



# **Fabric OS v9.2.2**

## **Fabric OS v9.2.2 Release Notes Digest**

**Version 1.0**

Copyright © 2024 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to [www.broadcom.com](http://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

<b>Chapter 1: Preface .....</b>	<b>5</b>
1.1 Contacting Technical Support for your Brocade® Product .....	5
1.2 Related Documentation .....	6
<b>Chapter 2: Locating Product Manuals and Release Notes .....</b>	<b>7</b>
2.1 Locating Product Manuals and Release Notes .....	7
2.1.1 Locating Product Manuals on Broadcom .....	7
2.2 Document Feedback .....	8
<b>Chapter 3: Overview .....</b>	<b>9</b>
<b>Chapter 4: What's New in FOS 9.2.2 .....</b>	<b>10</b>
4.1 Hardware .....	10
4.1.1 Platforms .....	10
4.2 New and Modified Software Features .....	10
4.2.2 MAPS .....	18
4.2.3 Unified Storage Fabric (USF) .....	20
4.2.4 Fabric Services .....	25
4.2.5 Miscellaneous .....	26
4.2.6 Web Tools .....	31
4.2.7 Deprecated Features and Commands .....	34
4.2.8 Obsolete Features and Commands .....	37
<b>Chapter 5: Software License Support .....</b>	<b>39</b>
5.1 Optionally Licensed Software .....	39
5.2 Temporary License Support .....	40
<b>Chapter 6: Hardware Support .....</b>	<b>41</b>
6.1 Supported Devices .....	41
6.2 Supported Blades .....	41
6.2.1 X6-8 and X6-4 Blade Support .....	41
6.2.2 X7-8 and X7-4 Blade Support .....	41
6.3 Supported Power Supplies .....	42
6.4 Supported Optics .....	42
<b>Chapter 7: Software Upgrades and Downgrades .....</b>	<b>43</b>
7.1 Platform Specific Downloads .....	43
7.1.1 Using FOS PSDs .....	43
FOS Image Filenames .....	44
7.2 Migration Path .....	45
7.2.1 Migrating to FOS v9.2.2 .....	45
7.2.2 Migrating from FOS v9.2.x .....	45
7.3 Brocade Trusted FOS (TruFOS) Certificate .....	47
7.4 Upgrade/Downgrade Considerations .....	47

<b>Chapter 8: Limitations and Restrictions .....</b>	<b>48</b>
<b>8.1 Scalability.....</b>	<b>48</b>
8.1.1 Flow Vision.....	48
<b>8.2 Compatibility/Interoperability .....</b>	<b>48</b>
8.2.1 Brocade SANnav Management Portal Compatibility .....	48
8.2.2 Web Tools Compatibility .....	49
8.2.3 Fabric OS Compatibility .....	49
8.2.4 SNMP Support .....	50
8.2.5 Obtaining MIBs.....	51
8.2.6 Flow Vision, IO Insight and VM Insight .....	51
8.2.7 REST API Support .....	51
<b>8.3 Important Notes.....</b>	<b>52</b>
8.3.1 4G Support on Gen 6 Switches .....	52
8.3.2 Access Gateway .....	52
8.3.3 ClearLink Diagnostics (D_Port).....	52
8.3.4 DDNS .....	53
8.3.5 Diagnostic POST.....	53
8.3.6 DWDM.....	53
8.3.7 Ethernet Management Interface .....	53
8.3.8 Extension .....	53
8.3.9 FCoE .....	54
8.3.10 FC-NVMe .....	54
8.3.11 Firmware Migration .....	54
8.3.12 Forward Error Correction .....	55
8.3.13 FPGA Upgrade.....	55
8.3.14 Optimized Credit Model for G630 and X7-8/4.....	56
8.3.15 Security .....	
8.3.16 Zoning .....	60
8.3.17 Brocade X6 Field Migration.....	60
8.3.18 Miscellaneous .....	60
<b>Chapter 9: Security Vulnerability Fixes.....</b>	<b>64</b>
<b>Chapter 10: Defects .....</b>	<b>65</b>
10.1 Closed with Code Changes in FOS v9.2.2 .....	65
10.2 Closed without Code Changes in FOS v9.2.2 .....	66
10.3 Open in FOS v9.2.2.....	67
<b>Revision History.....</b>	<b>68</b>

# 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](http://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 <a href="http://support.broadcom.com">support.broadcom.com</a>. (You must initially register to gain access to the Support portal.) Once registered, log on and then select <b>Brocade Products</b>. You can now navigate to the following sites:</p> <ul style="list-style-type: none"> <li>▪ <b>Case Management</b></li> <li>▪ <b>Software Downloads</b></li> <li>▪ <b>Licensing</b></li> <li>▪ <b>SAN Reports</b></li> <li>▪ <b>Brocade Support Link</b></li> <li>▪ <b>Training &amp; Education</b></li> </ul>	<p>For Severity 1 (critical) issues, call Brocade Fibre Channel Networking Global Support at one of the phone numbers listed at <a href="http://www.broadcom.com/support/fibre-channel-networking/contact-brocade-support">www.broadcom.com/support/fibre-channel-networking/contact-brocade-support</a>.</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 G730, G720, G710, G630, G620 and G610 – On the switch ID pull-out tab located on the bottom of the port side of the switch.
- Brocade 7810 and 7850 – On the pull-out tab on the front left side of the chassis underneath the serial console and Ethernet connection and on the bottom of the switch as well as on the left side underneath (looking from the front).
- Brocade X7-8, X7-4, X6-8 and X6-4, – Lower portion of the chassis on the non-port side beneath the fan assemblies.

- World Wide Name (WWN).

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

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

- License Identifier (License ID).

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

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

## 1.2 Related Documentation

White papers, data sheets are available at [www.broadcom.com](http://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 on the support portal. Although the illustrations show Fibre Channel and Fabric OS (FOS), they work for all Brocade products and operating systems.

### 2.1 Locating Product Manuals and Release Notes

#### 2.1.1 Locating Product Manuals on Broadcom

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

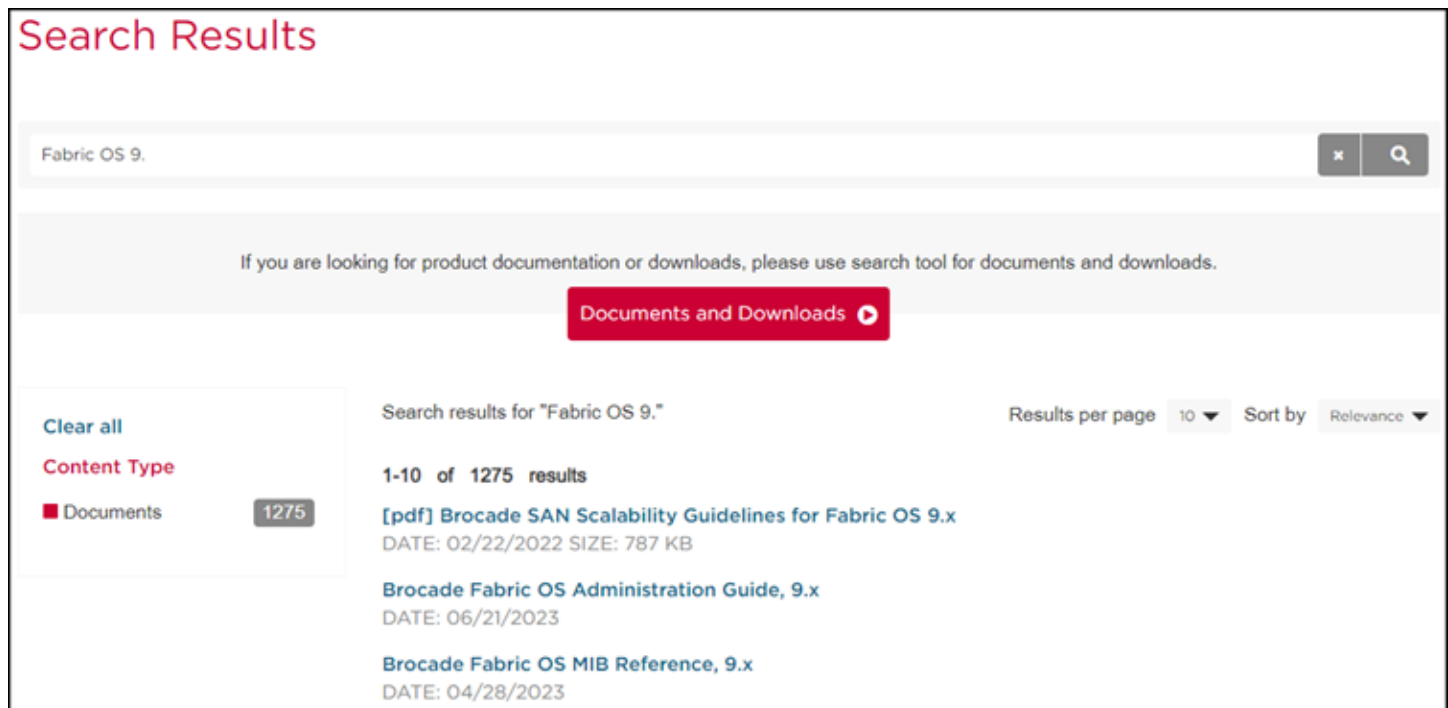
1. Go to [www.broadcom.com](http://www.broadcom.com).
2. Enter the product name or the software version number in the **Search** box.

For example, the following search is for software and documentation files for software version 9.



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 [support.broadcom.com](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](mailto:documentation.PDL@broadcom.com). Provide the publication title, publication number, and as much detail as possible, including the topic heading and page number, as well as your suggestions for improvement.



## Chapter 3: Overview

The Fabric OS v9.2.2 is a maintenance release based on FOS v9.2.1x.

This release supports all hardware platforms and features in FOS v9.2.1x.

Fabric OS v9.2.2 includes software enhancements and defect fixes for FOS v9.2.1x.

Fabric OS v9.2.2 is the initial release supporting the G710 entry level switch.

## Chapter 4: What's New in FOS 9.2.2

The Fabric OS v9.2.2 release includes new software features and enhancements of existing, with the main areas listed below and covered in more detail in the respective sections and chapters.

### 4.1 Hardware

Fabric OS v9.2.2 is the first release supporting the following new hardware:

- Brocade G710 Entry level switch

FOS v9.2.2 is the first release supporting the 25GbE SFP+ LR, PN: 57-1000504=01 (CBR-25G-LR-01) with serial number CDA9 xxxxxxxxxx (for the 7850 extension switch).

When this optic is present and downgrade from FOS v9.2.2 is performed, the `firmwaredownload` will fail.

#### 4.1.1 Platforms

In addition to the new hardware capabilities, FOS v9.2.2 also supports the same Brocade Gen 6 and Gen 7 Fibre Channel platforms supported in FOS v9.2.1x.

### 4.2 New and Modified Software Features

- System Security
  - Discontinued support for inline passwords and critical security parameters
  - StrictHostkeyChecking configuration for SSH
  - Algorithm configuration for SSH Hostkey/Pubkey
  - 4096 bits key size for FCAP/Commoncert
  - SMTPS TLS certificate and cipher support for MAPS
  - Increased password length for FOS user accounts
  - Default Secure: Complex password policy
  - Default Secure: HTTP “OPTIONS” method disabled
  - BSL data anonymization
- MAPS
  - MAPS alert reduction
  - MAPS secure SMTP support
- Unified Storage Fabric (USF)
  - USF Scale and topology support
  - iSNS support
  - IP Storage diagnostics
- Fabric Services
  - Upper layer object server
  - Platform name identifier
  - Simplified discovery

- Miscellaneous
  - Enhanced services recovery
  - Switchdisable command requiring confirmation
  - Supportlink enhanced to support user defined tags
  - Link Latency Determination (LLD)
  - ClearLink diagnostics on LD HBA links
  - ACC related SNMP traps on Access Gateway
  - PortCfg max speed
- Web Tools
  - Federated Authentication
  - Default protocol type for transfers
  - Display of management ports speed
  - Support for password with up to 510 characters
  - Web Tools tables improved to display full width
- REST API changes
- Deprecated features and commands
- Obsolete features and commands

## 4.2.1 System Security Enhancements

FOS v9.2.2 includes the following changes and enhancements to system security, each described in detail in the following sections:

- Discontinued support for inline passwords and critical security parameters
- StrictHostkeyChecking configuration for SSH
- Algorithm configuration for SSH Hostkey/Pubkey
- 4096 bits key size for FCAP/Commoncert
- SMTPS TLS certificate and cipher support for MAPS
- Increase supported password length for FOS user accounts
- Default Secure: Complex password policy
- Default Secure: HTTP "OPTIONS" method disabled
- BSL data anonymization

### 4.2.1.1 Discontinued support for inline passwords and critical security parameters

In FOS v9.2.2 execution of commands with passwords inline in the command string is no longer supported. Instead, the command must be executed without specifying the password and authentication is performed interactively. With this change full CLI history is reenabled in FOS v9.2.2.

This change applies to the following commands:

- Aaaconfig
- Configupload
- Configdownload
- Extncfg
- Factorycfg
- Femdump
- Firmwarecleaninstall

- Firmwaredownload
- Firmwarepatch
- Frudump
- License
- Secauthsecret
- Seccertmgmt
- Serviceshell
- Snmpconfig
- Sshutil
- Supportftp
- Supportlink
- Supportsave
- Tsclockserver
- Passwd
- Portcfg
- Portcfgupload

If a command is executed with an inline password it will fail since the option is no longer valid

Example:

```
switch:FID128:admin>userconfig --add fosadmin -r admin -h 128 -l 1-128 -p password
Error: Invalid option (-p).
```

```
Usage: userConfig --add <username> -r <LF role> -l <LF_ID list> [-h <LF_ID>] [-c <chassis
role>] [-d <description>] [-x] [-at <HH:MM-HH:MM> | -access-time <HH:MM-HH:MM>]
```

#### 4.2.1.2 StrictHostKeyChecking configuration for SSH

StrictHostKeyChecking is enabled by default in FOS v9.2.2 factory shipped units and is configurable with the command `sshUtil`:

```
sshutil stricthostkeycheck {-value <yes/no>}
```

When StrictHostKeyChecking is set to yes, for every ssh server that FOS will communicate with, known host entry must be present.

The known host entry can be added with the `sshutil` command, enhanced to take known host entry with the format `<IP_address:port>`.

Example:

```
switch:FID128:admin>sshutil addknownhost [10.123.45.7]:1234 -fp
SHA256:fr73BOo4IxWE7YADy/04QPmzliIEFlEeSIJ+q71f9I4
Known Host(s) added successfully.
```

```
switch:FID128:admin>shutil addknownhost [2610:100:0:96:123:7cff:a45:23]:1234 -fp
SHA256:fr73BOo4IxWE7YADy/04QPmzliIEFlEeSIJ+q71f9I4
Known Host(s) added successfully.
```

### 4.2.1.3 Algorithm Configuration for SSH Hostkey/Pubkey

In FOS versions prior to FOS 9.2.2, RSA SSH hostkey/pubkey use a hashing algorithm (SHA1) which is no longer considered adequately strong and commonly reported as a potential vulnerability by scanning tools (such as Qualys).

While users can generate and use ECDSA SSH hostkey/pubkey instead of RSA (removing the RSA hostkey/pubkey in the process, FOS v9.2.2 is enhanced to allow the admin to configure SSH HostkeyAlgorithms and PubkeyAlgorithms for SSH connections to/from FOS and allow stronger RSA hostkey/pubkey using the command `seccryptocfg`.

The cryptographic templates in FOS v9.2.2 are updated with “HostKeyAlgorithms” and “PubKeyAlgorithms” key entries under SSH.

Example for platforms shipping with FOS v9.2.2 from factory:

```
seccryptocfg --show
SSH Crypto:
SSH Cipher      : aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-
cbc,aes256-cbc
SSH Kex         : ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-nistp521,diffie-
hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha1
SSH MAC         : hmac-sha2-256,hmac-sha2-512
SSH HostkeyAlg  :rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp521
SSH PubkeyAlg   :rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp521
TLS Ciphers:
-----Truncated-----
```

Accordingly, the new attributes “HostkeyAlg” and “PubkeyAlg” are available with the command `seccryptocfg --apply` to configure platforms upgraded to FOS v9.2.2.

**NOTE** When configuring the SSH HostkeyAlgorithms and PubkeyAlgorithms using `seccryptocfg --apply` the SSH service (in FOS) is restarted to load the new configs and all the existing SSH sessions on the current cp as well as on the standby cp in case of chassis will be terminated.

Example:

```
seccryptocfg --apply -group SSH -attr HostkeyAlg -value 'rsa-sha2-512,rsa-sha2-256,ecdsa-
sha2-nistp521'
seccryptocfg --apply -group SSH -attr PubkeyAlg -value 'rsa-sha2-512,rsa-sha2-256,ecdsa-
sha2-nistp521'

seccryptocfg --show
SSH Crypto:
SSH Cipher      : aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc,aes192-
cbc,aes256-cbc
SSH Kex         : ecdh-sha2-nistp256,ecdh-sha2-nistp384,ecdh-sha2-
nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group-exchange-sha1,diffie-
hellman-group14-sha1
SSH MAC         : hmac-sha2-256,hmac-sha2-512
SSH HostkeyAlg  :rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp521
SSH PubkeyAlg   :rsa-sha2-512,rsa-sha2-256,ecdsa-sha2-nistp521
TLS Ciphers:
-----Truncated-----
```

#### 4.2.1.4 4096 bits key size for FCAP/Commoncert

Prior to FOS v9.2.2 the key sizes allowed for FCAP/Commoncert are 1024/2048.

In FOS v9.2.2 the key sizes allowed for both FCAP/Commoncert are 4096, allowing generation of CSR with 4096 bits key size.

Command syntax:

```
seccertmgmt generate -csr {fcap|commoncert} [-type rsa] [-keysize {1024|2048|4096}] [-hash {sha1|sha256}] [-years <x>] [-f]
```

#### 4.2.1.5 SMTPS TLS Certificate and Cipher Support for MAPS

FOS v9.2.2 is enhanced to support CA certificate and cryptographic cipher configurations for SMTPS TLS.

Enhancement of the commands in `seccertmgmt` and `seccryptocfg` provides the mechanism for certificate management and cipher configuration for SMTPS.

##### Certificate Management

To establish TLS connection from a FOS switch to an SMTP server, the CA certificate which signed the SMTP server certificate needs to be imported into FOS. This CA certificate will be used to validate the server certificate while establishing the connection during the TLS session establishment phase. The value 'smtps' is provided for the `-server` option with the command `seccertmgmt` to perform the operations associated with SMTPS.

(A maximum of 15 server CA certificates can be imported for SMTPS).

Command syntax for import/export/delete/show:

```
seccertmgmt import -ca -server {https|radius|ldap|syslog|rsa|fa|asc|smtps} [-protocol {scp|ftp}] [-ipaddr <IP address>] [-remotedir <remote directory>] [-certname <certificate name>] [-login <login name>] [-password <password>]
```

```
seccertmgmt export -ca -server {https|radius|ldap|syslog|rsa|fa|smtps} [-protocol {scp|ftp}] [-ipaddr <IP address>] [-remotedir <remote directory>] [-login <login name>] [-password <password>]
```

```
seccertmgmt delete -ca -server {https|radius|ldap|syslog|rsa|fa|asc|smtps|extn <certificate name>|all} [-f]
```

```
seccertmgmt delete -all {default|fcap|commoncert|https|radius|ldap|syslog|extn|smtps} [-f]
```

```
seccertmgmt show -ca -server {https|radius|ldap|syslog|asc|kafka|rsa|fa|smtps} [-hexdump|-verbose]
```

Command syntax for import/export/delete/show for SMTPS CA server certificate:

```
seccertmgmt import -ca -server smtps -protocol scp -ipaddr 1.1.1.1 -remotedir /path/to/certificate/folder -certname ca.cert.pem -login user_name
```

```
seccertmgmt export -ca -server smtps -protocol scp -ipaddr 1.1.1.1 -remotedir /path/to/certificate/folder -login user_name
```

```
seccertmgmt delete -ca -server smtps -f
```

```
seccertmgmt delete -all smtps
```

```
seccertmgmt show -ca -server smtps
```

### Example:

```
switch:FID128:admin> seccertmgmt show -all
```

```
ssh private key:
  Does not Exist
```

```
ssh public keys available for users:
  None
```

### Certificate Files:

Protocol	Client CA	Server CA	SW	CSR	PVT Key	Passphrase
FCAP	Empty	NA	Empty	Exist	Exist	Exist
RADIUS	Empty	Exist	Empty	Empty	Empty	NA
LDAP	Empty	Empty	Empty	Empty	Empty	NA
RSA	NA	Empty	NA	NA	NA	NA
FA	NA	Empty	NA	NA	NA	NA
SYSLOG	Empty	Exist	Empty	Empty	Empty	NA
HTTPS	NA	Empty	Empty	Empty	Empty	NA
KAFKA	NA	Empty	NA	NA	NA	NA
ASC	NA	Empty	NA	NA	NA	NA
<b>SMTPS</b>	<b>NA</b>	<b>Empty</b>	<b>NA</b>	<b>NA</b>	<b>NA</b>	<b>NA</b>

### NOTE :

- Client CA import as well as certificate import is not valid for 'smtps' and will result in an error
- CSR generation for 'smtps' is not supported
- SMTPS server CA certificates imported to the switch will be monitored by MAPS, similar to other certificates.
- Server CA certificate size cannot be more than 1 MB for import operation, else the import operation will fail.
- Zeroize will remove the server CA certificate for SMTPS

## Cryptographic configuration

Accordingly, the command `seccryptocfg` is enhanced to configure the TLS protocol and ciphers to be used for SMTPS communication.

### Default Values

#### **SMTPS\_Ciphers:**

```
ECDSA:ECDH:RSA:AES:3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!AESCCM8:!AESCCM:!ARIAGCM:!CAMELLIA:!CHACHA20:!SEED:!RC4
```

```
SMTPS_Protocol: Any
```

### Example:

```
seccryptocfg --show
```

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

```
SMTPS :
```

```
ECDSA:ECDH:RSA:AES:3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!AESCCM8:!AESCCM:!ARIAGCM:!CAMELLIA:!CHACHA20:!SEED:!RC4
```

```
TLS Protocol:
```

```
HTTPS : TLSv1.3
```

```
RADIUS : TLSv1.2
```

```
LDAP : TLSv1.2
```

```
SYSLOG : TLSv1.2
```

RSA : TLSv1.2  
 FA : TLSv1.2  
**SMTPS : Any**

-----Truncated-----

#### 4.2.1.6 Increase supported password length for FOS user accounts

Prior to FOS v9.2.2 supported user account password is 40 characters. In FOS v9.2.2 user account password length is increased to 510 characters to manage credentials rotation with longer passwords by centralized password management services.

Accordingly, password policies can be defined to enforce password length up to 510 characters.

There are no changes to user account commands with this enhancement.

Downgrade is allowed from FOS v9.2.2 with passwords of length >40 characters while the admin will be presented with the message to reconfigure the passwords with max 40 characters.

"WARNING:Login of users with password length more than 40 characters through REST/Webem will not be allowed. Login through CLI and change the password to supported length."

#### 4.2.1.7 Default Secure: Default password policy

In FOS v9.2.2 the default password policy is updated to enforce usage of more complex (stronger) passwords.

Listed in the below table is a comparison of the password policy prior to FOS v9.2.2 and in FOS v9.2.2.

Parameter	Default Value <FOS v9.2.2	FOS v9.2.2 Default Value
Minimum Length	8	<b>12</b>
Number of Lower case	0	<b>1</b>
Number of Upper case	0	<b>1</b>
Number of Charset	0	<b>1</b>
Number of Digits	0	<b>1</b>
Number of Special characters	0	<b>1</b>
Repeat of Characters	1	<b>2</b>
Sequence of Characters	1	<b>2</b>
Minimum difference in password	0	<b>2</b>
Allow user name	Yes	<b>No</b>

**NOTE** When upgrading to FOS v9.2.2 the new password policy is not in effect without user configuration.

During normal firmware upgrade, the values for the default password policy are not changed.

The admin must enforce the new default values by issuing the command `passwdcfg --setdefault`.

Changing individual parameters manually is still allowed using the command `passwdcfg --set`.



#### 4.2.1.7.1 Configurations and events which set the new default password policy

Execution of the command `passwdcfg --setdefault`, will set the new default password policy in effect.

Execution of `factoryreset --set securitydefault` will set the new default password policy in effect.

Performing `cleaninstall` will set the new default password policy in effect.

Once the parameters are set with these strong default values, if the user wants to change, each parameter can be changed using the existing cli `passwdcfg -set` command.

**Note:** Existing user account passwords in use will not be forced to change prior to expiry of the given password.

Default passwords of default accounts will continue to stay the same in FOS 9.2.2 and will be enhanced to adhere to new passwd attribute defaults in future release.

#### 4.2.1.8 Default Secure: HTTP “OPTIONS” method disabled

FOS v9.2.2 is enhanced to specifically enable/disable HTTP “OPTIONS” method in FOS.

The HTTP “OPTIONS” method is used to request information about the communication options available for the HTTP target resource. The response includes an “Allow” header indicating the allowed HTTP methods on the resource.

This is potentially a security vulnerability, making HTTP “OPTIONS” configurable in FOS allows the admin to control if HTTP “OPTIONS” is enabled (allowed).

The command `mgmtapp` is enhanced with to enable/disable HTTP “OPTIONS”.

Command syntax:

```
mgmtapp --enable httpoptions
mgmtapp --disable httpoptions
```

After the HTTP “OPTIONS” method is disabled, the user will get an error message “403 Forbidden” for all HTTP “OPTIONS” requests to the switch.

As part of Default Secure, HTTP “OPTIONS” method is disabled in FOS v9.2.2 and per default on platforms shipping with FOS v9.2.2 from factory or when the admin executes factory reset, config default and secure default.

#### 4.2.1.9 BSL data anonymization

BSL data anonymization can be configured for BSL data to be anonymized before it is uploaded and stored on the BSL Supportlink server.

When enabled FOS performs a one-way SHA-256 hash to replace IP addresses, FQDNs, switch names, user names, and email addresses which may be included in BSL data, before it is transmitted to the BSL server.

To configure BSL data anonymization use the command `supportlink -config -anonymize <enable/disable>` to enable and disable anonymization of BSL data.

For more detailed information see the *Fabric OS Administration Guide*.

## 4.2.2 MAPS

In FOS v9.2.2 MAPS is enhanced to with Alert Reduction to reduce alert flooding as well as support for Secure SMTP.

### 4.2.2.1 MAPS alert reduction

In FOS v9.2.1 MAPS was enhanced with the configuration option of Adaptive notifications applying progressive quiet time intervals for reoccurring alerts.

In FOS v9.2.2 as part of MAPS Alert Reduction, Adaptive notifications is enabled by default unless it has already been configured ON or explicitly configured OFF; described in the table below.

Pre FOS v9.2.2x	On upgrade to FOS v9.2.2x
Default configuration	Adaptive notification is enabled by default and is effective
Adaptive notification is configured ON and is effective	Unchanged: Adaptive notification is configured ON and is effective
Adaptive notification is configured OFF	Unchanged: Adaptive notification is configured OFF

Adaptive notification configuration when upgrading to FOS v9.2.2x

During the upgrade the following informational message is displayed when the Adaptive notification configuration is changed:

**WARNING:** MAPS Adaptive Notification feature will be enabled by default in the target firmware version

#### 4.2.2.1.1 Removal of EMAIL action for default rules

MAPS alert Reduction removes the `EMAIL` action from selected default MAPS rules, see the *Fabric OS MAPS User Guide* (Revision history) for details.

**NOTE** The `EMAIL` action can be added to custom rules.

### 4.2.2.2 MAPS Secure SMTP Support

MAPS provides alerting via email when the action `EMAIL` is configured in MAPS global configuration and being configured in a rule, then on this rule violation, MAPS sends emails to the configured recipient email addresses.

Per default the email is sent using plain SMTP protocol which is a mail server application used for sending, receiving and relaying emails between senders and receivers. Plain SMTP protocol has a major drawback where emails between sender and receiver are not encrypted. MAPS is being enhanced to use secure SMTP, also known as SMTPS.

SMTPS (secure SMTP) is a method for securing SMTP with transport layer security and is intended to provide authentication and data encryption between the FOS switch (SMTP client) and the SMTP server.

SMTPs establish a secure SMTP connection by using TLS and with the secure connection the source/destination email addresses and the message content is encrypted.

Importing "SMTP server CA certificates" is an optional step when configuring secure SMTP and is necessary to perform server validation.

In case a CA certificate is not installed it is still possible to establish a secure connection between FOS and the mail server, but there is no server validation.

Import of the CA certificate for the mail server is done with the command `seccertmgmt import -ca -server smtps`. Chained Certificates are supported for SMTP server CA certificate.

For more information, see the section [SMTPS TLS Certificate and Cipher Support for MAPS](#).

Secure SMTP is enabled using the command `relayConfig`. By default, the secure SMTP feature is disabled and the user needs to explicitly enable to use secure SMTP.

The current Audit log message MAPS-1017 is enhanced to indicate whether secure SMTP mode is Enabled or Disabled.

Command syntax and examples:

```
switch:FID128:admin> relayConfig
Usage:
-----
relayConfig --config -rla_ip <relay IP> -rla_dname <domain name>
relayConfig --config -secure_smtp {true|false}
relayConfig --config -rla_ip <relay IP> -rla_dname <domain name> -secure_smtp
{true|false}
relayConfig --show
relayConfig --delete
relayConfig --help
```

### Enabling secure SMTP mode

```
switch:FID128:admin:admin> relayConfig --config -rla_ip 1.1.1.1 -rla_dname
relay.smtp.company.com -secure_smtp true
2024/02/06-09:02:37 (PST), [MAPS-1017], 375, FID 128, INFO, cassian6, MAPS relayConfig
got updated to relay_IP: 1.1.1.1, domain: relay.smtp.company.com, secure SMTP mode:
Enabled.
```

### Disabling secure SMTP mode

```
switch:FID128:admin:admin> relayConfig --config -rla_ip 1.1.1.1 -rla_dname
relay.smtp.company.com -secure_smtp false
2024/02/06-09:03:20 (PST), [MAPS-1017], 376, FID 128, INFO, cassian6, MAPS relayConfig
got updated to relay_IP: 1.1.1.1, domain: relay.smtp.company.com, secure SMTP mode:
Disabled.
```

### Disabling secure SMTP mode without “secure\_smtp” option in the CLI

```
switch:FID128:admin:admin> relayConfig --config -rla_ip 1.1.1.1 -rla_dname
relay.smtp.company.com
2024/02/06-09:06:35 (PST), [MAPS-1017], 377, FID 128, INFO, cassian6, MAPS relayConfig
got updated to relay_IP: 1.1.1.1, domain: relay.smtp.company.com, secure SMTP mode:
Disabled.
```

The admin can also enable or disable secure SMTP mode after relay configurations are configured.

### Enabling secure SMTP mode

```
switch:FID128:admin:admin> relayConfig --config -secure_smtp true
2024/02/06-09:07:37 (PST), [MAPS-1017], 378, FID 128, INFO, cassian6, MAPS relayConfig
got updated to relay_IP: 1.1.1.1, domain: relay.smtp.company.com, secure SMTP mode:
Enabled.
```

Disabling secure SMTP mode

```
switch:FID128:admin:admin> relayConfig --config -secure_smtp false
2024/02/06-09:08:20 (PST), [MAPS-1017], 379, FID 128, INFO, cassian6, MAPS relayConfig
got updated to relay_IP: 1.1.1.1, domain: relay.smtp.company.com, secure SMTP mode:
Disabled.
cements:
```

4.2.2.3 Monitoring of CA certificate for Secure SMTP

Once the SMTP CA certificate is imported, MAPS automatically adds the imported certificate into the ALL\_CERTS logical group.

MAPS start monitoring the certificates using the existing monitoring systems:

- DAYS\_TO\_EXPIRE.
- EXPIRED\_CERTS.

Imported certificates can be verified by executing the command `logicalgroup -show`.

Example:

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

Group Name	Predefined	Type	Member Count	Members
ALL_CERTS	Yes	Certificate	6	HTTPS SW
Certificate,LDAP Server CA Certificate,RADIUS Server CA Certificate,KAFKA Server CA Certificate,IDP Server CA Certificate,SMTP Server CA Certificate				

If secure SMTP is configured and downgrade is attempted, an error message is displayed to indicate that secure SMTP configuration is not supported in pre-9.2.2 releases and the firmware downgrade operation will be blocked with the following message:

"Secure SMTP configuration is not supported prior to FOS v9.2.2 and must be removed prior to downgrade, using the command `relayConfig`."

4.2.3 Unified Storage Fabric (USF)

Unified Storage Fabric (USF), introduced in FOS v9.2.1, provides a dedicated network with integrated storage services for all types of storage, including Fibre Channel, FICON, iSCSI, NVMe/TCP, and NAS.

FOS v9.2.2 delivers the following enhancements to USF

- Increased number of supported devices
- Topology Support for L2 connected ToR
- IPS Diagnostics improvements
- Internet Storage Name Service (iSNS)

### 4.2.3.1 USF Scale

The supported number of devices are increased in FOS v9.2.2 to 1200. This increased limit is not enforced and downgrade to FOS v9.2.1 with the increased scale is allowed but not supported.

Below are the supported scale limits for USF with FOS v9.2.2:

- Chassis scale
  - 1 IP Storage Logical Switch.
  
- IPS LS (logical switch) scale
  - 192 ethernet ports (8 slots)
  - 96 ethernet ports (4 slots)
  - 48 LAGS
  
- Per IPS LF (logical fabric) scale
  - 8 Domains
  - **800** ethernet ports.
  - **1200 devices**
  - 4 VRF IDs
  - 256 VLANs
  - 512 Static routes

### 4.2.3.2 Topology Support for L2 Connected ToR

In FOS v9.2.1 connection of ToR switches is only supported at L3.

In FOS v9.2.2 connection of ToR switches is supported with both L2 and L3.

Downgrade to FOS v9.2.1 with ToR switches connected at L2 is allowed but not supported.

### 4.2.3.3 IPS Diagnostics

The following IP Storage diagnostics commands are enhanced:

- IpsPing
- IpsDiag

#### 4.2.3.3.1 IpsPing

IpsPing is enhanced with the option for the user to specify the number of ECHO requests using the option `-count`

Command syntax:

```
ipsPing <ipaddress> [-vrfId <vrf_id>] [-sourceGateway <ipaddress>] [-size <supported size(18-2024)>] [-count <count(1-500)>]
```

### 4.2.3.3.2 IpsDiag

IpsDiag is a new command providing frame statistics for IPS traffic.

Example:

```
switch:admin> ipsdiag --showFrameStats
outFrames      : 20713
inFrames       : 20740
outRequestFrames : 20000
inResponseFrames : 20000
inRequestFrames : 20000
outResponseFrames : 20000
inDroppedFrames : 136
outTimedoutFrames : 16
```

### 4.2.3.4 Internet Storage Name Service (iSNS)

In FOS v9.2.2 iSNS support is included in USF with one logical iSNS instance per VRF implemented as a fabric wide service.

iSNS is implemented according to [RFC 4147](#) providing:

- iSCSI device registration
- iSCSI device query
- Discovery Domain
- Discovery Domain Set

#### 4.2.3.4.1 iSNS Support and Configuration

This section outlines iSNS support and configuration in USF.

When upgrading to FOS v9.2.1 iSNS is disabled by default and must first be enabled and configured.

In USF, iSNS is specific to each IPS VRF and configured as a fabric wide operation for each individual VRF.

All IPS LSs in the fabric must have iSNS enabled, in case some switches have iSNS disabled at the time of merge, then those switches will merge to take on the iSNS configuration of the enabled switch, the fabric will segment if two fabrics with different iSNS addresses are attempted to merge.

**NOTE** A single CLI command is used to enable iSNS and configure iSNS at the same time.

When configuring iSNS, the admin will specify the VRF and IP address that will be used as the iSNS server address. The IP address must be on an existing subnet (that has already been created). The iSNS server address must be dedicated for iSNS and different from the gateway IP address on the subnet and any device addresses.

All subnets within a VRF can communicate (using inter VLAN routing) with the iSNS server to register clients and query.

There is no support for communication across VRFs and individual iSNS configuration must be performed per VRF.

#### 4.2.3.4.2 iSNS Configuration

iSNS configuration in FOS v9.2.2 consists of Storage Nodes, Discovery Domains (DD) and Discovery Domain Sets (DDSet) support. The admin can create and delete DDs and DDSets, as well as add/delete the members (storage nodes) to/from DDs/DDSets.

The following rules apply to iSNS configuration in FOS v9.2.2:

- Creating DDs and DDSets for non-existent VRF is not allowed.
- VRF cannot be deleted if referred by any DDs or DDSets
- Creating DDs and DDSets for VRF that do not have iSNS server enabled is not allowed.
- Disabling iSNS server does not require DDs and DDSets to be deleted.

- Only iSCSI device names (IQNs) are allowed as members of a DD. In addition, users are allowed to pre provision the devices and add to DD before the devices register with the iSNS server
- Creating empty DD and DDSets are allowed
- Enabling and disabling of empty DDSets is allowed
- Adding an empty DD to a DDSet is allowed
- Deleting a DD that exists in a DDSet, is not allowed

The following commands are used to configure and manage iSNS:

- **isnsConfig**
  - Used to configure and update iSNS server and associated attributes. Setting and clearing of the attributes are all supported through updating action.

Command syntax:

```
isnsConfig -show [ -vrfID <vrfID>]
isnsConfig -update [<vrfID>] -server <IP address>
```

- **isnsDD**
  - Used when creating/adding members/removing members/deleting/showing Discovery Domain (DD) and its members in IQN format.

Command syntax:

```
isnsDD --create <name> [-vrfID <vrfID>] [-storageNode {<iqn1>}[, {<iqn2>}...]]
isnsDD --delete <name> [-vrfID <vrfID>]
isnsDD --add <name> [-vrfID <vrfID>] -storageNode {<iqn1>}[, {<iqn2>}...]
isnsDD --remove <name> [-vrfID <vrfID>] -storageNode {<iqn1>}[, {<iqn2>}...]
isnsDD --deleteAll [-vrfID <vrfID>]
isnsDD --show [-vrfID <vrfID>] [-name <name>]]
```

- **isnsDDSet**
  - Used when creating/adding members/removing members/deleting/enable/disable/showing Discovery Domain Set (DDS) and Discovery Domain members.

Command syntax:

```
isnsDDSet --create <name> [-vrfID <vrfID>] [-discoveryDomain {<dd1>}[, {<dd2>}...]]
isnsDDSet --delete <name> [-vrfID <vrfID>]
isnsDDSet --enable <name> [-vrfID <vrfID>]
isnsDDSet --disable <name> [-vrfID <vrfID>]
isnsDDSet --add <name> [-vrfID <vrfID>] -discoveryDomain {<dd1>}[, {<dd2>}...]
isnsDDSet --remove <name> [-vrfID <vrfID>] -discoveryDomain {<dd1>}[, {<dd2>}...]
isnsDDSet --deleteAll [-vrfID <vrfID>]
isnsDDSet --show [-vrfID <vrfID>] [-name <name>]]
```

- **isnsShow**
  - Used to display registered devices according to Storage Nodes, Portals and Portal Groups or Network Entities.

Command syntax:

```
isnsShow --device [-details] [-vrfID <vrfID>] [-name <iqn>]
isnsShow --entity [-details] [-vrfID <vrfID>]
                  [-entityID <eid>]
isnsShow --pg [-details] [-vrfID <vrfID> [-storageNode <iqn> |
                  -portalIP <IP address> [-portalPort <port number>] |
                  -tag <tag>]]
isnsShow --portal [-vrfID <vrfID> [-portalIP <IP address>
                  [-portalPort <port number>] | -entityID <eid>]]
```

- **ipsConfigurationSize**
  - Used to display the configuration size database for iSNS.

Command syntax:

```
ipsConfigurationSize --show [-feature <featureName>]
```

#### 4.2.3.4.3 iSNS Deployment Example

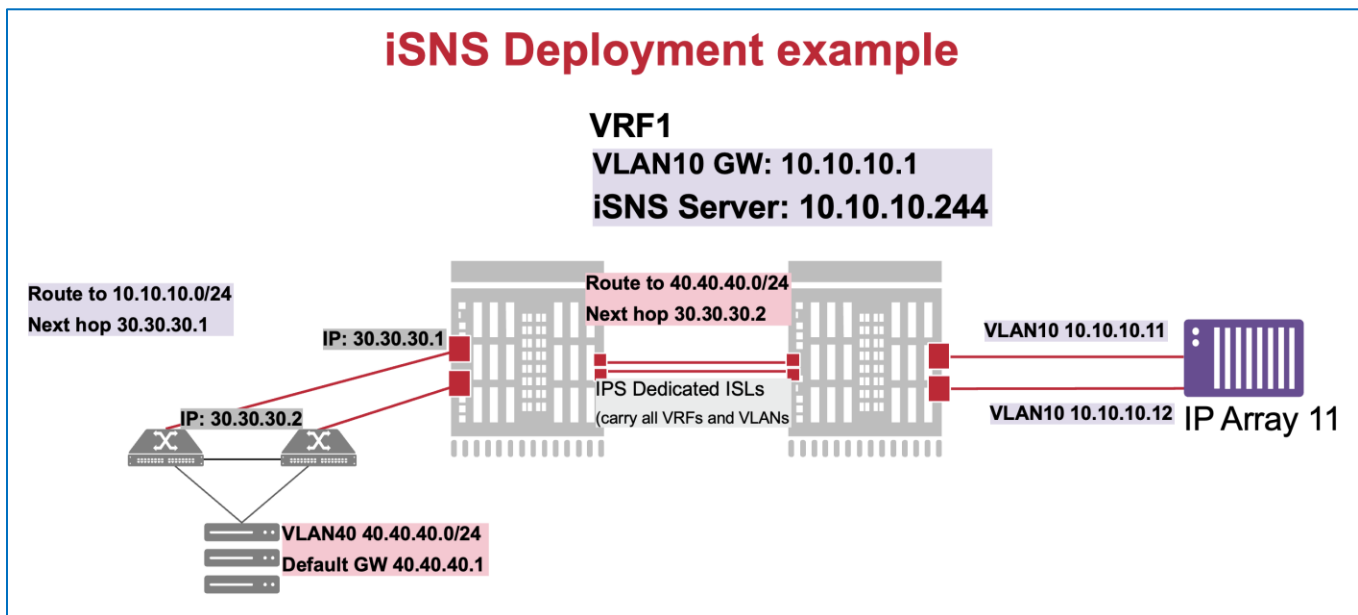


Figure 1: iSNS Deployment Example

Figure 1 depicts a topology with a typical iSNS deployment. The iSNS server virtually resides within one of the VLANs in the VRF using one dedicated IP address in the respective VLAN.

In this example, the iSNS server is assigned the IP Address 10.10.10.244, residing virtually in VLAN 10 of VRF 1.

Recommended best practice is to use a storage VLAN to host the iSNS server IP address to ensure no additional static routes are required from associated host subnets (although technically any VLAN for a given VRF can be used).

Once configured, the iSNS server is accessible from any devices residing within VRF 1. However, devices residing within other host subnets, must have appropriate static routes to reach the 10.10.10.0/24 subnet to access the iSNS with address 10.10.10.244. Inversely, appropriate static routes are needed to reach hosts in other subnets from the IPS fabric.



## 4.2.4 Fabric Services

The FC-GS9 standard specifies Generic Services that may be used to support management and operation of a Fibre Channel Fabric. It includes Services relating to device and topology discovery, Fabric Zoning, and Fibre Channel security.

In FOS v9.2.2 Fabric Services includes support for the following [FC-GS9](#) enhancements, described in more detail in the respective sections.

- Upper Layer Object Server
- Platform Name Identifier
- Simplified Discovery (GPN\_SD)

### 4.2.4.1 Upper Layer Object Server

The Upper Layer Object Server (aka Object Server) provides an infrastructure for all Upper Level Protocols, so that devices can register or deregister their logical entities (objects) with the Object server based on their FC4 type, ULP type and ULP Name. The Object Server provides a way to manage Upper Level Protocol (ULP) objects (e.g., ULP names). The ULP objects are used to identify logical entities defined by the Upper Level Protocols.

For NVMe, NQNs are the “ULP Name” object that is associated with NVMe connections. The object (ULP Name) registration details are distributed across the fabric. The ULP Name Objects stored in the fabric are used to identify which NQNs are associated with which ports.

Upper Layer Object Server support enables the storage admin, when performing namespace provisioning, to define access between host NQN(s) and NVME storage subsystems NQNs, without host access to register the NQN(s).

### 4.2.4.2 Platform Name Identifier

Platform Name Identifier (PNI) is a new object registered during Fabric Login (FLOGI). This information ties a port to a specific chassis which initiated the FLOGI and is the WWN of that chassis. The PNI, if provided, will be implicitly registered during Fabric Login.

Name Server queries for PNI or using PNI for device discovery are supported using the (new) Name Server query commands GNN\_PNI, GPN\_PNI, GPNI\_NN, GPNI\_PN, GPNI\_ID and RSPNI\_PNI.

### 4.2.4.3 Simplified Discovery (GPN\_SD)

The GPN\_SD query command provides a common device discovery method that can be used for various protocols such as FC-NVME and SCSI-FCP. A single GPN\_SD exchange can be issued with multiple query requests, each with different domain scope, FC4 type, and/or FC4 features. This is an efficient means to get a bulk response and can be used for zoned and unzoned lookup. GPN\_SD is the (per FC-GS9 standard) recommended query to use for device discovery.

## 4.2.5 Miscellaneous

This section describes miscellaneous enhancements in FOS v9.2.2

### 4.2.5.1 Enhanced services recovery

Enhanced services recovery enables recovery of non-critical services which may have crashed or failed to restart by doing an HA reboot and restart of the service. With this enhancement the HA state when synchronized has two levels:

Level 1: Absolute sync, at this level all components from all services are in sync and running.

Example:

```
Switch:FID128:admin> hashow
Local CP (Slot 1, CP0): Active, Warm Recovered
Remote CP (Slot 2, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized
```

Level 2: Conditional sync, at this level only critical services are guaranteed in sync, restartable services can be or may not be in sync.

Example:

```
Switch:FID128:admin> hashow
Local CP (Slot 1, CP0): Active, Warm Recovered
Remote CP (Slot 2, CP1): Standby, Healthy
HA enabled, Heartbeat Up, HA State synchronized (critical)
```

For both level 1 and level 2 the end user can issue the command `hafailover`.

When a system with hasync at level 2 (HA State synchronized (critical)) the restartable services that were crashed on the old active CP (at the time) will be started on the new active CP during the failover process. After the failover is completed, a sync is performed from the new active CP to the standby CP.

### 4.2.5.2 Switchdisable Requiring Confirmation

From FOS v9.2.2 the command `switchdisable` require confirmation prior to be executed, except if specifying `--force` to overrule interactive confirmation.

Example:

```
switch:FID128:admin> switchdisable
This will disable the switch and is disruptive to all connections.
Are you sure you want to continue disabling the switch? (yes, y, no, n): [no]: no
Aborting...
switch:FID128:admin>

switch:FID128:admin> switchdisable
This will disable the switch and is disruptive to all connections.
Are you sure you want to continue disabling the switch? (yes, y, no, n): [no]: y
switch:FID128:admin >

switch:FID128:admin> switchdisable --force
switch:FID128:admin >
```

### 4.2.5.3 Supportlink

From FOS v9.2.2 Supportlink configuration is enhanced to provide the flexibility to group switches logical groups using additional tags. The admin can configure up to 6 tags, of which 3 are predefined and 3 are custom tags. The predefined tag names are "Organization", "SiteID" and "OEM." The values for these tag names are configurable. For the custom tags both the name and value are configurable. For the predefined tags since the tag names are already defined the command syntax is slightly different from the syntax used for the custom tags.

Command syntax:

```
supportLink --configTag -Organization "Broadcom"
supportLink --configTag -SiteID "San Jose"
supportLink --configTag -OEM "OEM_Name"
supportLink --configTag -name "Custom_Desc1" -value "SANA"
supportLink --configTag -name "Custom_Desc2" -value "ExtensionFabric"
supportLink --configTag -name "Custom_Desc3" -value "XYZ"
```

Deleting a tag

```
supportLink --deletetag -name "CustomDesc1"
```

Display configuration

```
admin> supportlink --show
```

```
Support Link State           : Disabled
Next Collection Time        : Wed Nov 16 08:56:00 2024
Next Service Start Time     : Wed Nov 16 08:56:00 2024
```

Support Link Configurations:

```
Server Address               : bsnconnect.broadcom.com
Server Port                  : 443
User name                    : bsl_sl_default_user
Start Date                   : 10/01/2024
Start Time (in hour)         : 1
End Time Period (in hour)    : 12
```

```

Period (in day)           : 1
Retry Time (in hour)      : 0
Collection Time (in HH:MM) : 8:56
User Group Tag            :
Organization Name         : "Broadcom"
Site ID                   : "San Jose"
OEM.                      : "OEM_Name"
Custom Tags:

```

```

Custom_Desc1              : SANA
Custom_Desc2              : ExtensionFabric
Custom_Desc3              : XYZ

```

When no tags are configured only the predefined tags are displayed.

If `supportlink -default` is executed the tag values for the predefined tags will be reset to NULL and for free form tags both tag values and tag names will be reset to NULL.

Free form tags cannot exceed the length of 64 bytes and tag values length cannot exceed 32 bytes. Special characters are not allowed in tag names and tag values. Only alphanumeric characters are allowed.

#### 4.2.5.4 Link Latency Detection (LLD)

With FOS v9.2.2 on both inter-switch links (ISL) and inter-fabric links (IFL) will support independent measurement of link latency during link initialization. This enables calculation of Link Distance, and the results are displayed using existing commands (`portshow`, `islshow`, `iflshow`, `fabportshow`).

Link latency measurement is enabled by default for all FC ports. This feature can be disabled/enabled on a specific port using “`portcfglld`” CLI.

Command syntax:

```

switch:admin> portcfglld
Usage:  portCfgLld {--enable | --disable | --show } [<slot>/]<port>
        portCfgLld --help
Operands :
--enable      - Enable the Link Latency Determination feature
--disable     - Disable the Link Latency Determination feature
--show        - Show LLD configuration for the port
--help        - Help command to see Usage

```

```

switch:admin> portcfglld --show 8
LLD configuration is enabled.

```

```

switch:admin> portcfglld --disable 8
LLD configuration changes are disruptive. Are you sure you want to continue?
(yes, y, no, n): [no]: y
LLD configuration is disabled.

```

```

switch:admin> portcfglld --enable 8
LLD configuration changes are disruptive. Are you sure you want to continue?
(yes, y, no, n): [no]: y
LLD configuration is enabled.

```

**Islshow will display cable distance for ISL links**

```

switch:admin> islshow
  1: 0-> 0 10:00:c4:f5:7c:01:2d:40 237 Switch2 sp: 16.000G bw: 16.000G TRUNK QOS
CR_RECOV FEC 10 m

```

Ifshow will display the cable distance for IFL links

```
switch:admin> iflshow
```

#	E-Port	EX-Port	FCR-WWN	FCR FID	FCR Name	Speed	BW	
1:	40->	16	10:00:c4:f5:7c:01:2d:40	3	Switch3	32G	32G	QOS CR_RECOV FEC 20 m

The switches of both ends of the link must be on FOS v9.2.2 (or higher) for Link Latency and Link Distance functionality to work. In case the switch running FOS v9.2.2 is connected to a lower FOS version, interoperability is provided but measurements are not provided.

The supported matrix for both E-Port and EX-Port are as below:

Initiator/FCR	Responder/Edge	Result	Comments
<FOS v9.2.2	FOS v9.2.2	Not supported	Supported switch will display '0' for latency and cable distance
FOS v9.2.2	<FOS v9.2.2	Not supported	Supported switch will display '0' for latency and cable distance
FOS v9.2.2	FOS v9.2.2	Supported	Supported switch will display both latency and cable distance.

**Note:** When performing a non-disruptive upgrade to FOS v9.2.2 link distance will not be calculated nor displayed until there is a disruptive operation on the ISL/IFL link and LLD is triggered.

#### 4.2.5.5 ClearLink Diagnostics on Long Distance HBA Links

Currently, the long-distance support is available only on the HBAs listed below. The HBA must be connected directly (single mode Fibre optic cable). DWDM link cannot be used as the HBAs do not support it.

Supported HBA models:

- LPe35000
- LPe36000
- LPe37000
- LPe38000

Supported optics:

- 32G LW supported SFP - AFCT-57G5MZ-ELX
- 64G LW supported SFP - AFCT-57H5MZ-EL1

Supported firmware:

12.8, 14.0, 14.2 and 14.4.

These HBAs supports cable distances up to 10 KM. There is no additional configuration required on the HBA side for long distance support, as the HBA card is pre-configured for LWL optics. Only the "Dynamic DPort" mode either on switch or HBA must be configured.

Prior to running D-Port test on a long-distance cable connected between a switch and HBA, the port has to be configured with additional buffers using the command `portcfgfportbuffers`. There is no additional configuration required for ports like LS, LD or LE.

### 4.2.5.6 ACC Related SNMP Traps on AG

FOS v9.2.2 is enhanced to include two SNMP traps on switches in AG mode, necessary for ACC to identify case creation scenarios on AGs.

The traps `swFCPortScn` and `swEventTrap` defined in the SW-MIB is now available and enabled by default in AG mode. These two traps are already supported in the switch mode and now they will be supported in AG mode also.

The command `snmpconfig` can be used to display (and modify) mib capability features in SNMP. In the example below the `swFCPortScn` and `swEventTrap` traps defined in the SW-MIB are displayed.

Example:

```
AG:admin> snmpconfig --show mibcapability
SW-MIB: YES
FA-MIB: YES
HA-MIB: YES
IF-MIB: YES
BROCADE-MAPS-MIB: YES
SW-TRAP: YES
    swFCPortScn:      YES
    swEventTrap:      YES
-----Truncated-----
```

### 4.2.5.7 PortCfg Max Speed

In FOS v9.2.2 the command `portCfg` is enhanced to allow configuring the max speed of the port without specifying the actual speed value.

Command syntax:

```
switch:FID128:admin > portcfgspeed --help
Usage: portCfgSpeed [<SlotNumber>/]<PortNumber> {<Speed_Level> | 0 -m <max_auto_speed>}

OR

    portcfgspeed -h

OR

    portcfgspeed {-i | -x } {<port_index> | <portindex_range>} [-f] {<Speed_Level> | 0
    -m <max_auto_speed>}

OR

    portcfgspeed {-slot | -s} {<slot#> | <slotrange>} {<Speed_Level> | 0 -m
    <max_auto_speed>}
```

### 4.2.5.8 New RASLOG Messages LIC-1011 and LIC 1012

In FOS v9.2.2 new RASLOG messages related to TruFOS certificate expiration are added.

**LIC-1010** - Generic Expiration Message (Existing Message):

**Purpose:** To notify that a license or TruFOS certificate has expired.

**Message Text:** "License has expired."

**Condition:** Triggered when a TruFOS certificate has reached its expiration date.

**Severity:** Warning.

This message is an existing message and is logged when a TruFOS certificate has expired.

**LIC-1011 - Generic Expiration Warning (New Message):**

**Purpose:** To warn that a TruFOS certificate or a license is approaching its expiration date.

**Message Text:** "License is going to expire in %d days."

**Condition:** Triggered at configurable intervals (e.g., 10, 5, 1 day(s)) before the expiration date.

**Severity:** Warning.

This newly created message is logged when a TruFOS certificate expiration date approaches.

**Note:** LIC-1011 is a newly created message and is generic in nature.

**LIC-1012 - TruFOS Specific Certificate Warning (New Message):**

**Purpose:** To provide a specific warning about the impact of a missing or invalid TruFOS certificate.

**Message Text:** "A missing or invalid TruFOS certificate will not impact switch functionality except for upgrading or downgrading FOS."

**Condition:** Triggered when the license expiration check is specific to TruFOS certificates.

**Severity:** Warning.

This newly created message is specific to TruFOS certificates and will be logged alongside LIC-1010 and LIC-1011 for TruFOS certificates. The message will be generated **10, 5, and 1 day(s)** before the TruFOS certificate expiration.

**Note:** LIC-1012 is a new message, designed specifically to append additional information for TruFOS certificates.

### 4.2.5.9 VMID+ limits per LS

In FOS v9.2.2 the VMID+ target port limit per logical switch has been removed.

The total number of VMID+ target ports per platform is unchanged

- X7 directors support 64 VMID+ target ports
- Gen 7 switches support 16 VMID+ target ports

## 4.2.6 Web Tools

This section describes the enhancements in Web Tools with FOS v9.2.2

### 4.2.6.1 Federated Authentication

In FOS v9.2.2 it is supported to login to FOS using Federated Authentication. When configuring Federated Authentication in FOS, two different authentication modes are supported. The Web Tools authentication workflow is adapted accordingly.

**FA only Authentication Mode:**

Upon entering the Switch IP address in the browser, the URL will be redirected to the IDP server for authentication. After successful authentication at IDP, the URL will be redirected to the Web Tools Dashboard view. Web Tools login page will not be shown to the user in this workflow.

**Dual Authentication Mode:**

Upon entering the switch IP address in the browser, the Web Tools login screen will be displayed with two options:

1. Users can login with switch credentials by clicking the "Login" button (no change in existing Web Tools login workflow)

## 2. Users can “Login with SSO”.

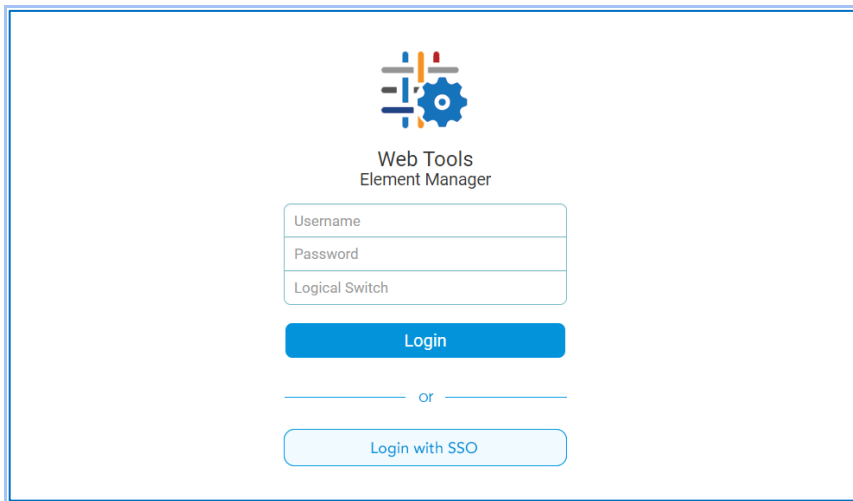
**Scenario-1:** User has **not yet logged** into IDP using the browser that is used to launch Web Tools

1. User clicks on “Login with SSO” button
2. IDP Server's login page is displayed
3. User logs into IDP
4. After successful login to IDP, Browser page is redirected to Web Tools Dashboard landing page

**Scenario-2:** User has **already logged** into IDP using the browser that is used to launch Web Tools

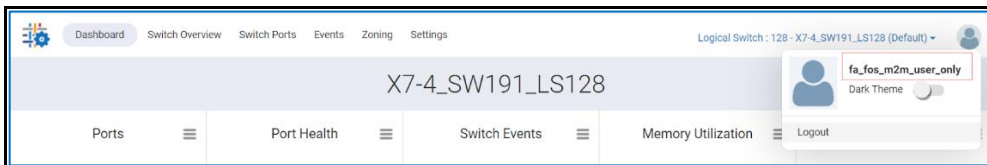
1. User clicks on “Login with SSO” button
2. Browser page is redirected to Web Tools Dashboard landing page

Login screen example:



The login screen for Web Tools Element Manager features a central logo at the top. Below the logo, there are three input fields labeled 'Username', 'Password', and 'Logical Switch'. A prominent blue 'Login' button is positioned below these fields. Underneath the 'Login' button, the word 'or' is centered, followed by a light blue 'Login with SSO' button.

After successful login, the FA user which is used for authentication will be shown in the user info section.



### 4.2.6.2 Default Protocol Type for Transfers

With FOS v9.2.2 Web Tools default protocol type selected for data transfers is set to SCP (previously it was set to FTP). The user can still select to use FTP if enabled in FOS.

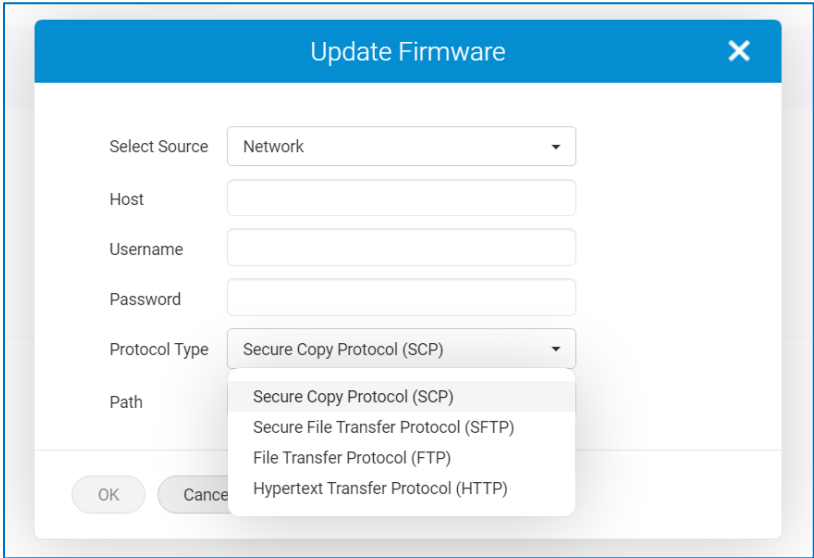
This applies to the following operations and dialogues:

- Update Firmware
- Add License
- Backup Configuration
- Restore Configuration



In the example below shown for Update Firmware.

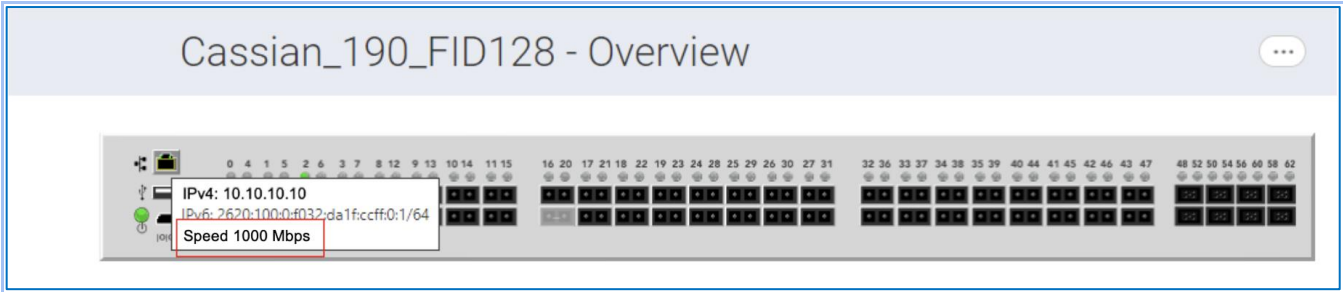
Example:



4.2.6.3    Displaying Management Port Speed

With FOS v9.2.2 Web Tools is updated to display the management port speed with unit **Mbps** (was previously M).  
The update is shown in the example below.

Example:



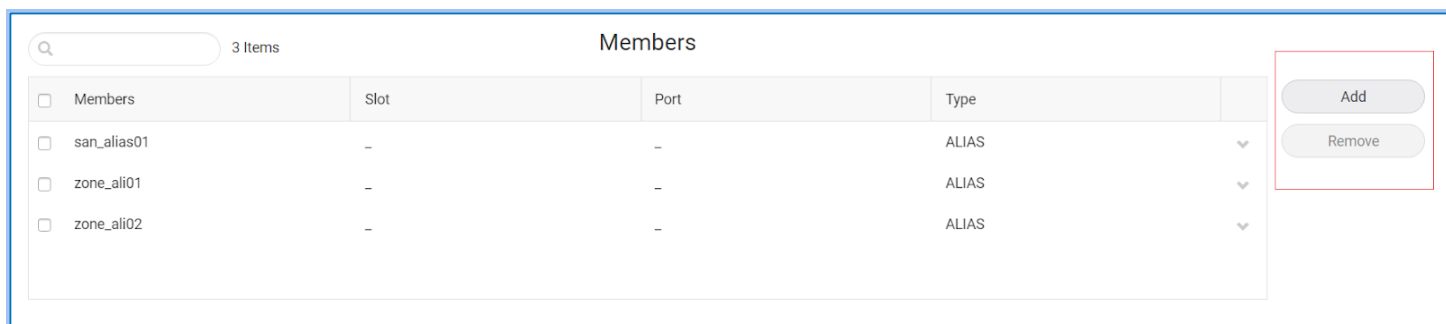
4.2.6.4    Web Tools Support for Password with up to 510 Characters

With FOS v9.2.2 support for 510 characters for user account passwords, Web Tools is updated accordingly to support 510 characters.

### 4.2.6.5 Web Tools Tables Improved to Display at Full Width

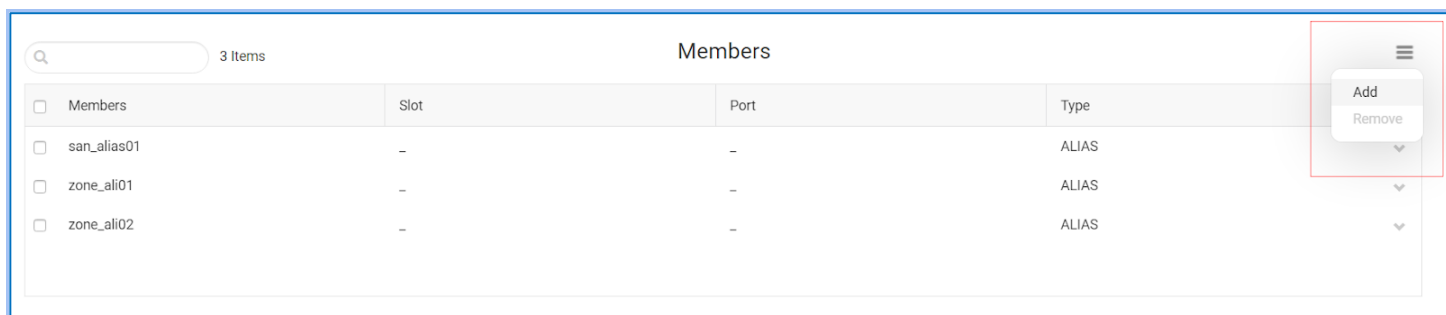
With FOS v9.2.2 displaying tables in Web Tools is improved to provide full width.

In previous FOS versions the menu buttons were placed right to the table and the table could not use the full available width even though there were no menu buttons.



Members	Slot	Port	Type
san_alias01	-	-	ALIAS
zone_ali01	-	-	ALIAS
zone_ali02	-	-	ALIAS

In FOS v9.2.2 the table action button is moved into the table hamburger menu and the table width is maximized to occupy the page.



Members	Slot	Port	Type
san_alias01	-	-	ALIAS
zone_ali01	-	-	ALIAS
zone_ali02	-	-	ALIAS

## 4.2.7 Deprecated Features and Commands

When discontinuing features and commands in FOS the procedure is to first deprecate the feature or command while functionality is intact, in a subsequent release the deprecated feature(s) and command(s) are obsoleted and no longer available. Commonly upgrade to the version where a feature or command is obsoleted is blocked when the feature is still in use.

In FOS v9.2.2 the following features are deprecated, see each specific section for details

- Non-secure protocols (HTTP, FTP, TELNET)
- TLS versions lower than 1.2
- SNMPv1
- IPFC
- TACACS+
- RADIUS
- Cascaded AG
- Extension: FICON Emulation Modes (XRC, TAPE)

- FSPF commands (`interfaceShow`, `nbrShow`)
- FCoE
- FCR
  - LSAN speed and enforce tag
  - Boot over SAN
- FSPF commands

#### 4.2.7.1 Non-secure protocols (HTTP, FTP, TELNET)

The non-secure protocols HTTP, FTP and TELNET are deprecated.

Functionality is kept intact.

**NOTE** There are no notifications when configuring non-secure protocols that these are deprecated.

#### 4.2.7.2 TLS versions lower than 1.2

TLS versions lower than 1.2 are deprecated.

Functionality is kept intact, and warning is displayed on CLI when configuring usage of TLS versions lower than 1.2

#### 4.2.7.3 SNMPv1

SNMPv1 is deprecated.

Functionality is kept intact, and warning is displayed on CLI (and Web Tools) when configuring usage of SNMPv1

#### 4.2.7.4 IPFC

IPFC used when directly accessing Logical Switch management interfaces on the LS IP address (instead of using `'setcontext'` from FID128) is deprecated.

Users are recommended to login to FID128 and use the command `'setcontext'` to change to the desired LS (FID) for operations.

Functionality is kept intact, and warning is displayed on Web Tools when using IPFC to connect to a Logical Switch.

**NOTE** There are no notifications when using SSH to the LS.

#### 4.2.7.5 TACACS+

TACACS+ is deprecated.

Functionality is kept intact, and warning is displayed on CLI when configuring usage of TACACS+

#### 4.2.7.6 RADIUS

RADIUS is deprecated.

Functionality is kept intact, and warning is displayed on CLI when configuring usage of RADIUS

### 4.2.7.7 Cascaded Access Gateway

Topologies with Cascaded Access Gateway are deprecated.

Functionality is kept intact.

**NOTE** There are no notifications when deploying Cascaded AGs with other switches than G710.

When attempting to deploy Cascaded AG with G710 as the core AG, the connected ports on both the edge and core AG switches will be disabled and an error message is displayed in the command output for `switchshow` specifying that Cascaded AG is not supported.

### 4.2.7.8 Extension: FICON Emulation Modes (XRC, TAPE)

FICON emulation modes for XRC and TAPE are deprecated.

Functionality is kept intact while the end user is notified with a warning message during FCIP CLI configuration.

### 4.2.7.9 FCoE

FCoE functionality is kept intact while the end user is notified with a warning message during FCoE CLI configuration.

A RASLOG message notifying deprecation will be posted during boot-up and configdownload

In FOS 9.2.2 release, FCoE users will be provided a warning message in CLI and via RASLOG about this deprecation.

The end user is notified with following warning message:

```
"Warning: FCoE is deprecated and will be obsoleted in a future FOS version.  
In this FOS version, FCoE functionality is unchanged. Please plan accordingly."
```

The above message will be displayed in following cases:

- When FCoE CLI commands are initiated by user which modify FCoE configuration
- During firmware upgrade from pre-9.2.2 to 9.2.2 release, if FCoE configuration is detected

Following will be the new RASLOG:

```
2024/03/07-10:56:55:627999 (GMT), [FCOE-1045], 28985/3687, SLOT 2 | FID 128, INFO, sw0,  
FCoE is deprecated and will be obsoleted in a future FOS version.  
In this FOS version, FCoE functionality is unchanged.
```

This RASLOG will be posted per logical switch in the following events:

- When FCoE configuration is detected during boot
- When FCoE configuration is detected during config download

For example, if FCoE configuration is detected in logical switches with FID 128 and 55, following RASLOGs will be observed:

```
2024/03/07-10:57:01:259799 (GMT), [FCOE-1045], 29033/3702, SLOT 2 | FID 128, INFO, sw0,  
FCoE is deprecated and will be obsoleted in a future FOS version.  
In this FOS version, FCoE functionality is unchanged.
```

```
2024/03/07-10:57:01:281062 (GMT), [FCOE-1045], 29035/3703, SLOT 2 | FID 55, INFO,  
switch_55, FCoE is deprecated and will be obsoleted in a future FOS version.  
In this FOS version, FCoE functionality is unchanged.
```

### 4.2.7.10 FCR speed and enforce tag

FCR speed and enforce tag configuration is deprecated in FOS v9.2.2, functionality is intact while users will be provided a warning message when executing `fcrlsan` commands.

For the following CLI commands:

```
fcrlsan --add
fcrlsan --remove
fcrlsan --show
fcrlsan --help
```

Users will receive the warning message

```
"Warning: This command will become obsolete in a future release."
```

Example:

```
switch:admin> fcrlsan --add -speed fast1
Warning: This command will become obsolete in a future release.
LSAN tag set successfully
```

### 4.2.7.11 FCR: Boot Over SAN

Boot over SAN with FCR is deprecated.

### 4.2.7.12 FSPF Commands

In FOS v9.2.2 the following commands are deprecated:

- `InterfaceShow`
- `NbrShow`

The user can display any necessary info with the commands `linkCost` and `nbrStateShow`.

## 4.2.8 Obsoleted Features and Commands

In FOS v9.2.2 the following features are obsoleted, see each specific section for details.

- Boot LUN Zoning
- Reboot -f

### 4.2.8.1 Boot LUN Zoning

Boot LUN Zoning was deprecated in a previous version of FOS and is obsoleted in FOS v9.2.2.

The command `bootluncfg` is removed in FOS v9.2.2.

Upgrade to FOS v9.2.2 is not permitted when Boot LUN zones exist in the zone database and must be deleted prior to upgrade.

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

Examples of blocked importation due to presence of boot LUN zones

- Zone Merges
- Downlevel switch creation
- Configdownload operations
- Firmwareupgrade
- HA sync from a downlevel Active CP

### 4.2.8.2 Reboot -f

In FOS v9.2.2 the command (option) `reboot -f` is obsoleted.

This command is redundant.

# Chapter 5: Software License Support

## 5.1 Optionally Licensed Software

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

Optionally licensed features include:

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

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

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

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

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

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

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

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

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

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

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

### On the Brocade X6-8:

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

### On the Brocade X6-4:

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

**On the Brocade X7-8:**

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

**On the Brocade X7-4:**

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

**On the Brocade 7810:**

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

## 5.2 Temporary License Support

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

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

**NOTE**

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

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

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



# Chapter 6: Hardware Support

## 6.1 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 G710 Switch
- Brocade G630 Switch
- Brocade G620 Switch
- Brocade G610 Switch
- Brocade G648 Blade Server SAN I/O Module
- Brocade 7850 Extension Switch
- Brocade 7810 Extension Switch

## 6.2 Supported Blades

### 6.2.1 X6-8 and X6-4 Blade Support

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

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

### 6.2.2 X7-8 and X7-4 Blade Support

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

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

## 6.3 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*.

## 6.4 Supported Optics

FOS v9.2.2 is the first release supporting the 25GbE SFP+ LR, PN: 57-1000504=01 (CBR-25G-LR-01) with serial number CDA9 xxxxxxxxxxxx (for the 7850 extension switch).

When this optic is present and downgrade from FOS v9.2.2 is performed, the `firmwaredownload` will fail.

FOS v9.2.0 is the first release supporting the Gen 7 FC QSFP+, PN: 57-1000481-01 (XBR-000420) with serial number BAB1yywwxxxxxxxxs.

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

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

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

# Chapter 7: Software Upgrades and Downgrades

## 7.1 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 [FOS Image Filenames](#).

### 7.1.1 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.

#### 7.1.1.1 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:

```
The server is inaccessible or firmware path is invalid or the firmware doesn't
support this platform. Please make sure the server name/IP address and the firmware
path are valid, the protocol and authentication are supported. It is also possible
that the RSA host key could have been changed and please contact the System
Administrator for adding the correct host key.
```

#### 7.1.1.2 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.

## 7.2 FOS Image Filenames

### Fabric OS v9.2.2

Image Filename	Description
v9.2.2.md5	Fabric OS v9.2.2 MD5 Checksums
v9.2.2_all_mibs.tar.gz	Fabric OS v9.2.2 SNMP MIBs
v9.2.2_EXT.tar.gz	Fabric OS v9.2.2 for Linux to install on 7810 and 7850 platforms
v9.2.2_EXT.zip	Fabric OS v9.2.2 for Windows to install on 7810 and 7850 platform
v9.2.2_EMB.tar.gz	Fabric OS v9.2.2 for Linux to install on G648 platform
v9.2.2_EMB.zip	Fabric OS v9.2.2 for Windows to install on G648 platform
v9.2.2_G6_ENTRY.zip	Fabric OS v9.2.2 for Windows to install on G610 platform
v9.2.2_G6_ENTRY.tar.gz	Fabric OS v9.2.2 for Linux to install on G610 platform
v9.2.2_G6_MID.tar.gz	Fabric OS v9.2.2 for Linux to install on G620 platform
v9.2.2_G6_MID.zip	Fabric OS v9.2.2 for Windows to install on G620 platform
v9.2.2_G6_ENTP.tar.gz	Fabric OS v9.2.2 for Linux to install on G630 platform
v9.2.2_G6_ENTP.zip	Fabric OS v9.2.2 for Windows to install on G630 platform
v9.2.2_G7_ENTRY.zip	Fabric OS v9.2.2 for Windows to install on G710 platform
v9.2.2_G7_ENTRY.tar.gz	Fabric OS v9.2.2 for Linux to install on G710 platform
v9.2.2_G7_MID.tar.gz	Fabric OS v9.2.2 for Linux to install on G720 platform
v9.2.2_G7_MID.zip	Fabric OS v9.2.2 for Windows to install on G720 platform
v9.2.2_G7_ENTP.tar.gz	Fabric OS v9.2.2 for Linux to install on G730 platform
v9.2.2_G7_ENTP.zip	Fabric OS v9.2.2 for Windows to install on G730 platform
v9.2.2_G6G7_DIR.tar.gz	Fabric OS v9.2.2 for Linux to install on X6-8, X6-4, X7-8 and X7-4 platforms
v9.2.2_G6G7_DIR.zip	Fabric OS v9.2.2 for Windows to install on X6-8, X6-4, X7-8 and X7-4 platforms
v9.2.2.releasenotes_v1.pdf	Fabric OS v9.2.2 Release Notes

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

## 7.3 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.

### 7.3.1 Migrating to FOS v9.2.2

The supported upgrade paths to Fabric OS v9.2.2 are as follows:

Current Version	Upgrade Path
FOS v9.2.0x	Nondisruptive upgrade
FOS v9.2.1x	Nondisruptive upgrade
FOS v9.1.x	Direct upgrade is not supported  First upgrade from v9.1.x to v9.2.0x, then upgrade to v9.2.2 (Install TruFOS certificate prior to upgrading to v9.2.x if not already present)
FOS v9.0.x	Direct upgrade is not supported.  First upgrade from v9.0.x to v9.2.0x, then upgrade to v9.2.2 (Install TruFOS certificate prior to upgrading to v9.2.x if not already present)  <b>Note:</b> Direct upgrade v9.0x to v9.2.0x is disruptive, for non-disruptive upgrade first upgrade v9.0x to v9.1x then v9.1x to v9.2.0x
FOS v8.2.x	First upgrade from FOS v8.2.x to FOS v9.0.x. Then install TruFOS Certificate and proceed according to above.

### 7.3.2 Migrating from FOS v9.2.x

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

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

Platforms	Fabric OS v9.2.x	Fabric OS v9.1.x	Fabric OS v9.0.x	Fabric OS v8.2.x
<b>Brocade Gen 7 (64G) Directors</b>				
Brocade X7-4 Director	Supported	Supported	Supported	Not Supported
Brocade X7-8 Director	Supported	Supported	Supported	Not Supported
<b>Brocade Gen 7 (64G) Fixed-Port Switches</b>				
Brocade G710 (Switch Type 191.0)	Supported (Fabric OS v9.2.2 and later)	Not Supported	Not Supported	Not Supported
Brocade G720 (Switch Type 181.0)	Supported	Supported	Supported	Not Supported
Brocade G720 (Switch Type 181.5)	Supported	Supported (Fabric OS v9.1.1 and later)	Not Supported	Not Supported
Brocade G730 (Switch Type 189.8)	Supported	Supported	Not Supported	Not Supported

<b>Brocade Gen 6 (32G) Directors</b>				
Brocade X6-4	Supported	Supported	Supported	Supported
Brocade X6-8	Supported	Supported	Supported	Supported
Brocade X6-4 (Switch Type 165.5)	Supported	Supported (Fabric OS v9.1.0b and later)	Not Supported	Not Supported
Brocade X6-8 (Switch Type 166.5)	Supported	Supported (Fabric OS v9.1.0b and later)	Not Supported	Not Supported
<b>Brocade Gen 6 (32G) Fixed-Port Switches</b>				
Brocade G610 (Switch Type 170.0 to 170.3)	Supported	Supported	Supported	Supported
Brocade G610 (Switch Type 170.4 or higher)	Supported	Supported	Supported (Fabric OS v9.0.1b and later)	Not Supported
Brocade G620 (Switch Type 162)	Supported	Supported	Supported	Supported
Brocade G620 (Switch Type 183.0)	Supported	Supported	Supported	Not Supported
Brocade G620 (Switch Type 183.5)	Supported	Supported (Fabric OS v9.1.1 and later)	Not Supported	Not Supported
Brocade G630 (Switch Type 173)	Supported	Supported	Supported	Supported
Brocade G630 (Switch Type 184)	Supported	Supported	Supported	Not Supported
<b>Brocade Extension Switches</b>				
Brocade 7850 Extension Switch	Supported	Not Supported	Not Supported	Not Supported
Brocade 7810 Extension Switch	Supported	Supported	Supported	Supported (Fabric OS v8.2.1 and later)
<b>Embedded Switches</b>				
Brocade G648 Blade Server SAN I/O Module	Supported	Supported	Supported	Supported
Brocade MXG610 Blade Server SAN I/O Module	Not Supported	Supported	Supported	Supported

## 7.4 Brocade Trusted FOS (TruFOS) Certificate

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

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

- G720
- G620
- G610
- 7850
- 7810

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

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

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

## 7.5 Upgrade/Downgrade Considerations

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

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

## Chapter 8: Limitations and Restrictions

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

### 8.1 Scalability

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

#### 8.1.1 Flow Vision

In FOS v9.2.1 (and later) the distribution of IT and ITL/ITN scale and stats granularity are changed as shown in the table below:

Property	FOS v9.2.0	FOS v9.2.1 and later
Total flows	72k	72k
IT	8k	32k
IT stats granularity	5 min	5 min
ITL/ITN	64k	56k
ITL/ITN stats granularity	6h	30 min
VITL/VITN	64k*	56k*
VITL/VITN stats granularity	6h	30 min

\*ITL/ITN and VITL/VITN share the same resource allocation and is provided on the principle of first come/first serve.

Flow Vision is not supported the Brocade 7850 Extension platform.

### 8.2 Compatibility/Interoperability

This section describes important compatibility and interoperability across Brocade products.

#### 8.2.1 Brocade SANnav Management Portal Compatibility

When managing SAN switches with SANnav Management Portal it is required to first upgrade SANnav Management Portal to v2.3.2 (or later) prior to upgrading SAN switches to FOS v9.2.2.

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



## 8.2.2 Web Tools Compatibility

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

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

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

## 8.2.3 Fabric OS Compatibility

- The following table lists the earliest versions of Brocade software supported in this release, that is, the earliest supported software versions that interoperate. Use the latest software versions to get the greatest benefit from the SAN.
- To ensure that a configuration is fully supported, always check the appropriate SAN, storage, or blade server product support page to verify support of specific code levels on specific switch platforms before installing on your switch. Use only Fabric OS versions that are supported by the provider.
- For a list of the effective End-of-Availability dates for all versions of Fabric OS software, refer to the *Brocade Software End-of-Availability Notice* published to the Brocade Product End-of-Life web page [www.broadcom.com/support/fibre-channel-networking/eol](http://www.broadcom.com/support/fibre-channel-networking/eol).
- For the latest support and posting status of all release of Brocade Fabric OS, refer to the *Brocade Software: Software Release Support and Posting Matrices* published to the Brocade Product End-of-Life web page [www.broadcom.com/support/fibre-channel-networking/eol](http://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 <sup>1</sup>
Brocade DCX 8510-8/DCX 8510-4 with FC16-64 blade	FOS v8.2.x <sup>1</sup>
Brocade 6505, 6510, 6520, 7840	FOS v8.2.x <sup>1</sup>
Brocade 6542	FOS v8.2.x <sup>1</sup>
Brocade 6543	FOS v8.2.x <sup>1</sup>
Brocade 6547, 6548, M6505, 6545, 6546	FOS v8.2.x <sup>1</sup>
Brocade 6558	FOS v8.2.x <sup>1</sup>

<sup>1</sup> Only qualified with FOS v9.0.0 or later.

Brocade G610 (switchType 170.0 to 170.3)	FOS v9.0.0 or later <sup>2</sup>
Brocade G610 (switchType 170.4 or higher)	FOS v9.0.1b or later
Brocade G620 (switchType 162)	FOS v9.0.0 or later
Brocade G620 (switchType 183.0)	FOS v9.0.0 or later
Brocade G620 (switchType 183.5)	FOS v9.1.1 or later
Brocade G630 (switchType 173)	FOS v9.0.0 or later <sup>Error! Bookmark not defined.</sup>
Brocade G630 (switchType 184)	FOS v9.0.0 or later
Brocade 7810	FOS v9.0.0 or later <sup>Error! Bookmark not defined.</sup>
Brocade X6-8/X6-4	FOS v9.0.0 or later <sup>Error! Bookmark not defined.</sup>
Brocade X6-8/X6-4 (switchType 166.5 and 165.5)	FOS v9.1.0b or later
Brocade G710 (switchType 191.0)	FOS v9.2.2 or later
Brocade G720 (switchType 181.0)	FOS v9.0.0 or later
Brocade G720 (switchType 181.5)	FOS v9.1.1 or later
Brocade G730 (switchType 189.8)	FOS v9.1.0 or later
Brocade X7-8/X7-4	FOS v9.0.0 or later
Brocade G648 <sup>3</sup>	FOS v9.0.0 or later
Brocade MXG610 <sup>4</sup>	FOS v9.0.1a or later
Brocade 7850	FOS v9.2.0 or later

## 8.2.4 SNMP Support

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

<sup>2</sup> While this platform is supported with FOS v8.x it is only qualified with FOS v9.0.0 or later.

<sup>3</sup> Brocade G648 is also supported with FOS v8.2.0\_gft release.

<sup>4</sup> Brocade MXG610 is also supported with FOS v8.1.0\_Inx2, v9.0.1a, and v9.1.0b.

## 8.2.5 Obtaining MIBs

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

1. Go to [support.broadcom.com](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.

Broadcom does not distribute standard MIBs. Download the required standard MIBs from the [www.oidview.com](http://www.oidview.com) or [www.simpleweb.org/ietf/mibs](http://www.simpleweb.org/ietf/mibs).

## 8.2.6 Flow Vision, IO Insight and VM Insight

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

## 8.2.7 REST API Support

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

### 8.2.7.1 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 [www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system](http://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 [github.com/broadcom/yang](https://github.com/broadcom/yang).

## 8.3 Important Notes

Brocade recommends to always review Important Notes for each release.

### 8.3.1 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).

### 8.3.2 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 4Gb/s Access Gateway.

### 8.3.3 ClearLink Diagnostics (D\_Port)

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

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

The following are specific adapter models and driver versions supported by Brocade with Fabric OS v9.2.x for ClearLink Diagnostics.<sup>5</sup>

	Emulex 16G Adapter	Emulex 32G Adapter	Emulex Gen 7 Adapter	QLogic 16G Adapter	QLogic 32G Adapter	QLogic 64G Adapter
Adapter Model	LPe16002B-M6	LPe32002-M2	LPe35002 LPe35004 LPe36000	QLE2672	QLE2742	QLE2872
Adapter Firmware	12.8.542.25	12.8.542.26	12.8.542.xx	v8.08.231	v9.0.6.02	V9.12.0.1
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	STOR Miniport 9.4.9.21

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.

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

## 8.3.4 DDNS

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

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

## 8.3.5 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 behavior.

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

## 8.3.7 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 10Mb/s, certain FOS operations such as `firmwaredownload` may fail.
- The 10Gb/s management interface on CPX6 blades is not supported.
- Half-duplex mode is not supported in FOS v9.x and is blocked.
- The `ethif --reseterror` command option is supported in FOS v9.1.x and later.

## 8.3.8 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 to 9.1.x	7840	8.2.1 or later
7810	9.0.0 to 9.1.x	7840	8.2.1 or later

**NOTE** Extension between a Brocade 7810 or SX6 running FOS v9.2x and a Brocade 7840 is not supported.

Extension between a Brocade 7850 and Brocade 7810 or SX6 is supported only if the 7810 or SX6 is running FOS 9.2.0 or later. The following table documents the combinations.

Site1 Switch/Blade	Site1 Firmware	Site2 Switch/Blade	Site2 Firmware
7850	9.2.0 or later	7810	9.2.0 or later
7850	9.2.0 or later	SX6	9.2.0 or later

**NOTE** Extension between a Brocade 7850 and a Brocade 7840 is not supported.

Downgrade from FOS v9.2.2 is not supported when the optic 25GbE SFP+ LR, PN: 57-1000504=01 (CBR-25G-LR-01) with serial number CDA9 xxxxxxxxxx is present on the switch.

## 8.3.9 FCoE

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

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

### 8.3.10 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.

### 8.3.11 Firmware Migration

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

**NOTE** This only applies when starting from FOS v9.0.x. When performing staged `firmwaredownload` migration starting from FOS v9.1.x to FOS v9.2.0 this does not apply.

**NOTE** When upgrading deployments with FCoE (UCS FI connected with Ethernet Uplinks) from FOS v9.1.0x the following order must be followed to ensure non-disruptive upgrades:  
FOS v9.1.0x -> v9.1.1x -> v9.2.0x in order to retain FCoE logins and traffic during the upgrade process.

**NOTE** An SNMP FFDC file may result as part of firmware migration to or from FOS v9.2.1 when the switch or director chassis is managed by SANnav v2.3.1. The conditions necessary to encounter the FFDC are the FOS level on the standby CP or secondary partition lack SHA512 authentication support. There is no functional impact however FFDC generation message appears repeatedly.

## 8.3.12 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 v9.x Compatibility Matrix* for supported DWDM equipment and restrictions on FEC use.

## 8.3.13 FPGA Upgrade

In general FPGA upgrades should only be performed when directed by your support provider.

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

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

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

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

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

### 8.3.13.1 FPGA Upgrade (for FOS v9.1.1 and Later)

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

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

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

7. Verify the FPGA on the first CR64 blade is upgraded with the command `fpgaupgrade -latest`.
  - a. Verify the FPGA code level is 0x01.0a
8. Enable the first CR64 blade with the command `portenable -s <core blade slot #> (as needed)`.
9. Persistently enable all ICL ports on the CR64 blade (which were disabled in step 5 prior to the upgrade) `portcfgpersistentenable <ICL port>`.

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

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

The FPGA upgrade is now complete.

### 8.3.14 Optimized Credit Model for G630 and X7-8/4

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

- FC32-48
- FC32-64
- SX6

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

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

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

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

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

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

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

```
System is not optimized for credit stall and over subscription flows.
```

Use `--set` command to optimize the flows.

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

Example:

```
Switch:FID128:admin> fossystem --set -qos 1
```

```
fossystem success
```

```
Switch:FID128:admin> fossystem --show -qos 1
```

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



## 8.3.15 Security

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

### Default Secure

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

### Default Session Limit

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

### OU field in FOS switch CSRs no longer available

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

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

Example of the Warning message:

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

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

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

Excerpt of certificate with OU field:

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

**Excerpt of certificate without OU field:**

```
openssl x509 -in 10.10.10.10-web.pem -text -noout
```

Certificate:

Data:

Version: 3 (0x2)

Serial Number: 4098 (0x1002)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, ST = California, L = San Jose, O = Brocade, CN = 10.10.10.10,

emailAddress = name@domain

Validity

Not Before: Apr 14 13:41:43 2023 GMT

Not After : Apr 11 13:41:43 2033 GMT

Subject: C = US, ST = California, O = Brocade, CN = 10.10.10.10, emailAddress = name@domain

**The Following Security Enhancements All Apply to FOS v9.x**

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

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

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

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

- FOS v9.x does not support F\_Port authentication to Marvell QLogic BR series (Former Brocade Product Line) HBAs as these HBAs only support legacy Brocade F\_Port authentication. For these devices to connect to FOS v9.x, F\_Port authentication must be disabled.
- FOS v9.x does not support F\_Port trunking when F\_Port authentication is enabled.

- Prior to upgrading to FOS v9.x:
  - First, ensure the secrets on both the switches (E-port authentication) are not the same. Otherwise, the E-port will segment after the upgrade to v9.x
  - Secondly, reconfigure shared secrets to be in compliance with FC-SP 2 standard.

If users configure any duplicated Virtual Fabric (VF) list with `ldapcfg -mapattr <ldaprole>` command, only the first mapping from the list will be used during LDAP authentication and authorization.
- FOS v9.x requires role mapping or VSA attributes to be configured for LDAP user authentication in a VF-enabled switch. In a non-VF switch, `ldapcfg --maprole` is mandatory. It should be configured before upgrading to FOS v9.x to avoid login failure for LDAP users.
- Users must specify the domain of an LDAP server when adding the LDAP server to the remote AAA configuration of a switch.
- Optional certificate extensions, such as BasicConstraints, KeyUsage, and ExtendedKeyUsage are ignored when a certificate containing these is imported in basic mode. During session establishment, the extensions are validated. Hence, invalid extensions will be rejected and result in session failure.
- Login of LDAP users using Distinguished Name (DN) will be supported only for the users created in container “Users” of the domain configured in the switch, even though the switch is configured with Global Catalog (GC) port of the server. Login using User Principal Name (UPN) and sAMAccountName will be supported irrespective of the domain and OU on which the user is created.

### 8.3.15.1 Syslog

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

Example, verifying `cfgload.secure` setting:

```
Switch:FID128:admin> configure --show -mod CHS
```

Key Name	Value
Add Suffix to the uploaded file name( <code>cfgload.cfgfile_suffix</code> )	0
Do you want to enable auto firmwaresync( <code>cfgload.firmware_sync</code> )	1
Enable secure switch mode( <code>cfgload.secure</code> )	1

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

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

Or

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

To change the `cfgload.secure` setting to 0 use the command

```
configure --set -mod CHS -key cfgload.secure -value 0
```

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

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

```
Switch:FID128:admin> configure --show -mod CHS
```

Key Name	Value
Add Suffix to the uploaded file name( <code>cfgload.cfgfile_suffix</code> )	0
Do you want to enable auto firmwaresync( <code>cfgload.firmware_sync</code> )	1
Enable secure switch mode( <code>cfgload.secure</code> )	0

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

## 8.3.16 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.

## 8.3.17 Brocade X6 Field Migration

- Field migration of a Brocade X6 switch to an upgraded X6 with Gen 7 support is not supported in FOS v9.2.x. In case a Brocade X6 switch is running FOS v9.2.x and it is desired to migrate to an upgraded X6 with Gen 7 support it is required to first downgrade to FOS v9.1.x and then perform the migration.
- FOS v9.1.x is the last release which supports a field migration of a Brocade X6 (Switch Type 165.5 and 166.5) to an upgraded X6 with Gen 7 support.
- Field migration of a Brocade X6 to an upgraded X6 with Gen 7 support is available with FOS v9.0.0x, FOS v9.0.1x and FOS v9.1.x.  
Refer to the *Brocade X6 Field Migration Guide* for step-by-step instructions.
- During field migration of Brocade X6 to a field upgraded X6 with Gen 7 support, the `portcfgupload` file will contain `portcfgtrunkport` commands for ICLs. A warning message is displayed to indicate that the command is not valid for ICL ports because trunking cannot be disabled on ICLs. This warning will not affect the ICLs and is harmless.

## 8.3.18 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 slot director, it can take up to five 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 behavior will not cause any functional impact.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades do not support 4G EX-Port.
- Brocade G620 with switchType 183, G630 with switchType 184, and FC32-X7-48 blades support 4G E-Port connected between any of the three listed only.
- When Connecting Brocade G730 with X7, G720, G620 switchType 183 or G630 switchType 184 these switches should run FOS v9.0.1c or later.
- When performing a configdownload operation this will not overwrite the existing MAPS Custom RASLog mode feature configuration on the switch. For example, if custom raslog mode is disabled in the switch but it is enabled in downloaded configuration, then the feature will remain disabled in switch and must be manually configured after the configdownload operation is complete.
- In FOS v9.1.1, CPX blades in X6 Switch Type 165.5 and 166.5 and X7 are displayed as CPX7 in slotshow command output.
- When upgrading from FOS v9.0.x to FOS v9.1.x, the AG ports will be moved from ALL\_HOST\_PORTS group to ALL\_OTHER\_F\_PORTS group. Consequently, the MAPS thresholds for ALL\_OTHER\_F\_PORTS will apply to these ports in FOS v9.1.x. The default thresholds for the groups ALL\_HOST\_PORTS and ALL\_OTHER\_F\_PORTS are the same and if these are not changed there is no impact. In case custom thresholds are used and these are configured differently for the groups ALL\_HOST\_PORTS and ALL\_OTHER\_F\_PORTS the thresholds (monitoring) for AG ports are impacted accordingly.
- When performing factory reset on an X6/X7, the cipher.syslog key is not reset to factory value.

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

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

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

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

The resolution is to enable RA to resolve IPv6 network connectivity issues.

- In case an NPIV flow is identified as SDDQ or Over Subscribed (and moved by Traffic Optimizer to an OS PG), the flow movement may cause some frames to be delivered Out of Order (OOO). In general, open systems devices have no issues when this happens.
- When performing `supportSave` with SCP as the selected transfer protocol, the command defaults to using SFTP internally. In environments where SFTP ports are blocked the `supportSave` upload will fail.
- When displaying the content of an attached USB with the command `usbstorage --list` the directory structure is displayed using "/" (slash) in previous versions of FOS this was "\" (back slash).
- GigE ports on SX6 and 7850 platforms can only be moved to a logical switch when the port has only speed and autonegotiation configuration. This is a change in behavior from earlier releases.
- The command `firmwarecleaninstall` is available only for install of FOS v9.2.0a (upgrade or downgrade is not supported).
- When upgrading a Gen 7 director or switch (X7-4, X7-8, G730, G720) to FOS v9.2.x, it is recommended to upgrade to FOS v9.2.0a or later. For additional information refer to *TSB 2023-289-A*.
- When doing repeated failovers on NetApp A400 and FAS9000 storage arrays, the switch can register very high counts of uncorrectable errors on the ports connected to the storage arrays. These errors do not have any impact on storage data transport.
- In FOS v9.2.1 the MAPS chassis\_memory -lnRange rule is unmonitored and obsoleted.

- In the FC port external schema (available through NB streaming from SANnav Management portal) the user\_port\_index has been replaced with port\_number for ease of use for end users:  
Previous schema (pre FOS v9.2.1):  

```
{ "name" : "user_port_index", "type" : "int", "doc": "The user port index of the front-end port." }
```

  
New schema (FOS v9.2.1):  

```
{ "name" : "port_number", "type" : "string", "doc": "The slot/port number of the port", "default": "" },
```
- An SNMP FFDC file may result as part of firmware migration to or from FOS v9.2.1 when the switch or director chassis is managed by SANnav v2.3.1. The conditions necessary to encounter the FFDC are the FOS level on the standby CP or secondary partition lack SHA512 authentication support. There is no functional impact however FFDC generation message appears repeatedly.

## Chapter 9: 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:

<https://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:

<https://support.broadcom.com/external/content/SecurityAdvisories/0/25000>



## Chapter 10: Defects

### 10.1 Closed with Code Changes in FOS v9.2.2

Defect ID	Description
FOS-810530	Zone merge slow performance and failure on that switch that has defzone all access defined. Along with this behavior IPC drops RASLOGs events and/or termination of process nsd maybe seen.
FOS-847781	The Hostname attribute is not returned in the GPAT response.
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-849948	EM-1014 raslog states unable to read sensor on PS 1.
FOS-850500	User observes Fan kick starts and stays at a very high speed.
FOS-851010	FCIP Tunnel went down after seeing high rate of CRC errors.
FOS-851639	Switch reboot with DIAG-1000 raslog, after POST2 failure due to sync issue between Diag daemon running on CP and Diag daemon running on DP.
FOS-851800	Ipfiler rule getting added with start port number value when port range was configured with space between port range separator(eg: start_port - end_port instead of start_port-end_port).
FOS-852616	The IPS fabric does not process the fragmented frames and it will discard them. All ICMP requests discarded due to fragmentation are not counted in "portStatsShow" command output.
FOS-853997	When "bulk" persistentEnable'ing ports from SanNav, ports would go to 'No_light' and disabled state.
FOS-854317	DP wait timeout causing ESM to go into Cold recovery during eHCL processing
FOS-854348	"tsclockserver --set/tsclockserver" with FQDN succeeds even if configured DNS is unable to resolve the configured NTP Server FQDN to an IP address
FOS-854359	Tsclockserver: RAS TS-1002 is flooded on non-principal switches when an active NTP server goes offline.
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-854587	The cfsd (Congestion Framework System daemon) terminated during supportsave, resulting in repeated UFCS-2007 messages for "UFCS Lock stage Failed". Also, CFS supportsave info is not collected from all logical switches.
FOS-854609	Adding default static route results in error message. "There are max number of nexthop gateways for a given route already."
FOS-855493	Switch shutdown after abnormal sensor temperatures such as (-1 C) or (191 C) are reported: [HIL-1506], 3498/333, FFDC   , CRITICAL, sw0, High temperature (-1 C) exceeds system temperature limit. System will shut down within 2 minutes., OID:0x43000000, SPOID:0x4300000
FOS-855507	Port Naming for Index showing as Port 0 on some ports
FOS-855788	Maps daemon (mdd) terminates during supportsave.
FOS-855962	Unexpected switch reboot after termination of lldpd process.
FOS-856210	Asic Data is no longer properly collected during supportsave.
FOS-856476	CLI fanshow shows FAN absent when re-inserted.
FOS-856702	E-Ports cannot come online and show incorrect VC assignment
FOS-856789	Unexpected termination of fclagd led to cold recovery
FOS-857267	Processor rebooted - Software Fault:ASSERT during supportsave
FOS-857277	Switch panic with Software Fault:Kernel Panic.
FOS-857387	CP watchdog exception due to excessive print messages
FOS-857418	Server Uplink ports in Bay 3 and 4 fail to come online when port speed is set to 32G.
FOS-857454	Restartable daemons such as mdd, cald, snmp etc terminate and could not be restarted properly, causing HA out of sync and daemons are left in a defunct state.
FOS-857609	cald terminated during flow operation such as CLI "flow --show -feature fabinfo -srcdev "" -egrport" and the performance data can no longer be gathered.
FOS-857638	Switch panic after cfs daemon (cfsd) holds large amount of memory.
FOS-857687	During large HA sync copy operations, switch encounters msd panic

FOS-857838	Switch panic showing HAM-1004 message "Processor rebooted - Software Fault:Kernel panic. With additional message showing "Kernel tried to execute NX-protected page" and "BUG: unable to handle page fault for address: ffffc9...."
FOS-858133	The administrative status will be shown as 'down' for the offline FC ports that have not been manually disabled(No_Module, No_Light, etc).
FOS-858197	BR7810 switches will report frequent ftrace triggers for an active Extension tunnel.
FOS-858263	The default Linux drivers in FOS v9.2x have an incompatibility with a small subset of 7810 switches that may result in 7810 being marked faulty after upgrading to FOS v9.2x
FOS-858427	Repetitive FICON-1056 errors logged after Feature Disable started for one or more extended FICON Devices.
FOS-858793	Observed termination of pdmd during Logical switch manipulation.
FOS-858848	The mdd process encounters a panic. There will be KSWD -1002. The chassis may encounter an HA out of sync condition.
FOS-858851	User experience performance issue on Gen7 after code upgrade.
FOS-858865	Tunnel offline and then back online 4 minutes later
FOS-859282	CLI "flow" fails with Segmentation fault and traffic optimizer dashboards no longer work as expected.
FOS-860003	Following an offline or online event with no zoning (using default zoning all access), an RSCN is not observed on the remote switch in the fabric.
FOS-860049	Transient PCS errors reported on G620.
FOS-860110	Switch firmware version changed to unknown/vpackage.
FOS-860262	Kernel panic while storing trace data.
FOS-860632	Standby CP in RRD state and/or SX6 blades are faulted during code upgrade. inetd on active CP no longer listens on port 514 on ipaddress of 127.3.1.x
FOS-860768	ISL disabled due to "Both Compression/Non-Compression connections exist to neighboring switch" after DWDM event.
FOS-860855	Supportsaves are failing collecting switch SS using SANnav.
FOS-861147	npd crashed as Standby CP was taking over as Active CP during firmwaredownload.

## 10.2 Closed without Code Changes in FOS v9.2.2

Defect ID	Description
FOS-845543	During HCL, observe RASlog ESS-2001 message followed by RASlog ESS-2002.
FOS-849473	Rest returns blank and/or error while switch has a large weblinker process.
FOS-851275	Panic on Standby CP when booting to Active on new firmware after hafailover during concurrent firmwaredownload.
FOS-853425	IpsArpTable --show output is not in sync across the fabric for unresolved devices. The unresolved ARP device is only displayed on the domain where it's being learned.
FOS-854060	Syslogadmin: IPv6 Syslog server IP is logging even after IPv6 addresses are removed from the switch.
FOS-854964	switches experienced snmpd termination and persistent loss of HA sync after customer upgraded snmp monitoring application.
FOS-856244	Switch reports "400 Bad Request" for GET /rest/running/brocade-chassis/chassis for all users
FOS-856472	Flash usage is close to full and observing large /var/log/syslog.* files.
FOS-859473	Switch failed firmware upgrade to FOS v9.2.0 with TruFOS license error

## 10.3 Open in FOS v9.2.2

Defect ID	Description
FOS-859174	Firmwarecommit failure message and HA went out of sync after Standby CP replacement in critical sync state.
FOS-859417	Flow monitor statistics of byte and frame count are higher than the "Frames Per Second" and "Throughput(BPS) " for flows in IPS virtual switch
FOS-860169	When the Static D-Port test is run on a switch connected to 64G Q-Logic HBA, port may get stuck in Offline state, and the Link Traffic test displays "NOT STARTED" state.
FOS-860355	Flowmonitor statistics for SCSI other commands like Inquiry, Reserve, Release, Request Sense, Test Unit Ready is not reported if an F-port trunk is being monitored.
FOS-860601	Lag interface to native vlan association will be missing when switch is enabled after config upload/download.
FOS-860788	iSNS configuration passes through a mixed firmware switch, even when ISL to that switch is segmented. The condition that fabric with a switch having lower firmware version than 9.2.2 shouldn't allow iSNS configuration gets overruled.
FOS-861577	IP filter activation fails on management interface
FOS-861742	Class 2 PLOGI response during RDP Polling leads to switch panic with ASSERT.
FOS-862000	"relayconfig" command does not accept an FQDN value of greater than 40 characters for "rla_ip"
FOS-862074	FCP/SCSI Tape read or write failures over FCIP tunnel with FW and OSTP enabled. XTUN-1002 followed by XTUN-1009 and server IO is terminated.
FOS-862145	When configuring email address to receive MAPS events, and error message 'Duplicate email address specified' shown when configuring multiple email addresses
FOS-862205	The ISL link will be segmented with reason as client timeout during fabric merge. Here the client is IPS configuration module UCID.
FOS-862215	RAS-1001 is generated indicating First Failure Detection Capture (FFDC) is generated for MAPS-5010 event
FOS-862251	REST GET on /brocade-supportlink/supportlink-anonymization incorrectly returns an empty list when data anonymization is disabled.

## Revision History

Version	Summary of changes	Publication date
1.0	Initial version of document	10/15/2024

