Fabric OS® v10.0.0

Fabric OS v10.0.0 Release Notes Digest

Version 3

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

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

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

Table of Contents

Chapter 1: Preface

1.1 Contacting Technical Support for your Brocade® Product

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

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

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

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

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

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

General Information:

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

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

- Switch Serial Number.

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

  The serial number label is located as follows:

  – Brocade G820, G730, G720, G710 – On the switch ID pull-out tab located on the bottom of the port side of the switch.
  – Brocade 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 X8-8, X8-4 – Lower portion of the chassis on the non-port side beneath the fan assemblies.
  – Brocade X7-8, X7-4 – Lower portion of the chassis on the non-port side beneath the fan assemblies.

- World Wide Name (WWN).

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

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

- License Identifier (License ID).

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

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

1.2 Related Documentation

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

Chapter 2: Locating Product Manuals and Release Notes

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

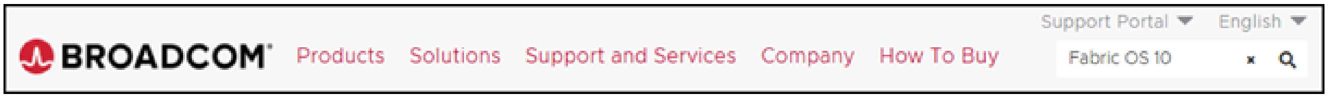
2.1 Locating Product Manuals and Release Notes

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.
2. Enter the product name or the software version number in the **Search** box.

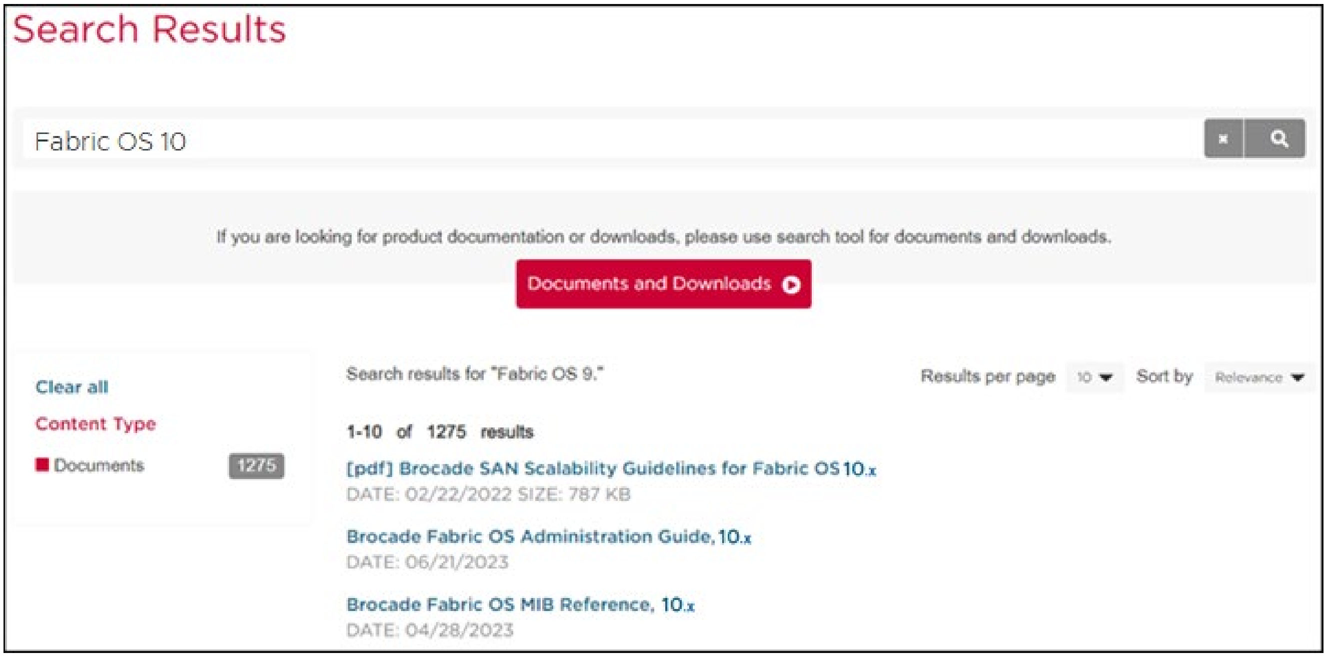
   For example, the following search is for software and documentation files for software version 10.



Fabric OS 10

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

   The list of documents available for the release displays.



Fabric OS 10

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

■ Documents 1275

Search results for "Fabric OS 9."

Results per page 10 Sort by Relevance

1-10 of 1275 results

[pdf] Brocade SAN Scalability Guidelines for Fabric OS 10.x
DATE: 02/22/2022 SIZE: 787 KB

Brocade Fabric OS Administration Guide, 10.x
DATE: 06/21/2023

Brocade Fabric OS MIB Reference, 10.x
DATE: 04/28/2023

2.1.2 Locating Product Manuals and Release Notes on the Support Portal

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

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

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

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

2.2 Document Feedback

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

Chapter 3: Overview

The Fabric OS v10.0.0 is a major release.

This release supports all Gen 8 and Gen 7 hardware platforms.

Fabric OS v10.0.0 includes software enhancements and defect fixes.

NOTE Environments with Gen 7 switches in Access Gateway (AG) mode must review section 7.3.1 Migration to FOS v10.0.0 prior to upgrading to FOS v10.x

Fabric OS v10.0.0 is the initial release supporting Gen 8 hardware.

Chapter 4: What's New in FOS v10.0.0

The Fabric OS v10.0.0 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 v10.0.0 is the first release supporting the following new hardware:

- Brocade X8-8 Director
- Brocade X8-4 Director
- Blades in X8
  - FC128-48
  - ICLX8-8/ICLX8-4
- Brocade G820 Midrange switch
- 128G SWL SFP+
- Gen 8 SWL OSFP (for ICL ports)
- Gen 8 LWL OSFP (for ICL ports)

4.1.1 Platforms

In addition to the new hardware, FOS v10.0.0 also supports all Gen 7 Fibre Channel platforms and optics supported on those platforms as listed below:

- Brocade X7-8 Director
- Brocade X7-4 Director
- Blades in X7 (and X6+)
  - FC64-48
  - FC64-64
  - FC32-X7-48
  - SX6
- Brocade G730 Enterprise switch
- Brocade G720 Midrange switch
- Brocade G710 Entry level switch
- Brocade 7850 Extension switch

NOTE X7 and X6+ (X6 upgraded to X7) with the blade FC32-48 is not supported on FOS v10.0.0 and attempts to upgrade to FOS v10.x will fail.

4.2 New and Modified Software Features

The following areas include new and modified features, described in more detail in respective sections

- SAN Fabric Intelligence
- System Security
- MAPS
- Adaptive Traffic Optimizer
- Fabric Services
- FOS Infrastructure
- Unified Storage Fabric (USF)
- Miscellaneous
- Web Tools
- REST API changes

4.2.1 SAN Fabric Intelligence (SAN FI)

SAN Fabric Intelligence (SAN FI) is a new feature providing a framework for holistic fabric wide visibility of all connected devices and components end to end. SAN FI enables unprecedented capability for monitoring, troubleshooting and cross correlation of servers, storage, VMs and fabric connections.

Many features, metrics, and troubleshooting guidelines already exist to help customers monitor or troubleshoot issues within their SAN fabrics. However, not a single application combines all those capabilities and provides the complete picture of the fabric, including SAN components as well as server and storage.

SAN FI is designed to integrate Server, Storage, and fabric objects, as well as existing and future SAN metrics and stats, as a single entity for monitoring and troubleshooting SAN issues.

NOTE A minimum of one Gen 8 switch must be part of the fabric to enable SAN FI, the command `sanFi` is only available on Gen 8 platforms. Gen 7 switches running FOS v10.0.0 in the same fabric with Gen 8 switch(es) are also supported as data providers.

SAN FI is used to solve the following use cases:

- Storage/server visibility in SAN
  - For example, number of VMs, names of VM and association with servers (hypervisors).
- Association between server, storage and SAN objects
  - Servers/VM/LUNs on a switch port
  - LUNs connected to VM/server/application
  - Switch ports used by a server
- Uplevel SAN telemetry
  - Aggregated IO & frame performance metrics for a VM/server/LUN
- Path enumeration
  - Enumerate fabric paths from source to destination
  - Server → storage
  - Switch port → switch port
  - VM → LUN

- Per hop & per path aggregated metrics
  - Fabric latency (with per hop latency granularity)
  - Physical errors
  - MAPS rules violations
- Fabric wide congestion analysis & characterization, upleveled to server and storage
  - Fabric congestions seen by a server
  - Fabric congestions seen by a VM

For more information on how to use SAN Fabric Intelligence, refer to the *Brocade Fabric OS Administration Guide, 10.x*.

4.2.1.1 SAN Fabric Intelligence Scalability

In FOS v10.0.0 the following scalability for SAN FI is supported per fabric:

vCenter registrations:	1
ESXi host clusters:	128
ESXi hosts:	2048
Max number of VMs per ESXi host:	256
Max number of VMs:	32K
Max number of HBAs per ESXi Host:	32
Max number of HBAs:	6K
Max number of HBA ports:	13K
Max number of ports per HBA:	8
Max number of LUNs:	8K

In FOS v10.0.0 the following scalability for SAN FI is supported per switch:

MAPs violation events:	12K
Congestion events:	20K
Switch ports:	3.6K

4.2.2 System Security Enhancements

This section describes System Security enhancements and changes.

FOS v10.0.0 is using OpenSSH version 9.9 and OpenSSL version 3.5.0

In FOS v10.x quantum resistant algorithms (per CNSA 2.0 classification) are supported. In parallel, for backward compatibility, encryption algorithms which are not considered quantum resistant are still supported as customers transition to only utilize Post Quantum Cryptography (PQC) algorithms.

4.2.2.1 New PQC Algorithms in FOS v10.x

The following PQC algorithms are available in FOS v10.x:

ML-KEM	(mlkem512, mlkem768, and mlkem1024)
ML-DSA	(mldsa44, mldsa65, and mldsa87)
LMS	(used for FOS firmware signatures)

4.2.2.1.1 Usage of PQC Algorithms in FOS v10.x

The following lists the usage of available PQC algorithms in FOS v10.x:

Supported PQC algorithms for SSH:

- mldsa44
- mldsa65
- mldsa87
- falcon512
- falcon1024

Supported PQC algorithms for open SSH KEX:

- ml-kem-512-sha256
- ml-kem-768-sha256
- mlkem768nistp256-sha256
- mlkem1024nistp384-sha384
- ml-kem-1024-sha384
- kyber-512-sha256
- kyber-768-sha384
- kyber-1024-sha512
- frodokem-640-aes-sha256
- frodokem-976-aes-sha384
- frodokem-1344-aes-sha512
- frodokem-640-shake-sha256
- frodokem-976-shake-sha384

- frodokem-1344-shake-sha512
- classic-mceliece-348864-sha256
- classic-mceliece-348864f-sha256
- classic-mceliece-460896-sha512
- classic-mceliece-460896f-sha512
- classic-mceliece-6688128-sha512
- classic-mceliece-6688128f-sha512
- classic-mceliece-6960119-sha512
- classic-mceliece-6960119f-sha512
- classic-mceliece-8192128-sha512
- classic-mceliece-8192128f-sha512
- hqc-128-sha256
- hqc-192-sha384
- hqc-256-sha512
- sntrup761-sha512
- sntrup761x25519-sha512@openssh.com
- ecdh-nistp256-ml-kem-512-sha256@openquantumsafe.org
- ecdh-nistp256-frodokem-640-aesr2-sha256@openquantumsafe.org
- ecdh-nistp384-frodokem-976-aesr2-sha384@openquantumsafe.org
- ecdh-nistp521-frodokem-1344-aesr2-sha512@openquantumsafe.org
- ecdh-nistp256-frodokem-640-shaker2-sha256@openquantumsafe.org
- ecdh-nistp384-frodokem-976-shaker2-sha384@openquantumsafe.org
- ecdh-nistp521-frodokem-1344-shaker2-sha512@openquantumsafe.org
- ecdh-nistp256-kyber-512r3-sha256-d00@openquantumsafe.org
- ecdh-nistp384-kyber-768r3-sha384-d00@openquantumsafe.org
- ecdh-nistp521-kyber-1024r3-sha512-d00@openquantumsafe.org
- ecdh-nistp256-classic-mceliece-348864r4-sha256@openquantumsafe.org
- ecdh-nistp256-classic-mceliece-348864fr4-sha256@openquantumsafe.org
- ecdh-nistp384-classic-mceliece-460896r4-sha512@openquantumsafe.org
- ecdh-nistp384-classic-mceliece-460896fr4-sha512@openquantumsafe.org
- ecdh-nistp521-classic-mceliece-6688128r4-sha512@openquantumsafe.org
- ecdh-nistp521-classic-mceliece-6688128fr4-sha512@openquantumsafe.org
- ecdh-nistp521-classic-mceliece-6960119r4-sha512@openquantumsafe.org
- ecdh-nistp521-classic-mceliece-6960119fr4-sha512@openquantumsafe.org
- ecdh-nistp521-classic-mceliece-8192128r4-sha512@openquantumsafe.org
- ecdh-nistp521-classic-mceliece-8192128fr4-sha512@openquantumsafe.org
- ecdh-nistp256-hqc-128r3-sha256@openquantumsafe.org
- ecdh-nistp384-hqc-192r3-sha384@openquantumsafe.org
- ecdh-nistp521-hqc-256r3-sha512@openquantumsafe.org

Supported PQC algorithms for TLS Sign/Verify:

- mldsa44
- mldsa65
- mldsa87
- falcon512
- falcon1024

Supported PQC algorithms for TLS Key Encapsulation:

- mlkem512
- mlkem768
- mlkem1024

4.2.2.2 Support for SHA-384 and SHA-512

In FOS v10.0.0 support for SHA-384 and SHA-512 is added along with (existing) SHA-256. These hash types are supported with the commands `authutil` and `seccertmgmt`.

4.2.2.3 Extension

In FOS v10.0.0 IKEv2 used for IPsec is enhanced to support ML-KEM-768 and ML-DSA-65.

A new IPsec profile is available supporting both ML-KEM-768 and ML-DSA-65. This new profile is the post-quantum cryptography (PQC) profile. The existing legacy Shared Key profile (PSK) and Public Key Infrastructure profile (PKI) will continue to be supported. Supported IPsec profiles include:

- PSK security profile with no changes
- PKI security profile with no changes
- New post-quantum cryptography (PQC) profile with support for ML-KEM-768 and ML-DSA-65.

4.2.2.3.1 How it Works

The command `SecCertMgmt` functionality is enhanced to perform:

- Creation of CSR of the type mldsa65
- Creation of self-signed certificate of the type mldsa65

A new IPSec profile “PQC” with corresponding changes to CLI/REST to allow configuration of IPSec policy to use this new profile.

Enhancements include passing the entire certificate across the network for the verification process for PQC based certificates.

- IKEv2 is enhanced to exchange the full certificate with the peer.
- PKI based remote-switch certificates will still need to be imported through `secCertMgmt` (no changes).
- PQC Self-Signed remote-switch certificates will still need to be imported with `secCertMgmt` (no changes).
- PQC CA signed remote-switch certificates do not need to be imported with `secCertMgmt`.

4.2.2.4 Obsoletion of FTP, HTTP, Telnet, TLSv1.0, TLSv1.1, and Non-secure Syslog

In FOS v10.0.0 the following protocols are obsoleted:

- FTP
- HTTP
- Telnet
- TLSv1.0
- TLSv1.1
- Non-secure Syslog

4.2.2.5 Obsoletion of RADIUS and TACACS+

In FOS v10.0.0 the following AAA protocols are obsoleted:

- RADIUS
- TACACS+

4.2.2.6 Obsoletion of MD5, SHA1, and DSA

In FOS v10.0.0 the following algorithms are obsoleted:

- Removal of md5 from password hash
- Removal and blocking of usage/import/generate (CSR/cert) for certificates with type DSA, MD5 and SHA1
- Firmware blocking scenarios for obsoleted protocols and algorithms
- Removal and blocking of hmac-sha1and hmac-md5 SSH MAC
- Removal and blocking of kex SSH value diffie-hellman-group1-sha1
- Removal and blocking of SSH key value dsa
- Removal and blocking of md5 and hmac-sha1 for NTP keys
- Removal of sha1 and md5 for authentication hash `[authutil]`

Device and Fabric authentication.

- Removal of cipher support for md5
- Removal of md5, sha and noauth for SNMP
- Mixed CP behavior whereby the active CP release maintains that release’s support.
- Firmware migration for supported and blocking conditions.
- Operations using `factoryreset` will remove md5, sha,1 and dsa.

The following commands no longer support configuration of MD5(HMAC-MD5), SHA1(HMAC-SHA1) and DSA:

- `Authutil`
- `Passwdcfg`
- `Seccertmgmt`
- `Seccryptocfg`

- `Snmpconfig`
- `Sshutil`
- `Tsclockserver`

4.2.2.6.1 Upgrade Considerations

In case any of the command configurations in FOS v9.2.2x (listed below) make use of MD5(HMAC-MD5), SHA1(HMAC-SHA1) or DSA upon upgrade from FOS v9.2.2x to FOS v10.0.0 the upgrade is blocked. The user will be presented with an error message directing the user to change the configuration to no longer make use of the obsoleted protocols/algorithms.

- `Authutil`
- `Passwdcfg`
- `Seccertmgmt`
- `Seccryptocfg`
- `Snmpconfig`
- `Sshutil`
- `Tsclockserver`

NOTE The key lengths for the Network Time Protocol Daemon (NTPD) have changed and rekey may be necessary after upgrade from FOS v9.2.2x when longer keys have been in use. The supported key lengths in FOS v10.x are:

HMAC-SHA256 = Minimum 64, Maximum 128 characters

CMAC-AES-128 = 32 characters

The following is a list of the respective error messages:

Authutil: `The current FOS firmware version does not support hashing types SHA1/MD5. Use CLI "authutil --set -h sha256" on the switches connected in this fabric running with firmware lower than FOS v10.0 to reconfigure to SHA256 hashing. Ports configured with SHA1/MD5 may get disabled with older configurations on any port disruptions.`

DSA Key: `DSA is obsolete and not supported in target version. Please delete the DSA key using "sshutil delprivkey -dsa" command`

DSA Hostkey: `DSA is obsolete and not supported in target version. Please delete the DSA hostkey using "sshutil delhostkey -dsa" command`

Passwdcfg Hash: `MD5 is obsolete and not supported in target version. Please change the passwdcfg hashtype to "sha256" or "sha512" using "passwdcfg --hash {sha256|sha512} -manual" command`

Tsclockserver: `MD5 and SHA1 are obsolete and not supported in the target version. Please use "tsclockserver --showkeys" command to identify the MD5/SHA1 specific keys and delete these using "tsClockServer --delkey {-index <key_index>>}" command`

SSH Kex: SHA1 and MD5 are obsolete and not supported in target version. Please change ssh kex sha1 configuration using "seccryptocfg --apply -group SSH -attr Kex -value <value>" command

SSH Mac: MD5 and SHA1 are obsolete and not supported in target version. Please configure SSH mac other than MD5/SHA1 using "seccryptocfg --apply -group SSH -attr Mac -value <value>" command

HTTPS Cipher: MD5, SHA1 and DSA are obsolete and not supported in target version. Please reconfigure the HTTPS cipher to use a ciphersuite excluding MD5, DSA and SHA1 using "seccryptocfg --apply -group HTTPS -attr Ciphers -value <value>" command

LDAP Cipher: MD5, SHA1 and DSA are obsolete and not supported in target version. Please reconfigure the LDAP cipher to use a ciphersuite excluding MD5, DSA and SHA1 using "seccryptocfg --apply -group AAA -attr LDAP_Ciphers -value <value>" command

SYSLOG Cipher: MD5, SHA1 and DSA are obsolete and not supported in target version. Please reconfigure the SYSLOG cipher to use a ciphersuite excluding MD5, DSA and SHA1 using "seccryptocfg --apply -group LOG -attr Syslog_Ciphers -value <value>" command

FA Cipher: MD5, SHA1 and DSA are obsolete and not supported in target version. Please reconfigure the FA cipher to use a ciphersuite excluding MD5, DSA and SHA1 using "seccryptocfg --apply -group AAA -attr FA_Ciphers -value <value>" command

RSA Cipher: MD5, SHA1 and DSA are obsolete and not supported in target version. Please reconfigure the RSA to use a ciphersuite excluding MD5, DSA and SHA1 using "seccryptocfg --apply -group AAA -attr RSA_Ciphers -value <value>" command

SMTPS Cipher: MD5, SHA1 and DSA are obsolete and not supported in target version. Please reconfigure the SMTPS cipher to use a ciphersuite excluding MD5, DSA and SHA1 using "seccryptocfg --apply -group SMTPS -attr SMTPS_Ciphers -value <value>" command

4.2.2.7 System TLS

In FOS v10.0.0 TLS configuration is defined by a system wide policy (for ciphers and protocol) and by default applied to all usage of TLS.

System wide configurations can be configured using the command `seccryptocfg` as in the example below:

```
seccryptocfg --apply -group SYSTEM -attr SYSTEM_Ciphers -value
'ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!
TLSv1:!AESCCM'
```

For a specific application the system wide configuration (ciphers / protocol) can be overridden. This is done using the command `seccryptocfg` specifying the specific application. For example, to override system cipher configuration for LDAP, the following command could be used:

```
seccryptocfg --apply -group TLS -attr LDAP_Ciphers -value
'ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!
TLSv1:!AESCCM'
```

NOTE Application specific configuration present in FOS v9.2.2x prior to upgrade to FOS v10.0.0 will remain unchanged. Application of system level cryptography occurs only when application configuration keys are not present. System level configurations do not override application specific configurations.

In case of downgrade from FOS v10.0.0 to FOS v9.2.2x, ensure the per application ciphers are configured.

Since TLS versions less than TLSv1.2 are not supported in FOS v10.0.0 for `seccryptocfg` configurations, the value “`Any`” for TLS protocol version refers to TLSv1.2-TLSv1.3 (minimum version TLSv1.2 and maximum version TLSv1.3). The supported values for TLS protocol are “`TLSv1.2`”, “`TLSv1.3`” or “`Any`”.

Default values for SYSTEM group configuration are:

Protocol: “`Any`” (which refer to TLSv1.2-TLSv1.3)

Cipher:

```
"ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!
TLSv1:!AESCCM:!CBC:!kRSA:!DH"
```

Cipher TLSv1.3:

```
“TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_8_SHA256:TLS_AES_128_CCM_S
HA256”
```

4.2.2.8 Configuration Examples

Example of changing SYSTEM group protocol:

```
sw0:FID128:admin> seccryptocfg --apply -group SYSTEM -attr SYSTEM_Protocol -value TLSv1.2
Config change is Successful
```

Example of changing SYSTEM group cipher suite:

```
sw0:FID128:admin> seccryptocfg --apply -group SYSTEM -attr SYSTEM_Ciphers -value
'ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!
TLSv1:!AESCCM'
Config change is Successful
```

Example of changing SYSTEM group TLSv1.3 cipher suite:

```
sw0:FID128:admin> seccryptocfg --apply -group SYSTEM -attr SYSTEM_Ciphers_tlsv1.3 -value
'TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_8_SHA256:TLS_AES_128_CCM_S
HA256'
Config change is Successful
```

Example of changing an application protocol which is under TLS group:

```
sw0:FID128:admin> seccryptocfg --apply -group TLS -attr LDAP_Protocol -value TLSv1.3
Config change is Successful
```

Example of changing an application cipher suite which is under TLS group:

```
sw0:FID128:admin> seccryptocfg --apply -group TLS -attr LDAP_Ciphers -value
'ECDSA:ECDH:RSA:AES:!3DES:!RSAPSK:!DHEPSK:!PSK:!DSS:!ARIAGCM:!CAMELLIA:!CHACHA20:!SSLv3:!
TLSv1:!AESCCM'
Config change is Successful
```

Example of changing an application TLSv1.3 cipher suite which is under TLS group:

```
sw0:FID128:admin> seccryptocfg --apply -group TLS -attr FA_Ciphers_tlsv1.3 -value
'TLS_AES_256_GCM_SHA384:TLS_AES_128_GCM_SHA256:TLS_AES_128_CCM_8_SHA256:TLS_AES_128_CCM_S
HA256'
Config change is Successful
```

NOTE Templates from previous FOS releases are not supported and import operations will fail.

Example:

```
sw0:FID128:admin> seccryptocfg --import default_generic_mod -server <host> -
name <user> -proto scp -file <file>
Input template version is not supported with the current firmware version

Invalid Header
Template import failed
```

4.2.2.9 Principle of Least Privilege

FOS v10.0.0 is based on a Principle of Least Privilege (PoLP) architecture as in SELinux. This architecture follows the security concept of mandatory access control, where all modules run in a unique security context. All services and commands are granted only the minimum level of access necessary to perform their respective tasks.

All FOS services and commands run as non-root and there is no longer a root account in FOS (prior to FOS v10.0.0 the root account is disabled).

This architecture drastically decreases the attack surface of the operating system and potential impact of any security breaches without any impact on end user interaction with FOS.

4.2.2.10 Unified IP Filter

In FOS v10.0.0 the IP Filter function is enhanced with the capability of defining a Unified IP Filter policy covering both IPv4 and IPv6. While legacy IP Filter policies are supported in FOS v10.0.0, when creating an IP Filter policy in FOS v10.0.0, the default is a Unified IP Filter policy.

The unified IP Filter policies have additional functionality such as support for rules for both incoming and outgoing traffic. Legacy IP Filter policies only support rules for incoming traffic (to the switch management interface).

NOTE Legacy IP Filter policies will be obsoleted in a later FOS release, and users are encouraged to switch to use a Unified IP Filter policy in FOS v10.0.0.

4.2.2.11 Switching between Legacy and Unified IP Filter Policies

Legacy IP Filter and Unified IP Filter policies are mutually exclusive. If legacy IPv4/v6 IP Filter policies are active, activation of a Unified IP Filter policy will disable both v4 and v6 policies.

Similarly, if a Unified IP Filter policy is active, the activation of a legacy IP Filter v4 or v6 policy will disable the Unified IP Filter policy. In addition, it will wipe out v4 or v6 rules based on the policy that got activated, respectively. The user will be informed to modify the other policy while moving (activate) from unified to non-unified policies.

Similarly, when moving from a unified to a non-unified policy, user will be informed as follows: *Activating a legacy IP v4 Filter will disable the Unified IP Filter policy and wipe out any v6 rules *Activating a legacy IP v6 Filter will disable the Unified IP Filter policy and wipe out any v4 rules.

For example, if a legacy v4 IP Filter policy is activated while a Unified IP Filter policy is in active state, this would block IP v6 completely for both INPUT and OUTPUT. After the v4 IP Filter policy is up and running, the user will need to activate a v6 IP Filter policy.

4.2.2.11.1 Command Changes

The IP Filter command changes are highlighted below:

The `type` field is optional. If no type is given, the policy is defaulted to "`any`" and thereby a Unified IP Filter policy.

```
ipfilter --create <policyname>  [-type {ipv4 | ipv6}]
```

There is a new `type` field to specify ingress and egress rules. In addition, the source IP can be defined as an ipv4 address, ipv6 address, and "`any`".

```
ipfilter --addrule <policyname> -rule <rule_number> -type {INPUT | OUTPUT} -sip
<source_IP> -dp <dest_port> -proto {tcp | udp} -act {permit | deny} [-dip
<destination_IP>]
ipfilter --ephemeral <start_port> <end_port>
```

4.2.2.12 FOS System Anti-Tampering

FOS v10.0.0 is enhanced with extensive Anti-Tampering detection.
If detected the user is alerted to contact support.

4.2.3 MAPS

This section describes MAPS enhancements and changes in FOS v10.0.0.

4.2.3.1 Director Management Interface Monitoring

MAPS monitors the state change of the Ethernet management interface(s) on all platforms and alerts based on the rule configurations and actions.

Prior to FOS v10.0.0 only the active CP's Ethernet management port was monitored on Director platforms. In FOS v10.0.0 the functionality is enhanced to monitor the state changes of both the active and the standby CP's Ethernet Management ports from the active CP.

4.2.3.1.1 How it Works

MAPS monitors the state change of the Ethernet management port of the active CP through the monitoring system ETH_MGMT_PORT_STATE and group CHASSIS. The group CHASSIS allows management of only one chassis level resource.

Since the Ethernet Management interface is a resource applicable at blade level; new rules based on the group ALL_SLOTS are used to monitor the Ethernet interface present on the blades. The members of the group ALL_SLOTS are all the blades of the chassis system which includes the standby CP.

For consistent management across the directors and fixed formfactor switches, from FOS10.0.0 the group ALL_SLOTS will be supported on all platforms including fixed formfactor switches. This is being done to support the new rules listed in the table below, with the group ALL_SLOTS, across all platforms.

Logical group CLI output on a chassis switch:

```
logicalgroup --show
--------------------------------------------------------------------------------------
Group Name                      |Predefined |Type              |Member Count |Members
--------------------------------------------------------------------------------------
ALL_SLOTS                       |Yes        |Blade             |8            |1-8
CHASSIS                         |Yes        |                  |1            |0
```

Logical group CLI output on a fixed formfactor switch:

```
logicalgroup --show
--------------------------------------------------------------------------------------
Group Name                      |Predefined |Type              |Member Count |Members
--------------------------------------------------------------------------------------
ALL_SLOTS                       |Yes        |Blade             |1            |0
CHASSIS                         |Yes        |                  |1            |0
```

Affected default rules:

In FOS v10.0.0, two new default rules `defALL_SLOTSETH_MGMT_PORT_STATE_UP` and `defALL_SLOTSETH_MGMT_PORT_STATE_DOWN` have been introduced to monitor the state change of the management Ethernet ports on all the platforms.

On X7 platforms, the existing default rules `defCHASSISETH_MGMT_PORT_STATE_UP` and `defCHASSISETH_MGMT_PORT_STATE_DOWN` are still available in FOS v10.0.0 but the associations with the default policies has been removed and these rules are deprecated in FOS v10.0.0 and will be obsoleted in a future release.

The following table shows the affected default rules:

Rules	Conditions	Pre FOS v10.0.0	FOS v10.0.0	Status
defALL_SLOTSETH_MGMT_PORT_STATE_UP	ALL_SLOTS(ETH_MGMT_PORT_STATE/NONE==UP)	NA	dflt_always_active_policy	A new rule supported on both Gen 8 as well as on Gen 7 platforms.
defALL_SLOTSETH_MGMT_PORT_STATE_DOWN	ALL_SLOTS(ETH_MGMT_PORT_STATE/NONE==DOWN)	NA	dflt_always_active_policy	A new rule supported on both Gen 8 as well as on Gen 7 platforms.
defCHASSISETH_MGMT_PORT_STATE_UP	CHASSIS(ETH_MGMT_PORT_STATE/NONE==UP)	*MAPS policies	None	Deprecated for Gen 7 and not supported on Gen 8 platforms.
defCHASSISETH_MGMT_PORT_STATE_DOWN	CHASSIS(ETH_MGMT_PORT_STATE/NONE==DOWN)	*MAPS policies	None	Deprecated for Gen 7 and not supported on Gen 8 platforms.

*MAPS policies:

`dflt_moderate_policy, dflt_conservative_policy, dflt_aggressive_policy,dflt_base_policy`

4.2.3.2 Dynamic SFP Threshold Values

MAPS monitoring of SFP stats is enhanced to dynamically read the SFP thresholds from the SFP and alert the user based on the configured SFP thresholds.

Monitoring of SFP stats is supported under the group ALL_PORTS.

The group ALL_SFP is not supported on Gen 8 platforms.

Prior to FOS v10.x, each SFP had a dedicated logical group along with a predefined set of default rules to monitor parameters such as current, voltage, temperature, RXP, TXP.
With the latest enhancement, SFP stats monitoring has been improved to dynamically read the thresholds and hence reduce the need for specific default rules for each SFP and for each specific Vendor.

Below is an example of two default SFP monitoring rules:

- ➢ defALL_PORTSCURRENT_HIGH ALL_PORTS(CURRENT/NONE>=SFP_HIGH_ALARM_TH) SFP_MARGINAL,RASLOG,SNMP,EMAIL 0 qt=3600
- ➢ defALL_PORTSCURRENT_LOW ALL_PORTS(CURRENT/NONE<=SFP_LOW_ALARM_TH) SFP_MARGINAL,RASLOG,SNMP,EMAIL 0 qt=3600

(See the MAPS Default Rules documentation for a complete list of the default rules)

The new default rules to monitor SFP are added to the default MAPS policies:

- `dflt_aggressive_policy`
- `dflt_moderate_policy`
- `dflt_conservative_policy`

If any SFP threshold is exceeded a MAPS alert is generated for the SFP, including the SFP module serial number, part number and low/high threshold values.

Example:

```
2025/09/16-19:32:55 (GMT), [MAPS-1003], 3278, FID 128 | PORT 0/1, WARNING, SW-G720,
port1, E-Port 1, Condition=ALL_PORTS(CURRENT/NONE>=SFP_HIGH_ALARM_TH), Current
Value:[CURRENT, 12345 mAmps, (part_num: 57-1000495-01, serial_num: MAA12104C012645S,
high_th: 10, low_th: 2) ], RuleName=defALL_PORTSCURRENT_HIGH, Dashboard Category=Port
Health, Quiet Time=1 hour.
```

4.2.3.3 Extension Ethernet SFP Monitoring

MAPS is enhanced to monitor the Ethernet SFPs on extension platforms. This is a new feature introduced in the FOS v10.0.0 release. Existing MAPS monitors the following smart data of the FC SFPs:

a) Voltage

b) Current

c) Temperature

d) RXP

e) TXP

In line with FC SFP stats monitoring, instead of using statically defined threshold values in rule definitions, at run time MAPS will dynamically retrieve the GE SFP threshold values directly from the SFP module - values which were programmed by the SFP vendor.

All the SFP stats will be monitored with the “ALL_EXT_GE_PORTS” logical group.

The GE SFP monitoring is applicable only on Extension platforms.

MAPS monitors the above parameters of the Ethernet SFPs using below default rules:

```
   ●  defALL_EXT_GE_PORTSVOLTAGE_HIGH
ALL_EXT_GE_PORTS(VOLTAGE/NONE>=SFP_HIGH_ALARM_TH) SFP_MARGINAL,RASLOG,SNMP,EMAIL 0 qt=3600

   ●  defALL_EXT_GE_PORTSVOLTAGE_LOW   :
ALL_EXT_GE_PORTS(VOLTAGE/NONE<=SFP_LOW_ALARM_TH) SFP_MARGINAL,RASLOG,SNMP,EMAIL 0 qt=3600
```

The new default rules to monitor SFP are added to the default MAPS policies:

- dflt_aggressive_policy
- dflt_moderate_policy
- dflt_conservative_policy

```
> mapsrule --show defALL_EXT_GE_PORTSCURRENT_HIGH
Rule Data:
----------
RuleName: defALL_EXT_GE_PORTSCURRENT_HIGH
Condition: ALL_EXT_GE_PORTS(CURRENT/NONE>=SFP_HIGH_ALARM_TH)
Actions: SFP_MARGINAL,RASLOG,SNMP,EMAIL
Associated Policies: dflt_aggressive_policy, dflt_moderate_policy, dflt_conservative_policy
```

If any GE SFPs threshold is exceeded MAPS generates the alert about the SFP. Alert also contains information about SFP module Serial number, Part number and low/high threshold values.

Example of the VOLTAGE alert:

```
         [MAPS-1003], 133, FID 22 | PORT 0/GE17, WARNING, switch_22, GE Port ge17,
Condition=ALL_EXT_GE_PORTS(VOLTAGE/NONE>=SFP_HIGH_ALARM_TH), Current Value:[VOLTAGE, 4500
mVolts, (part_num: 57-1000508-01  , serial_num: YTA92412UA0000T, high_th: 3630, low_th:
2970) ], RuleName=defALL_EXT_GE_PORTSVOLTAGE_HIGH, Dashboard Category=Extension GE Port
Health, Quiet Time=None
```

The SFP monitoring is being monitored in the “Extension GE Port Health” dashboard category.

4.2.3.4 Making MAPS Easier to Manage

MAPS is enhanced with the following to simplify the management of MAPS features:

- System Policy(dflt_always_active_policy): Critical resource monitoring rules are part of the system policy.
- Enabled RASLOG, EMAIL, SNMP Actions: These actions are enabled for the system rules - predefined or custom.
- Group Augmentation: The feature is limited to the predefined port groups below:
  - ALL_HOST_PORTS
  - ALL_TARGET_PORTS
  - ALL_OTHER_F_PORTS

- Custom Group: The feature is limited to PORT group type.
- Pause/Restart: Functionality is limited to port and switch group types.
    - Support for SFP is being deprecated.
- Support for Logical Operators: The operators ‘<’, ‘<=’, and ‘==’ for performance monitoring systems are removed

4.2.3.4.1 System Policy

The MAPS system policy, known as the default, always active policy (dflt_always_active_policy), encompasses all the predefined rules for managing critical system resources. This system policy is always active and cannot be customized or deactivated. Enhancements are being made to incorporate existing critical monitoring rules into the system policy, along with the addition of new rules.

To view the system policy, use the following command:

```
mapspolicy --show dflt_always_active_policy
```

4.2.3.4.2 Enabled RASLOG, EMAIL and SNMP Actions

Prior to FOS v10.0.0, triggering a MAPS action, due to a rule violation, required that the action is configured both globally and within the specific MAPS rule.

Configuring global actions is done using the command:

```
mapsconfig --actions
```

In FOS v10.x, the following five actions are configured globally:

- SW_CRITICAL
- SW_MARGINAL
- SFP_MARGINAL
- FPIN
- HA_RECOVER

In FOS v10.0.0, RASLOG and SNMP actions are automatically enabled for all system rules (if the corresponding rule has RASLOG or SNMP action configured), even if they are not configured at the global level.

This change simplifies the user configuration process by eliminating an additional step enabling basic MAPS actions, RASLOG and SNMP across multiple LSs for system rules.

Below is an example of the default FOS v10.x configured global actions - note that actions such as RASLOG and EMAIL are not configured by default:

RASLOG action is not configured globally:

```
sw0:FID128:admin> mapsconfig --show
Configured Notifications:       SW_CRITICAL,SW_MARGINAL,SFP_MARGINAL,FPIN,HA_RECOVER
Mail Recipient:                 Not Configured
Mail From Address:              Not Configured
Raslog Mode:                    Default
Decom Action Config:            Impair (No Disable)
Global Quiet Time:              Not Configured
Notification Behavior:          Default
```

RASLOG action is present in the system rule:

```
sw0:FID128:admin> mapspolicy --show dflt_always_active_policy
Policy Name: dflt_always_active_policy

Rule Name                                                               |Condition                                          |Actions                    |
--------------------------------------------------------------------------------------------------------------------------------------------------------
defCHASSISMEMORY_USAGE_STATE_CRIT                                       |CHASSIS(MEMORY_USAGE_STATE/NONE==CRITICAL)         |RASLOG,SNMP,EMAIL,HA_RECOVE|
                                                                        |                                                   |R                          |
defCHASSISMEMORY_USAGE_STATE_WARN                                       |CHASSIS(MEMORY_USAGE_STATE/NONE==WARNING)          |RASLOG,SNMP,EMAIL          |
defCHASSISTRUFOS_CERT_DAYS_TO_EXPIRE_60                                 |CHASSIS(TRUFOS_CERT_DAYS_TO_EXPIRE/NONE<60)        |RASLOG,SNMP,EMAIL qt=7 day |
defCHASSISTRUFOS_CERT_EXPIRED                                           |CHASSIS(TRUFOS_CERT_EXPIRED/NONE==TRUE)            |RASLOG,SNMP,EMAIL qt=30 day|
                                                                        |                                                   |                           |
defCHASSISTRUFOS_CERT_INSTALLED                                         |CHASSIS(TRUFOS_CERT_INSTALLED/NONE==FALSE)         |RASLOG,SNMP,EMAIL qt=30 day|
```

If a user needs to modify the behavior of the system rules such as changing actions, users can create duplicate rules, and that configuration takes precedence over the system policy rule.

4.2.3.4.3 Group Augmentation

The Augmentation feature allows users to add or remove members from predefined logical port groups. Prior to FOS v10.0.0 this feature is supported for all port groups except for ALL_QUARANTINED_PORTS, ALL_FC_PORTS, and ALL_ETH_PORTS.

In FOS10.0.0, the Augmentation feature is only supported for the predefined groups:

- ALL_HOST_PORTS
- ALL_TARGET_PORTS
- ALL_OTHER_F_PORTS.

Example:

```
> logicalGroup --addmember ALL_F_PORTS -members 3
Cannot delete or modify the ALL_F_PORTS group

> logicalGroup --delmember ALL_HOST_PORTS -members 3
```

Consequently, MAPS will not allow augmentation for any other predefined groups. If a user has already augmented any predefined groups prior to upgrading to FOS v10.0.0, firmware migration will be blocked.

4.2.3.4.4 Custom Group Support for `PORT` Only

In FOS v10.0.0 support for the creation of custom groups for `SFP` and `CIRCUIT` members is obsoleted.

If the user has already created any custom groups (prior upgrading to FOS v10.x), then MAPS will block the firmware migration.

Example for the creation of new group:

```
sw0:FID128:admin> logicalGroup --create ckt_group_1 -type circuit -members 16/0
Option '-type' must have one of the pre-defined types.

Usage:
------

logicalGroup --create <groupName> -type <groupType> [{-feature <featureName> -pattern
<val>} | {-members <member-string>}]

Valid Values for type:   PORT
```

4.2.3.4.5 Pause/Restart

Pause/Restart is a MAPS functionality which is used to temporarily stop monitoring an object and is used during maintenance activity such as server upgrades.

Once an object is paused, rule violations on that object are not triggered. Supported group types prior to FOS v10.x are `Port, Switch, SFP` and `CIRCUIT`.

Starting from FOS v10.0.0, supported group types for the Pause/Restart features are:

- `Port`
- `Switch`

Pause/Restart feature for `SFP` and `CIRCUIT` group type is no longer supported.

Example:

```
sw0:FID128:admin> mapsconfig --config pause -type sfp -members 1
Option '-type' must have one of the pre-defined types.
Usage:
------

Values for group type:          PORT, SWITCH, ALL
----------------------
```

4.2.3.4.6 Logical Operators Obsoleted

Removal of the “<”, “<=”, and “==” logical operators support for performance monitoring.

In FOS v10.0.0 these operators are no longer supported for following monitoring systems:

- `RX`
- `TX`
- `UTIL`

Consequently, custom or default rules having the “<”, “<=”, and “==” logical operators to monitor the above monitoring systems will be obsolete.

4.2.3.4.7 System Temperature Monitoring

MAPS temperature monitoring for Gen 8 platforms is enhanced to have explicit monitoring for ambient temperature. With this enhancement, MAPS monitors the following:

1. Ambient temperature (Surrounding Data Center temperature)
2. System temperature

Ambient temperature monitoring is introduced in FOS10.x for Gen 8 platforms. This enhancement simplifies the MAPS temperature monitoring and provides the temperature of the system and the surrounding environment. It will assist customers in diagnosing issues more quickly, as detailed in the table below:

MAPS Temperature Alert		**Recommended action**
System	**Ambient**	
Yes	No	Collect the SS and contact the BSN technical support
Yes	Yes	Lower the Data Center temperature
No	Yes	Lower the Data Center temperature

4.2.3.4.8 Ambient Temperature

To monitor the ambient temperature, MAPS is being enhanced with the monitoring system:

- AMBIENT_TEMP

Using the AMBIENT_TEMP monitoring system, MAPS monitors the ambient temperature through the rules:

- `defCHASSISAMBIENT_TEMP_OUT_OF_RANGE CHASSIS(AMBIENT_TEMP/NONE==OUT_OF_RANGE)`
- `defCHASSISAMBIENT_TEMP_IN_RANGE CHASSIS(AMBIENT_TEMP/NONE==IN_RANGE)`

The above default rules are part of the system policy and if the OUT_OF_RANGE rule violation happens then the room temperature is above the operating range.
Example of the alert from `defCHASSISAMBIENT_TEMP_OUT_OF_RANGE rule:`

```
[MAPS-1003], 1097, SLOT 6 | FID 128, WARNING, mojito14, Chassis,
Condition=CHASSIS(AMBIENT_TEMP/NONE==OUT_OF_RANGE), Current Value:[AMBIENT_TEMP,
OUT_OF_RANGE], RuleName=defCHASSISAMBIENT_TEMP_OUT_OF_RANGE, Dashboard Category=Switch
Resource
```

MAPS has a current capability (Pre-FOS v10.0.0) to monitor system temperature using the following rules:

- `defCHASSISSYSTEM_TEMP_CRIT |CHASSIS(SYSTEM_TEMP/NONE==CRIT_OUT_OF_RANGE)`

- `defCHASSISSYSTEM_TEMP_MARG CHASSIS(SYSTEM_TEMP/NONE==MARG_OUT_OF_RANGE)`

The ambient temperature sensor is the only temperature value exposed to the end user on Gen 8 platforms -displayed using the existing `tempshow` command:

```
admin> tempshow
Sensor ID|Slot  |Sensor Index|State               |Centigrade  |Fahrenheit   |
------------------------------------------------------------------------------
1        |0     |0           |OK                  |25          |77           |
```

Additionally, rules to monitor individual temperature are not supported on Gen 8. As a result, ALL_TS group and rules associated with this group will not be supported on Gen 8 platforms.

4.2.3.4.9 No Default Base Policy on Gen 8 Platforms

Default Base policy (`dflt_base_policy`) was introduced in the earlier FOS releases which is a de facto MAPS policy enabled on the Brocade FOS switches in the absence of a Fabric Vision License.

On Gen 8 systems Fabric Vision is enabled by default which negates the necessity of having base policy on the switch. Hence, on Gen 8 systems the support for Base policy is being removed.

The functionality on Gen 7 systems remains intact with no change in behavior.

Please find the output of "**`mapspolicy --show -summary`**" on Gen 8 systems.

```
> mapspolicy --show -summary

        Policy Name                         Number of Rules

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

dflt_aggressive_policy            :               384

dflt_moderate_policy              :               388

dflt_conservative_policy          :               388

dflt_always_active_policy         :                 5
```

Functionality on Gen 7 systems are not impacted and the output of "**`mapspolicy --show -summary`**" on Gen 7 systems is given below.

```
> mapspolicy --show -summary

        Policy Name                         Number of Rules

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

dflt_aggressive_policy            :               398

dflt_moderate_policy              :               402

dflt_conservative_policy          :               402

dflt_base_policy                  :                44

dflt_always_active_policy         :                 5
```

4.2.3.4.10 Backend (BE) Ports Monitoring

Existing MAPS supports monitoring of the backend ports as part of the system policy.

4.2.3.4.11 Out of Range Latency Values

MAPS is implementing restrictions on the thresholds for flow monitoring to match the max values supported by the hardware. These values are orders of magnitude higher than any reasonable latency values in a production SAN. The thresholds for FRT and ECT as outlined below.

ASIC/Platform	ECT Max Bit	ECT Max Latency	FRT Max Bits	FRT Max Latency
Gen 7	23 bits	8.38 seconds	21 bits	2.09 seconds
Gen 8	24 bits	16.77 seconds	23 bits	8.38 seconds

4.2.3.4.12 Consistent RAS Log Domain ID Notation

The MAPS alerts related to flows can have SID/DID value as a five- or six-digits hexadecimal number. To maintain consistency, in FOS 10x all SID/DID hexadecimal numbers will be six digits in length.

In FOS v9x, when the domain id of the switch is in the range of 0x0 to 0xf, the SID and DID value are shown as five-digit hexadecimal numbers such as 0x23e00, whereas in FOS v10.x a leading zero will be added to the SID/DID which then becomes a six-digit hexadecimal number such as 0x023e00.

Example:

FOS v9.2.2x Flow alert

```
2024/10/09-09:49:11 (GMT), [MAPS-1003], 82640, FID 3, WARNING, vesper_3, Flow
(SID=0x23e00,DID=0x52800,Host Port=62),
Condition=sys_flow_monitor(WR_STATUS_TIME/10sec>=1), Current Value:[WR_STATUS_TIME, 907
Microseconds], RuleName=8fUEihYuLhBcXo, Dashboard Category=IO Latency, Quiet Time=1 day.
```

FOS v10.0.0 Flow alert

```
2024/10/09-10:31:00:145609 (GMT), [MAPS-1003], 715748/82686, FID 3, WARNING, vesper_3,
Flow (SID=0x023e00,DID=0x052800,Host Port=62),
Condition=sys_flow_monitor(WR_STATUS_TIME/10SEC>=1), Current Value:[WR_STATUS_TIME, 1073
Microseconds], RuleName=test_rule, Dashboard Category=IO Latency, Quiet Time=1 day.,
raslogAction.c, line: 238, comp:md1, ltime:2024/10/09-10:31:00:145537
```

4.2.3.5 MAPS Alert Truncation

Due to limitations of RASLOGs in FOS it is not possible to display the entirety of information in the RASLOG for certain names defined by the user with more than the maximum available characters.

4.2.3.5.1 Truncation of SMTP RelayConfig

The command `RelayConfig` is used for configuration of relay SMTP server for sending EMAILs for the configured recipient email address. The configuration involves “relay IP address” and the “domain name”. As per standards the maximum number of characters allowed for both relay IP and the domain name is 253.

If the user configures either of the below beyond 110 characters, the information will be truncated.

Example:

Configure relay IP address and domain name having more than 110 characters:

```
sw0:admin> relayConfig --config -rla_ip
fdkjkfkfslajfkldsjlkfjsdlkjflksdjlkfjdslkjfklsd.jdjflksjdlkfjsdlkjflksdjflksjlkfjsldkjflk
sdjflkabcd.fjdjj.fjdkjkdf.broadcom.com -rla_dname
zmreiucxrejhjwkemncmruiewjnclknlnfjlsdflkjslkjlksd.fjsofjosfslknfldskn.jfklsjflkjskljlksj
klsfjksabcd.riemcnklg.urieie.brocade.com
```

Relay IP and Domain Name are truncated in the MAPS-1017 RASLOG::

```
2025/03/19-10:20:37 (GMT), [MAPS-1017], 840, FID 128, INFO, goose86, MAPS relayConfig got
updated to relay_IP:
fdkjkfkfslajfkldsjlkfjsdlkjflksdjlkfjdslkjfklsd.jdjflksjdlkfjsdlkjflksdjflksjlkfjsldkjflk
sdjflkabcd.fjdjj.fjdk..., domain:
zmreiucxrejhjwkemncmruiewjnclknlnfjlsdflkjslkjlksd.fjsofjosfslknfldskn.jfklsjflkjskljlksj
klsfjksabcd.riemcnklg..., secure SMTP mode: Enabled.
```

Relay IP and Domain Name are not truncated in the output of "`relayConfig --show`" CLI output

```
sw0:admin> relayconfig --show
Relay Host:
fdkjkfkfslajfkldsjlkfjsdlkjflksdjlkfjdslkjfklsd.jdjflksjdlkfjsdlkjflksdjflksjlkfjsldkjflk
sdjflkabcd.fjdjj.fjdkjkdf.broadcom.com
Relay Domain Name:
zmreiucxrejhjwkemncmruiewjnclknlnfjlsdflkjslkjlksd.fjsofjosfslknfldskn.jfklsjflkjskljlksj
klsfjksabcd.riemcnklg.urieie.brocade.com
Secure SMTP:                    Enabled
```

4.2.3.5.2 Truncation of Port Name

The maximum length of port name in the MAPS rule alert RASLOGs has been truncated to a max of 32 characters.

Example:

```
2025/02/24-09:40:00 (GMT), [MAPS-1003], 924, FID 128 | PORT 0/1, WARNING, sw0,
abcdefghijklmakfdlsaf..., E-Port 1, Condition=ALL_PORTS(VOLTAGE/NONE>=SFP_HIGH_ALARM_TH),
Current Value:[VOLTAGE, 5200 mVolts, (part_num: 57-1000495-01, serial_num:
MAA12104C012645S, high_th: 3630, low_th: 2970) ], RuleName=defALL_PORTSVOLTAGE_HIGH,
Dashboard Category=Port Health, Quiet Time=1 hour.
```

4.2.4 Adaptive Traffic Optimizer

Traffic Optimizer, TO introduced in FOS v9.0.0 with Gen7 platforms provides a mechanism to proactively optimize SAN traffic by placing traffic with same characteristics into predefined Performance Groups, PGs and thereby VC allocations.

On Gen 7 platforms PGs are statically defined through profiles, either a system defined profile, or a user defined custom profile.

In FOS v10.0.0 TO is enhanced on Gen 8 platforms in the way that the PGs are determined automatically based on the actual characteristics of the traffic flows present in the fabric. When traffic characteristics in the fabric change the Performance Groups dynamically adapt to provide the optimal PG configuration for the individual fabric.

4.2.4.1 How Adaptive TO Works

The adaptive nature of TO on Gen 8 platforms is backwards compatible with Gen 7 switches and can learn the fabric performance attributes across all TO capable switches in the fabric including Gen 7 platforms. Based here on the optimal PG configuration and thereby allocation of VCs and buffers.

TO provides visibility in terms of device speeds, storage protocols present in the fabric and dynamically adapt to changing parameters optimally provisioning “Performance Groups” in an on-going manner.

This includes providing an optimal PG-set per LS in a chassis with multiple LSs having varying performance attributes, as well as Base fabric/FCR backbone support at PG class level so that end to end isolation can be guaranteed at the class level across the entire SAN.

This capability also provides seamless integration with IPS LS support where the performance parameters characteristics are different from the FC fabric.

QoS Zones, CSCTL, SDDQ and Oversubscription functionalities continue to be supported the same way as in Gen7 systems.

When a Gen 8 platform boots up for the first time, based on all the speed/protocol parameters supported in the Gen 8, an initial set of PGs are provisioned in the switch. The Gen 8 system supports 4 speeds (128G, 64G, 32G and 16G) accordingly the “default PG set” provisioned in a Gen 8 switch after initial bootup includes a PG group for each speed respectively SCSI and NVME a default PG as well as OS PG, SDDQ PGs and QoS PGs.

Learning then happens on all Gen 7 and Gen 8 platforms in the fabric followed by adaptation on the Gen 8 platforms. Gen 7 platforms continue to apply PGs based on the configured profile on the switches.

Once the initial adaption period is done up to 23 PGs can be created including 4 OS PGs plus (legacy) PGs for backwards compatibility.

Periodically an evaluation algorithm performs validation based on the ongoing TO learning mechanism and in case a more optimal PG allocation is valid the adaption is performed on the Gen 8 platforms altering the PG composition across the fabric.

4.2.4.2 TO Logging

New log messages are added to inform the user about the adaptive TO optimization status:

- **`TO-1021`** `Fabricwide migration to Optimal Performance Group Set has started.`
- **`TO-1022`** `Fabricwide migration to Optimal Performance Group Set has completed.`
- **`TO-1023`** `Retry for Fabric Wide Migration to the Optimal TO Performance Group Set is marked and Retry Count is %d.`
- **`TO-1024`** `Adaptive Traffic Optimizer has been disabled after reaching the maximum retry limit for fabric-wide migration.`
- **`TO-1025`** `Adaptive Traffic Optimizer has been disabled because switch is part of FCR enabled backbone fabric.`

4.2.4.3 TO on LD Links

By default, the long-distance link credit/buffer resource is configured with a minimal buffer allocation model, which ensures good performance when all flows on the long-distance links are non-impaired. In scenarios where both impaired and non-impaired active flows are present, the default configuration allocates resources to achieve nominal congestion resilience.

On Gen 8 platforms the user can further enhance the tolerance to congestion by reserving additional buffers on the long-distance link, using a new option with the command `portCfgLongDistance` the user can specify the number of buffers and the given distance. Based on the number of buffers allocated, the congestion resilience of the link is categorized as respectively **Nominal**, **Moderate**, or **High**.

To determine the number of required buffers to be allocated for each congestion resilience level, use the command **`portbuffercalc.`**

Command syntax:

```
portbuffercalc [<SlotNumber>/]<PortNumber> [-distance <distance>] [-speed <speed>] [-
framesize <framesize>] [-compression <compression>]
```

Example :

```
portbuffercalc 44 -distance 10 -compression disable

646 buffers required for 10km at 128G, framesize of 2048bytes and compression
disabled

Buffers required for congested environments:

646 buffers provide normal congestion resilience.
1286 buffers provide intermediate congestion resilience.
1926 buffers provide advanced congestion resilience.


portbuffercalc 44 -distance 10 -compression enable

1286 buffers required for 10km at 128G, framesize of 2048bytes and compression
enabled

Buffers required for congested environments:

1286 buffers provide normal congestion resilience.
2566 buffers provide intermediate congestion resilience.

3846 buffers provide advanced congestion resilience.
```

When configuring congestion resilience with the command **`portCfgLongDistance`** the users must provide the option `-distance` along with `-buffers` to get desired congestion resilience level.

When configuring congestion resilience with the command **portCfgLongDistance,** users must provide the options `-distance` and `-buffers` to in order to obtain the desired congestion resilience level. If the `-distance` option is not provided, the system provides 'normal congestion resilience' on the long distance link.

Users can also provide the optional `-framesize` argument in case the average frame size is different than the default frame size (2048 Bytes).

Examples:

- Nominal congestion tolerance

```
> portCfgLongDistance 44 LS 1 -buffers 646 -distance 10
Port is configured with normal congestion resilience capability.
Warning: port (44) may be reserving more credits depending on port speed.
```

- Moderate congestion tolerance

```
> portCfgLongDistance 44 LS 1 -buffers 1286 -distance 10
Port is configured with intermediate congestion resilience capability.
Warning: port (44) may be reserving more credits depending on port speed.
```

- High congestion tolerance

```
> portCfgLongDistance 44 LS 1 -buffers 1926 -distance 10
Port is configured with advanced congestion resilience capability.
Warning: port (44) may be reserving more credits depending on port speed.
```

NOTE Congestion Resilience is only supported on LD links between Gen 8 platforms. If configured on LD link between Gen 8 and Gen 7 the buffer allocation will default to the same as Gen 7 to Gen 7.

4.2.5 Fabric Services

This section describes changes related to Fabric Services.

4.2.5.1 DefZone NoAccess Default Setting

The legacy default `DefZone` mode has previously been `AllAccess`.

Due to potential end-device connectivity issues related to RSCN storms when `DefZone` is configured to `AllAccess`, in FOS v10.x the default `DefZone` mode has been changed to `NoAccess` to encourage customers to use actual zoning configurations in their environment.

The default `DefZone` Mode is set to `NoAccess` in the following scenarios:

○ Logical Switch Creation:

Upon creating a new Logical Switch, the default `DefZone` Mode is set to `NoAccess` upon creation.

○ ‘`firmwarecleaninstall`’

○ ‘`factoryreset`’

○ After ‘`configremoveall`’ when the remove zone option is set to ‘`y`’:

```
Remove zone/AD database (no recovery) for fid 128: (yes, y, no, n): [no] y
```

The DefZone merge scenarios are modified by this setting change and will result in the following (see the highlighted cases for change-in-behavior cases):

#	Sw 1		Sw 2		Current Merge Behavior	New Merge Behavior (FOS v10.x)
	DefZone Mode	Configuration	DefZone Mode	Effective Cfg		
1	AllAccess	Def: None Eff: None	NoAccess	Def: None Eff: None	Zone Conflict	Zone Conflict
2	AllAccess	Def: Exist Eff: None	NoAccess	Def: Exist Eff: None	Fabric is formed, NoAccess is merged from Sw2 to Sw1	**Zone Conflict, If a 10.0.0+ switch is the Merge Init or Resp, it will segment the E-Port**
3	AllAccess	Def: None Eff: None	NoAccess	Def: Exist Eff: None	Fabric is formed, NoAccess is merged from Sw2 to Sw1	**Zone Conflict, If a 10.0.0+ switch is the Merge Init or Resp, it will segment the E-Port**
4	NoAccess	Def: None Eff: None	AllAccess	Def: Exist Eff: None	Fabric is formed, NoAccess is merged from Sw1 to Sw2	**Zone Conflict, If a 10.0.0+ switch is the Merge Init or Resp, it will segment the E-Port**
5	NoAccess	Def: None Eff: None	NoAccess	Def: Exist Eff: Yes	Fabric is formed	Fabric is formed
6	AllAccess	Def: None Eff: None	AllAccess	Def: Exist Eff: Yes	Fabric is formed	Fabric is formed
7	NoAccess	Def: None Eff: None	AllAccess	Def: Exist Eff: Yes	Zone conflict	Zone conflict

8	AllAccess	Def: None Eff: None	NoAccess	Def: Exist Eff: Yes	Fabric is formed, NoAccess is merged from Sw2 to Sw1. The Effective Cfg from Sw2 will be merged to Sw1. Defzone NoAccess will not get enabled in this particular case.	Fabric is formed, NoAccess is merged from Sw2 to Sw1. The Effective Cfg from Sw2 will be merged to Sw1. Defzone NoAccess will not get enabled in this particular case.

NOTE The ‘`configdefault’` operation does not affect zoning and therefore will not be affected by this feature. Customers are encouraged to configure ‘noaccess’ in fabrics consisting of FOS v9.x switches prior to adding FOS v10.x switches to the fabric.

4.2.5.2 FDMI Duplicate

FOS v10.0.0 is enhanced to notify the user when a valid duplicate HBA is detected.

FDMI already handles duplicate HBA entries but there was no indication to the user when a valid duplicate was removed. With this enhancement, a new RASLog FDMI-1001 will be added to notify the user when a valid duplicate HBA is detected and removed from the local FDMI database.

RASLog format:

```
[FDMI-1001]: Removed duplicate HBA ID %s registered on Port %d.
```

4.2.5.3 Nodefind Command

The command `nodefind` is enhanced in FOS v10.0.0. Consequently, executing `nodefind` without options is deprecated.

Old style Usage: (deprecated, still supported in FOS v10.0.0)

```
  nodefind {<wwn>|<pid>|<alias>}
```

New Usage: (supported in FOS v10.0.0 and later)

Usage:

```
  nodefind {-pid <pid> | -pwwn <wwn> | -nwwn <wwn> | -ali <alias> | --help}
```

4.2.6 FOS Infrastructure

This section describes FOS infrastructure changes which apply to end user interaction with FOS.

4.2.6.1 Checksum Verification for configDownload

In FOS v10.0.0 a checksum is added to the file when performing `configUpload`. The purpose of this enhancement is for customer environments which mandate that with restore of any infrastructure configuration backup it must be possible to verify that the backup has not been altered.

Upon usage of `configDownload` to replace/restore the configuration on the switch the user can decide to validate the checksum or perform the download without validation.

4.2.6.1.1 How it Works

Checksum is calculated and added with the uploaded configuration file `configUpload` and is verified while doing `configdownload`.

If the checksum embedded with the configuration file is not matched, with file checksum it indicates that the file has been modified.

If the user specifies integrity check during `configDownload`, the download operation will be blocked.

If the user has not specified integrity check, mismatch will be logged internally, but the `configDownload` will be allowed to continue.

NOTE If someone modifies any configuration <key.value> pair in the configuration file and recalculates the hash and and adds the recalculated hash as footer.chcksum, FOS will not have a way to identify the modification as the hash is present in the file itself.

4.2.6.2 Duplicate Address Detection (DAD)

FOS v10.0.0 is enhanced with Duplicate IP Address Detection. When a management IP address is being configured using the CLI or REST, there will be a check to see if the address is already configured in the subnet before proceeding to configure the address on the interface.
If the duplicate address is detected during configuration, then an error message will be displayed to the user and configuration will fail.
Duplicate address detection will also be performed after reboot and a RASLOG will be generated if a duplicate address is detected but the address will continue to be configured and used on the interface.
In such a scenario it is the responsibility of the user and network administrator to configure a different IP address.

4.2.6.3 Management Interface Speed Configuration on Gen 8

The management interface speed configurations supported on the Gen 8 platforms are 1/10G speeds with Auto negotiation ON by default and neither setting are user configurable.

4.2.6.4 USB Drive Support

While FOS switches support open USB drives, it is recommended to use validated USB drives only. The following USB drives are validated in FOS v10.0.0.

- Kingston 32GB DataTraveler 100 G3 USB 3.0 Flash Drive (DT100G3/32GB)
- Kingston 32GB USB3.2 Gen 1 DataTraveler Exodia (DTX/32GB)
- PNY Attache 3.0 4 USB 64GB Flash Drive

- PNY Attache 3.0 4 USB 32GB Flash Drive
- SanDisk Ultra 64GB USB 3.0 Flash Drive (SDCZ48-064G-A46)
- SanDisk 32 CZ48 USB 3.0 Flash Drive (SDCZ48-032G-UAM46)

4.2.7 Unified Storage Fabric (USF)

This section describes USF enhancements in FOS v10.0.0.

NOTE In FOS v10.0.0 USF is only supported for X7-8 and X7-4.
USF is not supported on X8-8 and X8-4 in the initial release of FOS v10.x.

4.2.7.1 Flow Vision Support for IP Storage Traffic

In FOS v10.0.0 Flow Vision is enhanced to support visibility to IP Storage flows

4.2.7.2 Scale Changes

The USF scale changes are highlighted below in the context of all scale parameters.

Chassis – Each Director chassis can have only one IPS logical switch.

IPS Logical Switch – Each IPS logical switch supports the following maximum number of ports based on the platform:

- 192 Ethernet ports (8-slot)
- 96 Ethernet ports (4-slot)
- 48 LAGs

IPS Logical Fabric – Each IPS logical fabric supports the following maximums:

- 8 Domains
- 800 Ethernet ports
- **2000 IP devices**
    - Any combination of directly attached IP devices, IP devices connected through L3 ToR, or IP devices connected through L2 ToR is allowed as long as the total sum of all the IP addresses is less than or equal to 2000.
    - Calculation examples:
        - A storage device directly connected through a single ethernet port with one IP address assigned counts as "1 IP device" and "1 ethernet port"
        - A storage device directly connected through a LAG with 8 ethernet ports with one IP address assigned counts as "1 IP device" and "8 ethernet ports"
        - L3 connected through a LAG of 8 ethernet ports with one next hop IP address assigned (with 100 host IP addresses behind it) counts as "100+1 IP devices" and "8 ethernet ports"
        - L2 connected through a LAG of 16 ethernet ports (with 100 host IP addresses behind it) counts as "100 IP devices" and "16 ethernet ports"
- 4 VRF IDs
- 256 VLANs
    - 16 VLANs per interface
        - A port or a LAG is considered an interface
    - 256 interfaces per VLAN
- 512 Static routes

- **64 User IP ACLs (new feature in FOS v10.0.0)**
- iSNS
  - 300 iSNS devices
  - 10 DDsets
  - 50 DDs

4.2.7.2.1 Scale Up Setting

Newly created IPS LS in FOS v10.0.0 per default support higher scale regardless of platform.

To support higher scale for IPS LS upgraded from FOS v9.2x to FOS v10.0.0 it is necessary for the user to execute the scale-up command which is applied non-disruptively across the fabric. This feature is only available on IPS LS.

Command syntax:

```
ipsCfgScale --upgrade
```

```
ipsCfgScale --show
```

4.2.7.3 IPS Replication over LD Links

In FOS v9.2x, Long Distance (LD) DISLs were not supported in an IPS LS.

In FOS v10.0.0 the configuration and use of LD ISLs in an IPS LS is supported with no additional restrictions. Since both distance ports and IPS ports require extra buffers, it is recommended to spread them out across multiple ASICS if possible.

Configuring AnyIO ports on an ASIC will be prevented if the minimum required buffers are not available. After configuration it is possible in some cases for all buffers to be used and for Ethernet port congestion to back up to ingress.

LD ISLs can be configured and can be configured to operate inin buffer limited mode when required buffers are not available. This behavior is unchanged for IPS logical switches.

4.2.7.3.1 Buffer Considerations and Behavior

Gen 7 platform buffer reservation behavior:

- When configuring AnyIO ports, the needed backend and frontend buffers are checked before succeeding.
  - The first AnyIO ports configured on an asic require 4104 (171 on each link) backend buffers to be reserved.
  - Each AnyIO port requires additional frontend buffers based on speed.
  - `portbuffershow` reflects the reserved buffers in “Remaining Buffers”
  - Each configured AnyIO port should show 100 or 250 under Max/Resv Buffers for 10G and 25G respectively.
  - If the necessary buffers are not available, the `portcfgAnyIO ports` command will fail with the error message “**Error: Not enough buffers to configure port SS/PP.**”
- LD ISL configuration is disallowed in most cases when not enough buffers are available.
  - The `portcfglongdistance` command will fail with the error message **“Failed: already exceeds Buffer credits allowed.”**
  - In the case of LD with QOS, more buffers would potentially be needed at link up time.
    - If an LD ISL with QOS comes online and there are not enough buffers, raslog C5-1032 will be issued, and the port will be shown as “Buffer Limited” in `switchshow`.

    -
      ```
      2025/01/28-00:22:10:873293 (GMT), [C5-1032], 38993/15127, CHASSIS |
      PORT 0/51, WARNING, G720, S0,P51(75): Required buffer unavailable for
      the port. req_buf:10006 port_buf:28 unused_buf:7698 est_buf:28.,
      OID:0x4302880b, SPOID:0x43068133, c6_buf.c, line: 5372, comp:insmod,
      ltime:2025/01/28-00:22:10:873187.
      ```

Gen 8 buffer reservation behavior:

- When configuring AnyIO ports, the needed buffers are checked before succeeding.
    - The first AnyIO ports configured on an asic require 2100 backend buffers to be reserved from the general asic pool.
    - Gen 8 AnyIO ports do not require additional front-end buffers.
    - `portbuffershow` reflects the reserved buffers in “Remaining Buffers”
    - Each configured AnyIO port should show the standard 32 under Max/Resv Buffers.
    - If the necessary buffers are not available, the portcfgAnyIO ports command will fail with the error message “**Error: Not enough buffers to configure port SS/PP.**”
- LD ISL configuration and bring up follows the same rules as Gen 7.
    - The C5-1032 RASLOG becomes a C6-1032 with Gen 8.

4.2.7.4 IPS ACL

In FOS v10.0.0 USF is enhanced to support subnet ACLs. The ACL support is implemented as part of the existing “`trafclass`” CLI with a new type of membership for the option `memberAdd/memberRemove`. This introduced membership type is only applicable for “`sysTcAclDeny`” Traffic class.

For user defined traffic class, there is no change to the existing supported membership type for the option `memberAdd/memberRemove`.

The new membership type is applicable for “`sysTcAclDeny`” traffic class will be VRF and IP subnet pairs.

Syntax and example:

```
trafClass --memberAdd sysTcAclDeny [-vrfID <vrf-id>] -ipSubnet <ip Subnet> -peerIpSubnets
<ip Subnet>[[,<ip Subnet>]...]
trafClass --memberRemove sysTcAclDeny [-vrfID <vrf-id>] -ipSubnet <ip Subnet> -
peerIpSubnets <ip Subnet>[[,<ip Subnet>]...]
trafClass --aclShow [-vrfID <vrf-id>]


trafclass –aclShow

trafficClassName   : sysTcAclDeny
vrfID              : 10
ipSubnet           : 10.10.10.1/24
peerIpSubnet       : 20.20.20.1/24
aclAccessMode      : deny
packetCount        : 120

trafficClassName   : sysTcAclDeny
vrfID              : 10
ipSubnet           : 10.10.10.1/24
peerIpSubnet       : 30.30.30.1/24
aclAccessMode      : deny
packetCount        : 150

trafficClassName   : sysTcAclDeny
vrfID              : 20
ipSubnet           : 30.30.30.1/24
peerIpSubnet       : 50.50.50.1/24
aclAccessMode      : deny
packetCount        : 50
```

4.2.7.5 Jumbo Frame Support

The Gen 7 MTU continues to be set to 2088 and is not configurable.

4.2.7.5.1 IPSPING

The command `ipsPing` is enhanced to support payload size of 9064.

```
ipsPing <ipaddress> [-vrfID <vrfID>] [-sourceGateway <ipaddress>] [-size <supported size
value(18-9188)>] [-count <count(1-200)>]
```

4.2.7.6 IPS Ethernet Port Statistics

IPS is enhanced in FOS v10.0.0 to provide Ethernet port statistics for frames dropped.

These are available with the command `ipsPortStats`

Command syntax:

```
  ipsPortStats --clear [<SlotNumber>/]<PortNumber>
  ipsPortStats --clearAll


  ipsPortStats --show [-interface [<SlotNumber>/]<PortNumber>]
```

4.2.8 Miscellaneous

This section describes miscellaneous enhancements in FOS v10.0.0

4.2.8.1 ICL Changes on Gen 8 Platforms

With the introduction of the ICL blades on the Gen 8 platforms the `switchshow` command is changed to display the OSFP cage on the ICL blade relation to the port connection on the core blades.

Example:

```
Sw_X8:FID128:admin> switchshow
======Truncated===============
Index Slot Port  ICL Slot/Cage/Channel Address Media  Speed        State    Proto
==========================================================================
 768    13    0       5/0/0    ------   id    106G      No_Light    FC
 769    13    1       5/0/1    ------   id    106G      No_Light    FC
 770    13    2       5/0/2    ------   id    106G      No_Light    FC
 771    13    3       5/0/3    ------   id    106G      No_Light    FC
 772    13    4       6/0/0    ------   id    106G      No_Light    FC
 773    13    5       6/0/1    ------   id    106G      No_Light    FC
 774    13    6       6/0/2    ------   id    106G      No_Light    FC
 775    13    7       6/0/3    ------   id    106G      No_Light    FC
 776    13    8       5/1/0    ------   id    106G      No_Light    FC
 777    13    9       5/1/1    ------   id    106G      No_Light    FC
 778    13   10       5/1/2    ------   id    106G      No_Light    FC
 779    13   11       5/1/3    ------   id    106G      No_Light    FC
 780    13   12       6/1/0    ------   id    106G      No_Light    FC
 781    13   13       6/1/1    ------   id    106G      No_Light    FC
 782    13   14       6/1/2    ------   id    106G      No_Light    FC
 783    13   15       6/1/3    ------   id    106G      No_Light    FC
======Truncated===============
```

4.2.8.2 Flow Vision

Support for Gen 8 platforms is included in FOS v10.0.0 without changes to scale.

4.2.8.3 FICON

Support for Gen 8 platforms is included in FOS v10.0.0 without changes to scale.

4.2.8.4 PortName Enhancement

A new PortName option is added to the commands `ficoncupshow` and `ficoncupset` to set the PortName based on the port addresses and can be executed (only) when FICON Management Server (FMS) mode is enabled.

4.2.8.5 FEC Mode for 128G FC

The Gen 8 platforms running 128G FC speed are per default configured with dual FEC.

This is applicable only for ports configured to 128G FC.

4.2.8.6 OSFP Ports

In the Gen 8 chassis, the ICL blade is introduced with the new type of SFP called OSFP. OSFP is a pluggable optic similar to the QSFP in Gen 7 core blades used to connect ICL ports, but it holds 8 lanes(ports) in a single cage whereas QSFP holds 4 lanes(ports).

For OSFPs in FOS v10.0.0 it is required that all 8 ports must run the same speed and be part of the same logical switch. It is not allowed to set port speeds individually on each port on the OSFP as well as split the OSFP among multiple logical switches.

4.2.8.7 Port Decommission

The command `portDecom -qsfp` is allowed on the Gen 8 chassis systems for OSFP-QSFP ICL links that are configured for 53G speed. This is supported on the Gen 8 side of the ICL links to mirror how it works from the Gen 7 side.

All the existing `portDecom` restrictions still apply on Gen 8 ICLs.

If `portDecom -qsfp` is executed for a port that is from an OSFP, but is not configured for 53G, the following error message is shown:

```
Error: The -qsfp option is supported for 53G ICL connectivity to Gen7 QSFPs
```

4.2.8.8 Fabricshow

In FOS v10.0.0 the `fabricshow` command output is modified since IPFC is obsoleted and consequently does not display the IPFC address column (highlighted below).

Prior to FOS v10.x:

```
Sw0:admin> fabricshow
Switch ID   Worldwide Name           Enet IP Addr     FC IP Addr      Name
-----------------------------------------------------------------------------------------
-------
  2: fffc02 10:00:c4:f5:7c:01:9c:78  10.155.110.82    0.0.0.0         "sw0"
194: fffcc2 10:00:38:ba:b0:39:e9:40  10.155.110.194   0.0.0.0         >"SWG720"

The Fabric has 2 switches
Fabric Name: EFS
```

In FOS v10.x:

```
Sw0:admin > fabricshow
Switch ID      Worldwide Name            Enet IP Addr    Name
---------------------------------------------------------------------------------
   2: fffc02   10:00:c4:f5:7c:01:9c:78   10.155.110.82   >"sw0"
194: fffcc2    10:00:38:ba:b0:39:e9:40   10.155.110.194   "SWG720"

The Fabric has 2 switches
Fabric Name: EFS
```

4.2.8.9 Fabric State

In FOS v10.x two new RASLOG messages are added to notify users about the Fabric State.

The Fabric and FSPF services in every switch, independently discover the other switches in the fabric. The Fabric service in the principal switch, allocates unique domain IDs to all the subordinate switches in the fabric and it reconfigures the fabric to reassign the domain IDs every time a new switch is connected to the fabric, or an existing switch is disconnected from the fabric.

The FSPF service finds routes to all the switches in the fabric and determines if the switches are reachable or not. It also recalculates the routes to the other switches in the fabric, if there is any change in the fabric topology.

The fabric state conditions are extensively used to throttle various operations within the switch, both internal and external. Several services register for the fabric state SCNs and start their operations only when the fabric is synchronized. Similarly, several CLIs check for fabric state condition and do not function when the fabric is synchronizing, and they respond to the user to retry the command when the fabric becomes synchronized.

In FOS v10.x the below two Raslog messages are added to notify the user about the current state of the fabric.

1. **FABR-1070: Fabric is Synchronizing**
   - **Message Example:**
     `2024/12/16-06:20:55 (GMT), [FABR-1070], 74858, FID 128, INFO, SWG720, Fabric is synchronizing.`
   - **Description:**
     This RASLOG notifies the user that the fabric state is synchronizing and is undergoing a reconfiguration process due to a disruptive operation.
2. **FABR-1069: Fabric is Synchronized**
   - **Message Example:**
     `2024/12/16-06:21:06 (GMT), [FABR-1069], 74861, FID 128, INFO, SWG720, Fabric is synchronized.`
   - **Description:**
     This RASLOG confirms that the fabric reconfiguration process has been successfully completed, and the fabric has returned to a synchronized state.

4.2.8.10 Disabling Web Tools in FOS

Web Tools allows users to monitor and manage switches, ports, and fabrics. It is installed on the switch by default and can be launched from a browser or the SANnav Management Portal.

In FOS, by default Web Tools is enabled. In FOS v10.x the user can enable/disable Web Tools using the command `mgmtapp` (or REST URI). After disabling Web Tools, if the user tries to launch it from the browser or/ SANnav the following error message will be displayed: “Web Tools interface is disabled in Fabric OS.”

When disabled all existing Web Tools sessions are terminated.

Command syntax:

Enable the Web Tools

```
mgmtapp --enable webtools
```

Disable the Web Tools

```
mgmtapp --disable webtools
```

Verify the current status

```
mgmtapp ––show
```

4.2.8.11 Supportlink Troubleshooting Without ICMP

The Supportlink troubleshooting option is used to diagnose common network connectivity problems.
BSL troubleshooting uses ICMP ping as one option for diagnosing network connectivity.
In some customer environments, ICMP traffic is blocked due to security concerns. Consequently, using ICMP ping can incorrectly show a connectivity failure, even when the network is functioning properly. To avoid the false positive condition, a new sub-option `'noping'` is added to the `supportlink` troubleshooting options.
By default, the ICMP ping option is used to diagnose the network. When the user specifies the `'noping'` option, the ICMP ping will be skipped, and the remaining diagnostic options will be executed.

Syntax:

```
Supportlink –troubleshoot -noping
```

4.2.8.12 LED Behavior for G-Port

The LED typically reflects the physical link status and activity, but it doesn't natively distinguish between a physical link up and a protocol issue (stuck at G-Port state). To indicate the failure, there is a modification in the LED behavior for Gen 8 platforms.

To distinguish between physical link up and a protocol issue, LED behavior has been modified on Gen 8 platforms:

- If a port is stuck in the G-port state, then the LED will show a Slow Green.
- For an active/online port, LED will display a Steady Green.

4.2.9 Web Tools

Web Tools is enhanced to support Gen 8 platforms in FOS v10.x as well as the additional enhancements.

4.2.9.1 HTTPS Support Only

FOS v10.x does not support connections using non secure protocols such as FTP and HTTP protocol. Attempting to launch Web Tools from a browser without specifying HTTPS protocol will fail to connect to the switch.

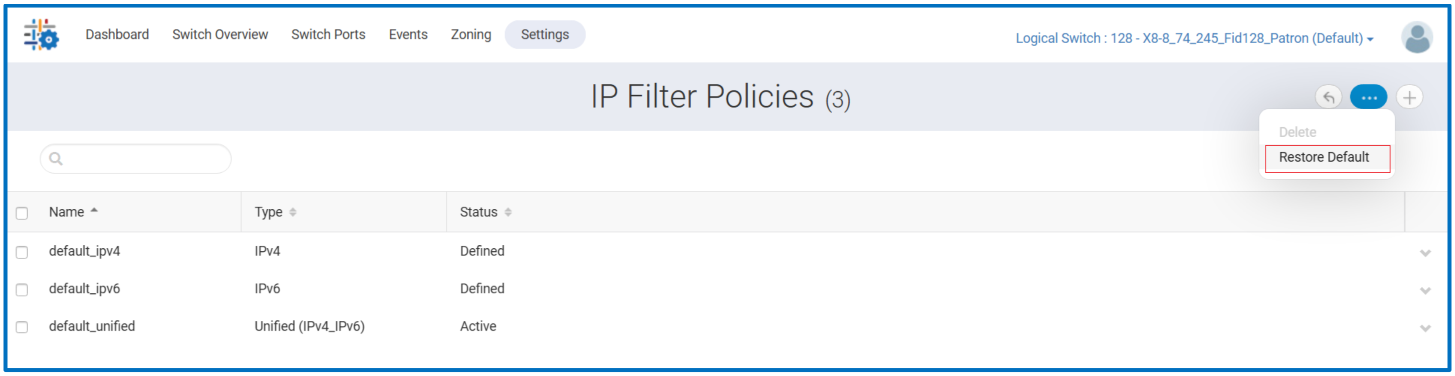
Accordingly, Web Tools pages will no longer allow specifying HTTP and port 80 as well as FTP (for Firmware download and Config backup).

4.2.9.2 IP Filter Restore

In FOS v10.x a new option is introduced for restoring the default IP Filter configuration from the Web Tools IP Filter Management view.

IP Filter Management:

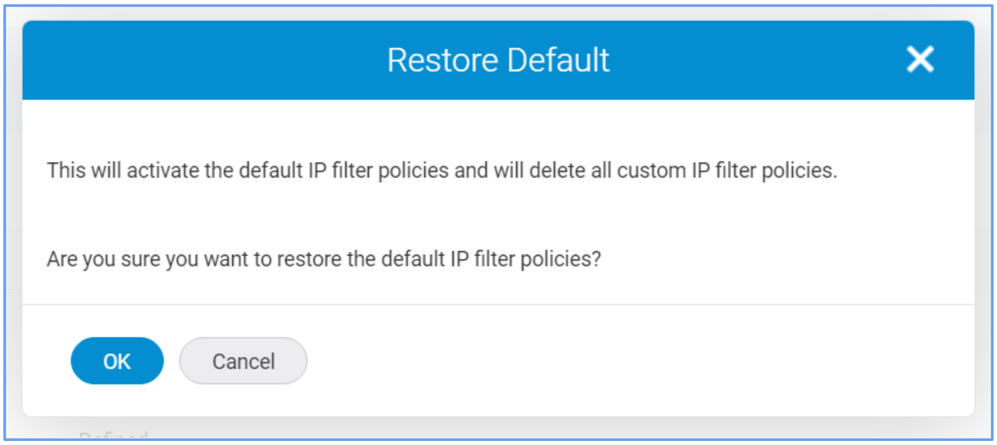
- Login to Web Tools
- Navigate to Settings -> Security Policies -> IP Filter Management



IP Filter Policies (3)

Name	Type	Status
default_ipv4	IPv4	Defined
default_ipv6	IPv6	Defined
default_unified	Unified (IPv4_IPv6)	Active

When choosing the option, a warning modal will be shown to the user to confirm the operation. After confirming, the default IP Filter configuration will be restored to default, and the corresponding policies will be listed on the IP Filter Management list view.

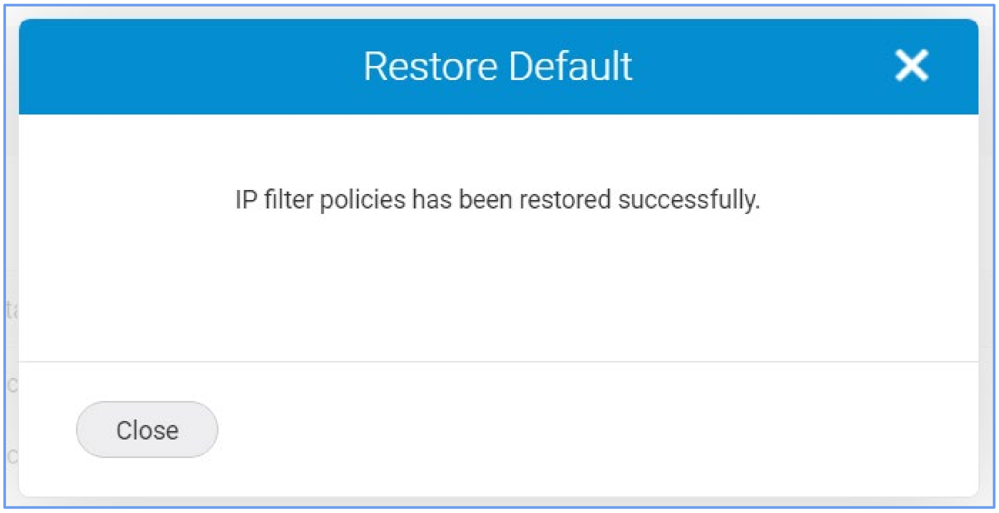


Restore Default

This will activate the default IP filter policies and will delete all custom IP filter policies.

Are you sure you want to restore the default IP filter policies?

The popup below will be shown when the IP Filter policy is restored without any error.



Restore Default

IP filter policies has been restored successfully.

Error modal will be shown if there is any error occurred during the restore process.

4.2.9.3 Unified IP Filter

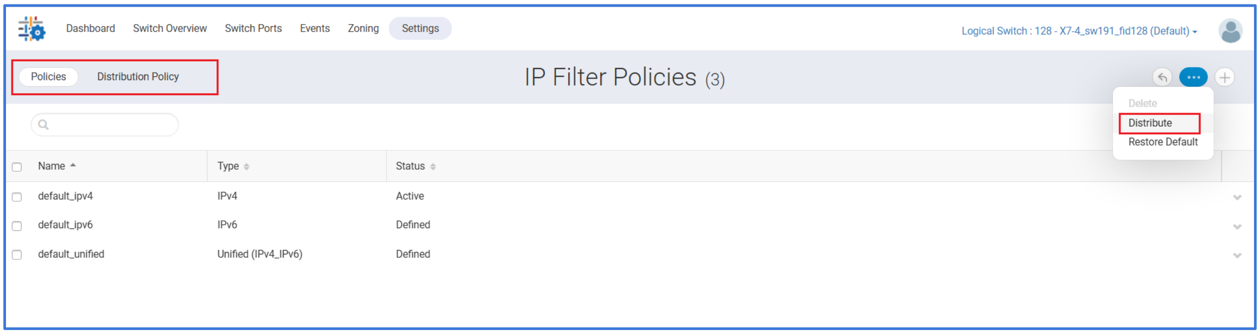
In FOS v10.0.0 IP Filter is enhanced to support Unified IP Filter policies as well as legacy IP Filter policies.

Accordingly, Web Tools supports creating a unified IP Filter policy.

In addition, IP Filter distribution support from IP Filter policy page in Web Tools is obsoleted.

IP Filter Policies:

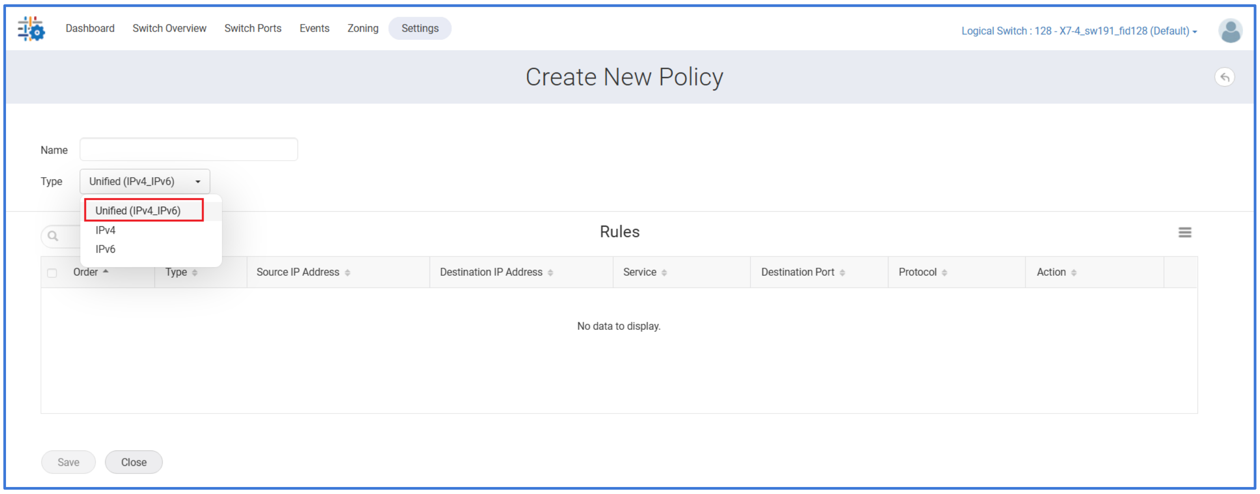
- Login to Web Tools
- Navigate to Settings -> Security Policies -> IP Filter Management.



IP Filter Policies (3)

Name	Type	Status
default_ipv4	IPv4	Active
default_ipv6	IPv6	Defined
default_unified	Unified (IPv4_IPv6)	Defined

In FOS v10.0.0, the Distribution and Distribution Policy option have been removed from the IP Filters list view.



Create New Policy

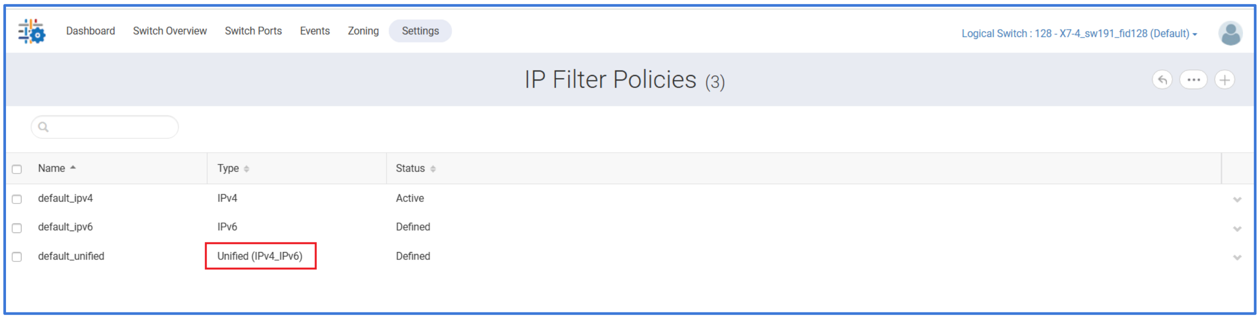
Name

Type: Unified (IPv4_IPv6)

Rules

Order	Type	Source IP Address	Destination IP Address	Service	Destination Port	Protocol	Action

No data to display.



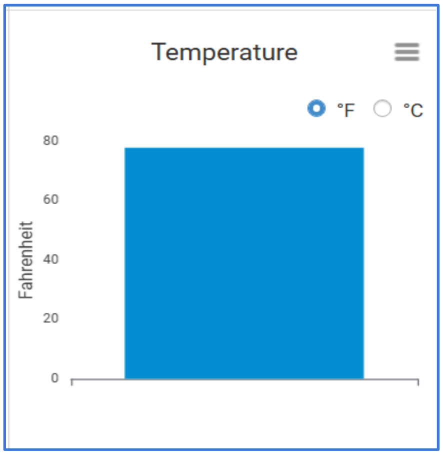
IP Filter Policies (3)

Name	Type	Status
default_ipv4	IPv4	Active
default_ipv6	IPv6	Defined
default_unified	Unified (IPv4_IPv6)	Defined

4.2.9.4 Switch Temperature

The existing temperature widget available in the dashboard page of Web Tools application shows the max sensor temperature of each slot for Chassis and each sensor's temperature for Gen 7 fixed form factor switches.

For Gen 8 platforms, only the ambient temperature sensor is exposed to the end user. Accordingly, Web Tools only displays the intake temperature for Gen 8 platforms.

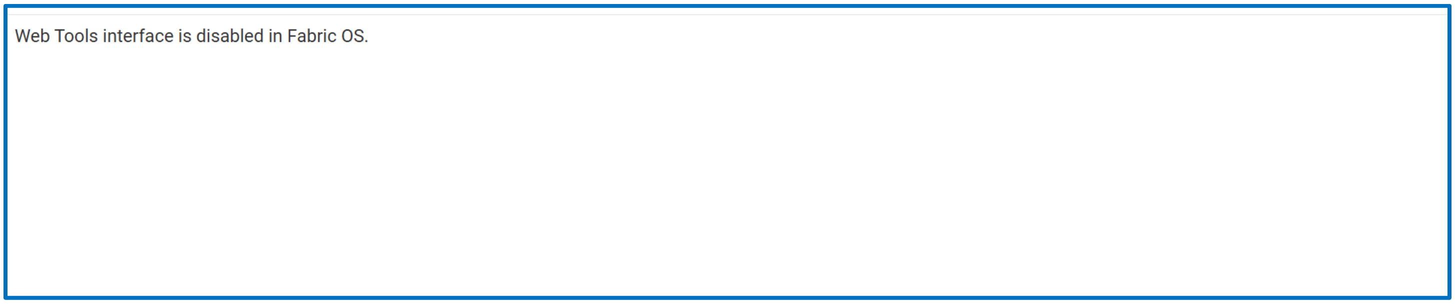


4.2.9.5 Web Tools Disabled

From FOS v10.x the user can disable or enable the Web Tools using CLI or REST. Per default Web Tools is enabled.

In case Web Tools is disabled the following message is displayed when attempting to access the switch with HTTPS:

“`Web Tools interface is disabled in Fabric OS.`”



Web Tools interface is disabled in Fabric OS.

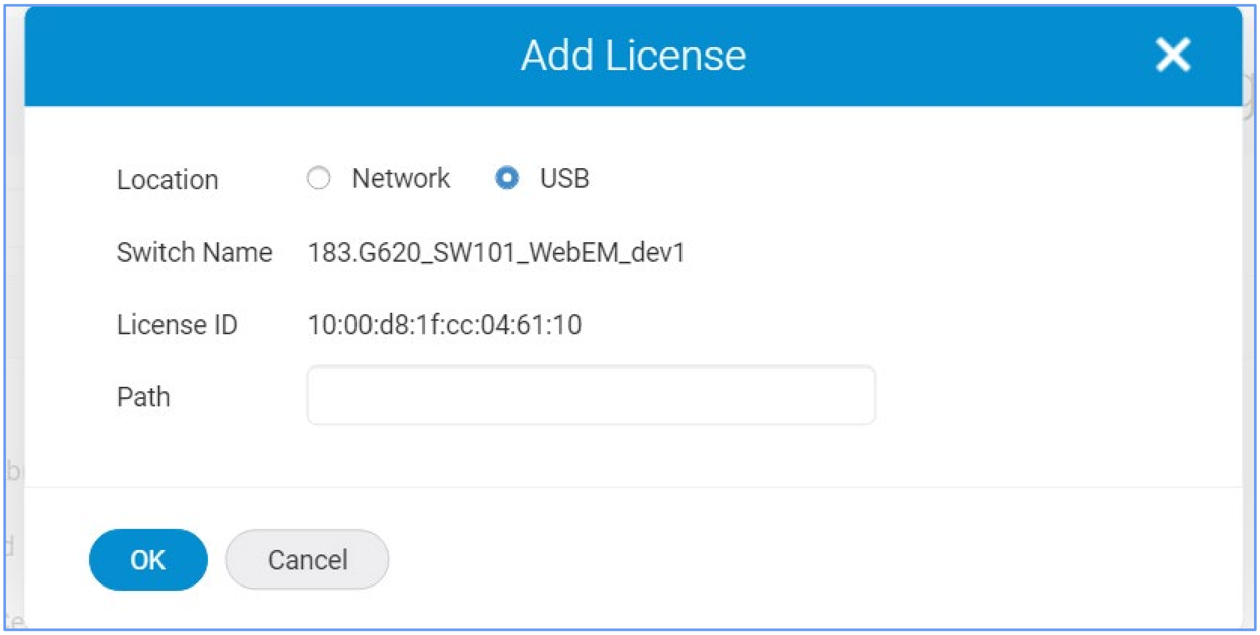
4.2.9.6 Install License from USB

In FOS v10.x Web Tools is enhanced to support license install from USB.

By selecting the USB option, the user can install the license by providing the license path from an USB drive.

License Management:

- Login to Web Tools
- Navigate to Settings -> Services -> License Management
- Click Plus (+) icon to add a new license.



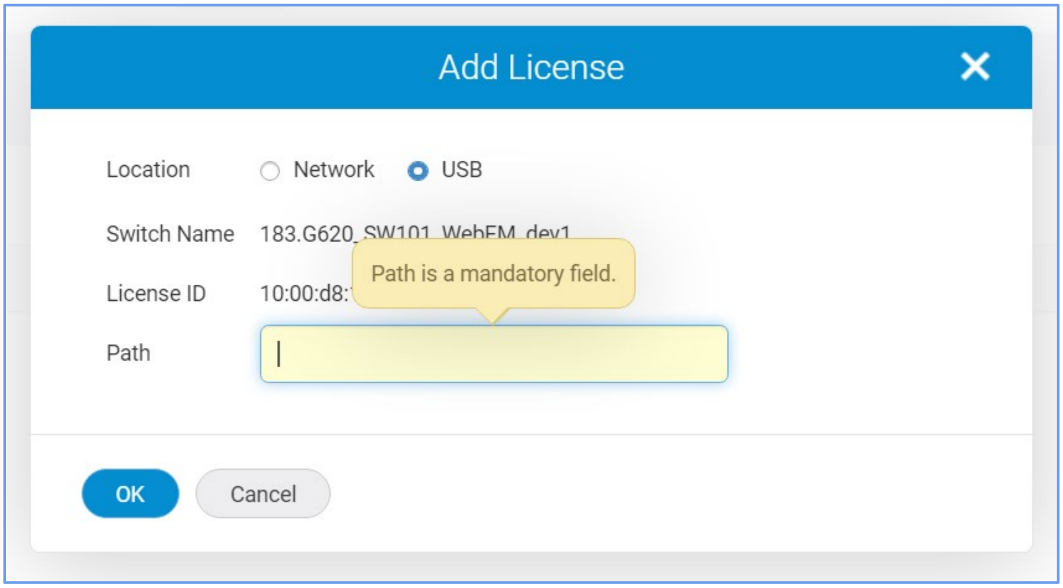
Location ○ Network ● USB

Switch Name 183.G620_SW101_WebEM_dev1

License ID 10:00:d8:1f:cc:04:61:10

Path

- Path is a mandatory field. Enter the complete & exact path to the license file on the USB drive.
- Validation error (Path is a mandatory field.) will be shown in the yellow balloon if the path field is empty. The character validation will be done only on the backend, and the Web Tools will show the corresponding error popup from the backend (will work as transparent).



Location ○ Network ● USB

Switch Name 183.G620_SW101_WebEM_dev1

License ID 10:00:d8:

Path

Path is a mandatory field.

Validation is done when the OK button is clicked and the corresponding error message will be shown if anything, similar to the existing validation of Network form. Upon successful installation of license from the USB, the license will be listed in the License Management list view.

An error modal with the actual error message will be shown if the path is invalid or the path does not have a proper license.

4.2.9.7 Export Licenses from FOS

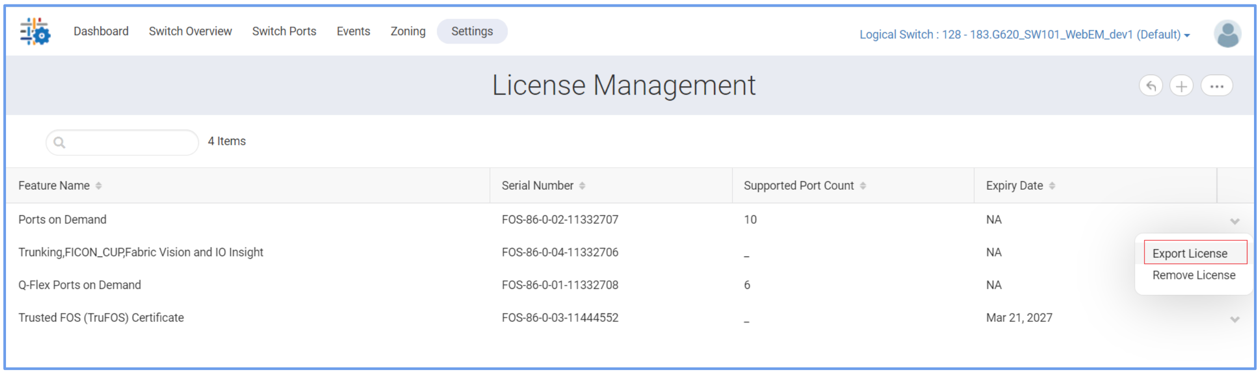
In FOS v10.x Web Tools is enhanced to support license export of v4 and v5 licenses.

The Export option is introduced in the License Management list view. The user can export a specific license or all the licenses available in the switch from the License Management view.

License Management:

- Login to Web Tools
- Navigate to Settings -> Services -> License Management.

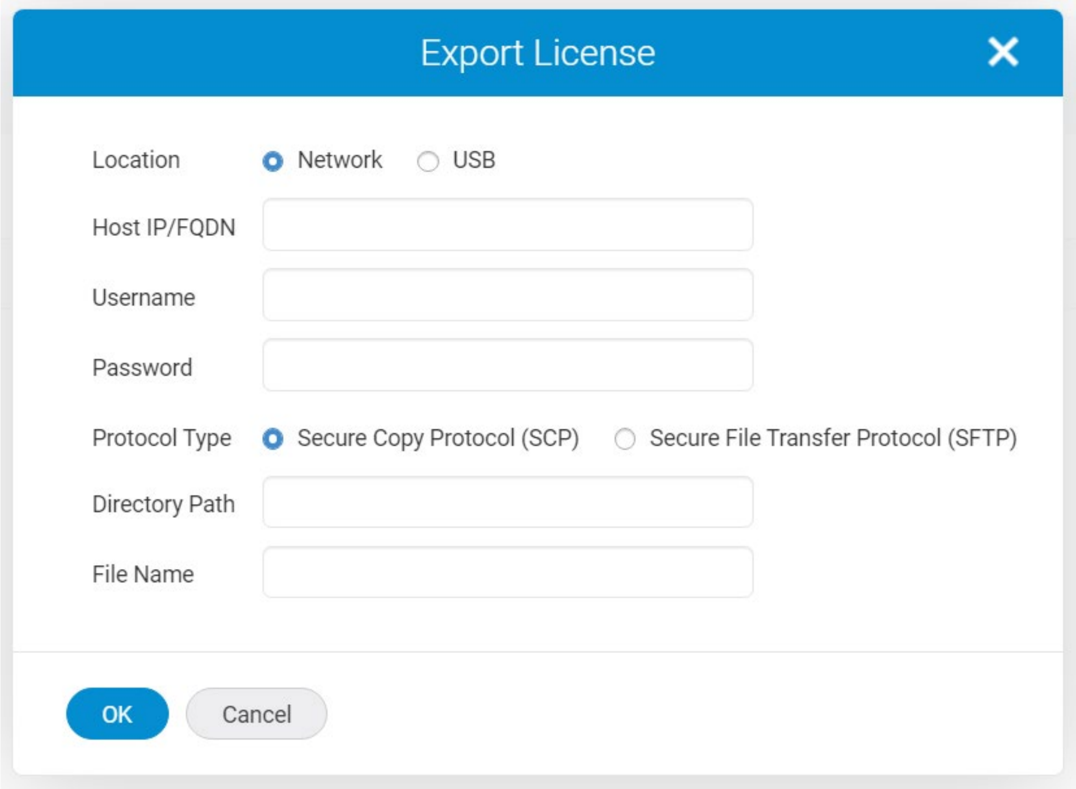
The Export License option will be added to each license row on the dropdown menu as shown below of the license Management list view. On choosing the option, the Export License modal is shown, and the user can export the license to an external server or to an USB device in XML format by providing the server information in the modal.



License Management

4 Items

Feature Name	Serial Number	Supported Port Count	Expiry Date
Ports on Demand	FOS-86-0-02-11332707	10	NA
Trunking,FICON_CUP,Fabric Vision and IO Insight	FOS-86-0-04-11332706	_	NA
Q-Flex Ports on Demand	FOS-86-0-01-11332708	6	NA
Trusted FOS (TruFOS) Certificate	FOS-86-0-03-11444552	_	Mar 21, 2027

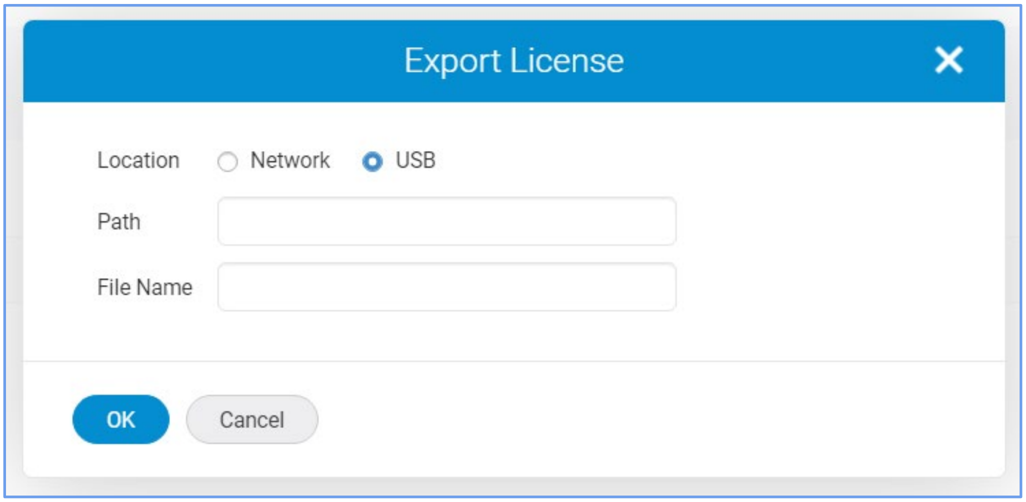


Export License

Location ● Network ○ USB

Protocol Type ● Secure Copy Protocol (SCP) ○ Secure File Transfer Protocol (SFTP)

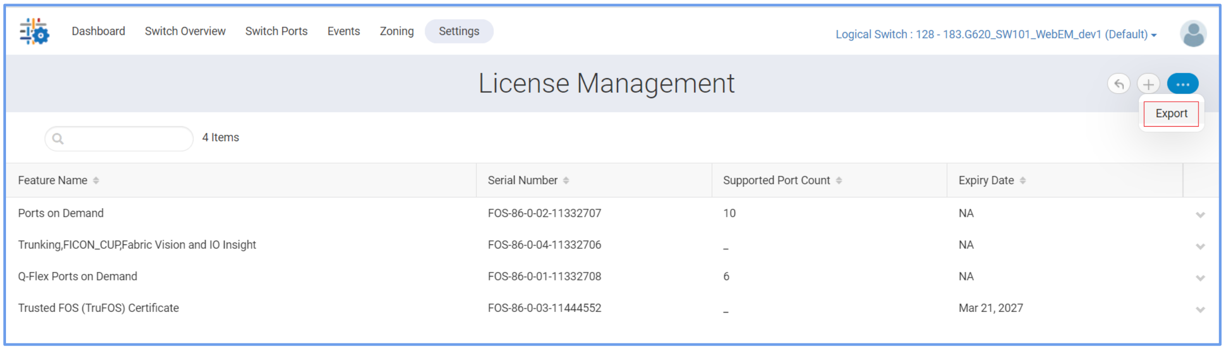
When USB is chosen:



Export License

Location ○ Network ● USB

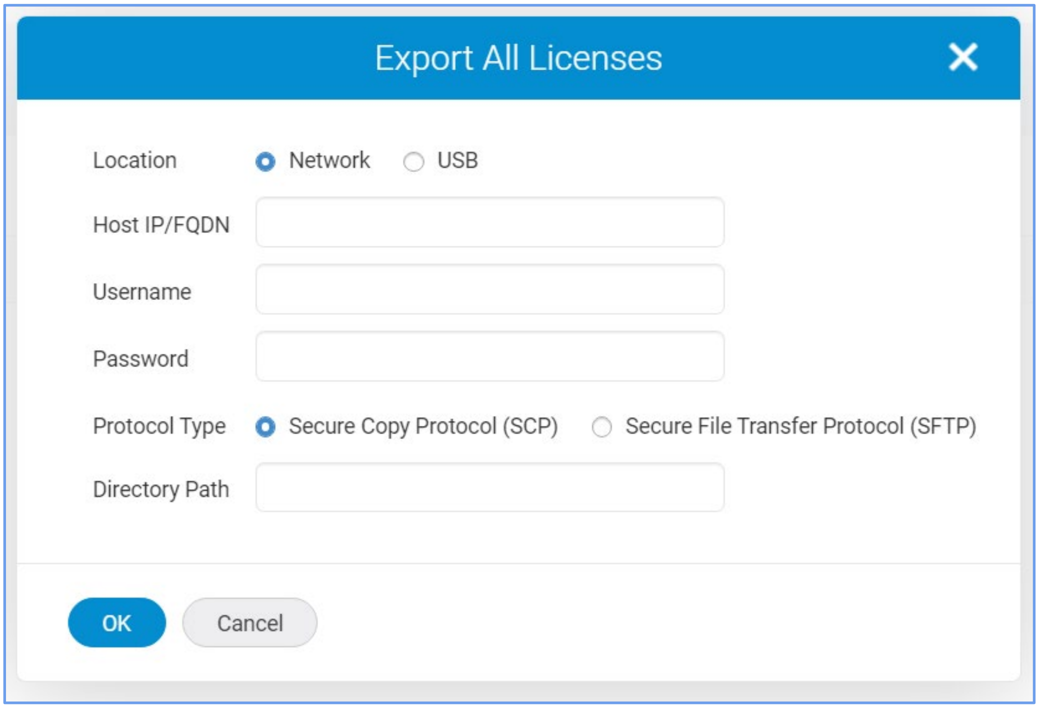
Also, a bulk Export option is added in the top right, as shown below, of the license Management list view. The user can export all the available licenses in the switch to an external server or USB drive.



License Management

4 Items

Feature Name	Serial Number	Supported Port Count	Expiry Date
Ports on Demand	FOS-86-0-02-11332707	10	NA
Trunking,FICON_CUP,Fabric Vision and IO Insight	FOS-86-0-04-11332706	_	NA
Q-Flex Ports on Demand	FOS-86-0-01-11332708	6	NA
Trusted FOS (TruFOS) Certificate	FOS-86-0-03-11444552	_	Mar 21, 2027



Export All Licenses

Location ● Network ○ USB

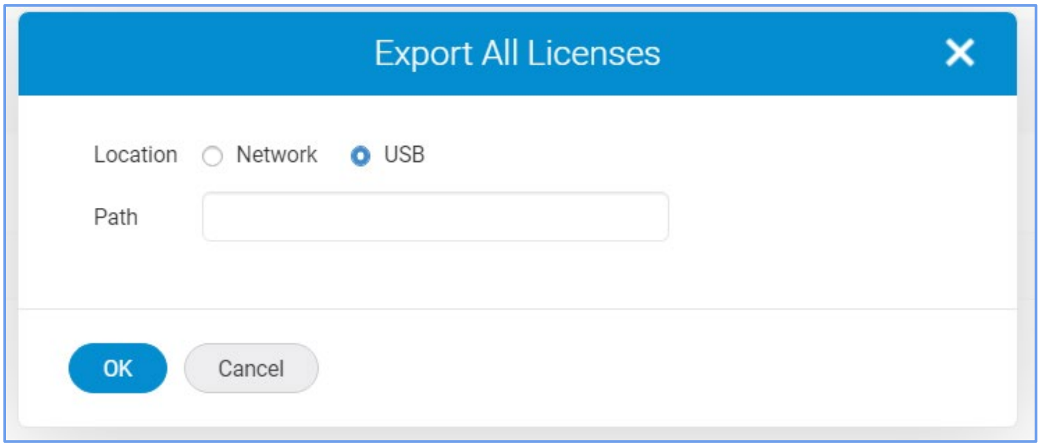
Host IP/FQDN

Username

Password

Protocol Type ● Secure Copy Protocol (SCP) ○ Secure File Transfer Protocol (SFTP)

Directory Path



Export All Licenses

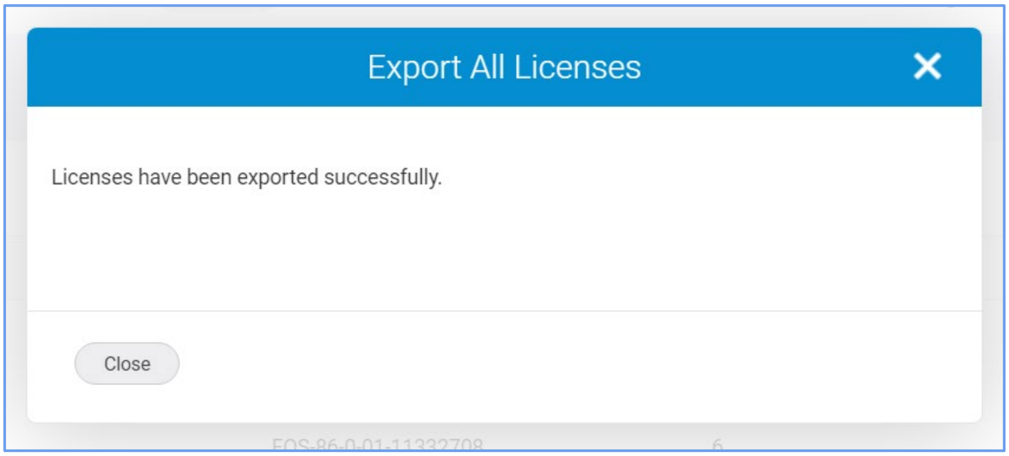
Location ○ Network ● USB

Path

Client validation covers only the empty check, valid IP Address and valid directory path as shown below.

Sequence	Field	Error Message
1	Host IP	Host IP is a mandatory field.
2		Invalid input. It must be a valid IP address.
3	Username	Username is a mandatory field.
4	Password	Password is a mandatory field.
5	Directory Path	Directory Path is a mandatory field.
6		Invalid input. It must be a valid directory path.

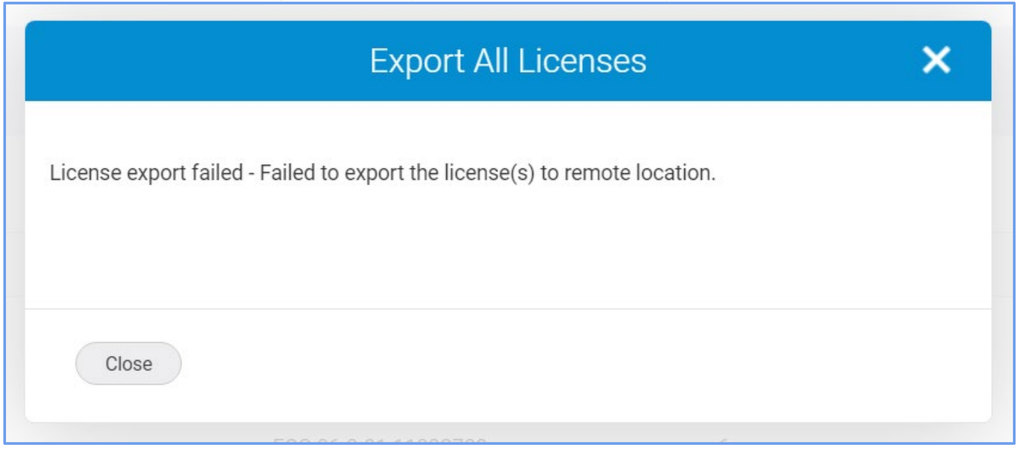
Success screen:



Licenses have been exported successfully.

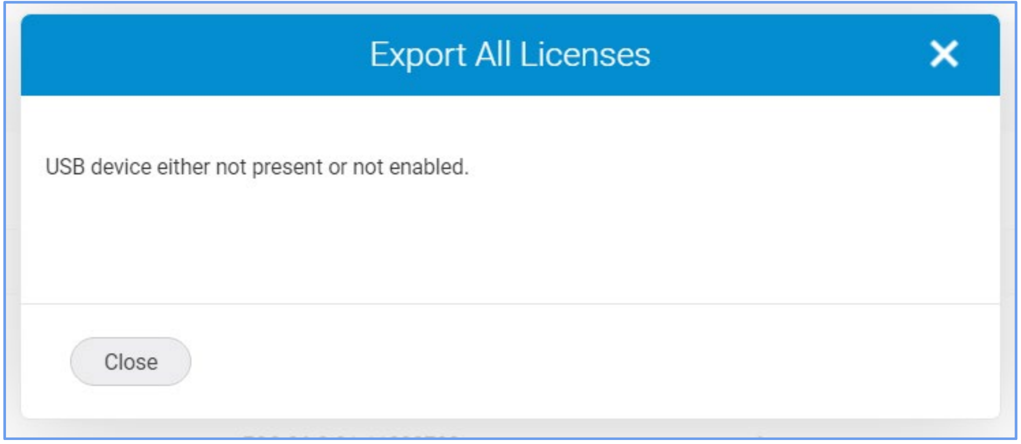
Error screen:
The error message from the server will be displayed if there are any errors such as invalid directory path, server, username or password (Web Tools works transparently).

The below error message is displayed when the directory path is invalid.



License export failed - Failed to export the license(s) to remote location.

The error message below is displayed if there is no USB connected.



USB device either not present or not enabled.

4.2.9.8 Trunking Table

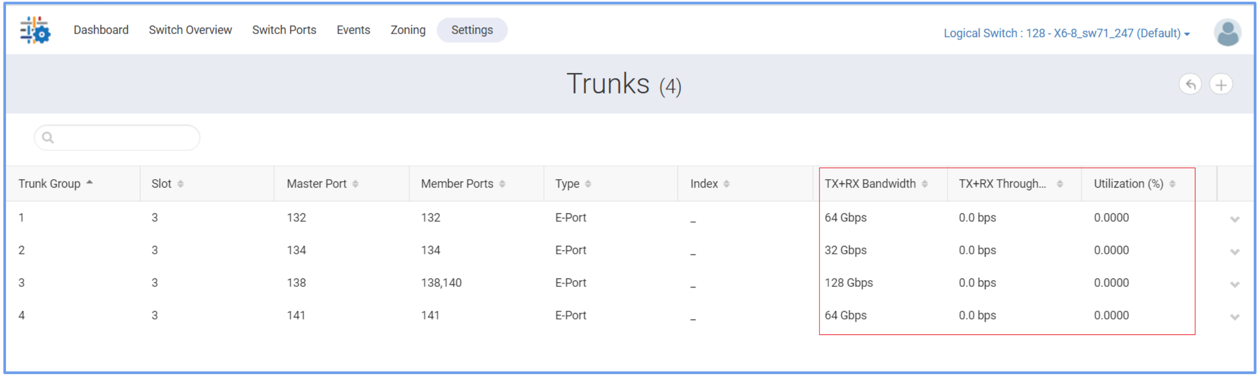
In FOS v10.x Web Tools Trunking tables are enhanced to display trunk capacities instead of bandwidth in addition to utilization.

Prior to FOS v10.x, the Trunking table had TX+RX Bandwidth and TX+RX Throughput columns in the Trunking view. In FOS v10.x the TX+RX Bandwidth column is replaced with two new columns TX Capacity and RX Capacity and similarly the TX+RX Throughput column is replaced with TX Utilization and RX Utilization in the trunking view. The summarized Utilization column is removed.

Trunking:

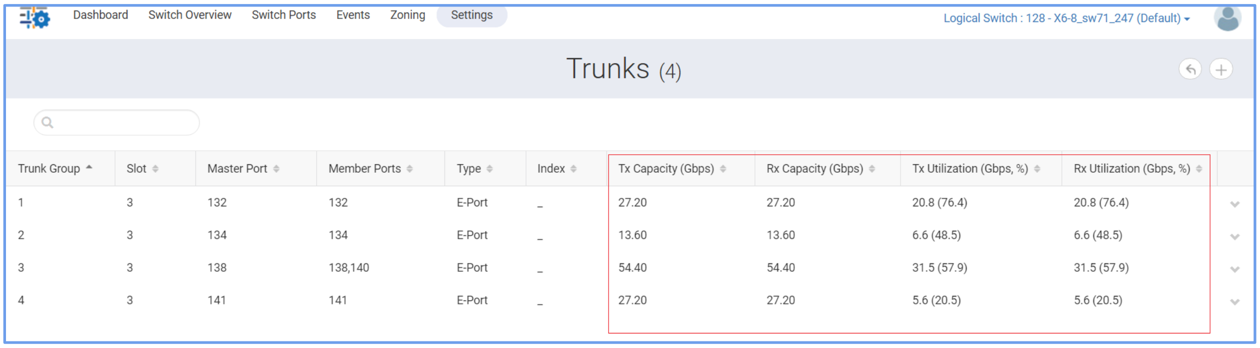
- Login to Web Tools
- Navigate to Settings -> Configuration -> Trunking.

Trunking table columns prior to FOS v10.x



Trunk Group	Slot	Master Port	Member Ports	Type	Index	TX+RX Bandwidth	TX+RX Through...	Utilization (%)
1	3	132	132	E-Port	_	64 Gbps	0.0 bps	0.0000
2	3	134	134	E-Port	_	32 Gbps	0.0 bps	0.0000
3	3	138	138,140	E-Port	_	128 Gbps	0.0 bps	0.0000
4	3	141	141	E-Port	_	64 Gbps	0.0 bps	0.0000

Trunking table columns in FOS v10.x



Trunk Group	Slot	Master Port	Member Ports	Type	Index	Tx Capacity (Gbps)	Rx Capacity (Gbps)	Tx Utilization (Gbps, %)	Rx Utilization (Gbps, %)
1	3	132	132	E-Port	_	27.20	27.20	20.8 (76.4)	20.8 (76.4)
2	3	134	134	E-Port	_	13.60	13.60	6.6 (48.5)	6.6 (48.5)
3	3	138	138,140	E-Port	_	54.40	54.40	31.5 (57.9)	31.5 (57.9)
4	3	141	141	E-Port	_	27.20	27.20	5.6 (20.5)	5.6 (20.5)

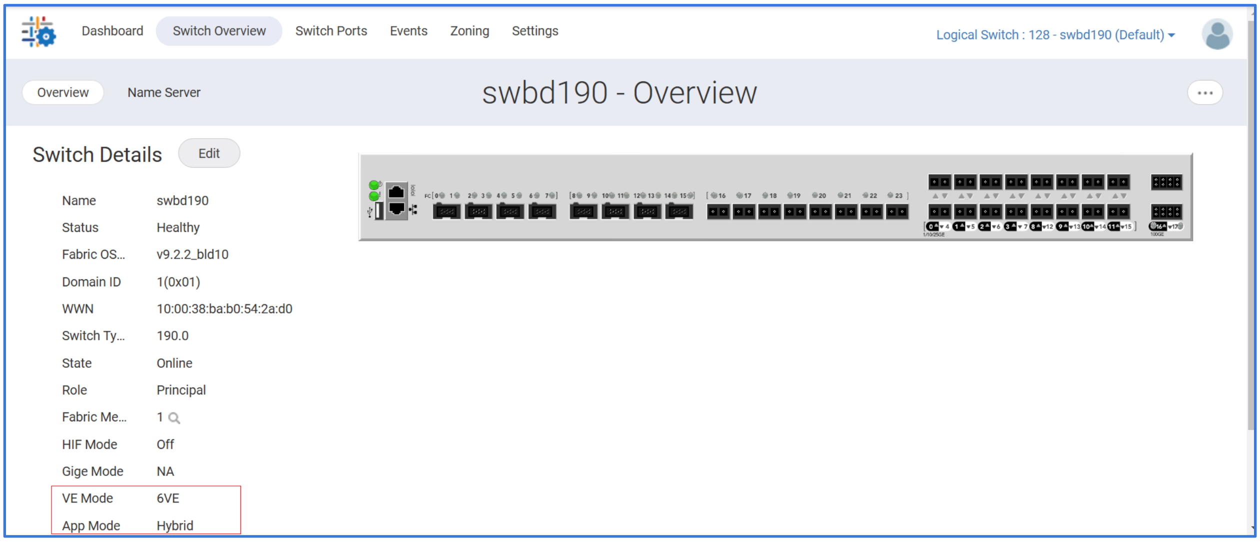
4.2.9.9 Extension VE and APP Mode

In FOS v10.x Web Tools is enhanced to support display of Extension switches VE and APP mode.

Displaying Extension VE and APP mode:

- Login to Web Tools
- Navigate to Switch Overview tab

For fixed form factor switches the VE and APP mode is displayed on the Switch Details section along with the other properties as shown below.

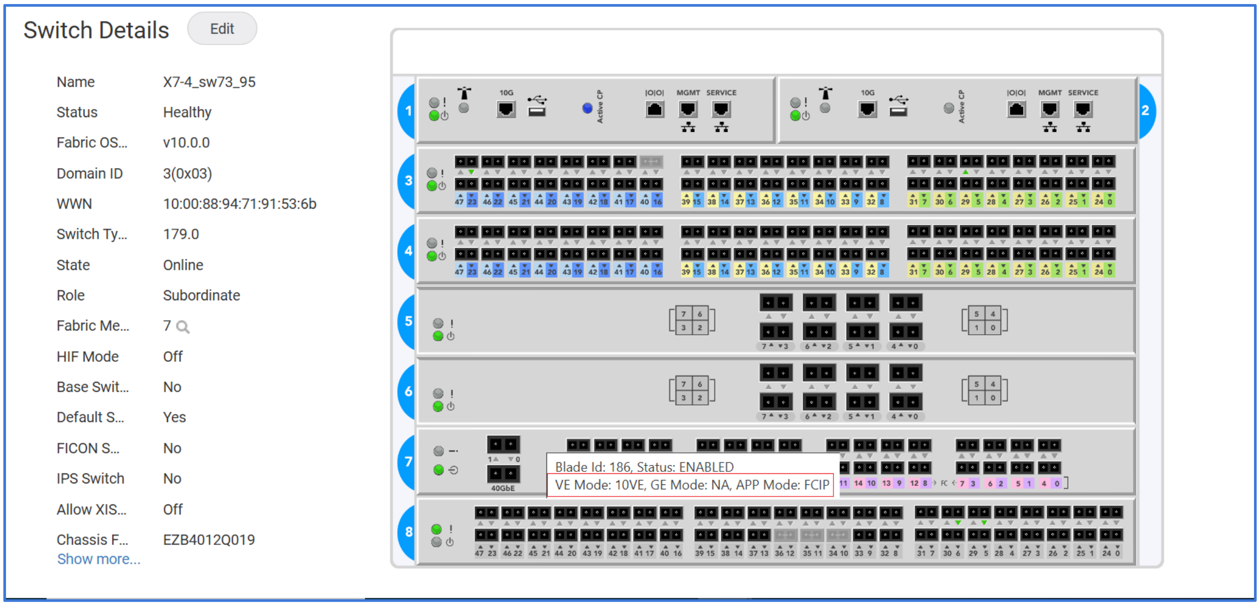


swbd190 - Overview

Switch Details

Name	swbd190
Status	Healthy
Fabric OS...	v9.2.2_bld10
Domain ID	1(0x01)
WWN	10:00:38:ba:b0:54:2a:d0
Switch Ty...	190.0
State	Online
Role	Principal
Fabric Me...	1
HIF Mode	Off
Gige Mode	NA
VE Mode	6VE
App Mode	Hybrid

For Directors, the VE and APP mode is shown on the tooltip of the Extension blade(s) as below, since there is a possibility more than one extension blade is present on a chassis.



Switch Details

Name	X7-4_sw73_95
Status	Healthy
Fabric OS...	v10.0.0
Domain ID	3(0x03)
WWN	10:00:88:94:71:91:53:6b
Switch Ty...	179.0
State	Online
Role	Subordinate
Fabric Me...	7
HIF Mode	Off
Base Swit...	No
Default S...	Yes
FICON S...	No
IPS Switch	No
Allow XIS...	Off
Chassis F...	EZB4012Q019

Blade Id: 186, Status: ENABLED
VE Mode: 10VE, GE Mode: NA, APP Mode: FCIP

4.2.10 REST

Major REST changes are described in this section

4.2.10.1 Support for Switch and Port Beaconing

Prior to FOS v10.x the REST interface did provide the status of switch beacon, but there was no provision to modify it. Additionally, the support to modify and view the port beacon mode is also required.

From FOS v10.x, users will be able to modify and view the port beacon and switch beacon modes via REST.

The following are the new additions to the REST interface.

- A new RPC operation module, `brocade-operation-switch` to perform switch beacon enable and disable operations.
- Add a new parameter in the `brocade-operation-port` module to enable or disable port beacon mode.
- A read only leaf to verify the status of port beacon mode in the `brocade-interface` module.

To verify the status of the switch beacon mode, one can perform GET with the existing URI `brocade-fibrechannel-switch/fibrechannel-switch/name/<wwn>/switch-beacon-enabled`

Switch beaconing can be used to locate a failing unit. When beaconing mode is turned on, the port LEDs flash amber, left to right and right to left, from port 0 to the highest port number and back to port 0. The beaconing mode continues until you turn it off.

Port beaconing mode is useful if you are trying to locate a specific port. When beaconing mode is enabled on a port, the port LED flashes amber and green for 2.5 seconds each in an alternating pattern. The beaconing mode continues until you turn it off.

4.2.10.2 IP Storage Statistics

A new REST module is added in FOS v10.0.0:

`brocade-operation-ip-storage-statistics`

Chapter 5: Software License Support

Fabric OS 10.x includes all basic switch and fabric support software, as well as all feature licenses.

5.1 Optionally Licensed Software

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.)

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.

Chapter 6: Hardware Support

6.1 Supported Devices

The following devices are supported in this release:

- Brocade X8-8 Director
- Brocade X8-4 Director
- Brocade X7-8 Director
- Brocade X7-4 Director
- Brocade G820 Switch
- Brocade G730 Switch
- Brocade G720 Switch
- Brocade G710 Switch
- Brocade 7850 Extension Switch

6.2 Supported Blades

6.2.1 X8-8 and X8-4 Blade Support

Fabric OS v10.0.x software is fully qualified and supports the blades for the X8-8 and X8-4 as noted in the following table.

Blades	FOS v10.0.x Support
FC128-48 128G FC Blade	Supported
ICLX8-8 ICL Blade	Supported in X8-8
ICLX8-4 ICL Blade	Supported in X8-4

6.2.2 X7-8 and X7-4 Blade Support

Fabric OS v10.0.x software is fully qualified and supports the blades for the X7-8 and X7-4 as noted in the following table.

Blades	FOS v10.0.x Support
FC64-64 64G FC Blade	Supported
FC64-48 64G FC Blade	Supported
FC32-X7-48 32G X7 FC Blade	Supported
SX6 Gen 6 Extension Blade	Supported. Up to a maximum of four blades of this type.

6.3 Supported Power Supplies

For the list of supported power supplies for Brocade X8 and power supply requirements, refer to the *Brocade X8 Director Technical Specification*.

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

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

Chapter 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 8 entry level switch on a Gen 8 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.
```

7.2 FOS Image Filenames

Fabric OS v10.0.0

Image Filename	Description
v10.0.0.sha512	Fabric OS v10.0.0 SHA512 Checksums
v10.0.0_all_mibs.tar.gz	Fabric OS v10.0.0 SNMP MIBs
v10.0.0_EXT.tar.gz	Fabric OS v10.0.0 for Linux to install on 7850 platforms
v10.0.0_EXT.zip	Fabric OS v10.0.0 for Windows to install on 7850 platform
v10.0.0_G7_ENTRY.zip	Fabric OS v10.0.0 for Windows to install on G710 platform
v10.0.0_G7_ENTRY.tar.gz	Fabric OS v10.0.0 for Linux to install on G710 platform
v10.0.0_G7_MID.tar.gz	Fabric OS v10.0.0 for Linux to install on G720 platforms
v10.0.0_G7_MID.zip	Fabric OS v10.0.0 for Windows to install on G720 platforms
v10.0.0_G8_MID.tar.gz	Fabric OS v10.0.0 for Linux to install on G820 platforms
v10.0.0_G8_MID.zip	Fabric OS v10.0.0 for Windows to install on G820 platforms
v10.0.0_G7_ENTP.tar.gz	Fabric OS v10.0.0 for Linux to install on G730 platform
v10.0.0_G7_ENTP.zip	Fabric OS v10.0.0 for Windows to install on G730 platform
v10.0.0_G7_DIR.tar.gz	Fabric OS v10.0.0 for Linux to install on X7-8 and X7-4 platforms
v10.0.0_G7_DIR.zip	Fabric OS v10.0.0 for Windows to install on X7-8, X7-4 platforms
v10.0.0_G8_DIR.zip	Fabric OS v10.0.0 for Windows to install on X8-8, X8-4 platforms
v10.0.0_G8_DIR.zip	Fabric OS v10.0.0 for Windows to install on X8-8, X8-4 platforms
v10.0.0.releasenotes_v3.pdf	Fabric OS v10.0.0 Release Notes

The image files for each respective platform can be downloaded from your switch vendor’s website and support.broadcom.com, except for YANG files which are available on 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 v10.0.0

The supported upgrade paths to Fabric OS v10.0.0 are as follows:

Current Version	Upgrade Path
FOS v9.2.2x	Nondisruptive upgrade
FOS v9.2.1x	Disruptive upgrade (allowed using `firmwaredownload -s`) not recommended for production environments
FOS v9.2.0x	Direct upgrade is not supported and will be blocked First upgrade from FOS v9.2.0x to v9.2.2x, then upgrade to v10.0.0
FOS v9.1.x	Direct upgrade is not supported and will be blocked First upgrade from FOS v9.1.x to v9.2.0x, then upgrade to v9.2.2x followed by upgrade to v10.0.0 (Install TruFOS certificate prior to upgrading to v9.2.x if not already present)

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

NOTE Environments with Gen 7 switches in AG mode and deployment of QoS zones should not upgrade to FOS v10.0.0. See section Miscellaneous under Important Notes for more information.

Environments with Gen 7 switches in AG mode and deployment SDDQ enabled should disable SDDQ (MAPS action) during upgrade to FOS v10.0.0. After upgrade is completed SDDQ can be reenabled.

NOTE If a Gen 7 platform is downgraded from FOS v9.2.2x to v9.2.1x -while weak SMTPS ciphers are configured- it is necessary to first upgrade to FOS v9.2.2x before proceeding with the upgrade to FOS v10.0.x.

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 v10.x* document.

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 v3.x prior to upgrading SAN switches to FOS v10.x.

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

8.2.2 Web Tools Compatibility

Web Tools supports firmware migration to v10.x from FOS v9.2.2x.

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

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.
- 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.

Supported Products	**Fabric OS Interoperability**
Brocade 7840	FOS v8.2.3x (Not compatible in the same fabric. Must use FCR)
Brocade 6520	FOS v8.2.3x (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 6543	FOS v8.2.3x (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 6547	FOS v8.2.3x (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade 6558	FOS v8.2.3x (Not compatible in the same fabric. Must use FCR or connect as AG)
Brocade G610 (switchType 170.0 to 170.3)	FOS v9.1.x
Brocade G610 (switchType 170.4 or higher)	FOS v9.1.x
Brocade G620 (switchType 162)	FOS v9.1.x
Brocade G620 (switchType 183.0)	FOS v9.1.x
Brocade G620 (switchType 183.5)	FOS v9.1.x
Brocade G630 (switchType 173)	FOS v9.1.x
Brocade G630 (switchType 184)	FOS v9.1.x
Brocade 7810	FOS v9.1.x
Brocade X6-8/X6-4	FOS v9.1.x
Brocade X6-8/X6-4 (switchType 166.5 and 165.5)	FOS v9.1.x
Brocade G710 (switchType 191.0)	FOS v9.2.2
Brocade G720 (switchType 181.0)	FOS v9.1.x
Brocade G720 (switchType 181.5)	FOS v9.1.1
Brocade G730 (switchType 189.8)	FOS v9.1.x
Brocade X7-8/X7-4	FOS v9.1.x
Brocade G648	FOS v9.1.x
Brocade MXG610	FOS v9.1.x
Brocade 7850	FOS v9.2.x or later
Brocade X8-8/X8-4	FOS v10.0.0
Brocade G820	FOS v10.0.0

8.2.4 SNMP Support

Fabric OS v10.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 v10.x*.

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, 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 or www.simpleweb.org/ietf/mibs.

8.2.6 REST API Support

Fabric OS v10.x documents the supported REST API functions in the *Brocade Fabric OS REST API Reference Manual*.

8.2.6.1 Obtaining YANG Files

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

1. Go to www.broadcom.com/products/fibre-channel-networking/software/fabric-operating-system.
2. Select **Downloads**.
3. The YANG files can be located under the Yang Module.
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.

8.3 Important Notes

Brocade recommends to always review Important Notes for each release.

8.3.1 Maximum Number of DCC Members

The maximum allowed number of Device Connection Control, DCC members that can be defined and active is enforced in FOS v10.x.

In FOS v9.2.2 environments with more than 3700 DCC policy members (the actual max number is a combination of DCC, SCC and FCS members) may encounter a situation where upgrade to FOS v10.x is blocked and the error message below will be displayed directing the user to reduce the DCC policy members.

```
"FID:<fid_num>, Current ACL POLICY active Database has exceeded the maximum allowed
policy member limit in the target version. Delete <num_of_dcc_members_to_be_deleted> DCC
members from the active policy Database using CLI \"secpolicyremove
<name>,<member>[;<member>...]\".
```

8.3.2 DWDM

When connecting Gen 8 platforms to DWDM from Adva it is necessary to use 64G SFP+ until connectivity support using 128G SFP+ is available from Adva.

8.3.3 ICL Connectivity between X7 and X8

ICL connectivity between X7 and X8 is supported with the following prerequisites:

- The QSFPs in the X7 must have serial number prefix BABxxxxxxx
- The X7 must be running FOS v10.x or later
- The QSFPs in the X7 must be upgraded to the latest firmware
- On the X8 the OSFP port speed must be configured to 53G
- Qualified break-out cables must be used for the connection

For the current list of qualified breakout cables, refer to the High-Density Cabling Design Guide.

1. Verify the QSFPs serial number in the X7 using the `sfpshow` command.

Example:
The BABxxxxxxx QSFP is supported

```
X7-8:FID128:admin> sfpshow | grep "Slot  7" |grep "BROCADE"
Slot  7/Port  0: id  0/0 (sw) Vendor: BROCADE          Serial No: BAB220410000028  Speed: 53_Gbps
Slot  7/Port  1: id  0/1 (sw) Vendor: BROCADE          Serial No: BAB220410000028  Speed: 53_Gbps
Slot  7/Port  2: id  0/2 (sw) Vendor: BROCADE          Serial No: BAB220410000028  Speed: 53_Gbps
Slot  7/Port  3: id  0/3 (sw) Vendor: BROCADE          Serial No: BAB220410000028  Speed: 53_Gbps
-----Truncated----
```

The BARxxxxxxx QSFP is not supported. If the QSFP is not supported it must be replaced, contact your vendor.

```
X7-8:FID128:admin> sfpshow | grep "Slot  8" |grep "BROCADE"
Slot  8/Port  0: id  0/0 (sw) Vendor: BROCADE          Serial No: BAR420230000163  Speed: 53_Gbps
Slot  8/Port  1: id  0/1 (sw) Vendor: BROCADE          Serial No: BAR420230000163  Speed: 53_Gbps
Slot  8/Port  2: id  0/2 (sw) Vendor: BROCADE          Serial No: BAR420230000163  Speed: 53_Gbps
Slot  8/Port  3: id  0/3 (sw) Vendor: BROCADE          Serial No: BAR420230000163  Speed: 53_Gbps
-----Truncated----
```

2. To verify the FOS version running on the X7 use the command `version.`
Example:

```
X7-8:FID128:admin> version
Kernel:     5.4.66_rt38
Fabric OS:  v10.0.0
Made on:    Fri Aug 22 10:04:32 2025
Flash:          Fri Aug 29 13:24:57 2025
BootProm:   4.0.14-sb
```

3. To upgrade the QSFPs on the X7 using the `sfpupgrade` command (the QSFP ports must be disabled prior to issuing the command).
Example:

```
X7-8:FID128:admin> sfpupgrade 7/0-63

X7-8:FID128:admin> sfpupgrade 8/0-63
```

Upon successful completion, verify the MCU version is 0x6, DSP version is 0x6 using the `sfpshow` command.
Example:

```
X7-8:FID128:admin> sfpshow 7/0 -f -verbose
```

4. Configure the speed on the OSFPs in X8 using the command `portcfgspeed.`
Example:

```
X8-8:FID128:admin> portcfgspeed -slot 13 53
```

```
Note: Consult the hardware installation guide for requirements to connect ICLs to Gen 7 ICLs.

X8-8:FID128:admin> portcfgspeed -slot 14 53
Note: Consult the hardware installation guide for requirements to connect ICLs to Gen 7 ICLs.
```

5. For the latest list of qualified breakout cables see the *Brocade High-Density Cabling Design Guide*.

8.3.4 SAN Fabric Intelligence

In FOS v10.0.0 the following applies to SAN Fabric Intelligence.

- When using SAN FI commands, EX_Ports are displayed as ‘Other’.
- When using SAN FI commands, to query F_Port trunks the subordinate ports are displayed as ‘Other’.
- For details on SAN Fabric Intelligence see SAN Fabric Intelligence (SAN FI).

8.3.5 Secure SMTP

In FOS v10.x, it is mandatory to import CA certificates when configuring and using Secure SMTP (without which TLS connection establishment with the SMTP server fails).

In FOS v9.2.x it was not required to import CA certificates when configuring Secure SMTP. Upgrade to FOS v10.x is blocked when Secure SMTP is configured without import of CA certificates.

8.3.6 Obsoletions in FOS v10.x

In FOS v10.x the following protocols and functions are obsoleted and upgrade to FOS v10.x from FOS v9.2x is blocked when configured or in use:

- Non-secure protocols
  - HTTP
  - FTP
  - TELNET
- TLS <1.2
- SNMPv1
- IPFC
- TACACS+
- RADIUS
- Cascaded AG
- Extension
  - FICON Emulation Modes (XRC, TAPE, Teradata, TinTIr, DcvAck)
  - Automated WTOOL, SLA
    - Note: The user WAN Test Tool is not obsoleted
- FSPF commands
  - `interfaceShow`
  - `nbrShow`

- FCR boot over SAN
- FCR LSAN Tags
- FCoE
- End Device/Port RSCN Suppression
- The command `psutil`

8.3.7 OUI

The OUI (Organizationally Unique Identifier) B8:CE:ED (for example, 10:00:B8:CE:ED:xx:xx:xx) introduced with newer switches is supported in topologies using AG or FCR with FOS v10.0.0.

8.3.8 Miscellaneous

- `chassisenable/switchenable` is blocked after executing `chassisdisable/switchdisable` followed by offline diagnostics. It is necessary to afterwards reenable the switch using the command `chassisreboot` on Directors or reboot on fixed form factor switches.
- When replacing/powering on core blades with POST enabled, it is necessary for the core blades to complete boot up before replacing/powering on other Core Blade, Port blades or ICL blades.
- When replacing/powering on ICL blades with POST enabled, it is necessary for the ICL blade to complete boot up before replacing/powering on other ICL blade and Core Blades.
- On X8-8/4 users might observe connection to the management port toggle once during boot up.
- In FOS v10.0.0 USF is only supported for X7-8 and X7-4.
  USF is not supported on X8-8 and X8-4 in the initial release of FOS v10.x.
- On Gen 7 platforms upgraded to FOS v10.x. When the intent is to downgrade from FOS v10.x to FOS v9.2.x after performing a clean install of firmware on FOS v10.x. It is necessary to first backup licenses prior to performing the `firmwarecleaninstall` on FOS v10.x -then reinstall the licenses and downgrade to FOS 9.2.x.
  Reinstall of the licenses are required after a clean install is performed, prior to downgrade to FOS v9.2.x.
  In case licenses were not backed up contact your support provider.
  Downgrade from FOS v10.x to v9.2.x does not require backup/restore of licenses when `firmwarecleaninstall` has not been performed prior.
- FOS 10.x introduces several security enhancements. Upon upgrade from FOS v9.2.x to FOS 10.x any customer scripts or test scripts that may have been previously installed are automatically deleted. This clean up during the firmware upgrade is performed to ensure that proper security of the system can be monitored and maintained.

  In FOS v10.x `snmpconfig` longer supports ‘No Security’ and ‘Authentication Only’. Consequently, upgrade to FOS v10.x is blocked if any active SNMPv3 user is configured with NoAuth and/or NoPriv.
- Environments with Gen 7 switches in AG mode and deployment of QoS zones should not upgrade to FOS v10.0.0a but instead postpone upgrade to a future FOS v10.x release.

  In case it is needed to upgrade the environment to FOS v10.0.0a, it is necessary to first replace all QoS zones with standard zones or peer zones. After upgrade the QoS zones can be reimplemented.
- Environments with Gen 7 switches in AG mode and deployment SDDQ enabled should disable SDDQ (MAPS action) during upgrade to FOS v10.0.0a. After upgrade is completed SDDQ can be reenabled.

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:

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 v10.x software releases are provided in the following security announcement:

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

Chapter 10: Defects

10.1 Closed with Code Changes in FOS v10.0.0

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-834569	Flow gets deactivated after reboot/hareboot in AG
FOS-839176	Customer might experience with an N-port from an AG being disabled with a misleading reason "Long distance mode not supported on AG".
FOS-841163	User can't perform firmware download on the switch from SANNav.
FOS-842564	The 7850 console is flooded with messages with string "cmicx_sbusdma_curr_op_details" affecting LAG and Ethernet port stats functionality.
FOS-845543	During HCL, observe RASlog ESS-2001 message followed by RASlog ESS-2002.
FOS-846574	REST GET on /brocade-security/dh-chap-authentication-secret does not match CLI output.
FOS-847080	Switch supportsave collection from SANnav fails.
FOS-847224	POST operation on leaf "action" with value "allow" gives an error message : "Target Port not provided for Allow action". There are other similar errors when attempting to POST or PATCH the 'action' leaf if all parameters are not entered.
FOS-847306	When performing a PATCH operation for the TCL 'default' in a configuration replay scenario, the switch will return an error 'Cannot modify input filters for default TCL' even when no parameters are being modified.
FOS-847501	After upgrade to FOS 9.1.1, switch logging TRCE-1005 message every 6 hours for "FTP Connectivity Test failed due to error" without other functional impact.
FOS-847538	Neighbor WWN missing/incorrect in brocade-interface response.
FOS-847781	The Hostname attribute is not returned in the GPAT response.
FOS-847860	REST PATCH operation on swEventTrap severity level with debug option returns an error, "Invalid severity level".
FOS-847952	CLI firmwareshow output will display "vpackage" string on the secondary partition instead of the build version. This does not affect the functioning of the switch.
FOS-848036	The 'zoneshow --validate' output for a zone that contains an alias member is incorrectly showing the alias member and not displaying the "Effective configuration:" section.
FOS-848121	On an X7 chassis with SX6 blades that have HA capable VE ports, the VE ports might occasionally toggle.
FOS-848182	snmpbulk /walk provides WWNs byte swapped in wrong order such as: 50:06:0e:80:08:9e:d4:20 is displayed wrongly as 80:0e:06:50:20:d4:9e:08
FOS-848228	Improper error message are displayed for invalid inputs to "framelog" command.
FOS-848316	printf limits input to "y" or "n" only, which hinders the ability to do scripting
FOS-848419	RESTfulAPI query sometimes doesn’t show any value for disabled ports
FOS-848422	HA Out of Sync due to SNMPd terminated in FOS upgrade HA window.
FOS-848635	Firmware download from 9.2.0 to 9.0.1e1 release does not complete when ECDSA hostkey is not configured on the switch.

FOS-848644	The SSH keys that are deleted before firmware download are recreated after firmware download.
FOS-848703	If RSC is enabled on the switch, changing authspec fails
FOS-848986	CLI "flow --create" option which worked on FOS8.x, now fails on FOS 9.x with the following error message: root> flow --create egress270 -feature monitor -egrport 4/41 -srcdev "*" -dstdev "*" -noactivate Invalid or nonexistent egress port 4/41 specified.
FOS-849027	User may encounter "Processor rebooted - Software Fault: ASSERT."
FOS-849287	CLI sensorshow displays normal Temperature value, but Fan speed is 14375 RPM and system LED Flashes "amber and green " status.
FOS-849402	Devices connected to AG cannot login. Single F-port trunk becomes multiple F-port trunks.
FOS-849473	Rest returns blank and/or error while switch has a large weblinker process.
FOS-849564	Firmware upgrade to FOS 9.2 on G730 required a manual reboot to finish.
FOS-849642	Switch reported a flood of hardware errors, followed by daemons watchdog timeout and switch reboot. Sometimes these hardware errors also triggered port fault and/or blade fault. A raslog similar to this one should also be observed: [TO-1006], 1011618/1002267, FID 128, INFO, Switch_100, Flows destined to b1a02 device have been moved to PG_OVER_SUBSCRIPTION_4G_16G PG., cfs_ctrlr.c, line: 1470, comp:cfsd, ltime:2023/05/17-06:15:33:923058
FOS-849643	ISL ports become disabled when connecting FOS 8.x with FOS 7.x switch after updating Enhanced Object Zoning. switchshow as below: Index Port Address Media Speed State Proto === 28 28 011c00 id 8G No_Sync FC Disabled (ESC Enhanced Zone Object Name Conflict)
FOS-849645	Network Patroller daemon (NPD) terminated even though the flow monitor was disabled via CLI "flow --deactivate sys_flow_monitor".
FOS-849751	Slow Drain devices on E or EX Port connected switches can cause excessive XTUN-1006 FCIP TX Frame Drop RASLOGs per second.
FOS-849790	Valid certificate not accepted
FOS-849829	FICN-1056 (ERROR) RASLOG reported, but traffic not interrupted
FOS-849852	G610 fails to boot after power outage with reason "ERROR: can't get kernel image!"
FOS-849929	Weblinker dies with a large CoreFile and SanNav may keeps showing "SNMP credentials invalid" state for the switch.
FOS-849942	Majority of ICLs in Hard_flt state after failover triggered by Watchdog Timeout on active CP after the switch crashes.
FOS-849954	PLOGI ACC not being received by host
FOS-849957	CLI sfpprogram command output debug information.
FOS-850029	FICN-1062E and FICN-1062I raslog's issued during eHCL sequences.
FOS-850464	Switch HA State goes out of sync following a FOS upgrade from FOS 8.x to 9.0.x and the switch Zoning DB contains duplicated WWNs.
FOS-850496	Repeated logging of following raslog (with no functional impact): [UFCS-2007], 1118300/13621, FID 128, WARNING,, UFCS Lock stage Failed - ..
FOS-850500	User observes Fan kick starts and stays at a very high speed.
FOS-850931	Switch rebooted because of Kernel Panic
FOS-851010	FCIP Tunnel went down after seeing high rate of CRC errors.

FOS-851141	SNMPd termination encountered during swBootPromLastUpdated query and "ps exfcl" command output (see below) shows stuck rpm query: 0 0 29270 2413 20 0 0 0 exit Z ? 0:00 _ snmpd <defunct> 0 0 23760 1 20 0 5144 3304 - R ? 5531:10 rpm
FOS-851164	Switch response for rest login request missing switch-parameters data for AAA non-local users.
FOS-851223	Switch ran out of kernel memory and triggered daemon panic, cpu busy or port/blade fault, etc.
FOS-851444	Observed kernel panic with the following stack trace: 000: Call Trace: 000: ? oidh_objget+0x39/0x50
FOS-851559	8Gb device slow to connect to 32G SFP on chassis.
FOS-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-851993	REST login fails, WebEM reports "Unable to access switch"
FOS-852431	User may encounter RASLOGs RAS-1001 flagging FFDC and "Termination of secd:<secd-process-id>"
FOS-852572	Core onserved while taking supportsave or segment fault during "RON --show" command.
FOS-852926	MAPS (module mdd) could go into a defunct state, and the state prevents MAPS from restarting, resulting in HA out of SYNC.
FOS-852945	fixed by merge
FOS-852964	Kernal panic after hareboot.
FOS-853019	FICN-2064 reports the wrong FID and port in a chassis based switch
FOS-853061	IO failure due to credit loss on 7850 VE-Port with associated AN-1014 and XTUN-1006 RASLOGs indicating Frame timeout detected on a VE-Port.
FOS-853174	FC-LAG is no longer functioning.
FOS-853249	cald process aborted due to memory resource not available.
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-853435	VF cannot enabled after disable.
FOS-853452	The memory corruption will result in mdd panic.
FOS-853582	sfpProgram --show: Need to add the ability to query if a given SFP has been programmed
FOS-853697	Name server daemon (nsd) panic is observed while running nsaliasshow command.
FOS-853775	FabricAdmin role not allowing users to run supportshow after upgrade to v9.0.x
FOS-853850	Telnet not working after FOS 9.1.1x upgrade.
FOS-853898	A small 24 bytes leak for each succesful login.
FOS-853997	When "bulk" persistentEnable'ing ports from SanNav, ports would go to 'No_light' and disabled state.
FOS-854080	Detected termination of a daemon (zoned) followed by CP panic from Sotware Watch Dog timeout.
FOS-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-854371	FC traffic over an FCIP Tunnel stopped. The tunnel remains active, but IO is not passing over the WAN. FC ingress timeouts are observed from local FC ports that should be using the tunnel.

FOS-854397	Observed the following flood of raslog: [MQ-1007], 783, SLOT 1 | FFDC | FID 128, WARNING, , queue fmFlowCopyQ: queue full (miss=1).
FOS-854555	Large debug file (weblsocket.txt) was not removed as part of code upgrade, causing high flash usage to remain.
FOS-854587	The cfsd (Congestion Framwork System daemon) terminated during supportsave, resulting in repeated UFCS-2007 messages for "UFCS Lock stage Failed". Also, CFS supportsave info is not collected from all logical switches.
FOS-854685	Core blade abruptly power cycled itself and CP panicked with assert: ASSERT - Failed expression: ope->offload_req != NULL
FOS-854964	switches experienced snmpd termination and persistent loss of HA sync after customer upgraded snmp monitoring application.
FOS-855035	Weblinker is not restart-able after watchdog timeout abort or segment fault.
FOS-855050	Flash usage goes to 100% due to an abnormally large file ss.log and user can no longer login into switch.
FOS-855365	NPIV devices lost connections.
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-855535	BSL inventory is intermittently missing chassis.json file.
FOS-855788	Maps daemon (mdd) terminates during supportsave.
FOS-855962	Unexpected switch reboot after termination of lldpd process.
FOS-855995	Zoning got stuck in a bad state and hung. This lead to a long waiting period and panic after multiple zone changes were made via CLI.
FOS-856210	Asic Data is no longer properly collected during supportsave.
FOS-856244	Switch reports "400 Bad Request" for GET /rest/running/brocade-chassis/chassis for all users
FOS-856472	Flash usage is close to full and observing large /var/log/syslog.* files.
FOS-856476	CLI fanshow shows FAN absent when re-inserted.
FOS-856702	E-Ports cannot come online and shows incorrect VC assignment
FOS-856789	Unexpected termination of fclagd led to cold recovery
FOS-856971	REST API reports blank defined zone configuration while there is zone configured on the switch.
FOS-856993	CLI "scgconfig --delete --force" reports " ‘Error: No Device is Managed by ESRS’"
FOS-856998	Ports stuck in G-Port after removed D-port configuration.
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-857546	Multiple 40Ge ports logged link down/offline that led to a double kernal panic and cold recovery.
FOS-857609	cald terminated during flow operation such as CLI "flow --show -feature fabinfo -srcdev "*" -egrport" and the performance data can no longer be gathered.

FOS-857638	Switch panic after cfs daemon (cfsd) holds large amount of memory.
FOS-857687	During large HA sync copy operations, switch encounters msd panic
FOS-857838	Switch panic showing HAM-1004 message "Processor rebooted - Software Fault: Kernel panic". With additional messages showing "Kernel tried to execute NX-protected page" and "BUG: unable to handle page fault for address: ffffc9...."
FOS-858004	While running FICON IO over an emulation enabled tunnel, observed FICON device selective reset.
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, and logs Raslog "KSWD -1002". The chassis may encounter an HA out of sync condition.
FOS-858851	User experience performance issue on Gen7 after code upgrade.
FOS-858865	Tunnel offline and then back online 4 minutes later
FOS-858950	Maps shows "0 mAmps" on SFP.
FOS-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-859473	Switch failed firmware upgrade to FOS v9.2.0 with TruFOS license error
FOS-859556	User may encounter "termination of snmpd" while performing an snmpwalk operation
FOS-859748	Duplicate PWWN exist in the FCR fabric, which resulted in degraded traffic and impacted customer end to end traffic .
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-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-860415	Daemon weblinker terminates and restarts, with no other impact to switch functionality.
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-860835	snmpd terminated due to segmentation fault.
FOS-860855	Supportsaves are failing to collect switch SS using SANnav.
FOS-860936	Detected termination of process 0.weblinker.fcg during a REST zoning API request.
FOS-861132	ipv6 gateway address is missing after code upgrade.

FOS-861134	Invalid port stats counters reported such as the inv_arb counter : er64_inv_arb 0 top_int : Invalid ARB 4292386144 bottom_int : Invalid ARB
FOS-861147	npd crashed as Standby CP was taking over as Active CP during firmwaredownload.
FOS-861360	Switch unexpectedly reboots due to termination of process fdmid.
FOS-861453	The "Statsclear" CLI command encounters Segmentation Fault
FOS-861577	IP filter activation fails on management interface
FOS-861585	Large sized firm_intg_mon.log.save file is observed.
FOS-861742	Class 2 PLOGI response during RDP Polling leads to switch panic with ASSERT.
FOS-861801	Customer may encounter the following raslog Message "HAM-1007 caused FFDC event, ffdcd.c, comp:raslogd" during firmwaredowngrade
FOS-861986	SNMP connUnitDomainId value in AG mode is shown as "11 11 00" instead of expected “11 11 11”.
FOS-862000	"relayconfig" command does not accept an FQDN value of greater than 40 characters for "rla_ip"
FOS-862037	Customer encounters issue with access to the switch via HTTP or HTTPS with error message "Unable to access the switch.”
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-862224	SNMP daemon terminates.
FOS-862251	REST GET on /brocade-supportlink/supportlink-anonymization incorrectly returns an empty list when data anonymization is disabled.
FOS-862733	Detected termination of a restartable daemon weblinker.
FOS-862741	In some occurrences, Slot column in Web Tools Switch Ports table is missing for Directors
FOS-862821	Observed link reset on F-ports while upgrading AG switch, resulting in lost path to some hosts.
FOS-862863	Hard zoning incorrectly enabled on FICON enabled switch with no zoning defined. All traffic will be blocked by the zoning checks.
FOS-862895	All Ethernet LAGs connected to a switch do not come online.
FOS-862948	SNMP requested for FEC Corrected rate, but received an invalid value.
FOS-863010	A chassis with FC32-X7-48 blade inserted is limited to 2k IT flows.
FOS-863077	The weblinker daemon memory usage continues to increase during SANnav monitoring and activities such as configupload start to fail.
FOS-863267	Extension platform observed DP panic and disruption of any IO running over that DP.
FOS-863340	Large number of empty *ipc* files observed under /tmp directory.
FOS-863404	The following Raslog message is logged even when the corresponding change is not successful - [ZONE-1044], 5229, SLOT 1 | FID 12, INFO,-ficon1, The Default Zone access mode is set to All Access.

FOS-863534	Compact flash utilization went up to >90%, and prevented firmware from committing.
FOS-863569	Kafka Schema bandwidth utilization, unit of measure, is denoted as outOctets and inOctets. But the actual unit of measure is "Words"
FOS-863661	Observed "Hasm Command Instantiation timed-out" resulting in Software Bootup Failure or detected termination of restartable daemons during boot time.
FOS-863896	Kernel panic observed when processing an RDP response
FOS-863898	TACACS+ user logs in, but only has reduced permissions.
FOS-864015	Firmware patch sanity check fails during installation of tcpdump patch build
FOS-864046	Switch responds with 'File copy failed' error message when ConfigDownload CAL API is called.
FOS-864106	Multiple daemon termination during supportsave collection.
FOS-864156	The ports on a switch to AG links fail to come online, and remain stuck at G-port on embedded switch.
FOS-864306	SNMP mib walk works properly for SNMPv3 configured with Auth and Priv protocols as MD5 and AES128 respectively. But it stops working if, while in this configuration, Auth protocol alone is changed and Priv protocol is kept as is to AES128.
FOS-864380	The switch unexpectedly rebooted due to "Detected termination of process lldpd".
FOS-864594	Spurious congestion reported as microburst episodes even though it's not running at greater than 70%.
FOS-864780	CLI firmwareshow shows an incorrect firmware version.
FOS-864968	DCC policy data support is not available in supportlink data collection
FOS-865109	configupload RestAPI call sometimes gives incorrect output.
FOS-865127	weblinker daemon terminated in a setup with ip storage.
FOS-865160	7810 VE Ports/Tunnel(s) reporting DEGRADED status, along with evidence of maximum WAN network packet size exceeded discards, after upgrading to FOS 9.1.0 or higher.
FOS-865397	CLI 'scgconfig --add' command fails.
FOS-866399	FICON Teradata read emulation started followed by RASLOG (FICN-1062) Ingress abort on the CHPID side switch.
FOS-866633	SCN queue overflow for Maps daemon (mdd).
FOS-866745	Standby CP encountered msd panic.
FOS-867112	After moving a device between two edge fabrics, a duplicate PWWN is detected.
FOS-867151	Switch unexpectedly rebooted due to the termination of the zone daemon and/or name server daemon.
FOS-867487	Connection between device and switch is not stable with Internet Storage Name Service (iSNS).
FOS-867918	MAPS report 0uW RXP while F port online
FOS-867953	REST API call to brocade-interface/fibrechannel responds with invalid data.
FOS-868067	Tunnel down and DP reboot after EXDP-5024
FOS-868199	The FDMI information is not currently being populated under the Dynamic Portname.
FOS-868304	A LUN discovery failure after PLOGI frames sent on the EX-port are dropped.
FOS-868397	Switch repeatedly reporting WEBD-1008 messages or other raslog entries. This continuous logging appears to be slowing down the system considerably and has, in some instances, led to kernel panics.

FOS-868468	The name server daemon is terminating after consuming a significant amount of memory.
FOS-868476	Observed a significant delay when the proxy router updates device information across two fabrics connected via FC routing (one for hosts and one for storage).
FOS-868588	Kernel panic triggered by accessing invalid freed memory.
FOS-868713	Devices lost communication and ports turned into a G-Port.
FOS-868771	The CLI command `firmwarecleaninstall` fails with the error message: "FirmwareCleaninstall failed, Rebooting system to recover."
FOS-868809	Switch panic during HA reboot.
FOS-869412	FCoE links unable to form LAG.
FOS-869878	Access gateway daemon (agd) panic and F ports stuck at G ports.
FOS-869883	Deskew value for the port connected in the trunk is shown as zero
FOS-869938	The CLI "fpgaupgrade" on the FC32-X7-48 blade failed with the following error message: ERROR: Missing blade id (218) (slot=4) for sanity check operation
FOS-870130	Fabric daemon terminates with a misbehaving device connected.
FOS-870353	Switch Panics and switch is left in disabled state during FC LAG enable.
FOS-870527	The list of firmwaredownload Blocking conditions, in the event of a firmwaredownload failure, may be truncated and the list may not be complete
FOS-870724	Dynamic LAG did not come up / recover following system reboot / power cycle.
FOS-870943	SNMPv3 Auth Password and Priv Password fields are not enforced to be mandatory entry fields during their updates from Web Tools
FOS-871061	Application Server daemon (appsrvrd) terminated.
FOS-871204	FCoE port-channel traffic is not balanced.
FOS-871556	Update current Eula text for more comprehensive coverage
FOS-871753	Switches end up with "Bad Certificate" when the concatenated root certs were pushed to FOS through BSL or SANnav.
FOS-871910	Access Gateway (AG) and Fibre Channel Routing (FCR) will not function in a fabric that includes a Brocade switch assigned with the new OUI (B8-CE-ED).
FOS-872299	Incorrect TruFOS expiration message on G610 with FOS v9.2.2

10.2 Closed without Code Changes in FOS v10.0.0

Defect ID	**Description**
FOS-633099	Using the SSH syntax "ssh admin@<ip address> <cli command>" in LS specific context, generates the output for the default switch.
FOS-804058	porterrshow does not display TX frames.
FOS-822366	cald terminated and kernel paniced during supportsave collections.
FOS-836443	IO flow statistics are not displayed when the lookup is done at the VM entity id.
FOS-839967	User may encounter E-ports get segmented with reason - Zone Merge Internal Error
FOS-843291	[PMGR-1006], 10392, SLOT 1 | CHASSIS, WARNING, , Attempt to move port(s) -1 on slot -1 to switch 21 failed. Error message: Not able to set port config on the switch. OR [HAM-1007], 2711, FFDC | CHASSIS, CRITICAL, , Need to reboot the system for recovery, reason: Software Bootup Failure:LS config timed out;
FOS-844810	Observed "termination of mdd" during fcippathtest

FOS-844986	Observed some unexpected messages such as "/var/tmp/rpm-tmp.CNGUPL: line 2: [: !=: unary operator expected" during firmware downgrade from 9.2.0 to 9.1.1x.
FOS-845513	Benign warning messages may get displayed on the console about being unable to delete non-existent files, even though firmware upgrade is successful
FOS-846503	REST PATCH on various /brocade-logging leafs with invalid values incorrectly return 204 No Content.
FOS-848254	CPU utilization at 100% during snmp polling.
FOS-848281	The applications that parse the improperly encoded XML responses can encounter XML parsing failures.
FOS-848800	Following a code upgrade, a VE port is in disabled state, even though it was not manually disabled.
FOS-849244	Switch ports get erroneously disabled during migration.
FOS-849917	On a G730 there is a probability of the switch getting into Credit loss (GE5-1012). Subsequent Link reset (GE5-1014) recovers the credit loss.
FOS-849948	EM-1014 raslog states unable to read sensor on PS 1.
FOS-850131	Configupload doesn't fail or error out when the server side file path is non existent.
FOS-850134	This issue is specific to Gen7 chassis systems (X7-4, X7-8). Traffic optimizer related software verify errors (RAS-1004) and kernel panic might be observed.
FOS-850507	Applications such as SANNav display incorrect switch model name.
FOS-850525	Applications such as SANnav, snmp churning errors about WWN change approximately every 12 minutes.
FOS-851275	Panic on Standby CP when booting to Active on new firmware after hafailover during concurrent firmwaredownload.
FOS-852416	The show, set operation with CLI "syslogadmin" and "auditcfg" commands are failing with "Unable to retrieve ...". Also on a director, standby CP Supportsave cannot be retrieved.
FOS-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-852724	Compact flash run out of space and observed large sized ss_util_err.log and ss_util_err.log.old files.
FOS-854060	Syslogadmin: IPv6 Syslog server IP is logging even after IPv6 addresses are removed from the switch.
FOS-854095	After a non-critical daemon failed, it did not restart successfully and the switch persistently lost HA sync.
FOS-854143	Kernel panic when 64G oversubscription is introduced in the fabric with many neighbors on the same chip.
FOS-854359	Tsclockserver: RAS TS-1002 is flooded on non-principal switches when an active NTP server goes offline.
FOS-854497	Observed "vpackage" on one of the standby partitions after firmwaredownload.
FOS-854609	Adding default static route results in error message. "There are max number of nexthop gateways for a given route already."
FOS-855888	Flash usage is close to full and observing large /var/log/syslog.* files.
FOS-858226	Observed assert failure and switch panic during a third party storage device POR or a continuous F-port flapping.
FOS-858339	Closing array bracket is missing. Invalid JSON data returned.
FOS-858457	Node symbolic name registration query is causing nameserver daemon (nsd) to terminate.

FOS-858752	On our new X7-8 with FOS v9.1.1d the field "inet-address" randomly disappears from queries to REST API endpoint "/rest/running/brocade-chassis/management-ethernet-interface" for the standby CP. The field is always there for the currently active CP.
FOS-859229	UFCS daemon reports message queue full.
FOS-859282	CLI "flow" fails with Segmentation fault and traffic optimizer dashboards no longer work as expected.
FOS-859350	SAN switch monitoring tools via SNMP do not function properly
FOS-859429	mdd termination during port related configuration.
FOS-860050	Observed Kernel panic during ISL configuration on G730/G710.
FOS-860168	The current traffic configuration may not be leveraging its maximum capabilities.
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-860255	High memory usage MAPS alert observed [MAPS-1003]
FOS-860262	Kernel panic while storing trace data.
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-860824	SANnav generates unnecessary SNMP notifications.
FOS-861858	IP address on a MXG610s embedded switch in VLAN mode is reported as 0.0.0.0
FOS-862189	User is unable to upload configuration file using anonymous ftp account.
FOS-863019	Supportsave, firmware upgrade and other support commands stop working
FOS-864085	Configuring an LDAP primary and local backup with incomplete configurations or if the server is unreachable results in the disabling of all access to the switch, including console access.
FOS-864483	CLI "dnsconfig --show" is empty.
FOS-864707	Incorrect data returned when performing an snmpbulkget with multiple OIDs
FOS-864811	Firmware update failed with SANnav, reporting the error "Known Host does not exist."
FOS-866953	Certain 32G speed devices are unable to connect to the G610.
FOS-868299	Role configuration updates (create/modify) using the REST URI "/rest/running/brocade-security/role-config" fail intermittently.
FOS-869114	Switch is no longer being monitored by management application .
FOS-871661	Target Driven Zones are not getting created or removed and require follow-up AAPZ or RAPZ operations.

10.3 Open in FOS v10.0.0

Defect ID	Description
FOS-823999	Flow monitor reports only SCSI stats for an IT flow with SCSI and NVMe exchanges across time.
FOS-846184	Timestamp of a port offline event is not consistent with its fenced timestamp message.
FOS-851800	Ipfilter 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-854015	trafopt --show -flow -pg PG_SYSTCDEFAULT shows no Rx numbers.
FOS-859318	Firmware migration from SANnav fails when there is a Weblinker restart.
FOS-861742	Class 2 PLOGI response during RDP Polling leads to switch panic with ASSERT.
FOS-867544	SSH login via device flow using federated authentication fails (times out).
FOS-869012	Devices stopped communication and Class 3 frame timeout logged on long-distance ISLs
FOS-869494	Distribution of password DB will be blocked if receiver has 'consoleaccess' password configuration enabled and sender has it disabled.
FOS-869548	REST does not have distance parameter under long distance config.
FOS-869905	Webserver will not restart while updating cipher for HTTPS.
FOS-870909	Inconsistency in the user/password configs defaulted via sboot on standby CP vs sboot on active CP/switches
FOS-871070	ETH statistics aren't cleared when using REST API.
FOS-871316	Trunk E-Port speed is incorrect in SanFI output, when different speed trunks are present between switches.
FOS-871704	"sanfi -switch -summary" CLI does not show the correct count of E-Ports/LISL links if multiple LISLs are present.
FOS-871874	'portcfgtrunkport' CLI without arguments will return invalid message such as 'Port -2 not present'.
FOS-871949	'sys_flow_monitor show stats' CLI indicates the flow direction is reversed for TX and RX.
FOS-871975	SanFI data information is not updated properly with no proper warning messages indicating vCenter connection timeout.
FOS-872020	SHA1 and DSS cryptography checks for the configured TLS ciphers will not function properly and blocking messages will not be listed.
FOS-872069	Not able to discover the switch in SANnav.
FOS-872083	Missing Ethernet IP and name of the switch in 'fabricshow' CLI output when issued during high CPU load.
FOS-872092	May see "rcmd: getaddrinfo: Temporary failure in name resolution" during non-disruptive firmware migration. No functional impact.
FOS-872103	Firmwaredownload from FOS 10.0.0 to FOS 9.2.2 when SX6 is present may take longer to complete. On rare occasions, it might lead to I/O timeouts.
FOS-872378	Gen6+ Chassis with v2 license will allow upgrade to FOS 10.0. Downgrade is blocked due to legacy v2 license.
FOS-872390	MAPS reports STATUS TIME and FIRST RESPONSE time threshold violations with invalid values for the 10-second rules once for an IT flow.

FOS-872392	Port blades remain powered off with the reason "Not Enough Power," even after the power has been fully restored.

Revision History

Version	Summary of changes	Publication date
1	Initial version of document	09/22/2025
2	Updated with OUI section.	10/22/2025
2	Updated sections Migrating to FOS v10.0.0 and Miscellaneous	12/05/2025

BROADCOM®