Cisco Firepower 4100/9300 FXOS Release Notes, 2.7(1)

First Published: 2019-11-12

Last Modified: 2021-05-17

Cisco Firepower 4100/9300 FXOS Release Notes, 2.7(1)

This document contains release information for Cisco Firepower eXtensible Operating System (FXOS) 2.7(1).

Use this release note 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 Firepower security appliance is a next-generation platform for network and content security solutions. The Firepower 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 Firepower 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

New Features in FXOS 2.7.1.131

Fixes for various problems (see Resolved Bugs in FXOS 2.7.1.131, on page 8).

New Features in FXOS 2.7.1.122

Fixes for various problems (see Resolved Bugs in FXOS 2.7.1.122, on page 10).

New Features in FXOS 2.7.1.106

Fixes for various problems (see Resolved Bugs in FXOS 2.7.1.106, on page 10).

New Features in FXOS 2.7.1.98

Fixes for various problems (see Resolved Bugs in FXOS 2.7.1.98, on page 10).

New Features in FXOS 2.7.1.92

Cisco FXOS 2.7.1.92 introduces the following new features:

Table 1: New Features in FXOS 2.7.1.92

Feature	Description
Support for ASA 9.13(1)	For more information about ASA 9.13.1, see Release Notes for the Cisco ASA Series, 9.13(x). For more information about version compatibility, see Cisco Firepower 4100/9300 FXOS Compatibility.
Support for Firepower Threat Defense 6.5	For more information about FTD 6.5, see Cisco Firepower Release Notes, Version 6.5.0. For more information about version compatibility, see Cisco Firepower 4100/9300 FXOS Compatibility.
Support for FTD with Firepower Device Manager	You can now deploy a native FTD instance and specify FDM management. Container instances are not supported. New/Modified commands: `scope ssa > enter logical-device > create mgmt-bootstrap >` **enter bootstrap-key MANAGEMENT_TYPE**, **set value LOCALLY_MANAGED** . New/modified Firepower Chassis Manager screens: **Logical Devices > Add Device > Settings > Management type of application instance** Note: Requires FTD 6.5.0 or later.
Support for hardware bypass OIR	You can now perform an Online Insertion and Removal (OIR) for hardware bypass network modules.

Feature	Description
TLS crypto acceleration for multiple container instances	TLS crypto acceleration is now supported on multiple container instances (up to 16) on a Firepower 4100/9300 chassis. Previously, you could enable TLS crypto acceleration for only *one* container instance per module/security engine. New instances have this feature enabled by default. However, the upgrade does *not* enable acceleration on existing instances. Instead, use the **create hw-crypto** and **scope hw-crypto** CLI commands. For more information, see the Cisco Firepower 4100/9300 FXOS Command Reference.
Support for ASA Security Service Exchange (SSE) Telemetry	With Cisco Success Network enabled in your network, device usage information and statistics are provided to Cisco, which are used to optimize technical support. The telemetry data that is collected on your ASA devices includes CPU, memory, disk, or bandwidth usage, license usage, configured feature list, cluster/failover information and the like.
Support for 500 VLANs without contingencies	Previously, the device supported between 250 and 500 VLANs, depending on the number of parent interfaces and other deployment decisions. You can now use 500 VLANs in all cases.
Support for downloading images using HTTP/HTTPS	You can now download FXOS images using HTTP/HTTPS through the FXOS CLI and RestAPI.
Chassis Manager support for LLDP configuration	You now have the option to enable or disable LLDP using the Firepower Chassis Manager interface.
New IPSec ciphers and algorithms	Added the following IKE and ESP ciphers and algorithms: • Ciphers—aes192. Existing ciphers include aes128, aes256, aes128gcm16. • Pseudo-Random Function (PRF) (IKE only)—prfsha384, prfsha512, prfsha256. Existing PRFs include prfsha1. • Integrity Algorithms—sha256, sha384, sha512, sha1_160. Existing algorithms include sha1. • Diffie-Hellman Groups—curve25519, ecp256, ecp384, ecp521, modp3072, modp4096. Existing groups include modp2048.
Keyring certificate request FQDN checks	The feature checks the subject name and DNS fields when a certificate request is created to ensure the values entered are FQDNs. Previously, the options that allowed adding subject alternative names to certificate requests only accepted one parameter. Now, you can add multiple values for dns, e-mail, ip, and ipv6 fields. Added the "set DNS" command to disable the FQDN check.

Feature	Description
SSH authentication enhancements	Added the following SSH server encryption algorithms: • aes128-gcm@openssh.com • aes256-gcm@openssh.com • chacha20-poly@openssh.com Added the following SSH server key exchange methods: • diffie-hellman-group14-sha256 • curve25519-sha256 • curve25519-sha256@libssh.org • ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521
ECDSA keys for keyrings	You can now use ECDSA keys for keyrings. Previously only RSA keys were supported.
User password improvements	Added password security improvements, including the following: • Local and remote user passwords can be up to 127 characters. The old limit was 80 characters. • Strong password check is enabled by default. • Prompt to set admin password. • Password expiration. • Limit password reuse. • Removed the **set change-during-interval** command, and added a **disabled** option for the **set change-interval**, **set no-change-interval**, and **set history-count** commands.
Secure erase for appliance components	You can now use the **erase secure** FXOS CLI command to securely erase a specified appliance component.
Fixes for various problems	For more information, see Resolved Bugs in FXOS 2.7.1.92, on page 11.

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

- To mitigate CSCvq34340, upgrading an FTD device to Version 6.5.0.2 turns off egress optimization processing regardless of whether the egress optimization feature is enabled or disabled. For more information, see Cisco Firepower Release Notes, Version 6.5.0.x.
- 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.
- If you reinitialize a security module after upgrading to FXOS 2.6(1), you might receive an error message about disk partitions on that security module being incompatible if you later downgrade to an earlier FXOS release. To resolve this issue, you need to reinitialize the security module again after downgrading.
- 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.

Adapter Bootloader Upgrade

FXOS 2.7(1) provides additional testing to verify the security module adapters on your security appliance. After installing FXOS 2.4.1.101 or later, you might receive a critical fault similar to the following indicating that you should update the firmware for your security module adapter:

Critical F1715 2017-05-11T11:43:33.121 339561 Adapter 1 on Security Module 1 requires a critical firmware upgrade. Please see Adapter Bootloader Upgrade instructions in the FXOS Release Notes posted with this release.

If you receive this, use the following procedure to update the boot image for your adapter. Note that this procedure may result in a traffic disruption, and thus should be performed during a maintenance window to avoid business impact.

1. Connect to the FXOS CLI on your Firepower security appliance. For instructions, see the "Accessing the FXOS CLI" topic in the Cisco Firepower 4100/9300 FXOS CLI Configuration Guide, 2.7(1) or Cisco Firepower 4100/9300 FXOS Firepower Chassis Manager Configuration Guide, 2.7(1).
2. Enter the adapter mode for the adapter whose boot image you are updating:

   fxos-chassis# **scope adapter 1/***security_module_number/adapter_number*
3. Enter **show image** to view the available adapter images and to verify that fxos-m83-8p40-cruzboot.4.0.1.62.bin is available to be installed:

```
fxos-chassis /chassis/server/adapter # show image
Name Type Version

------------------------------------------- ------------------- -------

fxos-m83-8p40-cruzboot.4.0.1.62.bin Adapter Boot 4.0(1.62)

fxos-m83-8p40-vic.4.0.1.51.gbin Adapter 4.0(1.51)
```

4. Enter **update boot-loader** to update the adapter boot image to version 4.0.1.62:

```
fxos-chassis /chassis/server/adapter # update boot-loader 4.0(1.62)
Warning: Please DO NOT reboot blade or chassis during upgrade, otherwise, it may cause
adapter to become UNUSABLE!
After upgrade has completed, blade will be power cycled automatically
fxos-chassis /chassis/server/adapter* # commit-buffer
```

5. Enter **show boot-update status** to monitor the update status:

```
fxos-chassis /chassis/server/adapter # show boot-update status
State: Updating
fxos-chassis /chassis/server/adapter # show boot-update status
State: Ready
```

6. Enter **show version detail** to verify that the update was successful:

Note Your **show version detail** output might differ from the following example. However, verify that Bootloader-Update-Status is "Ready" and that Bootloader-Vers is 4.0(1.62).

```
fxos-chassis /chassis/server/adapter # show version detail
Adapter 1:
Running-Vers: 5.2(1.2)
Package-Vers: 2.2(2.17)
Update-Status: Ready
Activate-Status: Ready
Bootloader-Update-Status: Ready
Startup-Vers: 5.2(1.2)
Backup-Vers: 5.0(1.2)
Bootloader-Vers: 4.0(1.62)
```

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 2.7(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 to FXOS 2.7(1) if it is currently running any FXOS 2.0(1) or later build.

For upgrade instructions, see the Cisco Firepower 4100/9300 Upgrade Guide.

Installation Notes

- An upgrade of a single chassis to FXOS 2.7(1) can take up to 45-60 minutes. Note that your upgrade time may vary depending on the hardware, software, and complexity of your deployment. Plan your upgrade activity accordingly.

  Use **scope system > show firmware monitor** in the FXOS CLI to monitor your upgrade progress.

- 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.

Open and Resolved Bugs

The open and resolved 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.

Open Bugs

The following table lists select bugs open at the time of this Release Note publication:

Table 2: Open Bugs Affecting FXOS 2.7(1)

Identifier	Description
CSCvq30293	Bootstrap configuration is not updated after FTD version downgrade

Identifier	Description
CSCvq47804	FXOS security module will not power up after FTD shutdown
CSCvq87570	" hostname transmission sts" script is getting failed due to exception Hostname null
CSCvr08375	ASA telemetry: add another FSM stage to check enrollment and call GET KEY before registration stage
CSCvr18121	Observed "Overall status : Disc failed" in show server status after acknowledging slot 1
CSCvr20219	MISMATCH between versions on FXOS UI and FMC shown after upgrade from 6.4.0.4 to 6.5

Resolved Bugs in FXOS 2.7.1.143

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.7.1.143:

Table 3: Resolved Bugs in FXOS 2.7.1.143

Identifier	Description
CSCvu78537	FXOS Multi-Instance fault F0479 Virtual Interface link state is down
CSCvv96092	Cisco FXOS and NX-OS Software UDLD DoS and Arbitrary Code Execution Vulnerability
CSCvw38984	Cisco FXOS and NX-OS Software UDLD DoS and Arbitrary Code Execution Vulnerability
CSCvx13861	QuoVadis root CA decommission on Firepower 9300/4100 Supervisor
CSCvx88998	\"System does not allow more than 16 TPs\" on 2.3.1.213
CSCvx90804	MIO SSD upgraded to wrong firmware version
CSCvy23422	QW:4112:FXOS traceback and reload after upgrade to 2.8.1.143
CSCvo14325	Make sure MIO reboot in case of firmware upgrade is graceful
CSCvu01873	CSP/SPA installation file name check wont allow valid characters
CSCvv05277	Need to support firmware upgrade for SSD in FXOS

Resolved Bugs in FXOS 2.7.1.131

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.7.1.131:

Table 4: Resolved Bugs in FXOS 2.7.1.131

Identifier	Description
CSCvj00997	"show open-network-ports" not showing the proper information on FPR4100 Series
CSCvn78002	FPR4100/9300 Smart Licensing fail - Error : Licensing internal error(68)
CSCvr68885	FXOS fault F0479 Virtual Interface link state is down
CSCvr74901	AppAG encoding for FXOS logical device bootstrap
CSCvr79926	FXOS crash (Traceback in cruz)
CSCvr88163	FPR9300 hangs after reboot is triggered for firmware upgrade
CSCvs34851	Continuous link flapping leading to snm_log corefile
CSCvs41966	Inconsistent interface status on the FXOS when Port is Down by Propagate Link State
CSCvs90447	FXOS 8x1G FTW continuous link flap
CSCvs92044	FXOS L3 Egress Object Resource Leak due to Port-Channel Member Interface Flaps
CSCvt06091	FXOS displays a WSP-Q40GLR4L transceiver from show interface as type QSFP-40G-LR4
CSCvt06743	FTW watch-dog kick delays which might cause inline sets to go down/Bypass-Fail
CSCvt17448	OSPF multicast mac getting removed from l2-table causing OSPF to fail
CSCvt17947	Need dedicated Rx rings for failover and OSPF on Firepower platform - Cruz fix
CSCvt20235	Firepower 4100 series all FTW interfaces link flap at the same time but occur rarely
CSCvt34160	"Link not connected" error after reboot when using WSP-Q40GLR4L transceiver on FPR9K-NM-4X40G
CSCvt39897	FP 4120 svc_sam_dcosAG crashed with crash type:139
CSCvt70832	fpr4100 snmp polling to fxos memory-usage shows incorrect value compare with CLI's output
CSCvt78809	Instance start failed due to VNIC configuration error
CSCvt90558	9300/4100 : Port-channel down after chassis software upgrade.
CSCvu11868	"Link not connected" error after reboot when using QSFP-40G-LR4 transceiver on FPR9K-NM-4X40G

Identifier	Description
CSCvu27487	FXOS ASA race condition leading to cluster join failure and network outage
CSCvu76107	ASA app-instance restart without audit log or trigger
CSCvu78537	FXOS Multi-Instance fault F0479 Virtual Interface link state is down
CSCvu85589	Firepower 9300 FPR-NM-4X100G or FPR-NM-2X100G interface may blackhole port-channel member traffic
CSCvu94706	FXOS dynamically learning mac-address of external machine causing outage

Resolved Bugs in FXOS 2.7.1.122

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.7.1.122:

Table 5: Resolved Bugs in FXOS 2.7.1.122

Identifier	Description
CSCvs23575	BladeAG reload due to memory leak with M5 blade

Resolved Bugs in FXOS 2.7.1.106

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.7.1.106:

Table 6: Resolved Bugs in FXOS 2.7.1.106

Identifier	Description
CSCvi48404	Firepower Chassis Reloads due to License Manager
CSCvn11962	FxOS randomly shows one NTP server as 'Unreachable Or Invalid Ntp Server' once added 4 NTP servers
CSCvq93572	Unable to add user on FTD using external authentication
CSCvr02367	[ciam] Apache HTTP Server mod_rewrite Configurations Open Redirect Vulnerability
CSCvr82740	mgmt bootstrap PASSWORD should not be in appAG log
CSCvs39368	DME process crash due to memory leak on Firepower 9300/4100

Resolved Bugs in FXOS 2.7.1.98

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.7.1.98:

Table 7: Resolved Bugs in FXOS 2.7.1.98

Identifier	Description
CSCvp69229	OpenSSL 0-byte Record Padding Oracle Information Disclosure Vulnerabil
CSCvq31946	Ability to disable auto-negotiation for SFP (1G optical)
CSCvr01651	Data interfaces bring up delayed after chassis reboot
CSCvr04845	DME crash after FXOS chassis reload with maximum number of https ip-blocks configured
CSCvr24920	FPR-4110: FXOS CLI crash in feature-mgr process
CSCvr40573	FPR-4100: FXOS CLI crash with fwm hap reset

Resolved Bugs in FXOS 2.7.1.92

The following table lists the previously release-noted and customer-found bugs that were resolved in FXOS 2.7.1.92:

Table 8: Resolved Bugs in FXOS 2.7.1.92

Identifier	Description
CSCvd90177	Security Module went to fault state after reloading Supervisor on 4150 with FXOS 2.2.1.57
CSCvj93832	SM40/48/56 x86 cpu fails to come up after x86 power cycle using "init 6" on blade
CSCvk26697	bcm_usd_log core files detected with 92.4.1.2889 image
CSCvn57429	Ftd app-instance is stuck in install failed with INSTALL_ERROR. Application internal script Error.
CSCvo03589	App agent heart beat can miss in MI scenario
CSCvo30356	Port-channels are in suspended state after upgrade
CSCvo55237	The global upgrade button is grayed out even though one security module is up
CSCvo55809	ASA App stuck in installing sate on 2.6.1.112 + ASA 9.12.0.125
CSCvo58998	FXOS Cruz Adapter doesn't validate data sent by logical device causing dropped offloaded packets
CSCvo60117	Interface not associated to MI instance even though it shows in chassis manager as allocated
CSCvo74625	6.4.0 - IPv6 routing doesn't work for WM and KP when mgmt gateway configure as data-interfaces
CSCvo83802	Cluster node management connectivity lost after reboot
CSCvp10674	FTD may not become online after installing vDP and upgrading FXOS to version 2.4.1

Identifier	Description
CSCvp44939	ASA app stuck in installing with error 'SMA_blade_reboot_inprogress' on 2.6.1.157 + 9.12.1.111

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 Firepower 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.