

Brocade Fabric OS v7.1.2b

Release Notes v1.0

August 14, 2014

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.1.2b Release Notes v1.0	Initial release	August 14, 2014

© 2014 Brocade Communications Systems, Inc. All Rights Reserved.

ADX, AnyIO, Brocade, Brocade Assurance, the B-wing symbol, DCX, Fabric OS, ICX, MLX, MyBrocade, OpenScript, VCS, VDX, and Vyatta are registered trademarks, and HyperEdge, The Effortless Network, and The On-Demand Data Center are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned may be trademarks of their respective owners.

Notice: This document is for informational purposes only and does not set forth any warranty, expressed or implied, concerning any equipment, equipment feature, or service offered or to be offered by Brocade. Brocade reserves the right to make changes to this document at any time, without notice, and assumes no responsibility for its use. This informational document describes features that may not be currently available. Contact a Brocade sales office for information on feature and product availability. Export of technical data contained in this document may require an export license from the United States government.

Contents

Overview	5
Warning – Applicable only if upgrading from FOS v7.1.0:.....	5
Resolution of Important Defects.....	5
New Features & Support	5
Optionally Licensed Software.....	6
Temporary License Support	8
Other Licensing Changes.....	8
Supported Switches.....	9
Standards Compliance	9
Technical Support.....	9
FOS Migration Considerations	11
FOS Upgrade and Downgrade Special Considerations.....	11
Recommended Migration Paths to FOS v7.1.2b	11
Important Notes.....	13
Brocade Network Advisor Compatibility	13
DCFM Compatibility	13
WebTools Compatibility	14
SMI Compatibility	14
Fabric OS Compatibility	14
Blade Support.....	16
Scalability.....	21
Other Important Notes and Recommendations	21
Adaptive Networking/Flow-Based QoS Prioritization	21
Access Gateway	21
Brocade HBA/Adapter Compatibility	22
D-Port.....	22
Edge Hold Time.....	22
Encryption Behavior for the Brocade Encryption Switch (BES) and FS8-18	23
FCIP (Brocade 7800 and FX8-24).....	25
FCoE/DCB/CEE (Brocade 8000 and FCOE10-24).....	26
FCR and Integrated Routing.....	28
Forward Error Correction (FEC)	28
FICON.....	28
FL_Port (Loop) Support.....	28
ICLs on DCX/DCX-4S	28
Licensing	29
Native Connectivity (M-EOS interoperability).....	29
Port Initialization	29

Port Mirroring	29
Port Statistics	29
Virtual Fabrics	29
WebTools	30
Zoning	30
Miscellaneous	30
Defects	32
Closed with Code Change in Fabric OS v7.1.2b	32
Closed with Code Change in Fabric OS v7.1.2a	34

Overview

Fabric OS (FOS) v7.1.2a is a patch release based on FOS v7.1.2. All hardware platforms and features supported in FOS v7.1.2 are also supported in FOS v7.1.2a. This release also contains fixes for many defects including those from the FOS v7.1.2 maintenance releases.

Warning – Applicable only if upgrading from FOS v7.1.0:

Before upgrading the firmware to FOS v7.1.2a from FOS v7.1.0, you must run the **supportSave** command to save any existing error log information. Once the switch is upgraded to FOS v7.1.2a, any previously existing error log entries on the switch will be permanently lost - only new error log entries created while running FOS v7.1.2a will be retained.

Note: This warning is not applicable if the current firmware version is not FOS v7.1.0. For example, if the upgrade is being performed from FOS v7.1.1x, FOS v7.1.0a, FOS v7.1.0b, FOS v7.1.0c, FOS v7.0.x to FOS v7.1.2a, the existing error log entries will be preserved even after upgrading to FOS v7.1.2a. Please refer to “FOS Migration Considerations” section of this document for additional considerations.

Resolution of Important Defects

Defect 484414: Under rare conditions, Access Gateway(AG) entries stay in management server (MS) database even after removing them from the fabric.

Defect 507447: Switch throughput utilization graph freezes.

Defect 513920: CVE-2014-0224: OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.

New Features & Support

In addition to fixes for defects, there is new support in FOS v7.1.2 including:

- Support disabling the Decision Feedback Equalization (DFE) mode on selected ports for 8Gb FC ports on Gen5 platforms.
 - Supported through the new CLI command *portCfgNonDfe* only.
 - Disabling DFE mode is only required to support attachment of select LTO tape devices to Brocade Gen 5 platforms when the tape devices do not comply with FC standards for fill word behavior and the fill word behavior cannot be changed on the tape device.

Optionally Licensed Software

Fabric OS v7.1 includes all basic switch and fabric support software, as well as optionally licensed software that is enabled via license keys.

Optionally licensed features supported in FOS v7.1 include:

Brocade Ports on Demand—Allows customers to instantly scale the fabric by provisioning additional ports via license key upgrade. (Applies to select models of switches).

Brocade Fabric or E_Port or Full Fabric— This license enables a switch to connect to a multi-switch fabric via E_Ports, forming ISL connections.

Note: This license is only required on select embedded switch models and the Brocade 300, and does not apply to other fixed-port switches or chassis-based platforms.

Brocade Extended Fabrics—Provides greater than 10km of switched fabric connectivity at full bandwidth over long distances (depending on the platform this can be up to 3000km)

Brocade ISL Trunking— Provides the ability to aggregate multiple physical links into one logical link for enhanced network performance and fault tolerance. Also includes Access Gateway ISL Trunking on those products that support Access Gateway deployment.

Brocade Advanced Performance Monitoring—Enables performance monitoring of networked storage resources. This license includes the Top Talkers feature.

Brocade Fabric Watch — Monitors mission-critical switch operations and provides notification if established limits or thresholds are exceeded. Fabric Watch includes Port Fencing capabilities.

FICON Management Server— Also known as “CUP” (Control Unit Port), enables host-control of switches in Mainframe environments.

Enhanced Group Management — This license enables full management of devices in a data center fabric with deeper element management functionality and greater management task aggregation throughout the environment. This license is used in conjunction with Brocade Network Advisor application software and is applicable to all FC platforms supported by FOS v7.0 or later.

Note: This license is enabled by default on all 16G FC platforms, and on DCX and DCX-4S platforms that are running Fabric OS v7.0.0 or later.

Adaptive Networking with QoS—Adaptive Networking provides a rich framework of capability allowing a user to ensure high priority connections obtain the bandwidth necessary for optimum performance, even in congested environments. The QoS SID/DID Prioritization and Ingress Rate Limiting features are included in this license, and are fully available on all 8Gb and 16Gb platforms.

Note: Brocade 6520 does not require the Adaptive Networking with QoS license to enable the capabilities associated with this license. These capabilities are included by default on the Brocade 6520.

Server Application Optimization (SAO) — When deployed with Brocade Server Adapters, this license optimizes overall application performance for physical servers and virtual machines by extending virtual channels to the server infrastructure. Application specific traffic flows can be configured, prioritized, and optimized throughout the entire data center infrastructure. This license is not supported on the Brocade 8000.

Note: Brocade 6520 does not require the SAO license to enable the capabilities associated with this license. These capabilities are included by default on the Brocade 6520.

Integrated Routing— This license allows any port in a DCX 8510-8, DCX 8510-4, Brocade 6510, Brocade 6520, DCX-4S, DCX, 5300, 5100, 7800, or Brocade Encryption Switch to be configured as an EX_Port or VEX_Port (on some platforms) supporting Fibre Channel Routing. This eliminates the need to add a dedicated router to a fabric for FCR purposes.

Encryption Performance Upgrade — This license provides additional encryption processing power. For the Brocade Encryption Switch or a DCX/DCX-4S/DCX 8510-8/DCX 8510-4, the Encryption Performance License can be installed to enable full encryption processing power on the BES or on all FS8-18 blades installed in a DCX/DCX-4S/DCX 8510-8/DCX 8510-4 chassis.

DataFort Compatibility — This license is required on the Brocade Encryption Switch or DCX/DCX-4S/DCX 8510-8/DCX 8510-4 with FS8-18 blade(s) to read and decrypt NetApp DataFort-encrypted disk and tape LUNs. DataFort Compatibility License is also required on the Brocade Encryption Switch or DCX/DCX-4S/DCX 8510-8/DCX 8510-4 Backbone with FS8-18 Encryption Blade(s) installed to write and encrypt the disk and tape LUNs in NetApp DataFort Mode (Metadata and Encryption Algorithm) so that DataFort can read and decrypt these LUNs. DataFort Mode tape encryption and compression is supported beginning with the FOS v6.2.0 release on DCX platforms. Availability of the DataFort Compatibility license is limited; contact your vendor for details.

Brocade 8000 FC Ports on Demand — This license enables all eight FC ports on the Brocade 8000.

Advanced Extension – This license enables two advanced extension features: FCIP Trunking and Adaptive Rate Limiting. The FCIP Trunking feature allows multiple IP source and destination address pairs (defined as FCIP Circuits) via multiple 1GbE or 10GbE interfaces to provide a high bandwidth FCIP tunnel and failover resiliency. In addition, each FCIP circuit supports four QoS classes (Class-F, High, Medium and Low Priority), each as a TCP connection. The Adaptive Rate Limiting feature provides a minimum bandwidth guarantee for each tunnel with full utilization of the available network bandwidth without impacting throughput performance under high traffic load. This license is available on the 7800 and the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis.

10GbE FCIP/10G Fibre Channel – This license enables the two 10GbE ports on the FX8-24 or the 10G FC capability on FC16-xx blade ports. On the Brocade 6510 and Brocade 6520, this license enables 10G FC ports. This license is available on the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 on an individual slot basis.

- **FX8-24:** With this license assigned to a slot with an FX8-24 blade, two additional operating modes (in addition to 10 1GbE ports mode) can be selected; 10 1GbE ports and 1 10GbE port, or 2 10GbE ports
- **FC16-xx:** Enables 10G FC capability on an FC16-xx blade in a slot that has this license
- **Brocade 6510, Brocade 6520:** Enables 10G FC capability on the switch

Advanced FICON Acceleration – This licensed feature uses specialized data management techniques and automated intelligence to accelerate FICON tape read and write and IBM Global Mirror data replication operations over distance, while maintaining the integrity of command and acknowledgement sequences. This license is available on the 7800 and the DCX/DCX-4S/DCX 8510-8/DCX 8510-4 for the FX8-24 on an individual slot basis.

7800 Upgrade – This license allows a Brocade 7800 to enable 16 FC ports (instead of the base four ports) and six GbE ports (instead of the base two ports). This license is also required to enable additional FCIP tunnels and also for advanced capabilities like tape read/write pipelining.

ICL 16-link, or Inter Chassis Links – This license provides dedicated high-bandwidth links between two Brocade DCX chassis, without consuming valuable front-end 8Gb ports. Each chassis must have the 16-link ICL license installed in order to enable the full 16-link ICL connections. Available on the DCX only.

ICL 8-Link – This license activates all eight links on ICL ports on a DCX-4S chassis or half of the ICL bandwidth for each ICL port on the DCX platform by enabling only eight links out of the sixteen links available. This allows users to purchase half the bandwidth of DCX ICL ports initially and upgrade with an additional 8-link license to utilize the full ICL bandwidth at a later time. This license is also useful for environments that wish to create ICL connections between a DCX and a DCX-4S, the latter of which cannot support more than 8 links on an ICL port. Available on the DCX-4S and DCX platforms only.

ICL POD License – This license activates ICL ports on core blades of DCX 8510 platforms. An ICL 1st POD license only enables half of the ICL ports on CR16-8 core blades of DCX 8510-8 or all of the ICL ports on CR16-4 core blades on DCX 8510-4. An ICL 2nd POD license enables all ICL ports on CR16-8 core blades on a DCX 8510-8 platform. (The ICL 2nd POD license does not apply to the DCX 8510-4.)

Enterprise ICL (EICL) License – The EICL license is required on a Brocade DCX 8510 chassis when that chassis is participating in a group of five or more Brocade DCX 8510 chassis connected via ICLs.

Note that this license requirement does not depend upon the total number of DCX 8510 chassis that exist in a fabric, but only on how many chassis are interconnected via ICLs. This license is only recognized/displayed when operating with FOS v7.0.1 but enforced with FOS v7.1.0 or later.

Note: The EICL license supports a maximum of nine DCX 8510 chassis connected in a full mesh topology or up to ten DCX 8510 chassis connected in a core-edge topology.

Fabric Insight/Fabric Vision License - The Fabric Vision license (included in some software bundles) is being introduced in 2013 to enable new functionality in FOS v7.2 and later releases. When installed on a switch operating with FOS v7.1.x, the `licenseshow` command will display this license as the “Fabric Insight license”. When running FOS v7.1.x or earlier, existence of this license does not affect any functionality on the switch.

Temporary License Support

The following licenses are available in FOS v7.1 as Universal Temporary or regular temporary licenses:

- Fabric (E_Port) license
- Extended Fabric license
- Trunking license
- High Performance Extension license
- Advanced Performance Monitoring license
- Adaptive Networking license
- Fabric Watch license
- Integrated Routing license
- Server Application Optimization license
- Advanced Extension license
- Advanced FICON Acceleration license
- 10GbE FCIP/10G Fibre Channel license
- FICON Management Server (CUP) license
- Enterprise ICL license

Note: Temporary Licenses for features available on a per slot basis enable the feature for any and all slots in the chassis.

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

Other Licensing Changes

- The capabilities associated with the Adaptive Networking and SAO licenses are included by default on the Brocade 6520. Hence these licenses are not applicable to the Brocade 6520 platform.

Supported Switches

- Fabric OS v7.1 supports the Brocade 300, 5410/5424/5430/5450/5460/5470/5480/NC-5480, 5100, 5300, VA-40FC, Brocade Encryption Switch (BES), DCX/DCX-4S, 8000, 7800, 6505, 6510, 6520, DCX 8510-8 and DCX 8510-4.

Access Gateway mode is also supported by Fabric OS v7.1, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 8000, 5450, 5430, 5460, 5470, 5480, NC-5480, M5424, 6510, 6505.

Standards Compliance

This software conforms to the Fibre Channel Standards in a manner consistent with accepted engineering practices and procedures. In certain cases, Brocade might add proprietary supplemental functions to those specified in the standards. For a list of FC standards conformance, visit the following Brocade Web site: <http://www.brocade.com/sanstandards>

The Brocade 8000 and FCOE10-24 blade conform to the following Ethernet standards:

- IEEE 802.1D Spanning Tree Protocol
- IEEE 802.1s Multiple Spanning Tree
- IEEE 802.1w Rapid reconfiguration of Spanning Tree Protocol
- IEEE 802.3ad Link Aggregation with LACP
- IEEE 802.3ae 10G Ethernet
- IEEE 802.1Q VLAN Tagging
- IEEE 802.1p Class of Service Prioritization and Tagging
- IEEE 802.1v VLAN Classification by Protocol and Port
- IEEE 802.1AB Link Layer Discovery Protocol (LLDP)
- IEEE 802.3x Flow Control (Pause Frames)

The following draft versions of the Converged Enhanced Ethernet (CEE) and Fibre Channel over Ethernet (FCoE) Standards are also supported on the Brocade 8000 and FCOE10-24 blade:

- IEEE 802.1Qbb Priority-based Flow Control
- IEEE 802.1Qaz Enhanced Transmission Selection
- IEEE 802.1 DCB Capability Exchange Protocol (Proposed under the DCB Task Group of IEEE 802.1 Working Group)
- FC-BB-5 FCoE (Rev 2.0)

Technical Support

Contact your switch supplier for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information immediately available:

1. General Information

- Technical Support contract number, if applicable
- Switch model
- Switch operating system version
- Error numbers and messages received
- **supportSave** command output and associated files
 - For dual CP platforms running FOS v6.2 and above, the **supportsave** command gathers information from both CPs and any AP blades installed in the chassis
- Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions

- Description of any troubleshooting steps already performed and the results
- Serial console and Telnet session logs
- Syslog message logs

2. Switch Serial Number

The switch serial number is provided on the serial number label, examples of which are shown here:



The serial number label is located as follows:

- Brocade Encryption Switch, VA-40FC, 300, 5100, 5300, 6510, 6505, 6520 — On the switch ID pull-out tab located on the bottom of the port side of the switch
- Brocade 7800 — On the pull-out tab on the front left side of the chassis underneath the serial console and Ethernet connection and on the bottom of the switch in a well on the left side underneath (looking from front)
- Brocade 8000 — On the switch ID pullout tab located inside the chassis on the port side on the left and also on the bottom of the chassis
- Brocade DCX, DCX 8510-8 — Bottom right of the port side
- Brocade DCX-4S, DCX 8510-4 — Back, upper left under the power supply

3. 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, except for the Brocade DCX/DCX-4S and DCX 8510-8/DCX 8510-4. For the Brocade DCX/DCX-4S and DCX 8510-8/DCX 8510-4 access the numbers on the WWN cards by removing the Brocade logo plate at the top of the non-port side. The WWN is printed on the LED side of both cards.

1. License Identifier (License ID)

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

Use the **licenseIdShow** command to display the License Identifier.

FOS Migration Considerations

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

FOS Upgrade and Downgrade Special Considerations

DCX/DCX-4S units running any FOS v7.0.x or FOS v7.1.0x can be non-disruptively upgraded to FOS v7.1.2b. This upgrade is non-disruptive to both FC and FCoE traffic (when using FCOE10-24 blades).

FR4-18i and FC10-6 blades are not supported on DCX/DCX-4S with FOS v7.1 or later. Hence these blades must be removed from the chassis before upgrading the firmware to FOS v7.1.2b.

Any firmware activation on Brocade 7800, or DCX, DCX-4S, DCX 8510-8, DCX 8510-4 with FX8-24 will disrupt I/O traffic on the [FCIP links](#).

Disruptive upgrades to Fabric OS v7.1.2b are allowed and supported from FOS 6.4.x (up to a two-level migration) using the optional “-s” parameter with the *firmwaredownload* command.

If there are multiple node EGs (encryption groups) in a fabric, please complete *firmwaredownload* on one node at a time before downloading on another node.

The Brocade 8000 does not support non-disruptive hot code loads (HCL). Upgrading the Brocade 8000 to FOS v7.1.2b will be disruptive to the I/O through the switch.

Recommended Migration Paths to FOS v7.1.2b

Migrating from FOS v7.1.1x

Any 8G or 16G platform running any FOS v7.1.1x (FOS v7.1.1, FOS v7.1.1a, FOS v7.1.0b, FOS v7.1.0c) firmware can be non-disruptively upgraded to FOS v7.1.2b.

Migrating from FOS v7.1.0

Warning

Before upgrading the firmware to FOS v7.1.2b from FOS v7.1.0, you must run the *supportSave* command to save any existing error log information. Once the switch is upgraded to FOS v7.1.2b, any previously existing error log entries on the switch will be permanently lost - only new error log entries created while running FOS v7.1.2b will be retained.

Any 8G or 16G platform running FOS v7.1.0 can be non-disruptively upgraded to FOS v7.1.2b. However, any previously existing error log entries with FOS v7.1.0 will be permanently lost once upgraded to FOS v7.1.2b.

Migrating from FOS v7.1.0x

Any 8G or 16G platform running any FOS v7.1.0x (FOS v7.1.0a, FOS v7.1.0b, FOS v7.1.0c) firmware can be non-disruptively upgraded to FOS v7.1.2b.

Migrating from FOS v7.0.1x or 7.0.2x

Any 8G or 16G platform running any FOS v7.0.1x /FOS v7.0.2x firmware can be non-disruptively upgraded to FOS v7.1.2b. However, users must pay close attention to the following before upgrading the DCX 8510 platforms to FOS v7.1.2b:

If the upgrade on a DCX 8510 from FOS v7.0.1x/FOS v7.0.2x to FOS v7.1.2b is blocked due to the absence of the EICL license, users must first install the EICL license on the DCX 8510 and then proceed with upgrading the firmware to FOS v7.1.2b.

Migrating from FOS v7.0.0x

Any 8G or 16G platform running any FOS v7.0.0x firmware can be non-disruptively upgraded to FOS v7.1.2b. However, users must pay close attention to the following before upgrading the DCX 8510 platforms to FOS v7.1.2b:

If the upgrade on a DCX 8510 from FOS v7.0.0x to FOS v7.1.2b is blocked due to the absence of the EICL license, users must first upgrade the DCX 8510 to FOS v7.0.1x or later, install the EICL license on the DCX 8510, and then proceed with upgrading the firmware to FOS v7.1.2b.

Migrating from FOS v6.4.x

DCX/DCX-4S units running any FOS v6.4.x firmware must be upgraded to FOS v7.0.x before they can be non-disruptively upgraded to FOS v7.1.2b.

Any 8G platforms (other than DCX/DCX-4S) that are currently operating at lower than FOS v6.4.1a must be upgraded to FOS v6.4.1a or later, they then must be upgraded to FOS v7.0.x, before non-disruptively upgrading to FOS v7.1.2b. Upgrading these platforms from any FOS V6.4.x release **lower than FOS v6.4.1a** to **FOS v7.0.x will cause disruption to FC traffic.**

Any 8G platform operating at FOS v6.4.1a or later versions of FOS v6.4.x must be upgraded to FOS v7.0.x or later before non-disruptively upgrading to FOS v7.1.2b.

Migrating from FOS v6.4.1_fcoe1

Units running FOS v6.4.1_fcoe1 must be upgraded to FOS v7.0.x before non-disruptively upgrading to FOS v7.1.2b.

Important Notes

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

Brocade Network Advisor Compatibility

Brocade® Network Advisor provides the industry's first unified network management solution for data, storage, and converged networks. It supports Fibre Channel Storage Area Networks (SANs), Fibre Channel over Ethernet (FCoE) networks, Layer 2/3 IP switching and routing networks, wireless networks, application delivery networks, and Multiprotocol Label Switching (MPLS) networks. In addition, Brocade Network Advisor supports comprehensive lifecycle management capabilities across different networks through a seamless and unified user experience. It is the next-generation successor product to legacy Brocade management products (Brocade Data Center Fabric Manager (DCFM), Brocade Fabric Manager (FM) and Brocade Enterprise Fabric Connectivity Manager (EFCM)).

Brocade Network Advisor is available with flexible packaging and licensing options for a wide range of network deployments and for future network expansion. Brocade Network Advisor 12.0.0 is available in

- SAN-only edition
- IP-only edition
- SAN+IP edition.

For SAN Management, Network Advisor 12.0 is available in three editions:

- **Network Advisor Professional:** a fabric management application that is ideally suited for small-size businesses that need a lightweight management product to manage their smaller fabrics. It manages one FOS fabric at a time and up to 1,000 switch ports. It provides support for Brocade FC switches, Brocade HBAs / CNAs, and Fibre Channel over Ethernet (FCoE) switches.
- **Network Advisor Professional Plus:** a SAN management application designed for medium-size businesses or departmental SANs for managing up to thirty-six physical or virtual fabrics (FOS) and up to 2,560 switch ports. It supports Brocade backbone and director products (DCX 8510-4/DCX-4S, 48Ks, etc.), FC switches, Fibre Channel Over IP (FCIP) switches, Fibre Channel Routing (FCR) switches/ Integrated Routing (IR) capabilities, Fibre Channel over Ethernet (FCoE) / DCB switches, and Brocade HBAs / CNAs.
- **Network Advisor Enterprise:** a management application designed for enterprise-class SANs for managing up to thirty-six physical or virtual fabrics and up to 9,000 switch ports. Network Advisor SAN Enterprise supports all the hardware platforms and features that Network Advisor Professional Plus supports, and adds support for the Brocade DCX Backbone (DCX 8510-8/DCX) and Fiber Connectivity (FICON) capabilities.

More details about Network Advisor's new enhancements can be found in the Network Advisor 12.0 Release Notes, Network Advisor 12.0 User Guide, and Network Advisor 12.0 Installation, Migration, & Transition Guides.

Note:

Brocade Network Advisor 12.0 is required to manage switches running FOS 7.1 or later, and also to manage the Brocade 6520 platform.

The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.

DCFM Compatibility

DCFM is not qualified with and does not support the management of switches operating with FOS v7.0 and later firmware versions. **You must first upgrade DCFM to Network Advisor 12.0 if you are planning to upgrade devices to FOS v7.1.0 or later.**

WebTools Compatibility

FOS v7.1.2b is qualified and supported with Oracle JRE 1.7.0 update 25, update 45, and update 51. Launching WebTools with Oracle JRE 1.7.0 update 51 through Brocade Network Advisor is only supported on version 12.1.5 or later. With JRE 1.7.0 update 51, users could see some browser warning messages that can be ignored.

SMI Compatibility

- It is important to note that host SMI-S agents cannot be used to manage switches running FOS v7.1.0. If users want to manage a switch running FOS v7.1.0 using SMI-S interface, they must use Brocade Network Advisor's integrated SMI agent.

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. Brocade recommends using 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 prior to installing on your switch. Use only FOS versions that are supported by the provider.

For a list of the effective end-of-life dates for all versions of Fabric OS, visit the following Brocade Web site:

http://www.brocade.com/support/end_of_life.jsp

Supported Products and FOS Interoperability	
Brocade 2000-series switches	Not supported, end of support (December 2007)
Brocade 3200, 3800	Direct E-port connections are not supported – must use FCR
Brocade 3000	Direct E-port connections are not supported – must use FCR v3.2.1c ³
Silkworm 3016, 3250, 3850, 3900, 24000	Direct E-port connections are not supported – must use FCR
4100, 4900, 7500, 7500e, 5000, 200E, 48K Brocade 4012, 4016, 4018, 4020, 4024, 4424	v6.2.2 or later ⁶
Silkworm 12000	v5.0.x ³ (Direct E_Port connections are not supported – must use FCR)
Brocade 5410, 5480, 5424, 5450, 5460, 5470, NC-5480	v6.2.0 or later ⁶
Brocade DCX, 300, 5100, 5300	v6.1.0e and later ^{2 6 8}
VA-40FC	v6.2.1_vfc ⁶ , v6.2.2 or later ⁶
Brocade DCX-4S	v6.2.0 or later ^{6 8}
Brocade DCX with FS8-18 blade(s), Brocade Encryption Switch	v6.1.1_enc or later ⁶
Brocade 7800, DCX and DCX-4S with FCOE10-24 or FX8-24 blades	V6.3.0 or later
Brocade 8000	V6.1.2_CEE1 or later

Supported Products and FOS Interoperability	
Brocade DCX/DCX-4S with FA4-18 blade(s)	DCX requires v6.0.x or later ⁶ , DCX-4S requires 6.2.x or later ^{5 6}
Brocade DCX 8510-8/DCX 8510-4	FOS v7.0 or later
Brocade 6510	FOS v7.0 or later
Brocade 6505	FOS v7.0.1 or later
Brocade 6520	FOS v7.1 or later
48000 with FA4-18 blade(s), Brocade 7600	V6.2.2 or later ⁶
Secure Fabric OS (on any model)	Not Supported
Mi10k, M6140, ED-6064, ES-3232, ES-4300, ES-4400, ES-4500, ES-4700 (McDATA Fabric Mode and Open Fabric Mode) ¹	Direct E_Port connections are not supported – must use FCR running pre-FOS v7.1. M-EOS v9.9.5 or later
McDATA ED-5000 32-port FC director	Not Supported

Multi-Protocol Router Interoperability	
Brocade 7420	Not supported
Brocade 7500 and FR4-18i blade	V6.2.2 and higher ^{4 6 8}
McDATA SANRouters 1620 and 2640	Not Supported

NOS (VDX Platform) Interoperability	
Brocade VDX6710, VDX6720, VDX6730	NOS v2.1.1 or later ⁷
Brocade VDX8770	NOS 3.0 or later

Table Notes:

- ¹ When routing to an M-EOS edge fabric using frame redirection, the M-EOS fabric must have a FOS-based product in order to configure the frame redirection zone information in the edge fabric.
- ² When directly attached to a Host or Target that is part of an encryption flow.
- ³ These platforms may not be directly attached to hosts or targets for encryption flows.
- ⁴ McDATA 1620 and 2640 SANRouters should not be used with FOS-based routing (FCR) for connections to the same edge fabric.
- ⁵ FA4-18 is not supported in a DCX/DCX-4S that is running FOS v7.0 or later
- ⁶ If operating with **FOS v6.2.2e or earlier**, Adaptive Networking QoS must be disabled when connecting to 16G FC platform. Otherwise, ISL will segment.
- ⁷ Connectivity to FC SAN is established via VDX6730 connected to FCR running FOS v7.0.1 or later. FCR platforms supported include 5100, VA-40FC, 5300, 7800, DCX, DCX-4S, DCX 8510-8, DCX 8510-4, 6510, 6520 (requires FOS v7.1 or later). For higher FCR backbone scalability (refer to separate “Brocade SAN Scalability Guidelines” documentation for details), please use 5300, 6520, DCX, DCX-4S, DCX 8510-8, DCX 8510-4.
- ⁸ FR4-18i and FC10-6 are not supported on DCX/DCX-4S on FOS v7.1 or later.

Zoning Compatibility Note:

Users are recommended to upgrade to the following versions of firmware when interoperating with a switch running FOS v7.0 or later in the same layer 2 fabric to overcome some of the zoning operations restrictions that otherwise exist:

Main code level	Patch code levels with full zoning compatibility
FOS v6.2	FOS v6.2.2d or later
FOS v6.3	FOS v6.3.2a or later
FOS v6.4	FOS v6.4.1 or later

If there are switches running FOS versions lower than the above listed patch levels in the same fabric as a switch with FOS v7.0 or later, then cfsave and cfsenable operations **initiated** from these switches will fail if the zoning database is greater than 128KB. In such scenarios zoning operations such as cfsave/cfsenable can still be performed successfully if initiated from a switch running FOS v7.0 or later.

Blade Support

Fabric OS v7.1.0 software is fully qualified and supports the blades for the DCX/DCX-4S noted in the following table:

DCX/DCX-4S Blade Support Matrix	
16-, 32-, 48- and 64-port 8Gbit port blades (FC8-16, FC8-32, FC8-48, FC8-64)	Supported with FOS v6.0 and above (FC8-64 requires FOS v6.4) with any mix and up to 8/4 of each. No restrictions around intermix.
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.
6 port 10G FC blade (FC10-6)	Not supported on FOS v7.1 or later
FCIP/FC Router blade (FR4-18i)	Not supported on FOS v7.1 or later
Virtualization/Application Blade (FA4-18)	Not supported on FOS v7.0 or later
Encryption Blade (FS8-18)	Up to a maximum of 4 blades of this type.
Next Generation Distance Extension Blade (FX8-24)	Up to a max of 4 blades of this type. Note: FR4-18i cannot coexist with FX8-24 in FOS v7.0 or later
FCoE/L2 CEE blade FCOE10-24	Up to a max of 4 blades of this type. Not supported in the same chassis with other intelligent blades or the FC8-64 port blade.
FC16-32, FC16-48	Not supported

Table 1 Blade Support Matrix for DCX and DCX-4S with FOS v7.1

Note: The iSCSI FC4-16IP blade is not qualified for the DCX/DCX-4S.

Fabric OS v7.1 software is fully qualified and supports the blades for the DCX 8510-8 and DCX 8510-4 noted in the table below.

DCX 8510-8/DCX 8510-4 Blade Support Matrix	
FC16-32, FC16-48 16G FC blades	Supported starting with FOS v7.0
FC8-64 64 port 8Gbit port blade	With any mix and up to 8/4 of each. No restrictions around intermix. Note: FC8-16, FC8-32, FC8-48 blades are not supported on DCX 8510 platforms
FC8-32E, FC8-48E Condor3 based 8G blades	Supported starting with FOS v7.0.1 ¹
FC10-6	Not supported.
Intelligent blade	Up to a total of 8/4 intelligent blades. See below for maximum supported limits of each blade.
FCIP/FC Router blade (FR4-18i)	Not supported.
Virtualization/Application Blade (FA4-18)	Not supported
Encryption Blade (FS8-18)	Up to a maximum of 4 blades of this type.
Next Generation Distance Extension Blade (FX8-24)	Up to a maximum of 4 blades of this type.
FCoE/L2 CEE blade FCOE10-24	Not supported

Table 2 Blade Support Matrix for DCX 8510-8 and DCX 8510-4 with FOS v7.1

Note: The iSCSI FC4-16IP blade is not qualified for the DCX 8510-8/DCX 8510-4.

1. Note that 16G SFP+ is not supported in FC8-32E and FC8-48E blades

Power Supply Requirements for Blades in DCX/DCX-4S				
Blades	Type of Blade	DCX/DCX-4S @110 VAC (Redundant configurations)	DCX/DCX-4S @200-240 VAC (Redundant configurations)	Comments
FC10-6 ¹ , FC8-16, FC8-32, FC 8-48, FC8-64	Port Blade	2 Power Supplies	2 Power Supplies	Distribute the Power Supplies evenly to 2 different AC connections for redundancy.
FR4-18i ¹	Intelligent Blade	Not Supported	2 Power Supplies	
FS8-18, FX8-24, FCOE10-24	Intelligent Blade	Not Supported	DCX: 2 or 4 Power Supplies DCX-4S: 2 Power Supplies	- For DCX with three or more FS8-18 Blades, (2+2) 220VAC Power Supplies are required for redundancy. - For DCX with one or two FS8-18 Blades, (2) 220VAC Power Supplies are required for redundancy. - For DCX-4S, (2) 220VAC Power Supplies provide redundant configuration with any supported number of FS8-18 Blades. - For both DCX and DCX-4S with FX8-24 blades, (1+1) 220VAC Power Supplies are required for redundancy.

Table 3 Power Supply Requirements for DCX and DCX-4S

1. Note that FC10-6 and FR4-18i are not supported with FOS v7.1 or later

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-8 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-8 Backbone Hardware Reference Manual)					
Configured Number of Ports ²	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant configurations)	DCX 8510-8 @200-240 VAC (Redundant configurations)	Comments
Any combination of 8Gb or 16Gb ports	FC8-64, FC16-32, FC8-32E	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 ¹ Power Supplies
256 16Gb ports	FC16-32, FC16-48 (Maximum of fully populated FC16-32 blades)	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 ¹ Power Supplies Max 8 FC16-32 port blades
256 8Gb ports	FC8-32E, FC8-48E (Maximum of fully populated FC8-32E blades)	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 ¹ Power Supplies Max 8 FC8-32E port blades
192 16Gb Ports & max 2 intelligent blades (FX8-24 /FS8-18/combination)	FC16-32, FC16-48, FX8-24, FS8-18 (Two intelligent blades and maximum of four slots populated with FC16-xx/FC8-xxE blades)	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 ¹ Power Supplies
192 8Gb Ports & max 2 intelligent blades (FX8-24 /FS8-18/combination)	FC8-32E, FC8-48E, FX8-24, FS8-18 (Two intelligent blades and maximum of four slots populated with FC16-xx/FC8-xxE blades)	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 ¹ Power Supplies
336 16Gb ports	FC16-48 (Maximum of seven FC16-48 blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 ¹ Power Supplies Max 7 FC16-48 port blades

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-8 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-8 Backbone Hardware Reference Manual)					
Configured Number of Ports ²	Blades	Type of Blade	DCX 8510-8 @110 VAC (Redundant configurations)	DCX 8510-8 @200-240 VAC (Redundant configurations)	Comments
336 8Gb ports	FC8-48E (Maximum of seven FC8-48E blades, with one empty port blade slot)	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 ¹ Power Supplies Max 7 FC8-48E port blades
384 16Gb ports	FC16-32, FC16-48	Port Blade	Not Supported	4 Power Supplies	200-240VAC: For DCX 8510-8, four (2+2) ¹ 220V AC Power Supplies are required
384 8Gb ports	FC8-32E, FC8-48E	Port Blade	Not Supported	4 Power Supplies	200-240VAC: For DCX 8510-8, four (2+2) ¹ 220V AC Power Supplies are required
Any combination of 8Gb or 16Gb ports and intelligent blades	FC16-32, FC16-48, FC8-64, FC8-32E, FC8-48E, FS8-18, FX8-24	Intelligent Blade /Combination	Not Supported	4 Power Supplies	For DCX 8510-8, four (2+2) ¹ 220V AC Power Supplies are required when any special purpose blade are installed

Table 4 Power Supply Requirements for DCX 8510-8

Notes:

1. When 2+2 power supply combination is used, the users are advised to configure the Fabric Watch setting for switch marginal state to be two power supplies. Users can use the CLI `switchstatuspolicyset` to configure this value if the current value is set to zero. In FOS v7.0.x, the default setting for the marginal state due to missing power supplies is incorrectly set to zero (Defect 000349586), which will prevent Fabric Watch from generating notifications when the switch enters the marginal state due to missing power supplies
2. The power draw of ICL ports is taken into account and does not change the listed PS requirements

Typical Power Supply Requirements Guidelines for Blades in DCX 8510-4 (For specific calculation of power draw with different blade combinations, please refer to Appendix A: Power Specifications in the 8510-4 Backbone Hardware Reference Manual)					
Configured Number of Ports ¹	Blades	Type of Blade	DCX 8510-4 @110 VAC (Redundant configurations)	DCX 8510-4 @200-240 VAC (Redundant configurations)	Comments
96 ports max	FC16-32, FC8-32E	Port Blade	2 Power Supplies	2 Power Supplies	1+1 redundancy with 110 or 200-240 VAC power supplies
Any combination of 8Gb or 16 Gb ports and intelligent blades	FC16-32, FC16-48, FC8-32E, FC8-48E, FC8-64, FS8-18, FX8-24	Intelligent Blade /Combination	Not Supported	2 Power Supplies	200-240VAC: 1+1 Power Supplies

Table 5 Power Supply Requirements for DCX 8510-4

1. The power draw of ICL ports is taken into account and does not change the listed PS requirements

Scalability

All scalability limits are subject to change. Limits may be increased once further testing has been completed, even after the release of Fabric OS. For current scalability limits for Fabric OS, refer to the *Brocade Scalability Guidelines* document, available under the *Technology and Architecture Resources* section at <http://www.brocade.com/compatibility>

Other Important Notes and Recommendations

Adaptive Networking/Flow-Based QoS Prioritization

- Any 8G or 4G FC platform running FOS v6.2.2e or lower version of firmware cannot form an E-port with a 16G FC platform when Adaptive Networking QoS is enabled at both ends of the ISL. Users must disable QoS at either end of the ISL in order to successfully form an E-port under this condition.

Users can disable QoS via `portcfgQos –disable` command. Please consult Fabric OS Command Reference manual for details related to `portcfgQos` command.

- When using QoS in a fabric with 4G ports or switches, FOS v6.2.2 or later must be installed on all 4G products in order to pass QoS info. E_Ports from the DCX to other switches must come up AFTER 6.2.2 is running on those switches.

Access Gateway

- AG cascading is not supported on Brocade 6510 or Brocade 6505.
- Users who want to utilize Access Gateway's Device-based mapping feature in the ESX environments are encouraged to refer to the SAN TechNote GA-TN-276-00 for best implementation practices. Please follow these instructions to access this technote:
 - Log in to <http://my.brocade.com>
 - Go to Documentation > Tech Notes.

- Look for the Tech Note on Access Gateway Device-Based Mapping in VMware ESX Server.

Brocade HBA/Adapter Compatibility

- Brocade HBA/Adapter should be using driver version 2.3.0.2 or later when attached to 16G ports on Brocade switches.

D-Port

- FOS v7.0.0a and later support the execution of D-Port tests concurrently on up to eight ports on the switch.
- Support of D-Port is extended to R_RDY flow control mode. The R_RDY mode is useful for active DWDM links that do not work in VC_RDY or EXT_VC_RDY flow control modes.
- A new sub-option “-dwdm” is added to “portcfgdport --enable” CLI to configure D-Port over **active** DWDM links. The “-dwdm” option will not execute the optical loopback test while performing D-Port tests as the **active** DWDM links do not provide necessary support to run optical loopback tests.

Edge Hold Time

- Edge Hold Time (EHT) default settings for FOS v7.x have changed from those in some FOS v6.4.x releases. The following table shows the Default EHT value based on different FOS release levels originally installed at the factory:

Factory Installed Version of FOS	Default EHT Value
FOS v7.X	220 ms
FOS v6.4.3x	500 ms
FOS v6.4.2x	500 ms
FOS v6.4.1x	220 ms
FOS v6.4.0x	500 ms
Any version prior to FOS v6.4.0	500 ms

Gen 5 platforms and blades are capable of setting an EHT value on an individual port basis. On 8G platforms EHT is set on an ASIC-wide basis, meaning all ports on a common ASIC will have the same EHT setting. Extra care should be given when configuring EHT on 8G platforms or Gen 5 platforms with 8G blades to ensure E_Ports are configured with an appropriate Hold Time setting.

When using Virtual Fabrics and creating a new Logical Switch when running FOS v7.1.0 or later, the default EHT setting for the new Logical Switch will be the FOS default value of 220ms. However, with FOS v7.1.0 and later, each Logical Switch can be configured with a unique EHT setting that is independent of other Logical Switches and the Default Switch. Any Gen 5 ports (Condor3 based) assigned to that Logical Switch will be configured with that Logical Switch's EHT setting. Any 8G ports (Condor2 based) will continue to share the EHT value configured for the Default Switch.

For more information on EHT behaviors and recommendations, refer to the Brocade SAN Fabric Resiliency Best Practices v2.0 document available on www.brocade.com.

Encryption Behavior for the Brocade Encryption Switch (BES) and FS8-18

- SafeNet's KeySecure hosting NetApp's LKM (SSKM) is supported for data encryption operations with FOS v7.0.1 or later.
 - Use of SSKM with the Brocade encryption solution is only supported for SSKM operating in PVM mode. Please see SSKM documentation for operating in PVM mode for details. Operation in HVM mode is not supported.
 - It is recommended to use Tight VNC connection to access the management console for SSKM and LKM key vaults instead of remote desktop. If remote desktop is used, customer may encounter the following errors related to smart card reader:
 - Error communicating with smart card reader.
 - Card reader already in use by default key.
 - Unable to complete TEP/TAP process as window for selecting card and entering password does not appear.
 - Please refer to SafeNet Keysecure install documentation for setting up and initially configuring the SSKM key vaults. There are some changes between setting up the SSKMs and the LKMs. Please refer SafeNet or NetApp documentation for any LKM to SSKM migration procedures. This migration is not tested/supported with FOS v7.0.1 or later.
 - The following is tested and supported with FOS v7.0.1 or later
 - Platform Serial Number: 27CJNQ1
 - Platform FW Version: SSKM-1.0-03
 - Platform Firmware Build ID: 0.5_secure
 - DB version: 166
 - SEP FW ID: SEPLuna TDB
 - SEP HW ID: Luna K6 TBD
 - SEP SW ID: 6.2.0 TBD
 - System Card FW ID: 200.5
 - Management console version: 1.0 build 18.
- For crypto tape operations, please ensure to use Emulex FC HBA firmware/drivers 2.82A4/7.2.50.007 or higher. Use of lower level firmware/drivers may result in hosts not being able to access their tape LUNs through a crypto target container.
- If the migration to FOS v7.0 or later does not occur from 6.4.1a, 6.4.1b, or 6.4.2, the following will result
 - BES will reboot if auto reboot is enabled otherwise it needs to be rebooted manually for recovery2010/11/08-04:54:35:485488, [FSS-1009], 4424/886, CHASSIS, ERROR, MACE, FSS Error: fcswo-vs: MISMATCH: component., svc.c, line: 2462, comp:FSSK_TH, ltime:2010/11/08-04:54:35:485484
- Adding of 3PAR Session/Enclosure LUNs to CTCs is now supported. Session/Enclosure LUNs (LUN 0xFE) used by 3PAR InServ arrays must be added to CryptoTarget (CTC) containers with LUN state set to "cleartext", encryption policy set to "cleartext". BES/FS8-18 will not perform any explicit enforcement of this requirement.
- When host clusters are deployed in an Encryption environment, please note the following recommendations:
 - If two EEs (encryption engines) are part of a HAC (High Availability Cluster), configure the host/target pair such that they form a multipath from both EEs. Avoid connecting both the host/target pairs to the same EE. This connectivity does not give full redundancy in the case of EE failure resulting in HAC failover.
 - Since quorum disk plays a vital role in keeping the cluster in sync, please configure the quorum disk to be outside of the encryption environment.
- The "-key_lifespan" option has no effect for "cryptocfg -add -LUN", and only has an effect for "cryptocfg -create -tapepool" for tape pools declared "-encryption_format native". For all other encryption cases, a new key is generated each time a medium is rewound and block zero is written or

overwritten. For the same reason, the “Key Life” field in the output of “cryptocfg –show –container –all –stat” should always be ignored, and the “Key life” field in “cryptocfg –show –tapepool –cfg” is only significant for native-encrypted pools.

- The Quorum Authentication feature requires a compatible DCFM or Brocade Network Advisor release (DCFM 10.3 or later for pre-FOS v7.0 and Network Advisor 11.1 or later for FOS v7.0 or later) that supports this feature. Note, all nodes in the EG must be running FOS v6.3.0 or later for quorum authentication to be properly supported.
- The System Card feature requires a compatible DCFM or Brocade Network Advisor release (DCFM 10.3 or later for pre-FOS v7.0 and Network Advisor 11.1 or later for FOS v7.0 or later) that supports this feature. Note, all nodes in the EG must be running FOS v6.3.0 or later for system verification to be properly supported.
- The Brocade Encryption switch and FS8-18 blade do not support QoS. When using encryption or Frame Redirection, participating flows should not be included in QoS Zones.
- HP SKM & ESKM are supported with Multiple Nodes and Dual SKM/ESKM Key Vaults. Two-way certificate exchange is supported. Please refer to the Encryption Admin Guide for configuration information. If using dual SKMs or ESKMs on BES/FS8-18 Encryption Group, then these SKM / ESKM Appliances must be clustered. Failure to cluster will result in key creation failure. Otherwise, register only one SKM / ESKM on the BES/FS8-18 Encryption Group.
- FOS 7.1.0 will use SHA256 signatures for the TLS certificates, used to connect to the ESKM 3.0 Server using ESKM 2.0 client. Upgrade from FOS versions (6.4.x/7.0.x) to FOS 7.1.0 and downgrade from FOS 7.1.0 to FOS versions (6.4.x/7.0.x) would require regeneration and re-registration of CA and signed KAC certificates to restore connectivity to the key vault. Please refer to Encryption AG for more details on ESKM/FOS compatibility matrix
- The RSA DPM Appliance SW v3.2 is supported. The procedure for setting up the DPM Appliance with BES or a DCX/DCX-4S/DCX 8510 with FS8-18 blades is located in the Encryption Admin Guide.
- Before upgrading from FOS versions (6.4.x/7.0.x) to FOS 7.1.0, it is required that the RKM server running SW v2.7.1.1 should be upgraded to DPM server running SW v3.2. Please refer to DPM/FOS compatibility matrix in the Encryption AG for more details.
- Support for registering a 2nd DPM Appliance on BES/FS8-18 is blocked. If the DPM Appliances are clustered, then the virtual IP address hosted by a 3rd party IP load balancer for the DPM Cluster must be registered on BES/FS8-18 in the primary slot for Key Vault IP.
- With Windows and Veritas Volume Manager/Veritas Dynamic Multipathing, when LUN sizes less than 400MB are presented to BES for encryption, a host panic may occur and this configuration is not supported in the FOS v6.3.1 or later release.
- Hot Code Load from FOS v6.4.1a to FOS v7.0 or later is supported. Cryptographic operations and I/O will be disrupted but other layer 2 FC traffic will not be disrupted.
- When disk and tape CTCs are hosted on the same encryption engine, re-keying cannot be done while tape backup or restore operations are running. Re-keying operations must be scheduled at a time that does not conflict with normal tape I/O operations. The LUNs should not be configured with auto rekey option when single EE has disk and tape CTCs.
- Gatekeeper LUNs used by SYMAPI on the host for configuring SRDF/TF using in-band management must be added to their containers with LUN state as “cleartext”, encryption policy as “cleartext” and without “-newLUN” option.
- FOS 7.1.0 introduces support for “disk device decommissioning” to following key vault types: ESKM, TEKA, TKLM and KMIP. To use disk device decommissioning feature for these KVs, all the nodes in the encryption group must be running FOS v7.1.0 or later. Firmware downgrade will be prevented from FOS v7.1.0 to a lower version if this feature is in use. Disk Device decommissioning for DPM and LKM key vaults will continue to work as with previous firmware versions.

- FOS7.1.0 introduces a new KMIP keyvault type for Safenet KeySecure SW v6.1 KMIP server. Firmware downgrade will be prevented from FOS v7.1.0 to a lower version if key vault type is set to KMIP. Please refer to the KMIP Encryption Admin Guide for more details.
- FOS 7.1.0 mandates regular zones for Hosts and Targets must be defined in the effective configuration before adding an initiator into a crypto container. If crypto commit operation is performed without regular zones for Host and Target, frame redirection zones will not be created. Hosts and targets must be zoned together by worldwide port name (WWPN) rather than worldwide node name (WWNN) in configurations where frame redirection will be used
- In FOS 7.1.0 the encryption FPGA has been upgraded to include parity protection of lookup memory (ROM) within the AES engine. This change enhances parity error detection capability of the FPGA.
- Special Notes for HP Data Protector backup/restore application
 - Tape Pool encryption policy specification:
 - On Windows Systems, HP Data Protector can be used with tape pool encryption specification only if the following pool label options are used:
 - Pick from Barcode
 - User Supplied – Only 9 characters or less

For other options, behavior defaults to Tape LUN encryption policy.

 - On HP-UX systems, HP Data Protector cannot be used with tape pool encryption specification for any of the pool options. The behavior defaults to Tape LUN Encryption Policy.
 - Tape LUN encryption policy specification:
 - No restrictions, tape LUN encryption policy specification can be used with HP Data Protector on HP-UX and Windows systems.
- BES/FS8-18 will reject the SCSI commands WRITE SAME, ATS(Compare and Write/Vendor Specific opcode 0xF1) and EXTENDED COPY, which are related to VAAI (vStorage APIs for Array Integration) hardware acceleration in vSphere 4.1/5.x. This will result in non-VAAI methods of data transfer for the underlying arrays, and may affect the performance of VM related operations.
- VMware VMFS5 uses ATS commands with arrays that support ATS. BES/FS8-18 does not support this command set and therefore VMFS5 with ATS is not supported. It is recommended to use VMFS3.

FCIP (Brocade 7800 and FX8-24)

- Any firmware activation will disrupt I/O traffic on FCIP links.
- Latency measurements supported on FCIP Tunnels:
 - 1GbE & 10GbE - 200ms round trip time and 1% loss.
- After inserting a 4G SFP in GE ports of an FX8-24 blade or 7800 switch, sometimes “sfps show” output might display “Cannot read serial data!” . Removing and re-inserting the SFP should resolve this issue. It is recommended that users perform sfps show immediately after inserting the SFP and ensure SFP is seated properly before connecting the cables.
- When running FOS v7.0.0 or later, if any of the following features are enabled in the FCIP configuration, a downgrade operation to pre-FOS v7.0.0 will be blocked until the features are removed from the FCIP configuration:
 - InBand Management
 - Multigigabit Circuit

- Shared GE among Logical Switches
- Auto-mode compression option
- VE as XISL
- 10GigE lossless failover
- Modified QoS percentages
- 10GigE ARL
- IP Configuration where multiple GigEs have same subnet values
- For a tunnel configuration on 1GE ports that has more than 4 circuits
- Teradata emulation enabled
- Circuits configured explicitly to be listeners or an initiators

FCoE/DCB/CEE (Brocade 8000 and FCOE10-24)

- When upgrading a Brocade 8000 or DCX/DCX-4S with one or more FCOE10-24 blades from FOS v6.x to FOS v7.0.0 or later, the user should carefully review Chapter 5 of the FOS v7.0.0 Converged Enhanced Ethernet Administrator's Guide.
- FOS v7.0 or later supports a new optimized model for provisioning FCoE with fewer configuration steps to enable FCoE on DCB ports. These changes do not allow the Brocade 8000 to retain FCoE configuration information following an upgrade to FOS v7.0 or later. After the upgrade to FOS v7.0 or later, all FCoE edge ports will need to be provisioned with the new model before any FIP FLOGIs will take place
- Although including Brocade 8000 in the path of TI (Traffic Isolation) and ETI (Enhanced Traffic Isolation) Zones is not prohibited, it is not supported. Configuring Brocade 8000 in the TI/ETI Zone path is not recommended and will result in undefined behavior.
- Ethernet L2 traffic with xSTP Hello timer set to less than or equal to 3 seconds may experience momentary traffic disruption during HA failover.
- The Brocade 8000 balances the FCoE bandwidth across all six port groups (each port group contains four ports). To get optimum performance for FCoE traffic it is recommended that the user distribute server CNA connections across these six port groups.
- Hot plugging a CP with firmware level less than FOS v6.3.0 into a DCX or DCX-4S with an active FCOE10-24 blade will result in the new standby CP not coming up.
- When operating in Converged Mode, tagged traffic on the native VLAN of the switch interface is processed normally. The host should be configured not to send VLAN tagged traffic on the switch's native VLAN.
- When operating in Converged Mode, tagged frames coming with a VLAN tag equal to the configured native VLAN are dropped.
- The Converged Network Adapter (CNA) may lose connectivity to the Brocade 8000/FCOE10-24 if the CNA interface is toggled repeatedly over time. This issue is related to the CNA and rebooting the CNA restores connectivity.
- The Brocade 8000 and FCOE10-24 support only one CEE map on all interfaces connected to CNAs. Additionally, CEE map is not recommended for use with non-FCoE traffic. QoS commands are recommended for interfaces carrying non-FCoE traffic.
- Before upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, if the CEE map "default" value already exists, the same "default" value is preserved after upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later. However, if the CEE map "default" is not configured before upgrading to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, then after upgrading to FOS

v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, the following CEE map “default” will be created automatically:

```
cee-map default
priority-group-table 1 weight 40 pfc
priority-group-table 2 weight 60
priority-table 2 2 2 1 2 2 2 2
```

- When upgrading from FOS v6.3.x or v6.4.x to FOS v6.4.1_fcoe/v6.4.1_fcoe1/v7.0.0 or later, the CEE start up configuration dcf.conf file will be incompatible with the FCoE provisioning changes implemented in v6.4.1_fcoe and later releases. Users can save the dcf.conf file as a backup and apply it once the firmware upgrade is completed to get the DCX/DCX-4S to the same startup configuration as in the older release.
- It is recommended that Spanning Tree Protocol and its variants be disabled on CEE interfaces that are connected to an FCoE device.
- The Fabric Provided MAC Address (FPMA) and the Fibre Channel Identifier (FCID) assigned to a VN_Port cannot be associated with any single front-end CEE port on which the FLOGI was received.
- LLDP neighbor information may be released before the timer expires when DCBX is enabled on a CEE interface. This occurs only when the CEE interface state changes from active to any other state. When the DCBX is not enabled, the neighbor information is not released until the timer expires, irrespective of the interface state.
- The FCoE login group name should be unique in a fabric-wide FCoE login management configuration. If there is a login group name conflict, the merge logic would rename the login group by including the last three bytes of the switch WWN in the login group name. As long as the OUI of the switch WWNs are identical this merge logic guarantees uniqueness in any modified login group name (switches with the same OUI will have unique last 3 bytes in WWN). However, if the participating switches have different OUIs but identical last three bytes in the switch WWNs, then the merge logic will fail to guarantee uniqueness of login group names. This will result in one of the login groups being dropped from the configuration. This means, no device can login to the login group that is dropped as a result of this name conflict. Users must create a new login group with a non-conflicting name to allow device logins.
- Ethernet switch services must be explicitly enabled using the command “*fosconfig -enable ethsw*” before powering on an FCOE10-24 blade. Failure to do so will cause the blade to be faulted (fault 9). Users can enable ethsw after upgrading firmware without FC traffic interruption.
- The Brocade 8000 does not support non-disruptive hot code loads (HCL). Upgrading the Brocade 8000 to FOS v7.1 or downgrading from v7.1 is disruptive to the IO through the switch.
- Upgrading firmware on a DCX or DCX-4S with one or more FCOE10-24 blades from FOS v6.4.1_fcoe1 to FOS v7.0 or later will be non-disruptive to FCoE traffic through FCOE10-24 blades and FC traffic.
- Upgrading firmware on a DCX or DCX-4S with one or more FCOE10-24 blades from FOS v6.3.x, v6.4.x, and v6.4.1_fcoe to FOS v7.0 or later will be disruptive to any traffic through the FCOE10-24 blades.
- Connecting Brocade 8000 to an FCR-capable switch with fcrbcast config enabled will cause a storm of broadcast traffic resulting in termination of iswitchd.
- When rebooting a DCX or DCX-4S with an FCOE10-24 blade, Qlogic CNA and LSAN zoning, the switch will become very unresponsive for a period of time. This is due to the CNA sending excessive MS queries to the switch.
- The Brocade 8000 and FCOE10-24 can handle 169 small FCoE frames in bursts. If you are using the Brocade 8000 or FCOE10-24, and you delete a large number of v-ports with HCM, some of the v-ports may not appear to be deleted. To correct this, disable and re-enable FCoE with the following CLI commands:

switch:admin>**fcoe -disable slot/port**

switch:admin>**fcoe -enable slot/port**

- When a FCOE10-24 blade is powered off during configuration replay, the interface specific configuration won't get applied. Later when FCOE10-24 blade is powered on, all physical interfaces will come up with default configurations. User can execute "copy startup-config running-config" command to apply the new configuration after powering on the FCOE10-24 blade.
- When IGMP Snooping is disabled on a VLAN, all configured IGMP groups are removed from that VLAN. User has to reconfigure the IGMP groups after enabling the IGMP snooping on that VLAN.

FCR and Integrated Routing

- With routing and dual backbone fabrics, the backbone fabric ID must be changed to keep the IDs unique.
- VEX edge to VEX edge device sharing will not be supported.
- To allow Hot Code Load on Brocade 5100 when using Integrated Routing, the edge switch connected to the 5100 must be running Fabric OS v6.1 or later code.

Forward Error Correction (FEC)

- Though FEC capability is generally supported on Condor3 (16G capable FC) ports when operating at either 10G or 16G speed, it is not supported when using active DWDM links. Hence FEC must be disabled on Condor3 ports when using active DWDM links by using portCfgFec command. Failure to disable FEC on active DWDM links may result in link failure during port bring up.

FICON

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

FL_Port (Loop) Support

- FL_Port is not supported on FC16-32, FC16-48, FC8-32E, FC8-48E, Brocade 6510, Brocade 6505 and Brocade 6520.
- The FC8-48 and FC8-64 blade support attachment of loop devices.
 - Virtual Fabrics must be enabled on the chassis and loop devices may only be attached to ports on a 48-port or 64-port blade assigned to a non-Default Logical Switch operating with the default 10-bit addressing mode (they may not be in the default Logical Switch).
- A maximum of 144 ports may be used for connectivity to loop devices in a single Logical Switch within a chassis in 10-bit dynamic area mode on DCX-4S.
- A maximum of 112 ports may be used for connectivity to loop devices in a single Logical Switch within a chassis in 10-bit dynamic area mode on DCX.
- Loop devices continue to be supported when attached to ports on the FC8-16, FC8-32 with no new restrictions.

ICLs on DCX/DCX-4S

- If a DCX with an 8-link ICL license is connected to a DCX with a 16-link license, the DCX with the 16-link license will report enc_out errors. The errors are harmless, but will continue to increment. These errors will not be reported if a DCX with a 16-link license is connected to a DCX-4S with only 8-link ICL ports.
- If ICL ports are disabled on only one side of an ICL link, the enabled side may see enc_out errors.

Licensing

- The Fabric Vision license (included in some software bundles) is being introduced in 2013 to enable new functionality in FOS v7.2 and later releases. When installed on a switch operating with FOS v7.1.x, the `licenseshow` command will display this license as the “Fabric Insight license”. When running FOS v7.1.x or earlier, existence of this license does not affect any functionality on the switch.

Native Connectivity (M-EOS interoperability)

- A switch running FOS v7.0 or later cannot form E-port connectivity with any M-EOS platform.
- Platform running FOS v7.1 does not support EX port configuration in Interopmode 2 or Interopmode 3.
- Device sharing between a switch running FOS v7.1 and McDATA fabrics is allowed via Integrated Routing platforms using FOS v7.0.x (or earlier) firmware.

Port Initialization

Users may observe that a port is in “Port Throttled” state when an F_Port is being initialized. This is mostly an informational message that is shown in `switchshow` output indicating systematic initialization of F_Ports.

However, a port may remain in “Port Throttled” state for an extended period of time and may never come online if it fails to negotiate speed successfully with the neighboring port. Users are advised to check the speed setting of the neighboring switch port to determine the cause of the speed negotiation failure.

Example Output:

```
74      9      10      36ed40      id      N8      In_Sync      FC      Disabled (Port
Throttled)
```

Port Mirroring

- Port Mirroring is not supported on the Brocade 7800.

Port Statistics

- On 16G capable ports, the `enc_in` (number of encoding errors inside of frames) and `enc_out` (number of encoding errors outside of frames) counters will not be updated when a port is *operating* at either 10G or 16G speed. This is due to the different encoding scheme used at 10G and 16G speeds when compared to 8G/4G/2G speeds. Because of this, Fabric Watch alerts and Port Fencing based on ITW (Invalid Transmission Word) thresholds will not function as these `enc_in` and `enc_out` counters will not be incremented when operating at either 10G or 16G (ITW is computed based on `enc_in` and `enc_out` counters). Also any CLI or GUI that displays `enc_in` and `enc_out` counters will show no incrementing of these counters when a port is operating at either 10G or 16G.

Both `enc_in` and `enc_out` counters contain valid information when a Condor3-based port is operating at speeds **other than** 10G and 16G.

Virtual Fabrics

- When creating Logical Fabrics that include switches that are not Virtual Fabrics capable, it is possible to have two Logical Switches with different FIDs in the same fabric connected via a VF incapable switch. Extra caution should be used to verify the FIDs match for all switches in the same Logical Fabric.
- A switch with Virtual Fabrics enabled may not participate in a fabric that is using Password Database distribution or Administrative Domains. The Virtual Fabrics feature must be disabled prior to deploying in a fabric using these features.
- ISL R_RDY mode is not supported in a base switch with FOS version 7.0 or higher.

WebTools

- WebTools since FOS v7.1.0 has a “SupportSave” interface. It only collects, however, information specifics to WebTools. It does not contain the same information as collected by supportSave initiated through CLI or Brocade Network Advisor.
- When launching WebTools on a computer without the Internet access, it could take upto 5 minutes to complete because the certificate revocation check performed for the WebTools application takes time to timeout. Users can turn off the certification revocation check on the Java control panel as a workaround.
- Launching WebTools with Oracle JRE 1.7.0 update 51 through Brocade Network Advisor is only supported on version 12.1.5 or later. With JRE 1.7.0 update 51, users could see browser warning messages that the WebTools application requires unrestricted access or the certificate signing the application is not recognized. These messages can be ignored. In addition, users must check the “Enable Java content in the browser” box under the Security tab of Java Control Console to allow launching WebTools from BNA server clients.

Zoning

- Support for up to 2MB zone database in a fabric with only DCX/DCX-4S/DCX8510 systems. The presence of any other platform in the fabric will limit the maximum zone database to 1MB. Please note that there is no enforcement by FOS 7.1 to restrict users to operate within a zone database limit - it is the responsibility of the user to not exceed this limit.
- There are limitations to zoning operations that can be performed from a FOS v6.x switch that is in the same fabric as a FOS v7.0 or later switch if the FOS v6.x switch is not running the recommended firmware version. Please see Fabric OS Interoperability section for details.

Beginning with the FOS v6.2.0 release, all WWNs containing upper-case characters are automatically converted to lower-case when associated with a zone alias and stored as part of a saved configuration on a switch. For example, a WWN entered as either “AA.BB.CC.DD.EE.FF.GG.HH” or “aa.bb.cc.dd.ee.ff.gg.hh” when associated with a zone alias will be stored as “aa.bb.cc.dd.ee.ff.gg.hh” on a switch operating with FOS v6.2.0 or later.

This behavioral change in saved zone alias WWN members will not impact most environments. However, in a scenario where a switch with a zone alias WWN member with upper case characters (saved on the switch with pre-FOS v6.2.0 code) is merged with a switch with the same alias member WWN in lower case characters, the merge will fail, since the switches do not recognize these zoning configurations as being the same.

For additional details and workaround solutions, please refer to the latest FOS Admin Guide updates or contact Brocade Customer Support.

Miscellaneous

- **Using a Windows anonymous FTP server for supportsave collection**

When using anonymous ftp, to avoid long delays or failure of simultaneous supportsave collections when AP blades are present in a director chassis, the number of unlimited anonymous users for a Windows FTP server should be configured as follows:

Number of anonymous FTP connections = (Number of director chassis) + (Number of installed Application Blades x 3)

- RASlog message AN-1010 may be seen occasionally indicating “Severe latency bottleneck detected”. Even though it is a “Warning” message, it is likely to be a false alarm and can be ignored.
- POST diagnostics for the Brocade 5100 have been modified beginning with FOS v6.3.1b and v6.4.0 to eliminate an “INIT NOT DONE” error at the end of an ASIC diagnostic port loopback test. This modification addresses BL-1020 Initialization errors encountered during the POST portloopbacktest. (Defect 263200)

- It is important to note that the outputs of slotshow -p and chassisshow commands also display the maximum allowed power consumption per slot. These are absolute maximum values and should not be confused with the real-time power consumption on 16G blades. The chassisshow command has a "Power Usage (Watts):" field that shows the actual power consumed in real-time on 16G blades.
- Class 3 frames that have been trapped to CPU will be discarded in the following scenarios on DCX/DCX-4S/DCX 8510 during the following conditions:
 - HA failover on DCX/DCX-4S/DCX 8510 platforms while running FOS v7.0 or later firmware
 - Firmware upgrade from v7.0 to a later release on Brocade 300, 5100, VA-40FC, 5300, 6510
 - Firmware upgrade from v7.0.1 to a later release on Brocade 6505
 - Firmware upgrade from v7.1.0 to a later release on Brocade 6520
- The QSFP information in the sfpshow output will indicate the ID field as all zeros. This is as designed.


```

ras080:FID128:root> sfpshow 5/32
QSFP No: 8 Channel No:0
Identifier: 13 QSFP+
Connector: 12 MPO Parallel Optic
Transceiver: 0000000000000000 16_Gbps id

```
- It is recommended that for directors with more than 300 E_Ports, the switch be disabled prior to executing the "switchCfgTrunk" command (used to disable or enable trunking on the switch).
- During non-disruptive firmware upgrades, E_Ports in R-RDY mode may cause some frame drops on the E-port links.
- When loading this FOS v7.1.x version of code, you may see a message stating "no maps warning". This is a benign message and can be ignored.
- The Brocade Network Advisor seed switch should always have the highest FOS version used in the fabric.
- For login authentication through RADIUS, Brocade switch should be able to reach RADIUS servers through TCP authentication port (default 1812) and accounting port (default 1813). Both of these ports must be kept open in any firewall settings.



BROCADE

Defects

Closed with Code Change in Fabric OS v7.1.2b

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of August 14, 2014, 2014 in Fabric OS v7.1.2b.

Defect ID: DEFECT000475645	
Technical Severity: Medium	Probability: Medium
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.0.2	Technology Area: End-to-end Performance Monitoring
Symptom: Updated End-to-End monitor shows previous data.	
Condition: After removing and replacing an EE monitor (with the SID and DID reversed) the data from the original EE monitor is shown instead of zeros.	

Defect ID: DEFECT000484414	
Technical Severity: High	Probability: Medium
Product: FOS	Technology: Virtualization
Reported In Release: FOS7.0.2	Technology Area: Access Gateway
Symptom: Under rare conditions, Access Gateway(AG) entries stay in management server (MS) database even after removing them from the fabric. FOS firmware is expected to remove these stale entries during execution of agshow CLI command. However, due to a timing issue the stale entries may not be removed from the database when agshow CLI command is run.	
Condition: This may be observed on a switch running firmware version higher than v7.0.	

Defect ID: DEFECT000494270	
Technical Severity: Medium	Probability: Low
Product: FOS	Technology: Security
Reported In Release: FOS7.1.0	Technology Area: Fabric Authentication
Symptom: Customer might see devices reported as unauthorized when they try to login to a switch even when DCC policy is configured properly. Sometimes when the DCC policy is activated, some of the ports might bounce.	
Condition: The WWN that starts with "80" has the most possibility to hit this issue. The issue might also be seen when the device WWNs starts with "C0", "50", "20", or "10".	
Workaround: Avoiding the device WWN that starts with "80" or greater from DCC policy would resolve the issue.	

Defect ID: DEFECT000500250	
Technical Severity: Medium	Probability: Medium
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.2.0	Technology Area: Fabric Watch
Symptom: FWtrap is not generated for "Power on hours" area for 16G LWL SFP when thresholds cross boundaries.	
Condition: This impacts 16GLWL trap only	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000507447	
Technical Severity: High	Probability: High
Product: FOS	Technology: Management
Reported In Release: FOS7.1.1	Technology Area: Web Tools
Symptom: Switch throughput utilization graph freezes	
Condition: Launch switch throughput utilization graph and Issue is applicable to FOS v7.1 and above.	

Defect ID: DEFECT000512057	
Technical Severity: Medium	Probability: High
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.2.0	Technology Area: Fabric Watch
Symptom: Error messages start after firmware update from FOS v7.0.x to FOS v7.1.x and continue when upgrading to FOS v7.2.x. After downgrading back to 7.0.x, faulty port messages stop from Fabric Watch.	
Condition: Running FOS 7.1 and above, with a port remains in passive mode, which would simply complete speed negotiation and failing link init, results in FW-xxxx flood in RAS log.	
Workaround: Disable the port that does not cut off light	

Defect ID: DEFECT000512507	
Technical Severity: High	Probability: Medium
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.2.0	Technology Area: Routing
Symptom: Observed performance issue on FX8-24 when there are exactly two equal bandwidth FCIP tunnels.	
Condition: Only applicable when there are two incoming paths (E-ports, trunks, EX-ports) on a given FX8-24 or BR7800 ASIC Chip.	
Workaround: Use one or greater than two incoming path to FX8-24 and 7800, or configure one of the links with a slightly lower bandwidth.	

Defect ID: DEFECT000513920	
Technical Severity: High	Probability: Low
Product: FOS	Technology: Security
Reported In Release: FOS7.1.0	Technology Area: Fabric Authentication
Symptom: CVE-2014-0224: OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.	
Condition: FOS switches that are not running LDAP or RADIUS with PEAP-MSCHAPv2 for authentication are not running OpenSSL client mode and are not at risk. To be at risk: • The FOS product must be running authentication using LDAP or RADIUS with PEAP-MSCHAPv2 protocols. • The OpenSSL server must also be running with a version of OpenSSL that contains this vulnerability (1.0.1 or 1.0.2-beta1)	
Workaround: For users requiring LDAP or RADIUS with PEAP-MSCHAPv2 for authentication, upgrading the OpenSSL server to a version of OpenSSL that does not contain this vulnerability will prevent exposure.	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000515486	
Technical Severity: Medium	Probability: Low
Product: FOS	Technology: Other
Reported In Release: FOS7.1.1	Technology Area: Other
Symptom: Director panic due to software watchdog timeout with pdmd daemon. Prior to the panic, switch logged repeat message: "FSS Error: pdm: not acked!"	
Condition: This happened after the standby CP was "REMOVED".	
Recovery: Director recovers by itself after CP reboot.	

Defect ID: DEFECT000516703	
Technical Severity: High	Probability: Medium
Product: FOS	Technology: Distance
Reported In Release: FOS7.1.0	Technology Area: FCIP
Symptom: FICN-1062 and FICN-1063 abort messages on XRC and IFCC on host.	
Condition: In a large FICON disk mirroring configuration that includes base and alias devices in the connected primary controllers	
Workaround: None required – IFCCs will occur and normal channel error recovery will complete	

Defect ID: DEFECT000519655	
Technical Severity: Medium	Probability: High
Product: FOS	Technology: Distance
Reported In Release: FOS7.1.0	Technology Area: FCIP
Symptom: FCIP GigE portstatsshow frame TX type counters show inaccurate counts.	
Condition: This is seen when using the CLI command portstatsshow geX, where geX is ge1-ge5 on the 7800 platform	
Workaround: Use portstatsshow ge0 output. It includes the aggregation of the TX frame type counters for all GigE ports on the 7800 platform.	

Closed with Code Change in Fabric OS v7.1.2a

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of May 9, 2014 in Fabric OS v7.1.2a.

Defect ID: DEFECT000453711	
Technical Severity: Medium	Probability: Low
Product: FOS	Technology: Security
Reported In Release: FOS7.1.0	Technology Area: Fabric Authentication
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Following certificate deletion, the certificate file size is truncated to zero, causing reboot loop on standby CP with weblinker panic. Console logs message with: SSLCertificateFile: file '/etc/fabos/certs/sw0/x.x.x.x.crt' does not exist or is empty	
Condition: Delete certificate from the non-default VF context using seccertutil CLI command.	
Recovery: Remove the zero sized certificate file on standby CP. Active CP will sync the new file.	

Defect ID: DEFECT000457972	
Technical Severity: High	Probability: Low
Product: FOS	Technology: Distance
Reported In Release: FOS7.0.0	Technology Area: FCIP
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Invalid buffers index error messages are generated on console and the TCP connections making up the tunnel/circuit aborts instead of closing gracefully.	
Condition: It happens after an FCIP tunnel bounces due to a network issue.	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000460296	
Technical Severity: Medium	Probability: Low
Product: FOS	Technology: FICON
Reported In Release: FOS7.0.0	Technology Area: FICON emulation
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Ficon emulation reported Error code 100 and Ficon aborted with switch logging raslog FICN-1056 messages.	
Condition: Unit check happened during tape re-positioning state.	

Defect ID: DEFECT000461485	
Technical Severity: Medium	Probability: High
Product: FOS	Technology: FICON
Reported In Release: FOS7.0.0	Technology Area: FICON emulation
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: When a VTS was placed into service mode and then restored to normal mode, not all paths were recovered.	
Condition: FCIP FICON Emulating Tunnel with VTS devices do not recover after the controller has exited service mode.	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000462091	
Technical Severity: Medium	Probability: Low
Product: FOS	Technology: Other
Reported In Release: FOS7.1.0	Technology Area: Other
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: ipfilter behavior varies depending on IPFC configuration	
Condition: This is a general issue, not on a specific switch, and can be reproduced by the following steps:	
1. Set the ipfilter. 2. Try to login from another ip address that is not allowed via telnet, ssh, and http. 3. Hit errdump.	

Defect ID: DEFECT000462673	
Technical Severity: Low	Probability: Medium
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.0.0	Technology Area: Fabric Watch
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Some of the Fabric Watch keys are multiplied by 100 after configdownload.	
Condition: When configdownload a configuration file with "thresh.Pktloss" keys	
Workaround: Use fabric watch threshold management CLI rather than configdownload for "thresh.Pktloss" keys	

Defect ID: DEFECT000466131	
Technical Severity: Low	Probability: Medium
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.1.1	Technology Area: Fabric Watch
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: FW-1440 about empty slot is generated at hafailover	
Condition: Fru state may be incorrectly updated in Logical Switch	
Recovery: No loss of functionality, message can be ignored.	

Defect ID: DEFECT000467843	
Technical Severity: Medium	Probability: Medium
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.0.2	Technology Area: End-to-end Performance Monitoring
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: The TX counter remains at "0x0000000100000000" after clears stats of EE performance monitors.	
Condition: No special condition is required: When EE monitor counters(TX/RX) are cleared on a port, 1 in top value of EE monitor counters(Tx/Rx) are not cleared. There is no functional impact.	

Defect ID: DEFECT000470487	
Technical Severity: Medium	Probability: Medium
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.2.0	Technology Area: Fabric Watch
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Erroneous FW-1190 error messages seen on different VEX tunnels: Event: , VEXport#3/16,Packet Loss, is above high boundary(High=100, Low=0). Current value is 1176 Percentage(%). Severity: Warning	
Condition: When using Fabric Watch and SNMP, etc to monitor a switch, E-port pktloss raslog, VE-port and E-port pktloss trap can be misleading.	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000471135	
Technical Severity: High	Probability: Medium
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.2.0	Technology Area: Trunking
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: RTWR-1003 RASLOG messages: Loss of connectivity.	
Condition: This is a rare occurrence that may be encountered when both E-ports of a 2-E-port trunk go offline during hafailover/hareboot.	
Recovery: Disable both ports in the 2-E-port trunk, then enable them again.	

Defect ID: DEFECT000473087	
Technical Severity: High	Probability: Low
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.2.0	Technology Area: FC-FC routing
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Customer could see different symptoms, such as: 1. RTWR error due to frame drop on 16G FCR 2. Fabric domains are inconsistent between fabric module and routing module, which cause Fport cannot come online.	
Condition: If non-trunked EX-port is configured, when remote side of the EX-port goes down (i.e E-port disabled), in a multiple 16G FCR Backbone-to-Edge configuration, iswitchd will not remove the LE domain. It will retain the LE domain even though its proxies are removed. During this time, all the domain controller frames to the LE domain are dropped. This does not impact 4G/8G FCR switches. However, SCN is not sent and could impact fabric rebuild.	

Defect ID: DEFECT000473289	
Technical Severity: High	Probability: Low
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.2.0	Technology Area: Routing
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: RTWR-1003 RAS logs.	
Condition: This problem may occur from the following sequence: 1. One switch is connected off a loop topology 2. The loop topology is physically changed to a linear topology 3. One of the switches that was in the loop undergoes an hareboot	
Recovery: Bounce an ISL connecting the switch originally outside the loop topology.	

Defect ID: DEFECT000475645	
Technical Severity: Medium	Probability: Medium
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.0.2	Technology Area: End-to-end Performance Monitoring
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Updated End-to-End monitor shows previous data.	
Condition: After removing and replacing an EE monitor (with the SID and DID reversed) the data from the original EE monitor is shown instead of zeros.	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000477795	
Technical Severity: Medium	Probability: Low
Product: FOS	Technology: Management
Reported In Release: FOS7.2.0	Technology Area: Web Tools
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Users will not be able to see the current data for SFP diagnostics.	
Condition: SFP tab on webtools not display the current data even after selecting “Refresh Now” option.	
Workaround: Use CLI sfpsnow	

Defect ID: DEFECT000477854	
Technical Severity: High	Probability: Low
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.0.2	Technology Area: ICLs - Inter-chassis Links
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: CRC with good EOF errors are reported on multiple ICL ports in DCX	
Condition: This issue is seen rarely on DCX platforms	

Defect ID: DEFECT000482106	
Technical Severity: Medium	Probability: Medium
Product: FOS	Technology: FICON
Reported In Release: FOS7.1.0	Technology Area: FICON CUP
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Fbusy encountered when trying to bring up CUP connections following FCIP tunnel bounces.	
Condition: This may be seen only on FICON switches when attempting to bring up CUP connection after an FCIP tunnel is bounced.	

Defect ID: DEFECT000482736	
Technical Severity: High	Probability: Low
Product: FOS	Technology: FICON
Reported In Release: FOS7.1.0	Technology Area: FICON CUP
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Enabling FMS mode leads to floods of internal FICU raslog after code upgrade.	
Condition: This happens when there are 10 or more outstanding FRU failure messages.	

Defect ID: DEFECT000484414	
Technical Severity: High	Probability: Medium
Product: FOS	Technology: Virtualization
Reported In Release: FOS7.0.2	Technology Area: Access Gateway
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Under rare conditions, Access Gateway(AG) entries stay in management server (MS) database even after removing them from the fabric. FOS firmware is expected to remove these stale entries during execution of agshow CLI command. However, due to a timing issue the stale entries may not be removed from the database when agshow CLI command is run.	
Condition: This may be observed on a switch running firmware version higher than v7.0.	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000485708	
Technical Severity: High	Probability: Medium
Product: FOS	Technology: Virtualization
Reported In Release: FOS6.4.3_dcb	Technology Area: NPIV
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: 3rd party application fails when connected to a BR8470 FCoE switch running FOS v6.4.3_dcb in Access Gateway mode. Device re-FDISC on one of its logins is incorrectly rejected by the Access Gateway.	
Condition: This issue occurs under the following conditions: 1. Switch is in Access Gateway mode 2. Device has already logged into a NPIV port on Access Gateway 3. NPIV device has also already logged in (with FDISC) to the same port 4. NPIV device logs in again (with FDISC) on the same port	
Recovery: Bounce (offline, then online) the Access Gateway port.	

Defect ID: DEFECT000486638	
Technical Severity: High	Probability: High
Product: FOS	Technology: FICON
Reported In Release: FOS7.1.0	Technology Area: FICON CUP
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: The following issue is observed often and leads to disruptive Ficon operations: "KSWD-1002 termination of process ficud".	
Condition: This may occur when there are more than 8 trunk groups in a fabric configuration.	

Defect ID: DEFECT000490533	
Technical Severity: High	Probability: Medium
Product: FOS	Technology: Distance
Reported In Release: FOS7.1.0	Technology Area: Extended Fabrics
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: FDR (Fast Dump Restore) disk copy MVS jobs fail with zHPF mode enabled.	
Condition: This may occur when zHPF mode is enabled and I/Os include a large number of frames in a FC sequence	
Workaround: Disable zHPF mode on the connected mainframes.	
Recovery: No recovery exists besides restarting the job with zHPF mode disabled	

Defect ID: DEFECT000490564	
Technical Severity: Medium	Probability: High
Product: FOS	Technology: Security
Reported In Release: FOS6.4.0	Technology Area: Encryption
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: User may experience failures on BES encryption switch in diagnostic tests such as POST Turboramtest.	
Condition: This may happen during stress testing with repeated power resets on BES.	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000490754	
Technical Severity: High	Probability: Medium
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.0.2	Technology Area: BB Credits
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Switch ports connected to storage controller become unresponsive.	
Condition: This rare condition may occur with Fabric Loop (FL) port after many resets. The port may get into "Port failed due to busy buffer stuck error" state.	
Recovery: Reboot switch to recover; portdisable/port enable does not recover.	

Defect ID: DEFECT000490979	
Technical Severity: Medium	Probability: Medium
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.2.1	Technology Area: FC-FC routing
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: FCR LSAN devices are stuck in initializing state	
Condition: This may occur when using BR7800s or FX8-24 in a VEX-VE configuration and when WWN read/write failed.	

Defect ID: DEFECT000492340	
Technical Severity: Medium	Probability: Low
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.3.0	Technology Area: BB Credits
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: User may notice frame drops on the back end edge and core ports with FS8-18 and FX8-24 in the chassis.	
Condition: This may be seen when FS8-18 and FX8-24 blades are used in a 8510-4 or 8510-8 chassis.	
Recovery: Upgrade code with fix and perform a power cycle of port blade to have the new credit buffer allocation scheme to take effect.	

Defect ID: DEFECT000492704	
Technical Severity: High	Probability: High
Product: FOS	Technology: Traffic Management
Reported In Release: FOS6.4.3	Technology Area: FC-FC routing
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: "CRC error with good EOF" errors detected and may cause credit loss.	
Condition: This may be seen on DCX-4S: 1. With FC8-64 blades installed in - Slot 7 ports 155, 76 or - Slot 2 port 154. 2. Core blade 3/19,3/26, 6/70	
Recovery: Auto Tuning/Manual Tuning	

Closed with Code Change in Prior released version of FOS

Defect ID: DEFECT000492854	
Technical Severity: High	Probability: Low
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.1.0	Technology Area: FC-FC routing
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Following a planned device outage, many ports are displayed as “FC Disabled (Port Throttled)”. Ports do not come online for a long time.	
Condition: This may occur when a large number of devices with laser on but cannot complete link initialization with a switch. It typically occurs during device power cycle, upgrade, or running diagnostics.	
Workaround: Stage the number of devices coming online at the same time.	
Recovery: Disable the devices that cannot come online to give other ports a chance.	

Defect ID: DEFECT000495636	
Technical Severity: High	Probability: High
Product: FOS	Technology: Traffic Management
Reported In Release: FOS7.1.0	Technology Area: Buffer Credit Recovery
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: Switch panic during CP blade replacement.	
Condition: On a very congested switch with lots of BE link resets, the event of bringing down a CP blade may cause a panic condition during the blade shutdown procedure.	

Defect ID: DEFECT000501917	
Technical Severity: Medium	Probability: Low
Product: FOS	Technology: Security
Reported In Release: FOS7.2.1	Technology Area: Encryption
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: In encryption environment with BES/FS8-18, switch or blade became faulty during initial discovery of target.	
Condition: It may happen after EE became online and during initial discovery of targets, if the target returns error for slow path commands(REPORT_LUN/INQUIRY).	

Defect ID: DEFECT000501919	
Technical Severity: Medium	Probability: High
Product: FOS	Technology: Monitoring/RAS
Reported In Release: FOS7.3.0	Technology Area: Diagnostic Port (D_Port)
Closed In Release(s): FOS7.1.2a(Fixed)	
Symptom: D-Port test PASSED with errors on D-Port Responder side.	
Condition: After electrical or optical loopback test, stats are not cleared in responder.	
Workaround: Ignore none zero stats on responder side when running D-Port test.	
Recovery: None needed.	