

Fabric OS v8.2.3e/v8.2.3e1/v8.2.3e2

Fabric OS v8.2.3e Release Notes Digest

Release Notes

Version 8.0

Copyright © 2024–2025 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to www.broadcom.com. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies.

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	6
1.1 Contacting Technical Support for your Brocade® Product	6
1.2 Related Documentation	7
Chapter 2: Locating Product Manuals and Release Notes	8
2.1 Document Feedback	8
Chapter 3: Overview	9
Chapter 4: What's New in FOS v8.2.3e	10
4.1 Resolution of Important Defects.....	10
4.2 Software Upgrades and Downgrades	10
Chapter 5: What's New in FOS v8.2.3d.....	11
5.1 Resolution of Important Defects.....	11
5.2 Software Upgrades and Downgrades	11
5.3 Software Features	11
5.3.1 System Security	11
Chapter 6: What's New in FOS v8.2.3c.....	12
6.1 Resolution of Important Defects.....	12
6.2 Software Upgrades and Downgrades	12
6.3 Software Features	12
6.3.1 MAPS	12
Chapter 7: What's New in FOS v8.2.3b.....	13
7.1 Resolution of Important Defects.....	13
7.2 Software Upgrades and Downgrades	13
Chapter 8: What's New in FOS v8.2.3a/v8.2.3a1	14
8.1 Resolution of Important Defects.....	14
8.2 Software Upgrades and Downgrades	14
8.3 Software Features	14
8.3.1 CLI Enhancements.....	14
Chapter 9: What's New in FOS v8.2.3.....	16
9.1 Resolution of Important Defects.....	16
Chapter 10: What's New in FOS v8.2.2.....	17
10.1 Software Features	17
10.1.1 Modified Software Features	17
10.1.2 Deprecated Software Features	17

Chapter 11: What's New in FOS v8.2.1	18
11.1 Hardware	18
11.1.1 New Devices	18
11.1.2 New Blades	18
11.1.3 New Optical Transceivers	18
11.1.4 Deprecated Hardware	18
11.2 Software Features	18
11.2.1 New Software Features.....	18
11.2.1.1 Counterfeit License Protection	19
11.2.1.2 REST API with New RESTCONF Modules.....	19
11.2.1.3 Management Interface Rate Limiting	19
11.2.2 Modified Software Features	19
11.2.2.1 MAPS Enhancements	20
11.2.2.2 Access Gateway Enhancements	20
11.2.2.3 Fabric Services Enhancements	21
11.2.2.4 System Security Enhancements	21
11.2.2.5 configure Command Enhancements.....	21
11.2.2.6 Extension Enhancements	21
11.2.2.7 Power Supply Microcontroller Firmware Utility	22
11.2.2.8 Miscellaneous Enhancements	22
11.3 CLI Command Changes	22
11.3.1 New Commands.....	22
11.3.2 Modified Commands	22
11.3.3 Deprecated Commands	23
11.4 Supported Standards and RFCs	23
 Chapter 12: Software License Support	 24
12.1 Optionally Licensed Software	24
12.2 Temporary License Support	26
 Chapter 13: Hardware Support	 28
13.1 Supported Devices	28
13.2 Supported Blades	28
13.2.1 DCX 8510-8/DCX 8510-4 Blade Support.....	28
13.3 Supported Power Supplies	29
13.3.1 DCX 8510-8 Power Supply Requirements.....	29
13.3.1.1 Typical Power Supply Requirements for Blades in DCX 8510-8 Backbones	29
13.3.2 DCX 8510-4 Power Supply Requirements.....	30
13.3.2.1 Typical Power Supply Requirements for Blades in DCX 8510-4 Backbones	30
13.3.3 Supported Optics	30
 Chapter 14: Software Upgrades and Downgrades	 31
14.1 Platform Specific Downloads	31
14.1.1 Using FOS PSDs	31
14.1.2 Loading FOS PSDs via Web Tools or FOS Command Line.....	31
14.1.2.1 Loading FOS PSDs via Brocade SANnav Management Portal.....	31
14.2 Image Filenames	32
14.3 Migration Path	33
14.3.1 Migrating to FOS v8.2.3e	33
14.3.2 Migrating from FOS v8.2.....	33
14.3.3 Migrating from FOS v8.1	33
14.3.4 Migrating from FOS v8.0	33
14.4 Upgrade/Downgrade Considerations	34

Chapter 15: Limitations and Restrictions	35
15.1 Scalability.....	35
15.2 Compatibility/Interoperability	35
15.2.1 Brocade SANnav Management Portal Compatibility	35
15.2.2 Web Tools Compatibility	35
15.2.3 SMI Compatibility	35
15.2.4 Fabric OS Compatibility	36
15.2.5 SNMP Support	36
15.2.5.1 Obtaining MIBs.....	37
15.2.6 REST API Support	37
15.2.6.1 Obtaining YANG Files	37
15.3 Important Notes.....	37
15.3.1 System Security	37
15.3.2 FCoE	38
15.3.3 FC-NVMe	38
15.3.4 In-flight Encryption and Compression	38
15.3.5 VM Insight	38
15.3.6 ClearLink Diagnostics (D_Port).....	39
15.3.7 Forward Error Correction	39
15.3.8 Access Gateway	39
15.3.9 Ingress Rate Limiting	40
15.3.10 Ethernet Management Interface	40
15.3.11 Extension	40
15.3.12 Brocade Analytics Monitoring Platform.....	41
15.3.13 Flow Vision.....	42
15.3.14 FICON	43
15.3.15 MAPS	43
15.3.16 Miscellaneous	43
Chapter 16: Security Vulnerability Fixes.....	44
Chapter 17: Defects	45
17.1 Closed with Code Changes in v8.2.3e2.....	45
17.2 Closed with Code Changes in v8.2.3e1.....	45
17.3 Closed with Code Changes in v8.2.3e.....	45
17.4 Closed with Code Changes in v8.2.3d	46
17.5 Closed with Code Changes in v8.2.3c.....	47
17.6 Closed with Code Changes in v8.2.3b	49
17.7 Closed with Code Changes in v8.2.3a1.....	51
17.8 Closed with Code Changes in v8.2.3.....	51
17.9 Closed with Code Changes in v8.2.3a.....	54
17.10 Closed without Code Changes in v8.2.3.....	55
Revision History.....	56

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
<p>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:</p> <ul style="list-style-type: none"> ▪ Case Management ▪ Software Downloads ▪ Licensing ▪ SAN Reports ▪ Brocade Support Link ▪ Training & Education 	<p>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.</p>

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 running Fabric OS 6.2 and above, 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 6520, 6510, 6505, G630, G620, G610 – On the switch ID pull-out tab located on the bottom of the port side of the switch.
- Brocade 7840, 7810 – 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 in a well on the left side underneath (looking from the front).
- Brocade DCX 8510-8 – Bottom right of the port side.
- Brocade DCX 8510-4 – Back, upper left under the power supply.
- Brocade X6-8, X6-4 – Lower portion of the chassis on the nonport 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 `licenseIdShow` command to display the license ID.

1.2 Related Documentation

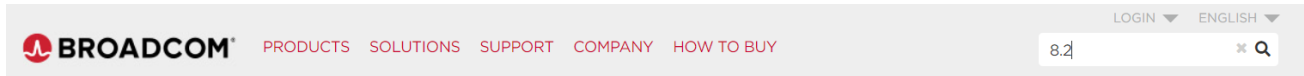
White papers and data sheets are available at www.broadcom.com. Product documentation and release notes for all supported releases is available at www.broadcom.com.

Chapter 2: Locating Product Manuals and Release Notes

This section outlines how to locate and download Brocade product manuals and release notes from myBroadcom. Although the illustrations show Fibre Channel and Fabric OS (FOS), they work for all Brocade products and operating systems.

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

1. Go to <https://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 8.2.



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

The list of documents available for the release displays.

Search Results

2.1 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 or 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

These Release Notes cover Fabric OS v8.2.3e/v8.2.3e1/v8.2.3e2.

Fabric OS v8.2.3e is a patch release based on Fabric OS v8.2.3d

All Gen 5 hardware platforms and features supported in FOS v8.2.3 are also supported in FOS v8.2.3e including patch releases of 8.2.2 (8.2.2a, 8.2.2b, 8.2.2c, and 8.2.2d). Gen 6 platforms are no longer supported with FOS v8.x.

FOS v8.2.3e requires a valid FOS Upgrade Certificate and contains minor enhancements, CVEs and fixes for the defects listed at the end of this document.

FOS v8.2.3e1 and FOS v8.2.3e2 includes defect fixes as described in the respective tables in the defect section.

Chapter 4: What's New in FOS v8.2.3e

4.1 Resolution of Important Defects

This release provides the following important defect fixes:

- FOS-857454 Restartable daemons such as mdd, cald, snmp etc terminated and could not restart properly, causing HA out of sync and daemons are left in a defunct state.
- FOS-853249 cald process aborted due to memory resource not available.
- 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-820856 High CPU load observed on switch once a connection via WebTools is made with https.

For a full list of fixes, see [Defects](#).

4.2 Software Upgrades and Downgrades

This release of FOS is available for entitled Gen 5 equipment with a valid FOS upgrade certificate.

For more details, see [Migrating to FOS v8.2.3e](#).

NOTE Embedded switch platforms (6543, 6547, 6548, 6558) do not require a FOS upgrade certificate.

Chapter 5: What's New in FOS v8.2.3d

5.1 Resolution of Important Defects

This release provides the following important defect fixes:

- FOS-840370 Firmwareupgrade failed due to time-out from a busy standby CP; HA lost sync after cold panic with a large sized core file and high compact flash usage.
- FOS-841163 User can't perform firmware download on the switch from SANNav.
- FOS-845216 User may encounter an unexpected sudden system reboot.
- FOS-845750 Support for non-disruptive EX port link cost changes.

For a full list of fixes, see [Defects](#).

5.2 Software Upgrades and Downgrades

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form.

For more details, see [Software Upgrades and Downgrades](#).

5.3 Software Features

This release includes the following enhancements.

5.3.1 System Security

FOS v8.2.3d includes the following enhancements and support updates:

- Support single bind for LDAP login

The following Microsoft LDAP versions are supported:

- Windows Server 2019, schema 88 -with certificate support
- Windows Server 2022, schema 88 -with certificate support

Support for previous versions of Microsoft LDAP is deprecated in FOS v8.2.3d.

Chapter 6: What's New in FOS v8.2.3c

6.1 Resolution of Important Defects

This release provides the following important defect fixes:

- 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-826227 Devices in default allaccess zone cannot communicate to each other across LISLs in FICON environment on all platforms.
- FOS-836531 Switch panic with maps daemon (MDD) watchdog timeout.
- FOS-839346 Path loss experienced after FOS upgrade on Access Gateway.

For a full list of fixes, see [Defects](#).

6.2 Software Upgrades and Downgrades

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form.

For more details, see [Software Upgrades and Downgrades](#).

6.3 Software Features

This release includes the following enhancements.

6.3.1 MAPS

FOS v8.2.3c provides MAPS support for monitoring of the following SmartOptics:

- 8G DWDM 80 km [ALL_80Km_8GELWL_SFP]
- 16G DWDM 40 km [ALL_40Km_16GELWL_SFP]
- 32G DWDM 40 km [ALL_40Km_32GELWL_SFP]

Note: Downgrade from FOS v9.x that support this feature to FOS v8.2.3c (or later) is blocked.

Chapter 7: What's New in FOS v8.2.3b

7.1 Resolution of Important Defects

This release provides the following important defect fixes:

- FOS-831875 SNMP application may lose connection to switch momentarily during snmp walk of IPV6 address table and occasionally the user may observe CP lost HA SYNC if the walk is performed during hafailover/hareboot.
- FOS-832434 After upgrading Brocade 6548 to FOS 8.2.3a, the user is unable to login to the switch, with the following error: login: admin "Inconsistency de" -Note: traffic may be impacted too.
- FOS-833935 Management application encounters errors after webtool runs out of file descriptor on switches with LDAP configuration.
- FOS-834912 SANnav reports error: "Registration for telemetry profile 'xxx' has failed and Switch panic after cald termination.
- FOS-836031 Switch panic after FDMI daemon terminated.
- 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 if cal.esrs configuration keys are present.

For a full list of fixes, see [Defects](#).

7.2 Software Upgrades and Downgrades

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form.

For more details, see [Software Upgrades and Downgrades](#).

Chapter 8: What's New in FOS v8.2.3a/v8.2.3a1

8.1 Resolution of Important Defects

This release provides the following important defect fixes:

- FOS-830052: Port initialization interop issues with a certain SFP, when connecting to a specific 3rd device. This may result in some ports showing errors and some going into no_sync, port_Flt state.
- FOS-831875: SNMP application may lose connection to switch momentarily during SNMP walk of IPV6 address table and occasionally the user may observe CP lost HA SYNC if the walk is performed during hafailover/hareboot
- FOS-832434: After upgrading Brocade 6548 to FOS 8.2.3a, the user is unable to login to the switch. Error shown as below: login: admin Inconsistency de Note: traffic is impacted too.
- FOS-823756: A third party device is unsuccessful in moving from one switch port to another switch port.
- FOS-828899: DP Panic after upgrading to FOS8.2.1 through FOS8.2.2d while running FICON XRC traffic over XRC Emulation enabled FCIP Tunnel.
- FOS-820640: Flash usage exceeds 90% resulting in a switch panic.
- FOS-827217: Switch panic during tracedump.
- FOS-829779: SANNAV fails to generate switch supportSave on switches running FOS v8.2.2 and above.
- FOS-827821: Device has login issue with certain optic types.

8.2 Software Upgrades and Downgrades

This release of FOS is available for entitled equipment download in **Platform Specific Download (PSD)** form.

For more details see [Software Upgrades and Downgrades](#).

8.3 Software Features

FOS 8.2.3a includes the following CLI enhancements.

8.3.1 CLI Enhancements

sysHealth

New command to perform PCIe link test between the Standby CP and the port or core blades in the chassis.

Use this command to run system health related tests.

Synopsis

```
syshealth --slotpcitest slot_number
syshealth --slotpcitest all
syshealth --help
```

aaaConfig

New option `-tls_mode` added to specify the mode of the connection with the LDAP Server.

Valid options include the following:

starttls

Initiates LDAP connection with StartTLS. The default port is 389.

ldaps

Initiates LDAPS connection. The default port is 636.

Synopsis

```
aaaconfig --add | --change server -conf radius | ldap | tacacs+  
[-p port] [-d domain] [-t timeout] [-s secret]  
[-a chap | pap | peap-mschapv2] [-e -encr_type none | aes256]  
[-tls_mode starttls | ldaps]
```

NOTE In a chassis, both CPs must be loaded with FOS v8.2.3a before configuring the LDAPS protocol. Before configuring LDAPS, verify that both CPs are running FOS v8.2.3a; otherwise, the command results in a no-op operation if the standby CP does not support LDAPS.

When LDAP TLS Mode configuration is set to LDAPS in FOS v9.0.1x, it's not recommended to downgrade to FOS v8.2.3a.

If downgrade to FOS v8.2.3a from FOS v9.0.1x is necessary, first configure LDAP TLS Mode to STARTTLS before downgrading to FOS v8.2.3a to avoid potential user login issues.

portCfgLosstov

New options `-dwdmloyncon` and `-dwdmlosyncoff` added to enable or disable the configuration for DWDM lossSync fixed speed port.

Synopsis

```
portcfglosstov port [-dwdmloyncon | -dwdmlosyncoff]
```

Chapter 9: What's New in FOS v8.2.3

9.1 Resolution of Important Defects

This release provides the following important defect fixes:

- FOS-825388: FCIP Tunnel up, but all I/O stops flowing over the tunnel and application times out.
- FOS-823765: Traffic disruption encountered when Encryption block errors occur due to errors, such as, "frames too long".
- FOS-823769: HA state went out of sync after duplicate "zonecreate --peerzone" and cfgadd CLIs.
- FOS-826655: Switch panic during code upgrade in a virtual fabric, if there were with stale LISL leftover from previous switchdisable/switchenable operations.
- FOS-800300: After running diagnostic test on G630, it cannot pass traffic without a reboot first.

Chapter 10: What's New in FOS v8.2.2

10.1 Software Features

The following sections list new, modified, and deprecated software features for this release.

10.1.1 Modified Software Features

This release includes the following enhancements to existing features and supports:

- Support 10Gb/s Ethernet ports in Brocade 7810 base configuration without the Extension Upgrade license.
- Support a user configurable port for SCP and SFTP protocols with the `firmwareDownload` and `supportSave` commands.
- Support a user configurable port attribute for SCP and SFTP protocols with the `brocade-operation-supportsave` REST API module.
- Support REST API GET operation without a session authorization key. HTTP GET operations can be completed with a single request using a Basic Authentication header.

10.1.2 Deprecated Software Features

This release includes the following deprecation of existing features and supports:

- The IPsec feature on Management Ethernet Interface is deprecated. Hence, the `ipseconfig` CLI command is deprecated.
- The `switchUptime` CLI command is deprecated.

Chapter 11: What's New in FOS v8.2.1

11.1 Hardware

The following sections list new hardware introduced with this release and hardware that is no longer supported with this release.

11.1.1 New Devices

Product Name	Device Name
Brocade 7810	Gen 6 (32Gb/s) Distance Extension Switch

11.1.2 New Blades

None.

11.1.3 New Optical Transceivers

FOS 8.2.1 supports the following new optical transceiver on the noted devices:

- 32Gb/s Fibre Channel 25 KM ELWL SFP (customer P/N XBR-000278) on the Brocade G620, G630, FC32-48, and SX6 blade.

11.1.4 Deprecated Hardware

None.

11.2 Software Features

The following sections list new, modified, and deprecated software features for this release.

11.2.1 New Software Features

The following software features are new in this release:

- Counterfeit License Protection
- REST API with New RESTCONF Modules
- Management Interface Rate Limiting

11.2.1.1 Counterfeit License Protection

FOS 8.2.1 introduces counterfeit license protection (CLP) on the Brocade 6505, 6510, G610, G620, and 7810 to prevent misuse of the `licenseAdd` command. CLP performs the following actions based on the number of times that the `licenseAdd` command is invoked:

- RASLOG WARNING message when 25 invalid `licenseAdd` operations are detected within a 24-hour period.
- RASLOG CRITICAL message when 40 invalid `licenseAdd` operations are detected within a 24-hour period.
- Shuts down a switch when 50 invalid `licenseAdd` operations are detected within a 24-hour period.

A switch that is shut down due to CLP detection will no longer be able to boot to a functional state. Customers may request a replacement unit from their support provider.

11.2.1.2 REST API with New RESTCONF Modules

FOS 8.2.1 expands REST API support from that supported in FOS 8.2.0a with the following new features and corresponding RESTCONF modules:

- Physical chassis, FRU, and optical transceiver: `brocade-chassis`, `brocade-fru`, and `brocade-media`
- Switch configuration: `brocade-fibrechannel-configuration`
- SupportSave: `brocade-operation-supportsave` and `brocade-operation-showstatus`
- Trunking: `brocade-fibrechannel-trunk`
- RASLOG and syslog configuration: `brocade-logging`
- System security: `brocade-security`
- System time zone and time server: `brocade-time`
- Monitoring and Alerting Policy Suite (MAPS): `brocade-maps`

FOS 8.2.1 enhances the following existing RESTCONF modules:

- `brocade-fibrechannel`
- `brocade-fibrechannel-switch`
- `brocade-access-gateway`

For a detailed description of the new modules and attributes, refer to the *Brocade Fabric OS REST API Reference Manual* for FOS 8.2.1.

11.2.1.3 Management Interface Rate Limiting

FOS 8.2.1 implements hardware-based ingress rate limiting on the management interface of X6 directors to prevent denial of service (DOS) attacks through the Ethernet management interface. When this feature is enabled, hardware performs ingress rate limiting when a DOS attack on the Eth0 or Eth3 management interface is detected. Normal management application traffic from Web Tools and SNMP is not affected when there is no DOS attack. These applications may appear sluggish when a DOS attack is detected.

11.2.2 Modified Software Features

The following software features have been enhanced in this release:

- MAPS (Monitoring and Alerting Policy Suite)
- Access Gateway
- Fabric Services
- System Security
- configure Command Enhancements
- Extension
- Power supply microcontroller firmware utility

- Miscellaneous

11.2.2.1 MAPS Enhancements

11.2.2.1.1 UCS/FI Login Imbalance Monitoring

FOS 8.2.1 adds MAPS monitoring of Cisco UCS Fabric Interconnect (FI) connections to Brocade switches in NPV mode. MAPS monitors the distribution of UCS servers over the uplinks between FI and Brocade switches to remain balanced over time. When MAPS detects an imbalance, it alerts the SAN administrator of the condition or triggers an automatic rebalance action.

11.2.2.1.2 Miscellaneous

11.2.2.1.2.1 Default Rule Change

FOS 8.2.1 replaces the default rule names in FOS 8.2.0x detailed in the following table with the new default rule names:

FOS 8.2.0x Rule Names	FOS 8.2.1 Rule Names
defALL_DPIP_EXTN_FLOW_C	defALL_DPIP_EXTN_FLOW_P_90
defALL_DPIP_EXTN_FLOW_M	defALL_DPIP_EXTN_FLOW_P_80
defALL_DPIP_EXTN_FLOW_A	defALL_DPIP_EXTN_FLOW_P_65
defALL_DPIP_EXTN_FLOW_MAX	defALL_DPIP_EXTN_FLOW_P_TOTAL

NOTE The default rules will be automatically converted to the new rule names during firmware upgrade from FOS 8.2.0x to FOS 8.2.1 or later. However, user-defined rules of the IP_EXTN_FLOW monitoring system must be changed manually to follow the new rule name format.

11.2.2.1.2.2 Alert Severity Change

FOS 8.2.1 changes the alert severity from ERROR to CRITICAL for the following default rule:

```
defALL_E_PORTSC3TXTO_20 ALL_E_PORTS(C3TXTO/MIN>20) RASLOG
```

FOS 8.2.1 changes the alert severity from WARNING to ERROR for the following default rule:

```
defALL_FANFAN_STATE_FAULTY ALL_FANS(FAN_STATE/NONE==FAULTY) RASLOG
```

11.2.2.2 Access Gateway Enhancements

11.2.2.2.1 Slow-Drain Device Quarantine on AG

FOS 7.4 and later support Slow-Drain Device Quarantine (SDDQ) to mitigate congestion due to slow-drain devices connected to switches in native mode. FOS 8.2.1 enhances SDDQ support on AG to be able to quarantine slow-drain devices connected to Access Gateway.

11.2.2.2.2 Port NPIV Configuration

FOS 8.2.1 adds support of the `portCfgNpivPort` command for a switch in AG mode. With this support, administrators can enable or disable NPIV mode for a port when a switch is in Access Gateway mode.

11.2.2.3 Fabric Services Enhancements

11.2.2.3.1 GZS and GAZS Commands

FOS 8.2.1 adds support of the Get Zone Set (GZS) and Get Active Zone Set (GAZS) commands under FC-GS-8 for zone servers. GZS queries for Zone Set Database, whereas GAZS queries for Active Zone Set (or Effective Configuration Set).

11.2.2.3.2 Impaired Port Enhancements

FOS 8.2.1 enhances the impaired port feature introduced in FOS 8.2.0. With FOS 8.2.0, an impaired port can be used as a principal link, which is used in fabric-related events, even though there are parallel nonimpaired links available. With FOS 8.2.1, when a principal link is impaired and parallel links exist, an alternate link will be selected as the principal link.

11.2.2.4 System Security Enhancements

11.2.2.4.1 Minimum Password Difference

FOS 8.2.1 adds the new `-minDiff` to `passwdcfg` CLI command to enable SAN administrators to configure the password policy to require the minimum number of characters that must be different between a current password and a new password.

11.2.2.4.2 Session Logout Message

FOS 8.2.1 displays a logout message for SSH or Telnet session logout, exit, or timeout on the standard session terminal window.

11.2.2.4.3 rootAccess Command Change

FOS 8.2.1 adds the `-force` option to the `rootAccess` command to bypass the interactive prompt of the command execution.

11.2.2.4.4 HTTPS KeepAlive

FOS 8.2.1 adds support of HTTP server connection KeepAlive. The server KeepAlive is supported only with secure HTTPS connections to switches. The KeepAlive support may be enabled with the command `mgmtapp --enable keepalive` in FOS 8.2.1 or later.

11.2.2.5 configure Command Enhancements

FOS 8.2.1 introduces options to the `configure` CLI command to allow a number of switch configuration parameters to be set without going through the interactive CLI menu. For details, refer to the *Brocade Fabric OS Command Reference Manual* for FOS 8.2.1.

11.2.2.6 Extension Enhancements

FOS 8.2.1 supports dynamic LAG (LACP) on Gigabit Ethernet LAN ports on extension platforms.

11.2.2.7 Power Supply Microcontroller Firmware Utility

Some power supply models for Brocade Gen 6 platforms support field upgrade of the firmware image used by their microcontrollers. FOS 8.2.1 introduces the `psutil` CLI command for field upgrade of the power supply microcontroller firmware. The power supply firmware is packaged as part of FOS 8.2.1 and later. Administrators can use the `psutil` command to check the power supply firmware version and when necessary upgrade to a later version.

11.2.2.8 Miscellaneous Enhancements

FOS 8.2.1 includes the following miscellaneous enhancements:

11.2.2.8.1 chassisName Command

FOS 8.2.1 enhances the `chassisName` command to increase the name length from 15 characters to 31 characters on the DCX 8510 and X6 directors.

11.2.2.8.2 ISL R_RDY in Base Switch

FOS 8.2.1 supports the `portcfgislmode` command to configure ISL R_RDY mode on the ISLs in a base switch, that is, the XISLs. With this enhancement, devices that support R_RDY mode can also be used on XISLs.

11.2.2.8.3 sfpShow -link Enhancement

FOS 8.2.1 displays the alert thresholds for peer port optics through the `sfpShow -link` option. The alert thresholds are displayed for voltage, temperature, Tx Bias, Tx Power, and Rx Power metrics. The alert thresholds are displayed for peer port optics only.

11.3 CLI Command Changes

The following sections list new, modified, and deprecated commands for this release.

11.3.1 New Commands

The following commands are new in this release:

- bladePortMap
- deviceLogin
- factoryFanShow
- psUtil

11.3.2 Modified Commands

Refer to the Modified Commands section of the *Brocade Fabric OS Command Reference Manual* for Fabric OS 8.2.1.

11.3.3 Deprecated Commands

The *Brocade Fabric OS Command Reference Manual* documents all FOS commands that are officially supported. Any commands not listed in the command reference for a specific release are not supported and may be subject to removal without notification. Refer to the Deprecated Commands section in the *Brocade Fabric OS Command Reference Manual* for Fabric OS 8.2.1.

11.4 Supported Standards and RFCs

This software conforms to the Fibre Channel standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. For a list of FC standards conformance, visit the following Broadcom SAN Standards website:

<https://www.broadcom.com/support/fibre-channel-networking/san-standards/>

Chapter 12: Software License Support

12.1 Optionally Licensed Software

Fabric OS 8.2 includes all basic switch and fabric support software, as well as optionally licensed software that is enabled using license keys.

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 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 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 DCX 8510-8, DCX 8510-4, Brocade 6510, Brocade 6520, Brocade 7840, or Brocade G620 to be configured as an EX_Port supporting Fibre Channel Routing (FCR). This eliminates the need to add an FR4-18i blade or use a Brocade 7500 for FCR purposes, and it also provides either quadruple or octuple the bandwidth for each FCR connection (when connected to another 16Gb/s- or 32Gb/s-capable port).

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. This eliminates the need to add an FR4-18i blade or use a Brocade 7500 for FCR purposes, and it also provides octuple the bandwidth for each FCR connection (when connected to another 32Gb/s-capable port).

Advanced Extension – This license enables two advanced extension features: FCIP Trunking and Adaptive Rate Limiting. The FCIP Trunking feature allows multiple IP source and destination address pairs (defined as FCIP circuits) via multiple 1GbE or 10GbE interfaces to provide a high-bandwidth FCIP tunnel and failover resiliency. In addition, each FCIP circuit supports four QoS classes (Class-F, High, Medium, and Low Priority), each as a TCP connection. The Adaptive Rate Limiting feature provides a minimum bandwidth guarantee for each tunnel with full utilization of the available network bandwidth without impacting throughput performance under a high-traffic load. This license is available on the DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis. The upgrade license on Brocade 7810 includes this license to enable 10GbE ports.

10GbE FCIP/10G Fibre Channel – This license enables the two 10GbE ports on the FX8-24 and/or the 10G FC capability on FC16-xx blade ports supported on DCX 8510 platforms except for the FC16-64 blade. On the Brocade 6510 and Brocade 6520, this license enables 10G FC ports. The upgrade license on Brocade 7810 includes this license to enable six 10GbE ports. This license is not applicable to the Brocade 7840, Brocade G620, or Brocade X6 platforms.

On the FX8-24:

With this license installed and assigned to a slot with an FX8-24 blade, two additional operating modes (in addition to 10x1GbE ports mode) can be selected:

10x1GbE ports and 1x10GbE ports
or

2x10GbE ports

On the FC16-xx:

Enables 10G FC capability on an FC16-xx blade in a slot that has this license.

On the Brocade 6510 and Brocade 6520:

Enables 10G FC capability on Brocade 6510 and Brocade 6520 switches.

This license is available on the DCX 8510-8 and DCX 8510-4 on an individual slot basis.

Advanced FICON Acceleration – This licensed feature uses specialized data management techniques and automated intelligence to accelerate FICON tape read and write and IBM Global Mirror data replication operations over distance, while maintaining the integrity of command and acknowledgement sequences. This license is available on the Brocade 7840 and the Brocade DCX 8510-8 and DCX 8510-4 for the FX8-24 on an individual slot basis.

ICL POD License – This license activates ICL ports on DCX 8510 or X6 platform core blades. An ICL license must be installed on the director platforms at both ends of the ICL connection.

On the Brocade DCX 8510-8 and X6-8:

The first ICL POD license enables 16 (half of the total) UltraScale ICL QSFP ports on the DCX 8510-8 or X6-8 Directors, enabling 8 ICL ports on each core blade. These are QSFP port numbers 0, 1, 2, 3, 4, 5, 6, and 7 on the DCX 8510-8; while on the X6-8, the QSFP port numbers are 0, 1, 2, 3, 8, 9, 10, and 11. The second ICL POD license enables the remaining 16 UltraScale ICL QSFP ports on the directors. These are QSFP port numbers 8, 9, 10, 11, 12, 13, 14, and 15 on each core blade of the DCX 8510-8; while on the X6-8, these are QSFP port numbers 4, 5, 6, 7, 12, 13, 14, and 15 on each core blade.

Note that the trunk boundaries are different between CR32-8 core blades on the X6-8 and CR16-8 core blades on the DCX 8510-8.

On the Brocade DCX 8510-4 and X6-4:

ICL POD licenses are different between X6-4 and DCX 8510-4 Directors. On the X6-4, the first ICL POD license enables 8 (half of the total) UltraScale ICL QSFP ports on the director, enabling 4 ICL ports on each core blade, which are QSFP port numbers 0, 1, 4, and 5. The second ICL POD license on the X6-4 enables the remaining 8 UltraScale ICL QSFP ports on the director, which are QSFP port numbers 2, 3, 6, and 7 on each core blade. On the DCX 8510-4, a single ICL POD license enables all 16 UltraScale ICL QSFP ports on the director.

Enterprise ICL (EICL) License – The EICL license is required on a Brocade DCX 8510 chassis when that chassis is connected to four or more Brocade DCX 8510 chassis via ICLs. This license is not applicable to X6 Directors.

This license requirement does not depend upon the total number of DCX 8510 chassis that exist in a fabric, but only on the number of other chassis connected to a DCX 8510 via ICLs.

NOTE The EICL license supports a maximum of nine (9) DCX 8510 chassis connected in a full-mesh topology or up to twelve (12) DCX 8510 chassis connected in a core-edge topology. Refer to the *Brocade SAN Scalability Guidelines* document for additional information.

WAN Rate Upgrade 1 License – The WAN Rate Upgrade 1 license provides additional WAN throughput up to 10Gb/s on a Brocade 7840. The base configuration for a Brocade 7840 without this license provides WAN throughput up to 5Gb/s.

WAN Rate Upgrade 2 License – The WAN Rate Upgrade 2 license provides unlimited WAN throughput (up to the hardware limit) on a Brocade 7840. WAN Rate Upgrade 2 licenses also enable the use of two 40GbE ports on a Brocade 7840. The 40GbE ports cannot be configured without the WAN Rate Upgrade 2 license. A WAN Rate Upgrade 1 license must be installed on a Brocade 7840 before a WAN Rate Upgrade 2 license is installed. A WAN Rate Upgrade 1 license cannot be removed before the WAN Rate Upgrade 2 license has been removed.

NOTE The WAN Rate Upgrade 1 and WAN Rate Upgrade 2 licenses apply only to Brocade 7840 platforms. They control the aggregate bandwidth for all tunnels on that Brocade 7840. The entire capacity controlled by the licenses can be assigned to a single tunnel, or a portion of the capacity can be assigned to multiple tunnels. The total bandwidth aggregated for all tunnels should not exceed the limits established by the licenses.

Extension Upgrade License – 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, 6 10Gb/s Ethernet 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.

NOTE FOS v8.2.2 and later supports 6 10Gb/s Ethernet ports in base configuration of Brocade 7810. 10Gb/s Ethernet ports can be enabled without the Extension Upgrade license.

12.2 Temporary License Support

The following licenses are available in Fabric OS 8.2.2 as either universal temporary or regular temporary licenses:

- Fabric (E_Port)
- Extended Fabric
- Trunking
- High Performance Extension
- Advanced Performance Monitoring
- Fabric Watch
- Integrated Routing
- Integrated Routing Ports on Demand
- Advanced Extension
- Advanced FICON Acceleration
- 10GbE FCIP/10GFibre Channel
- FICON Management Server (CUP)
- Enterprise ICL
- Fabric Vision
- WAN Rate Upgrade 1
- WAN Rate Upgrade 2
- Extension Upgrade

NOTE Temporary licenses for features available on a per-slot basis enable the feature for any and all slots in the chassis.

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 and universal temporary licenses for Brocade 7810 Extension Upgrade are supported with FOS v8.2.2 or later. Temporary and universal temporary license for Extension Upgrade do not enable additional ports on 7810.

Chapter 13: Hardware Support

13.1 Supported Devices

The following devices are supported in this release:

- 6505, 6510, 6520, DCX 8510-4, DCX 8510-8
- 6543, 6547, 6548, 6558
- 7840

Use of this Fabric OS release on a switch that has reached its end of support date will result in restricted use of some support level functions. Firmwaredownload, SupportSave and other support commands will not be available. All other basic operational capabilities will be unaffected.

13.2 Supported Blades

13.2.1 DCX 8510-8/DCX 8510-4 Blade Support

Fabric OS 8.2 software is fully qualified and supports the blades for the DCX 8510-8 and DCX 8510-4 as noted in the following table:

Blades	OS Support
FC16-32, FC16-48 16G FC blades	Supported.
FC16-64 blade ^{1, 2}	Supported.
FC8-64 64-port 8-Gb port blade	Not supported.
FC8-32E, FC8-48E	Not supported.
FCIP/FC Router blade (FR4-18i)	Not supported.
Virtualization/Application blade (FA4-18)	Not supported.
Encryption blade (FS8-18)	Not supported.
Extension blade (FX8-24)	Supported. Up to a maximum of four blades of this type.
FCoE/L2 CEE blade FCOE10-24	Not supported.

¹ 8510 core blade QSFPs, part numbers 57-1000267-01 and 57-0000090-01, are not supported in the FC16-64. The QSFPs supported in the FC16-64, part number 57-1000294-02, is supported on 8510 core blades.

² E_Port connections on the FC16-64 blade have the following restriction: connecting a QSFP port between an FC16-64 blade and an ICL QSFP port on a core blade is not supported.

13.3 Supported Power Supplies

13.3.1 DCX 8510-8 Power Supply Requirements

13.3.1.1 Typical Power Supply Requirements for Blades in DCX 8510-8 Backbones

(For a specific calculation of power draw with different blade combinations, see Appendix A, Power Specifications, in the *Brocade DCX 8510-8 Backbone Hardware Reference Manual*.)

Configured Number of Ports	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant Configurations)	DCX 8510-8 @200–240 VAC (Redundant Configurations)	Comments
Any combination of 8-Gb or 16-Gb ports with QSFP ICLs	FC16-32, FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2 ³ Power Supplies
256 16-Gb ports + QSFP ICLs	FC16-32, FC16-48 (Maximum of fully populated FC16-32 blades), FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2 ³ Power Supplies Max 8 FC16-32 port blades
192 16-Gb ports & max 2 intelligent blades (FX8-24) with QSFP ICLs	FC16-32, FC16-48, FC16-64, FX8-24	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2 ³ Power Supplies Max four FC16-48 port blades and max 2 intelligent blades
336 16-Gb ports + QSFP ICLs	FC16-48 (Maximum of seven FC16-48 blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2 ³ Power Supplies Max 7 FC16-48 port blades
384 16-Gb ports + QSFP ICLs	FC16-48	Port Blade	Not Supported	4 Power Supplies	200–240 VAC: For DCX 8510-8, four (2+2) ³ 220 VAC Power Supplies are required.
384 16-Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2 ¹ Power Supplies
Any combination of 8-Gb or 16-Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FX8-24	Intelligent Blade / Combination	Dependent on the configuration. Requires a power calculation for the specific configuration.	2 or 4 Power Supplies, depending on the configuration	For DCX 8510-8, four (2+2) ³ 220 VAC Power Supplies are required when any special-purpose blades are installed.

³When a 2+2 power supply combination is used, the users are advised to configure the MAPS setting for switch Marginal State to be one Bad Power Supply.

Configured Number of Ports	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant Configurations)	DCX 8510-8 @200–240 VAC (Redundant Configurations)	Comments
512 16-Gb ports	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2 ³ Power Supplies
512 16-Gb ports + QSFP ICLs	FC16-64	Port Blade	4 Power Supplies	2 Power Supplies	200–240 VAC: 1+1 Power Supplies 110 VAC: 2+2 ³ Power Supplies

13.3.2 DCX 8510-4 Power Supply Requirements

13.3.2.1 Typical Power Supply Requirements for Blades in DCX 8510-4 Backbones

(For a specific calculation of power draw with different blade combinations, refer to Appendix A, Power Specifications, in the *Brocade DCX 8510-4 Backbone Hardware Reference Manual*.)

Configured Number of Ports	Blades	Type of Blade	DCX 8510-4 @110 VAC (Redundant Configurations)	DCX 8510-4 @200–240 VAC (Redundant Configurations)	Comments
96 ports max with QSFP ICLs	FC16-32	Port Blade	2 Power Supplies	2 Power Supplies	1+1 redundancy with 110 or 200–240 VAC power supplies
Any combination of 8-Gb or 16-Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, FC16-64, FX8-24	Intelligent Blade / Combination	Not Supported	2 Power Supplies	200–240 VAC: 1+1 Power Supplies

13.3.3 Supported Optics

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

Note: In FOS 8.2.1 and later, the port speed configuration and SFP speed must match for WAN interfaces to come online on Extension platforms. See Extension for details.

Chapter 14: Software Upgrades and Downgrades

14.1 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 [Image Filenames](#).

14.1.1 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.

14.1.2 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.
```

14.1.2.1 Loading FOS PSDs via Brocade SANnav Management Portal

Brocade SANnav Management Portal version 2.1.1 or earlier does not support FOS PSD images. However, FOS PSD images are supported with SANnav 2.1.1.3 and later releases. SANnav 2.1.1.3 and later can both host and install FOS PSD images onto Brocade switches.

14.2 Image Filenames

Download the following images from <https://support.broadcom.com/>.

Fabric OS v8.2.3e

Image Filename	Description
v8.2.3e.md5	Fabric OS v8.2.3e Checksum
v8.2.3e_all_mibs.tar.gz	Fabric OS v8.2.3e MIBs
v8.2.3e_EXT.tar.gz	Fabric OS v8.2.3e for Linux to install on 7840 platforms
v8.2.3e_EXT.zip	Fabric OS v8.2.3e for Windows to install on 7840 platforms
v8.2.3e_pha.tar.gz	Fabric OS v8.2.3e for Linux to install on 6547 platforms
v8.2.3e_pha.zip	Fabric OS v8.2.3e for Windows to install on 6547 platforms
v8.2.3e_G5_ENTRY.tar.gz	Fabric OS v8.2.3e for Linux to install on 6505 platform
v8.2.3e_G5_ENTRY.zip	Fabric OS v8.2.3e for Windows to install on 6505 platform
v8.2.3e_G5_MID.tar.gz	Fabric OS v8.2.3e for Linux to install on 6510 platform
v8.2.3e_G5_MID.zip	Fabric OS v8.2.3e for Windows to install on 6510 platform
v8.2.3e_G5_ENTP.tar.gz	Fabric OS v8.2.3e for Linux to install on 6520 platform
v8.2.3e_G5_ENTP.zip	Fabric OS v8.2.3e for Windows to install on 6520 platform
v8.2.3e_G5_DIR.tar.gz	Fabric OS v8.2.3e for Linux to install on DCX 8510-8, DCX 8510-4 platforms
v8.2.3e_G5_DIR.zip	Fabric OS v8.2.3e for Windows to install on DCX 8510-8, DCX 8510-4 platforms
v8.2.3e_EMB.tar.gz	Fabric OS v8.2.3e for Linux to install on 6543, 6548 and 6558 platforms
v8.2.3e_EMB.zip	Fabric OS v8.2.3e for Windows to install on 6543, 6548 and 6558 platforms
v8.2.3e_releasenotes_v8.0.pdf	Fabric OS v8.2.3e Release Notes

The image files can be downloaded from <https://support.broadcom.com/>, with the exception of YANG files which are available on <https://www.broadcom.com>.

14.3 Migration Path

This section contains important details to consider before migrating to or from this FOS release.

14.3.1 Migrating to FOS v8.2.3e

Upgrading to FOS 8.2.3e can only be performed from FOS 8.2.3d, the upgrade is nondisruptive.

FOS v8.2.3e requires a Gen 5 FOS Upgrade Certificate to be installed on the switch prior to loading the new code. For switches with an active support contract, FOS Upgrade Certificates are available through the Broadcom Support Portal and OEM Assist sites.

FOS v8.2.3e is the first FOS version where the FOS Upgrade Certificate is required.

FOS Upgrade Certificate installation can be performed using the CLI command `licenseadd` or Web Tools.

Example:

```
switch:FID128:admin> licenseadd
SZFPCHMmKGrWYG4rLMHMQW3NYJQBr3xvzxvzxvzrGWPHrg3SN7fQWBRWCaF37amxxxxxx
```

```
License Added [ZFPCHMmKGrWYG4rLMHMQW3NYJQBr3xvzxvzxvzrGWPHrg3SN7fQWBRWCaF37amxxxxxx]
```

```
switch:FID128:admin> licenseshow
```

```
ZFPCHMmKGrWYG4rLMHMQW3NYJQBr3xvzxvzxvzrGWPHrg3SN7fQWBRWCaF37amxxxxxx:
```

```
Fabric OS Upgrade Certificate, valid for all FOS v8.2.3e releases
```

```
-----Truncated -----
```

NOTE Embedded switch platforms (6543, 6547, 6548, 6558) do not require a FOS upgrade certificate, and FOS upgrade certificates are not available on the Broadcom Support Portal and OEM Assist sites for these platforms.

14.3.2 Migrating from FOS v8.2

Any Brocade platform running FOS 8.2.0 or later can be non-disruptively upgraded to FOS 8.2.3d.

14.3.3 Migrating from FOS v8.1

Any Brocade platform running FOS 8.1.0a or later can be non-disruptively upgraded to FOS 8.2.3d.

On Brocade G610, nondisruptive firmware upgrade from FOS 8.1.0 to FOS 8.2.3d is not supported.

14.3.4 Migrating from FOS v8.0

Any Brocade platform and supported blades in the **DCX 8510-8/DCX 8510-4 Blade Support** table and the **X6-8/X6-4 Blade Support** table running any FOS 8.0 firmware must be upgraded to FOS 8.1.x firmware before it can be non-disruptively upgraded to FOS 8.2.3d.

14.4 Upgrade/Downgrade Considerations

Any firmware activation on a DCX 8510-8 or DCX 8510-4 with an FX8-24 blade installed will disrupt I/O traffic on the FCIP links.

Disruptive upgrades to Fabric OS 8.2.3d are allowed and are supported from FOS 8.0.x (up to a two-level migration) using the optional `-s` parameter with the `firmwaredownload` command.

Firmware downgrades from FOS 8.2.3d to FOS 8.2.0x or earlier versions on the Brocade G610 or 6505 are not allowed.

Firmware downgrade from FOS 9.0.0, 9.0.0a, and 9.0.0b to FOS 8.2.3x is not allowed. A workaround is to upgrade to FOS 9.0.1 first then to downgrade to FOS 8.2.3x. There is no such limitation on upgrade.

Chapter 15: Limitations and Restrictions

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

15.1 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 8.X* document.

15.2 Compatibility/Interoperability

15.2.1 Brocade SANnav Management Portal Compatibility

Brocade SANnav Management Portal and Global View are new SAN management software offerings for Brocade SAN environments. There are two distinct SANnav product offerings:

- Brocade SANnav Management Portal
- Brocade SANnav Global View

Brocade SANnav Management Portal allows management of one or more SAN fabrics that are in the same or different geographical locations and supports up to a maximum of 15,000 (15K) physical SAN ports. For environments that are larger than 15K ports, users can deploy multiple SANnav Management Portal instances.

Brocade SANnav Global View is a higher-level management application that provides visibility, summarization and seamless navigation across multiple SANnav Management Portal instances. Users can drill-down to any individual SANnav Management Portal instance from SANnav Global View to perform detailed monitoring, investigation, and troubleshooting.

The SANnav Management Portal 2.0.x supports managing SAN switches running Fabric OS up to v8.2.2x. Compatibility with FOS versions can be found in the SANnav Management Portal 2.0.x Release Notes. FOS v8.2.2a and later require FOS EULA acceptance during firmware migration. The SANnav Management Portal 2.0.x does not support firmware migration from FOS v8.2.2a and later to any FOS version. Use the SANnav 2.1 Management Portal 2.1.x for firmware migration. Alternatively, use WebTools or the CLI in FOS v8.2.2a or later for firmware migration.

15.2.2 Web Tools Compatibility

Fabric OS 8.2.2a is qualified and supported with Oracle Java version 8 update 202. See the “Important Notes” section for more details.

NOTE Microsoft Edge version 79 and later (Chromium-based) is not supported with Web Tools.

15.2.3 SMI Compatibility

It is important to note that host SMI-S agents cannot be used to manage switches running Fabric OS 8.2.2a. If you want to manage a switch running Fabric OS 8.2.2 using the SMI-S interface, you must use SMI agent integrated in either Professional Plus or Enterprise edition of Brocade Network Advisor.

15.2.4 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-life dates for all versions of Fabric OS software, visit the following Brocade website: <https://www.broadcom.com/support/fibre-channel-networking/eol>.

Supported Products	Fabric OS Interoperability
Brocade 5424, 5430, 5431, 5432, 5450, 5460, 5470, 5480, NC-5480	7.4.2 or later
Brocade 300	7.4.2 or later
Brocade 7800	7.4.2 or later
Brocade DCX 8510-8/DCX 8510-4	FOS 8.2.0 or later
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS 8.2.0 or later
Brocade 6505, 6510, 6520, 7840	FOS 8.2.0 or later
Brocade 6543	FOS 8.2.0 or later
Brocade 6547, 6548	FOS 8.2.0 or later
Brocade 6558	FOS 8.2.0 or later ⁴
Brocade G610	FOS 8.2.0 or later
Brocade G620	FOS 8.2.0 or later
Brocade G630	FOS 8.2.0 or later
Brocade 7810	FOS 8.2.1 or later
Brocade X6-8/X6-4	FOS 9.x
Brocade X6-8/X6-4 with FC32-48 blade or SX6 blade	FOS 9.x
Brocade X6-8/X6-4 with FC32-64 blade	FOS 9.x

15.2.5 SNMP Support

Fabric OS 8.2.3 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 8.2.2.

⁴Support merged from embedded FOS releases.

15.2.5.1 Obtaining MIBs

You can download the MIB files required for this release from the Downloads area of the Broadcom support portal. To download the Brocade-specific MIBs, you must have a user name 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 **Hardware > Brocade Storage Networking > My Downloads**.
3. Navigate to the FOS PSD image for your Brocade platform.
4. Navigate to the link for the MIBs package and download the file to your drive.

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

15.2.6 REST API Support

Fabric OS 8.2.3c documents the supported REST API functions in the *Brocade Fabric OS REST API Reference Manual*.

15.2.6.1 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 go to <https://www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system>.

Alternatively, download the YANG files for a specific FOS version from <https://github.com/brocade/yang>

15.3 Important Notes

15.3.1 System Security

FOS v8.2.3d includes the following enhancements and support updates:

- Support single bind for LDAP login

The following Microsoft LDAP versions are supported:

- Windows Server 2019, schema 88 -with certificate support
- Windows Server 2022, schema 88 -with certificate support

Support for previous versions of Microsoft LDAP is deprecated in FOS v8.2.3d.

15.3.2 FCoE

The following topologies for FCoE on the FC32-64 are not supported with FOS 8.2.2 or later:

- 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.

15.3.3 FC-NVMe

- FOS 8.1.0 or later is required to support FC-NVMe devices.
- FOS 8.2.1 or earlier does not support FC-NVMe over FCR configurations. FOS 8.2.1b supports FC-NVMe in edge fabric to edge fabric over FCR configuration.

15.3.4 In-flight Encryption and Compression

- FOS 8.2 supports in-flight encryption and compression on the Brocade 6510, 6520, DCX 8510, G620, G630, and FC32-48 port blade. In-flight encryption or compression on the Brocade G620 and G630 is supported with FOS 8.2.0a or later.
- To enable in-flight encryption on the Brocade G620, SFP ports 44 to 47 must be disabled. If ports 44 to 47 have been configured for in-flight compression with FOS 8.1.x or earlier, a firmware upgrade to FOS 8.2.0a or later will be blocked until in-flight compression is moved to other ports in the switch.
- FOS 8.2.1a or later is required to support trunking for encryption ports on the FC32-48 port blade.
- Firmware upgrade to FOS v8.2.2 or later with encryption ports enabled on FC32-48 blade is nondisruptive.

15.3.5 VM Insight

- VM Insight is supported on the Brocade G610, G620, G630, and X6 running FOS 8.1.0 and later. Brocade Gen 5 Fibre Channel platforms support frames with the optional FC Application Header for VM Insight to pass through. The Brocade 7840 and SX6 running FOS 8.1.0 support the Application Header in the FCP emulating tunnel. The FCP emulating tunnel or FICON emulation is not supported in other extension platforms or earlier firmware. Nonemulating tunnel on extension platforms support pass through of the Application Header.
- VM Insight is not supported across FCR, but frames with the Application Header may traverse through FCR.
- FOS 8.2.0 supports VM performance metrics in flows on the ingress F_Port only. The Brocade G610 and G620 support FC metrics. Brocade X6 Directors support both FC metrics and SCSI IO metrics.
- Legacy static flow does not monitor SCSI IOPS statistics for frames with the Application Header.
- Duplicate subflow entries are displayed after a switch HA failover or multiple restarts of VM traffic without clearing the status. The workaround is to use the `flow --reset sys_mon_all_vms` command.
- FOS 8.2.0 does not support VM Insight for FC-NVMe traffic.

15.3.6 ClearLink Diagnostics (D_Port)

- Fabric OS 8.2 supports D_Port tests between two Brocade switches and between Brocade switches and Gen 5 (16Gb/s) and Gen 6 (32Gb/s) Fibre Channel adapters from QLogic and Emulex. The following are specific adapter models and driver versions tested by Brocade with Fabric OS 8.2 for ClearLink.⁵

	Emulex 16G Adapter	Emulex 32G Adapter	QLogic 16G Adapter	QLogic 32G Adapter
Adapter Model	LPe16002B-M6	LPe32002-M2	QLE2672	QLE2742
Adapter Firmware	11.4.204.20	11.4.142.23	v8.05.44	v8.05.44
Adapter Driver	11.4.142.23	11.4.204.8	STOR Miniport 9.1.17.21	STOR Miniport 9.1.17.21

- The D_Port long-duration test can be run only on one port at a time.
- Long-duration electrical loopback tests are not supported.
- D_Port tests on 4x32GFC breakout QSFP optics (P/N 57-1000351-01) and 128GFC non-breakout QSFP optics (P/N 57-1000331-01) have the following restrictions:
 - D_Port for these modules in X6 ICL ports is supported without electric or optical loopback tests.
 - D_Port on any user port connected by a QSFP require all four user ports within the same QSFP to be in D_Port mode.
 - D_Port tests require all user ports in a QSFP to be in the same logical switch.
 - Dynamic or On-Demand D_Ports are not supported on the user ports in these modules.
- If a D_Port test between a Brocade switch and an Emulex adapter is stopped shortly after the test has started, the adapter firmware may display “No FC Cables connecting the port to switch.” The workaround is to restart the D_Port test until completion.
- If a D_Port test is run through optical media for long distance but the ports are not configured for long distance, D_Port test can fail without a pre-check error message about the configuration mismatch.

15.3.7 Forward Error Correction

- FEC is mandatory with Gen 6 Fibre Channel operating at 32Gb/s. 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 8.x Compatibility Matrix* for supported DWDM equipment and restrictions on FEC use.

15.3.8 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.

⁵ Adapter firmware or driver versions that are later than the ones listed in the table may not work.

15.3.9 Ingress Rate Limiting

- Fabric OS 8.2 does not support ingress rate limiting on Brocade Gen 6 (G610, G620, G630, or X6) platforms.

15.3.10 Ethernet Management Interface

- The recommended interface speed configuration for a Brocade G620 is 1G auto-negotiate. If a G620 is configured for 10/100M Gb/s forced-speed and fails to establish a link, use a cross-over cable.
- 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 are not supported since FOS v8.1.x and is blocked. Firmware upgrade to FOS v8.2.2 is blocked if half-duplex mode is configured.
- External default route to the private IPv4 Class B network of 172.16.0.0/16 is unreachable over the management interface due to the existence of a more specific route from an internal Virtual Fabric ID address of 172.16.0.61/16 for FID 128. The solution is to delete the external default route or change it to a more specific address. The Virtual Fabric address will no longer block management access to the IPv4 Class B address range of 172.16.0.0/16.

15.3.11 Extension

- IP extension (IPEXT) between a Brocade 7840 and an SX6 blade is supported only if the 7840 is running FOS 8.0.2 or later. FCIP extension between a Brocade 7840 with FOS 8.0.2 or later. An SX6 blade with FOS 8.0.2 or later is supported. Extension between a Brocade 7840 or SX6 and a Brocade 7810 is supported only if the 7840 or SX6 is running FOS 8.2.0 or later. The following table documents the combinations.

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware	Supported
7840	8.0.2 or later	7840	8.0.2 or later	Both FCIP and IPEXT traffic
SX6	8.0.2 or later	7840	8.0.2	FCIP traffic but not IPEXT traffic
SX6	8.0.2 or later	7840	8.0.2 or later	Both FCIP and IPEXT traffic
SX6	8.0.2 or later	SX6	8.0.2 or later	Both FCIP and IPEXT traffic
7840	8.2.0 or later	7810	8.2.1 or later	Both FCIP and IPEXT traffic
SX6	8.2.0 or later	7810	8.2.1 or later	Both FCIP and IPEXT traffic

- Do not to configure the HA VE pair (VE16, VE26), (VE17, VE27), (VE18, VE28), and so on, where each VE in the pair is in a different LS with a different traffic policy (port-based routing and exchange-based routing). The workaround is to configure different HA VE pairs such as (VE16, VE27), (VE17, VE26), and so on when putting each VE pair in a different LS with a different traffic policy.
- When Non-Terminate TCP (NT-TCP) is enabled on traffic control lists (TCLs) and a firmware downgrade to FOS 7.4.1d is attempted on the Brocade 7840, the downgrade will be blocked. Users must remove NT-TCP from the TCLs with NT-TCP enabled in order to downgrade the firmware. After the firmware is downgraded to FOS 7.4.1d, users can re-enable the NT-TCP flag.
- Nondisruptive firmware downloads for IP extension support nondisruption to IP traffic for all terminate TCP connections. UDP and non-terminate TCP traffic may be disrupted during HCL.
- After firmware downgrade completion, the Brocade 7840 needs a switch reboot and the SX6 needs a blade power-cycle. HCL is not supported on firmware downgrades.
- If a Brocade 7840 or Brocade X6 Director with an SX6 blade in a non-VF is assigned a fabric ID other than 128, then during a heavy traffic load, the back-end ports on the 7840 and SX6 may encounter credit loss, which can result in traffic disruption over the VE ports. This is tracked as Defect 660208.

- If a 10 Gb/s port is configured on a base configuration of Brocade 7810 with FOS v8.2.2 or later without an Extension Upgrade license, users may see configuration replay errors after the firmware on the 7810 is downgraded to FOS v8.2.1x.
- Some 10G SFP's can run at the 1G speed even though FOS 8.2.3 does not support the 1G setting. The unsupported setting causes issues. FOS 8.2.0 added a check to verify that the configured port speed matches the installed SFP; and displays a RASlog message if it does not match. Starting in FOS 8.2.1, when a 10G SFP is placed in a port configured to 1G, FOS displays the RASlog message and does not bring the port online. To resolve this issue, you must replace the SFP with a 1G SFP; or configure the port speed to 10G to match the SFP speed.
- Some 10G SFP's are able to run at 1G speed even though the setting is not supported. This was causing issues. In FOS 8.2.0 a check was added to verify the configured port speed matches the installed SFP and display a raslog message if it does not.

Starting from FOS 8.2.1 the messages will be displayed, and the port is not brought online when a 10G SFP is placed in a port configured to 1G.

The resolution is to replace the SFP with a 1G SFP or configure the port speed to 10G to match the SFP speed.

15.3.12 Brocade Analytics Monitoring Platform

- FOS 8.2.0 and later support vTap on Brocade Gen 5 and Gen 6 platforms to be monitored by the Brocade Analytics Monitoring Platform. The supported Brocade platforms include: 6505, 6510, 6520, DCX 8510, 6543, 6547, 6548, M6505, 6558, G610, G620, G630, X6.
- vTap is not supported on QSFP ports (port 96 to 127) on the Brocade G630 in Virtual Fabric (VF) mode. It is supported in non-VF mode only.
- If QSFP ports (port 96 to 127) on a Brocade G630 switch are part of the `sys_analytics_vtap` flow definition, the mirrored frames from these QSFP ports will be discarded for some duration after an HA reboot or after a `sys_analytics_vtap` flow de-activation.
- The Analytics Switch Link (ASL) connection is not supported on QSFP ports (port 96 to 127) on the Brocade G630. Enabling ASL on these ports will segment the link.
- vTap and auto-discovered AF_Ports do not support high availability. In the event that an AF_Port is rediscovered by a fabric switch after a domain change on the attached Analytics Monitoring Platform and is followed by a `hafailover` or `hareboot` of the fabric switch, the remote AF_Port information will be stale and vTap flows cannot be activated. In this case, use one of the following workarounds:
 - Manually configure the AF_Port after `hafailover` or `hareboot`.
 - Disable and then enable the AF_Port on the Analytics Monitoring Platform.
 - Deactivate the vTap flow before the firmware download, `hafailover`, or `hareboot`, and activate the vTap flow again.
- vTap and CS_CTL are mutually exclusive on a fabric switch. If CS_CTL is enabled on one port, the entire switch cannot enable vTap. An F_Port trunk supporting CS_CTL must have all ports in the trunk group enabling CS_CTL. Similarly, in order to enable vTap, all ports in an F_Port trunk must have CS_CTL disabled. In addition, the master port of a trunk should remain the same between CS_CTL enabling and disabling. If this sequence is not followed, vTap may remain active even after CS_CTL is enabled on an F_Port, or the error message "Disable QoS zones error" may be observed when enabling vTap. A suggested method is to use the following sequence:
 1. When enabling CS_CTL mode, enable it on all slave ports, followed by enabling it on the master port, noted as port M.
 2. When disabling CS_CTL mode, disable all active ports in the trunk, except the master port M. Disable CS_CTL mode on port M. Enable all ports in the trunk followed by disabling CS_CTL mode on the remaining ports.
 3. When CS_CTL is enabled on a port without any connection, after rebooting and disabling CS_CTL, vTap cannot be enabled. The workaround is to enable the port as a SIM port after disabling CS_CTL and then to toggle the port and remove the SIM port configuration.

- vTap and in-flight encryption or compression compatibility are supported only on the following platforms: Brocade DCX 8510, X6, G620, G630, and 6520. On DCX 8510 and 6520 platforms, the chassis configuration “vTap and Encryption/Compression Coexistence Mode” must be enabled when ports with vTap enabled and ports with in-flight encryption or compression enabled belong to the same ASICs. Refer to the hardware installation guides for these platforms for the port-to-ASIC mapping boundary.
- When “vTap and Encryption/Compression Coexistence Mode” is enabled, the total IOPS on the same ASIC is limited to 250,000. If the IOPS exceeds the limit, the vTap flow will be deactivated.
- When “vTap and Encryption/Compression Coexistence Mode” is enabled, the effective default zone access mode must not be “All Access.”
- Running the `flow --show sys_analytics_vtap` command when vTap and QoS High compatibility mode is enabled but the vTap flow is not active may display the following message incorrectly: “Enable vTap and QoS High Priority Zone Compatibility Mode to active vTap flow. Please use the `configurechassis` command to enable this compatibility mode.” This is tracked as Defect 604429.
- After a `configuredownload` followed by `switchenable` or a flow statistics reset on the Brocade X6 and G620, MAPS may incorrectly report a VTAP IOPS > 250,000 violation.
- AMPOS 2.2.0 or later is required to support FC32-64 blades. Users should upgrade the Brocade Analytics Monitoring Platform to AMPOS 2.2.0 or later before adding FC32-64 blades to the X6.

15.3.13 Flow Vision

- Flow Vision supports only logical group names that begin with alphabetic characters.
- Frame count statistics of a Flow Monitoring flow may stop incrementing after a `statsclear` command. To work around the problem, users may run the `slotstatsclear` command. To recover from such condition, complete the following steps:
 - a. Disable all flows in the logical switch.
 - b. Delete the problem flow.
 - c. Create a new flow to replace the problem flow.
 - d. Activate the new replacement flow.
 - e. Verify the new replacement flow.
 - f. Enable all other flows.
- IO Insight metrics are supported on ingress and egress ports on the Brocade X6 and on egress ports on Brocade G620 and G630 switches. They are not supported on Brocade G610 switches.
- Activating a Flow Monitoring flow on an egress port on the Brocade G610 with the `-frametype` parameter may cause a resource not available error.
- FC-NVMe flow IO Insight metrics are supported with a Flow Monitoring flow on a port defined on the Brocade G630 and FC32-64 blade only. Users must use the `-nsid` parameter with the `flow --create` command to monitor FC-NVMe flows. Either a valid Name Space ID (NSID) must be used or the `all` keyword must be used to select all valid NSIDs.
- When a flow is created with the `-frametype` parameter, FC-NVMe traffic is included in the metrics for the following SCSI frame types: SCSI, SCSTur, SCSEXferdy, and SCSTurGoodStatus.
- Flow Mirroring is not supported on QSFP ports (port 96 to 127) on the Brocade G630 with Virtual Fabric (VF) mode. It is supported in non-VF mode only.
- Mirror ports are not supported on QSFP ports (port 96 to 127) on the Brocade G630. Enabling a mirror port on these ports will disable the ports.
- If a flow is imported to MAPS and configured with incorrectly configured flow metrics thresholds, a high frequency violation of the thresholds may result in very slow display of the RASLOG alerts for the violations.

15.3.14 FICON

For FICON-qualified releases, refer to the Additional Considerations for FICON Environments section of the Appendix for details and notes on deployment in FICON environments. (This appendix is included only for releases that have completed FICON qualification.)

15.3.15 MAPS

MAPS monitoring of UCS server login does not support the FENCE action even though the `mapsrule` command does not block the configuration.

15.3.16 Miscellaneous

- If the ambient temperature is above the recommended operational limit, the power supply units may shut down, in particular when the ambient temperature is above 62°C for Brocade X6 Directors. This will result in the switch being shut down without any warning. Refer to the *Brocade G620 Hardware Installation Guide* and the *Brocade X6-8/X6-4 Hardware Installation Guide* for the recommended ambient temperature limits for the switches.
- 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.
- 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.
- ASN is not supported with 4x32GFC breakout optics (P/N 57-1000351-01).
- When connecting 4x32G FC breakout optics (P/N 57-1000351-01) to 32Gb/s SFP peer ports on Gen 6 platforms, ports may auto-negotiate to 16Gb/s after `switchdisable` and `switchenable` on the Gen 6 platforms with 32Gb/s SFP ports. To avoid this issue, the Gen 6 platforms with 32Gb/s SFPs should be upgraded to FOS 8.2.0 or later or to FOS 8.1.2b or later. This issue is more likely to occur when the Gen 6 platforms with 32Gb/s SFPs are X6 directors.
- Brocade G630 LEDs illuminate amber and green during power-up.
- When launching Web Tools over an HTTPS connection and a security warning message for an untrusted certificate pops up, the pop-up message should be responded to within 20 seconds.
- 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.
- In ISL between G720 or FC64-48 (64G optic) to a G630 (32G optic) may take longer to converge at 32G speed. This is applicable when the G630 switch is running pre-FOS 9.0.1. Upgrade the G630 to FOS 9.0.1 or later when connecting a G630 to a G720 or FC64-48.
- The output of CLI command `sfpshow` or any other interfaces to retrieve information from 32Gb/s 100m QSFP (Part Number 57-1000490) does not match the Part Numbers on the media sticker labels. The output shows Part Number 57-1000351 instead. This does not affect operation of the optics.

Chapter 16: 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 v8.2.x software releases are provided in the following security announcement:

<https://support.broadcom.com/external/content/SecurityAdvisories/0/24997>

Chapter 17: Defects

17.1 Closed with Code Changes in v8.2.3e2

Defect ID	Description
FOS-859350	SAN switch monitoring tools via SNMP do not function properly
FOS-863019	Supportsave, firmware upgrade and other support commands stop working

17.2 Closed with Code Changes in v8.2.3e1

Defect ID	Description
FOS-860255	High memory usage MAPS alert observed [MAPS-1003]

17.3 Closed with Code Changes in v8.2.3e

Defect ID	Description
FOS-820856	High CPU load observed on switch once a connection via WebTools is made with https.
FOS-825202	Audit log is not generated when LDAP authorization fails in non-VF mode.
FOS-826932	With a custom UDP port, syslog is not happening with IPv4 FQDN.
FOS-840406	SNMP stopped responding.
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-844544	High CPU utilization reported on switches during supportshow.
FOS-848254	CPU utilization at 100% during snmp polling.
FOS-848422	HA Out of Sync due to SNMPd terminated in FOS upgrade HA window.
FOS-849643	ISL ports become disabled when connecting FOS 8.x with FOS 7.x switch after updating Enhanced Object Zoning. switchshow as below: <pre> Index Port Address Media Speed State Proto ===== 28 28 011c00 id 8G No_Sync FC Disabled (ESC Enhanced Zone Object Name Conflict) </pre>

FOS-849751	Slow Drain devices on E or EX Port connected switches can cause excessive XTUN-1006 FCIP TX Frame Drop RASLOGs per second.
FOS-853249	cald process aborted due to memory resource not available.
FOS-854095	After a non-critical daemon failed, it did not restart successfully and the switch persistently lost HA sync.
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.

17.4 Closed with Code Changes in v8.2.3d

Defect ID	Description
FOS-806174	Duplicate member are allowed for a peer zone via GUI and CLI by different alias; However, switch loss HA sync after user created alias with same member.
FOS-810478	Switch HA out of sync in VF configuration.
FOS-824498	MAPS test email defaulted "From address" to root@switchname.domain.com on some switches and rejected by postmaster.
FOS-827306	Repeated XTUN-1997 RASLOGs generated in an Extension configuration through a 7810, 7840 or SX6 blade that may or may not be associated with a VE port down event. The specific trigger is: ttmh0933 tifa1243 timer [1] reset error
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-832909	FCR (iSwitchd) uses RSCNs to convey incremental updates to the device directory. When an RSCN fails to be delivered, the Name Server database can become out of sync across routed fabrics.
FOS-838584	Weblinker termination due to segmentation fault.
FOS-839810	User may see repeated logging of an internal firmwaredownload raslog messages.
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-841163	User can't perform firmware download on the switch from SANNav.
FOS-841254	Unexpected reboot or failover after running out of memory.
FOS-841520	Host reboot will trigger MAPs alert Condition=ALL_SFP(RXP<=200), Current Value:[RXP, 2 uW]
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-843045	MAPs alarms continue to be generated following the addition of WWN Data Protection license.
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-843463	Getting Alerts for HTTPS SW certificate triggered DAYS_TO_EXPIRE rule - defCHASSISCERT_VALIDITY.
FOS-843589	MAPs traps being sent to other monitoring software even though maps rule are configured with action 'NONE'.
FOS-844074	Detected termination of process snmpd.
FOS-844942	USERID account gets deleted.
FOS-845216	User may encounter an unexpected sudden system reboot
FOS-845750	Support for non-disruptive EX port link cost changes.
FOS-846479	Weblinker restart on switch.
FOS-847045	Switch panic is observed when a timer is added before the same exact timer expires.
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-847308	Brocade 7840 may encounter kernel panic due to OOM, with tunnels failing to come online after reboot
FOS-848567	WWN is missing in the oid when run snmpgetnext command to connUnitPortTable.

17.5 Closed with Code Changes in v8.2.3c

Defect ID	Description
FOS-800614	CLI "nsshow -t" does not list the correct device type (host or target); it shows as "Physical Unknown(initiator/target)".
FOS-806884	Detected termination of daemons during a non-disruptive firmware upgrade.
FOS-821090	weblinkerfcgd core files are generated on the switch.
FOS-821746	Edge to edge routing was not working and frames dropped on E-port or EX-port.
FOS-822366	cald terminated and kernel panicked during supportsave collections.
FOS-826227	Devices in default allaccess zone cannot communicate to each other across LISLs in FICON environment on all platform.
FOS-832152	All hosts on two AGs lost access to storage after ports were added to F-Port trunk group

FOS-832938	Class 2 Link Control frames (like ACK_1) are dropped.
FOS-835586	SNMP consumes more CPU cycles, resulting in MAPS alerts.
FOS-836232	The user will observe that Tunnel with Preshared key will not come up after config download.
FOS-836468	switchtype command not working on Admin account.
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-836531	Switch panic with maps daemon (MDD) watchdog timeout.
FOS-836572	'snmpconfig' CLI returns error 'Failed to get snmp config info' due to SNMP service not restarting after getting disrupted.
FOS-836573	FICN_1062 and FICN_1063 RASLOGs every 1.5 seconds on FICON Emulation enabled FCIP Tunnel
FOS-837088	FOS accepts REST request with an empty audit class list.
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-837280	Boot over SAN device does not work after upgrading firmware on 32G FC switches.
FOS-837538	Different (lower) tunnel throughput on 7800 or FX8-24 configuration after reboot or slot power cycle.
FOS-837583	SNMP daemon leaks memory and causes switch to hafailover/hareboot/panic when switch runs out of memory.
FOS-837755	Stale CAM entries are present on the ports, which were disabled.
FOS-837837	Performance stats for VE ports are not present in connunitportstat table
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-838514	7840, 7810 or SX6 blade encounters DP Linux out of Memory causing IO disruption
FOS-838549	Loss of paths after hafailover (firmwaredownload).
FOS-838915	Switch panic while processing an incoming Fibre Channel frame.
FOS-838977	Weblinkercfg continues crashing while processing Enumerate telemetry profile query.
FOS-839056	Frame drops affecting entire fabric after creating smaller trunks from larger trunks.
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-839346	Path loss experienced after FOS upgrade on Access Gateway
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-840717	High CPU usage reported on snmp daemon.
FOS-840768	Switch panic when trace module has memory corruptions.
FOS-840909	FCPH-1003 reports duplicate port WWN with a port that does not have the same port WWN.
FOS-841478	Duplicate PWWN detection resulted in disruption to the existing FICON CHPID.
FOS-841574	After upgrading from v8.2.1c to v8.2.3b the BSL report no longer included GE_PORT type in the report

17.6 Closed with Code Changes in v8.2.3b

Defect ID	Description
FOS-649549	Enable/disable root account using an AD account fails with error message: Cannot manage the target account due to conflicting AD permissions.
FOS-651997	One or more XTUN-1008 RASLOGs followed by tunnel down notifications at the peer switch.
FOS-658218	Switch shows the wrong ip addresses in the login information log
FOS-800722	F-ports can end up in G-port or other inconsistent state.
FOS-821089	Switch ports experience immediate hard fault or busy buffer stuck status which leads to a hard fault and possible switch fault of all ports.
FOS-825815	Kernel panic in DP during fcipathtest
FOS-827821	Device has login issue with certain optics types.
FOS-830052	Port initialization interop issues with a certain SFP, when connecting to a specific 3rd party device. This may result in some ports showing errors and some going into no_sync, port_Flt state.
FOS-830310	Firmwaredownload fails with a generic error-message: "Firmwaredownload sanity check failed. Please contact the service provider if the issue persists."
FOS-831592	3rd party applications cannot collect performance information.
FOS-831688	Various operations fail after the switch runs out of disk space.
FOS-831875	SNMP application may lose connection to switch momentarily during snmp walk of IPV6 address table and occasionally the user may observe CP lost HA SYNC if the walk is performed during hafailover/hareboot.
FOS-832112	Switch panic after receiving invalid length frame.

FOS-832434	After upgrading Brocade 6548 to FOS 8.2.3a, the user is unable to login to the switch, with the following error: login: admin "Inconsistency de" - Note: traffic may be impacted too.
FOS-832960	Disruption on Access Gateways when F-port trunks change trunk master.
FOS-833133	When doing firmwarecleaninstall, the following will be displayed on the console: INSTALL26: ERROR - Cannot get file - /sbin/create_release_file. Please verify the network is good and retry firmwarecleaninstall after reboot INSTALL26: install FAILED with 0 warnings. FirmwareCleaninstall failed, you can reboot to retry.
FOS-833550	CP may encounter kernel panic when the FCIP DP generates a large number of XTUN-1006 events per second.
FOS-833935	Encountered Weblinker posting raslog RAS-1004 with VERIFY after run out of file descriptor.
FOS-833940	SNMP panic resulted in director out of HA sync
FOS-834163	Extension tunnel on 7810, 7840 or SX6 blade will not come online in a NAT (Network Address Translation) enabled WAN environment.
FOS-834621	eHCL sequence encounters fatal FICON FD error, which results in VE recovery.
FOS-834628	User cannot create a tunnel after removing it.
FOS-834868	firmwareactivation CLI fails with SULB-1043, after staging a firmware upgrade/downgrade: 2021/09/22-14:58:50:367354, [SULB-1043], 76469/35239, SLOT 1 CHASSIS, INFO, , Firmwareactivate command failed.
FOS-834912	SANnav reports error: "Registration for telemetry profile 'xxx' has failed and Switch panic after cald termination.
FOS-834918	sfps show CLI displays all zeros for txp, rxp etc smart data, and it triggers MAPs alert event.
FOS-835154	Dual CP reboot following some zoning changes performed via HTTP.
FOS-835352	Customer experienced temporary traffic outage due to tunnel bounce.
FOS-835508	Switch panics while processing stale LISL entries.
FOS-835586	SNMP consumes more CPU cycles, resulting in MAPS alerts.
FOS-835791	Individual ports, that were previously disabled, are enabled while running CLI command switchcfgpersistentenable
FOS-836031	Switch panic after FDMI daemon terminated.
FOS-836043	DCX8510 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-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-836265	During code upgrade from FOS v8.2.1x to FOS v8.2.3x, FOS cannot completely be brought up due to cold core dumps. User observes the switch hanging.

17.7 Closed with Code Changes in v8.2.3a1

Defect ID	Description
FOS-830052	Port initialization interop issues with a certain SFP, when connecting to a specific 3rd device. This may result in some ports showing errors and some going into no_sync, port_Flt state.
FOS-831875	SNMP application may lose connection to switch momentarily during snmp walk of IPV6 address table and occasionally the user may observe CP lost HA SYNC if the walk is performed during hafailover/hareboot.
FOS-832434	After upgrading Brocade 6548 to FOS 8.2.3a, the user is unable to login to the switch. Error shown as below: login: admin Inconsistency de Note: traffic may be impacted too.

17.8 Closed with Code Changes in v8.2.3

Defect ID	Description
FOS-800300	Route is invalid on G630 E-ports.
FOS-801436	Customer encounters SNMP query failure on VF.
FOS-803493	X6 eth0 reverting to 10/half when ethif is used to configure speed/duplex settings while network connection is removed
FOS-803567	CLI sfpshow has incorrect SFP low tx values.
FOS-804873	Audit log only displays the last command issued.
FOS-804971	Switches showing MAPS-1003 raslog with 0mvolt messages on port with SFP and QSFP.
FOS-805305	D-Port test fails with Protocol Error on switch end and on HBA, EL failed despite the overall result states Passed
FOS-805457	Silent frame drops may be encountered on Brocade 6520.
FOS-806463	Following HA failover some ports appear to encounter ASIC stats errors which causes these ports to be fenced if MAPS is configured to fence ports for ITW.

FOS-806547	The ISL link between two G620 switches fails to recover and goes to "HRD_FLT" state.
FOS-807056	Test email is not sent out by switch.
FOS-807249	Switches lost management IP config after reboot.
FOS-807784	portloopbacktest is unable to detect CRC error.
FOS-808426	CLI "mapsdb --congestion" shows an event but "mapsdb --congestion -freq" doesn't show it.
FOS-808461	Switch panic during diagnostics test.
FOS-808514	After a host behind an NPIV device reboots, it is unable to discover any of its LSAN devices.
FOS-808560	When a longer FQHN is used for TACACS+ authentication, local accounts as well as AAA accounts are not accessible.
FOS-809213	Switch panics after various daemons, such as fcpd, tsd, webd, terminate while accessing configuration database resource key.
FOS-809425	When a crypto template is applied, the existing SSHd session is not terminated.
FOS-810413	Missing N-port info from "ag --show" after toggle N-ports.
FOS-810630	Users may encounter FDMI daemon termination.
FOS-811237	Zone daemon panic observed during zone change.
FOS-811459	System may encounter emd termination resulting in failover to Standby CP.
FOS-811539	POST on /rest/operations/device-management/ returns a PLOGI ELS reject error message. Credit field in portloginshow output may be large number. End devices may suddenly logout after hareboot/hafailover.
FOS-811952	Experience silent reboot (reboot reason: reset) or switch hung for hours/days.
FOS-812267	A good replacement blade cannot come up with raslog [EM-1134] rc=20074: 2019/11/19-11:28:33:895421, [EM-1134], 95966/2420, SLOT 2 FFDC CHASSIS, ERROR,, Slot 7 set to faulty, rc=20074., OID:0x43700000, em_board_lib.c, line: 1944, comp:emd, ltime:2019/11/19-11:28:33:895302 And after CLI "slotpoweron" bring back the blade, it is powered off again after active CP reboot,
FOS-812536	SNMP community strings with basic SNMPv1 queries are not recognized.
FOS-812556	Weblinker cannot restart with continuous messages; "system is not ready for HA/LS CLI cmd".
FOS-812883	Customer may encounter frame drops corresponding to specific SCSI task management commands.
FOS-812889	SX6 blade is not powered-on, when initializing the blade, after EM_INCONSISTENT failure during HA failover.
FOS-812985	Kernel or user daemon panic caused by trace module corruption.

FOS-813157	Some port stats are missing.
FOS-813299	After running statsclear on default switch, 'Current' counts of '4 History Data' section of maps database for Base Switch is cleared.
FOS-813523	BR7840 or SX6 FCIP Tunnel failure or disable can result in DP reset
FOS-813525	Fibre channel port statistics counters report large values such as "4294967295" after statistics reset.
FOS-813692	Lot of I/O failures and traffic disruption reported after performing HA failover on Gen6 chassis-based switches.
FOS-813777	SNMP OIDs swConnUnitPortTxRate and swConnUnitPortRxRate always show zero values when querying the switch in AG-mode.
FOS-813796	The user will observe the Tunnel bounce when changing circuit bandwidth.
FOS-814082	Switch panic due to esmd termination
FOS-814152	Customer enabled framelog to capture unroutables , but not all frame drops are captured in the framelog.
FOS-814430	Diag related logs are not present in SupportSave.
FOS-814484	Creating a user account with an uppercase password causes the login to fail.
FOS-814782	Firmwarecheck failure on ASC-G certificate file.
FOS-814807	SX6 AP blade fault occurs after internal backend port is disabled or a disruptive failover even though it reports HA-IN-SYNC.
FOS-815116	The BR6520 switch gets into a rolling reboot loop and needs a manual intervention to recover.
FOS-815150	AG default mapping is incorrectly set for Brocade 6547 switch.
FOS-815152	During firmwaredownload, the error message is not properly worded.
FOS-815189	Supportshow is incomplete due to "Permission denied" on /var/log directory.
FOS-815218	FCIP DP panics
FOS-815265	Observing RTWR error on fabric with DISL.
FOS-815327	Switch panic observed after essd daemon access freed memory.
FOS-815352	IPEX LAN TCP connection will report failed in the application.
FOS-815828	When changing templates and performing HA failover, the SSH config is not replicated to the standby CP.

17.9 Closed with Code Changes in v8.2.3a

Defect ID	Description
FOS-807030	Performing vulnerability scans (Qualys) leads to high CPU load and Multiple config and secnotify processes are showing as consuming all memory.
FOS-818045	Switch is flooded with messages, "attempts to send message type (1) to invalid dest (NSMIPC:0/0)", without any functional impact to switch.
FOS-820640	Flash usage exceeds 90% resulting in a switch panic.
FOS-820794	Switch remains in "MAPS Marginal state", and cannot be cleared.
FOS-820872	Periodic Cx-1014 "frame loss" raslog messages may be logged without any traffic impact. Additionally, a link reset follows each frame loss detected occurrence.
FOS-822511	After replacing MAC value in seccryptocfg, SSH and nmap show the value is not actually applied to one of the two CPs.
FOS-823675	On a 32G DWDM port, D_Port diagnostics fails on the spinfab throughput test and DWDM line flips fail.
FOS-825546	SX6 DP Panic causing IO Failures
FOS-826088	Switch panicked on long spinfab run - "ASSERT - Failed expression: VALID_PTR(ctl)"
FOS-826243	The REST peak counters for fibrechannel-statistics seen as zero despite traffic flowing.
FOS-826244	"sfpshow 5/31 -f -link" does not return correct information .
FOS-826780	Add fence and decommission actions for the monitoring items TXP and RXP in the MAPS policy.
FOS-826987	'filterportshow' output is incomplete and switch panic with console output, "BUG: Bad page map in process supportsave".
FOS-827021	In an EX-port trunk. frames routed to the slave port are dropped, result in LUN discovery issues after an edge fabric split and merge.
FOS-827217	Switch panic during tracedump.
FOS-827719	CORE and FFDC are generated on newly active CP after a dual CP firmwaredownload.
FOS-827741	MAPs messages use old port labels.
FOS-827821	Device has login issue with certain optics types.
FOS-827976	cold boot after ONMd crash when standby becomes active during hafailover process.
FOS-828208	Webtools hardware view does not show the Led status correctly for ports 50, 51 and 117 .
FOS-828373	seccertmgmt_create.py reports 400 as "client-error-code".

FOS-828392	Port Optics is not visible in Sannav with error: Fail to get SFP details.
FOS-828899	DP Panic after upgrading to FOS8.2.1 through FOS8.2.2d while running FICON XRC traffic over XRC Emulation enabled FCIP Tunnel.
FOS-829310	FICN-1062 or FICN-1063 with LastStates=0x005E005E0068 indicating that there were FICON Abort sequences processed on the emulated tunnel.
FOS-829423	FCIP DP Panic and DP Reset after switching an FCIP Circuit from wantool testing state back to active FCIP Circuit
FOS-829441	"XTUN-1001 : memory allocation error" messages in RASLOG after using FCIP SLA or manual WTOOL functionality.
FOS-829454	Port blade comes up as faulty after diagnostic run.
FOS-829537	Following an hareboot, the agautomapbalance configuration is not the same as it was before the hareboot.
FOS-829594	Issuing a switchenable when the switch is already enabled may lead to I/O disruption
FOS-829779	SANNAV fails to generate switch supportsave on switches running FOS v8.2.2 and above.
FOS-830884	WebTool "Switch Administration -> Extended Fabric" tab are missing slots for X6 directors.

17.10 Closed without Code Changes in v8.2.3

Defect ID	Description
FOS-810839	Switch rebooted after it ran out of memory.
FOS-816098	Raslog TS-1001, indicating NTP Query Failed, occurs daily or weekly.
FOS-820194	FSPF daemon crashes and causes failover.
FOS-826750	SNMP incorrectly reporting uptime of 497 days due to deprecation of switchuptime CLI command.

Revision History

Version	Summary of Changes	Publication Date
1.0	Initial document version.	4/17/2024
2.0	Correction in Migrating to FOS v8.2.3e .	5/31/2024
3.0	Specified that FOS upgrade certificates are not required and not available for embedded switch platforms in Migrating to FOS v8.2.3e . Updated Closed with Code Changes in v8.2.3e .	6/12/2024
4.0	Updated disclosed CVEs for FOS v8.2.3e in Security Vulnerability Fixes .	06/27/2024
5.0	Updated Closed with Code Changes in v8.2.3e1 .	06/27/2024
6.0	Updated disclosed CVE for FOS v8.2.3e1 in Security Vulnerability Fixes .	07/30/2024
7.0	Updated the section Security Vulnerability Fixes . Updated Closed with Code Changes in v8.2.3e2 .	12/17/2024
8.0	Updated the section Migrating to FOS v8.2.3e .	01/17/2025

