logical device may boot into failsafe mode because of large configuration.
CSCwi24461	Device/port-channel goes down with a core generated for portmanager
CSCwi46641	Threat defense virtual may traceback and reload in Thread Name 'PTHREAD-3744' when changing interface status
CSCwi55629	ASA/Threat Defense: Port-channels remain down on Firepower 1010 devices after upgrade
CSCwi62683	The SSH transport protocol with certain OpenSSH extensions, found in ... (CVE-2023-48795)
CSCwi76630	FP2100/FP1000: ASA Smart licenses lost after reload
CSCwi79703	Incorrect Timezone Format on FTD When Configured via FXOS
CSCwi90399	ASA/Threat Defense system clock resets to year 2023
CSCwj04154	FTD management interface DHCP server may fail to start causing connectivity issues or showing faults
CSCwj08015	FTW no longer working in NM3 on Warwick
CSCwj08083	An issue was discovered in libxml2 before 2.11.7 and 2.12.x before 2.1
CSCwj09999	Secure Firewall 3100 MTU change on management interface is NOT persistent across reboots (returns to default MTU)
CSCwj20118	FTDv reloads and generate backtrace after push EIGRP config
CSCwj29599	Device Manager bootstrap might be interrupted by extra reboot due to firmware upgrade
CSCwj30962	Upgrade failed on Secure Firewall 3140 3 MI instances
CSCwj34204	Disk quota for the corefile should be revisited based on platform

Identifier	Headline
CSCwj38928	High latency observed on Secure Firewall 3100 series devices
CSCwj49958	Crypto IPSEC Negotiation Failing At \"Failed to compute a hash value\"
CSCwj54717	Radius secret key of over 14 characters for external authentication does not get deployed (Secure Firewall 3100)
CSCwj56615	Build wireshark package with nghttp2
CSCwj57435	Cleanup stale logrotate files
CSCwj61086	High CPU usage in svc_sam_dme process during deployment post breaking cluster or deleting inline-set
CSCwj77877	Disable/Enable an MI instance results it in \"State Failed\"
CSCwj79895	ENH Logs Firepower 4110 (FXOS 2.10.1.179) Security module stopped responding after device reboot
CSCwk41007	ASA/Threat Defense may traceback and reload
CSCwk42676	Virtual ASA/Threat Defense may traceback and reload in thread PTHREAD
CSCwk48628	Threat Defense/FXOS - Upgrade/erase configuration result in App-instance '"Operational State: Starting"
CSCwk56467	Loading on Secure Firewall 3100 fails with Corruption of in-memory data detected and continously boots
CSCwk62296	Address SSP OpenSSH regreSSHion vulnerability
CSCwk67859	Threat Defense and FXOS: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS)
CSCwk71227	Threat Defense running on Firepower 2100 with LDAP skips backslash when updating ldap.conf
CSCwk75406	Mangement Center in CC-mode audit over syslog not working
CSCwk82557	Threat Defense upgrade to 7.4.2 via device manager is blocked
CSCwm03142	IPv6 Neighbor Discovery/multicast traffic affected on shared interface in multi instance setup
CSCwm06393	Changes in port-channel membership or member status may cause periodic OSPF/EIGRP adjacency flaps
CSCwm34333	Threat Defense - \u00a0Multi-Instance, docker0 interface overlap with private network 172.17.0.0/16
CSCwm35751	FPR3100: Interface may go to half duplex speed is hardcoded to 100mbps
CSCwm37363	Portmanager and lacp sync is not programmatic
CSCwm40531	Threat Defense/ASA : 1SXF interfaces on FP3100 stay in a link-down state when connected to a Nexus 9K Switch
CSCwm49154	FXOS fault F1738 seen in deploymet with Error: CSP_OP_ERROR. CSP signature verification error
CSCwm50936	100GB interface flaps with Innolight QSFPs in both ends

Identifier	Headline
CSCwm64553	Incompatible members warning message after Po member interface flaps unable to rejoin Po
CSCwm96280	Threat Defense device stuck in rommon mode after pressing reset button
CSCwn11728	FPR9K-SM-56 module intermittently lock up and cause traffic impact.
CSCwn13187	ASA upgrade failing from 9.20.2.21 to the target version 9.20.3.4
CSCwn19190	Memory fragmentation resulted in huge pages unavailable for lina
CSCwn22610	fs-daemon hap reset with core generation
CSCwn29611	Radius user ssh login fails with error: username is not defined with a service type that is valid
CSCwn40485	MI: Traffic fails to reach the Secondary FTD when enabled with data-sharing interface
CSCwn46426	ASA 21xx: 'sh environment temperature' shows incorrect temperature values
CSCwn71596	Intf Link down (Init, mac-link-down) seen - EtherChannel Membership in Down/Down/Down state after unplug/replug of the cable
CSCwn86002	Core corruption still seen with switching to quick core feature
CSCwn92248	Threat Defense Firepower 2100 port-channel interfaces flap with LACP
CSCwn98402	Debuggability: Firepower 2100 port-channel interfaces flap after upgrade
CSCwo42102	show tech-support fprm detail command is getting stuck for longer duration
CSCwo64788	FPR9K-SM-56 Cluster - FTD Stuck in an application install loop & error 'pooled address is unknown'
CSCwo65866	Network Outage when Primary threat defense Instance is Disabled from chassis manager
CSCwo71052	Firepower 1010 Ethernet1/1 trunk port is not passing Vlan traffic after a reload
CSCwo73467	Interface mac stuck issue seen with peer switch reloads or after upgrade
CSCwo86422	Unidirectional communication over ccl leading to split-cluster.
CSCwo94274	Firepower 4100/9300 Fatal error: Incomplete chain observed before watchdogs with reset code 0x0040
CSCwp18885	Firepower 9300/4100 may traceback & reload due to a \"Kernel Panic\"
CSCwp83345	Cluster: Multi-blade chassis not transmitting broadcast traffic outbound to specific vlan
CSCwe21884	Write wrapper around \"kill\" command to log who is calling it
CSCwe92324	Secure Firewall 3100 - SNMP poll reports incorrect FanTray Status at Down while actually operational
CSCwf82279	Excessive logging of ssp-multi-instance-mode messages to /opt/cisco/platform/logs/messages
CSCwf99303	Management UI presents self-signed cert rather than custom CA signed one after upgrade

Identifier	Headline
CSCwh21382	FXOS: Add time module troubleshoot was generated to tech_support_brief
CSCwh91976	Secure Firewall 4200 MI: Traps(linkup/down) from chassis is not seen on NMS even if unification is enabled
CSCwi00713	A memory leak flaw was found in Libtiff's tiffcrop utility. This issue
CSCwi14659	zeromq: detailed logging flooding the customer logs.
CSCwi36311	Use kill tree function in SMA instead of SIGTERM
CSCwi53987	SSL protocol settings does not modify the device manager GUI certificate configuration or disable TLSv1.1
CSCwi55599	Secure Firewall 3100/4200 KC - serviceability: pcie link training in downgraded state (QDMA monitor)
CSCwi57476	Interface idb logging log rotation to FXOS logrotate utility
CSCwi60430	CVE-2023-51385 (Medium Sev) In ssh in OpenSSH before 9.6, OS command injection might occur if a us
CSCwi67998	Policy deployment failures on Secure Firewall 3100 MI chassis after redeploying same instance
CSCwi68581	Need better way to handle for 35s and 10s sleep timeout in 300_os/001_verify_bundle.sh
CSCwi83821	Reword the CLI message shown after running the 'erase configuration' command
CSCwi84615	Some stdout logs not rotated by logrotate
CSCwj25629	Error when running 'show tech-support module detail' on FPR9K
CSCwj30576	Firepower 2100 RADIUS shared secret not updating if longer than 14 chars, need new field
CSCwj48801	High latency observed on Secure Firewall 4200
CSCwj55081	Secure Firewall 3100 loses connectivity to FMC via mgmt data interface on reboot
CSCwj83533	FAN is working as expected but FAN LED is in off state.
CSCwk14596	Patch pidof to get rid of can't read error message
CSCwk14685	Threat Defense: management interface showing down despite being up and operational
CSCwk59458	Firepower 2100: debug log process hangs preventing recovery from stuck writing operations
CSCwk75035	Vulnerability in core of Apache HTTP Server 2.4.59 and earlier are vul
CSCwk88225	Critical fault : [FSM:FAILED]: user configuration(FSM:sam:dme:AaaUserEpUpdateUserEp)
CSCwm07419	ldap.conf does not get generated using hostname impacting external radius authentication
CSCwm10964	CTLE peak value update for 10/25g modules in Secure Firewall 3100/4100
CSCwm49782	Enhance sma 2nd cruz heartbeat logging

Identifier	Headline
CSCwm51874	FXOS: messages rotates every 40 minutes due to Notification Daemon messages' being spammed
CSCwm52264	Not able to remove or clear Fault \"The password encryption key has not been set.\"
CSCwm52973	Low End Secure Firewall 3100: Changing interface speed from 1g to 100mbps/100mps to 1g bring downs the link
CSCwm58723	Finish integration of newer version of pam radius module from wind river
CSCwn21204	Serviceability to add extra logging capability to SAM logs to determine snmp bind failure.
CSCwn44335	FXOS - Download command generates an extra \"/\" over HTTP and HTTPS GET requests
CSCwn45049	Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808
CSCwn47308	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on Firepower 1100/2100 and Secure Firewall 3100
CSCwn70473	SFF_SFP_10G_25G_CSR_S from Finisar ports bouncing when use as HA link
CSCwn79553	Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on FTD
CSCwo26258	Default Route Changes from Management0 to Management1 After Reload or Upgrade on Secure Firewall 4200 Series
CSCwo75483	SNMP polling to chassis is unsuccessful with FTD Multi-instance in HA used as SNMP agent
CSCwo83389	Difference in RSA key length at multiple spots in FXOS
CSCwo95140	Secure Firewall 1200 DT - RMU Logs dumps in Portmgr.out file.
CSCwp83219	Secure Firewall 3100 (aldrin/aldrin2, CPSS 4.3.5) Intf Tx MAC stuck issue when peer reloads/flaps.
CSCwc57341	Inline pair has incorrect FTW bypass operation mode of 'Phy Bypass'
CSCwc75659	Secure Firewall 3100/4200 management sub-interface is not working
CSCwd83069	Add capability to disable auto-negotiation for 100G ports
CSCwe45584	Firepower 2130 - Incorrect spelling seen in tech_support_brief in FPRM
CSCwh36976	Firepower module \"show tech-support\" may traceback due to the non-ascii characters in the ASA|LINA
CSCwh99647	\"Proxy thread creation successful\" is presented as an Error in syslog messages, during bootup
CSCwi21894	\"zmq_poll return 1\" logs on the FTD console
CSCwi93080	Threat Defense: Messages file contains a flood of logs from \"Ipc\"
CSCwj76075	python package pymonetdb needs version updated to 1.8.2

Identifier	Headline
CSCwd34920	Need to preserve topout.log to contain data of last 5 days minimum
CSCwq19936	Removing acme reference from compile_email.py for chassis manager

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.