EFOS 3.4.4

Build Version 3.4.4.2 Release Notes

Release Date: 20 Dec 2019

**Contents**

[1 Overview 2](#_Toc27635660)

[2 Deliverables 2](#_Toc27635661)

[New Features in EFOS 3.4.4.2 2](#_Toc27635662)

[1. Compliance with **SB-327 Information privacy: connected devices** 2](#_Toc27635663)

[2. OpenSSH 3](#_Toc27635664)

[3. OpenSSL 3](#_Toc27635665)

[4. Support for Public Key Authentication. (CS6750088) 3](#_Toc27635666)

[5. "interactive ssh" and "scp" command support requirement for CSHM log collection (CSCS7712744) 3](#_Toc27635667)

[Defect Fixes in 3.4.4.2 6](#_Toc27635668)

[1. Need 'show fiber-ports optical transceiver-info all' for link length on various speed for DAC (CS7421550) 6](#_Toc27635669)

[2. Insert 10G SFP+, port does not link up as speed is still set to 25G if 25G was inserted (CS7621986) 6](#_Toc27635670)

[3. Switch is showing as Router instead of Switch in EFOS (CS8051566) 6](#_Toc27635671)

[4. "show interface fec" Needs to display actual FEC configured in on 25G/100G ports (CS7971646) 6](#_Toc27635672)

[3 Items Not Included in Delivery 7](#_Toc27635673)

[4 Platform Support 7](#_Toc27635674)

[5 Known Limitations 7](#_Toc27635675)

[6 Known Issues in EFOS 3.4.4.2 7](#_Toc27635676)

# Overview

EFOS 3.4.4.2 supports switching and routing for datacenter deployments.

# Deliverables

**Date of Delivery**

EFOS release 3.4.4.2 delivered on 20 Dec 2019

**Distribution Method**

EFOS 3.4.4.2 distributed via the Broadcom [Box](https://www.box.com/home) site

**Items included in delivery**

Following are the items included in this delivery:

### New Features in EFOS 3.4.4.2

#### Compliance with **SB-327 Information privacy: connected devices**

The requirement to change the default password applies at first power on or after factory reset, clear config, or any other mechanism that deletes/replaces the startup config file.

User Authentication through CLI

* User would be asked to change the password if CLI is logged in with default  
  password for any pre-configured user
* Once user changes password to a different one, user would be logged-out and  
  would be required to re-login with the changed password.
* At no time, user would be able to reset the password to the factory default  
  password again.
* On factory-reset, clear config and/or any other mechanism which deletes/replaces the start-up config file, the password for default user can get changed to factory-default password. The default user(s) would be asked to change the password  
  again before accessing CLI

**Note:** This is applicable to CLI session created to the switch by any means. That is session created over Console, Telnet or SSH.

#### OpenSSH

Upgraded to version 8.0p1

#### OpenSSL

Upgraded to version 1.1.1d

#### Support for Public Key Authentication. (CS6750088)

New cli command to enable/disable pub-key auth support.

* + - ip ssh pubkey-auth

New cli command for configuration of ssh client public keys.

* crypto key pubkey-chain ssh user-key <user-name> rsa|dsa

Modified show commands to display pubkey-auth info

* show ip ssh" and "show running-config" commands modified to display the public key authentication state

#### "interactive ssh" and "scp" command support requirement for CSHM log collection (CSCS7712744)

This adds support for "interactive ssh" that allows a remote client to send commands to the switch and receive the output on the client. By using an ssh public/private keypair a user external to the switch can authenticate via key exchange rather than a password.

Feature Functionality

This is an example of how this feature can be used:

Some commands must be run on the switch to configure ssh handling and some commands are needed on the client to generate the ssh public/private key pair and then install the public key on the switch.

* 1. On the Linux host generate the public/private keypair. There are many options to control how the keys are generated. The following command will generate a 2048 bit RSA key.  
     ssh-keygen -t rsa -b 2048  
       
     (Localhost):~$ ssh-keygen -t rsa -b 2048  
     Generating public/private rsa key pair.  
     Enter file in which to save the key (/home/(user)/.ssh/id\_rsa):          
     /home/(user)/.ssh/id\_rsa already exists.  
     Overwrite (y/n)? y  
     Enter passphrase (empty for no passphrase):  
     Enter same passphrase again:  
     Your identification has been saved in /home/(user)/.ssh/id\_rsa.  
     Your public key has been saved in /home/(user)/.ssh/id\_rsa.pub.  
     The key fingerprint is:  
     c5:05:66:38:79:5c:d8:16:08:27:2d:2d:2c:e1:c8:31 [(user)@i06-35](mailto:whaley@i06-35)  
     The key's randomart image is:  
     +--[ RSA 2048]----+  
     |    E .ooB=\*+.   |  
     |   . =. B\*B.o    |  
     |    o .. =o.     |  
     |         .       |  
     |        S        |  
     |                 |  
     |                 |  
     |                 |  
     |                 |  
     +-----------------+  
       
     This generates the public and private key pair and puts the files in "/home/(user)/.ssh/" where the username is the name of the Linux user.
  2. Make sure the switch has the rsa/dsa keys configured and the ssh/scp services configured.

config

(Config)#crypto key generate rsa

(Config)#crypto key generate dsa

exit  
ip ssh server enable  
ip ssh pubkey-auth  
ip scp server enable

Verify ip ssh config:

(Routing) #show ip ssh  
  
SSH Configuration  
  
Administrative Mode: .......................... Enabled  
SSH Port: ..................................... 22  
Protocol Level: ............................... Version 2  
SSH Sessions Currently Active: ................ 0  
Max SSH Sessions Allowed: ..................... 5  
SSH Timeout (mins): ........................... 5  
Keys Present: ................................. DSA RSA  
Key Generation In Progress: ................... None  
SSH Public Key Authentication Mode: ........... Enabled  
SCP server Administrative Mode: ............... Enabled

* 1. Copy the public key that was generated on the Linux client to the switch so it can be used for a specific login user. In this case we copy the public key created in .ssh/id\_rsa.pub to the switch as toaster.pub

(user)@i06-35:~$ scp .ssh/id\_rsa.pub [admin@10.27.21.251](mailto:admin@10.27.21.251):toaster.pub  
The authenticity of host '10.27.21.251 (10.27.21.251)' can't be established.  
RSA key fingerprint is f7:aa:e5:d4:d3:d7:f8:85:5f:7a:95:57:58:2b:6e:dd.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '10.27.21.251' (RSA) to the list of known hosts.  
[admin@10.27.21.251](mailto:admin@10.27.21.251)'s password:  
id\_rsa.pub   100%  395     0.4KB/s   00:00    

* 1. With the public key installed on the switch, configure the switch with the username toaster and the pointer to the public key.

username "toaster" password b683136794424d2c1ef0267fdbaad01d43ab9b6959973a13f92e847f7f2fb2cd7ca0ad09ce82dc0b41b53262ddebd87fcafcb97f20d0b81a322ba4d078e79c7b level 15 encrypted  
username "toaster" sshkey file toaster.pub

* 1. To allow commands to be executed from the client, make sure the aaa parameters are set and applied to the ssh configuration.

aaa authorization commands "noCmdAuthList" noneline ssh  
authorization commands noCmdAuthList  
exit

* 1. Test the connection with a simple command like show version

[(user)@i06-35](mailto:(user)@i06-35):~$ ssh [toaster@10.27.21.251](mailto:toaster@10.27.21.251) "show version"  
  
Switch: 1  
  
System Description............................. x86\_64-quanta\_common\_rglbmc-r0, 3.4.4.2, Linux 4.4.117-ceeeb99d, 2016.05.00.04  
Machine Type................................... x86\_64-quanta\_common\_rglbmc-r0  
Machine Model.................................. BES-53248  
Serial Number.................................. QTFCU39030018  
Maintenance Level.............................. A  
Manufacturer................................... 0xbc00  
Burned In MAC Address.......................... D8:C4:97:A5:7C:E8  
Software Version............................... 3.4.4.2  
Operating System............................... Linux 4.4.117-ceeeb99d  
Network Processing Device...................... BCM56873\_A0  
CPLD version................................... 0xff040c03  
Additional Packages............................ BGP-4  
                                                QOS  
                                                Multicast  
                                                IPv6  
                                                Routing  
                                                Data Center  
                                                OpEN API  
                                                Prototype Open API

### Defect Fixes in 3.4.4.2

#### Need 'show fiber-ports optical transceiver-info all' for link length on various speed for DAC (CS7421550)

CLI code was modified for "show fiber-ports optical-transceiver-info all" cmd to get the link length based on inserted module

#### Insert 10G SFP+, port does not link up as speed is still set to 25G if 25G was inserted (CS7621986)

Corrected dynamic programming for SFP transceivers

#### Switch is showing as Router instead of Switch in EFOS (CS8051566)

Added "S” to the isdp capability along with “R”

dhcp-10-52-130-50)#show isdp neighbors

Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge,

S - Switch, H - Host, I - IGMP, r - Repeater

Device ID Intf Holdtime Capability Platform Port ID

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

Localhost 0/13 151 R S Questone+ 0/7

#### "show interface fec" Needs to display actual FEC configured in on 25G/100G ports (CS7971646)

Sample:

(localhost) #show interface fec

Intf Configured Physical

FEC Mode FEC Status

--------- ------------- -------------  
0/1 Auto Not Available  
0/2 Auto Not Available  
...  
0/53 FEC 100G CL91  
0/54 FEC 100G CL91  
0/*55* FEC 100G CL91

# Items Not Included in Delivery

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

* Nothing Applicable

# Platform Support

This release contains support for the following platforms:

* Quanta BES-53248

# Known Limitations

* No known limitations

# Known Issues in EFOS 3.4.4.2

* No known issues