



Fabric OS v9.1.1d/v9.1.1d2/v9.1.1d7

Fabric OS v9.1.1d Release Notes Digest

Version 7.0

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 Locating Product Manuals and Release Notes	8
2.1.1 Locating Product Manuals on Broadcom	8
2.1.2 Locating Product Manuals and Release Notes on the Support Portal	8
2.2 Document Feedback	9
Chapter 3: Overview	10
Chapter 4: What is New in FOS v9.1.1d7.....	11
4.1 Hardware	11
4.2 Software	11
4.2.1 Resolution of Important Defects.....	11
Chapter 5: What's New in FOS 9.1.1d	12
5.1 Hardware	12
5.2 Software	12
5.2.1 Resolution of Important Defects.....	12
Chapter 6: What's New in FOS 9.1.1c.....	13
6.1 Hardware	13
6.2 Software	13
6.2.1 Resolution of Important Defects.....	13
Chapter 7: What's New in FOS 9.1.1b	14
7.1 Hardware	14
7.2 Software	14
7.2.1 Resolution of Important Defects.....	14
7.2.2 Enhancements	14
Chapter 8: What's New in FOS 9.1.1a.....	16
8.1 Certifications	16
8.2 Hardware	16
8.3 Software	16
8.3.1 Resolution of Important Defects.....	16
8.3.2 Enhancements	16
Chapter 9: What's New in FOS 9.1.1.....	17
9.1 Certifications	17
9.2 Hardware	17
9.2.1 Platforms	17
9.2.2 New Optical Transceivers	17
9.3 Software	18
9.3.1 Resolution of Important Defects.....	18
9.3.2 Enhancements	18

Chapter 10: Software License Support	21
10.1 Optionally Licensed Software	21
10.2 Temporary License Support	22
Chapter 11: Hardware Support	23
11.1 Supported Devices	23
11.2 Supported Blades	23
11.2.1 X6-8 and X6-4 Blade Support	23
11.2.2 X7-8 and X7-4 Blade Support	23
11.3 Supported Power Supplies	24
11.4 Supported Optics	24
Chapter 12: Software Upgrades and Downgrades	25
12.1 Platform Specific Downloads	25
12.1.1 Using FOS PSDs	25
12.2 FOS Image Filenames	25
12.3 Migration Path	26
12.3.1 Migrating to FOS 9.1.0	26
12.3.2 Migrating from FOS 9.1.x	27
12.4 Brocade Trusted FOS (TruFOS) Certificate	28
12.5 Upgrade/Downgrade Considerations	28
Chapter 13: Limitations and Restrictions	29
13.1 Scalability	29
13.2 Compatibility/Interoperability	29
13.2.1 Brocade SANnav Management Portal Compatibility	29
13.2.2 Web Tools Compatibility	29
13.2.3 Fabric OS Compatibility	29
13.2.4 SNMP Support	31
13.2.5 Obtaining MIBs	31
13.2.6 Flow Vision, IO Insight, and VM Insight	31
13.2.7 REST API Support	32
13.3 Important Notes	32
13.3.1 4G Support on Gen 6 switches	32
13.3.2 Access Gateway	32
13.3.3 Brocade Analytics Monitoring Platform	32
13.3.4 ClearLink Diagnostics (D_Port)	33
13.3.5 Diagnostic POST	33
13.3.6 DWDM	33
13.3.7 Ethernet Management Interface	34
13.3.8 Extension	34
13.3.9 FCoE	34
13.3.10 FC-NVMe	34
13.3.11 Firmware Migration	34
13.3.12 Forward Error Correction	35
13.3.13 FPGA Upgrade	35
13.3.14 Security	36
13.3.15 Zoning	37
13.3.16 Brocade X6 Field Migration	37
13.3.17 Miscellaneous	37
Chapter 14: Security Vulnerability Fixes	41

Chapter 15: Defects	42
15.1 Closed With Code Changes in FOS v9.1.1d7	42
15.2 Closed With Code Changes in FOS v9.1.1d2	43
15.3 Closed With Code Changes in FOS v9.1.1d1	43
15.4 Closed With Code Changes in FOS v9.1.1d	43
15.5 Closed With Code Changes in FOS v9.1.1c	44
15.6 Closed With Code Changes in FOS v9.1.1b	45
15.7 Closed With Code Changes in FOS v9.1.1a	46
15.8 Closed With Code Changes in FOS v9.1.1	46
Appendix A: CA Certificate Bundle Updates	48
A.1 Added CA certificates from FOS v9.1.1a	48
A.2 Removed CA certificates from FOS v9.1.1a	50
Revision History	54

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 the **supportSave** command gathers information from both CPs and any AP blades installed in the chassis.

- Detailed description of the problem, including the switch or fabric behavior immediately following the problem and any specific questions.
- Description of any troubleshooting steps already performed and the results.
- Serial console and telnet session logs.
- Syslog message logs.

Switch Serial Number.

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



The serial number label is located as follows:

- Brocade G630, G620, G610, G720, and G730 – On the switch ID pull-out tab located on the bottom of the port side of the switch.
- Brocade 7810 – 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 X6-8, X6-4, X7-8, and X7-4 – Lower portion of the chassis on the non-port side beneath the fan assemblies.

World Wide Name (WWN).

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

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

License Identifier (License ID).

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

Use the **licenseIdShow** command to display the license ID.

1.2 Related Documentation

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

Chapter 2: Locating Product Manuals and Release Notes

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

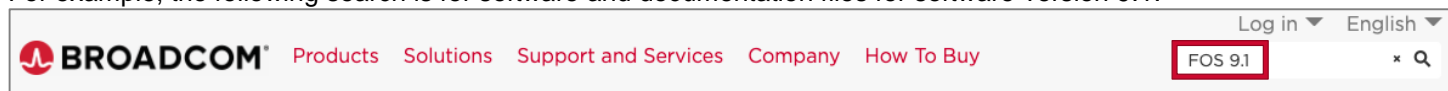
2.1 Locating Product Manuals and Release Notes

2.1.1 Locating Product Manuals on Broadcom

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

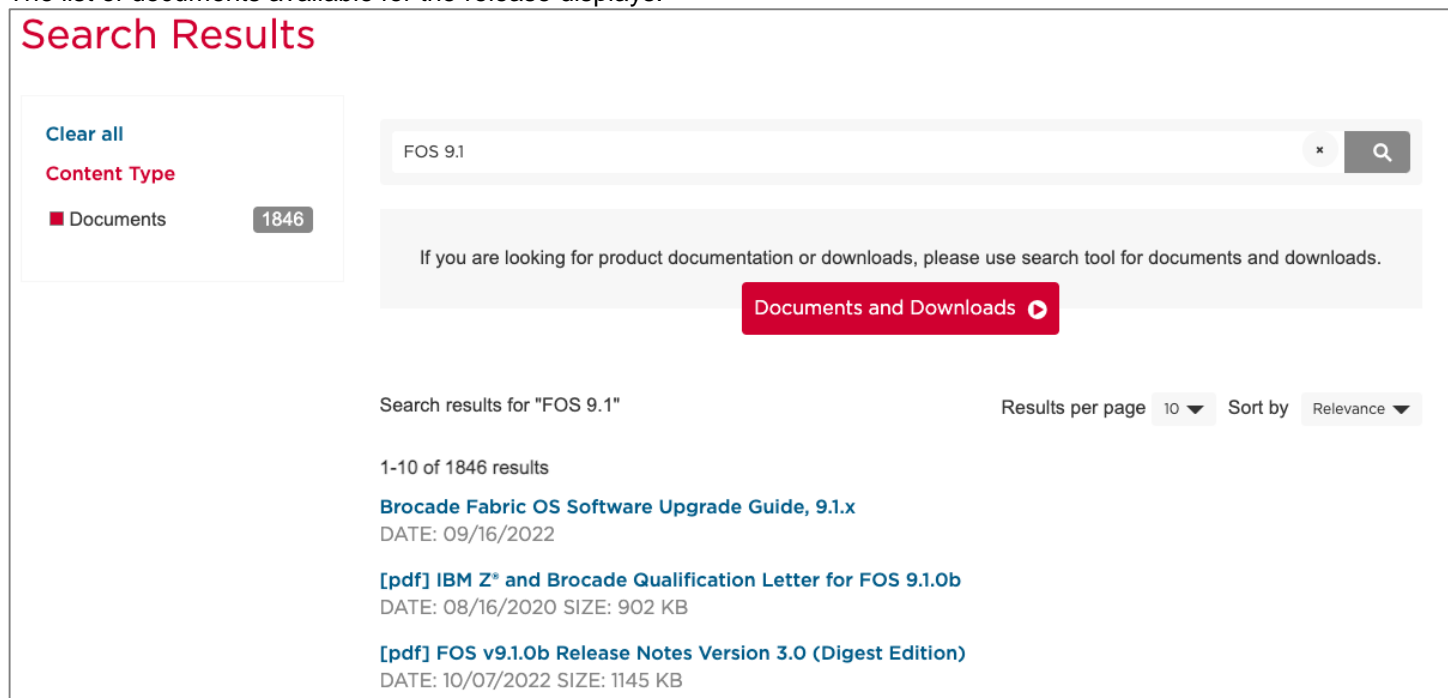
1. Go to <https://www.broadcom.com>.
2. Enter the product name or the software version number in the **Search** box.

For example, the following search is for software and documentation files for software version 9.1.



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

The list of documents available for the release displays.



2.1.2 Locating Product Manuals and Release Notes on the Support Portal

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

1. Go to <https://support.broadcom.com/>, click **Login**, and enter your username and password.
If you do not have an account, click **Register** to set up your account.
2. Select **Brocade Storage Networking** in the support portal.

2.2 Document Feedback

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

Chapter 3: Overview

The Fabric OS v9.1.1d/v9.1.1d2/v9.1.1d7 is a patch release based on FOS v9.1.1c.

The FOS v9.1.1d7 release includes all fixes from Fabric OS v9.1.1 including Fabric OS v9.1.1_01 through the following Fabric OS v9.1.1d releases:

FOS v9.1.1d

FOS v9.1.1d2

FOS v9.1.1d3 (non-public patch)

FOS v9.1.1d4 (non-public patch)

FOS v9.1.1d5 (non-public patch)

FOS v9.1.1d6 (non-public patch)

All hardware platforms and features supported in FOS v9.1.1 are supported in FOS v9.1.1d/v9.1.1d2/v9.1.1d7.

Fabric OS v9.1.1d7 includes support for the optic PN: 57-1000486-01 (32G LWL) with serial number prefix JDB.

For the following platforms:

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

Chapter 4: What is New in FOS v9.1.1d7

4.1 Hardware

The FOS v9.1.1d7 patch provides support for the optic PN: 57-1000486-01 (32G LWL) with serial number prefix JDB.

For the following platforms:

- Brocade G730
- Brocade G630
- Brocade G610
- Brocade G648
- Brocade MXG610S
- Brocade 7810 Extension Switch
- Brocade FC32-48
- Brocade SX6 Extension Blade

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

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

4.2 Software

The following lists the software changes with this release.

4.2.1 Resolution of Important Defects

The following important defects are resolved and included in FOS 9.1.1d7:

- | | |
|------------|---|
| FOS-862224 | SNMP daemon terminates. |
| FOS-858851 | User experience performance issue on Gen7 after code upgrade. |
| FOS-860632 | Standby CP in RRD state and/or SX6 blades are faulted during code upgrade. inetd on active CP no longer listens on port 514 on ipaddress of 127.3.1.x |

For a full list of closed defects included in this release see the [Defects](#) section.

Chapter 5: What's New in FOS 9.1.1d

5.1 Hardware

There is no new hardware supported with FOS v9.1.1d

5.2 Software

The following lists the software changes with this release.

5.2.1 Resolution of Important Defects

The following important defects are resolved in FOS 9.1.1d:

- FOS-849929 - Weblinker dies with a large CoreFile and SanNav keeps showing "SNMP credentials invalid" state for the switch.
- FOS-850464 - Switch HA State goes out of sync following a FOS upgrade from FOS 8.x to 9.0.x and the switch Zoning DB contains duplicated WWNs.
- FOS-851223 - Switch ran out of kernel memory and triggered daemon panic, cpu busy or port/blade fault.
- FOS-853249 - Cald process aborted due to memory resource not available.

For a full list of closed defects in this release see the [Defects](#).

Chapter 6: What's New in FOS 9.1.1c

6.1 Hardware

There is no new hardware supported with FOS v9.1.1c

6.2 Software

The following lists the software changes with this release.

6.2.1 Resolution of Important Defects

The following important defects are resolved in FOS 9.1.1c:

- FOS-849642 - Switch reported a flood of hardware errors, followed by daemons watchdog timeout and switch reboot.
- FOS-847091 - Repeat software 'verify' errors detected on X7 directors running FOS 9.1.x. Also, possible to see daemons crash due to watchdog timeout if congestion / oversubscription is severe.
- FOS-843005 – Switch panic, HA out of sync, with mdd core files during migration from FOS9.0.x to FOS9.1.x or later. Observed Raslog: [HAM-1013], 131574/20614, SLOT 1 | CHASSIS, CRITICAL, Can't restart (mdd (pid=30408)): System unready or LS trans in progress. Reboot/Failover manually if necessary.
- FOS-849852 – G610 fails to boot after power outage with reason "ERROR: can't get kernel image!".

For a full list of closed defects in this release see the [Defects](#).

Chapter 7: What's New in FOS 9.1.1b

7.1 Hardware

There is no new hardware supported with FOS v9.1.1b

7.2 Software

The following lists the software changes with this release.

7.2.1 Resolution of Important Defects

The following important defects are resolved in FOS 9.1.1b:

- FOS-844552 - Unexpected kernel panic/cold boot or HA out of sync
- FOS-846325 - On a MXG610 embedded switch, running FOS versions FOS9.0.x, FOS9.1.x, user may encounter IO service disruption after a reboot / hareboot, triggered by uboot tune DRAM failure leading to a Reset (power cycle) of the system
- FOS-843463 - The MAPS rule defCHASSISCERT_VALIDITY_15 is being triggered even though the certificate was recently replaced

7.2.2 Enhancements

FOS v9.1.1b includes the following enhancements, described in more detail below:

- The command `grep` is enhanced to allow all options to filter and sort FOS command output.

7.2.2.1 Allow all options to filter and sort FOS command output with grep

The command `grep` is enhanced to allow all options to filter and sort FOS command output. Command options `-r/R` designed for filesystem access are not allowed.

Full list of allowed options for `grep` is displayed below.

Pattern selection and interpretation:

<code>-E, --extended-regexp</code>	PATTERNS are extended regular expressions
<code>-F, --fixed-strings</code>	PATTERNS are strings
<code>-G, --basic-regexp</code>	PATTERNS are basic regular expressions
<code>-e, --regexp=PATTERNS</code>	use PATTERNS for matching
<code>-f, --file=FILE</code>	take PATTERNS from FILE
<code>-i, --ignore-case</code>	ignore case distinctions in patterns and data
<code>--no-ignore-case</code>	do not ignore case distinctions (default)
<code>-w, --word-regexp</code>	match only whole words
<code>-x, --line-regexp</code>	match only whole lines
<code>-z, --null-data</code>	a data line ends in 0 byte, not newline

Miscellaneous:

-s, --no-messages	suppress error messages
-v, --invert-match	select non-matching lines
-V, --version	display version information and exit
--help	display this help text and exit

Output control:

-m, --max-count=NUM	stop after NUM selected lines
-b, --byte-offset	print the byte offset with output lines
-n, --line-number	print line number with output lines
--line-buffered	flush output on every line
-H, --with-filename	print file name with output lines
-h, --no-filename	suppress the file name prefix on output
--label=LABEL	use LABEL as the standard input file name prefix
-o, --only-matching	show only nonempty parts of lines that match
-q, --quiet, --silent	suppress all normal output
--binary-files=TYPE	assume that binary files are TYPE; TYPE is 'binary', 'text', or 'without-match'
-a, --text	equivalent to --binary-files=text
-l	equivalent to --binary-files=without-match
-d, --directories=ACTION	how to handle directories; ACTION is 'read' or 'skip'
-D, --devices=ACTION	how to handle devices, FIFOs and sockets; ACTION is 'read' or 'skip'
-L, --files-without-match	print only names of FILES with no selected lines
-l, --files-with-matches	print only names of FILES with selected lines
-c, --count	print only a count of selected lines per FILE
-T, --initial-tab	make tabs line up (if needed)
-Z, --null	print 0 byte after FILE name

Context control:

-B, --before-context=NUM	print NUM lines of leading context
-A, --after-context=NUM	print NUM lines of trailing context
-C, --context=NUM	print NUM lines of output context
-NUM	same as --context=NUM
--color[=WHEN], --colour[=WHEN]	use markers to highlight the matching strings; WHEN is 'always', 'never', or 'auto'
-U, --binary	do not strip CR characters at EOL (MSDOS/Windows)

Chapter 8: What's New in FOS 9.1.1a

8.1 Certifications

FOS v9.1.1a is the first Fabric OS release at the 9.x level which is submitted for Common Criteria certification.

8.2 Hardware

There is no new hardware supported with FOS v9.1.1a

8.3 Software

The following lists the software changes with this release.

8.3.1 Resolution of Important Defects

The following important defects are resolved in FOS 9.1.1a:

- FOS-844849 - Credit loss observed on ISL link between two G730 switches
- FOS-841985 - Unable to capture supportsave via SANnav
- FOS-841961 - On a X7 director that had gone through CLI "firmwarecleaninstall" of FOS9.0.x, after an upgrade to FOS v9.1.x, the active CP will show FAULTY (53) and will essentially be unresponsive. No output on the serial console. The management and service ports are no longer accessible.
- FOS-841163 - User can't perform firmware download on the switch from the SANNav
- FOS-844483 - Following a power outage the switch may stay stuck in boot with the error message: "Can't get the kernel image".

8.3.2 Enhancements

FOS v9.1.1a includes the following enhancements, described in more detail below:

- Allow admin access via console with "enableadminlockout"
- SSL CA certificate bundle update

8.3.2.1 Allow admin access via console with "enableadminlockout"

The command `enableadminlockout` is enhanced to allow configuration of login via console access even when the admin account has been locked out. This configuration is optional and not enabled by default.

8.3.2.2 SSL CA certificate bundle update

The SSL CA certificate bundle in FOS is updated with FOS v9.1.1a. Expired CA certificates are removed, and new CA certificates are added.

For the list of changes in the SSL CA certificate bundle, see [CA Certificate Bundle Updates](#).

Chapter 9: What's New in FOS 9.1.1

9.1 Certifications

FOS v9.1.1 is the first Fabric OS release at 9.x level which is submitted for FIPS 140-3 level 1 certification.

9.2 Hardware

The following section lists hardware introduced with this release.

9.2.1 Platforms

FOS v9.1.1 supports the same Brocade Gen 6 and Gen 7 Fibre Channel platforms supported in FOS v9.1.0x.

Gen 6 and Gen 7 platforms which ship from factory with FOS v9.1.1 are configured with Default Secure, only allowing secure protocols to access the switch management interface, consequently the following protocols are blocked:

- SNMPv1 and SNMPv2
- Telnet
- FTP
- HTTP

NOTE The end user can configure the switch to allow unsecure protocols.

9.2.2 New Optical Transceivers

FOS v9.1.1 adds support for the following optical transceivers:

Speed	Type	Manufacturing PN	Product PN
64G	LWL SFP+	57-1000496-01	XBR-000468
64G	ELWL SFP+	57-1000497-01	XBR-000466
32G	ELWL SFP+	57-1000498-01	XBR-000479

NOTE The 32G ELWL SFP+ XBR-000479 is not compatible with the previously released 32G ELWL SFP+ XBR-000478.

9.3 Software

The following section lists software changes with this release.

9.3.1 Resolution of Important Defects

The following important defects are resolved in FOS v9.1.1:

- FOS-826227–Devices in default allaccess zone cannot communicate to each other across LISLs in FICON environment on all platform
- FOS-832042–Brocade 7810 switch panics or hangs on boot up
- FOS-834530–Switch panics during adding aliases to zone configuration
- FOS-835586–SNMP consumes more CPU cycles, resulting in MAPS alerts
- FOS-837583–SNMP daemon leaks memory and causes switch to hafailover/hareboot/panic when switch runs out of memory
- FOS-839847–Switch subtype incorrectly displayed

In FOS v9.0.1b, 9.0.1c, 9.0.1d, 9.1.0, and 9.1.0b the following platforms incorrectly changed subtype.

In FOS v9.1.1 this is corrected as shown below:

Incorrect Subtype Shown in FOS v9.0.1b, 9.0.1c, 9.0.1d, 9.1.0, and 9.1.0b	Corrected Subtype Shown in FOS 9.1.1
162.1	162.0
162.6	162.5
184.1	184.0

In FOS v9.1.0b the following platforms incorrectly changed subtype.

In FOS v9.1.1 this is corrected as shown below:

Incorrect Subtype Shown in FOS v9.1.0b	Corrected Subtype Shown in FOS 9.1.1
165.x	165.0
166.x	166.0

9.3.2 Enhancements

FOS v9.1.1 includes the following enhancements, described in more detail below:

- Increase Trunking deskew for 8G, 16G or 32G speeds and LD/LS ports
- Switch decommission support
- FOS security hardening
- Support for XML license install with USB
- License export command for v4 (XML format) licenses
- REST Enhancements

9.3.2.1 Increase Trunking deskew for 8G, 16G, or 32G Speeds and LD/LS Ports

In FOS v9.0.x, the trunk deskew value on Gen 7 platforms is set to 300ns regardless of port speed. As a result, trunking would not form when a Gen 5/6 platform was replaced with a Gen 7 platform but retained existing cabling and DWDM at 8/16/32G speeds.

Change in FOS v9.1.1:

- When the E_Port speed is 8G, 16G or 32G, the legacy trunk deskew value (2550ns) is applied.
- When the E_Port speed is 64G, the trunk deskew value remains 300ns.
- When the E_Port is configured as LD/LS mode regardless of the speed (64G, 32G, 16G, or 8G), the legacy trunk deskew value (2550ns) is applied.

9.3.2.2 Switch Decommission Support

Switch decommissioning is provided for customers who want to erase all data on the switch prior to physically decommissioning the switch.

This is a destructive operation requiring a Decommission Authorization Code (DAC) from Brocade TAC.

Following the execution of this operation, the switch will be unusable and unrecoverable.

Example:

```
switch:admin> switchdecommission
```

This operation will erase the firmware on the switch, and it should be returned to the service provider.

```
*****
```

Please contact your service provider for a special authorization code.

License ID : (10:00:c4:f5:7c:16:9c:94)

```
*****
```

Enter decommission authorization code (DAC) :

Authorization successful. Switch decommission started.....

```
/*****/
```

Switch decommission has started. Please do not power off the switch.

Switch Decommission is completed.

Please return the switch to the service provider.

```
/*****/
```

9.3.2.3 FOS Security Hardening

To provide additional security in FOS, the following commands have been removed:

- – awk
- – du
- – find
- – head
- – kill
- – pidof

- – rpm
- – sed

The following commands are hardened in FOS v9.1.1 by restricting and confining them to only execute specific functions and prohibiting the command from accessing the root shell:

- cat
- fosredirout
- grep
- less
- ls
- more
- rm
- scp
- touch

9.3.2.4 Support for an XML License Installation with a USB

Installation of licenses in XML format (version 4 licenses) are now supported with a USB.

The following is an example of the CLI syntax:

```
license --install {-key <lic_key>} |{-usb <lic_path>} | {-h <hostip> -t <protocol> [-m
<server_port_number>] -u <user>
[-p <password>] -f <filepath/xmlfile>}
```

NOTE Prior to executing the `license -install -usb` command, you must first enable the USB storage by executing the command `usbstorage -enable`.

9.3.2.5 License Export Command for v4 (XML Format) Licenses

Backup of switch licences in XML format (version 4 licenses) is now supported.

The following is an example of the CLI syntax:

```
license --export {-s <serial-number | all> -h <hostip> -t <protocol> [-m
<server_port_number>] -u <user> [-p <password>] {-f <path/file_name> | -d <directory>}}
```

9.3.2.6 REST Enhancements

The REST URIs covering the following commands have been updated to provide full parity with the CLI:

- devicelogin
- fabstatsshow
- mapsdb
- portshow (Extension not included)
- portstats64show
- sfpslow
- switchshow

Chapter 10: Software License Support

10.1 Optionally Licensed Software

Fabric OS v9.1.x includes all basic switch and fabric support software, as well as optionally licensed software that is enabled via license keys or license files.

Optionally licensed features include:

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

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

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

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

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

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

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

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

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

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

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

On the Brocade X6-8:

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

On the Brocade X6-4:

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

On the Brocade X7-8:

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

On the Brocade X7-4:

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

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, 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.

10.2 Temporary License Support

The following licenses are available in Fabric OS v9.1.x as either universal temporary or regular temporary licenses:

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

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

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

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

Chapter 11: Hardware Support

11.1 Supported Devices

The following devices are supported in this release:

- Brocade X7-8 Director
- Brocade X7-4 Director
- Brocade X6-8 Director
- Brocade X6-4 Director
- Brocade G730 Switch
- Brocade G720 Switch
- Brocade G630 Switch
- Brocade G620 Switch
- Brocade G610 Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade MXG610 Blade Server SAN I/O Module
- Brocade 7810 Extension Switch

11.2 Supported Blades

11.2.1 X6-8 and X6-4 Blade Support

Fabric OS v9.1.x software is fully qualified and supports the blades for the X6-8 and X6-4 as noted in the following table.

Blades	FOS v9.1.x Support
FC32-48 32G FC blade	Supported.
SX6 Gen 6 Extension blade	Supported. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE blade	Supported.

11.2.2 X7-8 and X7-4 Blade Support

Fabric OS v9.1.x software is fully qualified and supports the blades for the X7-8 and X7-4 as noted in the following table.

Blades	FOS v9.1.x Support
FC32-X7-48 32G X7 FC blade	Supported.
FC64-48 64G FC blade	Supported
FC32-48 32G FC blade	Supported.
SX6 Gen 6 Extension blade	Supported. Up to a maximum of four blades of this type.
FC32-64 32G FC/FCoE blade	Supported.

11.3 Supported Power Supplies

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

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

11.4 Supported Optics

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

Chapter 12: Software Upgrades and Downgrades

12.1 Platform Specific Downloads

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

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

12.1.1 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.

12.1.1.1 Loading FOS PSDs via Web Tools or FOS Command Line

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

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

12.1.1.2 Loading FOS PSDs via Brocade SANnav Management Portal

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

12.2 FOS Image Filenames

Fabric OS v9.1.1d

Image Filename	Description
v9.1.1d.md5	Fabric OS v9.1.1d MD5 Checksums
v9.1.1d_all_mibs.tar.gz	Fabric OS v9.1.1d SNMP MIBs
v9.1.1d_EXT.tar.gz	Fabric OS v9.1.1d for Linux to install on 7810 platform
v9.1.1d_EXT.zip	Fabric OS v9.1.1d for Windows to install on 7810 platform
v9.1.1d_EMB.tar.gz	Fabric OS v9.1.1d for Linux to install on G648 and MXG610 platforms
v9.1.1d_EMB.zip	Fabric OS v9.1.1d for Windows to install on G648 and MXG610 platforms

v9.1.1d_G6_ENTRY.zip	Fabric OS v9.1.1d for Windows to install on G610 platform
v9.1.1d_G6_ENTRY.tar.gz	Fabric OS v9.1.1d for Linux to install on G610 platform
v9.1.1d_G6_MID.tar.gz	Fabric OS v9.1.1d for Linux to install on G620 platform
v9.1.1d_G6_MID.zip	Fabric OS v9.1.1d for Windows to install on G620 platform
v9.1.1d_G6_ENTP.tar.gz	Fabric OS v9.1.1d for Linux to install on G630 platform
v9.1.1d_G6_ENTP.zip	Fabric OS v9.1.1d for Windows to install on G630 platform
v9.1.1d_G7_MID.tar.gz	Fabric OS v9.1.1d for Linux to install on G720 platform
v9.1.1d_G7_MID.zip	Fabric OS v9.1.1d for Windows to install on G720 platform
v9.1.1d_G7_ENTP.tar.gz	Fabric OS v9.1.1d for Linux to install on G730 platform
v9.1.1d_G7_ENTP.zip	Fabric OS v9.1.1d for Windows to install on G730 platform
v9.1.1d_G6G7_DIR.tar.gz	Fabric OS v9.1.1d for Linux to install on X6-8, X6-4, X7-8 and X7-4 platforms
v9.1.1d_G6G7_DIR.zip	Fabric OS v9.1.1d for Windows to install on X6-8, X6-4, X7-8 and X7-4 platforms
v9.1.1d.releasenotes_v7.0.pdf	Fabric OS v9.1.1d Release Notes

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

12.3 Migration Path

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

NOTE For Brocade X6, G630, X7, and G730 a valid Trusted FOS (TruFOS) Certificate is required to upgrade to FOS v9.1.x. For details on how to obtain a TruFOS Certificate, see [Brocade Trusted FOS \(TruFOS\) Certificate](#).

12.3.1 Migrating to FOS 9.1.0

The supported upgrade paths to Fabric OS v9.1.x are as follows:

Current Version	Upgrade Path
FOS v9.0.x	Nondisruptive upgrade
FOS v8.2.x	Nondisruptive upgrade: First upgrade from FOS v8.2.x to FOS v9.0.x. Then if applicable (X6 and G630) install TruFOS Certificate and proceed with upgrade to FOS v9.1.x.

12.3.2 Migrating from FOS 9.1.x

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

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

Platforms	Fabric OS v9.1.x	Fabric OS v9.0.x	Fabric OS v8.2.x
Brocade Gen 7 (64G) Fixed-Port Switches			
Brocade G720 (Switch Type 181.0)	Supported	Supported	Not Supported
Brocade G720 (Switch Type 181.5)	Supported (Fabric OS v9.1.1 and later)	Not Supported	Not Supported
Brocade G730 (Switch Type 189.8)	Supported	Not Supported	Not Supported
Brocade Gen 7 (64G) Directors			
Brocade X7-4 Director	Supported	Supported	Not Supported
Brocade X7-8 Director	Supported	Supported	Not Supported
Brocade Gen 6 (32G) Fixed-Port Switches			
Brocade G610 (Switch Type 170.0 to 170.3)	Supported	Supported	Supported
Brocade G610 (Switch Type 170.4 or higher)	Supported	Supported (Fabric OS v9.0.1b and later)	Not Supported
Brocade G620 (Switch Type 162)	Supported	Supported	Supported
Brocade G620 (Switch Type 183.0)	Supported	Supported	Not Supported
Brocade G620 (Switch Type 183.5)	Supported (Fabric OS v9.1.1 and later)	Not Supported	Not Supported
Brocade G630 (Switch Type 173)	Supported	Supported	Supported
Brocade G630 (Switch Type 184)	Supported	Supported	Not Supported
Brocade 7810 Extension Switch	Supported	Supported	Supported (Fabric OS v8.2.1 and later)
Brocade G648 Blade Server SAN I/O Module	Supported	Supported	Supported
Brocade MXG610 Blade Server SAN I/O Module	Supported	Supported	Supported
Brocade Gen 6 (32G) Directors			
Brocade X6-4	Supported	Supported	Supported
Brocade X6-8	Supported	Supported	Supported
Brocade X6-4 (Switch Type 165.5)	Supported (Fabric OS v9.1.0b and later)	Not Supported	Not Supported
Brocade X6-8 (Switch Type 166.5)	Supported (Fabric OS v9.1.0b and later)	Not Supported	Not Supported

12.4 Brocade Trusted FOS (TruFOS) Certificate

Brocade TruFOS Certificates are factory installed on applicable platforms shipping with FOS v9.x. For X6 Directors and G630, you may need to install a TruFOS Certificate prior to upgrading to FOS v9.1.x.

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

```
Switch:admin> license -install -h 10.155.2.154 -t ftp -u UserName -p Password -f
/20211013171159568_10_00_c4_f5_7c_64_5b_60.xml
License Installed [FOS-87-0-04-11209683]
```

12.5 Upgrade/Downgrade Considerations

When upgrading a Gen 7 director or switch (X7-4, X7-8, G730, G720) to FOS v9.1.x, it is recommended to upgrade to FOS v9.1.1c or later. For additional information see TSB 2023-289-A.

During a firmware downgrade from v9.1.x to a pre-v9.1.0 firmware version, a transitory SEC-3089 error message may be displayed after `firmwaredownload` completes, but before a reboot is done.

The following platforms cannot be downgraded from FOS 9.1.1:

Brocade G620 (switchType 183.5)

Brocade G720 (switchType 181.5)

In FOS 9.1.x when performing `firmwaredownload`, the HA reboot triggers the broadcast message "The system is going down for reboot NOW!" -this is a standard Linux message when a system is doing a graceful shutdown.

This is non-disruptive to IO-traffic during this process.

Example below:

```
Do you want to continue (Y/N) [Y]:
Firmware download in progress, please wait.

Broadcast message from root@Switch (Fri Aug 26 10:59:01 2022):

The system is going down for reboot NOW!
```

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

Prior to downgrading to a pre-v9.1.1 firmware version, any 64G LWL secure SFP must be removed. Firmware downgrade with 64G LWL secure SFP inserted fails since the SFP is not supported pre-v9.1.1. If attempted, remove the 64G LWL secure SFP and retry `firmwaredownload`.

Chapter 13: Limitations and Restrictions

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

13.1 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 9.X document.

13.2 Compatibility/Interoperability

This section describes important compatibility and interoperability across Brocade products.

13.2.1 Brocade SANnav Management Portal Compatibility

When managing SAN switches with SANnav Management Portal it is recommended to first upgrade SANnav Management Portal to v2.2.1 (or later) prior to upgrading SAN switches to FOS v9.1.1.

While SANnav Management Portal v2.2.0 supports SAN switches running FOS v9.1.1, the use of IO Insight and Flow Vision features with SANnav requires SANnav Management Portal v2.2.1 (or later). For details, review the latest SANnav Management Portal v2.2 Release Notes.

13.2.2 Web Tools Compatibility

Web Tools supports firmware migration to v9.1.x from FOS v9.0.x.

Upgrading to FOS v9.0.x is supported from FOS v8.2.2a or later and FOS v8.2.1d or later.

To migrate from FOS v8.2.2 or from FOS v8.2.1c or earlier versions to FOS v9.0.x using Web Tools, switches must first migrate to FOS v8.2.1d or later or to FOS v8.2.2a or later as a first step, then to FOS v9.0.x or later as the final step.

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

13.2.3 Fabric OS Compatibility

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

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

Supported Products	Fabric OS Interoperability
Brocade 5424, 5431, 5432, 5480, NC-5480	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 300	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 7800	FOS v7.4.2 or later (Not compatible in the same fabric. Must use FCR) Note: There is no interoperability on VE interface(s) with another VE interface on a device running FOS v9.1.x (Brocade 7810 or Director with SX6 blade)
Brocade 7840	FOS v8.2.0 or later Note: When running FOS v8.2.1 or later there is interoperability on VE interface(s) with another VE interface on a device running FOS v9.1.x (Brocade 7810 or Director with SX6 blade)
Brocade DCX 8510-8/DCX 8510-4	FOS v8.2.x
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS v8.2.x
Brocade 6505, 6510, 6520, 7840	FOS v8.2.x
Brocade 6542	FOS v8.2.x
Brocade 6543	FOS v8.2.x
Brocade 6547, 6548, M6505, 6545, 6546	FOS v8.2.x
Brocade 6558	FOS v8.2.x
Brocade G610 (switchType 170.0 to 170.3)	FOS v8.2.0 or later
Brocade G610 (switchType 170.4 or higher)	FOS v9.0.1b or later
Brocade G620 (switchType 162)	FOS v8.2.0 or later
Brocade G620 (switchType 183.0)	FOS 9.0.0 or later
Brocade G620 (switchType 183.5)	FOS 9.1.1 or later
Brocade G630 (switchType 173)	FOS 8.2.0 or later
Brocade G630 (switchType 184)	FOS 9.0.0 or later
Brocade 7810	FOS 8.2.1 or later
Brocade X6-8/X6-4	FOS v8.2.0 or later
Brocade X6-8/X6-4 with FC32-64 blade	FOS 8.2.0 or later
Brocade X6-8/X6-4 (switchType 166.5 and 165.5)	FOS 9.1.0b or later
Brocade G720 (switchType 181.0)	FOS 9.0.0 or later
Brocade G720 (switchType 181.5)	FOS 9.1.1 or later
Brocade G730 (switchType 189.8)	FOS 9.1.0 or later
Brocade X7-8/X7-4	FOS 9.0.0 or later

Brocade G648 ¹	FOS 9.0.0 or later
Brocade MXG610 ²	FOS 9.0.1a or later

13.2.4 SNMP Support

Fabric OS v9.1.x documents the supported MIBs in the *Brocade Fabric OS MIB Reference Manual*. For information about SNMP support in Fabric OS software and how to use MIBs, refer to the *Brocade Fabric OS Administration Guide for Fabric OS v9.1.x*.

NOTE Fabric OS v9.1.x support SNMPv1 and SNMPv3, SNMPv2 deprecated in Fabric OS v9.0.1a, SNMP walk using SNMPv2 is blocked in Fabric OS v9.1.x.

13.2.5 Obtaining MIBs

You can download the MIB files required for this release from the Downloads area of the support portal site. To download the Brocade-specific MIBs, you must have a 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 **Brocade Storage Networking** in the support portal.

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

13.2.6 Flow Vision, IO Insight, and VM Insight

- The VMID+ feature is mutually exclusive with extended ISL (XISL) usage on logical switches. Therefore, you should disable the VMID+ to allow the XISL-usage feature to work, and you should turn off the XISL usage feature for the VMID+ to work.
- The VMID+ feature is not supported with Fibre Channel Router (FCR).
- Configuring an EX_Port and F_Port with the application header on the same chassis is not supported in VF and non-VF mode. However, the configuration is not blocked.
- The VMID+ feature is not supported on FICON logical switch ports.
- Enabling the VMID+ configuration on F_Ports connected to encryption-supported third-party devices is not supported.

¹ Brocade G648 is also supported with FOS v8.2.0_gft release.

² Brocade MXG610 is also supported with FOS 8.1.0_lnx2, 9.0.1a, and 9.1.0b.

13.2.7 REST API Support

Fabric OS v9.1.x documents the supported REST API functions in the *Brocade Fabric OS REST API Reference Manual*.

13.2.7.1 Obtaining YANG Files

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

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

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

13.3 Important Notes

Brocade recommends to always review Important Notes for each release.

13.3.1 4G Support on Gen 6 switches

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

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

13.3.2 Access Gateway

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

13.3.3 Brocade Analytics Monitoring Platform

FOS v9.1.x supports vTap on Brocade legacy Gen 6 platforms to be monitored by the Brocade Analytics Monitoring Platform. The supported Brocade platforms include: G610, G620, G630, X6-4, and X6-8.

13.3.4 ClearLink Diagnostics (D_Port)

Fabric OS v9.1.x supports D_Port tests between two Brocade switches and between Brocade switches and Gen 5 (16Gb/s), Gen 6 (32Gb/s), and Gen 7 (64Gb/s) Fibre Channel adapters from QLogic and Emulex. The following are specific adapter models and driver versions supported by Brocade with Fabric OS v9.1.x for ClearLink Diagnostics.²

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

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

13.3.5 Diagnostic POST

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

13.3.6 DWDM

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

² Adapter firmware or driver versions that are later than the ones listed in the table may not work.

13.3.7 Ethernet Management Interface

- The recommended interface speed configuration for a Brocade Gen 6 or Gen 7 switch or director chassis is 1G auto-negotiate.
- If a Brocade switch management interface is running at 10 Mb/s, certain FOS operations such as `firmwaredownload` may fail.
- The 10Gb/s management interface on CPX6 blades is not supported.
- Half-duplex mode is not supported in FOS v9.x and is blocked.
- The `ethif --reseterror` command option is not supported in FOS v9.0.x.
- The `ethif --reseterror` command option is supported in FOS v9.1.x.

13.3.8 Extension

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

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware
7840	8.2.1 or later	7840	8.2.1 or later
SX6	9.0.0 or later	7840	8.2.1 or later
7810	9.0.0 or later	7840	8.2.1 or later

13.3.9 FCoE

The following topologies for FCoE on the FC32-64 are not supported with FOS 9.1.x:

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

13.3.10 FC-NVMe

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

13.3.11 Firmware Migration

When doing staged firmware download migration from FOS 9.0.x to FOS 9.1.x using `firmwaredownload -r` option if there is any explicit expected or unexpected switch reboot before the firmware is activated it can result in the switch or chassis being in an unrecoverable state. Consequently, the system will end up in an erroneous state and will not be able to boot up correctly.

13.3.12 Forward Error Correction

- FEC is mandatory with Gen 6 and Gen 7 Fibre Channel operating at 32Gb/s or higher bandwidth. This means that the `portcfgfec` command applies only to ports that are running at 16Gb/s or 10Gb/s.
- FEC capability is not supported with all DWDM links. This means that FEC may need to be disabled on 16Gb/s or 10Gb/s ports when using DWDM links with some vendors. This is done using the `portcfgfec` command. Failure to disable FEC on these DWDM links may result in link failure during port bring-up. Refer to the *Brocade Fabric OS 9.x Compatibility Matrix* for supported DWDM equipment and restrictions on FEC use.

13.3.13 FPGA Upgrade

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

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

In FOS 9.1.1, the FPGA upgrade can be performed non-disruptively by upgrading the CR64 blades one by one.

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

13.3.13.1 FOS v9.1.1 FPGA Upgrade

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

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

After verification proceed to the next step.

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

Repeat this step for all connected E-ports (ICL ports) on the CR64 blade.

10. Verify the ICL ports are online with the command `switchshow`.
11. Repeat steps 4 through 11 on the second CR64 blade.

The FPGA upgrade is now complete.

13.3.14 Security

The security enhancements in this section all apply to both FOS v9.0.x and FOS v9.1.x

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

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

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

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

- FOS v9.x does not support F_Port authentication to Marvell QLogic BR series (Former Brocade Product Line) HBAs as these HBAs only support legacy Brocade F_Port authentication. For these devices to connect to FOS v9.x, F_Port authentication must be disabled.
- FOS v9.x does not support F_Port trunking when F_Port authentication is enabled
- Prior to upgrading to FOS v9.x:
 - First, ensure the secrets on both the switches (E-port authentication) are not the same. Otherwise, the E-port will segment after the upgrade to 9.x
 - Secondly, reconfigure shared secrets to be in compliance with FC-SP 2 standard

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

- FOS 9.x requires role mapping or VSA attributes to be configured for LDAP user authentication in a VF-enabled switch. In a non-VF switch, `ldapcfg --maprole` is mandatory. It should be configured before upgrading to FOS v9.x to avoid login failure for LDAP users.
- Users must specify the domain of an LDAP server when adding the LDAP server to the remote AAA configuration of a switch.

- Optional certificate extensions, such as BasicConstraints, KeyUsage, and ExtendedKeyUsage are ignored when a certificate containing these is imported in basic mode. During session establishment, the extensions are validated. Hence, invalid extensions will be rejected and result in session failure.
- Login of LDAP users using Distinguished Name (DN) will be supported only for the users created in container “Users” of the domain configured in the switch, even though the switch is configured with Global Catalog (GC) port of the server. Login using User Principal Name (UPN) and sAMAccountName will be supported irrespective of the domain and OU on which the user is created.

13.3.15 Zoning

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

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

13.3.16 Brocade X6 Field Migration

- FOS v9.1.1x supports a field migration of a Brocade X6 switch Type 165.5 and 166.5 to an upgraded X6 with Gen 7 support.
- Field migration of a Brocade X6 (switch Type 165 and 166) to an upgraded X6 with Gen 7 support is available with FOS v9.0.0x, FOS v9.0.1x and FOS v9.1.0x.
Refer to the *Brocade X6 Field Migration Guide* for step by step instructions.
- During field migration of Brocade X6 to a field upgraded X6 with Gen 7 support, the portcfgupload file will contain portcfgtrunkport commands for ICLs. A warning message is displayed to indicate that the command is not valid for ICL ports because trunking cannot be disabled on ICLs. This warning will not affect the ICLs and is harmless.

13.3.17 Miscellaneous

- After a power supply unit is removed from a Brocade G620, the historyshow command may miss the entries for this FRU removal or insertion event. In addition, the RASLog error message EM-1028 may be logged when the power supply is removed. This condition can be corrected by power-cycling the switch.
- After running offline diagnostics mode 1 on QSFP ports, a Brocade G620 must be rebooted before operational use.
- After running offline diagnostics with portledtest, portloopbacktest, or turboramtest commands on FOS v9.x, Brocade G630 with switchType 184 must be rebooted before operational use.
- All links in an ICL QSFP connection on a Brocade X6 Director must be configured to the same speed using the portcfgspeed command from one of the following supported speeds: 16Gb/s, 32Gb/s, or ASN. To connect an ICL from an X6 with a 4x32GFC breakout optic (P/N 57-1000351-01) or a 4x16G FC optic to a 4x16G FC optic in a DCX 8510, the X6 port's speed must be set to 16Gb/s.
- Brocade G630 LEDs illuminate amber and green during power-up.
- The CLI command option snmpconfig -set accesscontrol is planned to be deprecated in the next major release.
- When replacing a FC32-64 blade with a FC32-48 blade, flexport and FCoE configurations should be removed before the FC32-64 blade is removed.

- Enhanced checks are performed on optics during firmware upgrade to FOS v9.0.0 or later. Firmware download is blocked if unsupported optics are discovered. The scanning of the optics takes a few minutes to complete. The amount of time it takes is dependent on the number of ports on a switch. On a fully loaded eight (8) slot director, it can take up to five (5) minutes to complete. In addition, ports with optics that fail the enhanced checks in FOS v9.x will not be able to come online due to the optics as invalid module.
- Brocade G620 with `switchType 183` and G630 with `switchType 184` do not support the following legacy optical modules:
 - 16G SWL (HAA1, HAA2 serial number)
 - 16G LWL (HDA1, HDA2, HDA3 serial number)
 - 32G QSFP SWL (ZTA serial number)

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

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

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

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

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


```
[FABR-1001], 35, FID 128, WARNING, port 62, incompatible VC count
```
- FOS v9.x has disabled directory listing in CLI shell. As a result, entering `<tab><tab>` key does not list all CLIs available. Users can enter help command to list the commands. The shell tab completion by entering the first letter followed by `<tab>` key is supported.
- The FCR support of "Long Distance Fabric" mode conflict cannot coexist with long distance port configuration. If long distance mode (LD, LS, or LE) is enabled on the EX_Port and the EX_Port detected Backbone Fabric's "Long distance fabric" configuration is different from the connected Edge Fabric's "Long distance fabric" configuration, then the EX_Port will be disabled.
- If "Long Distance Fabric" is enabled on a switch via the `configure` command, it is recommended to upgrade the switch from FOS v8.2.x directly to FOS v9.0.0a or later. If the "Long Distance Fabric" configuration is enabled on an E_Port or EX_Port, firmware upgrade or downgrade to FOS v9.0.0 will effectively cause the "Long Distance Fabric" configuration to be disabled.
- If an HTTPS certificate is installed on a switch in FOS v9.x, HTTP access is blocked by default as HTTPS access is supported.

- When `portloopbacktest mode1` test runs on multiple Gen 7 ICL ports with multiple iterations, the test may fail. The workaround is to run the test on one ICL port at a time with a reduced number of iterations.
- Running long distance LE mode between any blades or switches among FC32-X7-48, FC64-48, or G720 with port QoS mode enabled and `vc_translation_link_init` mode enabled may result in frame timeouts. The workaround for this problem is to use LS or LD mode for long distance.
- If downloading firmware on an unsupported platform, a write post to `/rest/operations/show-status/message-id/20000` occurs and will incorrectly concatenate firmware download error messages. No recovery is needed, and this behaviour will not cause any functional impact.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades do not support 4G EX-Port.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades support 4G E-Port connected between any of the three listed only
- When Connecting Brocade G730 with X7, G720, G620 switchType 183 or G630 switchType 184 these switches should run FOS v9.0.1c or later.
- When performing a configdownload operation this will not overwrite the existing MAPS "Custom RASLog mode" feature configuration on the switch. For example, if custom raslog mode is disabled in the switch but it is enabled in downloaded configuration, then the feature will remain disabled in switch and must be manually configured after the configdownload operation is complete.
- In case an NPIV flow is identified as SDDQ or Over Subscribed (and moved by Traffic Optimizer to an OS PG), the flow movement may cause some frames to be delivered Out of Order (OOO). In general, open systems devices have no issues when this happens.
- In FOS v9.1.1, CPX blades in X6 Switch Type 165.5 and 166.5 and X7 are displayed as CPX7 in `slotshow` command output.
- When upgrading from FOS v9.0.x to FOS v9.1.x, the AG ports will be moved from ALL_HOST_PORTS group to ALL_OTHER_F_PORTS group. Consequently, the MAPS thresholds for ALL_OTHER_F_PORTS will apply to these ports in FOS v9.1.x. The default thresholds for the groups ALL_HOST_PORTS and ALL_OTHER_F_PORTS are the same and if these are not changed there is no impact. In case custom thresholds are used and these are configured differently for the groups ALL_HOST_PORTS and ALL_OTHER_F_PORTS the thresholds (monitoring) for AG ports are impacted accordingly.
- When performing factory reset on an X6/X7, the cipher.syslog key is not reset to factory value. Consequently, TLS handshake failure messages are displayed ongoing on standby CP:
 Message: [SEC-3077], 123, SLOT 1 | CHASSIS, INFO, sw0, Event: TLS SESSION, TLS handshake failed, Info: certificate verify failed. Host=x.x.x.x
 To work around this perform factoryreset in the following way:
 1. Factoryreset
 2. When TLS handshake failure message is displayed -reboot the standby CP.
- When connecting a switch running FOS v9.1.x to a switch running pre FOS v9.1.x firmware, a FSPF-1006 RASLOG may be reported by the down-level neighbour switch.
 The FSPF-1006 RASLOG is reported by the down-level switch since the FSPF version identified by the FOS v9.1.x switch does not match what the pre FOS v9.1.x switch is expecting. The FSPF version is higher on the neighbour switch running 9.1.x. This log message is of informational character since the switch running 9.1.x automatically reverts to use the same code level as the switch running pre FOS 9.1.x firmware.
- In FOS 9.1.x, to conform to RFC3315 and RFC5942, the default value of prefix length for IPv6 DHCP address changed from 64 to 128. The prefix and gateway information are provided by the Router Advertisement (RA) and it is expected that RA is enabled in the network. If IPv6 RA is not enabled in the network, IPv6 connectivity issues will occur.
 The resolution is to enable RA to resolve IPv6 network connectivity issues.

- On G610 running FOS v9.1.1, in rare cases following a power outage the switch may be stuck in boot with the error message: "can't get kernel message". This may be seen on G610 switches with FOS v9.1.1 only following a power outage / power cycle. For this reason, it is recommended to run G610 switches on FOS v9.1.1a (or later) or v9.0.1x.
- When performing `supportSave` with `SCP` as the selected transfer protocol, the command defaults to using `SFTP`. In environments where `SFTP` ports are blocked the `supportSave` upload will fail.
- When upgrading a Gen 7 director or switch (X7-4, X7-8, G730, G720) to FOS v9.1.x, it is recommended to upgrade to FOS v9.1.1c or later. For additional information see TSB 2023-289-A.

Chapter 14: Security Vulnerability Fixes

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

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

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

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

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

Chapter 15: Defects

15.1 Closed With Code Changes in FOS v9.1.1d7

Defect ID	Description
FOS-848548	A RPM process stuck and/or firmwaredownload timed out after RPM DB corruption.
FOS-852416	The show, set operation with CLI "syslogadmin" and "auditcfg" commands are failing with "Unable to retrieve ...". Also on a director, standby CP Supportsave cannot be retrieved.
FOS-852572	Core observed while taking supportsave or segment fault during "RON --show" command.
FOS-854397	Observed the following flood of raslog: [MQ-1007], 783, SLOT 1 FFDC FID 128, WARNING, , queue fmFlowCopyQ: queue full (miss=1).
FOS-856702	E-Ports cannot come online and shows incorrect VC assignment
FOS-856789	Unexpected termination of fclagd led to cold recovery
FOS-857267	Processor rebooted - Software Fault:ASSERT during supportsave
FOS-857387	CP watchdog exception due to excessive print messages
FOS-858133	The administrative status will be shown as 'down' for the offline FC ports that have not been manually disabled(No_Module, No_Light, etc).
FOS-858197	BR7810 switches will report frequent ftrace triggers for an active Extension tunnel.
FOS-858848	The mdd process encounters a panic, and logs Raslog "KSWD -1002". The chassis may encounter an HA out of sync condition.
FOS-858851	User experience performance issue on Gen7 after code upgrade.
FOS-859282	CLI "flow" fails with Segmentation fault and traffic optimizer dashboards no longer work as expected.
FOS-860049	Transient PCS errors reported on G620.
FOS-860262	Kernel panic while storing trace data.
FOS-860632	Standby CP in RRD state and/or SX6 blades are faulted during code upgrade. inetd on active CP no longer listens on port 514 on ipaddress of 127.3.1.x
FOS-860768	ISL disabled due to "Both Compression/Non-Compression connections exist to neighboring switch" after DWDM event.
FOS-860855	Supportsaves are failing to collect switch SS using SANnav.
FOS-861134	Invalid port stats counters reported such as the inv_arb counter : er64_inv_arb 0 top_int : Invalid ARB 4292386144 bottom_int : Invalid ARB
FOS-861360	Switch unexpectedly reboots due to termination of process fdmid.
FOS-861742	Class 2 PLOGI response during RDP Polling leads to switch panic with ASSERT.
FOS-862224	SNMP daemon terminates.
FOS-863010	A chassis with FC32-X7-48 blade inserted is limited to 2k IT flows.
FOS-863077	The weblinker daemon memory usage continues to increase during SANnav monitoring and activities such as configupload start to fail.

15.2 Closed With Code Changes in FOS v9.1.1d2

Defect ID	Description
FOS-855788	Maps daemon (mdd) terminates during supportsave.
FOS-856244	Switch reports "400 Bad Request" for GET /rest/running/brocade-chassis/chassis for all users
FOS-857687	During large HA sync copy operations, switch encounters msd panic

15.3 Closed With Code Changes in FOS v9.1.1d1

Defect ID	Description
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.

15.4 Closed With Code Changes in FOS v9.1.1d

Defect ID	Description
FOS-836972	'portname' output shows ports as persistently disabled which are not persistently disabled, and vice versa.
FOS-843393	A flooding of TS-1019 RASLOG and switch is dropping TS updates
FOS-844810	Observed "termination of mdd" during fcippathtest
FOS-847080	Switch supportsave collection from SANnav fails.
FOS-848419	RESTfulAPI query sometimes doesn't show any value for disabled ports
FOS-849287	CLI sensorshow displays normal Temperature value, but Fan speed is 14375 RPM and system LED Flashes "amber and green " status.
FOS-849402	Devices connected to AG cannot login. Single F-port trunk becomes multiple F-port trunks.
FOS-849751	Slow Drain devices on E or EX Port connected switches can cause excessive XTUN-1006 FCIP TX Frame Drop RASLOGs per second.
FOS-849790	Valid certificate not accepted
FOS-849929	Weblinker dies with a large CoreFile and SanNav keeps showing "SNMP credentials invalid" state for the switch.
FOS-849954	PLOGI ACC not being received by host
FOS-850464	Switch HA State goes out of sync following a FOS upgrade from FOS 8.x to 9.0.x and the switch Zoning DB contains duplicated WWNs.
FOS-850496	Repeated logging of following raslog (with no functional impact): [UFCS-2007], 1118300/13621, FID 128, WARNING,, UFCS Lock stage Failed - ..
FOS-850500	User observes Fan kick starts and stays at a very high speed.
FOS-850931	Switch rebooted because of Kernel Panic
FOS-851141	SNMPd termination encountered during swBootPromLastUpdated query and "ps exfcl" command output (see below) shows stuck rpm query: 0 0 29270 2413 20 0 0 0 exit Z ? 0:00 _ snmpd <defunct> 0 0 23760 1 20 0 5144 3304 - R ? 5531:10 rpm
FOS-851223	Switch ran out of kernel memory and triggered daemon panic, cpu busy or port/blade fault.
FOS-851444	Observed kernel panic with the following stack trace: 000: Call Trace: 000: ? oidh_objget+0x39/0x50
FOS-851559	8Gb device slow to connect to 32G SFP on chassis.

FOS-852926	MAPS (module mdd) could go into a defunct state, and the state prevents MAPS from restarting, resulting in HA out of SYNC.
FOS-852945	The output of CLI command "firmwaredownloadstatus" continues to show the firmwaredownload status of SX-6 Blade as still in progress. This is seen during an FOS upgrade on X6 director,
FOS-852964	Kernal panic after hareboot.
FOS-853019	FICN-2064 reports the wrong FID and port in a chassis based switch
FOS-853174	FC-LAG is no longer functioning.
FOS-853249	cald process aborted due to memory resource not available.
FOS-853452	The memory corruption will result in mdd panic.
FOS-853775	FabricAdmin role not allowing users to run supportshow after upgrade to v9.0.x
FOS-853850	Telnet not working after FOS 9.1.1x upgrade.
FOS-853997	When "bulk" persistentEnable'ing ports from SanNav, ports would go to 'No_light' and disabled state.
FOS-854080	Detected termination of a daemon (zoned) followed by CP panic from Software Watch Dog timeout.
FOS-854095	After a non-critical daemon failed, it did not restart successfully and the switch persistently lost HA sync.
FOS-854143	Kernel panic when 64G oversubscription is introduced in the fabric with many neighbors on the same chip.
FOS-854371	FC traffic over FCIP Tunnel stopped, tunnel still up, but not passing IO over the WAN. FC ingress timeouts from local FC ports that should be using the tunnel.
FOS-854964	switches experienced snmpd termination and persistent loss of HA sync after customer upgraded snmp monitoring application.
FOS-855493	Switch shutdown after abnormal sensor temperatures such as (-1 C) or (191 C) are reported: [HIL-1506], 3498/333, FFDC , CRITICAL, sw0, High temperature (-1 C) exceeds system temperature limit. System will shut down within 2 minutes., OID:0x43000000, SPOID:0x43000000

15.5 Closed With Code Changes in FOS v9.1.1c

Defect ID	Description
FOS-822366	cald terminated and kernel panicked during supportsave collections.
FOS-835714	An incorrect error message is returned when the flows of an NPIV port are being quarantined.
FOS-837592	Deadlock condition with SNMP causing the message queue to full and snmpd termination.
FOS-838045	User may see verify error while running IO over the long duration and SANnav monitoring.
FOS-839810	User may see repeated logging of an internal firmwaredownload raslog messages.
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-843005	Switch panic, HA out of sync, with mdd core files during migration from FOS9.0.x to FOS9.1.x or later. Observed Raslog: [HAM-1013], 131574/20614, SLOT 1 CHASSIS, CRITICAL, , Can't restart (mdd (pid=30408)): System unready or LS trans in progress. Reboot/Failover manually if necessary
FOS-843176	Switch panic after network timer server daemon (nptd) hang and watchdog timeout: 2022/08/30-02:03:10 (MDT), [KSWD-1002], 1147, FFDC CHASSIS, WARNING, sw0, Detected termination of process tsd: 2849.
FOS-843291	[PMGR-1006], 10392, SLOT 1 CHASSIS, WARNING, , Attempt to move port(s) -1 on slot -1 to switch 21 failed. Error message: Not able to set port config on the switch..
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-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-844217	Zoning errors observed with raslog ZONE-1007 but traffic is moving fine.
FOS-844453	User may see the following VERIFY message during firmwaredownload: VERIFY - Failed expression: 0 && "NULL Neigh"
FOS-844544	High CPU utilization reported on switches during supportshow.
FOS-844912	Frames that have a DID with domain controller format (0xffcxx), such as FDMI query, are being dropped as zone_miss.

FOS-845272	MAPS defALL_FAN_AIR_FLOW_MISMATCH is only reported in the default FID.
FOS-846852	Egress & Ingress power TxRx values are incorrect in the diagnostic test results when D-Port test is run from SANNav
FOS-847045	Switch panic is observed when a timer is re-added before the same exact timer expires.
FOS-847063	Director hits panic when eth0 interface frequently bounces.
FOS-847091	Repeated software 'verify' errors detected on X7 directors running FOS 9.1.x. Also possible to see daemons crash due to watchdog timeout if congestion / oversubscription is severe.
FOS-847130	D-Port test stuck in not started from one end but another end succeeds.
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-847501	After upgrade to FOS 9.1.1, switch logging TRCE-1005 message every 6 hours for "FTP Connectivity Test failed due to error" without other functional impact.
FOS-847770	3rd party device boot over SAN failed.
FOS-848121	On an X7 chassis with SX6 blades that have HA capable VE ports, the VE ports might occasionally toggle.
FOS-848182	snmpbulk /walk provides WWNs byte swapped in wrong order such as: 50:06:0e:80:08:9e:d4:20 is displayed wrongly as 80:0e:06:50:20:d4:9e:08
FOS-848316	printf limits input to "y" or "n" only, which hinders the ability to do scripting
FOS-848422	HA Out of Sync due to SNMPd terminated in FOS upgrade HA window.
FOS-848986	CLI "flow --create" option which worked on FOS8.x, now fails on FOS 9.x with the following error message: root> flow --create egress270 -feature monitor -egrport 4/41 -srcdev "" -dstdev "" -noactivate Invalid or nonexistent egress port 4/41 specified.
FOS-849027	User may encounter "Processor rebooted - Software Fault: ASSERT."
FOS-849564	Firmware upgrade to FOS 9.2 on G730 required a manual reboot to finish.
FOS-849642	Switch reported a flood of hardware errors, followed by daemons watchdog timeout and switch reboot. Sometimes these hardware errors also triggered port fault and/or blade fault. A raslog similar to this one should also be observed: [TO-1006], 1011618/1002267, FID 128, INFO, Switch_100, Flows destined to b1a02 device have been moved to PG_OVER_SUBSCRIPTION_4G_16G PG., cfs_ctrlr.c, line: 1470, comp:cfsd, ltime:2023/05/17-06:15:33:923058
FOS-849643	ISL ports become disabled when connecting FOS 8.x with FOS 7.x switch after updating Enhanced Object Zoning. switchshow as below: Index Port Address Media Speed State Proto ===== 28 28 011c00 id 8G No_Sync FC Disabled (ESC Enhanced Zone Object Name Conflict)
FOS-849645	Network Patroller daemon (NPD) terminated even though the flow monitor was disabled via CLI "flow --deactivate sys_flow_monitor".
FOS-849852	G610 fails to boot after power outage with reason "ERROR: can't get kernel image!"
FOS-849917	On a G730 there is a probability of the switch getting into Credit loss (GE5-1012). Subsequent Link reset (GE5-1014) recovers the credit loss.
FOS-850134	This issue is specific to Gen7 chassis systems (X7-4, X7-8). Traffic optimizer related software verify errors (RAS-1004) and kernel panic might be observed.

15.6 Closed With Code Changes in FOS v9.1.1b

Defect ID	Description
FOS-835031	REST POST on /rest/operations/security-certificate incorrectly returns 400 Bad Request.
FOS-838584	Weblinker termination due to segmentation fault.
FOS-843260	SNMP cannot get port address on FOS v9.1.0x.
FOS-844552	Unexpected kernel panic/cold boot or HA out of sync.
FOS-845216	User may encounter an unexpected sudden system reboot
FOS-845716	Ports Fenced upon Power Cycle of switch or blades.
FOS-846314	SfpShow indicating "Media not installed" and switchShow showing a port state of "Mod_Val"
FOS-846325	On a MXG610 embedded switch, running FOS versions FOS9.0.x, FOS9.1.x, user may encounter IO service disruption after a reboot / hareboot, triggered by uboot tune DRAM failure leading to a Reset (power cycle) of the system.
FOS-846838	Available ports section in Ports Widget shown in red color instead of green.

15.7 Closed With Code Changes in FOS v9.1.1a

Defect ID	Description
FOS-837451	DWDM is reporting a "loss of lock" error and the switch is showing no light on the port.
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-839936	User may encounter a CP Assert, upon initial failover to Fabric OS v9.x
FOS-840370	Firmwareupgrade via SANnav failed due to time-out from a busy standby CP.
FOS-840717	High CPU usage reported on SNMP daemon.
FOS-840909	FCPH-1003 Raslog reports duplicate port WWN with a port that does not have the same port WWN.
FOS-840971	If switch uptime is more than 99 days, then only the first two digits of the uptime days is displayed in Dashboard.
FOS-841163	User can't perform firmware download on the switch from the SANNav.
FOS-841478	Duplicate PWWN detection resulted in disruption to the existing FICON CHPID.
FOS-841961	On a X7 director that had gone through CLI "firmwarecleaninstall" of FOS9.0.x, after an upgrade to FOS v9.1.x, the active CP will show FAULTY (53) and will essentially be unresponsive. No output on the serial console. The management and service ports are no longer accessible.
FOS-841985	Unable to capture supportsave via Sannav.
FOS-842035	'Launch the Web Tools application' step is unnecessarily displayed in 'Support Data Collection' screen.
FOS-842160	Performing a firmwarecleaninstall to FOS v9.1.0b or FOS v9.1.1 from any other version prior to FOS v9.1.0b will fail. Firmware upgrades to these same versions will succeed.
FOS-842607	MXG610s embedded switch panics after Fabric Resource Director daemon (fredd) crashes or holds a large amount of memory.
FOS-843396	SNMP password has to be set twice.
FOS-843643	Web tools cannot save zone configurations when launched from the Dell Chassis UI
FOS-844393	Enabling DHCP from Static (v4) does not reflect the DHCP ipv4 address on embedded blade switches supported on HPE synergy chassis.
FOS-844483	Following a power outage the switch may stay stuck in boot with the error message: "Can't get the kernel image"
FOS-844625	Configdownload fails on embedded platforms.
FOS-844849	Credit loss observed on ISL link between two G730 switches

15.8 Closed With Code Changes in FOS v9.1.1

Defect ID	Description
FOS-825993	Failure status should be sent, if SS fails on any of the CP
FOS-826227	Devices in default allaccess zone cannot communicate to each other across LISLs in FICON environment on all platform.
FOS-832042	Brocade 7810 switch panics or hangs on boot up.
FOS-833824	The "Max UDP conn exceeded" counter in the output of "lan-stats -global" remains always at 0 even though the number of running UDP flows are more than the supported emulated UDP flows.
FOS-834530	Switch panics during adding aliases to zone configuration.
FOS-835586	SNMP consumes more CPU cycles, resulting in MAPS alerts.
FOS-835781	D-Port test is stuck in "In Progress" on 32G ADVA DWDM links.

FOS-835809	'Unmount USB Drive' option is displayed in WebEM after USB device is inserted. User would not be able to use the USB device connected to the switch as there is no option to mount the device.
FOS-835872	The output for the "ficonshow rrid" and "ficonshow rrid table" CLI does not include Node Descriptors for online E-Ports.
FOS-835998	tsclockserver Active server shows as NONE on non-principal switches however working fine on Principal switch with legacy mode disabled. Similarly, tsclockserver Active server shows as NONE when set to LOCL in legacy mode disabled.
FOS-836031	Switch panic after FDMI daemon terminated.
FOS-836043	Director-class switches returning chassis S/N when being queried for brocade-chassis info via REST, when WWN 1 S/N was previously returned and used for entitlement.
FOS-836077	On Standby CP, lines with '0's appear on console during hot code load.
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.
FOS-836313	The session which gets modified to HTTPS from HTTP based session, gets terminated when HTTP protocol is disabled after HTTPS certificate generation.
FOS-836339	REST GET operation on brocade-security/sshutil-public-key fails with error "Named account does not exist"
FOS-836369	D-Port test does not start on the secondary port links of a 53G BMF QSFP, when the test is initiated using "portdporttest -start" command option on all 4 ports.
FOS-836491	flow CLI does not report TIMEOUT count for an Initiator or Target device.
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-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-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-837405	Flow vision reports the wrong direction of flows for the SCSI devices that don't register FC4 features.
FOS-837518	ESMd panic seen when issuing a `portcfgge lan -set -lan` command.
FOS-837563	Brocade G630 switch (Switch type = 184) may experience sudden reboot – resets.
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-837911	Observed switch Panic from UCID termination resulting in UCID core file
FOS-838223	Devices in 64G switch with default allaccess zone cannot communicate to each other in FICON environment.
FOS-838514	7840, 7810 or SX6 blade encounters DP Linux out of Memory causing IO disruption
FOS-839056	Frame drops affecting entire fabric after creating smaller trunks from larger trunks.
FOS-839346	Path loss experienced after FOS upgrade on Access Gateway
FOS-839847	Switch subtype incorrectly displayed
FOS-840535	Link errors observed on port 47 of G620 (switch type 162) during HA upgrade

Appendix A: CA Certificate Bundle Updates

A.1 Added CA certificates from FOS v9.1.1a

Certificate Name:

GLOBALTRUST 2020

Data:

Version: 3 (0x2)

Serial Number:

5a:4b:bd:5a:fb:4f:8a:5b:fa:65:e5

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=AT, O=e-commerce monitoring GmbH, CN=GLOBALTRUST 2020

Validity

Not Before: Feb 10 00:00:00 2020 GMT

Not After : Jun 10 00:00:00 2040 GMT

Certificate Name:

ANF Secure Server Root CA

Data:

Version: 3 (0x2)

Serial Number: 996390341000653745 (0xdd3e3bc6cf96bb1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: serialNumber=G63287510, C=ES, O=ANF Autoridad de Certificacion, OU=ANF CA Raiz, CN=ANF Secure

Server Root CA

Validity

Not Before: Sep 4 10:00:38 2019 GMT

Not After : Aug 30 10:00:38 2039 GMT

Certificate Name:

Certum EC-384 CA

Data:

Version: 3 (0x2)

Serial Number:

78:8f:27:5c:81:12:52:20:a5:04:d0:2d:dd:ba:73:f4

Signature Algorithm: ecdsa-with-SHA384

Issuer: C=PL, O=Asseco Data Systems S.A., OU=Certum Certification Authority, CN=Certum EC-384 CA

Validity

Not Before: Mar 26 07:24:54 2018 GMT

Not After : Mar 26 07:24:54 2043 GMT

Certificate Name:

Certum Trusted Root CA

Data:

Version: 3 (0x2)

Serial Number:

1e:bf:59:50:b8:c9:80:37:4c:06:f7:eb:55:4f:b5:ed

Signature Algorithm: sha512WithRSAEncryption

Issuer: C=PL, O=Asseco Data Systems S.A., OU=Certum Certification Authority, CN=Certum Trusted Root CA

Validity

Not Before: Mar 16 12:10:13 2018 GMT

Not After : Mar 16 12:10:13 2043 GMT

Certificate Name:

TunTrust Root CA

Data:

Version: 3 (0x2)

Serial Number:

13:02:d5:e2:40:4c:92:46:86:16:67:5d:b4:bb:bb:b2:6b:3e:fc:13

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=TN, O=Agence Nationale de Certification Electronique, CN=TunTrust Root CA

Validity

Not Before: Apr 26 08:57:56 2019 GMT

Not After : Apr 26 08:57:56 2044 GM

Certificate Name:

HARICA TLS RSA Root CA 2021

Data:

Version: 3 (0x2)

Serial Number:

39:ca:93:1c:ef:43:f3:c6:8e:93:c7:f4:64:89:38:7e

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA TLS RSA Root CA 2021

Validity

Not Before: Feb 19 10:55:38 2021 GMT

Not After : Feb 13 10:55:37 2045 GMT

Certificate Name:

HARICA TLS ECC Root CA 2021

Data:

Version: 3 (0x2)

Serial Number:

67:74:9d:8d:77:d8:3b:6a:db:22:f4:ff:59:e2:bf:ce

Signature Algorithm: ecdsa-with-SHA384

Issuer: C=GR, O=Hellenic Academic and Research Institutions CA, CN=HARICA TLS ECC Root CA 2021

Validity

Not Before: Feb 19 11:01:10 2021 GMT

Not After : Feb 13 11:01:09 2045 GMT

A.2 Removed CA certificates from FOS v9.1.1a

Certificate Name:

GlobalSign Root CA - R2

Data:

Version: 3 (0x2)

Serial Number:

04:00:00:00:00:01:0f:86:26:e6:0d

Signature Algorithm: sha1WithRSAEncryption

Issuer: OU=GlobalSign Root CA - R2, O=GlobalSign, CN=GlobalSign

Validity

Not Before: Dec 15 08:00:00 2006 GMT

Not After : Dec 15 08:00:00 2021 GMT

Certificate Name:

QuoVadis Root CA

Data:

Version: 3 (0x2)

Serial Number: 985026699 (0x3ab6508b)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=BM, O=QuoVadis Limited, OU=Root Certification Authority, CN=QuoVadis Root Certification Authority

Validity

Not Before: Mar 19 18:33:33 2001 GMT

Not After : Mar 17 18:33:33 2021 GMT

Certificate Name:

Sonera Class 2 Root

Data:

Version: 3 (0x2)

Serial Number: 29 (0x1d)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=FI, O=Sonera, CN=Sonera Class2 CA

Validity

Not Before: Apr 6 07:29:40 2001 GMT

Not After : Apr 6 07:29:40 2021 GMT

Certificate Name:

DST Root CA

Data:

Version: 3 (0x2)

Serial Number:

44:af:b0:80:d6:a3:27:ba:89:30:39:86:2e:f8:40:6b

Signature Algorithm: sha1WithRSAEncryption

Issuer: O=Digital Signature Trust Co., CN=DST Root CA X3

Validity

Not Before: Sep 30 21:12:19 2000 GMT

Not After : Sep 30 14:01:15 2021 GMT

Certificate Name:
Cybertrust Global Root

Data:
Version: 3 (0x2)
Serial Number:
04:00:00:00:00:01:0f:85:aa:2d:48
Signature Algorithm: sha1WithRSAEncryption
Issuer: O=Cybertrust, Inc, CN=Cybertrust Global Root
Validity
Not Before: Dec 15 08:00:00 2006 GMT
Not After : Dec 15 08:00:00 2021 GMT

Certificate Name:
Chambers of Commerce Root - 2008

Data:
Version: 3 (0x2)
Serial Number:
a3:da:42:7e:a4:b1:ae:da
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=EU, L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287, O=AC
Camerfirma S.A., CN=Chambers of Commerce Root - 2008
Validity
Not Before: Aug 1 12:29:50 2008 GMT
Not After : Jul 31 12:29:50 2038 GMT

Certificate Name:
Global Chambersign Root - 2008

Data:
Version: 3 (0x2)
Serial Number:
c9:cd:d3:e9:d5:7d:23:ce
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=EU, L=Madrid (see current address at www.camerfirma.com/address)/serialNumber=A82743287, O=AC
Camerfirma S.A., CN=Global Chambersign Root - 2008
Validity
Not Before: Aug 1 12:31:40 2008 GMT
Not After : Jul 31 12:31:40 2038 GMT

Certificate name:
EC-ACC

Data:
Version: 3 (0x2)
Serial Number:
(Negative)11:d4:c2:14:2b:de:21:eb:57:9d:53:fb:0c:22:3b:ff
Signature Algorithm: sha1WithRSAEncryption
Issuer: C=ES, O=Agencia Catalana de Certificacio (NIF Q-0801176-I), OU=Serveis Publics de Certificacio,
OU=Vegeu <https://www.catcert.net/verarrel> (c)03, OU=Jerarquia Entitats de Certificacio Catalanes, CN=EC-ACC
Validity
Not Before: Jan 7 23:00:00 2003 GMT
Not After : Jan 7 22:59:59 2031 GMT

Certificate Name:

Hellenic Academic and Research Institutions RootCA 2011

Data:

Version: 3 (0x2)

Serial Number: 0 (0x0)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011

Validity

Not Before: Dec 6 13:49:52 2011 GMT

Not After : Dec 1 13:49:52 2031 GMT

Certificate Name:

Trustis FPS Root CA

Data:

Version: 3 (0x2)

Serial Number:

1b:1f:ad:b6:20:f9:24:d3:36:6b:f7:c7:f1:8c:a0:59

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=GB, O=Trustis Limited, OU=Trustis FPS Root CA

Validity

Not Before: Dec 23 12:14:06 2003 GMT

Not After : Jan 21 11:36:54 2024 GMT

Certificate Name:

GlobalSign ECC Root CA - R4

Data:

Version: 3 (0x2)

Serial Number:

2a:38:a4:1c:96:0a:04:de:42:b2:28:a5:0b:e8:34:98:02

Signature Algorithm: ecdsa-with-SHA256

Issuer: OU=GlobalSign ECC Root CA - R4, O=GlobalSign, CN=GlobalSign

Validity

Not Before: Nov 13 00:00:00 2012 GMT

Not After : Jan 19 03:14:07 2038 GMT

Certificate Name:

GTS Root R1

Data:

Version: 3 (0x2)

Serial Number:

6e:47:a9:c5:4b:47:0c:0d:ec:33:d0:89:b9:1c:f4:e1

Signature Algorithm: sha384WithRSAEncryption

Issuer: C=US, O=Google Trust Services LLC, CN=GTS Root R1

Validity

Not Before: Jun 22 00:00:00 2016 GMT

Not After : Jun 22 00:00:00 2036 GMT

Certificate Name:

GTS Root R2

Data:

Version: 3 (0x2)

Serial Number:

6e:47:a9:c6:5a:b3:e7:20:c5:30:9a:3f:68:52:f2:6f

Signature Algorithm: sha384WithRSAEncryption

Issuer: C=US, O=Google Trust Services LLC, CN=GTS Root R2

Validity

Not Before: Jun 22 00:00:00 2016 GMT

Not After : Jun 22 00:00:00 2036 GMT

Certificate Name:

GTS Root R3

Data:

Version: 3 (0x2)

Serial Number:

6e:47:a9:c7:6c:a9:73:24:40:89:0f:03:55:dd:8d:1d

Signature Algorithm: ecdsa-with-SHA384

Issuer: C=US, O=Google Trust Services LLC, CN=GTS Root R3

Validity

Not Before: Jun 22 00:00:00 2016 GMT

Not After : Jun 22 00:00:00 2036 GMT

Certificate Name:

GTS Root R4

Data:

Version: 3 (0x2)

Serial Number:

6e:47:a9:c8:8b:94:b6:e8:bb:3b:2a:d8:a2:b2:c1:99

Signature Algorithm: ecdsa-with-SHA384

Issuer: C=US, O=Google Trust Services LLC, CN=GTS Root R4

Validity

Not Before: Jun 22 00:00:00 2016 GMT

Not After : Jun 22 00:00:00 2036 GMT

Revision History

Version	Summary of changes	Publication date
1.0	Initial version of document	01/11/2024
2.0	Updated disclosed CVEs for FOS v9.1.1d in Security Vulnerability Fixes	04/19/2024
3.0	Updated with CVE included in FOS v9.1.1d1 in Security Vulnerability Fixes	05/20/2024
4.0	Included Closed With Code Changes in FOS v9.1.1d1 .	05/31/2024
5.0	Included Closed With Code Changes in FOS v9.1.1d2 .	07/11/2024
6.0	Updated with CVEs included in FOS v9.1.1d2 in Security Vulnerability Fixes .	07/30/2024
7.0	Updated with details for FOS v9.1.1d7. Updated the section Security Vulnerability Fixes .	04/03/2025

