

EFOS 3.4.4

Build Version 3.4.4.4 Release Notes

Release Date: 27 Mar 2020

Contents

1	Overview	2
2	Deliverables	2
	New Features in EFOS 3.4.4.4	2
	Changed Security Functionality in EFOS 3.4.4.4	3
	Defect Fixes in 3.4.4.4	3
	1. Unable to provide reliable link through MWDM connection (CS9354319)	3
	2. Persistent logs no retained after reboot	4
	3. Unable to login to DUT via RESTful API using HTTPS	4
	4. Two switches reset at exactly the same time (CS9579396)	4
	5. Internal Security fixes	4
	6. Internal Bug fixes	5
3	Items Not Included in Delivery	5
4	Platform Support	5
5	Known Limitations	5
6	Known Issues in EFOS 3.4.4.4	5

1 Overview

EFOS 3.4.4.4 supports switching and routing for datacenter deployments.

2 Deliverables

Date of Delivery

EFOS release 3.4.4.4 delivered on 27 March 2020

Distribution Method

EFOS 3.4.4.4 distributed via the Broadcom [Box](#) site

Items included in delivery

Following are the items included in this delivery:

New Features in EFOS 3.4.4.4

- Password lockout feature is enabled by default. The "passwords lock-out" command currently has a default of 0 (no lockout) - this is changed to 3.
- Enable password complexity

Default Password complexity has the follow requirement:

- Minimum Uppercase letters 2
 - Minimum Lowercase letters 2
 - Minimum Numeric characters 2
 - Minimum special characters 2
 - Maximum consecutive characters 0
 - Maximum repeated characters 0
 - Minimum character classes 4
-
- By default, password aging is disabled
 - Force a password change on first login to the switch - SB-327 Information privacy: connected devices

- CA Privacy Law: Telnet/ssh stay on the mandatory change password page. Closing the telnet/ssh session will not cause DUT be inaccessible
- Support Password recovery. An option provided for "Password Recovery Procedure" under the boot menu options. This will allow the switch to boot one time without prompting for a console password
- Add privilege-15 users to default user group, allows unlock of other users
- Ensure all commands are logged when command logging is enabled
- Enable digital signing for image download by default
- Added support for malicious code detection during image upgrade. Starting from the EFOS-3.4.4.4 version, users will now be required to use an officially signed EFOS STK image to upgrade or downgrade code version on the switch. The signed EFOS STK image is provided as a deliverable as part of the EFOS release package.
- GPL License banner displayed during system boot.

Changed Security Functionality in EFOS 3.4.4.4

- Disable unsecured open ports (telnet, http)
- Support Externally/CA signed certificates for TLS communication. Allow the creation of CSR
- Disable SSLv3, TLS1.0, TLS 1.1. Only TLS1.2 should be enabled by default
- No passwords or private keys will be part of the factory default image
- Use only NIST-SP-800 131a(latest revision) supported cryptographic algorithms and ciphers for TLS, SSH communication
- RSA key pair generation default 2048 bit key size
- Disable root password in /etc/passwd
- Disable Dying gasp feature
- Disable HTTP unsecure mode and enable HTTPS
- Enable persistent logging by default
- Enable authorization features
- Disable the 'publickey-image' download option
- The public key is packaged in root file system
- Public Key authentication and CSR CLI support has been added
- "Certificate Present" is showing as "False" when "ip http secure-server" is enabled with certificate2. When we repeat the same with certificate1 then it is showing as "True".

Defect Fixes in 3.4.4.4

1. Unable to provide reliable link through MWDM connection (CS9354319)

Unreliable LOS bit enabled in the PHY for 10Gb optical connections.

EFOS Release Notes

2. Persistent logs no retained after reboot

Corrected CLI command to fully engage persistent logging

3. Unable to login to DUT via RESTful API using HTTPS

Corrected SSL to validate IP addresses when using HTTPS

4. Two switches reset at exactly the same time (CS9579396)

Corrected a problem when jumbo packets ingress the service port.

5. Internal Security fixes

- Fix for IP SSH public key authentication config is not retaining after save and reload.ssh: enable password can be exposed if ssh client includes a remote command
- "no passwords strength-check" config is not showing in running-config and functionality is not working.
- Unable to delete RSA SSH key using no-form of the command.
- Fix for IP SSH public key authentication config is not retaining after save and reload.
- Fix for "IP SSH public key authentication with DSA key config is not applying completely in running-config which results in authentication failure."
- Fix for "Active certificate" status in "show ip http" is showing as 1 even after deleting certificate-1.
- "Certificate Present" is showing as "False" when "ip http secure-server" is enabled with certificate2. When we repeat the same with certificate1 then it is showing as "True".
- Fix for "Wrong CLI help test for - 'crypto certificate 1 ?' import field." Fix for "IP SSH public key authentication with DSA key config is not applying completely in running-config which results in authentication failure."
- Fix for "Active certificate" status in "show ip http" is showing as 1 even after deleting certificate-1.
- Fix for "no passwords lock-out" not working
- Fix for "Default user's, non-default password is not retained after save and reload."
- Fix for "A level-15 user when added with password as new line command not added to default user group"
- Fix for "Password lockout should not apply to serial port"
- Fix for "linuxsh" CLI command is accessible for guest user (privilege level 1). This can create a scenario where guest user can get access to Linux shell and make changes to configuration.

6. Internal Bug fixes

- MIB walk operation is unsuccessful with "agentDigitalSignatureVerifyMode" and "agentTransferDownloadDigitalSignatureVerifySelect" mibs.
- Mac address display error in "show authentication clients" command

3 Items Not Included in Delivery

The following items are specifically not included in this delivery and will be considered for future deliveries:

- Nothing Applicable

4 Platform Support

This release contains support for the following platforms:

- Quanta BES-53248

5 Known Limitations

- No known limitations

6 Known Issues in EFOS 3.4.4.4

- No known issues