Cisco Firepower 4100/9300 FXOS Release Notes, 2.11(1)

First Published: 2021-08-06

Last Modified: 2023-08-04

Cisco Firepower 4100/9300 FXOS Release Notes, 2.11(1)

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.11(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.
- 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 2.11.1 introduces the following:

New Features in FXOS 2.11.1.205

Fixes for various problems (see Resolved bugs in FXOS 2.11.1.205, on page 10).

New Features in FXOS 2.11.1.200

Fixes for various problems (see Resolved bugs in FXOS 2.11.1.200).

New Features in FXOS 2.11.1.182

Fixes for various problems (see Resolved bugs in FXOS 2.11.1.182).

New Features in FXOS 2.11.1

Cisco FXOS 2.11.1 introduces the following new features:

Feature	Description
Integration of MIO health with existing health monitoring infra and FMC UI	You can now use the newly added **scope health monitoring policy** CLI to enable or disable the health monitoring and set the required fault threshold for each type of resource. You can also use the **show storage** CLI to display the partitions and current disk usage in a disk.

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 2.11(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 2.11(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 2.11(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 2.11(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 2.11.1.200

Identifier	Headline
CSCwc74905	FXOS: FPR-X-NM-8X10G ports 7 and 8 are unconfigurable.
CSCwc45356	FXOS: Support a single PID type for Secure Firewall 3100 platforms.
CSCwb25926	TPK Netmods - Debug Proto card ACT2 authentication failures.
CSCwb89257	Remote user log in via SSH access with password authentication method fails after FXOS upgrade.
CSCwd37560	Adding forceReboot option for bundle install REST API.
CSCwd45784	FXOS SWIMS Engine update to version 3.0.4.

Resolved bugs in FXOS 2.11.1.182

Identifier	Headline
CSCwa32286	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 125, seq 21).
CSCwb12119	CIAM: expat - CVE-2022-25235 and others
CSCwb05042	CIAM: python - CVE-2022-0391
CSCwb71582	CIAM: strongswan - CVE-2021-45079
CSCwa20758	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 20).
CSCwa62167	CIAM: Apache-http-server CVE-2021-44790 and CVE-2021-44224.
CSCwb70138	CIAM: python CVE-2015-20107
CSCwa00038	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted.
CSCvu47035	Reject the NTP server on the MIO side when the stratum value is higher than device can handle.
CSCwc08683	The interface's LED remains green blinking when the optical fiber is unplugged on FPR1150.

Identifier	Headline
CSCwb02689	FXOS should check reference clock stratum instead of NTP server's local clock stratum.
CSCwc46569	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 34).
CSCwa69303	ASA running on SSP platform generate critical error "[FSM:FAILED]: sam:dme:MgmtIfSwMgmtOobIfConfig".
CSCwb70030	MIO: No blade reboot during CATERR if fault severity is non-Severe or CATERR sensor is different.
CSCwa33686	CIAM: bind 9.11.4
CSCwc38361	Cisco FXOS Software Command Injection Vulnerability.
CSCwc41590	Upgrade fail App Instance fail to start with err "CSP_OP_ERROR. CSP signature verification error."
CSCwb40662	ENH: FCM should include option for modifying the interface 'link debounce time'
CSCwb41361	WR8, LTS18 and LTS21 commit id update in CCM layer (seq 26).
CSCwa76822	Tune throttling flow control on syslog-ng destinations.
CSCwb71554	CIAM: libxml - CVE-2022-23308
CSCwa33688	CIAM: cpio 2.12
CSCwb27099	FXOS: Third-party interop between Ciena Waveserver with firepower chassis.
CSCwa90615	WR8 and LTS18 commit id update in CCM layer (seq 24)
CSCwa70299	CIAM: expat multiple Vulnerabilities
CSCwb01633	FXOS misses logs to diagnose root cause of module show-tech file generation failure
CSCwa53271	CIAM: mod-security - CVE-2021-42717
CSCwa05385	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 124, seq 19)
CSCwb44662	CIAM: zlib - CVE-2018-25032
CSCwa06608	WM 1010 HA Failover is not successful when we give failover active in secondary.
CSCwc08676	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 32)
CSCwa85297	Multi-instance internal portchannel VLANs may be misprogrammed causing traffic loss
CSCwb13294	WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 25)
CSCwa42350	ASA installation/upgrade fails due to internal error "Available resources not updated by module"
CSCwb32772	Evaluation of ssp for vulnerabilities resolved in Apache httpd 2.4.53

Identifier	Headline
CSCwb46949	LTS18 commit id update in CCM layer (seq 27)
CSCwb12465	FIPS self-tests must be run when CC mode is enabled - files are missing
CSCwb57988	The smConLogger traceback is caused by memory leak.
CSCwa52215	Uploading firmware triggers data port-channel to flap
CSCwa65681	TPK/KP/WM-RM: Assign FXOS interface MAC address to LLDP linux interfaces
CSCwb74498	Cisco FXOS and NX-OS Software CDP DoS and Arbitrary Code Execution Vulnerability
CSCwa81112	CIAM: expat - CVE-2022-23852
CSCvz83432	WR6, WR8 and LTS18 commit id update in CCM layer(sprint 121, seq 18)
CSCwb62105	CIAM: glibc 2.33 CVE-2022-23219 and others
CSCwc25207	WR6, WR8, LTS18 and LTS21 commit id update in CCM layer (Seq 33)
CSCwb83166	Upgrade to CiscoSSL FOM 7.3sp and CiscoSSL 1.1.1o.7.3sp.143-fips in SSP MIO
CSCwb48166	FXOS upgrade to 2.11 is stuck
CSCwa88148	ENH: Fail-to-Wire feature switching standby/bypass from CLI
CSCwb24367	Evaluation of ssp for Dirty Pipe vulnerability
CSCwb10884	WM11xx: Getting "ERROR: waiting for fxos_log_shutdown" during shutdown.
CSCwa71071	Update certificate bundle for 7.2 release.
CSCwa49417	WR8 and LTS18 commit id update in CCM layer (sprint 126, seq 22).
CSCvy84945	Interface is down after RBD wizard CLI execution.
CSCwa24265	FXOS changes to provide dmidecode access to container.
CSCwc08094	Update CiscoSSL to 1.1.1o.7.3sp.143
CSCvv21522	Integrate SSD firmware image into lfbff_parser.
CSCvy77245	"zgrep" tool missing from ftd 2100 models.
CSCvz93644	Add strace to internal debug builds.
CSCwa16251	USB kernel modules required for FMC.
CSCwa25995	NBN: New PSU PID support in MIO.
CSCwb20072	Update LTS18 to RCPL 24.
CSCwa47567	Move 7.1 branches to the LTS18 code base.

Identifier	Headline
CSCvz44638	FXOS changes for CSCvy86319 - Data are not getting destroy after formatting disk0 on ISA3K.
CSCwb74973	FXOS: WARNING: Configuration file format is too old, syslog-ng is running in compatibility mode.
CSCwa46997	Back out CSCvy28132 as eBPF is not needed in FXOS for 7.1 or 7.2.
CSCwa67086	Swapping different speed ftw causes admin speed issues.
CSCwb90344	TPK 3120 in 7.1.0.2-16, interface went down with 1016 sub-interfaces, HA changed to Failed.
CSCwc03510	Kilburn Park freezes / crashes on netboot system load.
CSCwa90735	ASAconsole.log files fail to rotate.
CSCwa10201	Cisco FXOS Software Command Injection Vulnerability.
CSCwc02133	Root shell injection in security module "support fileview" command.
CSCwa99171	Chassis and application sets the time to Jan 1, 2010 after reboot

Resolved bugs in FXOS 2.11.1.154

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.11.1.154:

Caveat ID Number	Description
CSCvu84127	Firepower may reboot for no apparent reason
CSCvv79459	WR6, WR8 and LTS18 commit id update in CCM layer (sprint 94, seq 1)
CSCvv84358	VIC adapter kernel crash at boot
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)
CSCvw30887	MIO crashed due to HA policy of Reset with Service: bcm_usd hap reset
CSCvw62255	"Link not connected" error when using WSP-Q40GLR4L transceiver and Arista switch
CSCvw79465	FXOS upgrade does not do proper compatibility check for FTD image
CSCvw72260	ASA upgrade failed with: "CSP directory does not exist - STOP_FAILED Application_Not_Found"
CSCvx16700	FXOS clock sync issue during blade boot up due to "MIO DID NOT RESPOND TO FORCED TIME SYNC"

Caveat ID Number	Description
CSCvx25336	ENH: add a way to disable the FQDN check
CSCvx29429	ma_ctx*.log consuming high diskspace on FPR4100/FPR9300 despite the fix forCSCvx33904 CSCvx07389
CSCvx33904	Sudo before 1.9.5p2 has a Heap-based Buffer Overflow, allowing privile
CSCvx73164	Lasso SAML Implementation Vulnerability Affecting Cisco Products: June 2021
CSCvx78005	top.log file missing and sftop process exiting every minute on FDM after FXOS 2.10.1 upgrade
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
CSCvy48764	SSH access with public key authentication requires user password
CSCvy95497	Chassis SSD firmware upgrade may be prevented improperly
CSCvz15676	In WM-1010 model, after upgrading ASA app, device going for fail safe mode
CSCvs37955	Confusing message about 'without removing the physical hardware' during Acknowledge Security Module
CSCvs73924	FCM should say is not possible to change AAA server when same protocol is configured for Auth
CSCvu70493	FXOS - AAA/RADIUS - NAS-IP Field set to 127.0.01
CSCvz91266	FXOS A crafted request uri-path can cause mod_proxy to forward the request to an origin server...
CSCvz94740	FXOS Crash- %SYSMGR-2-HEARTBEAT_FAILURE: Service "ascii-cfg" sent SIGABRT for not setting heartbeat
CSCvv36788	MsgLayer[PID]: Error : Msglyr::ZMQWrapper::registerSender() : Failed to bind ZeroMQ Socket
CSCvv74658	FTD/ASA creates coredump file with "!" character in filename (zmq changes (fxos) for CSCvv40406)
CSCvw05392	Message appearing constantly on diagnostic-cli
CSCvw33536	4100/9300: Cannot associate port channel / interface to App
CSCvw53494	CRUZ paloview is not accessible on release build
CSCvw67974	SSH access with public key authentication fails after FXOS upgrade
CSCvw95181	FXOS upgrade fails with error "does not support application instances of deployment type container"
CSCvx01786	Pre-login-banner not showing on FCM WebUI

Caveat ID Number	Description
CSCvx38047	FXOS show fault warning code F4526902
CSCvx82705	Evaluation of ssp for OpenSSL March 2021 vulnerabilities
CSCvx48862	Unable to save new cluster node configs on FCM due to java error
CSCvy66942	FPR4100/9300 IPv6 config cannot be applied using Rest API LTP on 9300/4100 Supervisor
CSCvx14602	Firepower memory leak in svc_sam_dcosAG
CSCvw77924	Radius Key with the ASCII character " configured on FXOS does not work after chassis reload.
CSCvw98315	FXOS reporting old FTD version after FTD upgrade to 6.7.0
CSCvy39791	Lina traceback and core file size is beyond 40G and compression fails.
CSCvy72185	FXOS Apache HTTP Server Multiple Vulnerabilities (CVE-2020-11993) and (CVE-2020-9490)
CSCvy80380	Disk utilization increasing /var/tmp in FPR4150-ASA chassis
CSCvy83657	FXOS process core pruned/deleted from system files (no validation)
CSCvy89648	ma_ctx files with '.backup' extension seen after applying the workaround for CSCvx29429
CSCvz50201	FXOS may display fault F1256 about missing local disk 0
CSCvz53884	SNMP OID HOST-RESOURCES-MIB (1.3.6.1.2.1.25) does not exist on FMC
CSCvz66474	Snmpd core files generated on FTD
CSCvz94217	App-instance startup version is ignored and set to running-version after copy config

Open Bugs in FXOS 2.11.1.154

The following table lists the open bugs in FXOS 2.11.1.154:

Caveat ID Number	Description
CSCvv82681	FTD device stuck with "watchdog: BUG: soft lockup - CPU#0 stuck" error on console
CSCvz90937	SFDatacorrelator exits - missing libgnutls.so - on new installation or after FTD upgrade
CSCwa00038	Disk corruption occurs when /mnt/disk0 partition is full and blade is rebooted
CSCwa21333	FTD app-instance start-failed with STOP_FAILED CSP_Stop_App_Error
CSCvj95701	Firepower configured in inline-pair interfaces are admin and link down
CSCvr17111	FXOS may display fault F1758 about external port conflict with application

Caveat ID Number	Description
CSCvy12991	Chassis local date and time may drift back to midnight Jan 1 2015 after reboot

Resolved bugs in FXOS 2.11.1.205

Identifier	Headline
CSCwc61106	Unable to configure domain\username under cfg-export-policy in FXOS.
CSCwd99813	Supervisor does not reboot unresponsive module/blade due to CATERR with minor severity sensor ID 50.
CSCwe33130	Supervisor does not reboot unresponsive module/blade due to IERR with minor severity sensor ID 79.
CSCwc30239	CIAM: apache-http-server - CVE-2022-31813 and Others.
CSCwc34082	CIAM: curl - CVE-2022-22576 and others.
CSCwc65508	CIAM: libtirpc - CVE-2021-46828.
CSCwc78220	CIAM: zlib - CVE-2022-37434.
CSCwe25314	Refresh the ios.pem.
CSCwe32972	stdout_env_manager.log is full of Unknown board type 3 messages.
CSCwf22483	SSH to Chassis allows a 3-way handshake for IPs that are not allowed by the config.
CSCwf30824	Add CIMC reset as auto-recovery for CIMC IPMI hung issues.
CSCwf50358	FCM: jacoco lib needs upgrade.
CSCwb66175	MIO is not able to register. appAG process issue.
CSCwd06758	No input validation for logical device DNS servers in bootstrap configuration on chassis manager.
CSCwa55772	FPR 4100 saw an unexpected reload with reason "Reset triggered due to HA policy of Reset".
CSCwc82169	FPR4100/9300 High traffic redirected to CPU causes internal communication failure with blade adapter.
CSCwb84967	FPR4K/FPR9K: Generating FXOS Chassis show tech may result to flap of 40Gig Netmod Port.
CSCwf16886	Universal p4tickets are in plaintext in source code.

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.