Fabric OS v9.2.0c/v9.2.0c1/v9.2.0c2/v9.2.0c3/v9.2.0c4/v9.2.0c5

Fabric OS v9.2.0c Release Notes Digest

Version 8.0

Broadcom reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom is believed to be accurate and reliable. However, Broadcom does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights nor the rights of others.

The product described by this document may contain open source software covered by the GNU General Public License or other open source license agreements. To find out which open source software is included in Brocade products or to view the licensing terms applicable to the open source software, please download the open source attribution disclosure document in the Broadcom Support Portal. If you do not have a support account or are unable to log in, please contact your support provider for this information.

Use of all versions of Brocade’s Fabric OS is subject to the terms and conditions of the Brocade Fabric Operating System and Feature Licenses and License Keys End User License Agreement, effective October 1, 2019, as amended by Brocade from time to time. It is the user’s responsibility to understand and comply with the terms of the EULA. By downloading, installing, using, posting, distributing or otherwise making available FOS, you agree to be bound on an ongoing basis by the EULA as updated by Brocade from time to time.

Table of Contents

Chapter 1: Preface

1.1 Contacting Technical Support for your Brocade® Product

If you purchased Brocade product support directly from Broadcom, use one of the following methods to contact the Technical Assistance Center 24x7. For product support information and the latest information on contacting the Technical Assistance Center, go to www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

Online	Telephone
For nonurgent issues, the preferred method is to log on to the Support portal at support.broadcom.com. (You must initially register to gain access to the Support portal.) Once registered, log on and then select **Brocade Products**. You can now navigate to the following sites: ▪ **Case Management** ▪ **Software Downloads** ▪ **Licensing** ▪ **SAN Reports** ▪ **Brocade Support Link** ▪ **Training & Education**	For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at www.broadcom.com/support/fibre-channel-networking/contact-brocade-support.

If you purchased Brocade product support from a Broadcom OEM/solution provider, contact your OEM/solution provider for all your product support needs.

- OEM/solution providers are trained and certified by Broadcom to support Brocade products.
- Broadcom provides backline support for issues that cannot be resolved by the OEM/solution provider.
- Brocade Supplemental Support augments your existing OEM support contract, providing direct access to Brocade expertise. For more information on this option, contact Broadcom or your OEM.

For questions regarding service levels and response times, contact your OEM/solution provider.

To expedite your call, have the following information immediately available:

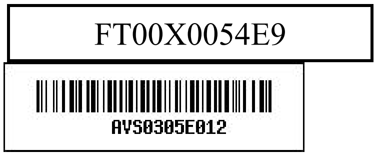
General Information:

- Technical support contract number, if applicable.
- Switch model.
- Switch operating system version.
- Error numbers and messages received.
- **`supportSave`** command output and associated files.

  For dual-CP platforms the **`supportSave`** command gathers information from both CPs and any AP blades installed in the chassis.
- Detailed description of the problem, including the switch or fabric behavior immediately following the problem and any specific questions.
- Description of any troubleshooting steps already performed and the results.
- Serial console and telnet session logs.
- Syslog message logs.

- Switch Serial Number.

  The switch serial number is provided on the serial number label, examples of which follow:

  The serial number label is located as follows:

  – Brocade G630, G620, G610, G720, and G730 – On the switch ID pull-out tab located on the bottom of the port side of the switch.

  – Brocade 7810 and 7850 – On the pull-out tab on the front left side of the chassis underneath the serial console and Ethernet connection and on the bottom of the switch as well as on the left side underneath (looking from the front).

  – Brocade X6-8, X6-4, X7-8, and X7-4 – Lower portion of the chassis on the non-port side beneath the fan assemblies.

- World Wide Name (WWN).

  When the Virtual Fabric feature is enabled on a switch, each logical switch has a unique switch WWN. Use the **`wwn`** command to display the switch WWN.

  If you cannot use the **`wwn`** command because the switch is inoperable, you can get the primary WWN from the same place as the serial number.

- License Identifier (License ID).

  There is only one license ID associated with a physical switch or director/backbone chassis. This license ID is required as part of the ordering process for new FOS licenses.

  Use the **`license --show -lid`** command to display the license ID.

1.2 Related Documentation

White papers, data sheets are available at www.broadcom.com. Product documentation for all supported releases is available on the support portal to registered users. Registered users can also find release notes on the support portal.

Chapter 2: Locating Product Manuals and Release Notes

The following sections outline how to locate and download Brocade product manuals and release notes from Broadcom and the support portal. Although the illustrations show Fibre Channel and Fabric OS (FOS), they work for all Brocade products and operating systems.

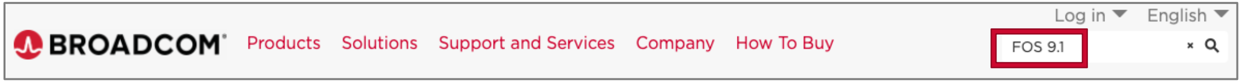
2.1 Locating Product Manuals and Release Notes

2.1.1 Locating Product Manuals on Broadcom

Complete the following steps to locate your product manuals on Broadcom.com.

1. Go to www.broadcom.com.
2. Enter the product name or the software version number in the **Search** box.

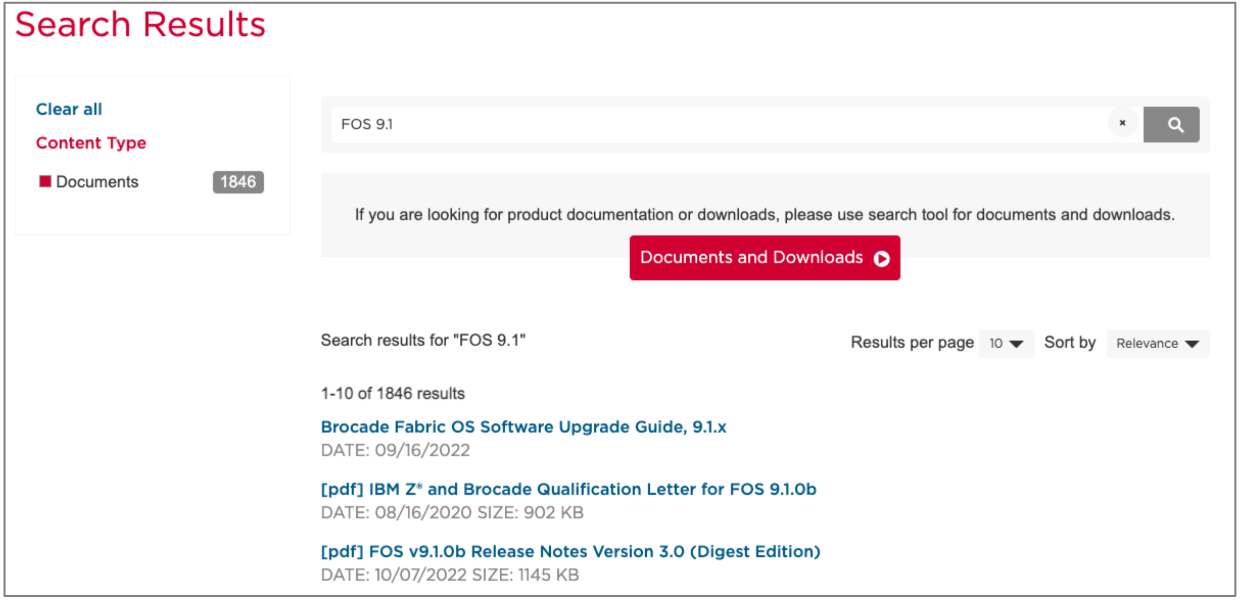
   For example, the following search is for software and documentation files for software version v9.1.



FOS 9.1

3. Select the **Documents** check box to list only the documents.

   The list of documents available for the release displays.



Search Results

Clear all

Content Type

■ Documents 1846

FOS 9.1

If you are looking for product documentation or downloads, please use search tool for documents and downloads.

Documents and Downloads

Search results for "FOS 9.1"

Results per page 10 Sort by Relevance

1-10 of 1846 results

Brocade Fabric OS Software Upgrade Guide, 9.1.x
DATE: 09/16/2022

[pdf] IBM Z® and Brocade Qualification Letter for FOS 9.1.0b
DATE: 08/16/2020 SIZE: 902 KB

[pdf] FOS v9.1.0b Release Notes Version 3.0 (Digest Edition)
DATE: 10/07/2022 SIZE: 1145 KB

2.1.2 Locating Product Manuals and Release Notes on the Support Portal

Complete the following steps to locate your product manuals on the support portal.

1. Go to support.broadcom.com/, click **Login**, and enter your username and password.

   If you do not have an account, click **Register** to set up your account.
2. Select **Brocade Storage Networking** in the support portal.

2.2 Document Feedback

Quality is our first concern and we have made every effort to ensure the accuracy and completeness of this document. If you find an error, omission or think that a topic needs further development, we want to hear from you. You can provide feedback by sending an email to documentation.PDL@broadcom.com. Provide the publication title, publication number, and as much detail as possible, including the topic heading and page number, as well as your suggestions for improvement.

Chapter 3: Overview

The Fabric OS v9.2.0c/v9.2.0c1/v9.2.0c2/v9.2.0c3/v9.2.0c4/v9.2.0c5 is a patch release based on FOS v9.2.0b/v9.2.0b1.

This release supports all hardware platforms and features in FOS v9.2.0 through FOS v9.2.0c/v9.2.0c1/v9.2.0c2/v9.2.0c3/v9.2.0c4/v9.2.0c5.

Fabric OS v9.2.0c/v9.2.0c1/v9.2.0c2/v9.2.0c3/9.2.0c4/v9.2.0c5 includes software enhancements and defect fixes.

NOTE The v9.2.0c1 patch provides a critical defect fix for the issue described by TSB-2024-293-A.

NOTE The v9.2.0c4 patch provides a critical defect fix to recognize the OUI B8:CE:ED introduced with newer switches.

NOTE The v9.2.0c5 patch provides a critical defect fix for the issue described by TSB-2025-295-A.

Fabric OS v9.2.0c3 includes support for the optic PN: 57-1000486-01 (32G LWL) with serial number prefix JDB.

For the following platforms:

- Brocade G730
- Brocade G630
- Brocade G610
- Brocade G648
- Brocade MXG610S
- Brocade 7810 Extension Switch
- Brocade FC64-64
- Brocade FC32-48

Chapter 4: What is New in FOS v9.2.0c5

The FOS v9.2.0c5 patch includes resolution for important defects and security fixes.

4.1.1 Resolution of Important Defects

The following important defects are resolved in FOS v9.2.0c5:

FOS-871546 - Excessive link errors reported, followed by a switch fault or a blade fault within a director.

FOS-872941 - The MXG610 is repeatedly panicking when a QSFP is installed and running a later version of FOS.

FOS-873148 - Multiple SFPs in the same port group report “Mod-Val” state at the same time.

FOS-873602 - Multiple SFPDDs/SFPs in the same port group report “Mod-Val” state at the same time.

FOS-873503 - Unable to launch webtools in SCG environment.

Chapter 5: What is New in FOS v9.2.0c4

The FOS v9.2.0c4 patch provides resolution for important

5.1.1 Resolution of Important Defects

The following important defects are resolved in FOS v9.2.0c4:

FOS-871910 - Access Gateway (AG) and Fibre Channel Routing (FCR) will not function in a fabric that includes a Brocade switch assigned with the new OUI (B8-CE-ED).

Chapter 6: What is New in FOS v9.2.0c3

The FOS v9.2.0c3 patch provides support for the optic PN: 57-1000486-01 (32G LWL) with serial number prefix JDB.

For the following platforms:

- Brocade G730
- Brocade G630
- Brocade G610
- Brocade G648
- Brocade MXG610S
- Brocade 7810 Extension Switch
- Brocade FC64-64
- Brocade FC32-48

The optic is already supported with Fabric OS release v9.2.0c2 for the following platforms:

- Brocade SX6 Extension Blade
- Brocade 7850 Extension Switch

The optic is already supported (with prior FOS releases, v9.1.1a, v9.2.0, and higher) on the following platforms:

- Brocade FC64-48
- Brocade FC32-X7-48
- Brocade G720
- Brocade G620

6.1 Software

The following lists the software changes with this release:

- Behavioral change for MAPS SNMP trap forwarding to SANnav 2.4.0 (and later), when MAPS Quiet Time is configured or MAPS Action is not configured for MAPS SNMP trap forwarding.

  The change is described in more detail in the MAPS section under Important Notes.

6.1.1 Resolution of Important Defects

The following important defects are resolved in FOS v9.2.0c3:

- FOS-863077 – The weblinker daemon memory usage continues to increase during SANnav monitoring and activities such as configupload start to fail.
- FOS-833439 – The device file /dev/mtd2 is not being created and cannot be accessed by management application.

Chapter 7: What is New in FOS v9.2.0c2

The FOS v9.2.0c2 patch provides support for the optic PN: 57-1000486-01 (32G LWL) with serial number prefix JDB.

For the following platforms:

- Brocade SX6 Extension Blade
- Brocade 7850 Extension Switch

The optic is already supported (with prior FOS releases, v9.1.1a, v9.2.0, and higher) on the following platforms:

- Brocade FC64-48
- Brocade FC32-X7-48
- Brocade G720
- Brocade G620

There are no other changes in the FOS v9.2.0c2 patch.

Chapter 8: What is New in FOS v9.2.0c1

The v9.2.0c1 patch provides a critical defect fix for the issue described by **TSB-2024-293-A**.

8.1.1 Resolution of Important Defects

The following important defects are resolved in FOS v9.2.0c1:

- FOS-862863 – Hard zoning incorrectly enabled on FICON enabled switch with no zoning defined. All traffic will be blocked by the zoning checks.

Chapter 9: What is New in FOS v9.2.0c

9.1 New Optics Support

The following optics are supported in FOS v9.2.0c on the FC64-64 port blade

- 32G FC SFP+ SWL XBR-000412

9.2 Software

The following lists the software changes with this release.

- Optimized credit model for credit stall and over subscription flows on G630 and X7-8/4.
  - Described in detail in

- Optimized Credit Model for G630 and X7-8/4.

9.2.1 Resolution of Important Defects

The following important defects are resolved in FOS v9.2.0c:

- FOS-855788 – Maps daemon (mdd) terminates during supportsave
- FOS-857454 – Restartable daemons such as mdd, cald, snmp etc terminate and could not be restarted properly, causing HA out of sync and daemons are left in a defunct state.
- FOS-858851 – User experience performance issue on Gen7 after code upgrade
- FOS-860632 – Standby CP in RRD state and/or SX6 blades are faulted during code upgrade. inetd on active CP no longer listens on port 514 on ipaddress of 127.3.1.x
- FOS-860855 – Supportsaves are failing collecting switch SS using SANnav

Chapter 10: What is New in FOS v9.2.0b

10.1 New Hardware

There is no new hardware supported with FOS v9.2.0b

10.2 Software

The following lists the software changes with this release.

10.2.1 Resolution of Important Defects

The following important defects are resolved in FOS v9.2.0b:

- FOS-851223 – Switch ran out of kernel memory and triggered deamon panic, cpu busy or port/blade fault
- FOS-853249 - cald process aborted due to memory resource not available
- FOS-854143 - Kernel panic when 64G oversubscription is introduced in the fabric with many neighbors on the same chip
- FOS-850131 - Configupload doesn't fail even when the server side file path is non existent

Chapter 11: What is New in FOS v9.2.0a

11.1 New Hardware

There is no new hardware supported with FOS v9.2.0a

11.2 Software

The following lists the software changes with this release.

11.2.1 Resolution of Important Defects

The following important defects are resolved in FOS v9.2.0a:

- FOS-849642 - Switch reported a flood of hardware errors, followed by daemons watchdog timeout and switch reboot.
- FOS-847091 - Repeat software 'verify' errors detected on X7 directors running FOS 9.1.x. Also, possible to see daemons crash due to watchdog timeout if congestion / oversubscription is severe.
- FOS-849852 - G610 fails to boot after power outage with reason "ERROR: can't get kernel image!"

For a full list of closed defects in this release, see Defects.

11.2.2 Enhancements

FOS v9.2.0a includes the following enhancements, described in more detail below:

- System Security
  - AAA configuration with RSA SecurID is enhanced:
    - Multi-factor authentication on RSA SecurID extended to support REST API over HTTPS
    - Support Multi Factor Authentication using PIN+OTP
    - Map RSA users to FOS roles

11.2.2.1 AAA Configuration with RSA SecurID

RSA SecurID provides the facility to verify the identity of users using MFA. Users provide a passcode which is a combination of PIN and OTP to get their identity verified. FOS supports this mechanism to provide MFA login for users accessing FOS platforms.

To use the RSA SecurID Authentication Manager for user authentication the following steps must be performed in FOS:

- RSA server configuration (`aaaconfig`).
- Role configuration for the RSA user(s) (`aaaconfig --autherconf`) to map RSA user(s) to FOS roles.
- RSA server CA certificate needs to be imported on the switch (`seccertmgmt`)
  - (RSA certificates are monitored by MAPS)

The default crypto configurations must be updated (`seccryptocfg`)

NOTE Token policy in the RSA Authentication manager for wrong passcode limit reached, requiring the user input the next token in rotation in order to clear the Next Token Required state is not supported by FOS. In this state the user will be required to reach out to the administration of the RSA Authentication Manager to clear and return the value to Active.

Chapter 12: What is New in FOS v9.2.0

The Fabric OS v9.2.0 release includes both support for new hardware, new software features and enhancements of existing, with the main areas listed below and covered in more detail in the respective sections and chapters.

12.1 New Hardware

Fabric OS v9.2.0 is the first release supporting the following new hardware:

- Brocade 7850 Extension Switch
- Brocade FC64-64 High Density blade

12.1.1 Platforms

In addition to the new hardware support, FOS v9.2.0 also supports the same Brocade Gen 6 and Gen 7 Fibre Channel platforms supported in FOS v9.1.0x.

12.1.2 New Optical Transceivers

FOS v9.2.0 adds support for the following optical transceivers:

Speed	Type	Manufacturing PN	Product PN
100GbE	SR4 QSFP	57-1000508-01	XBR-100G-SR4-01
25GbE (25/10)	SR SFP	57-1000505-01	XBR-25G-SR-01
25GbE (25/10)	LR SFP	57-1000504-01	XBR-25G-LR-01
10GbE (10/1)	SR SFP	57-1000507-01	XBR-10G-SR-01

12.2 New and Modified Software Features

- System Security
  - Chassis Admin role assignment
  - Default Secure by design
  - OpenSSL upgrade
  - RBAC Default deny
  - OU no longer accepted for TLS/SSL certificates
  - Maximum number of login sessions for specific accounts
  - CyberArk support
- MAPS and Fabric Performance Impact
  - Monitoring the chassis-wide zone database usage
  - Enhanced system memory monitoring
  - Always Active system policy
  - SDDQ REST enhancement
  - Port name details in MAPS alerts
  - N-Ports are removed from the NON_E_F_PORTS group

  - Extension certificates monitoring
  - MAPS actions on FCIP circuits
  - Adaptive MAPS notifications
  - FPI alerts to include latency/congestion time
- Traffic Optimizer (TO)
  - Custom profile support
- Extension
  - TO support on FCIP
  - New and modified commands
- Flow Vision
  - Real-time IO violations
  - VMID+ supported with XISLs
- Fabric Infrastructure
  - Firmware download check for free space
  - Firmware patch
- FCR
  - REST Enhancements: brocade-fibrechannel-logical-switch
  - fcrxlateconfig --show stalexd gives RBAC Permission denied while running via fosexec remote domain
- Miscellaneous
  - Signal Loss metric from dBm to dB in sfpshow -link output
  - CLI command Usage/Help menu changes in FOS v9.2.0
  - Chassisshow displays HW version
  - OUI list updated with new UCS FI modules
  - Microsoft Windows Server, NPS, LDAP and Global Catalog
  - Clear-Link Diagnostics
  - SNMP MIB Include objects for SFP PN and SN
- Web Tools
  - Dark mode
  - Title bar displays
  - AAA page displays
  - Syslog panel
  - Display warning
  - RBAC enforcement
  - AG port mapping
- REST API
  - CamelCase support
  - API changes

12.2.1 System Security Enhancements

Fabric OS System Security provides functionalities such as User Management, Cryptography Management, Certificate Management, Firewall (IP Filter) and other miscellaneous features. Role Based Access Control (RBAC), Authenticated access to the switch, Fabric, and management interface (Ethernet) modules ensure that the integrity of the switch is upheld in terms of access, authentication, and handling vulnerabilities

FOS v9.2.0 supports the following system security enhancements:

- Chassis Admin role assignment
- Default Secure by design
- OpenSSL upgrade
- RBAC Default deny
- OU no longer accepted when generating CSR for TLS/SSL certificates
- Max number of login sessions for specific accounts
- CyberArk support

12.2.1.1 Chassis Admin Role Assignment

Prior to FOS v9.2.0, when the switch is configured with VF enabled and default admin account is disabled, the chassis admin roles are not automatically assigned to non-default accounts with admin roles.

As a result, when maintenance and default admin accounts were disabled on a switch in non-VF mode, the non-default admin accounts would not be able to execute commands requiring ‘chassis admin’ privilege after enabling virtual fabrics as all other locally configured user accounts would not be assigned chassis admin role permissions. Although they had admin roles while VF was disabled, these local non-default users would not inherit the chassis admin role. The role can only be added to user accounts by an account with chassis admin privilege, but because default user accounts are disabled, there is no account with chassis admin permission available anymore.

From FOS v9.2.0, when VF is enabled and default admin account is disabled, the chassis admin roles are automatically assigned to all non-default accounts with admin roles.

This assignment will not be undone when VF is disabled.

12.2.1.1.1 New/Modified/Deprecated CLI Commands

```
Switch:AdminUser> fosconfig --enable vf
WARNING:  This is a disruptive operation that requires a reboot to take effect.
All EX ports will be disabled upon reboot.
Enabling VF will cause other non-default admin accounts to gain chassis admin role
permissions if default admin account is disabled.
Would you like to continue [Y/N]:
```

12.2.1.1.2 Fabric OS Compatibility

No impact on firmware upgrade/downgrade from FOS v9.2.0 -all admin users will continue to have chassis admin role.

12.2.1.2 Default Secure by Design

Switches shipping with FOS v9.2.0 are configured with Default Secure (DS) settings.

Switches upgrading from pre-FOS v9.2.0 to FOS v9.2.0 keep the already configured settings, while a new command (`factoryreset -set securitydefault`) is available to explicitly set Default Secure configuration settings for FOS.

In addition, the existing feature for configuring a single TLS protocol version or all supported versions is enhanced to also support configuring the range of protocol versions with enhancements to the command `seccryptocfg`.

The Default Secure Configuration Settings Include:

- Disable SNMPv1 and SNMPv2; SNMP password encryption is enabled.
- Modify the default ipfilter policies (default_ipv4 and default_ipv6) for rule 2 and 3 to block the Telnet and HTTP ports. Delete all the custom ipfilter policies if they exist.
  - Non-secure protocols, including FTP, are all disabled under secure settings.
- Configure crypto configurations like ciphers, protocol version to default strong configuration. This is similar to applying the default strong security template.
- Modify the password policy to enable `adminlockout` and `adminlockoutconsoleaccess`; set the default lockout duration to 5 minutes and password hashing to sha512.

NOTE The command `adminlockoutconsoleaccess` was implemented in FOS v9.1.1a and when set provides separate lockout control for console access apart from the switch IP management interface.

- Regenerate SSH host keys with key-size of 2048 for RSA and curve of P521 for ECDSA (Existing SSH keys (host keys and pub key authentication keys) will be deleted).
- Existing TLS certificates and associated keys/CSRs will be deleted
- Configure SSH rekey, with rekey duration set to 900 seconds
- All commands which perform file transfer to/from FOS are only allowed with secure protocols
- Non-secure Syslog, either previously configured or configured after DS is configured will fail.

NOTE If secure Syslog is configured prior to issuing the command `factoryreset -set securitydefault` it must be reconfigured as the command removes all certificates.

12.2.1.2.1 DS IP Filter

Default IP Filter Policies

With Default Secure the Default IP Filter policies *default_ipv4* and *default_ipv6* are defined with rule 2 and 3 to block the Telnet and HTTPS ports, details displayed below:

```
Name: default_ipv4, Type: ipv4, State: defined
Rule     Source IP                Protocol   Dest Port   Action
1     any                                            tcp       22                permit
2     any                                            tcp       23                deny
3     any                                            tcp       80                deny
4     any                                            tcp       443               permit
5     any                                            udp      161                permit
6     any                                            udp      123                permit
7     any                                            tcp      600 - 1023         permit
8     any                                            udp      600 - 1023         permit


Name: default_ipv6, Type: ipv6, State: defined
Rule     Source IP                 Protocol   Dest Port   Action
1     any                                            tcp       22                permit
2     any                                            tcp       23                deny
3     any                                            tcp       80                deny
4     any                                            tcp       443               permit
5     any                                            udp     161                 permit
6     any                                            udp     123                 permit
7     any                                            tcp      600-1023           permit
8     any                                            udp     600-1023            permit
```

12.2.1.2.2 DS Crypto Default Configurations

The default values for crypto configuration keys like ciphers, protocols etc., for TLS applications and SSH are modified to stronger cryptographic algorithms.

Configurations are chosen based on the recommendations from NIST and the security strength of a given cipher.

Below is the list of configuration keys and their corresponding value for secure configuration.

Key	Value
HTTPS CIPHER	ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!TLSv1:!AESCCM
HTTPS TLS1.3 CIPHER	TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_8_SHA256:TLS_AES_128_CCM_SHA256
HTTPS PROTOCOL	TLSv1.3
RADIUS CIPHER	ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!TLSv1:!AESCCM
RADIUS PROTOCOL	TLSv1.2
LDAP CIPHER	ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!TLSv1:!AESCCM
LDAP PROTOCOL	TLSv1.2
SYSLOG CIPHER	ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!TLSv1:!AESCCM
SYSLOG PROTOCOL	TLSv1.2
SSH CIPHER	aes128-ctr,aes192-ctr,aes256-ctr
SSH KEX	ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,curve25519-sha256
SSH MAC	hmac-sha2-256,hmac-sha2-512
X509 VALIDATION	Basic

12.2.1.2.3 DS Password Policy

The default password policy configurations are modified to strengthen the password security and control the login access and violations. The modified password policies are as below.

- Admin lockout, enabled by default.
- Lockout threshold will be set to 3.
- Admin lockout console access, enabled by default.

12.2.1.2.4 DS SSH Key

The Default Secure configuration will regenerate SSH host keys with key-size of 2048 for RSA and curve of P521 for ECDSA. Existing SSH keys (host keys and pub key authentication keys) will be deleted.

SSH rekey duration is set to 900 seconds.

12.2.1.2.5 DS TLS

Existing TLS certificates and associated keys/CSRs will be deleted.

NOTE The following disruptions can be expected when executing the command `factoryreset -set securitydefault` after migration to FOS v9.2.0:

- SSH connection to the switch will fail if there is mismatch in supported ciphers or will require known_hosts update on ssh client due to hostkey regeneration. Existing sessions will be terminated.
- SSH public key authentication will fail for users that were already setup.
- TLS connections (LDAP, RADIUS PEAP-MSCHAP, Syslog, HTTPS) will fail if there is mismatch (unsupported) in the configured supported ciphers or protocol versions.
- In case of TLS certificates being used, re-generation and re-signing of certificates may be required as existing certificates will be deleted.
- If any port is in permit state explicitly via an ip filter rule of the active policy and was in use for a specific application, it would stop working after the securitydefault operation. For eg: HTTP based applications on port 80, telnet on port 23 and any other ports permitted via custom IP filter policies.

12.2.1.2.6 New/Modified/Deprecated CLI Commands

Users can use the command `factoryreset -set securitydefault` to set Default Secure configuration.

Users can use the command `seccryptocfg` to set TLS protocol versions.

Users can use the command `sshutil` to generate SSH keys with varying key size strength.

Users can use the command `ipfilter --default` to activate DS default IP Filter policies and will delete all custom IP Filter policies.

Examples:

```
Switch:FID128:admin>factoryreset -set securitydefault
This command requires the daemon(s) HTTP, SSH and Syslog to be restarted.
Existing sessions will be terminated.
Please confirm and provide the preferred option
Press Yes(Y,y), No(N,n) [N]:
Switch successfully configured to secure default configurations.
```

```
secCryptoCfg
--replace -type {SSH | https} {[-cipher  < cipher string >] [-kex  <value>] [-mac
<value>]}  [-force]
Configures the provided ciphers or Kex or Mac
Change the group's attribute to value given
--default -type {https | SSH} [-force]
Delete the existing ciphers,Kex and Mac, revert to default (default if not configured)
--apply {<template_name> | -group {SSH | AAA | LOG | HTTPS | X509v3 | Compliance} -attr
<attribute> -value <value for attribute>} [-force]
```

```
sshutil genkey {-rsa[-keysize {2048|4096|8192}]|-dsa|-ecdsa[-keysize {P256|P384|P521} ]}:

sshutil genhostkey {-rsa[-keysize {2048|4096|8192}]|-dsa|-ecdsa[-keysize {P256|P384|P521}
]}:

ipfilter --default
```

12.2.1.2.7 Fabric OS Compatibility

Manageability Considerations

Default secure only allow HTTPS access to FOS and thereby will impact accessibility with SANnav and Web Tools in case HTTPS is not already used.

On Firmware Upgrade to FOS v9.2.0

All the active configurations would be retained after upgrading to FOS v9.2.0.

For IP filter policies, the active policy continues to be active after upgrade.

On Firmware Downgrade from FOS v9.2.0

All active configurations will be retained after downgrade.

12.2.1.3 OpenSSL 3.0

Prior to FOS v9.2.0, OpenSSL 1.1.1d was used for all general-purpose cryptography and secure communication. The OpenSSL Technical and Management committee has decided to stop supporting this release from September 2023, thereby requiring upgrade of OpenSSL from OpenSSL 1.1.1d to OpenSSL 3.0.

In FOS v9.2.0 all secure applications which use OpenSSL 1.1.1d will be using OpenSSL 3.0.7, such as OpenLDAP, syslog, openssh, apache, freeradius, pam and ntp.

12.2.1.3.1 Fabric OS Compatibility

There are no migration impacts due to openssl 3.0 upgrade. Applications that worked with openssl 1.1.1d in pre-FOS v9.2.0, will continue to work with FOS v9.2.0.

12.2.1.4 RBAC Default Deny

In FOS v9.2.0 any command for which the user does not have RBAC permissions to execute will be blocked in shell and RBAC error returned, as shown in the example below.

Example:

```
Switch:FID128:admin> Non-Permitted-Command
RBAC permission denied.
```

12.2.1.5 Organizational Unit Name (OU) Field from CSR and Self-Signed Certificates

Effective August 24, 2022, the OU field will no longer appear in order forms for digital certificates from public Certificate Authorities and will be ignored in API requests. In addition, the OU field will not be included in all new, renewed, and reissued public TLS/SSL certificates. This is due to a change by the CA/Browser forum, who dictates and issues guidelines to all Certificate Authority vendors. This requirement is to enhance FOS to adhere to the change proposed by CA/Browser forum.

In FOS v9.2.0 the OU field is not included when generating a CSR, nor in self-signed certificates. A warning message is displayed when an imported certificate includes OU (except for imported CA certificates, these will not generate a warning if the OU field is present).

12.2.1.5.1 New/Modified/Deprecated CLI Commands

The command `seccertmgt` is modified to not prompt for OU field (when generating CSR).

12.2.1.6 Maximum Number of Simultaneous Login Sessions

In FOS v9.2.0 the maximum number of simultaneous login sessions is increased to 12 for locally authenticated *admin* and *maintenance* users.

In FOS v9.1.x the number of simultaneous login sessions allowed for locally authenticated *admin* and *maintenance* users on FOS switches is limited to four (individually).

This change in FOS v9.2.0 will allow for a combined limit of max 12 sessions, between locally authenticated *admin* and *maintenance* users. This means that there can be at max 12 sessions shared between admin and maintenance accounts (locally authenticated) on a FOS switch. On Brocade director systems, the Active CP can have up to 12 sessions for these accounts and the Standby CP can have up to 12 sessions. These sessions can be console sessions, SSH sessions or telnet sessions.

Once this limit of 12 sessions is reached, any new *admin* and *maintenance* user session will not be allowed.

The example below illustrates the error message when the max session limit has already been reached for admin/maintenance account:

```
$ ssh -l admin 10.10.10.10
admin@10.10.10.10 password:
Max remote sessions for login:admin and login:maintenance is 12
Connection to 10.10.10.10 closed.
```

NOTE All connections to FOS across available interfaces CLI, REST, WebTools and SANnav count as sessions.

12.2.1.7 CyberArk Privileged Session Management Support

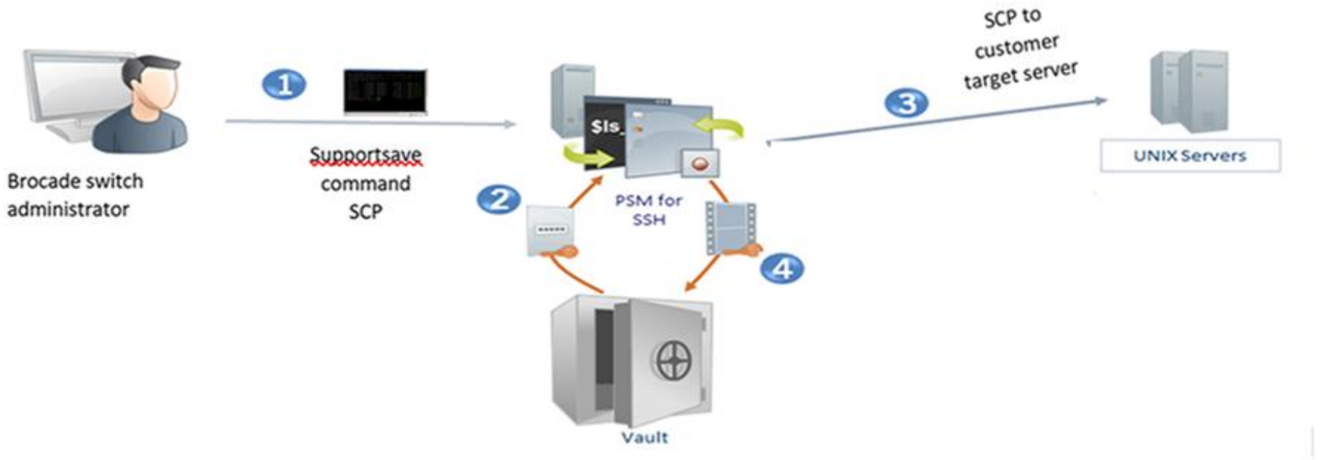
In data centers using CyberArk for Privileged Session Management (PSM), the session management when transferring files to/from a file repository is governed by CyberArk and the end user does not have credentials to access the file repository. In FOS v9.2.0 CyberArk PSM is supported for the following commands requiring file transfers:

- `Supportsave`
- `Configupload`
- `Configdownload`
- `Firmwaredownload`
- `Firmwarecleaninstall`
- `Seccertmgmt`
- `Seccryptocfg`
- `License`

CyberArk provides a vault to store passwords of users. Once the password for a user is stored in the vault, it will change the password periodically to avoid illegal access. In that case, the server can be accessed through the jump server provided by CyberArk.

The PSM is a CyberArk component that enables it to initiate, monitor, and record the sessions established to the server.

FOS users will not have credentials to access the remote repository server to transfer the files. Credentials for remote servers are stored in the Cyberark vault. In which case, the user must access the server through PSM for SSH provided by Cyberark.



For example, let's say *RepositoryUser* is the user in remote server *Repository.server.net* whose credentials are not known to the switch user. It is stored in the Cyberark vault *CyberArk.psm.server.net*. The switch user has credentials *CyberArkUser* to be validated and authorized by the CyberArk PSM server to access the Repository server. The switch user can then access the remote Repository server using the following command format: `<cyberark_user>@<remoteserver_user>@cyberarkserver`.

Which in this example is `CyberArkUser@RepositoryUser @CyberArk.psm.server.net`.

Example:

```
Switch:FID128:AdminUser> supportsave
This command collects RASLOG, TRACE, supportShow, core file, FFDC data
and then transfer them to a FTP/SCP/SFTP server or a USB device.
This operation can take several minutes.
OK to proceed? (yes, y, no, n): [no] y

Host IP or Host Name: Repository.Server.net
User Name: CyberArkUser@RepositoryServerUser@CyberArk.psm.server.net
Remote Directory: /repository/SAN/supportSave
Protocol (ftp | scp | sftp): scp
SCP/SFTP Server Port Number [22]:
Do you want to continue with CRA (Y/N) [N]:
Password:
Saving support information:
 SLOT  SWITCH              MODULE               CLI SIZE     FILE SIZE        CLI
TIME     MODULE TIME LOAD AVERAGE
CP0    Switch             RAS                164.354 KB      0.000
KB  23.96416  secs  41.251469 secs 0.0/0.1/0.3
….
CP0    Switch              RAS_POST            227.331 KB      0.000 KB   4.582320
secs   7.556573 secs 2.5/1.2/0.7
Summary worker: 4, cpu load: 3 upload size:  8001 KB, time:215 secs upload: 4
load:2.9/1.2/0.7

SupportSave completed (Duration : 3 minutes 35 seconds). .
```

12.2.1.7.1 New/Modified/Deprecated CLI Commands

The following commands are enhanced to support CyberArk PSM

- `Supportsave`
- `Configupload`
- `Configdownload`
- `Firmwaredownload`
- `Firmwarecleaninstall`
- `Seccertmgmt`
- `Seccryptocfg`
- `License`

12.2.2 MAPS and Fabric Performance Impact (FPI) Enhancements

FOS v9.2.0 supports the following MAPS and FPI enhancement:

- Monitoring the chassis-wide zone database usage
- Enhanced system memory monitoring
- Always Active system policy
- SDDQ Rest enhancement
- Port name details in MAPS alerts
- Include all N-Ports in the group ALL_N_PORTS
- Extension certificates monitoring
- MAPS actions on FCIP circuits
- Adaptive MAPS notifications
- Enable threshold customization in FPI Profile
- FPI alerts to include latency/congestion time

12.2.2.1 Monitor Chassis-Wide Zone DB

MAPS is enhanced to monitor the chassis-wide committed Zone DB size and if this size exceeds threshold (percentage of the maximum chassis Zone DB size limit), then MAPS alerts are generated.

12.2.2.1.1 New/Modified/Deprecated CLI Commands

The `mapsrule` command is enhanced to manage the rule to monitor zone DB.

Example:

```
mapsrule --create zone_chas_rule -monitor ZONE_CFGSZ_PER -group chassis -timebase none -
op g -value 70 -action raslog -policy custom_policy
```

12.2.2.1.2 Fabric OS Compatibility

On firmware downgrade from FOS9.2.0 to a lower version, if the user has configured any rule for monitoring system ZONE_CFGSZ_PER and group as CHASSIS then a warning message is displayed as below.

```
WARNING:MAPS user defined rules or default rules in user defined policy for
ZONE_CFGSZ_PER, CHASSIS will not be monitored in pre-9.2.0 release. Please delete these
from FID: 128
```

12.2.2.2 Monitor System Memory

MAPS is enhanced to monitor the physical as well as virtual memory using new default rules to monitor the memory.

- `defCHASSISMEMORY_USAGE_STATE_CRIT CHASSIS(MEMORY_USAGE_STATE/NONE==CRIT_OOM) RASLOG,SNMP,EMAIL`
- `defCHASSISMEMORY_USAGE_STATE_IN_RANGE CHASSIS(MEMORY_USAGE_STATE/NONE==IN_RANGE) RASLOG,SNMP,EMAIL`
- `defCHASSISMEMORY_USAGE_STATE_WARN CHASSIS(MEMORY_USAGE_STATE/NONE==WARN_OOM) RASLOG,SNMP,EMAIL`

The above listed rules monitor the system all the time as part of the MAPS active policy. These rules cannot be deleted by the end user. The rules are being monitored under switch resource category.

```
CHASSIS(MEMORY_USAGE_STATE == CRIT_OOM) RASLOG
CHASSIS(MEMORY_USAGE_STATE == MARG_OOM) RASLOG
```

Example of RASLOG alert:

```
2022/11/22-23:19:45 (GMT), [MAPS-1001], 41, FID 14, CRITICAL, SwitchName, Chassis,
Condition=CHASSIS(MEMORY_USAGE_STATE/NONE==CRIT_OOM), Current Value:[MEMORY_USAGE_STATE,
CRIT_OOM], RuleName=defCHASSISMEMORY_USAGE_STATE_CRIT, Dashboard Category=Switch
Resource, Quiet Time=None.
```

The moment MAPS detects critical level of memory usage, the alert below is raised, and the user is recommended to perform an HA failover and contact the Brocade support team.

```
CRITICAL, SwitchName, Chassis, Condition=CHASSIS(MEMORY_USAGE_STATE == CRIT_OOM), Current
Value:[MEMORY_USAGE_STATE, CRIT_OOM], RuleName=defCHASSISMEMORY_USAGE_STATE_CRIT,
Dashboard Category=Switch Resource.0
```

The rule is being monitored under the switch resource dashboard.

12.2.2.2.1 New/Modified/Deprecated CLI Commands

The following commands are modified to support this feature:

- `mapssam`
- `mapsrule`

Examples:

```
 mapssam --show memory

      Showing Memory Usage:
         Memory Usage      : 27.55%
         Used Memory       : 514024k
         Free Memory       : 1352020k
         Free Kernel Memory[1]      : 50%
         Total Memory      : 1866044k
mapsrule –-help
------truncated-----------------
Switch Resource      TEMP, FLASH_USAGE, CPU, MEMORY_USAGE, ETH_MGMT_PORT_STATE,
VTAP_IOPS, IT_RES_USAGE, ITL_RES_USAGE, MEMORY_USAGE_STATE
------truncated-----------------

Memory usage state: CRIT_OOM, MARG_OOM, IN_RANGE
------truncated-----------------
```

[1] Not all platforms display Free Kernel Memory.

12.2.2.2.2 Fabric OS Compatibility

When downgrading from FOS v9.2.0 the following message is displayed:

```
WARNING: MAPS user defined rules or default rules in user defined policy for
         MEMORY_USAGE_STATE will not be monitored in pre-9.2.0 release.
         Please delete these from FID: 1
```

12.2.2.3 System Policy: Always Active Policy

MAPS is enhanced to support a new default policy to manage existing or new system rules. The new default policy is called always active policy (`dflt_always_active_policy`). The always active policy (`dflt_always_active_policy`) behaves the same way as any other default policy except for the following:

- It contains only default system rules.
- This policy is always enabled in addition to the end user selected Active Policy.

12.2.2.3.1 New/Modified/Deprecated CLI Commands

The `mapspolicy` command is modified to support this enhancement:

```
mapspolicy –help

Values for policy name:    dflt_conservative_policy, dflt_aggressive_policy,
dflt_moderate_policy, dflt_base_policy, dflt_always_active_policy, <Custom Policies>

mapspolicy --show -summary
              Policy Name                     Number of Rules
      ------------------------------------------------------------
      dflt_aggressive_policy           :               374
      dflt_moderate_policy             :               378
      dflt_conservative_policy         :               378
      dflt_base_policy                 :                45
      dflt_always_active_policy        :                45

      Active Policy is 'dflt_aggressive_policy'. dflt_always_active_policy is always
      active.
```

12.2.2.3.2 Fabric OS Compatibility

On firmware downgrade from FOS9.2.0 to a lower version, the `dflt_always_active_policy` is removed.

12.2.2.4 REST Enhancement for SDDQuarantine

In FOS v9.2.0 MAPS is being enhanced to support the REST interfaces corresponding to the following CLI commands under `sddQuarantine:`

```
sddQuarantine –show
sddQuarantine –clear {[<slot>/]<port> | all}
```

New supported URIs:

```
rest/operations/quarantine-clear/all
rest/operations/quarantine-clear/port-index/<value>
rest/running/brocade-maps/quarantined-devices
rest/running/brocade-maps/quarantined-devices/port-index/<value>
```

12.2.2.5 Port Name in Maps Alerts and Emails for SFP TX/RX Alerts

In FOS v9.2.0 MAPS is enhanced to include the port name details in MAPS notifications for SFP alerts in RASLOG and other MAPS alerts for SFP rules monitoring. Prior to FOS v9.2.0 port name information is printed only for port monitoring systems.

RASLOG example with the port name details:

```
2021/08/27-19:21:04:271084 (GMT), [MAPS-1003], 657/92, FID 88 | ssd_port10, SFP 0/97,
WARNING, SW_G730, SFP 97, Condition=ALL_SFP(VOLTAGE/NONE>SFP_HIGH_TH_ALARM), Current
Value:[VOLTAGE, 3676 mVolts, (high_th: 3630, low_th: 2970, part_num: 57-1000495-01,
serial_num: MAA12034C154835)], RuleName=defALL_SFP_VOLTAGE, Dashboard Category=Port
Health, Quiet Time=1 day.
```

12.2.2.6 N-Ports are Removed from the NON_E_F_PORTS Group

In the FOS v9.1.0 release a new default group called ALL_N_PORTS in AG Mode was introduced. All the N-ports are grouped under this new default group.

These N-ports should be present only in the ALL_N_PORTS group and not in NON_E_F_PORTS. But in order to support backward compatibility, N-ports were kept in both ALL_N_PORTS and NON_E_F_PORTS default groups in the FOS v9.1.0 release.

In FOS v9.2.0 on AG mode, N-ports are grouped only in the ALL_N_PORTS default group and not in NON_E_F_PORTS group.

Example:

In pre-9.2.0 release:

```
sw0:admin> logicalgroup --show

------------------------------------------------------------------------------------------
Group Name           |Predefined |Type                 |Member Count |Members
------------------------------------------------------------------------------------------
ALL_PORTS            |Yes        |Port                 |64           |0-63
ALL_F_PORTS          |Yes        |Port                 |1            |4
ALL_N_PORTS          |Yes        |Port                 |5            |3,16-19
ALL_OTHER_F_PORTS    |Yes        |Port                 |1            |4
NON_E_F_PORTS        |Yes        |Port                 |63           |0-3,5-63
```

In FOS9.2.0 release:

```
sw0:admin> logicalgroup --show

------------------------------------------------------------------------------------------
Group Name           |Predefined |Type                 |Member Count |Members
------------------------------------------------------------------------------------------
ALL_PORTS            |Yes        |Port                 |64           |0-63
ALL_F_PORTS          |Yes        |Port                 |1            |4
ALL_N_PORTS          |Yes        |Port                 |5            |3,16-19
ALL_OTHER_F_PORTS    |Yes        |Port                 |1            |4
NON_E_F_PORTS        |Yes        |Port                 |58           |0-2,5-15,20-63
```

12.2.2.7 Monitor EXTN Certificates

In FOS v9.2.0 MAPS is being enhanced to monitor Extension switch certificates (SW) and Extension CA certificates.

Impacted monitoring systems are DAYS_TO_EXPIRE and EXPIRED_CERTS.

In addition to the existing support to monitor certificates, MAPS will monitor Extension certificates which includes local EXTN SW certificates, remote EXTN SW certificates, local EXTN CA certificates and remote EXTN CA certificates.

Below is the complete list of CERTS monitored by MAPS.

- HTTPS
- SYSLOG
- LDAP
- RADIUS
- FCAP
- ASC
- KAFKA
- EXTN SW
- EXTN CA

Prior to FOS v9.2.0 releases there was a limit on the number of certificates which can be imported and can be monitored by MAPS. The limit was 64 certificates.

In the FOS v9.2.0 release it is increased to 384 to support Extension certificates.

12.2.2.7.1 New/Modified/Deprecated CLI Commands

Example output for Extension certificates which are imported in MAPS.

```
ExtensionSwitch:FID128:admin> logicalgroup --show ALL_CERTS

--------------------------------------------------------------------------------------------
---------------------
Group Name                      |Predefined |Type              |Member Count |Members
--------------------------------------------------------------------------------------------
---------------------
ALL_CERTS                       |Yes        |Certificate       |7            |HTTPS SW
Certificate, Extension SW Certificates, Extension CA Certificates.
```

MAPS RASLOG for certificate Expiry is enhanced to include Certificate Name and the Serial number of the certificate. Issuing Authority ID is not displayed in RASLOG as it was done in earlier releases. Certificate name and Serial number uniquely identifies the certificate, consequently providing time for the end user to replace with a new certificate.

Example RASLOG messages:

```
2022/08/19-05:55:31 (GMT), [MAPS-1003], 125, FID 128, WARNING, sw0, Extension SW
Certificate, [Name:testExtnSw.pem SN:D36AADA11E69853D],
Condition=ALL_CERTS(DAYS_TO_EXPIRE/NONE<20), Current Value:[DAYS_TO_EXPIRE, 0 days],
RuleName=defCHASSISCERT_VALIDITY_20, Dashboard Category=Security Violations, Quiet
Time=None.

2022/08/19-06:55:31 (GMT), [MAPS-1003], 1305, FID 128, WARNING, sw0, RADIUS Server CA
Certificate, [Name:swRadca.pem SN:1012], Condition=ALL_CERTS(DAYS_TO_EXPIRE/NONE<100),
Current Value:[DAYS_TO_EXPIRE, 23 days], RuleName=daystoexpire, Dashboard
Category=Security Violations, Quiet Time=None.


2022/08/19-06:55:31 (GMT), [MAPS-1003], 1306, FID 128, WARNING, sw0, RADIUS Server CA
Certificate, [Name:swRadca.pem SN:118A], Condition=ALL_CERTS(DAYS_TO_EXPIRE/NONE<100),
Current Value:[DAYS_TO_EXPIRE, 23 days], RuleName=daystoexpire, Dashboard
Category=Security Violations, Quiet Time=None.

2022/08/19-06:55:31 (GMT), [MAPS-1003], 1307, FID 128, WARNING, sw0, RADIUS Server CA
Certificate, [Name:swRadca.pem SN:C60AE09B2F0E5ACB],
Condition=ALL_CERTS(DAYS_TO_EXPIRE/NONE<100), Current Value:[DAYS_TO_EXPIRE, 23 days],
RuleName=daystoexpire, Dashboard Category=Security Violations, Quiet Time=None.
```

NOTE MAPS currently monitors EXPIRED_CERTS, which gives a total number of expired certificates. If there are any expired Extension certificates, it is monitored by EXPIRED_CERTS MS.

12.2.2.8 MAPS Actions on FCIP Circuits Based on FCIP QOS Triggers

MAPS is enhanced to monitor the individual circuit QOS states and take necessary actions like fencing or toggling the circuit if a particular QOS goes down.

The existing **STATE_CHG MS** is enhanced to monitor the Circuit QOS states. Existing circuit state monitoring remains intact.

Monitoring:

STATE_CHG monitoring is enhanced for FCIP QOS groups.

If the tunnel is configured only for FCIP mode, then QOS state changes are monitored for the QOS groups:

- ALL_CIRCUIT_F_QOS
- ALL_CIRCUIT_HIGH_QOS
- ALL_CIRCUIT_MED_QOS
- ALL_CIRCUIT_LOW_QOS

If the tunnel is configured in hybrid mode (FCIP + IPEXT), then additionally QOS state changes is monitored for the three groups:

- ALL_CIRCUIT_IP_HIGH_QOS
- ALL_CIRCUIT_IP_MED_QOS
- ALL_CIRCUIT_IP_LOW_QOS

Actions Supported:

RASLOG, SNMP, EMAIL, FENCE

Rules:

Below default rules are added in MAPS but are not associated with any default policies. Users can add the default rules shown below to any policy.

```
defALL_CIRCUIT_F_QOS_STATE_CHG_4    |ALL_CIRCUIT_F_QOS(STATE_CHG/MIN>4)    |RASLOG,SNMP,EMAIL,FENCE
defALL_CIRCUIT_HIGH_QOS_STATE_CHG_4 |ALL_CIRCUIT_HIGH_QOS(STATE_CHG/MIN>4) |RASLOG,SNMP,EMAIL,FENCE
defALL_CIRCUIT_LOW_QOS_STATE_CHG_4  |ALL_CIRCUIT_LOW_QOS(STATE_CHG/MIN>4)  |RASLOG,SNMP,EMAIL,FENCE
defALL_CIRCUIT_MED_QOS_STATE_CHG_4  |ALL_CIRCUIT_MED_QOS(STATE_CHG/MIN>4)  |RASLOG,SNMP,EMAIL,FENCE

defALL_CIRCUIT_IP_HIGH_QOS_STATE_CHG_4 |ALL_CIRCUIT_IP_HIGH_QOS(STATE_CHG/MIN>4)
|RASLOG,SNMP,EMAIL,FENCE
defALL_CIRCUIT_IP_LOW_QOS_STATE_CHG_4  |ALL_CIRCUIT_IP_LOW_QOS(STATE_CHG/MIN>4)
|RASLOG,SNMP,EMAIL,FENCE
defALL_CIRCUIT_IP_MED_QOS_STATE_CHG_4  |ALL_CIRCUIT_IP_MED_QOS(STATE_CHG/MIN>4)
|RASLOG,SNMP,EMAIL,FENCE
```

12.2.2.8.1 New/Modified/Deprecated CLI Commands

There are no changes to the CLI.

However, users can create/delete/display custom rules for the STATE_CHG monitoring system with Circuit QOS groups

12.2.2.8.2 Fabric OS Compatibility

Firmware Upgrade:

No Impact.

Firmware Downgrade:

If a user has configured any custom rule on STATE_CHG for Circuit QOS groups, during firmware downgrade, a warning message is displayed to indicate that STATE_CHG on circuit QOS groups are not supported in releases prior to FOS v9.2.0.

```
"WARNING: User defined rules are present for STATE_CHG on CIRCUIT QOS groups and it is
not supported in pre-FOS9.2.0 release. The impacted FID(s): 128"
```

12.2.2.9 Adaptive MAPS Notifications

MAPS introduces a new feature called Adaptive MAPS Notification. With Adaptive MAPS Notification in place, alert throttling is applied progressively.

This feature replaces the existing features such as Global Quiet Time and Rule Quiet Time.

Functionality of Adaptive MAPS Notification:
New alert patterns can be either progressively increasing or decreasing in nature.

- In FOS v9.2, MAPS provides two default notification profiles (these are not customizable) and are applied for respective notification pattern.
- The Adaptive Notifications profile have the Quiet Time windows after the real time notification, as shown in the table below:

Progressively Increasing Alert Profile:

Quiet Time Window	Quiet Time Value
Window 1	1 hour
Window 2	6 hours
Window 3	1 day
Window 4	1 week
Window 5	1 month

Progressively Decreasing Alert Profile:

Quiet Time Window	Quiet Time Value
Window 1	Month
Window 2	Week
Window 3	Day

- The progressively decreasing notification profile is applied to Certificates Expiry (Days_To_Expiry) or License Expiry (TruFOS expiry) monitoring and progressively increasing notification profile is applied to “Port” and other non-FRU monitoring.
- After the first notification, the Quiet Time profile is selected based on the violated object and monitoring system. For example, if CRC error is violated on the port, then an increasing alert profile is applied. If an alert is generated during the Quiet Time Windows, it is suppressed.
- At the end of the QT window a Quiet Time summary alert notification is provided and the next quiet time window is selected.
- In FOS v9.2, MAPS will monitor the violated object for Issue Resolution window. The decision is based on the time window, and it is fixed as 24-hours for all the objects.
- If no issue is observed in 24 hours since the last violation, then Quiet time is cleared, and the MAPS notifications will restart from Quiet Time window 1. Also, the Quiet window is restarted automatically after the last window has expired.
- Critical MAPS alerts such as FRU and SSP is in real-time based on the events.
- Every violated object will have an individual notification QT cycle. However, enabling the new policy or re-enabling the policy will clear the quiet time and restart the notification cycles for all the violated objects.

Adaptive MAPS Notification feature is not enabled by default.

The feature must be enabled by the end user, with the command displayed below, and is supported for all types of MAPS notifications such as RASLOG, EMAIL and SNMP.

```
mapsconfig --notification {default|adaptive}
WARNING: Adaptive MAPS Notification feature is enabled. Quiet Time configurations will be
ignored.
```

New update raslog MAPS-1220 is triggered after the successful configuration of notification mode.

```
2022/10/07-18:07:28 (GMT), [MAPS-1220], 294, FID 128, INFO, sw0, MAPS Notification mode
is set to Adaptive.
```

Upgrading to FOS v9.2.0 does not change the MAPS notification configuration (and behavior) while notification mode is set to Default notification mode. The existing QT CLI/REST interfaces are deprecated in FOS v9.2.0 but end users can continue to use the CLI/REST interfaces to add or edit the QT configurations.

The custom QT configurations from older releases are supported in FOS v9.2.0 (with plans to deprecate in future releases). End users using the QT feature are recommended to migrate to the new Adaptive Notifications mode. Similarly, the default rule QT or Global QT (default in G730) is enabled, then MAPS will continue to use the configuration and it will stop using the custom/default configurations after enabling the Adaptive Notification feature. However, end users are allowed to edit or add QT configurations, but the modified configurations will only effective when the switch is configured to Default notification mode.

12.2.2.9.1 New/Modified/Deprecated CLI Commands

The following command `mapsconfig` is used to change the notification mode to adaptive and ignore QT configurations and display notification settings.

Upgrade to v9.2 with QT Configuration

After upgrading, the notification behavior is set to Default.

```
Gen7:admin> mapsconfig --show
Configured Notifications:       RASLOG,SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL,SDDQ
Mail Recipient:                 Not Configured
Mail From Address:              Not Configured
Raslog Mode:                    Default
Decom Action Config:            Impair (No Disable)
Global Quiet Time:              2 Days and 0 Hours
Notification Behavior:             Default
```

Enabling Adaptive Notification Feature (with or without QT Configurations)

```
Gen7:admin> mapsconfig --notification adaptive
WARNING: Adaptive MAPS Notification feature is enabled. Quiet time configurations will be
ignored.
```

If QT was already configured, then it will be still present but not in effect.

```
Gen7:admin> mapsconfig –show
Configured Notifications:       RASLOG,SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL,SDDQ
Mail Recipient:                 Not Configured
Mail From Address:              Not Configured
Raslog Mode:                    Default
Decom Action Config:            Impair (No Disable)
Global Quiet Time:              2 Days and 0 Hours (Not Effective)
Notification Behavior:             Adaptive
```

Global Quiet Time and Rule Quiet Time Features

The CLI interfaces to enable Global Quiet Time and configure Rule Quiet time will be deprecated but continue to be supported in FOS v9.2.0 release with warning message saying that “Quiet time feature are deprecated in v9.2.0”. Both CLI and REST interfaces will be obsolete in future releases.

```
mapsConfig --qt {-value <value> [-unit {hour|day}] | -clear}
mapsrule --create/config  [-qt <quiet time> [-unit {min|hour|day}] | -qtclear]
```

12.2.2.9.2 Fabric OS Compatibility

Firmware Upgrade:

If a user performs firmware upgrade and has configured either Global QT or Rule QT, then it will be honored, and a warning message will be printed saying that feature is deprecated in v9.2.0 release.

```
"WARNING: MAPS Global Quiet Time and Rule Quiet Time features are deprecated in v9.2.0
and these configurations are ignored when Adaptive Notification feature is enabled"
```

Firmware Downgrade:

If a user performs firmware downgrade from FOS v9.2.0 to an earlier release and if Adaptive MAPS Notification feature is enabled, firmware downgrade will throw a warning message indicating Adaptive notification is not applicable and the MAPS notifications will enable the legacy behavior.

```
“WARNING: MAPS Adaptive Notification feature is not available in pre-FOS v9.2.0 releases.
Downgrading to pre-FOS v9.2.0 release will enable MAPS legacy notification.”
```

12.2.2.10 Displaying Latency/Congestion Time Period in FPI Clear Alert

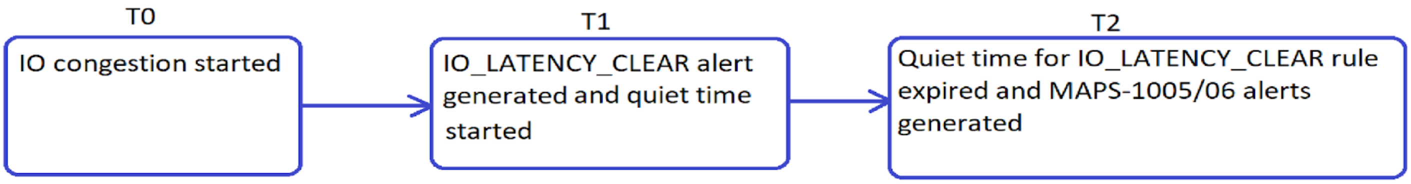
In FOS v9.2.0, the additional information of congested time duration is displayed in the IO_LATENCY_CLEAR MAPS alert. This provides visibility into the amount of time a port remains in the congestion state after every time it enters a congested state.

In addition, if Quiet Time (QT) is configured on FPI Rules, on quiet time expiry Total Congestion Duration and Maximum Congestion Duration along with the last FPI state will be displayed in the QT Summary alerts (MAPS-1006).

Total Congestion Duration – the total time in which a port was in a congestion state within its quiet time period.

Maximum Congestion Duration – the maximum time duration in which a port was in the congestion state in its last quiet time period.

Figure 1 Time Diagram for IO_LATENCY_CLEAR Alerts


T0
IO congestion started
T1
IO_LATENCY_CLEAR alert generated and quiet time started
T2
Quiet time for IO_LATENCY_CLEAR rule expired and MAPS-1005/06 alerts generated

Example:

1. Consider at T0, IO_FRAME_LOSS rule is triggered due to C3TXTO error and so congestion starts.
2. At T1, congestion gets cleared and a latency clear alert, MAPS-1004 is generated. In this IO_LATENCY_CLEAR alert, additional information about the congestion duration (T1-T0) would be displayed.

```
2021/08/20-21:15:20 (GMT), [MAPS-1004], 19563, FID 128 | PORT 0/34, INFO, sw0,
port34, F-Port 34, Condition=ALL_PORTS(DEV_LATENCY_IMPACT/NONE==IO_LATENCY_CLEAR),
Current Value:[DEV_LATENCY_IMPACT, IO_LATENCY_CLEAR, (Duration: 1m)],
RuleName=defALL_PORTS_IO_LATENCY_CLEAR, Dashboard Category=Fabric Performance
Impact,
Quiet Time=15 min.
```

3. Subsequently, if the IO_FRAME_LOSS and IO_LATENCY_CLEAR rules have Quiet Time (QT) configured, then no RASLOGs will be generated if the port toggles multiple times between IO_FRAME_LOSS and IO_LATENCY_CLEAR states until QT.

   In FOS v9.2.0 MAPS give more visibility into the congestion states when QT is in effect

4. At T2, quiet time for latency clear rule expires and so raslogs MAPS-1005 and MAPS-1006 triggers. Raslog MAPS-1006 will display the summarized congestion information i.e. Total Congestion Duration and Maximum Congestion Duration.

```
2021/08/20-21:31:00 (GMT), [MAPS-1005], 19580, FID 128 | PORT 0/34, WARNING, sw0,
port34, F-Port 34, Condition=ALL_PORTS(DEV_LATENCY_IMPACT/NONE==IO_LATENCY_CLEAR),
Current Value:[DEV_LATENCY_IMPACT, IO_LATENCY_CLEAR], Rule
defALL_PORTS_IO_LATENCY_CLEAR triggered 10 times in 15 min and last trigger time
Fri Aug 20 21:27:30 2021,
Dashboard Category=Fabric Performance Impact.

2021/08/20-21:31:00 (GMT), [MAPS-1006], 19581, FID 128 | PORT 0/34, INFO, sw0,
port34, F-Port 34, Latest Value=[DEV_LATENCY_IMPACT, IO_LATENCY_CLEAR],
Total Congestion Duration: 8m, Maximum Congestion Duration: 5m.
```

NOTE Congestion time duration is displayed in `<hr>h <min>m <sec>s` format with `10h 34m 20s` representing 10 hours 34 minutes and 20 seconds.

12.2.3 Traffic Optimizer

The Traffic Optimizer predefined profiles are suitable for most advanced SAN environments with higher generation speed devices and NVMe devices. In an environment like FICON fabric, the older generation speeds are still widely used, and such environments do not have NVMe support today.

12.2.3.1 TO Custom Profile

To optimally support environments with older generation speeds FOS v9.2.0 allows the user to define and enable a custom TO profile.

FOS v9.2.0 supports the customization based on the following parameters:

- Protocol_SCSI
  - Supported Speeds
    - 4G, 8G, 16G, 32G, 64G
- Protocol NVMe
  - Supported Speeds
    - 32G, 64G

The user can input only *a maximum of three protocol/speed* combinations.

Based on the user inputs, the system will allocate a separate PG for each protocol/speed combination input by the user. The system will also allocate a default PG (PG_DEFAULT) which will be used for flows that do not match the selected protocol/speed parameters.

When the user selects a smaller number of protocol/speed combinations, the system will allocate more than one PG for the same protocol/speed combination and flows will be distributed amongst those PGs, thereby improving the “fault” domain for the PGs.

In the custom profile, after provisioning PGs for the selected protocol/speed combinations, the system will also allocate Over-subscription PGs for all speeds selected by the user. Thus, whenever flows belonging to a user selected speed become oversubscribed, they are moved to their respective speed-based OS PGs. When an OS event is detected for flows belonging to the default PG, they are moved to the corresponding default OS PG.

Examples:

Use Case Example	Configuration
Custom TO Profile - FICON Use Case 1	Selected Protocol/Speed SCSI_4G, SCSI_8G, SCSI_16G Supported PGs – PG_SCSI_16G – PG_SCSI_8G – PG_SCSI_4G – PG_DEFAULT[contains normal flows that don’t belong to the above PGs] – PG_OVER_SUBSCRIPTION_16G – PG_OVER_SUBSCRIPTION_8G – PG_OVER_SUBSCRIPTION_4G – PG_OVER_SUBSCRIPTION_DEFAULT [contains oversubscribed flows that belong to PG_DEFAULT] **NOTE** In addition to above, 5 QoS High PGs and 2 QoS Low (sddq) PGs are supported.

Custom TO Profile - FICON Use Case 2	Selected Protocol/Speed SCSI_8G, SCSI_16G, SCSI_32G Supported PGs ▪ PG_SCSI_32G ▪ PG_SCSI_16G ▪ PG_SCSI_8G ▪ PG_DEFAULT [contains normal flows that don't belong to the above PGs] ▪ PG_OVER_SUBSCRIPTION_32G ▪ PG_OVER_SUBSCRIPTION_16G ▪ PG_OVER_SUBSCRIPTION_8G ▪ PG_OVER_SUBSCRIPTION_DEFAULT [contains oversubscribed flows that belong to PG_DEFAULT] **NOTE** In addition to above, 5 QoS High PGs and 2 QoS Low (sddq) PGs are supported.
Custom TO Profile - Example 3 [Greenfield Deployment]	Selected Protocol/Speed SCSI_32G, SCSI_64G, NVME_64G Supported PGs ▪ PG_SCSI_64G_1 ▪ PG_SCSI_64G_2 ▪ PG_SCSI_32G ▪ PG_NVME_64G ▪ PG_DEFAULT[contains normal flows that don't belong to the above PGs] ▪ PG_OVER_SUBSCRIPTION_64G ▪ PG_OVER_SUBSCRIPTION_32G ▪ PG_OVER_SUBSCRIPTION_DEFAULT [contains oversubscribed flows that belong to PG_DEFAULT] **NOTE** In addition to above 5 QoS High PGs and 2 QoS Low (sddq) PGs are supported.
Custom TO Profile - Example 4 [Greenfield Deployment]	Selected Protocol/Speed SCSI_64G Supported PGs ▪ PG_SCSI_64G_1 ▪ PG_SCSI_64G_2 ▪ PG_SCSI_64G_3 ▪ PG_SCSI_64G_4 ▪ PG_SCSI_64G_5 ▪ PG_DEFAULT [contains normal flows that don't belong to the above PGs] ▪ PG_OVER_SUBSCRIPTION_64G ▪ PG_OVER_SUBSCRIPTION_DEFAULT [contains oversubscribed flows that don't belong to the above speed based over subscription PGs] **NOTE** In addition to above, 5 QoS High PGs and 2 QoS Low (sddq) PGs are supported.

Custom TO Profile - Example 5 [Greenfield Deployment]	Selected Protocol/Speed SCSI_64G, NVME_64G Supported PGs ▪ PG_SCSI_64G_1 ▪ PG_SCSI_64G_2 ▪ PG_SCSI_64G_3 ▪ PG_NVME_64G_1 ▪ PG_NVME_64G_2 ▪ PG_DEFAULT [contains normal flows that don't belong to the above PGs] ▪ PG_OVER_SUBSCRIPTION_64G ▪ PG_OVER_SUBSCRIPTION_DEFAULT [contains oversubscribed flows that belong to PG_DEFAULT] **NOTE** In addition to above, 5 QoS High PGs and 2 QoS Low (sddq) PGs are supported.

12.2.3.1.1 New and Modified CLI Commands

FOS v9.2.0 includes the following CLI changes for TO:

- `trafopt --show -profile`
- `trafopt --show -pg`
- `trafopt –-update -profile -add/remove -protocol -speed`

See TO command options for reference:

```
Switch:FID128:admin> trafopt
Mandatory options not specified
Traffic Optimizer operations help
SYNTAX - trafopt <trafopt operations> <options>

<trafopt operations>
--help
/* Trafopt command help */
--show
/* Display Performance Group Dashboard and available TO profile */
                  [-profile]
/* Display all available Profiles*/
                  [-profile <profile_name>]|
/* Display information for performance group part of a specified profile */
                  [-pg]
/* Displays all active Performance Groups */
                  [-pg <performance_group_name>]|
/* Display detailed statistics and VC for specified performance group */
                  [-flow
                     <-pg <performance_group_name> > |
/* Display flows associated with specified Performance Group */
                     <-srcdev <devID|"*"> > |
/* Display flows associated with specified Source FCID */
                     <-dstdev <devID|"*"> > |
/* Display flows associated with specified Destination FCID */
                     <-srcdev <devID|"*"> -dstdev <devID|"*">>]
/* Display flows associated with specified Source FCID and Destination FCID */
--activate        <profile_name>
/* Activate given profile */
--schedule        <profile_name> -delay <1-60 days>
/* Schedule to activate given profile after 'delay' days */
```

```
--abort_schedule
/* Abort the already scheduled profile */
--update
/* Customize the profile. Incremental updates allowed*/
                  <-profile <profile_name>>
/* Profile's name whose configuration being updated */
                  <-add|-remove>
/* Edit the configuration of the profile */
                  <-protocol <scsi|nvme>
/* Customize profile with speed and protocol combination.
                  -speed <speeds separated by comma>
Users can configure for SCSI and NVME separately.
For each Protocol, speeds can be updated incrementally. */
```

12.2.3.1.2Fabric OS Compatibility

Firmware Upgrade

Non-disruptive upgrade is supported from v9.x.x firmware to v9.2.0 firmware.

Whatever predefined TO profile activated prior to upgrade will continue to be enforced after upgrade to v9.2.0.

Users can migrate to a custom profile only after migrating to v9.2 firmware.

Migrating to and from the custom profile is a disruptive operation.

Firmware Downgrade

Downgrade to v9.1.x will be non-disruptive when V1 or V2 profile is active.

Non-disruptive downgrade from FOS v9.2.0 to FOS v9.1.x is not allowed when the custom TO profile is active. Update the Profile to V2/V1 profile (using the `trafopt` command) before initiating the downgrade. This profile update operation is disruptive.

After firmware downgrade, whatever profile that was active before downgrade will continue to be active.

12.2.4 Extension

12.2.4.1 TO Support on FCIP

TO feature support with FCIP (only applies to Brocade 7850):

- TO features apply when traversing the FC fabric.
- While the traffic goes over VE port, only three priorities are supported (High, Medium, and Low). PG_QOS_HIGH PGs map to High priority, PG_SDDQ_LOW PGs map to Low priority, and the rest of the PGs map to Medium priority.
- The TO performance group classification information will be preserved across the TO supported FCIP tunnel so that the PG classification is again enforced at the rear end of the tunnel through the rest of the FC fabric.

12.2.4.2 New/Modified/Deprecated CLI commands

Summary of the CLI modifications and additions in FOS v9.2.0.

`extncfg –ve-mode`	Added 6VE and 18VE modes
`portcfgge`	Added newly supported speeds
`portcfg fciptunnel / fcipcircuit`	Increase bandwidth limits and new comm-rate syntax

Examples:

```
Usage: extncfg { --ve-mode <args> | --ge-mode <args> | --app-mode <args> | --show <args>
| --config <args> | --fwdl-prep <args> }

Arguments:
  --ve-mode { 6VE | 18VE }               - Set VE-Mode to specified mode.
  --ge-mode { copper | optical }         - Set GE-Mode to copper or optical.
  --show                                 - Display APP & VE mode details.
  --config { -default | -manager }       - Manage the extension configurations.
                                           '-default': Default the running
                                             extension configurations.
                                           '-manager': Run the extension
                                             configuration manager utility.
  --fwdl-prep [-version #.#.#] [-abort]  - Prepare the switch for firmware
                                           download to the target version.
  -h,--help                              - Print this usage statement.

---

Usage: portCfgGe [<slot>/][<port>] [<args>]

Port Format:
   ge#

Args:
   --enable -autoneg         - Enable the auto-negotiate mode of the 1 GE ports only.
   --disable -autoneg        - Disable the auto-negotiate mode of the 1 GE ports only.
   --set -speed <speed>      - Set the port speed of the GE ports. Allowable speeds:
                               [1G, 10G, 25G] (port dependent)
   --set -lan                - Set the port as lan.
   --set -wan                - Set the port as wan.
   --set -channel <channel>  - Set the port tunable SFP channel ID of the 10 GE ports
only.
                               Allowable channel ID Range [1] - [102]
   --show                    - Show the current GE port configurations.
   --show -lmac              - Show the Local MAC addresses for GE/LAN ports.
                              - Print this usage statement.

---

Brocade 7850:FID128:admin> portcfg fcipcircuit --help

Usage:   portCfg fcipcircuit [<slot>/]<port> <option> <cid> [<args>]

Option:    create - Create the specified tunnel/circuit
           modify - Modify the specified tunnel/circuit
           delete - Delete the specified tunnel/circuit

Optional Arguments:
  -a,--admin-status <enable|disable> -
                               -  Set the admin-status of the circuit.
  -S,--local-ip <ipaddr>|none  -  Set local IP address.
  -D,--remote-ip <ipaddr>|none -  Set remote IP address.
     --local-ha-ip <ipaddr>|none -
                               -  Set local HA IP address. This allows for HCL
                                  operations on local switch. [7840 / SX6 only]
     --remote-ha-ip <ipaddr>|none -
```

```
                               -  Set remote HA IP address. This allows for HCL
                                  operations on remote switch. [7810 / 7840 /
                                  SX6 only]
  -x,--metric <0|1>            -  Set the metric. 0=Primary 1=Failover.
  -g,--failover-group <0-9>    -  Set the failover group ID.
  -b,--min-comm-rate { <kbps> | <mbps>M | <gbps>G }
                               -  Set the minimum committed rate in Kbps|Mbps|Gbps.
  -B,--max-comm-rate { <kbps> | <mbps>M | <gbps>G }
                               -  Set the maximum committed rate in Kbps|Mbps|Gbps.
-arl-algorithm <mode>    -  Set the ARL algorithm. Allowable modes are
                                  [auto] [reset] [step-down] [timed-step-down].
------------------------------- Truncated -----------------------------------------------
```

12.2.4.2.1 Fabric OS Compatibility

The Brocade 7850 platform is only interoperable with 7810 and SX6 platforms running FOS v9.2.0 (or later) for VE link interoperability.

Config upload and config download will behave the same as existing extension platforms.

The main restriction regarding `configdownload` is the file being downloaded must have a matching VE-Mode configuration. This is the same behavior as SX6. When applying the new `configdownload` file, the switch must be rebooted to apply the config. Without a reboot, the switch will remain in the previous state operationally. No extension configuration changes will be allowed after the `configdownload` is performed until the reboot is performed.

NOTE The extension platforms 7840 and FX8-24 cannot form an FCIP tunnel to an extension platform running FOS v9.2.0.

12.2.5 Flow Vision (FV)

12.2.5.1 I/O Violation Streaming

In FOS v9.2.0 Flow Vision supports real time hardware violations at the I/O level for ECT/FRT metrics and time-based software violations for pending I/Os and other I/O health related counts.

With this new streaming feature, FV starts sending violation stats along with metric value on a separate telemetry topic (`fos_violation_stats`).

Applications like SANnav, FA or any north bound application that subscribe to this violation topic can provide a dashboard to the end user showing the health of fabric based on these flow level violations.

Feature Design

Violation stats are only streamed for the flows with violations (If there are no violations in any of the metrics then the flow record is not sent).

- Streamed at 5 minutes for 5-minute and 6-hour flows (all the IT/ITL/VITL flows).
- Streamed at 10 seconds for flows monitored in real time investigation mode

Flow vision monitors I/O violations either automatically or through user configured rules

When the end user has not configured any rules, then MAPS has default thresholds for these metrics that are pushed to FV and based on these thresholds’ violations are reported to the end user.

FV support for real time monitoring of I/O violations was implemented in FOS v9.1.0 where either the end user can configure rules through SANnav using collections or through MAPS policy.

These rules can be I/O based for ECT and FRT metric and time based (10 second) for Pending I/Os and other I/O health related metrics.

I/O Based Rules

MAPS will push thresholds to FV which configures this threshold in the switch for monitoring of ECT, FRT metrics of each I/O and provides the count of I/Os that violated these MAPS thresholds

FV pulls these violation counts for all the flows from hardware every 10 seconds and aggregates for 5 minutes.

Time-based Rules

MAPS pushes thresholds to FV internal rules engine.

The FV rules engine compares metric with these thresholds every 10 seconds and sets SW violation count to 1 if its exceeding that threshold value (so in 5 minute this value can vary from 0 to 30).

All these counts along with metric values will be streamed to SANnav on separate Kafka topic every 5 minute for regular IT/ITL/VITL flows and after every 10 second for real time flows.

I/O-Based Violations:

Metric	Stats to Stream
I/O Count	▪ Read I/O count ▪ Write I/O count
Exchange Completion Time	▪ Read Command – Number of violated I/Os – ECT Accumulated – ECT Max ▪ Write command – Number of violated I/Os – ECT Accumulated – ECT Max
First Response Time	▪ Read Command – Number of violated I/Os – FRT Accumulated – FRT Max ▪ Write command – Number of violated I/Os – FRT Accumulated – FRT Max

Time-Based Violations:

Metric	Stats to Stream
Pending I/O	▪ Read Command – Number of SW violations – Pending I/O Accumulated – Pending I/O Max – Pending I/O Average ▪ Write command – Number of SW violations – Pending I/O Accumulated – Pending I/O Max – Pending I/O Average
Errors and Exceptions	▪ Aborts – Number of SW violations – Total number of aborts ▪ Timeout – Number of SW violations – Total number of timeouts ▪ Reserve – Number of SW violations – Total number of Reserve ▪ Total errors – Number of SW violations – Total error status / exceptions received

	GEN6	GEN7
ASIC	No Support	Condor5 GE5
SUPPORTED PLATFORMS	No Support	Brocade G720 Switch Brocade FC64-48 Brocade FC32-X7-48 (Only IT level) Brocade G730 Switch Brocade FC64-64

Example:

```
X7-8_FID41:FID41:admin > flow --show sys_flow_monitor -port 350
====================================================================================================
Name              : sys_flow_monitor
Definition        : Port(350)
Port Speed        : DstDev(32G)
Active Flow       : 1086
Timebase          : 5Min
Protocol          : SCSI
-----------------------------------------------------------------------------------------------------
Monitor Time      : | Fri Nov 18 13:58:52 PST 2022 |
RD Elapsed Time   : | 30s |
WR Elapsed Time   : | 30s |
---------- TRUNCATED  --------------------

I/O Violation Count |
--------------------------------------------------------------------------------|-------------------------
RD|          |     Total      |      Violations        |       Violations       |      Violations       |
| WR| Timebase |  Violations   |         ECT            |          FRT           |      Pending IOs       |
---------------------------------------------------------------------------------------------------------
| RD| Current  |        5.908K |    4.628K /    100.0m |    1.280K /    90.00m |           /           |
|   |    All   |        5.908K |    4.628K /    100.0m |    1.280K /    90.00m |           /           |
-------------------------------------------------------------------------------------------------------
| WR| Current  |        6.292K |    5.396K /    100.0m |      896  /    90.00m |           /           |
|   |    All   |        6.292K |    5.396K /    100.0m |      896  /    90.00m |           /           |
---------------------------------------------------------------------------------------------------------

I/O Exceptions Count |
--------------------------------------------------------------------------------------------------------
|
RD|          |              |                                           SCSI
       |
|   | Timebase |     Total    |-------------------------------------------------|-------------------------
| WR|          |  Exceptions |  TIMEOUT    |      BUSY    |  RESERVE    |   CHECK     |     TASK    |  TASK
SET  |   OTHERS   |
|   |          |              |             |            |  CONFLICT  |  CONDITION
|   ABORT    |     FULL    |             |
---------------------------------------------------------------------------------------------------------
| RD| Current  |         9246 |        8576 |         111 |         110 |         117 |         113 |         111
|        108 |
|   |   All    |         9246 |        8576 |         111 |         110 |         117 |         113 |         111
|        108 |
------------------------------------------------------------------------------------------------------------------------
----------
| WR| Current  |        10018 |        9344 |         100 |         118 |         124 |         109 |         107
|        116 |
|   |   All    |        10018 |        9344 |         100 |         118 |         124 |         109 |         107
|        116 |
---------------------------------------------------------------------------------

SCSI Other Command Counts |
---------------------------------------------------------------------------------------------------------
|   Timebase    |     Total     |   INQUIRY    |    RESERVE    |   RELEASE     |   REQ
SENSE  |      TUR      |   READ CAP    |     ABORT     |
---------------------------------------------------------------------------------------------------------
|   Current     |              |              |              |              |              |              |
        |              |
|   All         |          512 |          409 |              |              |              |          75
|           28 |              |
---------------------------------------------------------------------------------------------------------
```

12.2.5.1.1 New/Modified/Deprecated CLI Commands

ECT, FRT and pending I/O violations are displayed in the existing flow show CLIs.

12.2.5.2 VMID+ Enhancements

Prior to FOS v9.2.0 VMID+ and the use of XISL was mutually exclusive, and it was not permitted to use VMID+ on logical switches and fabrics configured for XISLs.

With FOS v9.2.0 using both VMID+ and XISL is supported, and a logical switch and fabric can be configured for VMID+ (`portCfgAppHeader`).

12.2.5.2.1 Platforms Supported

This feature is supported on all Gen 7 products except the Brocade 7850 extension switch.

12.2.5.2.2 FCR

VMID+ is not supported with FCR.

In addition, the same chassis (Director or pizza-box switch) cannot be configured with both EX-ports and VMID+. In FOS v9.2.0 these are mutually exclusive on the same chassis.

12.2.5.2.3 Fabric OS Compatibility

Firmware Downgrade is blocked when this configuration is enabled on any port of the logical switch and XISL usage is turned on. The end user must disable the VMID+ configuration (`portCfgAppHeader`) on the port(s) of the logical fabric to proceed with the downgrade.

12.2.6 Fabric Infrastructure

12.2.6.1 Firmware Download Check for Free Space

Prior to FOS v9.2.0 execution of the command `firmwaredownload` will proceed even if there is not enough disk memory space and will get stuck during package installation and the `firmwaredownload` fails.

In FOS v9.2.0 version, if there is not enough space available to load a new image using `firmwaredownload` operation, warning messages are displayed and `firmwaredownload` prompts the user with `Do you want to continue? [Y/N]:`

Before proceeding with the firmware download, use the `firmwaredownload -v` option to perform disk memory space validation and display disk space availability messages accordingly.

Disk memory space availability is checked on all partitions. In case of dual CP systems, disk memory space availability is checked on both partitions in the active and standby CPs. In case of chassis, `firmwaredownload -s` will be validating disk space of both partitions on the CP in which `firmwaredownload -s` is executed.

The minimum CF space required for `firmwaredownload` varies per platform and is calculated based on the maximum RPM size.

If there is not enough disk memory space to perform `firmwaredownload`, users can use the command `cleanup` to free up space and perform `firmwaredownload.` The command `cleanup` is available under the maintenance account.

Example:

```
Switch:FID128:maintenance> serviceexec cleanup

This utility will remove obsoleted files on the local CP.

Be aware the tool will remove all unauthorized code from both partitions.
Note that all the support files will be removed as well.
In case you want to save any of the support files,
execute supportsave before running this command.

Do you want to continue (Y/N) [Y]:
```

12.2.6.1.1 New/Modified/Deprecated CLI Commands

```
Switch:FID128:admin> firmwaredownload -v
There is not enough free space left on the switch.
Please use cleanup command to free up disk space.
sw0:FID128:admin>
```

12.2.6.2 Firmwarepatch

In FOS v9.2.0 the firmware management feature `firmwarepatch` is introduced. `Firmwarepatch` is implemented to provide a more efficient method to support customers that need a patch release. `Firmwarepatch` provides the ability to install the patch on the current FOS version of the switch instead of a full firmware download process with a CVR release build which replaces the FOS image on the switch.

12.2.6.2.1 New/Modified/Deprecated CLI Commands

`Firmwarepatch` is provided with the following command options:

```
firmwarepatch {--install -protocol <proto_type> -force
[<host>,<user>,<path>,<password>] | --remove | --show | --help}
```

Examples:

firmwarepatch –install

```
Server Name or IP Address: 10.10.10.10
User Name: SwitchAdmin
File Name:
/Repository/FOS_9.2.0_CVR003
Network Protocol(1-SCP, 2-SFTP) [1]: 1
Do you want to input SCP/SFTP options (Y/N) [N]:
Verifying if the public key authentication is available.
Please wait ...
The public key authentication is not available.
Password:
```

firmwarepatch –show

```
sw0:FID128:maintenance> firmwarepatch --show
Name of the patch: FOS_9.2.0_CVR003
Description: Patch purpose
Firmware_compatability: 9.2.0
Exception_FW_list_from_compatible: v9.2.0
Reboot required: Yes
```

12.2.7 FCR Updates

12.2.7.1 REST Enhancements: brocade-fibrechannel-logical-switch

Prior to FOS v9.2.0, the three REST leafs:

- base-switch-enabled
- ficon-mode-enabled
- logical-isl-enabled

Defined in the brocade-fibrechannel-logical-switch yang model are used with the integer value.

From FOS v9.2.0 these leaves are modified to support the boolean value aligned with the FOS REST standard. The existing leafs will be marked as deprecated, and the new leafs will be added with -v2 at the end of every leaf name indicating version 2 of that leaf.

The three new leafs are renamed as Base-switch-enabled-v2, Ficon-mode-enabled-v2 and Logical-isl-enabled-v2.

12.2.7.2 fcrxlateconfig --show stalexd Gives RBAC Permission Denied while Running via fosexec Remote Domain

From FOS v9.2.0 onwards the following CLI’s are not allowed to execute through the fosexec feature.

1. fcrxlateconfig –show
2. fcrlsan –show
3. fcrlsanmatrix –display

12.2.8 Miscellaneous

This section includes miscellaneous enhancements and changes in FOS v9.2.0

12.2.8.1 Signal Loss Metric from dBm to dB in sfpshow -link Output

In FOS v9.2.0 the Signal Loss metric over the F-port link in `sfpshow slot/port -link` display output is changed from uW and dBm to uW, dBm and dB.

The *Sfpshow with -link* option can compute the upstream and downstream signal loss over the fibre optic cable when the switch port is connected to an F-port capable of supporting the RDP Extended Link Service.

Prior to FOS v9.2.0 the display shows the signal loss in micro watts (uW) units and also the signal loss in dBm with reference to one milliwatt.

Here is an example of the relevant part of the `sfpshow slot/port -link` display output pre FOS v9.2.0:

```
Signal Loss (Upstream)  :  -9.4    dBm (115.8 uW)
Signal Loss (Downstream):  -11.1   dBm (78.1  uW)
```

In FOS v9.2.0 the signal loss at Rx port with reference to Tx port in dB for both upstream and downstream channels of the fibre optic cable display the signal loss in dB along with existing units uW/ dbM in the `sfpshow slot/port -link` display output

The sfpshow CLI will display the signal loss also in dB as shown below. The existing display of the signal loss in micro watt and dBm units will be retained as is for the existing applications / consumers to work as before.

```
Switch:FID128:admin> switchshow |grep -i F-Port
 127    4   31   027f00   id    N64       Online      FC  F-Port  10:00:00:10:9b:5a:25:3d
Switch:FID128:admin> sfpshow 4/31 -link -f
Identifier:  3    SFP
Connector:   7    LC
Transceiver: 0204406000000000 16,32,64_Gbps M5 sw Inter,Short_dist
Encoding:    8    PAM4
Baud Rate:   255  (units 100 megabaud)
Length 9u:   0    (units km)
Length 9u:   0    (units 100 meters)
Length 50u (OM2):  2    (units 10 meters)
Length 50u (OM3):  7    (units 10 meters)
Length 62.5u:   0    (units 10 meters)
Length 50u (OM4):  10   (units 10 meters)
Vendor Name: BROCADE
Vendor OUI:  00:05:1e
Vendor PN:   57-1000495-01
Vendor Rev:  B
Wavelength:  850  (units nm)
Options:     0a3a Loss_of_Sig,Tx_Fault,Tx_Disable
BR Max:      231
BR Min:      0
Serial No:   MAA12033C016485S
Date Code:   200818
```

```
DD Type:     0x68
Enh Options: 0xfa
Status/Ctrl: 0x30
Pwr On Time: 1.72 years (15092 hours)
E-Wrap Control: 0
O-Wrap Control: 0
Alarm flags[0,1] = 0x0, 0x0
Warn Flags[0,1] = 0x0, 0x0
Temperature: 34      Centigrade
Current:     6.858   mAmps
Voltage:     3244.7  mVolts
RX Power:    -0.6    dBm (877.6uW)
TX Power:    -0.9    dBm (819.1 uW)

State transitions: 1
Port Speed Capabilities         16Gbps   32Gbps 64Gbps

PEER Port SFP Info

Vendor Name: BROCADE
Serial num:  MAA12112C073835S
Vendor PN:   57-1000495-01
Vendor Rev:  B
Date Code:   210320
        Laser Type:     Short Wave Laser
        SFP Type:       Optical Port Type
        Connector Type: SFP+
Following SFP Parameters are Valid
        Temperature: 47      Centigrade [Range -128 - +128 C]
        Current:     7.140   mAmps    [Range 0 - 131 mAmps]
        Voltage:     3297.4  mVolts   [Range 0 - 3600 mVolts]
        Rx Power:    703.3   uW      [Range 0 - 6550 uW]
        Tx Power:    955.7   uW      [Range 0 - 6550 uW]
Signal Loss (Upstream)  :  -9.4    dBm (115.8 uW) (uu.vv dB)
Signal Loss (Downstream):  -11.1   dBm (78.1  uW)  (xx.yy dB)
Port Speed Capabilities         16Gbps   32Gbps 64Gbps
                Alarm                       Warn
               low        high             low           high
Temperature alerts(Centigrade): -1280        20480          0               19200
Voltage alerts(mVolts)        : 2970         3630           3134            3465
Tx Bias alerts(uA)            : 2000         10000          3000            8500
Tx Power alerts(uW)           : 83           5011           165             2511
Rx Power alerts(uW)           : 44           5011           89              2511
Last poll time: 06-20-2022 GMT Mon 22:09:21
```

12.2.8.2 CLI Command Usage/Help Menu Changes in FOS v9.2.0

In FOS v9.2.0, the CLI help/usage command format is updated to comply with industrial standards.

The changes are made as per the below table:

Notation	Description
Text without brackets or braces	Items you must type as shown.
<Text inside angle brackets>	Placeholder for which you must supply a value.
[Text inside square brackets]	Optional items.

Vertical bar (|)	Separator for mutually exclusive items. You must choose one.
Ellipsis (…)	Items that can be repeated and used multiple times.

12.2.8.2.1 Fabric OS Compatibility

Since the change is limited to “help” text, no compatibility issues are expected. In some extreme cases a user may have scripted a parser for the help text and such scripts might be adversely impacted.

12.2.8.3 Chassisshow Displays HW Version

In FOS v9.2.0 the command `chassisshow` will display the FPGA hardware version for all the blades and fixed-port switches.

Example:

```
Switch:FID128:admin> chassisshow
 Chassis Family:                       X6-8
…
 SW BLADE  Slot: 3
 Hardware Version:   2
…
```

12.2.8.4 OUI List Updated with New UCS FI Modules

In FOS v9.2.0 the OUI list is updated with new UCS Fabric Interconnect OUIs for automatic identification of UCS uplinks.

The OUI list is updated based on the changes made to the list of OUIs maintained by IEEE Registration Authority.

12.2.8.5 Microsoft Windows Server, NPS, LDAP and Global Catalog

FOS v9.2.0 is tested with NPS, LDAP/GC on Windows Server 2019 and 2022 schema 88 with certificate support.

Support for previous versions of Microsoft LDAP is deprecated.

12.2.8.6 Clear-Link Diagnostics

From FOS v9.2.0 onwards, D-Port test will perform only link traffic test, E/O wrap is obsolete together with link distance measurement.

The electrical loopback test, optical loopback test and the link distance measurement features are obsoleted (for distances less than 1000m) in CLI and in REST interface as well. Obsoleting these features supersedes all the feature combinations within the D-port such as Static/Dynamic/On Demand subset of features.

12.2.8.7 SNMP MIB Include Objects for SFP PN and SN

From FOS v9.2 SFP Part Number and Serial Number is included in the FAEXT mib.

```
SwSfpStatEntry ::= SEQUENCE {
        swSfpTemperature  OCTET STRING,
        swSfpVoltage OCTET STRING,
        swSfpCurrent OCTET STRING,
        swSfpRxPower OCTET STRING,
        swSfpTxPower OCTET STRING,
        swSfpPoweronHrs Integer32,
        swSfpUnitId   Integer32,
        swSfpPartNum   SnmpAdminString,
        swSfpSerialNum SnmpAdminString
  }

  swSfpPartNum OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "This object identifies part number of SFP."
  ::= { swSfpStatEntry 8 }

  swSfpSerialNum OBJECT-TYPE
        SYNTAX SnmpAdminString
        MAX-ACCESS read-only
        STATUS current
        DESCRIPTION "This object identifies the serial number of SFP."
  ::= { swSfpStatEntry 9 }
```

12.2.9 Web Tools

12.2.9.1 Dark Mode

With FOS v9.2.0 dark mode (theme) is supported with Web Tools.

The user-selected theme will be applied to the entire application.

Dark mode is introduced for users who prefer reduced light emitted by device screens while maintaining the minimum color contrast ratios required for readability.

Dark mode is introduced with a toggle button in the user profile - popup dialog to switch the theme as per the user's preference. The selected theme reference will be persisted in the browser cache and retained in the next login.

From FOS v9.2.0 the following themes are supported:

Classic Theme:

This theme is with white background, which is used in all the previous releases. This is the default theme.

Dark Theme:

The dark mode design reduces the light emitted by device screens while maintaining the minimum color contrast ratios required for readability. The advantages of dark mode are, it enhances visual ergonomics by reducing eye strain, facilitating screens to adjust according to current light conditions and providing comfort of use at night or in dark environments.

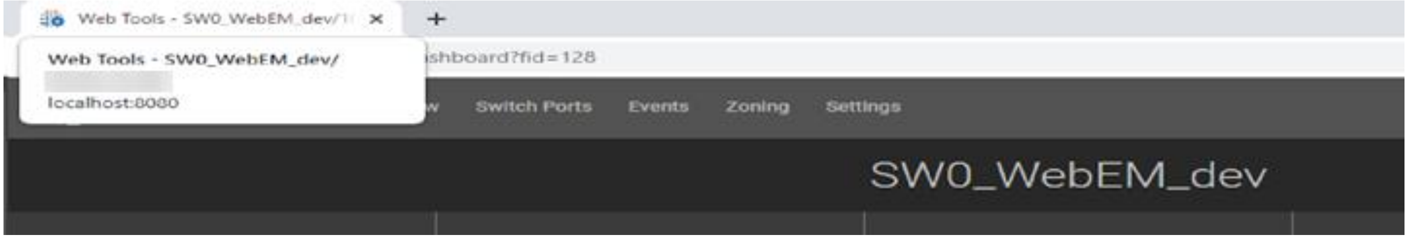
The dark mode theme changes the style of all scrollbars, chart background, legend and labels, investigation view, dropdown, popover, filters, tables related to all the activities and text colors, etc. The applied theme will reflect immediately, no need to start a new session.

The user-selected theme is persisted in the browser's cache.

12.2.9.2 Title Bar Displays Switch Name and IP Address

With FOS v9.2.0, after successful login with Web Tools, the browser's title bar will display Web Tools – Switch Name / Switch IP Address.

Example:

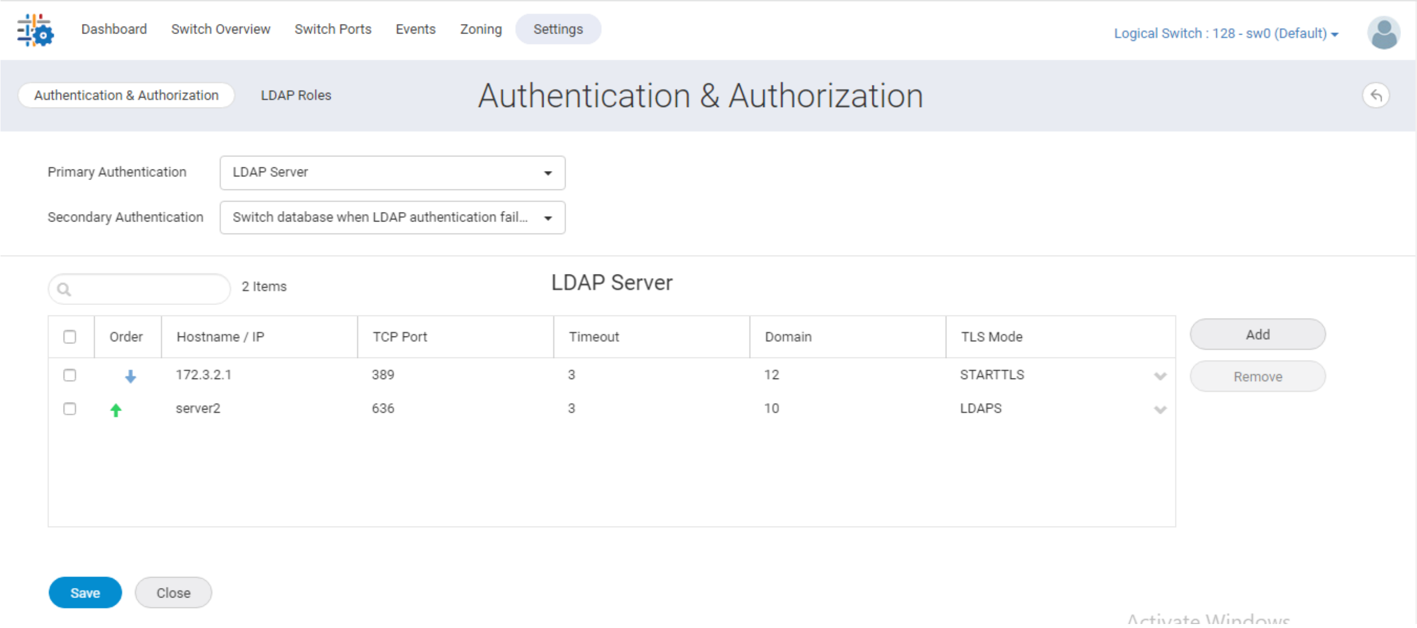


12.2.9.3 AAA Page Displays TLS Mode

With FOS v9.2.0, a new column called TLS Mode is added in the Authentication & Authorization section for the LDAP server table.

In pre-FOS v9.2.0, to view the TLS mode the user had to click on the configure option for the specific server. Now users can see the TLS mode straight away after navigating to the Authentication & Authorization page.

Example:



Primary Authentication: LDAP Server

Secondary Authentication: Switch database when LDAP authentication fail...

LDAP Server

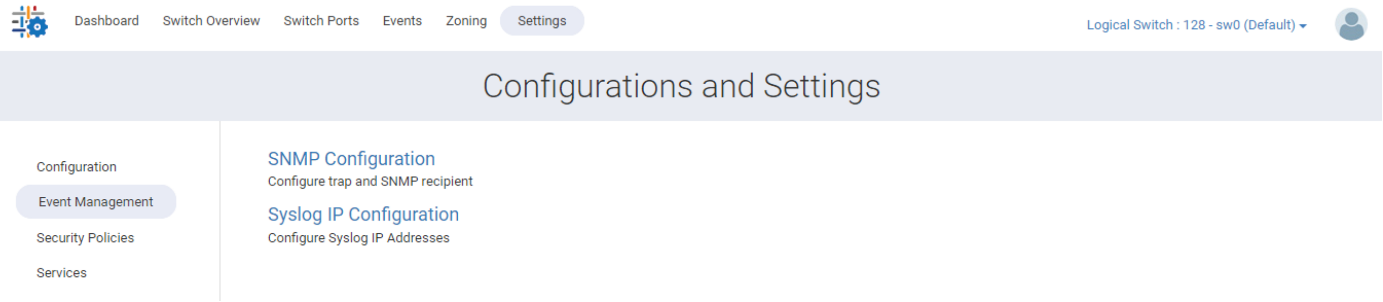
2 Items

□	Order	Hostname / IP	TCP Port	Timeout	Domain	TLS Mode
□	↓	172.3.2.1	389	3	12	STARTTLS
□	↑	server2	636	3	10	LDAPS

12.2.9.4 Syslog Panel Located under Event Management

With FOS v9.2.0, the syslog configuration settings are located under Event Management instead of IP Address Management. This is a more logical placement of syslog configuration management.

Example:



12.2.9.5 Display Warning when SNMPv3 User is Using Weak Cipher Protocols

The SNMPv3 authentication protocols, MD5 and SHA are deprecated. Hence a warning message is shown to the end user while configuring the weak cipher authentication protocols.

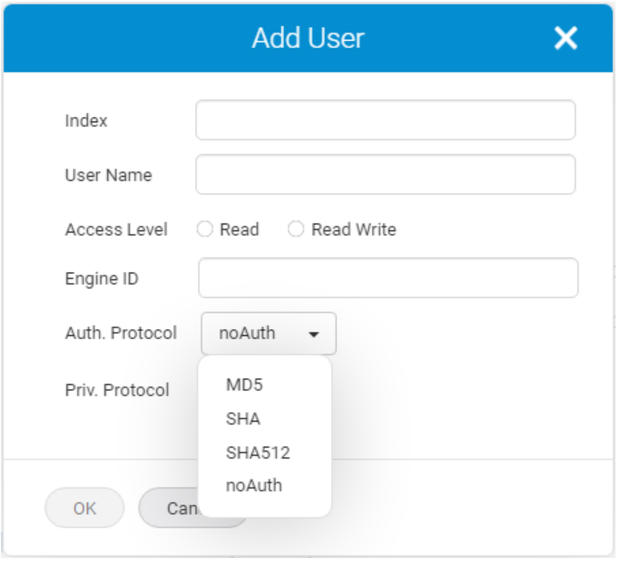
The SNMPv3 privacy protocol DES is deprecated. Hence a warning message is shown to the end user while configuring the weak cipher privacy protocol.

In addition, FOS v9.2.0 supports SHA512 authentication protocol for the snmpv3 user account and is supported for configuration with Web Tools.

End User Experience:

- When Adding / Configuring SNMP v3 users with Authentication protocol MD-5 or SHA, a warning message will be shown to indicate it is deprecated.
- When Adding / Configuring SNMP v3 users with Private protocol DES, a warning message will be shown to indicate it is deprecated.
- When Adding / Configuring SNMP v3 users new Authentication protocol SHA512 will be shown in the auth protocol dropdown

Example:



12.2.9.6 RBAC Enforcement in Web Tools

With FOS v9.2.0, Auth Mode is enabled by default (to configure Auth Mode use the command `mgmtapp –authmode`), which means only users with the following roles are allowed to login to Web Tools.

Auth Mode Enabled:

- Admin
- User
- Zone admin

The user privileges and functionality for the roles are unchanged.

NOTE In case a LS has a different user role than admin, user and zone admin, then that LS will not be listed in Web Tools.

Auth Mode Disabled:

When Auth mode is disabled all user roles are allowed to login from Web Tools, with the same privileges and functionality as in previous FOS releases.

End User Experience

Auth Mode Enabled (default):

Case 1: If any user role other than admin, user and zone admin tries to login.

- The user will be blocked in login screen
- The user will be notified with the following message:

  Login failed. This Account is restricted to login from Web Tools.

Case 2: If any of the LS has different roles other than admin, user or zone admin

- Only the LS with admin will be shown

Auth Modeis Disabled:

- No change in existing functionality

CLI Syntax:

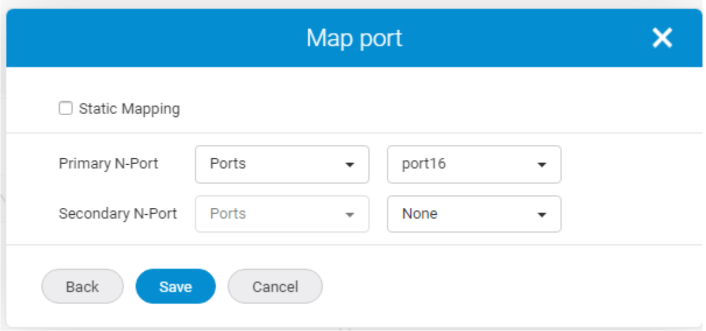
```
Switch:Switch:admin> mgmtapp --authmode enable

Switch:admin> mgmtapp --authmode disable
Warning: Auth mode disable is not secured,
Do you want to continue?  (yes, y, no, n): [no]y

Switch:admin> mgmtapp --authmode disable -force
```

12.2.9.7 AG – Port Mapping

With FOS v9.2.0, when defining Port Mapping of F-Ports on and AG the secondary N-port drop down menu includes the option to select None.

By default, the secondary N-port will have the value None.

Example:



Map port

□ Static Mapping

Primary N-Port: Ports, port16

Secondary N-Port: Ports, None

12.2.10 REST

12.2.10.1 CamelCase Support

Prior to FOS v9.2.0, REST was using a kebab case (hyphenated) for the REST names and URI. This is causing issues for end users running scripts with hyphenated names.

In FOS v9.2.0 REST is supported with camelCase without impacting any of the existing applications or scripts using kebab case (hyphenated).

REST supports camelCase using a new HTTP header parameter *Camel-Case-Mode*. This parameter takes two values *on* or *off*. (If no Camel-Case-Mode is mentioned, it is considered *off)*.

To receive REST output in the camelCase, input must be in the camelCase.

Same goes for the kebabCase as well.

Sample REST URI for the kebabCase:

```
/rest/running/brocade-maps/maps-policy
```

Sample REST URI for the camelCase:

```
/rest/running/brocadeMaps/mapsPolicy
```

12.2.10.2 REST API Changes in FOS v9.2.0

The following list provides an overview of REST API changes in FOS v9.2.0

URI	Summary of Changes
.../rest/running/brocade-access-gateway/port-group-mode	Refactoring
.../rest/running/brocade-access-gateway/n-port-map	Refactoring
.../rest/running/brocade-access-gateway/f-port-list	Refactoring
.../rest/running/brocade-access-gateway/policy	Refactoring
.../rest/running/brocade-chassis/chassis	New elements
.../rest/running/brocade-chassis/version	New elements
.../rest/running/brocade-chassis/ha-status	Refactoring
.../rest/running/brocade-chassis/management-interface-configuration	New elements
.../rest/running/brocade-chassis/management-ethernet-interface	Refactoring
.../rest/running/brocade-extension-ip-route/extension-ip-route	Refactoring
.../rest/running/brocade-extension-ipsec-policy/extension-ipsec-policy	Refactoring
.../rest/running/brocade-extension-tunnel/extension-tunnel	Refactoring
.../rest/running/brocade-extension-tunnel/extension-tunnel-statistics	Refactoring
.../rest/running/brocade-extension-tunnel/extension-circuit	Refactoring, New elements
.../rest/running/brocade-extension-tunnel/extension-circuit-statistics	Refactoring
.../rest/running/brocade-extension/lan-flow-statistics	Refactoring
.../rest/running/brocade-fdmi/hba	Refactoring
.../rest/running/brocade-fibrechannel-configuration/chassis-config-settings	Element removed (obsolete)
.../rest/running/brocade-fibrechannel-configuration/switch-configuration	Refactoring
.../rest/running/brocade-fibrechannel-configuration/f-port-login-settings	Refactoring
.../rest/running/brocade-fibrechannel-diagnostics/fibrechannel-diagnostics	Refactoring, Elements removed (obsolete)
.../rest/running/brocade-fibrechannel-logical-switch/fibrechannel-logical-switch	Refactoring
.../rest/running/brocade-fibrechannel-routing/routing-configuration	New element
.../rest/running/brocade-fibrechannel-routing/edge-fabric-alias	Backward-incompatible backend API change
.../rest/running/brocade-fibrechannel-switch/fibrechannel-switch	Refactoring
.../rest/running/brocade-firmware/firmware-config	Elements removed (obsolete)
.../rest/running/brocade-fru/blade	Refactoring, Add elements
.../rest/running/brocade-fru/sensor	Add elements
.../rest/running/brocade-fru/wwn	Added elements

.../rest/running/brocade-interface/gigabitethernet	Refactoring
.../rest/running/brocade-interface/fibrechannel	Refactoring, Add elements
.../rest/running/brocade-interface/fibrechannel-statistics	Refactoring
.../rest/running/brocade-license/ports-on-demand-license-info	Typedef refactoring
.../rest/running/brocade-logging/raslog	Remove elements
.../rest/running/brocade-logging/log-setting	Add elements
.../rest/running/brocade-logging/audit-log	Extensibility
.../rest/running/brocade-management-ip-interface/management-ip-interface	Add elements
.../rest/running/brocade-maps/system-resources	Add elements
.../rest/running/brocade-maps/maps-config	Deprecation; Add elements
.../rest/running/brocade-maps/rule	Deprecation; Remove elements
.../rest/running/brocade-maps/maps-policy	Add elements
.../rest/running/brocade-maps/monitoring-system-matrix	Deprecation; Add elements
.../rest/running/brocade-maps/quarantined-devices	New list
.../rest/running/brocade-media/media-rdp	Refactoring
.../rest/running/brocade-security/security-certificate-generate	Remove elements
.../rest/running/brocade-security/ssh-util-key	Exensibility; Add elements
.../rest/running/brocade-snmp/v1-account	Backend API change
.../rest/running/brocade-snmp/v3-account	Backend API change; Refactoring
.../rest/running/brocade-snmp/system	Backend API change
.../rest/running/brocade-traffic-optimizer/performance-group-profile	Add elements
.../rest/running/brocade-traffic-optimizer/partial-performance-group	New list
.../rest/running/brocade-usb/usb-file	Exensibility
.../rest/running/brocade-zone/effective-configuration	Refactoring; Add elements

12.3 Deprecated Software Features

- Boot LUN zones
- Fabric Assigned PWWN
- msConfigure

12.3.1 Deprecation of Boot LUN Zones

Support for Boot LUN zones is deprecated starting in FOS v9.2.0.

Deprecation/obsoletion will be done in two phases:

Phase 1:

Boot LUN zoning functionality will be honored in FOS v9.2.0. The `bootLunCfg` CLI will still function normally, but a warning message will be displayed to the user's terminal session:

```
Note: The Boot LUN zoning feature will be deprecated in a future version of Fabric OS.
Please plan accordingly.
```

In a future version of Fabric OS, Phase 2 (obsoletion) will occur.

Phase 2:

The `bootLunCfg` CLIs will be removed.

Firmware upgrade will not be permitted when Boot LUN zones exist in the zone database.

Boot LUN zones will not be allowed to be imported. A RASLOG will be posted and in certain cases, port segmentation will occur (e.g. zone merge cases) or loss of HA Sync will occur. Examples of blocked importation:

- Zone Merges
- Downlevel switch creation
- Configdownload operations (via CLI or Mgmt Interfaces)
- Firmware upgrade
- HA sync from a downlevel CP

12.3.1.1 Fabric OS Compatibility

Upgrade to FOS v9.2.0 no impact

Downgrade to pre-FOS v9.2.0 no impact

12.3.2 Deprecation of Fabric Assigned WWN (FA PWWN)

Support for Fabric Assigned PWWN (FA PWWN) is deprecated starting in FOS v9.2.0.

Deprecation/obsoletion will be done in two phases:

Phase 1:

FA PWWN functionality will be honored in FOS v9.2.0. The `fapwwn` CLI command will still function normally, but a warning message will be displayed to the user's terminal session:

```
Note: The FA PWWN feature will be deprecated in a future version of Fabric OS. Please
plan accordingly.
```

In a future version of Fabric OS, Phase 2 (obsoletion) will occur.

Phase 2:

The `fapwwn` CLI command will be removed.

Firmware upgrade will not be permitted when FA PWWN configuration exist on the switch.

FA PWWN configuration will not be allowed to be imported or configured/created.

Examples of blocked importation:

- Configdownload operations
- Firmware upgrade
- HA sync from a downlevel CP

12.3.2.1 Fabric OS Compatibility

Upgrade to FOS v9.2.0 no impact

Downgrade to pre-FOS v9.2.0 no impact

12.3.3 Deprecation of msConfigure

With the implementation of MS ACL (`portcfgmsacl`) in FOS v9.1.0, the `msConfigure` command was deprecated (phase 1) because it was overlapping/redundant.

In FOS v9.2.0 the command `msConfigure` is obsoleted and no longer available for execution.

12.3.3.1 Fabric OS Compatibility

Manageability Considerations

Upgrade to FOS v9.2.0 includes a preinstall check when upgrading to FOS v9.2.0 to prevent upgrade in case there is any configuration in msConfigure with the message `msConfigure is deprecated. Please remove all entries and transfer the configuration to portcfgmsacl.`

Chapter 13: Software License Support

13.1 Optionally Licensed Software

Fabric OS v9.2.x includes all basic switch and fabric support software, as well as optionally licensed software that is enabled via license keys or license files.

Optionally licensed features include:

Brocade Ports on Demand – This license allows customers to instantly scale the fabric by provisioning additional SFP ports via license key upgrade. (Applies to select switch models.)

Brocade Double Density Ports on Demand – This license allows customers to instantly scale the fabric by provisioning additional SFP-DD ports via license key upgrade. (Applies to select switch models.)

Brocade Q-Flex Ports on Demand – This license allows customers to further scale the fabric and increase flexibility by provisioning additional 4x32G QSFP ports via license key upgrade. (Applies to the Brocade G620 and G630 only.)

Brocade Extended Fabrics – This license provides greater than 10 km of switched fabric connectivity at full bandwidth over long distances (depending on the platform, this can be up to 3000 km).

Brocade ISL Trunking – This license provides the ability to aggregate multiple physical links into one logical link for enhanced network performance and fault tolerance. It also includes Access Gateway ISL Trunking on those products that support Access Gateway deployment.

Brocade Fabric Vision – This license enables support for MAPS (Monitoring and Alerting Policy Suite), Flow Vision, and ClearLink (D_Port) when connecting to non-Brocade devices. MAPS enables rules-based monitoring and alerting capabilities, and it provides comprehensive dashboards to quickly troubleshoot problems in Brocade SAN environments. Flow Vision enables host-to-LUN flow monitoring, application flow mirroring for nondisruptive capture and deeper analysis, and a test traffic flow generation function for SAN infrastructure validation. Support for D_Port to non-Brocade devices allows extensive diagnostic testing of links to devices other than Brocade switches and adapters.

NOTE On Brocade G620, G630, Brocade X6-8, and Brocade X6-4 platforms, this license enables the use of IO Insight capability. The license itself is identified as *Fabric Vision and IO Insight* on these platforms.

FICON Management Server – Also known as CUP (Control Unit Port), this license enables host control of switches in mainframe environments.

Integrated Routing – This license allows any Fibre Channel port in a Brocade X7-4, X7-8, G720, G730 and G620 to be configured as an EX_Port supporting Fibre Channel Routing (FCR).

Integrated Routing Ports on Demand – This license allows any Fibre Channel port in a Brocade 7810, G630, X6-8, or X6-4 to be configured as an EX_Port supporting Fibre Channel Routing. The maximum number of EX_Ports supported per platform is provided in the license.

ICL POD License – This license activates ICL ports on X6 or X7 platform core blades. An ICL license must be installed on the director platforms at both ends of the ICL connection.

On the Brocade X6-8:

The first ICL POD license enables 8 UltraScale ICL QSFP ports on each core blade of the X6-8 director, which are QSFP port numbers 0-3 and 8-11. The second ICL POD license enables all UltraScale ICL QSFP ports on each core blade of the director.

On the Brocade X6-4:

On the X6-4, the first ICL POD license enables 4 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0, 1, 4, and 5. The second ICL POD license enables all UltraScale ICL QSFP ports on each core blade of the director.

On the Brocade X7-8:

On the X7-8, the first ICL POD license enables 4 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0, 1, 8, and 9. The second ICL POD license on the X7-8 enables 8 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0-3 and 8-11. The third ICL POD license on the X7-8 enables 12 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0-5 and 8-13. The fourth ICL POD license on the X7-8 enables all UltraScale ICL QSFP ports on each core blade of the director.

On the Brocade X7-4:

On the X7-4, the first ICL POD license enables 4 UltraScale ICL QSFP ports on each core blade of the director, which are QSFP port numbers 0, 1, 4, and 5. The second ICL POD license on the X7-4 enables all UltraScale ICL QSFP ports on each core blade of the director.

On the Brocade 7810: The Extension Upgrade license is available on the Brocade 7810, enabling additional ports, capacity, and features that provide the following: 12 32Gb/s FC ports, 4 tunnels, 6 circuits per tunnel, 2.5Gb/s WAN throughput, Fabric Vision, Extension Trunking, Brocade ISL Trunking, Integrated Routing Ports on Demand, and Brocade Extended Fabrics. This license is shown as a combination of existing FOS licenses that enable the above capabilities and features.

13.2 Temporary License Support

The following licenses are available in Fabric OS v9.2.x as either universal temporary or regular temporary licenses:

- Fabric (E_Port)
- Extended Fabric
- Trunking
- Integrated Routing
- Integrated Routing Ports on Demand
- FICON Management Server (CUP)
- Fabric Vision
- Extension Upgrade

NOTE

- Temporary licenses for features available on a per-slot basis enables the feature for all slots in the chassis.
- There are no temporary licenses for the Brocade 7850 platform.

Temporary and universal temporary licenses have durations and expiration dates established in the licenses themselves. FOS will accept up to two temporary licenses and a single universal license on a unit. Universal temporary license keys can be installed only once on a particular switch, but they can be applied to as many switches as desired. Temporary use duration (the length of time for which the feature will be enabled on a switch) is provided with the license key. All universal temporary license keys have an expiration date after which the license can no longer be installed on any unit.

Temporary or universal temporary licenses for Extension Upgrade do not enable additional ports on 7810.

Chapter 14: Hardware Support

14.1 Supported Devices

The following devices are supported in this release:

- Brocade X7-8 Director
- Brocade X7-4 Director
- Brocade X6-8 Director
- Brocade X6-4 Director
- Brocade G730 Switch
- Brocade G720 Switch
- Brocade G630 Switch
- Brocade G620 Switch
- Brocade G610 Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade 7850 Extension Switch
- Brocade 7810 Extension Switch

14.2 Supported Blades

14.2.1 X6-8 and X6-4 Blade Support

Fabric OS v9.2.x software is fully qualified and supports the blades for the X6-8 and X6-4 as noted in the following table.

Blades	FOS v9.2.x Support
FC32-48 32G FC blade	Supported.
SX6 Gen 6 Extension blade	Supported. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE blade	Supported.

14.2.2 X7-8 and X7-4 Blade Support

Fabric OS v9.2.x software is fully qualified and supports the blades for the X7-8 and X7-4 as noted in the following table.

Blades	FOS v9.2.x Support
FC64-64 64G FC blade	Supported
FC64-48 64G FC blade	Supported.
FC32-X7-48 32G X7 FC blade	Supported.
FC32-48 32G FC blade	Supported.
SX6 Gen 6 Extension blade	Supported. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE blade	Supported.

14.3 Supported Power Supplies

For the list of supported power supplies for Brocade X6 and power supply requirements, refer to the Brocade X6 Director Technical Specifications section of *Brocade X6-8 Director Hardware Installation Guide* and *Brocade X6-4 Director Hardware Installation Guide*.

For the list of supported power supplies for Brocade X7 and power supply requirements, refer to the *Brocade X7 Director Technical Specification*.

14.4 Supported Optics

FOS v9.2.0 is the first release supporting the Gen 7FC QSFP+, PN:57-1000481-01 (XBR-000420) with serial number BAB1yywwxxxxxxxs.

When this optic is present and downgrade from FOS v9.2.0 is performed, the `firmwaredownload` will fail with the following error:

```
Downgrade is not allowed as some of the ICL ports are connected with GEN7 100M QSFPs.
Please remove the QSFP(s) flagged and retry firmwaredowngrade.
```

For a list of supported fibre optic transceivers that are available from Brocade, refer to the latest version of the *Brocade Transceiver Support Matrix* available online at www.broadcom.com.

Chapter 15: Software Upgrades and Downgrades

15.1 Platform Specific Downloads

This release of FOS is available for entitled equipment download in Platform Specific Download (PSD) form. FOS PSD releases provide a smaller version of the FOS image that can only be loaded on a single hardware platform, consisting of a single switch model or group of switch models. These FOS PSD images enable much faster download and file transfer times since they are between 65-90% smaller in size than traditional full FOS images.

Unlike traditional FOS release images that can be installed on any supported Brocade switch and director, FOS PSD images must be downloaded separately for each platform that the FOS release will be used on. The full list of unique FOS PSD images available for this release and the models that each PSD image supports is noted in section FOS Image Filenames.

15.1.1 Using FOS PSDs

FOS PSD images are generally used in the same manner as traditional full FOS release images.

Once loaded onto a switch, the FOS image running is identical to what would be in use if a traditional full image was used for the installation. Issuing a `firmwareshow` command on a switch will display only the FOS version level, with no indication of whether the code was loaded from a FOS PSD image or a full FOS image.

15.1.1.1 Loading FOS PSDs via Web Tools or FOS Command Line

Installing a FOS PSD image on a switch is performed in the same manner as using a traditional full FOS image. If a FOS PSD image is loaded on an incorrect switch model (for example, attempting to load a FOS PSD image for a Gen 6 entry level switch on a Gen 6 Director), the following error message displays:

```
Cannot download the requested firmware because the firmware doesn't support this
platform. Please enter another firmware.
```

15.1.1.2 Loading FOS PSDs via Brocade SANnav Management Portal

Brocade SANnav Management Portal v2.1.1 or earlier does not support FOS PSD images. However, FOS PSD images are supported with SANnav v2.1.1.3 and later releases. SANnav v2.1.1.3 and later can both host and install FOS PSD images onto Brocade switches.

15.2 FOS Image Filenames

Fabric OS v9.2.0c

Image Filename	Description
v9.2.0c.md5	Fabric OS v9.2.0c MD5 Checksums
v9.2.0c_all_mibs.tar.gz	Fabric OS v9.2.0c SNMP MIBs
v9.2.0c_EXT.tar.gz	Fabric OS v9.2.0c for Linux to install on 7810 and 7850 platforms
v9.2.0c_EXT.zip	Fabric OS v9.2.0c for Windows to install on 7810 and 7850 platform
v9.2.0c_EMB.tar.gz	Fabric OS v9.2.0c for Linux to install on G648 platform
v9.2.0c_EMB.zip	Fabric OS v9.2.0c for Windows to install on G648 platform
v9.2.0c_G6_ENTRY.zip	Fabric OS v9.2.0c for Windows to install on G610 platform
v9.2.0c_G6_ENTRY.tar.gz	Fabric OS v9.2.0c for Linux to install on G610 platform
v9.2.0c_G6_MID.tar.gz	Fabric OS v9.2.0c for Linux to install on G620 platform
v9.2.0c_G6_MID.zip	Fabric OS v9.2.0c for Windows to install on G620 platform
v9.2.0c_G6_ENTP.tar.gz	Fabric OS v9.2.0c for Linux to install on G630 platform
v9.2.0c_G6_ENTP.zip	Fabric OS v9.2.0c for Windows to install on G630 platform
v9.2.0c_G7_MID.tar.gz	Fabric OS v9.2.0c for Linux to install on G720 platform
v9.2.0c_G7_MID.zip	Fabric OS v9.2.0c for Windows to install on G720 platform
v9.2.0c_G7_ENTP.tar.gz	Fabric OS v9.2.0c for Linux to install on G730 platform
v9.2.0c_G7_ENTP.zip	Fabric OS v9.2.0c for Windows to install on G730 platform
v9.2.0c_G6G7_DIR.tar.gz	Fabric OS v9.2.0c for Linux to install on X6-8, X6-4, X7-8 and X7-4 platforms
v9.2.0c_G6G7_DIR.zip	Fabric OS v9.2.0c for Windows to install on X6-8, X6-4, X7-8 and X7-4 platforms
v9.2.0c.releasenotes_v8.0.pdf	Fabric OS v9.2.0c Release Notes

The image files for each respective platform can be downloaded from your switch vendor's website and https://support.broadcom.com/, except for YANG files which are available on https://www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system.

15.3 Migration Path

This section contains important details to consider before migrating to or from this FOS release. Refer to the *Brocade Fabric OS Software Upgrade User Guide* for detailed instructions on non-disruptive and disruptive upgrade procedures.

15.3.1 Migrating to FOS v9.2.0

The supported upgrade paths to Fabric OS v9.2.x are as follows:

Current Version	Upgrade Path
FOS v9.1.x	Nondisruptive upgrade (Install TruFOS certificate prior to upgrade to v9.2.0 if not already present on the switch)
FOS v9.0.x	Disruptive upgrade (Install TruFOS certificate prior to upgrade to v9.2.0 if not already present on the switch) Nondisruptive upgrade, first upgrade to FOS v9.1.x.
FOS v8.2.x	Nondisruptive upgrade: First upgrade from FOS v8.2.x to FOS v9.0.x. Then install TruFOS Certificate and proceed with upgrade to FOS v9.1.x.

15.3.2 Migrating from FOS v9.2.x

The following table lists the currently supported Fabric OS downgrade versions and platforms.

Table 1 Gen 6 and Gen 7 Platforms and Supported Firmware Downgrade Versions from Fabric OS v9.2.x

Platforms	Fabric OS v9.2.x	Fabric OS v9.1.x	Fabric OS v9.0.x	Fabric OS v8.2.x
Brocade Gen 7 (64G) Fixed-Port Switches				
Brocade G720 (Switch Type 181.0)	Supported	Supported	Supported	Not Supported
Brocade G720 (Switch Type 181.5)	Supported	Supported (Fabric OS v9.1.1 and later)	Not Supported	Not Supported
Brocade G730 (Switch Type 189.8)	Supported	Supported	Not Supported	Not Supported
Brocade Gen 7 (64G) Directors				
Brocade X7-4 Director	Supported	Supported	Supported	Not Supported
Brocade X7-8 Director	Supported	Supported	Supported	Not Supported
Brocade G610 (Switch Type 170.0 to 170.3)	Supported	Supported	Supported	Supported
Brocade G610 (Switch Type 170.4 or higher)	Supported	Supported	Supported (Fabric OS v9.0.1b and later)	Not Supported
Brocade G620 (Switch Type 162)	Supported	Supported	Supported	Supported
Brocade G620 (Switch Type 183.0)	Supported	Supported	Supported	Not Supported
Brocade G620 (Switch Type 183.5)	Supported	Supported (Fabric OS v9.1.1 and later)	Not Supported	Not Supported
Brocade G630 (Switch Type 173)	Supported	Supported	Supported	Supported
Brocade G630 (Switch Type 184)	Supported	Supported	Supported	Not Supported
Brocade 7810 Extension Switch	Supported	Supported	Supported	Supported (Fabric OS v8.2.1 and later)

Brocade G648 Blade Server SAN I/O Module	Supported	Supported	Supported	Supported
Brocade MXG610 Blade Server SAN I/O Module	Not Supported	Supported	Supported	Supported
Brocade X6-4	Supported	Supported	Supported	Supported
Brocade X6-8	Supported	Supported	Supported	Supported
Brocade X6-4 (Switch Type 165.5)	Supported	Supported (Fabric OS v9.1.0b and later)	Not Supported	Not Supported
Brocade X6-8 (Switch Type 166.5)	Supported	Supported (Fabric OS v9.1.0b and later)	Not Supported	Not Supported

15.4 Brocade Trusted FOS (TruFOS) Certificate

Brocade TruFOS Certificates are factory installed on applicable platforms shipping with FOS v9.x.
When upgrading to FOS v9.2x a valid TruFOS certificate is required for all platforms (except embedded switches).

FOS v9.2.0 is the first FOS version where TruFOS applies to the following platforms:

- G720
- 7850
- G620
- G610
- 7810

TruFOS certificate installation can be performed using SANnav or using the CLI command license as shown in the example below:

```
Switch:admin> license –install -h 10.10.10.10 -t ftp -u UserName -p Password -f
/20211013171159568_10_00_c4_f5_7c_64_5b_60.xml
License Installed [FOS-87-0-04-11209683]
```

NOTE When downgrading from FOS v9.2.0 MAPS TruFOS rules become unmonitored for the platforms listed above.

15.5 Upgrade/Downgrade Considerations

When upgrading a Gen 7 director or switch (X7-4, X7-8, G730, G720) to FOS v9.2.x, it is recommended to upgrade to FOS v9.2.0a or later. For additional information see TSB 2023-289-A.

In FOS v9.1.x (and later) when performing `firmwaredownload`, the HA reboot triggers the broadcast message: `The system is going down for reboot NOW!` This is a standard Linux message when a system is doing a graceful shutdown.

This is non-disruptive to I/O traffic during this process.

Example below:

```
Do you want to continue (Y/N) [Y]:
Firmware download in progress, please wait.
Broadcast message from root@Switch (Fri Aug 26 10:59:01 2022):
The system is going down for reboot NOW!
```

Refer to the *Brocade Fabric OS Software Upgrade User Guide* for detailed instructions on non-disruptive and disruptive upgrade procedures.

Chapter 16: Limitations and Restrictions

This chapter contains information that you should consider before you use this Fabric OS release.

16.1 Scalability

All scalability limits are subject to change. Limits may be increased once further testing has been completed, even after the release of this version of the Fabric OS software. For current scalability limits for Fabric OS software, refer to the Brocade SAN Scalability Guidelines for Brocade Fabric OS v9.X document.

16.2 Compatibility/Interoperability

This section describes important compatibility and interoperability across Brocade products.

16.2.1 Brocade SANnav Management Portal Compatibility

When managing SAN switches with SANnav Management Portal it is recommended to first upgrade SANnav Management Portal to v2.3.0 (or later) prior to upgrading SAN switches to FOS v9.2.0.

For details, review the latest SANnav Management Portal v2.2 Release Notes.

16.2.2 Web Tools Compatibility

Web Tools supports firmware migration to v9.2.x from FOS v9.1.x.

NOTE Web Tools will always show English language irrespective of Browser or Operating System language setting.

If a DSA algorithm is used for the HTTPS certificate, then Web Tools cannot discover the switch because all the supported ciphers for this algorithm are no longer supported.

16.2.3 Fabric OS Compatibility

- The following table lists the earliest versions of Brocade software supported in this release, that is, the earliest supported software versions that interoperate. Use the latest software versions to get the greatest benefit from the SAN.
- To ensure that a configuration is fully supported, always check the appropriate SAN, storage, or blade server product support page to verify support of specific code levels on specific switch platforms before installing on your switch. Use only Fabric OS versions that are supported by the provider.
- For a list of the effective end-of-availability dates for all versions of Fabric OS software, refer to the *Brocade Software End of Availability Notice* published to the Brocade Product End-of-Life web page https://www.broadcom.com/support/fibre-channel-networking/eol.

- For the latest support and posting status of all release of Brocade Fabric OS, refer to the *Brocade Software: Software Release Support and Posting Matrices* published to the Brocade Product End-of-Life web page https://www.broadcom.com/support/fibre-channel-networking/eol.

Supported Products	**Fabric OS Interoperability**
Brocade 5424, 5431, 5432, 5480, NC-5480	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 300	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 7800	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR) Note: There is no interoperability on VE interface(s) with another VE interface on a device running FOS v9.1.x (Brocade 7810 or Director with SX6 blade)
Brocade 7840	FOS v8.2.0 or later Note: When running FOS v8.2.1 or later there is interoperability on VE interface(s) with another VE interface on a device running FOS v9.1.x (Brocade 7810 or Director with SX6 blade)
Brocade DCX 8510-8/DCX 8510-4	FOS v8.2.x[2]
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS v8.2.x[2]
Brocade 6505, 6510, 6520, 7840	FOS v8.2.x[2]
Brocade 6542	FOS v8.2.x[2]
Brocade 6543	FOS v8.2.x[2]
Brocade 6547, 6548, M6505, 6545, 6546	FOS v8.2.x[2]
Brocade 6558	FOS v8.2.x[2]
Brocade G610 (switchType 170.0 to 170.3)	FOS v9.0.0 or later[3]
Brocade G610 (switchType 170.4 or higher)	FOS v9.0.1b or later
Brocade G620 (switchType 162)	FOS v9.0.0 or later[3]
Brocade G620 (switchType 183.0)	FOS v9.0.0 or later
Brocade G620 (switchType 183.5)	FOS v9.1.1 or later
Brocade G630 (switchType 173)	FOS v9.0.0 or later[3]
Brocade G630 (switchType 184)	FOS v9.0.0 or later
Brocade 7810	FOS v9.0.0 or later[3]
Brocade X6-8/X6-4	FOS v9.0.0 or later[3]
Brocade X6-8/X6-4 (switchType 166.5 and 165.5)	FOS v9.1.0b or later
Brocade G720 (switchType 181.0)	FOS v9.0.0 or later
Brocade G720 (switchType 181.5)	FOS v9.1.1 or later

[2] Only qualified with FOS v8.2.3x.

[3] While this platform is supported with FOS v8.x it is only qualified with FOS v9.0.0 or later.

Brocade G730 (switchType 189.8)	FOS v9.1.0 or later
Brocade X7-8/X7-4	FOS v9.0.0 or later
Brocade G648[4]	FOS v9.0.0 or later
Brocade MXG610[5]	FOS v9.0.1a or later

16.2.4 SNMP Support

Fabric OS v9.2.x documents the supported MIBs in the *Brocade Fabric OS MIB Reference Manual*. For information about SNMP support in Fabric OS software and how to use MIBs, refer to the *Brocade Fabric OS Administration Guide for Fabric OS v9.2.x*.

16.2.5 Obtaining MIBs

You can download the MIB files required for this release from the Downloads area of the support portal site. To download the Brocade-specific MIBs, you must have a username and password. Perform the following steps.

1. Go to https://support.broadcom.com/, click **Login**, and enter your username and password.

   If you do not have an account, click **Register** to set up your account.

2. Select **Brocade Storage Networking** in the support portal.

   Distribution of standard MIBs has been stopped. Download the required standard MIBs from the http://www.oidview.com/ or https://www.simpleweb.org/ietf/mibs/.

16.2.6 Flow Vision, IO Insight and VM Insight

- In FOS v9.2.x the VMID+ feature is supported with extended ISL (XISL) usage on logical switches.
- The VMID+ feature is not supported with Fibre Channel Router (FCR).
- Configuring an EX_Port and F_Port with the application header on the same chassis is not supported in VF and non-VF mode. However, the configuration is not blocked.
- The VMID+ feature is not supported on FICON logical switch ports.
- Enabling the VMID+ configuration on F_Ports connected to encryption-supported third-party devices is not supported.

[4] Brocade G648 is also supported with FOS v8.2.0_gft release.

[5] Brocade MXG610 is also supported with FOS v8.1.0_lnx2, v9.0.1a, and v9.1.0b.

16.2.7 REST API Support

Fabric OS v9.2.x documents the supported REST API functions in the *Brocade Fabric OS REST API Reference Manual*.

16.2.7.1 Obtaining YANG Files

YANG is a standard data modelling language that defines the data sent over the FOS REST API. Each FOS REST API module is defined in a YANG module file with a .yang name extension. To download the Brocade FOS-specific YANG files from the Broadcom website, perform the following steps:

1. Go to https://www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system/.
2. Select **Downloads**.
3. The YANG files can be located under the Yang Modules.
4. Unzip or untar the Fabric OS package file; the `yang.tar.gz` file contains the collection of YANG module files that this FOS release version supports. Untar the `yang.tar.gz` file to obtain individual YANG module files.

   Alternatively, the YANG modules for a specific FOS version can be downloaded from https://github.com/brocade/yang.

16.3 Important Notes

Brocade recommends to always review Important Notes for each release.

16.3.1 4G Support on Gen 6 Switches

The Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades do not support 4G EX-Port.

Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades support 4G E-Port connected between those three only (switchType 183, 184 and FC32-X7-48).

16.3.2 Access Gateway

- The 32G links with 4x32G QSFP ports (port 48 to port 63) do not have default mappings. These ports will be disabled by default when a Brocade G620 is enabled for Access Gateway mode or when the configuration is set to the default.
- Attempts to remove failover port mapping from N_Port number 0 on an Access Gateway fail. This problem does not exist on other N_Port numbers.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades do not support N-port connection from 4Gbps Access Gateway.

16.3.3 Brocade Analytics Monitoring Platform

FOS v9.2.x supports vTap on Brocade legacy Gen 6 platforms to be monitored by the Brocade Analytics Monitoring Platform. The supported Brocade platforms include: G610, G620, G630, X6-4, and X6-8.

16.3.4 ClearLink Diagnostics (D_Port)

Fabric OS v9.2.x supports D_Port tests between two Brocade switches and between Brocade switches and Gen 5 (16Gb/s), Gen 6 (32Gb/s), and Gen 7 (64Gb/s) Fibre Channel adapters from QLogic and Emulex.

NOTE From FOS v9.2.0, Electrical and Optical loopback tests are deprecated from D-Port test functionality and CLI output. Link distance is only provided for distances over 1000 meters.

The following are specific adapter models and driver versions supported by Brocade with Fabric OS v9.2.x for ClearLink Diagnostics.[6]

	Emulex 16G Adapter	Emulex 32G Adapter	Emulex Gen 7 Adapter	QLogic 16G Adapter	QLogic 32G Adapter
Adapter Model	LPe16002B-M6	LPe32002-M2	LPe35002 LPe35004 LPe36000	QLE2672	QLE2742
Adapter Firmware	12.8.542.25	12.8.542.26	12.8.542.xx	v8.08.231	V9.0.6.02
Adapter Driver	12.6.165.0	12.6.165.0	12.6.165.0 12.8.351.x	STOR Miniport 9.4.4.20	STOR Miniport 9.4.5.20

D_Port tests will fail between a port with a 64G optic on a switch or director operating with FOS v9.0.1b and a port on a G720, X7, G620 (switchType 183), or G630 (switchType 184) operating with FOS v9.0.0x. Any of these platforms operating with FOS v9.0.0x should be upgraded to FOS v9.0.1a or later prior to running D_Port tests to a 64G optic.

16.3.5 DDNS

Enabling and disabling the DDNS for IPv6 are disruptive operations which leads to DHCPv4 management IP change. Enabling this operand without caution will lead to losing all active SSH sessions due to IP address change. The users can login back to the switch only after finding the newly leased DHCPv4 address using the serial console.

NOTE When using MS Windows DHCP server, DNS should be configured on the switch (static or dynamic) for IPv6 DDNS feature to work with the Windows DHCP server.

16.3.6 Diagnostic POST

If Diagnostic POST is enabled, `supportSave` should not be started until the POST tests are completed after a switch or director boots up. Starting `supportSave` collection when POST tests are still running can result in unpredictable behaviour.

[6] Adapter firmware or driver versions that are later than the ones listed in the table may not work.

16.3.7 DWDM

- For best performance and resiliency when deploying native FC ISLs over DWDM, best practice is to deploy distinct ISLs over DWDM with in-order delivery (iodset) configured on the switches.
- Trunking over DWDM is not recommended or supported by Brocade due to the risk of out-of-order frame delivery. Trunking relies on deterministic deskew values across all trunked links to provide in-order delivery as well as FC primitives for trunk formation. These deskew values cannot be guaranteed with DWDM equipment in the path.
- Use of trunking over DWDM links should only be done when validated and supported by the DWDM vendor.
- With Gen 7 switches, the permitted deskew (variance in latency due to difference in cable length) is less at 64G compared to lower interface speeds.

16.3.8 Ethernet Management Interface

- The recommended interface speed configuration for a Brocade Gen 6 or Gen 7 switch or director chassis is 1G auto-negotiate.
- If a Brocade switch management interface is running at 10 Mb/s, certain FOS operations such as `firmwaredownload` may fail.
- The 10Gb/s management interface on CPX6 blades is not supported.
- Half-duplex mode is not supported in FOS v9.x and is blocked.
- The `ethif --reseterror` command option is supported in FOS v9.1.x and later.

16.3.9 Extension

Extension between a Brocade 7810 or SX6 running FOS v9.x and a Brocade 7840 is supported only if the 7840 is running FOS 8.2.1 or later. The following table documents the combinations.

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware
7840	8.2.1 or later	7840	8.2.1 or later
SX6	9.0.0 to 9.1.x	7840	8.2.1 or later
7810	9.0.0 to 9.1.x	7840	8.2.1 or later

16.3.9.1 Fabric OS Compatibility

The Brocade 7850 platform is only interoperable with 7810 and SX6 platforms running FOS v9.2.0 (or later) for VE link interoperability.

Config upload and config download will behave the same as existing extension platforms.

The main restriction regarding `configdownload` is the file being downloaded must have a matching VE-Mode configuration. This is the same behavior as SX6. When applying the new `configdownload` file, the switch must be rebooted to apply the config. Without a reboot, the switch will remain in the previous state operationally. No extension configuration changes will be allowed after the `configdownload` is performed until the reboot is performed.

NOTE The extension platforms 7840 and FX8-24 cannot form an FCIP tunnel to an extension platform running FOS v9.2.0.

16.3.10 FCoE

The following topologies for FCoE on the FC32-64 are not supported with FOS v9.2.x:

- Cisco UCS server directly connected to the FC32-64 without a Fabric Interconnect module.
- Cisco UCS server with a Fabric Interconnect module connected to the FC32-64 via a Nexus 5000 series switch in between. Neither running FCoE NPV mode nor L2 switching mode on the Nexus 5000 is supported.
- FCoE devices are supported in edge-to-edge fabric topology. They are not supported in edge-to-backbone fabric topology over FCR configurations.

16.3.11 FC-NVMe

- FC-NVMe is supported in edge-to-edge fabric topology with device type information (e.g. Initiator or Target) over FCR configurations.
- FC-NVMe is supported in edge-to-backbone fabric topology without device type information over FCR configurations.

16.3.12 Firmware Migration

When doing staged firmware download migration from FOS v9.0.x to FOS v9.2.0 using `firmwaredownload -r` option if there is any explicit expected or unexpected switch reboot before the firmware is activated it can result in the switch or chassis being in an unrecoverable state. Consequently, the system will end up in an erroneous state and will not be able to boot up correctly.

NOTE

- This only applies when starting from FOS v9.0.x. When performing staged `firmwaredownload` migration starting from FOS v9.1.x to FOS v9.2.0 this does not apply.
- When upgrading deployments with FCoE (UCS FI connected with Ethernet Uplinks) from FOS v9.1.0x the following order must be followed to ensure non-disruptive upgrades:
  FOS v9.1.0x -> v9.1.1x -> v9.2.0x in order to retain FCoE logins and traffic during the upgrade process.

16.3.13 Forward Error Correction

- FEC is mandatory with Gen 6 and Gen 7 Fibre Channel operating at 32Gb/s or higher bandwidth. This means that the `portcfgfec` command applies only to ports that are running at 16Gb/s or 10Gb/s.
- FEC capability is not supported with all DWDM links. This means that FEC may need to be disabled on 16Gb/s or 10Gb/s ports when using DWDM links with some vendors. This is done using the `portcfgfec` command. Failure to disable FEC on these DWDM links may result in link failure during port bring-up. Refer to the *Brocade Fabric OS v9.x Compatibility Matrix* for supported DWDM equipment and restrictions on FEC use.

16.3.14 FPGA Upgrade

When deploying the Gen 7 Fibre Channel 2KM QSFP (XBR-00476) for ICLs on Brocade X7, the Field Programmable Gate Array (FPGA) on each Core Routing blade (CR64) must be upgraded. If a Gen 7 Fibre Channel 2KM optic is plugged into CR64 blade with a down level FPGA version the RAS-LOG BL-1087 is displayed.

Example:
```
[BL-1087], 2973/525, SLOT 1 | CHASSIS, CRITICAL, X7-4, FPGA in slot 5 should be upgraded to support the Gen7 ICL QSFP for blade ID 214.
```

From FOS v9.1.1 (and later), the FPGA upgrade can be performed non-disruptively by upgrading the CR64 blades one by one.

The upgrade process can take up to 20 minutes per CR64 blade.

NOTE If for any reason the FPGA upgrade fails it is recommended to reissue the upgrade steps, do NOT power-cycle the director or the affected slot.

16.3.14.1 FPGA Upgrade (for FOS v9.1.1 and later)

To upgrade the FPGA on the CR64 blades perform the following steps:

1. Perform the following command to verify current FPGA code level `fpgaupgrade --latest`
2. Verify the *current* FPGA code level is lower than 0x01.0a for the CR64 blade slots
   - Slot 7 and 8 on X7-8
   - Slot 5 and 6 on X7-4

   After verification proceed to the next step.
3. Verify both CR64 blades are online with the command `slotshow.`
4. Prepare for upgrade of the FPGA on the first CR64 blade with the command `portdecom <ICL port> -qsfp` perform this for all connected E-ports (ICL ports) on the CR64 blade.
5. Disable the first CR64 blade on which the ICL ports were decommissioned in the previous step `portdisable -s <core blade slot #>.`
6. Upgrade the FPGA on the first CR64 blade with the command `fpgaupgrade -s <core blade slot #>`
   a. Respond `Yes` to automatically power-off and power-on the blade.
      (i) `Do you want to power-off and power-on the slot # automatically, after FPGA and/or CPLD upgrade (y/[n])?:`
   b. In case you respond `No` to automatically power-off and power-on the blade perform these steps manually.
      (i) `slotpoweroff <core blade slot #>`
      (ii) `slotpoweron <core blade slot #>`
7. Verify the FPGA on the first CR64 blade is upgraded with the command `fpgaupgrade –latest.`
   a. Verify the FPGA code level is 0x01.0a
8. Enable the first CR64 blade with the command `portenable -s <core blade slot #>` (as needed).
9. Persistently enable all ICL ports on the CR64 blade (which were disabled in step 5 prior to the upgrade) `portcfgpersistentenable <ICL port>.`

   Repeat this step for all connected E-ports (ICL ports) on the CR64 blade.
10. Verify the ICL ports are online with the command `switchshow.`
11. Repeat steps 4 through 11 on the second CR64 blade.

    The FPGA upgrade is now complete.

16.3.15 Optimized Credit Model for G630 and X7-8/4

The following only applies to G630 (SWDB 184) and X7-8, X7-4 provisioned only with the following blades:

- FC32-48
- FC32-64
- SX6

If any Gen 7 blades are present in the X7 director the credit model optimization does not apply.

FOS v9.2.0c optimized credit model for credit stall and over subscription flows is available for the above mentioned platforms and recommended to be configured.

To verify if the optimized credit model is already applied execute the following CLI:

```
fossystem --show -qos 1
```

If the credit model is already optimized, the following is returned:

```
System is optimized for credit stall and over subscription flows.
```

If the credit model is not optimized, the following is returned:

```
System is not optimized for credit stall and over subscription flows.
Use --set command to optimize the flows.
```

In this case run the following command to optimize the credit model.

Example:

```
Switch:FID128:maintenance> fossystem --set -qos 1
fossystem success
Switch:FID128: maintenance > fossystem --show -qos 1
System is optimized for credit stall and over subscription flows.
```

16.3.16 MAPS

In FOS v9.2.0c3 (and later versions of FOS v9.2.0x), MAPS SNMP trap forwarding to SANnav v2.4.0 (and later) is suppressed when:

- MAPS Quiet Time is configured (QT or AQT)
- MAPS Action is not configured for MAPS SNMP trap forwarding.

Resulting in the desired behavior as the violation alerts will not appear in SANnav.

NOTE In environments where SNMP trap forwarding to SANnav is desired, but MAPS Action has not been configured this must be performed before or after upgrade to FOS v9.2.1b using the command `mapsconfig --actions SNMP`.

First issue the command `mapsconfig –show` to list configured MAPS Actions, then add the SNMP action to the list.

Example:

```
switch:admin> mapsconfig –show
Configured Notifications:
RASLOG,EMAIL,SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL,FPIN,HA_RECOVER
```

------ Truncated -------

```
switch:admin> mapsconfig –actions
SNMP,RASLOG,EMAIL,SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL,FPIN,HA_RECOVER

switch:admin> mapsconfig –show
Configured Notifications:
SNMP,RASLOG,EMAIL,SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL,FPIN,HA_RECOVER
```

------ Truncated -------

NOTE SANnav 2.4.0 (and later) managing switches running FOS versions prior to v9.2.0c3 will still receive MAPS SNMP traps regardless of MAPS QT/AQT or MAPS Action configuration.

16.3.17 OUI

The OUI (Organizationally Unique Identifier) B8:CE:ED (for example, 10:00:B8:CE:ED:xx:xx:xx) introduced with newer switches is not supported in topologies using AG or FCR with FOS v9.2.0c1, v9.2.0c2 or v9.2.0c3.

Support for the OUI is available with upgrade to FOS v9.2.0c4 or later.

16.3.18 Security

In this section important security notes relevant to FOS v9.2.x are listed.

Default Secure

Platforms shipping with FOS v9.2.x from factory have Default Secure enabled. This means that unsecure protocols are blocked, and stronger cryptographic settings are applied. For more details see the *Brocade Fabric OS Administration Guide for Fabric OS v9.2.x*.

Default Session Limit

Default session limit is increased to 12 for local admin and maintenance accounts. The session limit is shared between the two accounts.

OU Field in FOS Switch CSRs No Longer Available

Effective August 24, 2022, the OU field will no longer appear in order forms for digital certificates, will be ignored in API requests, and will not be included in all new, renewed, and reissued public TLS/SSL certificates. This is due to a change by the CA/Browser forum, who dictates and issues guidelines to all Certificate Authority vendors. Accordingly, FOS v9.2.x is enhanced to adhere to the change imposed by CA/Browser forum.

This applies to certificates but excludes CA certificates. The OU field is removed in CSRs, self-signed certs, and a warning will be displayed on imports if the OU field is present.

Example of the Warning message:

```
FID128:admin> seccertmgmt import -cert https
Select protocol [ftp or scp]: scp
Enter IP address: 10.10.10.10
Enter remote directory: <certificate path>
Enter certificate name (must have ".crt" or ".cer" or ".pem" suffix):10.10.10.10-web.pem
Enter Login Name: <server username>
<user>@192.0.2.1's password:
```

Enter certificate name (must have `.crt` or `.cer` or `.pem` suffix)`:10.10.10.10-web.pem`)

WARNING Imported certificate contains OU field, which is deprecated starting with Fabric OS v9.2.0 based on the recommendations form CA/Browser forum.

Excerpt of certificate with OU field:

```
openssl x509 -in signed.10.10.10.10-web.pem -text -noout
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 1 (0x1)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Brocade, OU = test, CN =
192.0.2.1, emailAddress = name@domain
        Validity
            Not Before: Jul 27 14:16:38 2016 GMT
            Not After : Jul 27 14:16:38 2017 GMT
        Subject: C = US, ST = California, L = San Jose, O = Brocade, OU = Demo, CN =
CA@demo
```

Excerpt of certificate without OU field:

```
openssl x509 -in 10.10.10.10-web.pem -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 4098 (0x1002)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Brocade, CN = 10.10.10.10,
emailAddress = name&domain
        Validity
            Not Before: Apr 14 13:41:43 2023 GMT
            Not After : Apr 11 13:41:43 2033 GMT
        Subject: C = US, ST = California, O = Brocade, CN = 10.10.10.10, emailAddress =
name@domain
```

The Following Security Enhancements All Apply to FOS v9.x

- FOS v9.x requires passwords for admin and user accounts to be changed from the default password string "password". In the following scenarios, default password may still be present in FOS v9.0.x and v9.1.x. It is recommended to change the password in this scenario or at the next login prompt:
  - A default password is used in an earlier FOS version (prior to v9.0.0). FOS is upgraded from the earlier FOS version to FOS v9.x.
  - A default password is used in an earlier FOS version on active CP. The standby CP runs FOS v9.x and becomes active due to HA failover.
  - A default password is used in an earlier FOS version. Password is distributed from the earlier FOS version to FOS v9.x.
- It is recommended to reconfigure shared secrets for F_Port authentication between Access Gateway and switch before firmware upgrade to FOS v9.x. The shared secrets should be configured as given in the following table.

Access Gateway FOS Version	Edge Switch FOS Version	Shared Secret Configuration
Pre-9.0.0	9.0.0 or later	AG local secret = Switch local secret AG peer secret = Switch peer secret
9.0.0 or later	9.0.0 or later	AG local secret = Switch peer secret AG peer secret = Switch local secret

- It is recommended to reconfigure shared secrets for F_Port authentication between HBAs and a switch before the switch is upgraded to FOS v9.0.0 or later. Without reconfiguration, shared secrets configured in earlier FOS versions will fail F_Port authentication when a device port resets. The shared secrets should be configured as given in the following table.

FOS Version	Shared Secret Configuration
Pre-v9.0.0	Device local secret = Switch local secret Device peer secret = Switch peer secret
9.0.0 or later	Device local secret = Switch peer secret Device peer secret = Switch local secret

- FOS v9.x does not support F_Port authentication to Marvell QLogic BR series (Former Brocade Product Line) HBAs as these HBAs only support legacy Brocade F_Port authentication. For these devices to connect to FOS v9.x, F_Port authentication must be disabled.
- FOS v9.x does not support F_Port trunking when F_Port authentication is enabled.
- Prior to upgrading to FOS v9.x:
  - First, ensure the secrets on both the switches (E-port authentication) are not the same. Otherwise, the E-port will segment after the upgrade to v9.x
  - Secondly, reconfigure shared secrets to be in compliance with FC-SP 2 standard

    If users configure any duplicated Virtual Fabric (VF) list with `ldapcfg –mapattr <ldaprole>` command, only the first mapping from the list will be used during LDAP authentication and authorization.

- FOS v9.x requires role mapping or VSA attributes to be configured for LDAP user authentication in a VF-enabled switch. In a non-VF switch, `ldapcfg --maprole` is mandatory. It should be configured before upgrading to FOS v9.x to avoid login failure for LDAP users.
- Users must specify the domain of an LDAP server when adding the LDAP server to the remote AAA configuration of a switch.
- Optional certificate extensions, such as BasicConstraints, KeyUsage, and ExtendedKeyUsage are ignored when a certificate containing these is imported in basic mode. During session establishment, the extensions are validated. Hence, invalid extensions will be rejected and result in session failure.
- Login of LDAP users using Distinguished Name (DN) will be supported only for the users created in container "Users" of the domain configured in the switch, even though the switch is configured with Global Catalog (GC) port of the

server. Login using User Principal Name (UPN) and sAMAccountName will be supported irrespective of the domain and OU on which the user is created.

16.3.18.1 Syslog

When using non secure syslog server configuration in FOS 9.1x and upgrading to FOS v9.2x the `cfgload.secure` configuration setting should be verified prior to upgrade. When this setting is set to 1 non secure syslog is no longer permitted after upgrade to 9.2x.

Example, verifying `cfgload.secure` setting:

```
Switch:FID128:admin> configure --show -mod CHS
Key Name                                                                  Value
Add Suffix to the uploaded file name(cfgload.cfgfile_suffix)                  0
Do you want to enable auto firmwaresync(cfgload.firmware_sync)                1
Enable secure switch mode(cfgload.secure)                                     1
```

When the `cfgload.secure` setting is set to 1 the end user must make the following decision:

- Move to using a secure syslog server (this is the recommended best practice)

Or

- Change the `cfgload.secure` setting to 0, prior to upgrade to FOS v9.2x

To change the cfgload.secure setting to 0 use the command `configure --set -mod CHS -key cfgload.secure -value 0`

Example, configuring `cfgload.secure` setting to 0 and verifying:

```
Switch:FID128:admin> configure --set -mod CHS -key cfgload.secure -value 0

Switch:FID128:admin> configure --show -mod CHS
Key Name                                                                  Value
Add Suffix to the uploaded file name(cfgload.cfgfile_suffix)                  0
Do you want to enable auto firmwaresync(cfgload.firmware_sync)                1
Enable secure switch mode(cfgload.secure)                                     0
```

Setting `cfgload.secure` to 0, also implies that FTP and HTTP protocols are permitted in FOS. These protocols can be blocked using IPFilter policy.

16.3.19 Zoning

When performing configdownload with a file that contains unsorted zone membership, any unsorted members will be automatically sorted in the system when configdownload completes. As a result, when a switch is later re-enabled, port segmentation may occur due to adjacent switches having the same zones with unsorted membership lists. Users can recover from segmentation by executing cfgDisable, cfgClear, and cfgSave operations in order to clear the zoning database from the switch that just performed configdownload. After segmented ISL ports are re-enabled, zone merge can proceed.

NOTE These steps should ONLY be performed if the zone database is the same on the configdownload switch as it is on the rest of the fabric.

16.3.20 Brocade X6 Field Migration

- Field migration of a Brocade X6 switch to an upgraded X6 with Gen 7 support is not supported in FOS v9.2.x. In case a Brocade X6 switch is running FOS v9.2.x and it is desired to migrate to an upgrade X6 with Gen 7 support it is required to first downgrade to FOS v9.1.x and then perform the migration.

- FOS v9.1.x is the last release which supports a field migration of a Brocade X6 switch Type 165.5 and 166.5 to an upgraded X6 with Gen 7 support.
- Field migration of a Brocade X6 (switch Type 165 and 166) to an upgraded X6 with Gen 7 support is available with FOS v9.0.0x, FOS v9.0.1x and FOS v9.1.x.

  Refer to the *Brocade X6 Field Migration Guide* for step-by-step instructions.
- During field migration of Brocade X6 to a field upgraded X6 with Gen 7 support, the `portcfgupload` file will contain `portcfgtrunkport` commands for ICLs. A warning message is displayed to indicate that the command is not valid for ICL ports because trunking cannot be disabled on ICLs. This warning will not affect the ICLs and is harmless.

16.3.21 Miscellaneous

- After a power supply unit is removed from a Brocade G620, the historyshow command may miss the entries for this FRU removal or insertion event. In addition, the RASLog error message EM-1028 may be logged when the power supply is removed. This condition can be corrected by power-cycling the switch.
- After running offline diagnostics mode 1 on QSFP ports, a Brocade G620 must be rebooted before operational use.
- After running offline diagnostics with `portledtest`, `portloopbacktest`, or `turboramtest` commands on FOS v9.x, Brocade G630 with `swtichType` 184 must be rebooted before operational use.
- All links in an ICL QSFP connection on a Brocade X6 Director must be configured to the same speed using the `portcfgspeed` command from one of the following supported speeds: 16Gb/s, 32Gb/s, or ASN. To connect an ICL from an X6 with a 4x32GFC breakout optic (P/N 57-1000351-01) or a 4x16G FC optic to a 4x16G FC optic in a DCX 8510, the X6 port's speed must be set to 16Gb/s.
- Brocade G630 LEDs illuminate amber and green during power-up.
- The CLI command option `snmpconfig -set accesscontrol` is planned to be deprecated in the next major release.
- When replacing a FC32-64 blade with a FC32-48 blade, flexport and FCoE configurations should be removed before the FC32-64 blade is removed.
- Enhanced checks are performed on optics during firmware upgrade to FOS v9.0.0 or later. Firmware download is blocked if unsupported optics are discovered. The scanning of the optics takes a few minutes to complete. The amount of time it takes is dependent on the number of ports on a switch. On a fully loaded eight (8) slot director, it can take up to five (5) minutes to complete. In addition, ports with optics that fail the enhanced checks in FOS v9.x will not be able to come online due to the optics as invalid module.
- Brocade G620 with `switchType` 183 and G630 with `switchType` 184 do not support the following legacy optical modules:
  - 16G SWL (HAA1, HAA2 serial number)
  - 16G LWL (HDA1, HDA2, HDA3 serial number)
  - 32G QSFP SWL (ZTA serial number)

    The following examples show the `sfpShow` CLI outputs with the serial numbers of the legacy optical module

    ```
    sfpshow <port> -f
    ...
    Serial No: HAA11213107BTY2
    ...

    sfpshow <port> -f
    ....
    Serial No: HDA318014000DN1
    ....

    sfpshow <port> -f
    ....
    Serial No: ZTA11517000001K
    ```

- All user ports in a Gen 7 ICL QSFP port must be assigned to the same logical switch when Virtual Fabric is configured. Port 0 of the ICL QSFP must be enabled first before port 1, port 2, and port 3 within the same QSFP to be enabled. If port 0 of the Gen 7 ICL QSFP becomes offline, port 1, port 2, and port 3 of the QSFP will become offline as a result.
- All user ports in a Gen 7, 2KM ICL QSFP port must be assigned to the same logical switch when Virtual Fabric is configured. Port 3 of the ICL QSFP must be enabled first before port 0, port 1, and port 2 within the same QSFP to be enabled. If port 3 of the Gen 7, 2KM ICL QSFP becomes offline, port 0, port 1, and port 2 of the QSFP will become offline as a result.
- The output of CLI command `sfpShow` or any other interfaces to retrieve information from Gen 7 SWL QSFP (Part Number 57-1000490) and LWL QSFP (Part Number 57-1000491) does not match the Part Numbers on the media sticker labels. The output shows Gen 6 Part Number (57-1000351 for SWL or 57-1000480 for LWL). This does not affect operation of the optics.
- When a fabric with FOS v9.x is connected to a fabric with pre-FOS v9.0.0, RASLOG message FABR-1001 is generated as shown in the following example. This is an expected message. There is no impact on the ISL functionality.

  ```
  [FABR-1001], 35, FID 128, WARNING,, port 62, incompatible VC count
  ```
- FOS v9.x has disabled directory listing in CLI shell. As a result, entering <tab><tab> key does not list all CLIs available. Users can enter help command to list the commands. The shell tab completion by entering the first letter followed by <tab> key is supported.
- The FCR support of “Long Distance Fabric” mode conflict cannot coexist with long distance port configuration. If long distance mode (LD, LS, or LE) is enabled on the EX_Port and the EX_Port detected Backbone Fabric's Long Distance Fabric configuration is different from the connected Edge Fabric's Long Distance Fabric configuration, then the EX_Port will be disabled.
- If Long Distance Fabric is enabled on a switch via the `configure` command, it is recommended to upgrade the switch from FOS v8.2.x directly to FOS v9.0.0a or later. If the Long Distance Fabric configuration is enabled on an E_Port or EX_Port, firmware upgrade or downgrade to FOS v9.0.0 will effectively cause the Long Distance Fabric configuration to be disabled.
- If an HTTPS certificate is installed on a switch in FOS v9.x, HTTP access is blocked by default as HTTPS access is supported.
- When `portloopbacktest` mode1 test runs on multiple Gen 7 ICL ports with multiple iterations, the test may fail. The workaround is to run the test on one ICL port at a time with a reduced number of iterations.
- Running long distance LE mode between any blades or switches among FC32-X7-48, FC64-48, or G720 with port QoS mode enabled and `vc_translation_link_init` mode enabled may result in frame timeouts. The workaround for this problem is to use LS or LD mode for long distance.
- If downloading firmware on an unsupported platform, a write post to /rest/operations/show-status/message-id/20000 occurs and will incorrectly concatenate firmware download error messages. No recovery is needed, and this behaviour will not cause any functional impact.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades do not support 4G EX-Port.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades support 4G E-Port connected between any of the three listed only.
- When Connecting Brocade G730 with X7, G720, G620 switchType 183 or G630 switchType 184 these switches should run FOS v9.0.1c or later.
- When performing a configdownload operation this will not overwrite the existing MAPS Custom RASLog mode feature configuration on the switch. For example, if custom raslog mode is disabled in the switch but it is enabled in downloaded configuration, then the feature will remain disabled in switch and must be manually configured after the configdownload operation is complete.
- In FOS v9.1.1, CPX blades in X6 Switch Type 165.5 and 166.5 and X7 are displayed as CPX7 in `slotshow` command output.
- When upgrading from FOS v9.0.x to FOS v9.1.x, the AG ports will be moved from ALL_HOST_PORTS group to ALL_OTHER_F_PORTS group. Consequently, the MAPS thresholds for ALL_OTHER_F_PORTS will apply to these ports in FOS v9.1.x. The default thresholds for the groups ALL_HOST_PORTS and ALL_OTHER_F_PORTS are the same and if these are not changed there is no impact. In case custom thresholds are used and these are configured differently for the groups ALL_HOST_PORTS and ALL_OTHER_F_PORTS the thresholds (monitoring) for AG ports are impacted accordingly.

- When performing factory reset on an X6/X7, the cipher.syslog key is not reset to factory value.

  Consequently, TLS handshake failure messages are displayed ongoing on standby CP:

  Message: [SEC-3077], 123, SLOT 1 | CHASSIS, INFO, sw0, Event: TLS SESSION, TLS handshake failed, Info: certificate verify failed. Host=x.x.x.x

  To work around this, perform `factoryreset` in the following way:

  1. Factoryreset
  2. When TLS handshake failure message is displayed -reboot the standby CP.
- In FOS v9.1.x (or later), to conform to RFC3315 and RFC5942, the default value of prefix length for IPv6 DHCP address changed from 64 to 128. The prefix and gateway information are provided by the Router Advertisement (RA) and it is expected that RA is enabled in the network. If IPv6 RA is not enabled in the network, IPv6 connectivity issues will occur.

  The resolution is to enable RA to resolve IPv6 network connectivity issues.
- In case an NPIV flow is identified as SDDQ or Over Subscribed (and moved by Traffic Optimizer to an OS PG), the flow movement may cause some frames to be delivered Out of Order (OOO). In general, open systems devices have no issues when this happens.
- When performing `supportSave` with `SCP` as the selected transfer protocol, the command defaults to using SFTP internally. In environments where SFTP ports are blocked the `supportSave` upload will fail.
- When displaying the content of an attached USB with the command `usbstorage --list` the directory structure is displayed using “/” (slash) in previous versions of FOS this was “\” (back slash).
- GigE ports on SX6 and 7850 platforms can only be moved to a logical switch when the port has only speed and autonegotiation configuration. This is a change in behavior from earlier releases.
- The command `firmwarecleaninstall` is available only for install of FOS v9.2.0a or later (upgrade or downgrade is not supported.
- When upgrading a Gen 7 director or switch (X7-4, X7-8, G730, G720) to FOS v9.2.x, it is recommended to upgrade to FOS v9.2.0a or later. For additional information see TSB 2023-289-A.
- When doing repeated failovers on NetApp A400 and FAS9000 storage arrays, the switch can register very high counts of uncorrectable errors on the ports connected to the storage arrays. These errors do not have any impact on storage data transport.

Chapter 17: Security Vulnerability Fixes

In addition to defect fixes, software releases may also contain updates to address Common Vulnerabilities and Exposures (CVEs). The latest security vulnerability disclosures and descriptions of each CVE can be found by visiting the Brocade Security Advisories web page:

www.broadcom.com/support/fibre-channel-networking/security-advisories

Specific CVEs addressed within any given software release will be publicly released a short period after the initial posting of the software. This is done to provide enough time for OEMs to qualify security updates prior to public disclosure.

The exact CVEs addressed within the Fabric OS v9.x software releases are provided in the following security announcement:

support.broadcom.com/external/content/SecurityAdvisories/0/25000

Chapter 18: Defects

18.1 Closed with Code Changes in FOS v9.2.0c5

Defect ID	Description
FOS-871546	Excessive link errors reported, followed by a switch fault or a blade fault within a director.
FOS-872646	Storage ports connected to Gen6 blade or switch will not come online.
FOS-872941	The MXG610 is repeatedly panicking when a QSFP is installed and running a later version of FOS.
FOS-873148	Multiple SFPs in the same port group report “Mod-Val” state at the same time.
FOS-873503	Unable to launch webtools in SCG environment.
FOS-873602	Multiple SFPDDs/SFPs in the same port group report “Mod-Val” state at the same time.

18.2 Closed with Code Changes in FOS v9.2.0c4

Defect ID	Description
FOS-871910	Access Gateway (AG) and Fibre Channel Routing (FCR) will not function in a fabric that includes a Brocade switch assigned with the new OUI (B8-CE-ED).

18.3 Closed with Code Changes in FOS v9.2.0c3

Defect ID	Description
FOS-833439	A device file is not being created and switch cannot be accessed by management application.
FOS-861134	Invalid port stats counters reported such as the inv_arb counter : er64_inv_arb 0 top_int : Invalid ARB 4292386144 bottom_int : Invalid ARB
FOS-862224	SNMP daemon terminates.
FOS-863010	A chassis with FC32-X7-48 blade inserted is limited to 2k IT flows.
FOS-863077	The weblinker daemon memory usage continues to increase during SANnav monitoring and activities such as configupload start to fail.

18.4 Closed with Code Changes in FOS v9.2.0c2

None.

18.5 Closed with Code Changes in FOS v9.2.0c1

Defect ID	Description
FOS-862863	Hard zoning incorrectly enabled on FICON enabled switch with no zoning defined. All traffic will be blocked by the zoning checks.

18.6 Closed with Code Changes in FOS v9.2.0c

Defect ID	Description
FOS-847781	The Hostname attribute is not returned in the GPAT response.
FOS-848703	If RSC is enabled on the switch, changing authspec fails
FOS-849948	EM-1014 raslog states unable to read sensor on PS 1.
FOS-851010	FCIP Tunnel went down after seeing high rate of CRC errors.
FOS-851993	REST login fails, WebEM reports "Unable to access switch"
FOS-854348	"tsclockserver --set/tsclockserver" with FQDN succeeds even if configured DNS is unable to resolve the configured NTP Server FQDN to an IP address
FOS-854397	Observed the following flood of raslog: [MQ-1007], 783, SLOT 1 | FFDC | FID 128, WARNING, , queue fmFlowCopyQ: queue full (miss=1).
FOS-854587	The cfsd (Congestion Framwork System daemon) terminated during supportsave, resulting in repeated UFCS-2007 messages for "UFCS Lock stage Failed". Also, CFS supportsave info is not collected from all logical switches.
FOS-855507	Port Naming for Index showing as Port 0 on some ports
FOS-855788	Maps daemon (mdd) terminates during supportsave.
FOS-855888	Flash usage is close to full and observing large /var/log/syslog.* files.
FOS-855962	Unexpected switch reboot after termination of lldpd process.
FOS-855995	Zoning got stuck in a bad state and hung. This lead to a long waiting period and panic after multiple zone changes were made via CLI.
FOS-856210	Asic Data is no longer properly collected during supportsave.

FOS-856244	Switch reports "400 Bad Request" for GET /rest/running/brocade-chassis/chassis for all users
FOS-856702	E-Ports cannot come online and shows incorrect VC assignment
FOS-857267	Processor rebooted - Software Fault:ASSERT during supportsave
FOS-857277	Switch panic with Software Fault:Kernel Panic.
FOS-857387	CP watchdog exception due to excessive print messages
FOS-857454	Restartable daemons such as mdd, cald, snmp etc terminate and could not be restarted properly, causing HA out of sync and daemons are left in a defunct state.
FOS-857546	Multiple 40Ge ports logged link down/offline that led to a double kernal panic and cold recovery.
FOS-857609	cald terminated during flow operation such as CLI "flow --show -feature fabinfo -srcdev "*" -egrport" and the performance data can no longer be gathered.
FOS-857638	Switch panic after cfs daemon (cfsd) holds large amount of memory.
FOS-857687	During large HA sync copy operations, switch encounters msd panic
FOS-857838	Switch panic showing HAM-1004 message "Processor rebooted - Software Fault: Kernel panic". With additional messages showing "Kernel tried to execute NX-protected page" and "BUG: unable to handle page fault for address: ffffc9...."
FOS-858133	The administrative status will be shown as 'down' for the offline FC ports that have not been manually disabled(No_Module, No_Light, etc).
FOS-858197	BR7810 switches will report frequent ftrace triggers for an active Extension tunnel.
FOS-858263	The default Linux drivers in FOS v9.2x have an incompatibility with a small subset of 7810 switches that may result in 7810 being marked faulty after upgrading to FOS v9.2x
FOS-858339	Closing array bracket is missing. Invalid JSON data returned.
FOS-858427	Repetitive FICON-1056 errors logged after Feature Disable started for one or more extended FICON Devices.
FOS-858793	Observed termination of pdmd during Logical switch manipulation.
FOS-858848	The mdd process encounters a panic, and logs Raslog "KSWD -1002". The chassis may encounter an HA out of sync condition.
FOS-858851	User experience performance issue on Gen7 after code upgrade.
FOS-858865	Tunnel offline and then back online 4 minutes later
FOS-858950	Maps shows "0 mAmps" on SFP.
FOS-859282	CLI "flow" fails with Segmentation fault and traffic optimizer dashboards no longer work as expected.

FOS-859429	mdd termination during port related configuration.
FOS-859473	Switch failed firmware upgrade to FOS v9.2.0 with TruFOS license error
FOS-860003	Following an offline or online event with no zoning (using default zoning all access), an RSCN is not observed on the remote switch in the fabric.
FOS-860049	Transient PCS errors reported on G620.
FOS-860110	Switch firmware version changed to unknown/vpackage.
FOS-860262	Kernel panic while storing trace data.
FOS-860632	Standby CP in RRD state and/or SX6 blades are faulted during code upgrade. inetd on active CP no longer listens on port 514 on ipaddress of 127.3.1.x
FOS-860768	ISL disabled due to "Both Compression/Non-Compression connections exist to neighboring switch" after DWDM event.
FOS-860824	SANnav generates unnecessary SNMP notifications.
FOS-860835	snmpd terminated due to segmentation fault.
FOS-860855	Supportsaves are failing to collect switch SS using SANnav.
FOS-860936	Detected termination of process 0.weblinker.fcg during a REST zoning API request.
FOS-861132	ipv6 gateway address is missing after code upgrade.
FOS-861147	npd crashed as Standby CP was taking over as Active CP during firmwaredownload.
FOS-861360	Switch unexpectedly reboots due to termination of process fdmid.

18.7 Closed with Code Changes in FOS v9.2.0b1

Defect ID	Description
FOS-855788	Maps daemon (mdd) terminates during supportsave.
FOS-856244	Switch reports "400 Bad Request" for GET /rest/running/brocade-chassis/chassis for all users
FOS-857454	Restartable daemons such as mdd, cald, snmp etc terminate and could not be restarted properly, causing HA out of sync and daemons are left in a defunct state.
FOS-857687	During large HA sync copy operations, switch encounters msd panic
FOS-858263	The default Linux drivers in FOS v9.2x have an incompatibility with a small subset of 7810 switches that may result in 7810 being marked faulty after upgrading to FOS v9.2x
FOS-859473	Switch failed firmware upgrade to FOS v9.2.0 with TruFOS license error

18.8 Closed with Code Changes in FOS v9.2.0b

Defect ID	Description
FOS-822366	cald terminated and kernel paniced during supportsave collections.
FOS-839176	Customer might experience with an N-port from an AG being disabled with a misleading reason "Long distance mode not supported on AG".
FOS-847080	Switch supportsave collection from SANnav fails.
FOS-848419	RESTfulAPI query sometimes doesn’t show any value for disabled ports
FOS-848422	HA Out of Sync due to SNMPd terminated in FOS upgrade HA window.
FOS-849287	CLI sensorshow displays normal Temperature value, but Fan speed is 14375 RPM and system LED Flashes "amber and green " status.
FOS-849402	Devices connected to AG cannot login. Single F-port trunk becomes multiple F-port trunks.
FOS-849473	Rest returns blank and/or error while switch has a large weblinker process.
FOS-849790	Valid certificate not accepted
FOS-849929	Weblinker dies with a large CoreFile and SanNav may keeps showing "SNMP credentials invalid" state for the switch.
FOS-849954	PLOGI ACC not being received by host
FOS-849957	CLI sfpprogram command output debug information.
FOS-850029	FICN-1062E and FICN-1062I raslog's issued during eHCL sequences.
FOS-850131	Configupload doesn't fail or error out when the server side file path is non existent.
FOS-850496	Repeated logging of following raslog (with no functional impact): [UFCS-2007], 1118300/13621, FID 128, WARNING,, UFCS Lock stage Failed - ..
FOS-850500	User observes Fan kick starts and stays at a very high speed.
FOS-850931	Switch rebooted because of Kernel Panic
FOS-851141	SNMPd termination encountered during swBootPromLastUpdated query and "ps exfcl" command output (see below) shows stuck rpm query: 0 0 29270 2413 20 0 0 0 exit Z ? 0:00 _ snmpd <defunct> 0 0 23760 1 20 0 5144 3304 - R ? 5531:10 rpm
FOS-851164	Switch response for rest login request missing switch-parameters data for AAA non-local users.
FOS-851223	Switch ran out of kernel memory and triggered daemon panic, cpu busy or port/blade fault, etc.
FOS-851275	Panic on Standby CP when booting to Active on new firmware after hafailover during concurrent firmwaredownload.

FOS-851444	Observed kernel panic with the following stack trace: 000: Call Trace: 000: ? oidh_objget+0x39/0x50
FOS-851559	8Gb device slow to connect to 32G SFP on chassis.
FOS-852416	The show, set operation with CLI "syslogadmin" and "auditcfg" commands are failing with "Unable to retrieve ...". Also on a director, standby CP Supportsave cannot be retrieved.
FOS-852572	Core onserved while taking supportsave or segment fault during "RON --show" command.
FOS-852724	Compact flash run out of space and observed large sized ss_util_err.log and ss_util_err.log.old files.
FOS-852926	MAPS (module mdd) could go into a defunct state, and the state prevents MAPS from restarting, resulting in HA out of SYNC.
FOS-852945	fixed by merge
FOS-852964	Kernal panic after hareboot.
FOS-853019	FICN-2064 reports the wrong FID and port in a chassis based switch
FOS-853174	FC-LAG is no longer functioning.
FOS-853249	cald process aborted due to memory resource not available.
FOS-853452	The memory corruption will result in mdd panic.
FOS-853582	sfpProgram --show: Need to add the ability to query if a given SFP has been programmed
FOS-853697	Name server daemon (nsd) panic is observed while running nsaliasshow command.
FOS-853775	FabricAdmin role not allowing users to run supportshow after upgrade to v9.0.x
FOS-853850	Telnet not working after FOS 9.1.1x upgrade.
FOS-853898	A small 24 bytes leak for each succesful login.
FOS-853997	When "bulk" persistentEnable'ing ports from SanNav, ports would go to 'No_light' and disabled state.
FOS-854080	Detected termination of a daemon (zoned) followed by CP panic from Sotware Watch Dog timeout.
FOS-854095	After a non-critical daemon failed, it did not restart successfully and the switch persistently lost HA sync.
FOS-854143	Kernel panic when 64G oversubscription is introduced in the fabric with many neighbors on the same chip.
FOS-854317	DP wait timeout causing ESM to go into Cold recovery during eHCL processing
FOS-854371	FC traffic over an FCIP Tunnel stopped. The tunnel remains active, but IO is not passing over the WAN. FC ingress timeouts are observed from local FC ports that should be using the tunnel.

FOS-854497	Observed "vpackage" on one of the standby partitions after firmwaredownload.
FOS-854555	Large debug file (weblsocket.txt) was not removed as part of code upgrade, causing high flash usage to remain.
FOS-854685	Core blade abruptly power cycled itself and CP panicked with assert: ASSERT - Failed expression: ope->offload_req != NULL
FOS-854964	switches experienced snmpd termination and persistent loss of HA sync after customer upgraded snmp monitoring application.
FOS-855035	Weblinker is not restart-able after watchdog timeout abort or segment fault.
FOS-855493	Switch shutdown after abnormal sensor temperatures such as (-1 C) or (191 C) are reported: [HIL-1506], 3498/333, FFDC | , CRITICAL, sw0, High temperature (-1 C) exceeds system temperature limit. System will shut down within 2 minutes., OID:0x43000000, SPOID:0x4300000
FOS-855535	BSL inventory is intermittently missing chassis.json file.
FOS-856476	CLI fanshow shows FAN absent when re-inserted.

18.9 Closed with Code Changes in FOS v9.2.0a

Defect ID	Description
FOS-840406	SNMP stopped responding.
FOS-847091	Repeated software 'verify' errors detected on X7 directors running FOS 9.1.x. Also possible to see daemons crash due to watchdog timeout if congestion / oversubscription is severe.
FOS-847224	POST operation on leaf "action" with value "allow" gives an error message : "Target Port not provided for Allow action". There are other similar errors when attempting to POST or PATCH the 'action' leaf if all parameters are not entered.
FOS-847306	When performing a PATCH operation for the TCL 'default' in a configuration replay scenario, the switch will return an error 'Cannot modify input filters for default TCL' even when no parameters are being modified.
FOS-847538	Neighbor WWN missing/incorrect in brocade-interface response.
FOS-848121	On an X7 chassis with SX6 blades that have HA capable VE ports, the VE ports might occasionally toggle.
FOS-848182	snmpbulk /walk provides WWNs byte swapped in wrong order such as: 50:06:0e:80:08:9e:d4:20 is displayed wrongly as 80:0e:06:50:20:d4:9e:08
FOS-848316	printf limits input to "y" or "n" only, which hinders the ability to do scripting
FOS-848548	A RPM process stuck and/or firmwaredownload timed out after RPM DB corruption.

FOS-848635	Firmware download from 9.2.0 to 9.0.1e1 release does not complete when ECDSA hostkey is not configured on the switch.
FOS-848644	The SSH keys that are deleted before firmware download are recreated after firmware download.
FOS-848986	CLI "flow --create" option which worked on FOS8.x, now fails on FOS 9.x with the following error message: root> flow --create egress270 -feature monitor -egrport 4/41 -srcdev "*" -dstdev "*" -noactivate Invalid or nonexistent egress port 4/41 specified.
FOS-849564	Firmware upgrade to FOS 9.2 on G730 required a manual reboot to finish.
FOS-849642	Switch reported a flood of hardware errors, followed by daemons watchdog timeout and switch reboot. Sometimes these hardware errors also triggered port fault and/or blade fault. A raslog similar to this one should also be observed: [TO-1006], 1011618/1002267, FID 128, INFO, Switch_100, Flows destined to b1a02 device have been moved to PG_OVER_SUBSCRIPTION_4G_16G PG., cfs_ctrlr.c, line: 1470, comp:cfsd, ltime:2023/05/17-06:15:33:923058
FOS-849645	Network Patroller daemon (NPD) terminated even though the flow monitor was disabled via CLI "flow --deactivate sys_flow_monitor".
FOS-849829	FICN-1056 (ERROR) RASLOG reported, but traffic not interrupted
FOS-849852	G610 fails to boot after power outage with reason "ERROR: can't get kernel image!"
FOS-849917	On a G730 there is a probability of the switch getting into Credit loss (GE5-1012). Subsequent Link reset (GE5-1014) recovers the credit loss.
FOS-849942	Majority of ICLs in Hard_flt state after failover triggered by Watchdog Timeout on active CP after the switch crashes.
FOS-850134	This issue is specific to Gen7 chassis systems (X7-4, X7-8). Traffic optimizer related software verify errors (RAS-1004) and kernel panic might be observed.

18.10 Closed with Code Changes in FOS v9.2.0

Defect ID	**Description**
FOS-844552	Unexpected kernel panic/cold boot or HA out of sync.
FOS-844483	Following a power outage the switch may stay stuck in boot with the error message: "Can't get the kernel image"
FOS-844625	Configdownload fails on embedded platforms.
FOS-844453	User may see the following VERIFY message during firmwaredownload: VERIFY - Failed expression: 0 && "NULL Neigh"

FOS-846325	On a MXG610 embedded switch, running FOS versions FOS9.0.x, FOS9.1.x, user may encounter IO service disruption after a reboot / hareboot, triggered by uboot tune DRAM failure leading to a Reset (power cycle) of the system.
FOS-845216	User may encounter an unexpected sudden system reboot
FOS-847130	D-Port test stuck in not started from one end but another end succeeds.
FOS-846314	SfpShow indicating "Media not installed" and switchShow showing a port state of "Mod_Val"
FOS-845716	Ports Fenced upon Power Cycle of switch or blades.
FOS-844849	Credit loss observed on ISL link between two G730 switches
FOS-847091	Repeated software 'verify' errors detected on X7 directors running FOS 9.1.x. Also possible to see daemons crash due to watchdog timeout if congestion / oversubscription is severe.
FOS-847308	Brocade 7840 may encounter kernel panic due to OOM, with tunnels failing to come online after reboot
FOS-842607	MXG610s embedded switch panics after Fabric Resource Director daemon (fredd) crashes or holds a large amount of memory.
FOS-839186	Code upgrade turned into cold recovery when weblinker cannot restart in time, or on a normal operation switch, user may encounter failures in config change operations (e.g. portcfg or lscfg)
FOS-836247	Port IDs get dropped from Name Server database after HAfailover.
FOS-836232	The user will observe that Tunnel with Preshared key will not come up after config download.
FOS-836339	REST GET operation on brocade-security/sshutil-public-key fails with error "Named account does not exist"
FOS-839346	Path loss experienced after FOS upgrade on Access Gateway
FOS-837518	ESMd panic seen when issuing a `portcfgge lan --set -lan` command.
FOS-833753	1. Continuous console flooding of "query updated FCS dbs(s)" messages observed on primary FCS switch after FCS policy distribution. 2. HA out of sync when primary FCS switch is a chassis platform.
FOS-841961	On a X7 director that had gone through CLI "firmwarecleaninstall" of FOS9.0.x, after an upgrade to FOS v9.1.x, the active CP will show FAULTY (53) and will essentially be unresponsive. No output on the serial console. The management and service ports are no longer accessible.
FOS-841985	Unable to capture supportsave via Sannav
FOS-842771	REST PATCH operation on /brocade-interface/fibrechannel/name/{name}/persistent-disable-v2 URI does not change value.

FOS-838915	Switch panic while processing an incoming Fibre Channel frame.
FOS-835031	REST POST on /rest/operations/security-certificate incorrectly returns 400 Bad Request.
FOS-835720	"/var/tmp/install: line 259: sync: command not found" message is seen multiple times during firmwarecleaninstall
FOS-843422	UCS Server FLOGI is being held. Issue doesn't disappear when server is shutdown. Server cannot see paths through this adapter, can only see storage through other Fabric.
FOS-837563	Brocade G630 switch (Switch type = 184) may experience sudden reboot - resets.
FOS-843005	Switch panic, HA out of sync, with mdd core files during migration from FOS9.0.x to FOS9.1.x or later. Observed Raslog: [HAM-1013], 131574/20614, SLOT 1 | CHASSIS, CRITICAL, , Can't restart (mdd (pid=30408)): System unready or LS trans in progress. Reboot/Failover manually if necessary
FOS-840909	FCPH-1003 Raslog reports duplicate port WWN with a port that does not have the same port WWN.
FOS-838514	7840, 7810 or SX6 blade encounters DP Linux out of Memory causing IO disruption
FOS-841478	Duplicate PWWN detection resulted in disruption to the existing FICON CHPID.
FOS-841523	On G620 Switches, Rules in the group sys_flow_monitor are marked with *, implying that they are not monitored:
FOS-835872	The output for the "ficonshow rnid" and "ficonshow rnid table" CLI does not include Node Descriptors for online E-Ports.
FOS-836031	Switch panic after FDMI daemon terminated.
FOS-836458	User may encounter a series of RTWR errors following fastboot of one of the core switch in cores-edges topology 2021/12/02-14:05:11 (PST), [RTWR-1003], 1260, SLOT 2 | FID 3, INFO, Core-X7-8_Upgraded_130057_LS3, essd15: RTWR retry 64 to domain 17, iu_data 31000000.
FOS-823675	On a 32G DWDM port, D_Port diagnostics fails on the spinfab throughput test and DWDM line flips fail.
FOS-839936	User may encounter a CP Assert, upon initial failover to Fabric OS v9.x
FOS-838223	Devices connected to the Gen7 switch with default allaccess zone cannot communicate to each other in the FICON environment.
FOS-847171	G610 switch state is set to faulty after switchdisable/switchenable. G610:admin> switchshow ... switchType: 170.2 switchState: Faulty switchMode: Native switchRole: Faulty ...
FOS-844810	Observed "termination of mdd" during fcippathtest
FOS-843291	[PMGR-1006], 10392, SLOT 1 | CHASSIS, WARNING, , Attempt to move port(s) -1 on slot -1 to switch 21 failed. Error message: Not able to set port config on the switch. OR [HAM-

	1007], 2711, FFDC | CHASSIS, CRITICAL, , Need to reboot the system for recovery, reason: Software Bootup Failure:LS config timed out;
FOS-841694	Frame drops are seen on EX-ports after the edge fabric switch reboot and devices are stuck in init state without being imported.
FOS-837403	Local switch sends SCSI Inquiry with 0 bytes Allocation Length to attached storage devices.
FOS-840370	Firmwareupgrade failed due to time-out from a busy standby CP; HA lost sync after cald panic with a large sized core file and high compact flash usage.
FOS-841254	Unexpected reboot or failover after running out of memory.
FOS-839056	Frame drops affect the entire fabric after creating smaller trunks from larger trunks.
FOS-838549	Loss of paths after hafailover (firmwaredownload).
FOS-847045	Switch panic is observed when a timer is re-added before the same exact timer expires.
FOS-826227	Devices in default allaccess zone cannot communicate to each other across LISLs in FICON environment on all platform.
FOS-834530	Switch panics during adding aliases to zone configuration.
FOS-835586	SNMP consumes more CPU cycles, resulting in MAPS alerts.
FOS-837911	Observed switch Panic from UCID termination resulting in UCID core file
FOS-838045	User may see verify error while running IO over the long duration and SANNav monitoring.
FOS-840297	The CLI command: roleconfig --show -all -default, fails with the error "Operation failed"
FOS-840972	Port will be in decommissioned state (Persistent Disable) even though SANnav/REST indicates recommission action is successful.
FOS-836265	During code upgrade from FOS v8.2.1x to FOS v8.2.3x, FOS cannot completely be brought up due to cald core dumps. User observes the switch hanging.
FOS-833202	SSH to active CP on X6-4 is failing when the switch has only DSA and ECDSA host keys.
FOS-833824	The "Max UDP conn exceeded" counter in the output of "lan-stats --global" remains always at 0 even though the number of running UDP flows are more than the supported emulated UDP flows.
FOS-848670	SANnav inventory gets invalid device details, such as FXP name, Node WWN, Port WWN etc.
FOS-845272	MAPS defALL_FAN_AIR_FLOW_MISMATCH is only reported in the default FID.
FOS-836572	'snmpconfig' CLI returns error 'Failed to get snmp config info' due to SNMP service not restarting after getting disrupted.
FOS-836468	switchtype command not working on Admin account.

FOS-836381	VE Recovery during eHCL, causing IO failures.
FOS-836219	CLI "sfpshow -all" did not display complete output and the polling of smart SFP data stopped. It reported an very old "Last poll time:"
FOS-836313	The session which gets modified to HTTPS from HTTP based session, gets terminated when HTTP protocol is disabled after HTTPS certificate generation.
FOS-844393	Enabling DHCP from Static (v4) does not reflect the DHCP ipv4 address on embedded blade switches supported on HPE synergy chassis.
FOS-838047	During the FOS upgrade process, initiated from SANnav, directors can experience unexpected reboots during the upgrade process. In each director where this occurred the FOS upgrade had completed on the Standby CP and then an unexpected reboot occurred. Both CR blades reset and started POST diagnostics.
FOS-836972	'portname' output shows ports as persistently disabled which are not persistently disabled, and vice versa.
FOS-836573	FICN_1062 and FICN_1063 RASLOGs every 1.5 seconds on FICON Emulation enabled FCIP Tunnel
FOS-843300	snmpd terminated after running out of memory and failed to restart, left switch with HA out of sync
FOS-842160	firmwarecleaninstall from versions lower than FOSv9.1.0b directly to FOS v9.1.0b or v9.1.1 does not complete and indicates "Firmware commit failed"
FOS-833982	REST PATCH on /brocade-security/sec-crypto-cfg incorrectly return 400 Bad Request on configuration replay.
FOS-840768	Switch panic when trace module has memory corruptions.
FOS-839507	Switch fault after Portledtest causing EM-1334 & BL-1020 raslog.
FOS-839810	User may see repeated logging of an internal firmwaredownload raslog messages.
FOS-838584	Weblinker termination due to segmentation fault.
FOS-837405	Flow vision reports the wrong direction of flows for the SCSI devices that don't register FC4 features.
FOS-835940	The difference of the "cfgshow --transdiffsonly" output would be when a cfgadd CLI is executed, in 9.0.1x version: the output of the zoning cfg got changed will list all of existing non-changed zone member with "-+" in front of all zone member. But with 8.2.x version, there is no "-+" in front of all untouched zoning member.
FOS-836024	The configdownload operation will not overwrite the existing MAPS "Custom RASLog mode" feature configuration in switch. For example, if custom raslog mode is disabled in switch but it is enabled in downloaded configuration, then the feature will remain disabled in switch.

FOS-835998	tsclockserver Active server shows as NONE on non-principal switches however working fine on Principal switch with legacy mode disabled. Similarly, tsclockserver Active server shows as NONE when set to LOCL in legacy mode disabled.
FOS-837837	Performance stats for VE ports are not present in connunitportstat table
FOS-836506	Periodic XTUN-1997 triggers when running FICON and FCP/SCSI flows over an FCIP Tunnel Port Based or Device Based Routing configuration. The XTUN-1997 triggers are for Keepalive timeouts on the medium priority circuits.
FOS-835809	'Unmount USB Drive' option is displayed in WebEM after USB device is inserted. User would not be able to use the USB device connected to the switch as there is no option to mount the device.
FOS-843176	Switch panic after network timer server daemon (nptd) hang and watchdog timeout: 2022/08/30-02:03:10 (MDT), [KSWD-1002], 1147, FFDC | CHASSIS, WARNING, sw0, Detected termination of process tsd:2849.
FOS-836043	Director-class switches returning chassis S/N when being queried for brocade-chassis info via REST, when WWN 1 S/N was previously returned and used for entitlement.
FOS-835714	An incorrect error message is returned when the flows of an NPIV port are being quarantined.
FOS-844912	Frames that have a DID with domain controller format (0xfffcxx), such as FDMI query, are being dropped as zone_miss.
FOS-836077	On Standby CP, lines with '0's appear on console during hot code load.
FOS-837183	TX rules for ISL ports do not get triggered for MAPS custom policy that includes both RX and TX rules for the ISL ports.
FOS-833984	REST PATCH on /brocade-security/user-config incorrectly return 400 Bad Request on configuration replay.
FOS-843393	A flooding of TS-1019 RASLOG and switch is dropping TS updates
FOS-832042	Brocade 7810 switch panics or hangs on boot up.
FOS-841986	64GB longwave optics do not display 64 Gb capability in CLI command 'sfpshow'
FOS-848548	A RPM process stuck and/or firmwaredownload timed out after RPM DB corruption.
FOS-836491	flow CLI does not report TIMEOUT count for an Initiator or Target device.
FOS-843260	SNMP cannot get port address on FOS v9.1.0x.
FOS-846852	Egress & Ingress power TxRx values are incorrect in the diagnostic test results when D-Port test is run from SANNav
FOS-837394	'diagshow' command output shows port error statistics incrementing while link itself has no error.

FOS-837352	Standby CP is no longer accessible after staging firmware on it and then running 'firmwareactivate'.
FOS-842657	SANnav receives the syslogs with source address as CP IP address and not with Chassis IP address
FOS-843643	Web tools cannot save zone configurations when launched from the Dell Chassis UI
FOS-843463	Getting Alerts for HTTPS SW certificate triggered DAYS_TO_EXPIRE rule - defCHASSISCERT_VALIDITY.
FOS-847770	3rd party device boot over SAN failed or device LUN cannot be recognized.
FOS-835781	D-Port test is stuck in "In Progress" on 32G ADVA DWDM links.
FOS-832033	The following BL-1061 message could be seen for GigE ports on 7810 when there is no mismatch in SFP speed and port speed config. [BL-1061]ERROR, aw16, port speed(10G) and SFP speed(1G) mismatch in port(ge2) slot number(0). Insert SFP matching port speed.
FOS-846479	Weblinker restart on switch.
FOS-845750	Support for non-disruptive EX port link cost changes.
FOS-839812	firmwaredownload failed with disk full with a large firm_intg_mon.log left on switch.
FOS-839682	When 1 PSU is powered off, one of the Fan shows faulty instead of OK. Also, once Maps detects BAD_PWR and sets current switch policy status to CRITICAl, it stays at CRITICAL. Current Switch Policy Status: CRITICAL Contributing Factors: --------------------- *BAD_PWR (CRITICAL).
FOS-837592	Deadlock condition with SNMP causing the message queue to full and snmpd termination.
FOS-837921	LUN count is counted twice for LUNS from IT pair in the same switch but different Chip
FOS-825237	Occasional glitches reported in total byte count and total IO count when an external script pulls data at the same time flow statistics are being updated in the backend.
FOS-823009	Sys_flow_monitor is not automatically activated after installing the Fabric vision license.
FOS-840971	If switch uptime is more than 99 days, then only the first two digits of the uptime days is displayed in Dashboard.
FOS-837088	FOS accepts REST requests with an empty audit class list.
FOS-846838	Available ports section in Ports Widget shown in red color instead of green.
FOS-806764	User sees the following error when executing the CLI command portshow: porttrunkarea is configured for F-port trunks.'-i or -x' option not supported.

18.11 Closed without Code Changes in FOS v9.2.0

Defect ID	Description
FOS-837483	Code upgrade was disruptive after HA recovery failed for all online 32G QSFP ports.
FOS-840082	The following similar raslog may be see without actual excessive power consumption: EM-1230 1 of 3 Excessive Power usage detected PS1(564)+PS2(144)=708W. System will shutdown on consecutive readings above 700W.
FOS-837451	DWDM is reporting a "loss of lock" error and the switch is showing no light on the port.
FOS-839820	Brocade 8510-8 director class switches with a single faulty WWN card, running FOS v8.2.3a or FOS v8.2.3b may encounter a failure reading from the WWN cards.
FOS-837678	When an initiator logs in to the fabric, the discovery of targets on a remote (different domain) G730 can be delayed or fail.
FOS-840010	LSAN traffic stopped after adding a new switch to the edge fabric.
FOS-841964	Standby CP encounters hasmd panic with no ffdc and no raslogs triggered.
FOS-843045	MAPs alarms continue to be generated following the addition of WWN Data Protection license.
FOS-837280	Boot over SAN device does not work after upgrading firmware on 32G FC switches.
FOS-836531	Switch panic with maps daemon (MDD) watchdog timeout.
FOS-844297	TruFOS Certificate cannot be installed on switches running 9.0.1e from SANnav server
FOS-829100	Path unstable when zone miss counter increases but the cam entries are verified to be good. Plogi ack , abts frames are dropped.
FOS-837583	SNMP daemon leaks memory and causes switch to hafailover/hareboot/panic when switch runs out of memory.
FOS-832168	SX6 blade might be faulty with error code 21.
FOS-836944	Cannot firmwaredownload PSD package via SANNAV on some platforms.
FOS-841520	Host reboot will trigger MAPs alert Condition=ALL_SFP(RXP<=200), Current Value:[RXP, 2 uW]
FOS-838166	type2 frame drop when portdecom cli is invoked
FOS-837573	flow mon failed to relearn flows
FOS-837755	Stale CAM entries are present on the ports, which were disabled.
FOS-825993	Failure status should be sent, if SS fails on any of the CP
FOS-840196	User may encounter Core blade in faulty state, leading to chassis in RRD state

FOS-840221	User may encounter SANnav reporting a successful firmwaredownload but the new Firmware image has not been downloaded to some switches
FOS-844942	USERID account gets deleted.
FOS-831001	When a G720 powers up (cold boot) with a single power supply, all fans are on high as expected. If a second power supply is later inserted without a power cord and with the power switch in the Off position, the power supply is put into a Faulty state. Even after the power cord is plugged in and it is turned on, the power supply never recovers & fans remain High.
FOS-836856	Weblinker process is getting terminated frequently on the switch.
FOS-836369	D-Port test does not start on the secondary port links of a 53G BMF QSFP, when the test is initiated using "portdporttest --start" command option on all 4 ports.
FOS-836304	Frames to the remote fabric across the IFL are dropped after D-port testing.
FOS-844074	Detected termination of process snmpd.
FOS-841141	MAPS test email using FROM address of "root@switchname.domain.com" which is not always supported.
FOS-837538	Different (lower) tunnel throughput on 7800 or FX8-24 configuration after reboot or slot power cycle.
FOS-833402	A user account, with a user defined role assigned with user management privileges for chassis but not for current VF, will fail to exercise any user account management operations.
FOS-840717	High CPU usage reported on SNMP daemon.
FOS-840406	SNMP stopped responding.
FOS-843396	SNMP password has to be set twice.
FOS-835082	Import of HTTPS certificates results in continuous restart of weblinker. Enabling HTTPS fails.
FOS-843589	MAPS traps being sent to other monitoring software even though maps rule are configured with action 'NONE'.
FOS-844217	Zoning errors observed with raslog ZONE-1007 but traffic is moving fine.
FOS-834340	During core or port blade insertion/removal in a chassis, Web Tools will not be able to get data from switch and it will become blank for 3-5 minutes. A browser refresh after this period will re-enable the Web Tools functionality.
FOS-842988	High flash usage on switches running FOS9.1.1.
FOS-836048	The CP will get stuck in hung state and no CLI's can be executed on the switch.
FOS-834539	Users will see "-rbash: clihistory: command not found" sometimes, while running "serviceshell --show"

FOS-847063	Director hits panic when eth0 interface frequently bounces.
FOS-848567	WWN is missing in the oid when run snmpgetnext command to connUnitPortTable.
FOS-844544	High CPU utilization reported on switches during supportshow.
FOS-842145	User may encounter VPD write error to WWN card after the system transitions to CF_ACTV state for WWN Data Protection (WDP).
FOS-841574	After upgrading to FOS 8.2.3b, the BSL report no longer included GE_PORT type in the report.
FOS-842033	Storage ports on specific vendor storage devices show extremely high uncorrectable errors on these ports during storage hafailover.
FOS-826015	Device authentication policy mismatch between switch and HBA causes trunk master port to attain G-port state while slave port remains F-port.
FOS-815150	AG default mapping is incorrectly set for Brocade 6547 switch.
FOS-569827	Port beaconing stops after spinfab is ran.
FOS-656241	During HAfailover a cold recovery was required

18.12 Open in FOS v9.2.0

Defect ID	**Description**
FOS-823999	Flow monitor reports only SCSI stats for an IT flow with SCSI and NVMe exchanges across time.
FOS-847781	The Hostname attribute is not returned in the GPAT response.
FOS-839967	User may encounter E-ports get segmented with reason - Zone Merge Internal Error
FOS-848121	On an X7 chassis with SX6 blades that have HA capable VE ports, the VE ports might occasionally toggle.
FOS-836443	IO flow statistics are not displayed when the lookup is done at the VM entity id.
FOS-810530	Zone merge slow performance and failure on that switch that has defzone all access defined. Along with this behavior IPC drops RASLOGs events and/or termination of process nsd maybe seen.
FOS-848644	The SSH keys that are deleted before firmware download are recreated after firmware download.
FOS-847538	Neighbor WWN missing/incorrect in brocade-interface response.

FOS-847224	POST operation on leaf "action" with value "allow" gives an error message : "Target Port not provided for Allow action". There are other similar errors when attempting to POST or PATCH the 'action' leaf if all parameters are not entered.
FOS-849244	Switch ports get erroneously disabled during migration.
FOS-848316	printf limits input to "y" or "n" only, which hinders the ability to do scripting
FOS-847306	When performing a PATCH operation for the TCL 'default' in a configuration replay scenario, the switch will return an error 'Cannot modify input filters for default TCL' even when no parameters are being modified.
FOS-842564	The 7850 console is flooded with messages with string "cmicx_sbusdma_curr_op_details" affecting LAG and Ethernet port stats functionality.
FOS-845543	During HCL, observe RASlog ESS-2001 message followed by RASlog ESS-2002.
FOS-848281	The applications that parse the improperly encoded XML responses can encounter XML parsing failures.
FOS-848036	The 'zoneshow --validate' output for a zone that contains an alias member is incorrectly showing the alias member and not displaying the "Effective configuration:" section.
FOS-848635	Firmware download from 9.2.0 to 9.0.1e1 release does not complete when ECDSA hostkey is not configured on the switch.
FOS-834569	Flow gets deactivated after reboot/hareboot in AG
FOS-841163	User can't perform firmware download on the switch from SANNav.
FOS-848182	snmpbulk /walk provides WWNs byte swapped in wrong order such as: 50:06:0e:80:08:9e:d4:20 is displayed wrongly as 80:0e:06:50:20:d4:9e:08
FOS-848703	If RSC is enabled on the switch, changing authspec fails
FOS-846574	REST GET on /brocade-security/dh-chap-authentication-secret does not match CLI output.
FOS-847952	CLI firmwareshow output will display "vpackage" string on the secondary partition instead of the build version. This does not affect the functioning of the switch.
FOS-633099	Using the SSH syntax "ssh admin@<ip address> <cli command>" in LS specific context, generates the output for the default switch.
FOS-845513	Benign warning messages may get displayed on the console about being unable to delete non-existent files, even though firmware upgrade is successful
FOS-848228	Improper error message are displayed for invalid inputs to "framelog" command.
FOS-847860	REST PATCH operation on swEventTrap severity level with debug option returns an error, "Invalid severity level".

FOS-848986	CLI "flow --create" option which worked on FOS8.x, now fails on FOS 9.x with the following error message: root> flow --create egress270 -feature monitor -egrport 4/41 -srcdev "*" -dstdev "*" -noactivate Invalid or nonexistent egress port 4/41 specified.
FOS-844986	Observed some unexpected messages such as "/var/tmp/rpm-tmp.CNGUPL: line 2: [: !=: unary operator expected" during firmware downgrade from 9.2.0 to 9.1.1x.
FOS-846503	REST PATCH on various /brocade-logging leafs with invalid values incorrectly return 204 No Content.

Revision History

Version	Summary of changes	Publication date
1.0	Initial version of document.	09/27/2024
2.0	Updated the defect tables.	10/08/2024
3.0	Updated with FOS v9.2.0c1.	10/30/2024
4.0	Updated with FOS v9.2.0c2.	12/04/2024
5.0	Updated with FOS v9.2.0c3. Correction in the section Optimized Credit Model for G630 and X7-8/4. Added the section MAPS. Correction in Closed with Code Changes in FOS v9.2.0c.	01/27/2025
6.0	Updated Extension section under New and Modified Software Features and Important Notes.	02/14/2025
7.0	Updated with OUI section.	10/22/2025
8.0	Updated with FOS v9.2.0c5.	01/21/2026