Cisco Firepower 4100/9300 FXOS Release Notes, 2.16

First Published: 2024-09-16

Last Modified: 2026-06-03

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.16.0.

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 2.16.2.127

Fixes for various problems (see Resolved bugs in Resolved Bugs in FXOS 2.16.2.127, on page 4)

New Features in FXOS 2.16.2.119

Fixes for various problems (see Resolved bugs in Resolved Bugs in FXOS 2.16.2.119, on page 5)

New Features in FXOS 2.16.1.147

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.16.1.147, on page 6)

New Features in FXOS 2.16.0.136

Fixes for various problems (see Resolved bugs in Resolved bugs in FXOS 2.16.0.136, on page 10)

New Features in FXOS 2.16.0

Cisco FXOS 2.16.0 introduces the following new features:

Feature	Description
Smart Licensing using Smart Transport	Smart Transport is the new transport mechanism used by Smart Licensing to communicate with the Cisco Smart Software Manager (CSSM) server. Smart Transport uses a direct URL to send Smart License messages to the CSSM server. In Firepower 9300 chassis, the transport type is set to Smart Transport by default. You can change it to Call Home from the FXOS CLI. New and modified commands: **scope transport, set transport, set transport smart, set transport-url, set transport callhome, show license transport.** Modified page: **System** > **Licensing** > **Server Configuration**

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 2.16.0 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 2.16.0 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 2.16.0 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	-

FXOS Upgrade Without Firmware Upgrade	Duration(in mins)
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 2.16.2.127

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.16.2.127:

Identifier	Headline
CSCwt88545	Remove diffie-hellman-group14-sha1 from ssh/sshd configuration.
CSCwu32199	SNMP faults in FXOS,
CSCwr94589	FXOS - DME crashes with NULL pointer dereference in SockBioHandle::accept().
CSCwp18885	Firepower 9300/4100 may traceback & reload due to a "Kernel Panic".
CSCwu06269	Firepower 1100 copper SFP ports show link up with GLC-TE/GLC-T despite no cable.
CSCws68206	ASA on hyper-v: couldn't configure VLAN after upgrade.

Identifier	Headline
CSCwt62145	ARP requests are not forwarded to all FTDs on the chassis in multi-instance deployment.
CSCwt55431	Secure Firewall 4200 - Multi-Instance threat defense fails to start with error "Insufficient shaping queue, resource allocation is pending".
CSCwt86672	FXOS: All threat defense instances down on Firepower 4115.
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.
CSCwp83219	Secure Firewall 3100 (aldrin/aldrin2, CPSS 4.3.5) Intf Tx MAC stuck issue when peer reloads/flaps.
CSCwt61597	Continued Evolution of persistence mechanism against Cisco Secure Firewall Adaptive Security Appliance and Secure Firewall Threat Defense.
CSCws51772	Deployment failing with ERR-http-initializing.

Resolved Bugs in FXOS 2.16.2.119

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.16.2.119:

Identifier	Headline
CSCwr59870	ASAv on Hyper-v encountering boot loop issues when running netvsc driver
CSCws79626	FXOS CLI Command Execution Failures Due to Intermittent DME Timeouts
CSCws46901	Management center M6 direct install kernel crash and device struck during baseline.
CSCws25638	Secure Firewall 3110 MI (shared subinterface) - Traffic outage when disabling multicast routing on one FW instance
CSCws91179	Warning about the usage of failsafe-exit
CSCwt43658	Primary Failover interface down after secondary upgrade
CSCwr31136	SNMP OID Polling for Chassis temperature not giving response
CSCwt55803	Secure Firewall 4225 losing communication with netmod
CSCwr22479	Threat defense virtual dropped packets after NAT64 with reason "failed-to-setup-pdts-flow-param"
CSCwr77055	Frequent DME timeouts when run fxos cli command without dme crash
CSCws33462	Faults generated during first boot on 6.x can't be cleared
CSCws01587	Device entering failsafe mode and not exiting even though the app launches
CSCws37370	Threat defense, dcosAG continuously crashing

Identifier	Headline
CSCws26357	Multiple issues with either Interface not coming up or CRC errors with 25/50G LR SFP
CSCws21415	Inotify user watch limits require adjustment for 3100 and 4200 platforms running MI threat defense
CSCwr83390	Secure Firewall 4200: Port-channel flaps while generating chassis FPRM

Resolved bugs in FXOS 2.16.1.147

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.16.1.147:

Identifier	Headline
CSCwk82557	Threat defense upgrade to 7.4.2 via FDM is blocked
CSCwo75483	SNMP polling to chassis is unsuccessful with threat defense Multi-instance in HA used as SNMP agent
CSCwo61241	Logical App Stuck in 'Start Failed' Due to checkSystemCPUs Failure
CSCwq96870	Interfaces are coming up when the Firepower is shutting down
CSCwm52973	TPK Low End FPR3100:Changing interface speed from 1g to 100mbps/100mps to 1g bring downs the link
CSCwo83389	Difference in RSA key length at multiple spots in FXOS
CSCwr22508	Device doesn't boot and gets stuck after a successful upgrade
CSCwo76436	3100 Marvell 4.3.14 CPSS patch for the interface mac stuck issue seen with peer switch reloads
CSCwn40485	MI: Traffic fails to reach the Secondary threat defense when enabled with data-sharing interface
CSCwo50417	Warwick Avenue: LLDP neighbours are not discovered if MGMT 1/2 interface is down
CSCwb02701	FXOS does not retry NTP sync with servers
CSCwq52255	SSH login to FTD management IP address lands in FXOS shell instead of FTD CLISH due to missing /mnt/boot/application/*.def file
CSCwq66838	Multiple heartbeat response failures observed from service orchestration
CSCwo91436	Secure Firewall 4125 multi instance: High Snort and System Core CPU Usage (100%) Triggering FMC Critical Alerts
CSCwn70473	SFF_SFP_10G_25G_CSR_S from Finisar ports bouncing when use as HA link

Identifier	Headline
CSCwf04460	The fxos directory disappears after cancelling show tech fprm detail command with Ctr+c is executed.
CSCwq70133	Password Expiry Age does not reset after Password Change
CSCwm54190	Firepower 1010 and Secure Firewall 1200: ASA app instance stuck in start failed state START_FAILED, CPU resources Unavailable
CSCwq92373	For 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.
CSCwh78517	Failed to import the configuration fail @FSM-STAGE:sam:dme:MgmtImporterImport:config in 92.16.0.125
CSCwi48918	FXOS sends fast LACP PDUs even if partner requests slow rate
CSCwq60586	Threat Defense upgrade failed due to bundle image existence verification failure
CSCwm48550	Secure Firewall CSF-1200: sma reported fault: Lina has started, but is not yet running
CSCwq36466	expat/xml FW rebooted itself and no crashinfo generated
CSCwm49154	FXOS fault F1738 seen in deploymet with Error: CSP_OP_ERROR. CSP signature verification error
CSCwo71052	FPR1010 Ethernet1/1 trunk port is not passing Vlan traffic after a reload
CSCwq26863	FP2110 - ntpd process constantly crashing
CSCwq31342	FPR4200 | FPR3100 Multi Instance Chassis Deployment Failed in DNS configuration
CSCwd40371	9300 date setting shows Jan 1 2012 - causing 9300 threat defense registration with management center to fail
CSCwm06393	Changes in port-channel membership or member status may cause periodic OSPF/EIGRP adjacency flaps
CSCwq21442	3RU MI instances offline after baseline/creation
CSCwj98673	Fail to start a disabled container on chassis reboot and misses to log the activity to Heimdall
CSCwd92327	On Firepower 2100 platform, external authentication fails for users starting with number
CSCwp89969	Prolonged delays in firewall restart/reboot completion
CSCwo42102	show tech-support fprm detail command is getting stuck for longer duration
CSCwo75810	SNMP configuration is not applied consistently across same FTDs type and version
CSCwo86422	Unidirectional communication over ccl leading to split-cluster.
CSCwr88733	Collecting "show tech-support fprm" results in corefile in TAR process

Identifier	Headline
CSCwm51747	SSH access with public key authentication fails after FXOS upgrade
CSCwq53328	Multicast and unicast packets do not reach the correct instance for random subinterfaces
CSCwm03142	IPv6 Neighbor Discovery/multicast traffic affected on shared interface in multi instance setup
CSCwn71596	Intf Link down (Init, mac-link-down) seen - EtherChannel Membership in Down/Down/Down state after unplug/replug of the cable
CSCwq74986	FTD: Instance stuck in Boot Loop
CSCwo94274	FP4100/9300 Fatal error: Incomplete chain observed before watchdogs with reset code 0x0040
CSCwm49782	enhance sma 2nd cruz heartbeat logging
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
CSCwo26258	Default Route Changes from Management0 to Management1 After Reload or Upgrade on FPR 4200 Series
CSCwj69632	Default Hashing Algorithm is SHA1 for Firepower Chassis Manager Certificate on 4110
CSCwo57740	'${dsk_a} missing or inoperable. Rebooting Blade.' error does not specify missing or inoperable disk
CSCwn98402	Debuggability: FP2100 port-channel interfaces flap after upgrade
CSCwk62297	Evaluation of ssp for OpenSSH regreSSHion vulnerability
CSCwn13187	ASA upgrade failing from 9.20.2.21 to the target version 9.20.3.4
CSCwk67859	Threat Defense and FXOS: RADIUS Protocol Spoofing Vulnerability (Blast-RADIUS): July 2024
CSCwq65955	Secure Firewall 4200: HA link arp packets getting dropped, internal uplink linkChange counters incrementing
CSCwn11728	FPR9K-SM-56 module intermittently lock up and cause traffic impact.
CSCwh19613	ASA crashed with Saml scenarios
CSCwi13062	Debug messages seen on console on executing show tech-support fprm detail
CSCwo65866	Network Outage when Primary FTD Instance is Disabled from FCM
CSCwk88225	Critical fault : [FSM:FAILED]: user configuration(FSM:sam:dme:AaaUserEpUpdateUserEp)
CSCwm50936	100GB interface flaps with Innolight QSFPs in both ends

Identifier	Headline
CSCwm34333	Threat Defense - Multi-Instance, docker0 interface overlap with private network 172.17.0.0/16
CSCwn06641	FTD syslog-over-TLS allowing too many curves in CC mode
CSCwn47308	Critical health alerts 'user configuration(FSM.sam.dme.AaaUserEpUpdateUserEp)' on FPR 1100/2100/3100
CSCwm64553	Incompatible members warning message after Po member interface flaps unable to rejoin Po
CSCwn00093	ASA may traceback and reload in snp_fp_shared_ingress and generate a LINA core
CSCwm95189	Redis is an open source, in-memory database that persists on disk. An
CSCwi79120	some ssh sessions not timing out, leading to ssh and console unable to connect to the FXOS CLI
CSCwr59870	ASAv on Hyper-v encountering boot loop issues when running netvsc driver
CSCwn29611	Radius user ssh login fails with error: username is not defined with a service type that is valid
CSCwm96280	Threat Defense device stuck in rommon mode after pressing reset button
CSCwq85986	For Secure Firewall 4225, interface with SFP - 10/25G_LR_S (or CSR_S) is not coming up after reboot of peer side.
CSCwo05712	Serviceability Enhancement - Make FXOS disk errors more descriptive
CSCwm30872	Insufficient Input Validation Vulnerability
CSCwn92248	Firepower 1100/2100: Port-channel interfaces flap with LACP
CSCwn46426	The **sh environment temperature** shows incorrect temperature values on 2100 platform
CSCwq23394	Threat Defense may drop traffic in the Azure cloud at mlx5 driver level.
CSCwp33410	dmesg and kern.log file flooded with Tx Queue=0 logs
CSCwm30886	Insufficient Input Validation Vulnerability
CSCwn45049	Coverity System SA warnings 2024-09-09, Coverity Defects 922530 922529 922528 922630 921809 921808
CSCwq31988	Errors on all interface of Firepower 1010, line protocol is down (not associated with supervisor)
CSCws07111	Secure Firewall 4200: port-manager: ERROR: portmanager DIED after doing 'no shut' for Ethernet interfaces
CSCwn93411	FXOS reset and reload due to snmpd service failure
CSCwi59271	Suppress "End of script output before headers" syslog on FXOS

Identifier	Headline
CSCwm52264	Not able to remove or clear Fault "The password encryption key has not been set."
CSCwn19190	Memory fragmentation resulted in huge pages unavailable for lina
CSCwn79553	Unreachable LDAP/AD referrals may cause delays or timeouts in external authentication on FTD
CSCwm35751	For Secure Firewall 3100, interface may go to half duplex speed is hardcoded to 100mbps
CSCwn44335	FXOS - Download command generates an extra "/" over HTTP and HTTPS GET requests
CSCwp06890	SFF_SFP_10G_25G_CSR_S V03 modules from Finisar ports bouncing when connected.
CSCwp02224	FPR failover split brain when upgrade primary/standby device's FXOS version
CSCwn59032	Secure Firewall Chassis Manager GUI became inaccessible after upgrading to ASA 9.18.4.22 on FPR 2130 Platform Mode
CSCwq95241	Reboots on FP2130 due to missing heimdall PID
CSCwq39942	CVE-2025-32463: sudo: Sudo before 1.9.17p1 allows local users to obtain
CSCwq39943	CVE-2025-32462: sudo: Before 1.9.17p1, allows users to execute commands on unintended machines.
CSCws21415	Inotify user watch limits require adjustment for 3100 and 4200 platforms running MI FTDs
CSCwi00713	A memory leak flaw was found in Libtiff's tiffcrop utility. This issue

Resolved bugs in FXOS 2.16.0.136

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.16.0.136:

Identifier	Headline
CSCwb77894	Firepower 1000/2100 may boot to ROMMON mode
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
CSCwj98673	Fail to start a disabled container on chassis reboot and misses to log the activity to Heimdall
CSCwn44335	FXOS - Download command generates an extra "/" over HTTP and HTTPS GET requests

Identifier	Headline
CSCwn21204	SNMPv3 on Management Interface Intermittently Unresponsive with Frequent SNMP Core Files Generated
CSCwm49154	FXOS fault F1738 in multi-instance deploymet. Error: CSP_OP_ERROR. CSP signature verification error
CSCwm52264	Not able to remove or clear Fault "The password encryption key has not been set."
CSCwn19190	memory fragmentation resulted in hugepages unavailable for lina
CSCwn46426	ASA 21xx: 'sh environment temperature shows incorrect temperature values
CSCwm03142	IPv6 Neighbor Discovery failure on shared interface in multi instance setup
CSCwm52973	Secure Firewall 3100:Changing interface speed from 1g to 100mbps/100mps to 1g bring downs the link
CSCwm35751	FPR3100: Interface may go to half duplex speed is hardcoded to 100mbps
CSCwn13187	ASA upgrade failing from 9.20.2.21 to the target version 9.20.3.4
CSCwm49782	Enhance sma 2nd cruz heartbeat logging
CSCwm06393	Changes in port-channel membership or member status may cause periodic OSPF/EIGRP adjacency flaps
CSCwn40485	MI: Traffic fails to reach the Secondary threat defense when enabled with data-sharing interface
CSCwm34333	Threat defense - Multi-Instance, docker0 interface overlap with private network.

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.