BROCADE

Brocade Fabric OS v7.0.0b Release Notes v2.0

October 5th, 2011

Document History

Document Title	Summary of Changes	Publication Date
Brocade Fabric OS v7.0.0b Release Notes v1.0	Initial Release	August 24, 2011
Brocade Fabric OS v7.0.0b Release Notes v2.0	Added an Important Note related to ISL segmentation when QoS is enabled on an ISL connecting 4G or 8G FC platform to a 16G FC platform. Update with additional Important Notes for Brocade 8000 and FCOE10-24 blades.	October 5th, 2011

© 2011 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, DCX, Fabric OS, and SAN Health are registered trademarks, and Brocade Assurance, Brocade NET Health, Brocade One, CloudPlex, MLX, VCS, VDX, and When the Mission Is Critical, the Network Is Brocade are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. Other brands, products, or service names mentioned are or may be trademarks or service marks 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.

The authors and Brocade Communications Systems, Inc. shall have no liability or responsibility to any person or entity with respect to any loss, cost, liability, or damages arising from the information contained in this book or the computer programs that accompany it.

Notice: The product described by this document may contain “open source” software covered by the GNU General Public License or other open source license agreements. To find-out which open source software is included in Brocade products, view the licensing terms applicable to the open source software, and obtain a copy of the programming source code, please visit *http://www.brocade.com/support/oscd*.

Export of technical data contained in this document may require an export license from the United States Government.

Contents

Overview

Quick Look

If you are already using the most recent version of the Fabric OS v7.0.0a Release Notes, the following are the significant changes in this version:

- The defects closed in Fabric OS v7.0.0b are tabulated at the end of this document.

New Hardware Support

FOS v7.0 introduces support for the following new 16G FC hardware platforms:

- DCX8510-8 and DCX8510-4
  - Includes support for FC16-32 and FC16-48 16 Gbps FC port blades on DCX8510-8 and DCX8510-4 platforms
  - New 16G core blades, CR16-8 on DCX8510-8 and CR16-4 on DCX8510-4
  - Supports 2/4/8/10/16 Gbps FC for both open systems and FICON environments
  - Supports increased ICL bandwidth up to 2 Tbps (with optional licenses) on DCX8510-8, and up to 1 Tbps on DCX8510-4, and ICL distance up to 50m enabling flexible topologies
  - Supports up to eight slots for port blades and/or application blades on DCX8510-8 and up to four slots for port blade and/or application blades on DCX8510-4

Note: Complete blade matrix supported on DCX8510platforms in FOS v7.0 can be found in the *Blade Support* section of this release note.

- Brocade 6510
  - Supports 48 16 Gbps FC ports
  - Ports are capable of operating 2/4/8/10/16 Gbps FC for both open systems and FICON
  - Supports Access Gateway mode
  - Supports Virtual Fabrics with up to 4 Logical Switches

These new hardware platforms also support several unique features and capabilities enabled by FOS v7.0 that are described throughout this document.

Summary of New Software Features

In addition to support for the new hardware, there are numerous new features and enhancements in FOS v7.0, including:

- In-flight Encryption and Compression on 16G capable ISLs
- Buffer Credit Loss Detection and Automatic Recovery on 16G capable ISLs
- 10G FC Capability on 16G FC platforms
- Advanced Diagnostics Support on 16G FC Platforms, including D-Port support and Forward Error Correction (FEC)
- FCIP Enhancements
  - 10GigE lossless failover on FX8-24
  - Multi-Gigabit circuits on FX8-24 10GigE
  - Adaptive Rate Limiting on FX8-24 10GigE ports
  - Configurable QoS for FCIP tunnels on FX8-24 and 7800
  - Auto-mode option for compression on FX8-24 and 7800
  - XISL Support on FX8-24 – Ability to use VE ports as XISLs
  - InBand Management for FX8-24 and 7800
  - Relaxing subnet restrictions for FX8-24 and 7800
  - FCIP FICON Acceleration Enhancements for FX8-24 and 7800

    - GigE/xGigE port sharing across Logical Switches on FX8-24
    - Increase in number of circuits per tunnel on 1GigE ports (6 circuits per tunnel on 7800 and 10 circuits per tunnel on FX8-24)
- Encryption Platform Enhancements (Brocade Encryption Switch/FS8-18)
    - Support for Key Vault Diagnostics
- Access Gateway Enhancements
    - Detection of unreliable N-port links
    - RADIUS/LDAP support
    - APM (Advanced Performance Monitoring) capability
    - F-port static mapping
- Fabric Watch Enhancements
    - Switch Status Policy enhancements
    - Support for multiple e-mail recipients for Fabric Watch events
    - Advanced SFP monitoring based on SFP type – 16G SFP+, 10G SFP+, 4 x 16G QSFP
    - SFP monitored as a FRU (Field Replaceable Unit)
    - Additional Fabric Watch enhancements
- Advanced Performance Monitoring (APM) Enhancements
    - Coexistence of TopTalkers and APM on 16G platforms
    - E-port TopTalkers support and E-port End to End monitor support on 16G platforms
    - APM support on Access Gateway – End to End monitors and Frame monitors
- Security Enhancements
    - User defined roles/RBAC
    - SSH public key authentication support for multiple users
    - SFTP support for firmware download/config upload/download
    - IPv6 support for LDAP authentication
    - Switch banner support
    - Removing support for Brocade certificates for FCAP authentication
- Dynamic Fabric Provisioning - Fabric Assigned WWN
- Fabric Services Enhancements and Updates
    - Allow a switch with default zone “no access” to merge with a fabric
    - Detection and resolution of duplicate WWNs
    - RASlogs to indicate invalid TI (Traffic Isolation) zones
    - Ability to assign names to logical fabrics
- Additional RAS and Diagnostics Enhancements
- FCoE Enhancements (Also supported in FOS v6.4.1_fcoe1)
    - High Availability of the FCoE storage traffic going through FCOE10-24 blades on DCX/DCX-4S
    - Enhanced FCoE provisioning
    - Auditlog support for DCB/CEE configuration events
    - Enhanced scalability - Increased the number of FCOE10-24 blades supported on the DCX and DCX-4S from 2 to 4. Support for up to 96 10 GE DCB ports per DCX/DCX-4S
    - Support for additional DCB/CEE MIBs

New Feature Descriptions

In-flight Encryption and Compression on 16G capable ISLs

The in-flight encryption/decryption and compression/decompression features allow frames to be encrypted or compressed while traversing 16G capable ISLs. In-flight encryption provides security for frames while they are passing between two switches. Compression improves bandwidth utilization on the ISLs, especially over long distance. Encryption and compression are both disabled by default but may be enabled at an individual port level. A maximum of 2 ports at a time on Brocade 6510 and a maximum of 4 ports at a time on each FC16-XX blade can support encryption and compression. Encryption and compression can be enabled simultaneously on an ISL, or just encryption or compression can be enabled. There is no additional license required to use the in-flight encryption or compression capabilities.

Note: This feature is enabled by the ASIC used on 16G FC platforms and it is independent of the speed at which the ISL is currently operating.

Buffer Credit Loss Detection and Automatic Recovery on 16G capable ISLs

FOS v7.0 adds support for the detection and automatic recovery of buffer credits on 16G capable ISLs (both ends of the link must be terminating on 16G capable port). Loss of a single buffer credit is detected at individual virtual channel level and is automatically recovered without performing link reset. Loss of multiple buffer credits and stuck VC (VC in permanent zero buffer credit condition) conditions are recovered by performing link reset. RASlogs are generated when credit loss is detected and when the link reset is performed.

10G FC Capability on 16G FC Platforms

A port on a Brocade 6510 switch or on an FC16 blade can be configured to operate at 10G FC. This feature requires a 10G FC slot based license on DCX8510 (for each blade that will have 10G FC ports) and 10G FC license on Brocade 6510. In FOS v7.0 this feature is supported only on the first eight ports of Brocade 6510 and each FC16-XX blade.

Advanced Diagnostics Support on 16G FC Platforms

D-port Support

FOS v7.0 introduces the concept of the Diagnostic port or D-port. D-Port feature diagnoses the components associated with a link such as SFPs and cables. This test performs connectivity checks between various components on the ISL, drives link saturation and measures link distance. This feature is supported on ISLs between 16G FC platforms using Brocade branded 16G SFP+.

Forward Error Correction (FEC)

The FEC feature allows recovering of error bits in a 10G or a 16G data stream. It can correct up to 11 error bits in every 2112-bit transmission. This feature is enabled by default on all ISLs of 16G FC platforms.

Real-time Power Monitoring

The new 16G blades (FC16-32, FC16-48, CR16-8 and CR16-4) support real-time measurement of power being consumed by those blades. The real-time power consumption of 16G blades can be displayed using the chassisshow command.

Advanced SFP Monitoring

Fabric Watch has been enhanced to monitor 16G SFP+, 10G SFP+ and 4 x 16G QSFP. It also allows thresholds to be configured based on the type of the SFP.

Dynamic Fabric Provisioning - Fabric Assigned WWN

In order to simplify and accelerate server deployment and improve operational efficiency, FOS v7.0 now provides Fabric Assigned WWN or FA-WWN which uses a virtual WWN for a server instead of the server's physical PWWN to create zoning and LUN mapping/masking. When a FA-WWN capable server is attached to the SAN, this feature allows the fabric to assign this virtual WWN to that server. This feature requires servers to

be using Brocade HBAs/Adapters with appropriate HBA drivers that support this capability. Also, configuration is required at the HBA to utilize FA-WWN.

Note: The minimum required Brocade HBA driver version and the FOS release that supports this capability will be documented once the Brocade HBA driver is available.

FCIP Enhancements

FOS v7.0 implements the following FCIP enhancements:

10GigE lossless failover on FX8-24

The 10GigE lossless failover feature allows users to configure a new set of IP addresses and allow a tunnel to failover to the secondary 10GigE port. There are two types of configuration that are supported: active/active and active/passive. In active/active case, the data will be sent on both 10GigE ports thus load-balanced across 10GigE ports. In active/passive case, the data is failed-over to a passive circuit (one with a higher metric) if all active circuit paths fail. This feature is supported on FX8-24 blades only in 10G mode.

Multi-Gigabit circuits on FX8-24 - allowing more than 1Gbit/s to be configured on a single FCIP Circuit

The Multi-Gigabit Circuit implementation has the following capabilities:

- Support for circuits with a rate configured at more than 1 Gbit/s
- Allow for up to 10Gbit/s minimum rate circuit using a single IP address pair
- Support for 10GigE to 10GigE connections only on multi-gigabit circuits

This feature is supported on FX8-24 blades only in 10G mode.

10GigE Adaptive Rate Limiting (ARL) on FX8-24

The 10GigE ARL feature allows users to configure minimum and maximum rates for each circuit of a tunnel that is using xge0 or xge1 on an FX8-24 blade.

The 10GigE ARL feature provides the following capabilities:

- Support for ARL on tunnels over the 10GigE ports
- Maximum guaranteed rate of 10Gbit/s combined for all tunnels over a single 10GigE port
- Maximum rate of 10Gbit/s for any single circuit

Configurable QoS on FCIP tunnel

The configurable QoS option allows a user to override the default percentages of bandwidth assigned to each of the QoS classes within an FCIP tunnel. The default values will be that of pre-FOS v7.0 predefined rates; 50% for high, 30% for medium, and 20% for low priority traffic. This feature is supported on FX8-24 and 7800.

Auto-mode option for compression

On FX8-24 and 7800, a new compression mode called "auto-mode" is supported starting with FOS v7.0. This feature will adjust the compression mode (1, 2 or 3) based on the maximum configured tunnel bandwidth. In the auto mode, best compression mode is selected based on the configured maximum bandwidth of the tunnel and advanced compression bandwidth usage in the system.

XISL Support ON FX8-24– Ability to use VE ports as XISLs

This feature enables multiple logical fabrics to share a single base fabric while providing fabric-level isolation in Virtual Fabrics environment. Specifically, it will enable logical connectivity over FCIP between otherwise disconnected segments of a fabric. This feature is supported only on FX8-24 blades in both 1G and 10G modes.

InBand Management on FX8-24 and 7800

The InBand Management feature allows a user to define one or more IP addresses on the non-management GE ports and provide a management path from WAN (Wide Area Network) to the switch CP. Users can then use these IP addresses to access SNMP events, establish telnet sessions, etc.

Relaxing subnet restrictions

On FX8-24 and 7800 running pre-FOS v7.0 there is a restriction where each IPv4 Gigabit Ethernet interface must have IP addresses on a separate subnet from all other interfaces and IPv6 addresses must be on separate prefixes from all other interfaces. Additionally the IPv6 interfaces must have a unique link-local address from the peer node on that interface.

Beginning with FOS v7.0 the above restrictions have been lifted.

FCIP FICON Acceleration Enhancements

There are several new capabilities added for FICON acceleration in FOS v7.0. They are:

- Support for Optica's Prizm connected to 3480, 3490 and 3590 ESCON Tape control units
- Support for Optica's Prizm and ESBT connected to 3480 Bus and Tag Tape control units
- New FICON Acceleration Feature for Teradata controllers

GigE/xGigE port sharing across Logical Switches

On FX8-24 running pre-FOS v7.0, to create a tunnel in an LS, both the VE-port and the corresponding GE-port must be in the same Logical Switch (LS). Starting with FOS v7.0, this limitation is removed, that is, VE ports in different LSs will be able to share a GE-port/xGE-port which is present in the Default Switch.

Increase in number of circuits on 1GE ports

In FOS v7.0 the number of circuits supported per tunnel on 1GE ports has been increased as follows:

- Up to 6 circuits per tunnel on 7800
- Up to 10 circuits per tunnel on FX8-24

Encryption Platform Enhancements (BES/FS8-18)

Key Vault Diagnostics

FOS v7.0 includes support for the key vault diagnostics. The key vault connectivity information will be periodically collected and any connectivity errors are reported as RASlog.

Access Gateway Enhancements

Detection of Unreliable N-Port Links

This feature monitors the reliability of a link on every N-port of an Access Gateway. If the number of ONLINE/OFFLINE SCNs (State Change Notifications) for a port exceeds a certain threshold within a predefined time period, the link is considered unreliable and failback is disabled for that port. Once the port is reliable again, user configured failback settings will be enforced. The port becomes reliable when the number of SCNs is less than the threshold value in the most recent time interval.

RADIUS/LDAP support

RADIUS/Active Directory for user management is supported on the switches operating in AG mode starting with FOS v7.0.

APM (Advanced Performance Monitoring) End to End and Frame Monitoring capability

Select Advanced Performance Monitoring capabilities in AG mode are new features introduced in the FOS v7.0 release. Two types of performance monitors are supported in AG mode: End to End Monitor and Frame Monitor.

F-Port Static Mapping

This feature allows users to change an existing F to N-port mapping by executing a single CLI. Here, F-ports are statically mapped to an N-port and port properties such as failover/failback/preferred are always disabled. This new static mapping capability is in addition to previously supported F to N-port mappings where a user must execute multiple CLIs to map an F-Port to an N-port.

Fabric Watch Enhancements

Switch Status Policy enhancements

In FOS v7.0 the switch status policy of Fabric Watch has been enhanced as follows:

- The new component "Error Ports" is introduced in the switch status policy to monitor ports which are segmented and disabled due to several reasons such as security violations and port fencing.
- The unit for thresholds (both default and user defined) of Marginal, Faulty, Error Ports and Missing SFPs are changed to the percentage of the current number of physical ports present in the switch at a given instance of time rather than the absolute number of physical ports that a switch can support. The total number of physical ports accounted in the switch status policy during threshold calculation excludes FCoE /VE ports/Internal Ports.

Support for multiple e-mail recipients for Fabric Watch Events

The Fabric Watch mail alert feature is used to notify the user of events through a configured email address. In pre-FOS v7.0 releases, Fabric Watch allowed users to configure a single email recipient for each class to receive the email alerts. In FOS v7.0, this feature is enhanced to configure multiple email recipients. A maximum of five recipients per class can be configured using the "fwMailCfg" command.

Advanced SFP monitoring based on SFP type

In FOS v7.0 Fabric Watch can monitor voltage, current, RXP (receive power), TXP (transmit power), temperature and operational hours of 16G SFP+.

Fabric Watch monitors voltage, temperature, RXP, and current for the 4 x 16G QSFP media.

Fabric Watch monitors voltage, temperature, RXP, TXP and current for the 10G FC SFP+.

Fabric Watch applies "sfptype" based thresholds for SFP monitoring. If Fabric Watch does not find the SFP's sfptype in its threshold database then it applies the "Other" thresholds (pre-FOS v7.0 thresholds) on the SFP.

Note: By default Fabric Watch monitoring is disabled on 16G SFP+, 10G SFP+, and 4 x 16G QSFP. Advanced "sfptype" monitoring can be enabled on these SFPs using the new command "thmonitor".

SFP monitored as a FRU (Field Replaceable Unit)

In FOS v7.0 Fabric Watch has been enhanced to monitor SFPs as FRUs (Field Replaceable Units).

If a FRU state changes, Fabric Watch sends an email or generates a RASlog message. Users can configure email or RASlog actions for each FRU state using the "`fwFruCfg`" CLI.

Additional Fabric Watch Enhancements

- Pause and Continue monitoring functionality is provided to monitor specific components at an element level granularity in FOS v7.0. This feature allows users to stop or start monitoring of a set of thresholds related to certain class, area, and index.
- Thresholds for Packet loss area of VE port class can configured to a real number up to two decimal places (0.00 to 100.00)
- All parameters under port monitoring and SFP monitoring will not be monitored on port(s) without SFP(s). Also, only voltage, temperature, and power-on-hours parameters of SFPs will be monitored for offline ports (where SFPs are physically present but ports are offline).
- Fabric Watch supports monitoring End to End and Frame monitor classes on Access Gateway platforms
- fwconfigure and fwshow CLIs are not supported in FOS v7.0
- Second time base and changed event are not supported in FOS v7.0. If any of this is configured, then the upgrade to FOS v7.0 will be blocked.

Advanced Performance Monitoring (APM) Enhancements

Coexistence of TopTalkers and FCR on 16G platforms

In FOS v7.0 TopTalkers (Fabricmode/Port level) and FCR features can be enabled simultaneously on 16G platforms such as DCX8510-8/DCX8510-4 with 16G based blades only, and on Brocade 6510 switch.

E-port TopTalkers support and E-port End to End monitors support on 16G platforms

In FOS v7.0 the Port level TopTalkers are supported on E-port(s) of 16G platforms. The functionality provided by the Port level TopTalkers on E-ports is the same as the one provided by the Port level TopTalkers on F-ports.

Security Enhancements

User defined roles/RBAC

The User-defined role is a feature in FOS v7.0 that provides the ability to create user roles dynamically to manage the switch. This is in contrast to pre-defined user roles supported in pre-FOS v7.0 releases.

The maximum number of user-defined roles that are allowed on a chassis is 256.

Switch banner support

A new command *motd* is added to configure whether a chassis banner should be displayed before user login.

Removing support for Brocade certificates for FCAP authentication

Starting with FOS v7.0, FOS will **not support** installation/FCAP-authentication using **Brocade issued certificates**. However, third-party certificates can still be used for FCAP authentication.

SSH authentication using public keys

FOS v7.0 supports SSH public key based authentication for multiple users.

SFTP support for firmwaredownload, configupload and configdownload

Users now have the flexibility of choosing SFTP protocol for performing firmwaredownload, configupload/configdownload operations.

IPv6 support for LDAP authentication

FOS v7.0 includes IPv6 support for LDAP authentication. FOS now accepts IPv6 addresses for Active Directory servers.

Fabric Services Enhancements and Updates

Allow a switch with default zone “no access” to merge with a fabric

FOS v7.0 allows a switch with default zone “no access” and with no zoning configuration to merge with a fabric that has active zone configuration.

Duplicate WWN detection and resolution

FOS v7.0 implements a feature to detect duplicate device WWNs in a fabric. It also enables users to configure a policy to take actions once duplicate WWNs are detected.

RASlog upon detecting Invalid TI zones

In a failover disabled configuration of a TI zone, if the switch (domain) becomes unreachable, users will be informed about this domain unreachable condition via a RASlog message which helps users to diagnose and resolve this problem quickly.

Ability to assign names to logical fabrics

The fabric naming feature allows users to assign a user friendly name to identify and manage a logical fabric.

No direct E-port support with legacy M-series (McDATA) switch

FOS v7.0 supports only interopmode 0 and does not support interoperability with an M-series (McDATA) switch via direct E-port connectivity. FCR can be used to establish connectivity between a fabric with M-series switch and a fabric with FOS v7.0 switch.

Additional RAS and Diagnostics Enhancements

Spinfab enhancements

The spinfab diagnostics utility has been enhanced to test ISLs at higher link utilization by using all buffers available at a port. This feature is supported on both 8G and 16G FC platforms.

Frame Viewer

The Frame Viewer feature introduced in FOS v7.0 is intended to provide more visibility to SAN administrators regarding discarded frames due to timeout reason. This feature is supported both on 8G and 16G platforms.

Port Decommission

The Port Decommission feature provides users with the ability to non-disruptively remove an ISL from service. When an ISL is selected for decommissioning, the switches communicate with each other to coordinate the movement of flows off of the ISL to alternative paths. Once the flows are moved to alternative paths, the switches block the E_Ports associated with the ISL being decommissioned to complete the decommission process.

Firmware History Log

FOS v7.0 implements a log that keeps track of the firmware versions installed on a switch. The firmware history log retains details of up to the last twenty versions of firmware installed on a switch. This log is available from and stored on the switch.

Ability to assign longer port names

FOS v7.0 allows users to assign a port name up to 128 characters which is an increase from a maximum of 32 characters supported in a pre-FOS v7.0 release.

FOS version in Auditlog message header

FOS v7.0 adds the FOS version to Auditlog messages to enable users identify which FOS version generated a specific Auditlog.

FCoE Enhancements

FOS v7.0 includes all FCoE enhancements implemented in FOS v6.4.1_fcoe1 release. This includes support for High Availability for FCoE traffic going through FCOE10-24 blades in DCX/DCX-4S. Please refer the latest FOS v6.4.1_fcoe1 release notes for additional feature details. Upgrade from FOS v7.0 to a future FOS release on DCX/DCX-4S will be non-disruptive to both FC and FCoE traffics. A CP fail-over on a DCX/DCX-4S running FOS v7.0 will not disrupt the FCoE traffic through FCOE10-24 blade.

Optionally Licensed Software

Fabric OS v7.0 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 v7.0 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 Extended Fabrics—Provides greater than 10km of switched fabric connectivity at full bandwidth over long distances (depending on 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.

High Performance Extension over FCIP/FC (formerly known as "FCIP Services") (For the FR4-18i blade) — This license key also includes the FC-FastWrite feature and IPsec capabilities.

Note: The FC-FastWrite feature is not supported on FR4-18i in FOS v7.0.

Brocade Accelerator for FICON – This license enables unique FICON emulation support for IBM's Global Mirror (formerly XRC) application (including Hitachi Data Systems HXRC and EMC's XRC) as well as Tape Pipelining for all FICON tape and virtual tape systems to significantly improve XRC and tape backup/recovery performance over virtually unlimited distance for FR4-18i.

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.

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.

Server Application Optimization — 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.

Integrated Routing— This license allows any port in a DCX8510-8, DCX8510-4, Brocade 6510, 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/DCX8510-8/DCX8510-4, 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/DCX8510-8/DCX8510-4 chassis.

DataFort Compatibility — This license is required on the Brocade Encryption Switch or DCX/DCX-4S/DCX8510-8/DCX8510-4 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/DCX8510-8/DCX8510-4 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/DCX8510-8/DCX8510-4 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, this license enables 10G FC ports. This license is available on the DCX/DCX-4S/DCX8510-8/DCX8510-4 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**: 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/DCX8510-8/DCX8510-4 for the FX8-24 on an individual slot basis.

7800 Port 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 DCX8510 platforms. An ICL 1st POD license only enables half of the ICL ports on CR16-8 core blades of DCX8510-8 or all of the ICL ports on CR16-4 core blades on DCX8510-4. An ICL 2nd POD license enables all ICL ports on CR16-8 core blades on a DCX8510-8 platform. (The ICL 2nd POD license does not apply to the DCX8510-4.)

Temporary License Support

The following licenses are available in FOS v7.0 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
- Advanced Extension license
- Advanced FICON Acceleration license
- 10GbE FCIP/10G Fibre Channel license

- FICON Management Server (CUP)

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 Support

The following list of licenses are available as Universal Temporary licenses, meaning the same license key can be installed on any switch running FOS v6.3 or later that supports the specific feature. 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.

- 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
- Advanced Extension license
- Advanced FICON Acceleration license
- 10GbE license/10G Fibre Channel license
- FICON Management Server (CUP) license

Supported Switches

Fabric OS v7.0 supports the Brocade 300, 5410/5424/5450/5460/5470/5480/NC-5480, 5100, 5300, VA-40FC, Brocade Encryption Switch (BES), DCX/DCX-4S, 8000, 7800, 6510, DCX8510-8 and DCX8510-4.

Access Gateway mode is also supported by Fabric OS v7.0, and is supported on the following switches: the Brocade 300, 5100, VA-40FC, 8000, 5450, 5460, 5470, 5480, NC-5480, M5424 and 6510.

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, 5000, 5100, 5300, 6510 — 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, DCX8510-8 — Bottom right of the port side
- Brocade DCX-4S, DCX8510-4 — 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 DCX8510-8/DCX8510-4. For the Brocade DCX/DCX-4S and DCX8510-8/DCX8510-4 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.

4. **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 **licenseId** command to display the License Identifier.

FOS Migration Considerations

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

TSBs - Critical Issues to Consider Prior to Installing This FOS Release

Technical Support Bulletins (TSBs) are produced to provide detailed information about high priority defects or issues present in FOS releases. The following sections specify all current TSBs that have been identified as being a risk to or resolved with this specific version of Fabric OS. Please review carefully and refer to the complete TSB for relevant issues prior to migrating to this version of code. TSBs can be found at http://my.brocade.com under the "*Technical Documentation*" section of the "*documentation*" tab.

TSB Issues Outstanding in FOS v7.0.0b

Issues in the following list of TSBs are known to be potential risks to using FOS v7.0.0b and should be considered carefully prior to using this release of code:

TSB	Summary
None	

TSB Issues Resolved in FOS v7.0.0b

Issues in the following list of TSBs are known FOS v7.0.x risks that are not exposures in FOS v7.0.0b. Note that the issues addressed in this list of TSBs may also be resolved in other FOS releases. Refer to the specific Release Notes for each release to verify resolution details.

TSB	Summary
None	

Recommended Migration Paths to FOS v7.0

Migrating from FOS v6.4.x

DCX/DCX-4S units running any FOS v6.4.x release can be non-disruptively upgraded to FOS v7.0.

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 before non-disruptively upgrading to FOS v7.0. Upgrading these platforms from any FOS V6.4.x release **lower than FOS v6.4.1a to FOS v7.0 will cause disruption to FC traffic**.

Upgrading any 8G platform operating at FOS v6.4.1a or later to FOS v7.0 is non-disruptive to FC traffic.

Migrating from FOS v6.4.1_fcoe1

The upgrade from FOS v6.4.1_fcoe1 to FOS v7.0 is non-disruptive to both FC and FCoE traffic on DCX and DCX-4S.

Note: Upgrading from FOS v6.4.1_fcoe or FOS v6.4.x releases other than v6.4.1_fcoe1 to FOS v7.0 will be disruptive to FCoE traffic going through FCOE10-24 blades in DCX/DCX-4S. When loading FOS v7.0 with Brocade Network Advisor v11.1.1/11.1.1a, there is no warning flagging this FCoE traffic disruption.

Migrating from FOS v6.3.x

To non-disruptively migrate from FOS v6.3.x to v7.0, units should first load FOS v6.4.1a (v6.4.1b should be used for encryption platforms, units operating in Access Gateway mode, or units with ports configured as EX or VEX for FCR), and then migrate to FOS v7.0.

FOS Upgrade and Downgrade Special Considerations

The DCX/DCX-4S units running any FOS v6.4.x can be non-disruptively upgraded to FOS v7.0. This upgrade is non-disruptive to FC traffic only. When loading FOS v7.0 to a DCX chassis with FCOE10-24 blades with Brocade Network Advisor v11.1.1/11.1.1a, there is no warning flagging FCoE traffic disruption.

The DCX/DCX-4S units running FOS v6.4.1_fcoe1 can be non-disruptively upgraded to FOS v7.0. This upgrade is non-disruptive to both FCoE traffic through FCOE10-24 blades and FC traffic.

Non-disruptive upgrade to FOS v7.0 on 8G switches is allowed from **FOSv6.4.1a** or later.

Disruptive upgrades to Fabric OS 7.0 are allowed and supported from FOS 6.3 (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 v7.0 will be disruptive to the I/O through the switch.

FC FastWrite , EX_Ports, and TCP byte streaming on FR4-18i must be disabled prior to upgrading to FOS v7.0. Failure to do so will cause the upgrade to be blocked.
Upgrading a switch currently operating in interopmode 2 or 3 to FOS v7.0 is disruptive. The interopmode must be changed to 0 prior to upgrading to FOS v7.0, as interopmodes 2 and 3 are not supported on FOS v7.0. Changing the interopmode is an offline operation.

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 11.1.0 is available in

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

For SAN Management, Network Advisor 11.1 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 four physical or virtual fabrics (FOS, M-EOS and Mixed fabrics) and up to 2,560 switch ports. It supports Brocade backbone and director products (DCX8510-4/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 24 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 (DCX8510-8/DCX) and Fiber Connectivity (FICON) capabilities.

More details about Network Advisor's new enhancements can be found in the Network Advisor 11.1 Release Notes, Network Advisor 11.1 User Guide, and Network Advisor 11.1 Installation, Migration, & Transition Guides.

Note: Brocade Network Advisor 11.0 and DCFM 10.4 cannot manage switches running FOS v7.0 or later.

DCFM Compatibility

DCFM is not qualified or support the management of switches operating with FOS v7.0 and later firmware versions. **You must first upgrade DCFM to Network Advisor 11.1 or later if you are planning to upgrade devices to FOS v7.0 or you risk losing management connectivity.**

WebTools Compatibility

FOS v7.0 is qualified and supported only with Oracle JRE 1.6.0 update 24.

SMI Compatibility

- It is important to note that host SMI-S agents cannot be used to manage switches running FOS v7.0.

- If users want to manage a switch running FOS v7.0 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]
VA-40FC	v6.2.1_vfc [6], v6.2.2 or later [6]
Brocade DCX-4S	v6.2.0 or later [6]
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
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]
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. M-EOS v9.9.5 or later
McDATA ED-5000 32-port FC director	Not Supported

Multi-Protocol Router interop	
Brocade 7420	Not supported
Brocade 7500 and FR4-18i blade	V6.2.2 and higher [4] [6]
McDATA SANRouters 1620 and 2640	Not Supported

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

[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.

Zoning Compatibility Note:

Users are recommended to upgrade to the following versions of firmware when interoperating with a FOS v7.0 switch 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, then cfgsave and cfgenable operations **initiated** from these switches will fail if the zoning database is greater than 128KB. In such scenarios zoning operations such as cfgsave/cfgenable can still be performed successfully if initiated from a FOS v7.0 switch.

Blade Support

Fabric OS v7.0 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) and the 6-port 10G FC blade (FC10-6)	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.
FCIP/FC Router blade (FR4-18i)	Up to a maximum of 4 blades of this type. This can be extended under special circumstances, but must be approved by Brocade's Product Team. Up to 8 FR4-18i blades can be installed in a DCX if they are used only for FCIP without routing. **Note**: FR4-18i cannot coexist with FX8-24 in FOS v7.0 FR4-18i does not support EX-ports, FC FastWrite and WAN optimization features in FOS v7.0 FR4-18i supports VEX ports on FOS v7.0
Virtualization/Application Blade (FA4-18)	Not supported on FOS v7.0
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
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 v7.0

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

Fabric OS v7.0 software is fully qualified and supports the blades for the DCX8510-8 and DCX8510-4 noted in the table below.

DCX8510-8/DCX8510-4 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 DCX8510 platforms in FOS v7.0
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 on DCX8510 in FOS v7.0**

Table 2 Blade Support Matrix for DCX8510-8 and DCX8510-4 with FOS v7.0

Note: The iSCSI FC4-16IP blade is not qualified for the DCX8510-8/DCX8510-4.

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, 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	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

Power Supply Requirements for Blades on DCX 8510-8					
Number of Ports	**Blades**	**Type of Blade**	**DCX 8510-8 @110 VAC (Redundant configurations)**	**DCX 8510-8 @200-240 VAC (Redundant configurations)**	**Comments**
Any combination of 8Gb or 16Gb ports with QSFP ICLs	FC8-64, FC16-32	Port Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 [1] Power Supplies
256 16Gb ports + QSFP ICLs	FC16-32, FC16-48, FC8-64	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
192 16Gb Ports & max 2 intelligent boards (FX8-24 /FS8-18/combination) with QSFP ICLs	FC16-32, FC16-48, FX8-24, FS8-18	Port / Intelligent Blade	4 Power Supplies	2 Power Supplies	200-240VAC: 1+1 Power Supplies 110VAC: 2+2 [1] Power Supplies Max four FC16-48 port blades and max 2 Intelligent blades
384 16Gb ports + QSFP ICLs	FC16-32, FC16-48, FC8-64	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 with QSFP ICLs	FC16-32, FC16-48, FC8-64, 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

[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, 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.)

Power Supply Requirements for Blades on DCX 8510-4					
Number of Ports	**Blades**	**Type of Blade**	**DCX 8510-4 @110 VAC (Redundant configurations)**	**DCX 8510-4 @200-240 VAC (Redundant configurations)**	**Comments**
96 ports max with QSFP ICLs	FC16-32	Port Blade	2 Power Supplies	2 Power Supplies	1+1 redundancy with 110 or 200-240 VAC power supplies
Any combination of 8Gb or 16 Gb ports and intelligent blades with QSFP ICLs	FC16-32, FC16-48, 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

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 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 in FOS v7.0.
- 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.
- D-Port tests may only be executed on ports configured for "*portcfglongdistance port# L0*" or normal port distance mode. Executing D-Port tests on long distance ports may cause tests to fail due to time out exceeded.

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

- When doing a firmware upgrade to FOS v7.0 or downgrade from FOS v7.0, message SPM-1016 will be observed on FOS v7.0. nodes in the EG (Encryption Group) when there are other nodes in that EG that are still running pre-FOS v7.0. Though this is a warning message, it is transient and is only observed during firmware upgrade/downgrade operation and can be ignored.
- "2011/04/12-18:41:08, [**SPM-1016**], 17132, FID 128, WARNING, pt1b-tw-102, Security database is out of sync. This warning can be ignored if the nodes in the EG are running different versions of FOS."
- Recommendation for IBM's Tivoli Key Lifecycle Manager V2 (TKLM) users is to install TKLM fix pack 2 and set the values for config.keystore.batchUpdateSize and config.keystore.batchUpdateTimer as follows:
- batchUpdateSize=10000
- batchUpdateTimer=60000
- Users upgrading BES/FS8-18 from FOS v6.4.1x or later to FOS v7.0 or later should follow the procedure described below to correctly configure the BES/FS8-18 with TKLM Key Vault. Users should note down the TKLM "device addition/approval" settings using the procedure described below:
- Login to the TKLM, click on go, after selecting "BRCD_ENCRYPTOR" option from the drop down menu below "Guided key and device creation" under "Key and device management" section. A new page opens up with Configure keys. Please select "Step2 Identify drives" option to check the option selected for new devices, mentioned below "**Choose how to handle requests from new devices**".
- There can be three different options available to the users, namely:
    - Only accept manually added devices for communication
    - Automatically accept all new device requests for communication
    - Hold new device requests pending my approval
- Users have to follow one of the following steps based on the current settings at the TKLM Key Vault for key retrieval/archival to succeed from the BES/FS8-18. These steps need to be performed for each BES/FS8-18 node in the EG (Encryption Group) for both primary and secondary TKLM Key Vaults separately.
    - **Only accept manually added devices for communication**
        - Run "cryptocfg --reg -KAClogin" CLI on the BES/FS8-18 running FOS v7.0.0 or later. It will return the device serial name to be used for the node while adding it on the TKLM Key Vault.

- On the TKLM GUI, add the new device with the device serial name returned by the BES/FS8-18 from the above step, under "Devices".

  NOTE: After firmware upgrade is done to FOS v7.0.0 or later, key operations to the TKLM will succeed only after this step is complete.

- **Automatically accept all new device requests for communication**

  - No action is required from the users on BES/FS8-18 for this setting. After the firmware is upgraded to FOS v7.0.0 or later, key operations to the TKLM Key Vault will automatically succeed.

    NOTE: This action modifies the new device acceptance for LTO family and not just BRCD_ENCRYPTOR device group.

- **Hold new device requests pending my approval**

  - Run "cryptocfg --reg -KAClogin" CLI on BES/FS8-18 running FOS v7.0.0. or later This will return the device serial name to be used for the node while adding it on the TKLM Key Vault.
  - On the TKLM GUI, approve the new device request for the device serial name returned by the BES/FS8-18 from the above step.

Note: If the device serial name already exists on the TKLM, there is no effect of running the CLI "cryptocfg –reg –KAClogin" on BES/FS8-18 for any of the above steps.

- Data-at-rest encryption support for IBM SVC LUNs configuration
  - A highly available encryption group is a requirement for IBM SVC deployments. This can be achieved using either an encryption HA cluster (HAC) or a DEK cluster. Failure to deploy high availability in the encryption group could lead to IBM SVC nodes going offline and into service mode when there is no encryption engine online.

    Note: In the case of IBM SVC nodes going offline and into service mode, all SVC ports are affected and not just those configured for encryption operations.

  - Refer to the following IBM publication for general IBM SVC best practices. Specifically for data-at-rest encryption, crypto target container and LUN configuration must be defined in front of the SVC nodes and not between the SVC nodes and disk storage targets.

    - *SAN Volume Controller Best Practices and Performance Guidelines* (http://www.redbooks.ibm.com/abstracts/sg247521.html)

- If the migration to FOS v7.0 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: fcsw0-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.
- The "*cryptocfg –manual_rekey –all*" command should not be used in environments with multiple encryption engines (FS8-18 blades) installed in a DCX/DCX-4S/DCX8510 chassis with more than one encryption engine has access to the same LUN. In such situations, use the "*cryptocfg –manual_rekey <CTC> <LUN Num> <Initiator PWWN>*" command to manually rekey these LUNs.
- When adding nodes to an Encryption Group, ensure all node Encryption Engines are in an enabled state.

- 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) 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) 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.
- When using Brocade Native Mode, in LKM installations, manual rekey is highly recommended. If auto rekey is desired, the key expiry date should be configured only when the LUN is created. Never modify the expiry date after configuring a LUN. If you modify the expiry time, after configuring the LUN the expiration date will not update properly.
- 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.
- For dual NetApp LKM configuration on the Brocade Encryption Switch (BES) or a DCX/DCX-4S/DCX8510 with FS8-18 blades as the primary and secondary key vaults, these LKM appliances must be clustered (linked). Failure to cluster will result in key creation failure. Otherwise, register only one LKM on the BES/FS8-18 Encryption Group. Please refer to the Encryption Admin Guide for configuration information.
- The RSA RKM Appliance A1.6, SW v2.7.1.1 is supported. The procedure for setting up the RKM Appliance with BES or a DCX/DCX-4S/DCX8510 with FS8-18 blades is located in the Encryption Admin Guide.
- Support for registering a 2nd RKM Appliance on BES/FS8-18 is blocked. If the RKM Appliances are clustered, then the virtual IP address hosted by a 3rd party IP load balancer for the RKM 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 is supported. Cryptographic operations and I/O will be disrupted but other layer 2 FC traffic will not be disrupted.

- Relative to the BES and a DCX/DCX-4S/DCX8510 with FS8-18, all nodes in the Encryption Group must be at the same firmware level of FOS v6.2 or later before starting a rekey or First Time Encryption operation. Make sure that existing rekey or First Time Encryption operations complete before upgrading any of the encryption products in the Encryption Group. Also, make sure that the upgrade of all nodes in the Encryption Group completes before starting a rekey or First Time Encryption operation.
- To clean up the stale rekey information for the LUN, follow one of the following two methods:

  Method 1:

  1. First, modify the LUN policy from "encrypt" to "cleartext" and commit. The LUN will become disabled.
  2. Enable the LUN using "cryptocfg --enable –LUN". Modify the LUN policy from "clear-text" to "encrypt" with "enable_encexistingdata" to enable the first time encryption and do commit. This will clear the stale rekey metadata on the LUN and the LUN can be used again for encryption.

  Method 2:

  1. Remove the LUN from Crypto Target Container and commit.
  2. Add the LUN back to the Crypto Target Container with LUN State="clear-text", policy="encrypt" and "enable_encexistingdata" set for enabling the First Time Encryption and commit. This will clear the stale rekey metadata on the LUN and the LUN can be used again for encryption.
- TEMS (Thales Encryption Manager for Storage) key vault support:
- Regarding TEMS key vault (KV) communication with a Brocade encryption group, the default communication port setting for the TEMS KV is 37208, however, the Brocade encryption members and leader use port number 9000, so this needs to be reset on TEMS. Additionally, the following is a checklist of things to review if the initial attempt to connect to the TEMS KV fails:
  - Check physical and logical connection via a ping on port 9000, this should be the first check.
  - For the group leader node, the KAC client certificate and the KV certificate files should be identical.
  - For group member nodes the KV file is to be the same as the KV file on the group leader node.
  - Crosscheck to ensure the private key file corresponds to the KAC public certificate file on any node.
  - For TEMS (Thales Encryption Manager for Storage) users, the following steps need to be done if the user is upgrading TEMS from 1.x to 2.x
    - KV should be deregistered
    - Certificates should be regenerated and KAC certificate of BES should be signed on TEMS 2.x by setting the option on TEMS to SHA1 instead of SHA512
    - Signed KAC certificate and KV certificate should be registered on BES (as documented in Encryption Admin Guide)
    - After the upgrade of TEMS1.0 to TEMS2.0.3 user will need to perform the following:
      - Regenerate CA certs through CLI (officer role) with options SHA-1
      - Regenerate SSL cert though CLI (officer role) with options "users for web server"
      - Log into TEMS GUI as manager
      - Delete all clients and they are not valid anymore

- Follow the details provided in the Fabric OS Encryption Administrator's Guide for TEMS to establish connection between Encryption node and TEMS.

- 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.
- For new features added to encryption in FOS v6.4.0, such as, disk device decommissioning, combined disk-tape encryption support on the same encryption engine, and redundant key ID metadata option for replication environments, all the nodes in the encryption group must be running FOS v6.4.0 or higher versions of FOS. Firmware downgrade will be prevented from FOS v6.4.0 to a lower version if one or more of these features are in use.
- 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 and EXTENDED COPY, which are related to VAAI (vStorage APIs for Array Integration) hardware acceleration in vSphere 4.1. This will result in non-VAAI methods of data transfer for the underlying arrays, and may affect the performance of VM related operations.

FCIP (FR4-18i, Brocade 7800 and FX8-24)

- FX8-24 and FR4-18i blades cannot coexist in a DCX or a DCX-4S chassis.
- IPSec is supported on VE group 12 – 21 and not supported on VE group 22 – 31.
- IPSec is supported on FCIP tunnels that use only IPv4 connections.
- In order to enable IPSec, both ends of the tunnel must be running FOS v7.0.
- FICON networks with FCIP tunnels do not support DPS (aptpolicy 3) configurations. This applies to both emulating and non-emulating FCIP tunnels.
- Both ends of FICON emulating tunnels must run FOS v7.0.
- The maximum supported MTU size for the Brocade 7800/FX8-24 is 1500.
- FCIP connections are supported only between the Brocade 7800/FX8-24 and another 7800/FX8-24. FCIP tunnels are not supported between the 7800/FX8-24 and the previous generation Brocade 7500/FR4-18i platforms.

- When multiple FCIP tunnels are present on a switch and additional circuits (and the network bandwidth provided by those circuits) are added to an already active tunnel, there may be a short period of time where some frame loss can occur due to the process to re-fresh the internal FC frame routing tables in the switch. Therefore, additional circuits should only be added during low I/O periods utilizing the FCIP Tunnel being modified. In addition, if the circuit operation (addition/deletion) to the tunnel increases/decreases the total tunnel bandwidth, an FCIP Tunnel (VE port) disable/enable sequence should be performed after the addition/deletion of the circuit. This will allow the switch to adjust the internal routes to utilize the new bandwidth fully.
- Switching modes between 10G and 1G is disruptive for FCIP traffic.
- The FCIP Circuit Keep alive timeout has a FOS default value of 10000ms (10 seconds). If FICON is configured, the recommended value is 1000ms (1 second). The Keep Alive value needs to be set based on the application needs. If the local and remote circuit configurations' Keep Alive Timeout values do not match, the tunnel will use the lower of the two configured values.
- The configured FCIP Circuit Keep Alive Timeout should be set to the same value on both ends of the FCIP connection(s).
- In order to perform the following operations it is necessary to delete the FCIP configuration on the affected ports first:
    - Switching modes between 1G/10G/Dual.
    - Moving VE/GE port between logical switches.
    - Clean up the configuration before removing the blade.
- "InBand Management" on the Brocade 7800 or FX8-24 blades has following restrictions:
    - Firmwaredownload over the Inband interface is not supported.
    - IPv6 addressing is not supported.
- FOS v7.0 supports up to six 1 Gig Circuits on 7800 and up to ten 1Gig circuits on FX8-24 per VE/FCIP Tunnel on 1GbE interfaces. As a best practice, the FC-traffic through VE tunnel shouldn't exceed recommended over-subscription guidelines. General guidelines are 2:1 over-subscription without compression (e.g. 1G FC traffic over 500Mbps tunnel) and 4:1 with compression.
- Any firmware activation will disrupt I/O traffic on FCIP links.
- Under Traffic Isolation Zone, configurations with fail over enabled, Non-TI zone traffic will use the dedicated path if no other E or VE paths through the fabric exist, or if the non-dedicated paths are not the shortest paths. (A higher bandwidth tunnel with multiple circuits will become the shortest path compared to a single tunnel).
- Under Traffic Isolation Zone, configurations with fail over enabled, Non-TI zone traffic will use the dedicated path if no other E or VE paths through the fabric exist, or if the non-dedicated paths are not the shortest paths. (A higher bandwidth tunnel with multiple circuits will become the shortest path compared to a single tunnel).
- A VE/VEX Tunnel and E/EX FC port cannot connect to the same domain at the same time.
- Latency measurements supported on FCIP Tunnels:
    - 1GbE & 10GbE - 200ms round trip time and 1% loss.
- Brocade 7800 supports Optical and Copper Media types on GE0 and GE1 interfaces. Copper Media type is default on GE0/GE1 ports and does not support auto-sense functions.
- When GE0 and GE1 have copper media connected, auto-negotiation must be enabled on the other end of this port. Only speed that can be auto-negotiated with copper media is 1G.

- After inserting a 4G SFP in GE ports of an FX8-24 blade or 7800 switch, sometimes "sfpshow" output might display "Cannot read serial data!" . Removing and re-inserting the SFP should resolve this issue. It is recommended that users perform sfpshow 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/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 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. After the upgrade to FOS v7.0, 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 v7.0 or downgrading from v7.0 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.
- When using FC Routing in a backbone to edge configuration with an Mi10K in the edge fabric, users may experience slow throughput for hosts attached to the Mi10K. Users may encounter this following a bounced IFL connection between the backbone and edge fabric. This slowdown can be resolved by disabling/enabling the Mi10K ports for the hosts that are impacted.
- Mi10K Directors operating with firmware prior to M-EOSn v9.9.5 may experience repeated system faults when attached as an FCR edge switch to a Brocade 7800 EX Port. To avoid this, ensure that the Mi10K is operating with M-EOSn v9.9.5 or later when in an edge fabric that will be attached to a Brocade 7800 FCR Backbone.
- 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.

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 and Brocade 6510.
- 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.

Native Connectivity (M-EOS interoperability)

- A switch running FOS v7.0 cannot form E-port connectivity with any M-EOS platform. A switch running FOS v7.0 can only operate in Brocade native mode (interopmode 0). Connectivity between M-EOS platforms and a switch running FOS v7.0 is supported via FCR.

Port Mirroring

- On the Brocade 5300, the port mirroring feature has a limitation where all port mirror resources must stay within the same ASIC port group. The resources are the configured mirror port, Source Device, and Destination Device or ISL, if the Destination Device is located on another switch. The ASIC port groups are 0-15, 16-31, 32-47, 48-63, and 64-79. The routes will be broken if the port mirror resources are spread across multiple port groups.
- Port Mirroring is not supported on the Brocade 7800.

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.

Zoning

- 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 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

- 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 chassishow 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/DCX8510 during the following conditions:
  - HA failover on DCX/DCX-4S/DCX8510 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, and 6510
- 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.
- For the configure command, in FOS v6.4, or later the default value that displays for Maximum Logins per switch is different than the value that displays in FOS v6.3.x. The default value has not changed; it was displayed incorrectly in FOS v6.3.x, and is now corrected.

Defects

Closed with Code Change in Fabric OS v7.0.0b

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of August 24, 2011 in Fabric OS v7.0.0b.

Defect ID: DEFECT000300506	**Technical Severity:** High
Summary: Observed routing problem after switch running in fmsmode (FICON) changed FID assignment	
Symptom: Connectivity problems in the fabric after changing FID assignment, switch in fabric reported [RTWR-1002] and [RTWR-1003] RAS log messages.	
Workaround: Reboot or power cycle the affected switch or switches	
Feature: 8G ASIC Driver	**Function:** C2 ASIC driver
Probability: Medium	
Found in Release: FOS6.4.0	
Where Else Fixed: FOS6.4.2 a	

Defect ID: DEFECT000341971	**Technical Severity:** High
Summary: Loop attached device loses secondary disk path after port disable/enable	
Symptom: Secondary paths will not appear in the output from disk query commands.	
Feature: 8G Platform Services	**Function:** Other
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000344506	**Technical Severity:** High
Summary: Port fenced during supportsave	
Symptom: Port without errors are fenced during supportsave	
Feature: FABRIC WATCH	**Function:** PORT FENCING
Probability: High	
Found in Release: FOS6.4.0	
Where Else Fixed: FOS6.4.2 a	

Defect ID: DEFECT000347632	**Technical Severity:** High
Summary: Delays in Name Server observed during FICON CEC IMLs	
Symptom: Invalid Attachment and Name Server Query failures may be observed due to delays in Name Server processing when programming CAM entries for the ASIC.	
Feature: 8G ASIC Driver	**Function:** Other
Probability: Medium	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0b

Defect ID: DEFECT000352764	**Technical Severity:** High
Summary: Remote data replication application fails with multiple paths (multiple port pairs between arrays) when FastWrite is enabled on the FCIP tunnel.	
Symptom: With FastWrite enabled on an FCIP tunnel, and two data replication port pairs, the application commands to move data between the arrays will fail. With only a single port pair or with FastWrite disabled, everything works fine.	
Feature: FCIP	**Function:** Emulation
Probability: High	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000353981	**Technical Severity:** High
Summary: D-Port failures seen in stress and corner case scenarios.	
Symptom: D-port test stays "in progress" for a long period of time and eventually times out.	
Workaround: portdporttest --stop and disable/enable the port	
Feature: FC Services	**Function:** D-port
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000354980	**Technical Severity:** High
Summary: FIPS: Firmwaredownload signature verification fails for directors	
Symptom: During a firmwaredownload, invalid packages might not be detected by directors. This could lead to invalid packages being loaded as valid firmware.	
Feature: FOS-Infrastructure	**Function:** Firmware Download
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000355613	**Technical Severity:** High
Summary: Fabricd crash encountered during D-port testing	
Symptom: Fabricd crash could be encountered when utilizing D_Port functionality	
Feature: FC Services	**Function:** D-port
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000355830	**Technical Severity:** High
Summary: Fabric Watch and Port Fencing Threshold settings should not apply to D-Ports.	
Symptom: D-Ports become fenced during d-port testing.	
Feature: FABRIC WATCH	**Function:** PORT FENCING
Probability: Medium	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0b

Defect ID: DEFECT000356351	**Technical Severity:** High
Summary: Frame drops are observed after changing the FCR backbone domain ID.	
Symptom: Hosts lost access to storage after changing FCR backbone domain ID on a DCX/DCX-4S Backbone with FC8-64 and FC8-48 blades. Frame drops happen on the FC8-64/FC8-48 backend ports.	
Feature: Field Escalation	**Function:** FC Layer 2 Routing
Probability: Medium	
Found in Release: FOS6.4.1	**Service Request ID:** 628477
Where Else Fixed: FOS6.4.2 a	

Defect ID: DEFECT000357193	**Technical Severity:** High
Summary: C2-1012 Between DCX-4S Core and FX8-24 Blade	
Symptom: Stuck VC on DCX-4S backend ports between Core Blade in slot 3 and FX8-24 Blade in slot 7.	
Feature: 8G ASIC Driver	**Function:** Other
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000357780	**Technical Severity:** High
Summary: Excessive encoding out errors on Brocade 300 ISL ports running at 8G	
Symptom: Customer may notice excessive port errors (enc out) on Brocade 300 ISL ports in a configuration consisting of a mix of 4G user ports interconnected via 8G ISLs.	
Feature: 4G Platform Services	**Function:** ASIC Driver
Probability: Medium	
Found in Release: FOS6.4.0	

Defect ID: DEFECT000357938	**Technical Severity:** High
Summary: Backend CRC errors seen on a FC8-64 blade in a DCX 8510	
Symptom: CRC errors and possibly I/O timeouts	
Feature: 8G ASIC Driver	**Function:** ASIC Driver
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000357942	**Technical Severity:** High
Summary: LOSN not recognized by portautodisable	
Symptom: Ports that leave AC state and lose sync are not auto disabled	
Feature: 8G ASIC Driver	**Function:** ASIC Driver
Probability: High	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0b

Defect ID: DEFECT000357943	**Technical Severity:** High
Summary: Trackchanges is not generating TRK-1003 for SSH logout.	
Symptom: With a Trackchanges setting of 1,1, the track changes feature is not generating the TRCK-1003 message when a SSH session is logged out.	
Feature: FOS Security	**Function:** Authentication
Probability: High	
Found in Release: FOS6.4.1	**Service Request ID:** 631887

Defect ID: DEFECT000359245	**Technical Severity:** High
Summary: The NS contains stale entries after a bad disk is remove from a loop attached device.	
Symptom: When a disk is removed from a loop attached device, the pid still shows up in the name server.	
Workaround: port bounce where the device connected.	
Feature: FC Services	**Function:** Name Server
Probability: Medium	
Found in Release: FOS6.3.2	**Service Request ID:** 641021

Defect ID: DEFECT000359493	**Technical Severity:** High
Summary: If FX8-24 blades are swapped, the Inband Mgmt configuration is not properly loaded onto the new blade.	
Symptom: Inband Mgmt is not functioning after FX8-24 blade is replaced (swapped).	
Workaround: Reboot CP	
Feature: FCIP	**Function:** Other
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000360527	**Technical Severity:** High
Summary: An FCIP Tunnel in an FCR Backbone may lose buffer credits and go down if FastWrite is enabled.	
Symptom: FCIP Tunnel in an FCR backbone fabric goes down due to credit loss.	
Workaround: Disable FCIP FW.	
Feature: FCIP	**Function:** Other
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000349412	**Technical Severity:** Medium
Summary: portcfgshow output displays "Fill Word (Current)" incorrectly	
Symptom: portcfgshow displays incorrect values for "Fill Word (Current)" field	
Feature: 8G ASIC Driver	**Function:** Other
Probability: Medium	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0b

Defect ID: DEFECT000349465	**Technical Severity:** Medium
Summary: TopTalker Monitor fails if user changes the monitor from Egress to Ingress	
Symptom: User will be unable to create Top Talkers in Ingress mode	
Feature: Mgmt Embedded - HTTP	**Function:** Other
Probability: High	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000351796	**Technical Severity:** Medium
Summary: Duplicate E_Port SCN from Port... error messages seen after an HAFailover.	
Symptom: Duplicate E_Port SCN error messages being seen after an HAFailover	
Feature: FC Services	**Function:** Other
Probability: Low	
Found in Release: FOS6.4.2	

Defect ID: DEFECT000352406	**Technical Severity:** Medium
Summary: Storage Port logging in as unknown will be displayed as an initiator in BNA.	
Symptom: Certain storage devices may log in with an unknown FC4 type. This will result in BNA incorrectly displaying the device as an initiator.	
Feature: FC Services	**Function:** FCP
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000352773	**Technical Severity:** Medium
Summary: CRC errors on large data transfers using 3rd party Tape Drives on encryption products	
Symptom: Customers have experienced intermittent CRC errors when performing large data reads from 3rd party tape drives which may result in data read failures.	
Feature: FC Services	**Function:** Other
Probability: Low	
Found in Release: FOS6.4.0	
Where Else Fixed: FOS6.4.2 a	

Defect ID: DEFECT000354137	**Technical Severity:** Medium
Summary: User cannot config TE interface after ceeportloopbacktest	
Symptom: Cannot config TE interface after running ceeportloopbacktest Following message is displayed: "% Error: Invalid input detected at '^' marker."	
Feature: Man Pages	**Function:** Edit/Correct
Probability: High	
Found in Release: FOS6.4.2	**Service Request ID:** 629643

Closed with Code Change in Fabric OS v7.0.0b

Defect ID: DEFECT000354560	**Technical Severity:** Medium
Summary: Failed tape jobs encountered with tape pipelining enabled when utilizing a FICON to ESCON converter	
Symptom: Tape jobs intermittently fail with tape pipelining enabled when utilizing a FICON to ESCON converter.	
Workaround: Disable tape pipelining	
Feature: Field Escalation	**Function:** FCIP
Probability: Medium	
Found in Release: FOS6.4.2	
Where Else Fixed: FOS6.4.2 a	

Defect ID: DEFECT000354750	**Technical Severity:** Medium
Summary: Unable to access the boot prom on a 5480 when it is installed in a C-7000 chassis	
Symptom: Unable to access the boot prom on a 5480.	
Feature: UNDETERMINED	**Function:** UNDER REVIEW
Probability: Low	
Found in Release: FOS6.3.1	**Service Request ID:** 589577

Defect ID: DEFECT000354967	**Technical Severity:** Medium
Summary: WebTools: When attempting to upgrade a switch in IM2/IM3 to FOS v7.0, fail message should direct user to Interoperability tab to change switch to Brocade Native Fabric Mode	
Symptom: When upgrading a switch in IM2/IM3 to v7.0 via WebTools, the failure message references the interopmode command, but does not provide WebTools instructions.	
Feature: FC Services	**Function:** Other
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000355888	**Technical Severity:** Medium
Summary: D_Port (CLI): Caution message should not mention Brocade Branded SFPs.	
Symptom: Caution message seen when executing D_Port CLI mentions "only Brocade Branded SFPs".	
Feature: FC Services	**Function:** D-port
Probability: High	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000355909	**Technical Severity:** Medium
Summary: perfaddusermonitor/fmconfig not correctly counting SOFf frames	
Symptom: SOFf frame counter is not detecting SOFf frame ingress/egress when filter monitor is enabled.	
Feature: Field Escalation	**Function:** ASIC Driver
Probability: High	
Found in Release: FOS6.4.2	**Service Request ID:** 632819

Closed with Code Change in Fabric OS v7.0.0b

Defect ID: DEFECT000356559	**Technical Severity:** Medium
Summary: Need more detailed error message for blocking firmware upgrade from FOS 6.4.0c to FOS 7.0 due to a deprecated feature.	
Symptom: Firmware upgrade from v6.4 to v7.0 is blocked, and user does not get sufficient information from the error message.	
Feature: FABRIC WATCH	**Function:** Other
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000356933	**Technical Severity:** Medium
Summary: configdownload fails on 6510	
Symptom: config download fails with the following error message: configDownload: Invalid Time Zone tz = (Asia/Tokyo) Process function of configdownload failed for filter ts, lrc = -1	
Feature: Field Escalation	**Function:** OS: Configuration
Probability: Low	
Found in Release: FOS7.0.0	**Service Request ID:** 635015

Defect ID: DEFECT000357707	**Technical Severity:** Medium
Summary: FICON XRC processing is not correctly reporting RRS Sequence Validation failures (via 0x0F52 command reject) in all cases.	
Symptom: If this issue is encountered, it can lead to LOGREC entries with Command Rejects with reason code 0x0F61 against a 0xFF command. This will result in XRC suspensions.	
Feature: FCIP	**Function:** Emulation
Probability: Medium	
Found in Release: FOS6.4.0	

Defect ID: DEFECT000358793	**Technical Severity:** Medium
Summary: DCX8510-4 panics during systemverification	
Symptom: DCX8510-4 panics during systemverification when systemverification is run repeatedly.	
Feature: Diagnostics	**Function:** Other
Probability: Low	
Found in Release: FOS7.0.0	**Service Request ID:** 636925

Defect ID: DEFECT000359151	**Technical Severity:** Medium
Summary: All clear text and encrypted LUN states are unavailable	
Symptom: All clear text and encrypted LUNs are reporting: LUN state unavailable.	
Feature: Data Security	**Function:** Encryption Group
Probability: Medium	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0b

Defect ID: DEFECT000359160	**Technical Severity:** Medium
Summary: Not able to enable NPIV on FCoE ports.	
Symptom: If NPIV had been disabled on FCoE ports prior to upgrading to v7.0, NPIV cannot be enabled on those FCoE ports.	
Feature: Field Escalation	**Function:** FCoE
Probability: Low	
Found in Release: FOS7.0.0	**Service Request ID:** 639985

Defect ID: DEFECT000360186	**Technical Severity:** Medium
Summary: Brocade Encryption Engine doesn't handle Logout Extended Link with Initiator correctly.	
Symptom: When the initiator issues logout to Encryption engine it received a response it was successful, but then the initiator is able to successfully issue a read command to the encryption engine.	
Feature: Data Security	**Function:** Other
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000360329	**Technical Severity:** Medium
Summary: FSPF error message, "FSPF returned count_size 4 rc -5!!!!!" due to MSd call in FICON mode	
Symptom: FSPF error message appears out as soon as the CEC POR is started. It does not appear in the errdumpall output.	
Feature: FC Services	**Function:** FSPF
Probability: Low	
Found in Release: FOS6.4.2	

Defect ID: DEFECT000360537	**Technical Severity:** Medium
Summary: Certain traffic patterns causing back end CRC errors on FC8-64 Blades in Slots 3 and 9 of DCX	
Symptom: Experiencing CRC errors with good EOF when FC8-64 blades are installed in slots 3 or 9 of a DCX system.	
Feature: 16G Platform Services	**Function:** Other
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000361820	**Technical Severity:** Medium
Summary: CS_CTL potential marking issue due to Condor-2 to Blaster port toggle on FWDL	
Symptom: With the CS_CTL bit being set properly, data is not traversing the correct FCIP H/M/L QoS connection.	
Feature: 8G ASIC Driver	**Function:** ASIC Driver
Probability: Low	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0b

Defect ID: DEFECT000361822	**Technical Severity:** Medium
Summary: FastWrite is clearing the F_CTL priority bit resulting in CS_CTL values not being maintained/used	
Symptom: Configured CS_CTL values are no longer valid on write data frames (F_CTL priority bit disabled) once frames are carried over FCIP links with FastWrite enabled.	
Feature: FCIP	**Function:** Emulation
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000363258	**Technical Severity:** Medium
Summary: Documentation Defect: CEE command reference guide missing operands in "show running-config"	
Symptom: CEE command reference guide missing operands in "show running-config"	
Feature: Tech Pubs	**Function:** Guides
Probability: Medium	
Found in Release: FOS7.0.0	**Service Request ID:** 656483

Closed with Code Change in Fabric OS v7.0.0a – GA June 2, 2011

This section lists the defects with Critical, High and Medium Technical Severity closed with a code change as of June 2, 2011 in Fabric OS v7.0.0a.

Defect ID: DEFECT000321855	**Technical Severity:** High
Summary: CRC and/or CDR-5021 errors seen on DCX, DCX-4S, or 5100 switch platforms	
Symptom: CRC or other errors as described below: 1. Port 7/0 detected CRC error with good EOF when FC8-16 is placed in DCX-4s Slot7. For the solution to be effective, one must execute: serdestunemode --set; 2. Port 7/0, 7/10 detected CRC error when FX8-24 is placed in DCX-4s slot7. May also see CRC error on corresponding core blade backend port 3/10 6/30. Solution is effective upon upgrade, hafailover or re-init of blade. 3. 5100 experience CRC error with 3rd party tape device. 4. FC10-6 in DCX detects backend port with stuck VC after link level error (CDR-5021)	
Feature: FC10-6 Platform Services	**Function:** ASIC Driver
Probability: Low	
Found in Release: FOS6.3.1	**Service Request ID:** 451697
Where Else Fixed: FOS7.0.0 GA	

Defect ID: DEFECT000345259	**Technical Severity:** High
Summary: FC8-64 blade set to FAULTY 51 after removal/insertion of that blade in DCX 8510 chassis with diagpost on	
Symptom: May see a faulted blade upon insertion due to diagnostics failure.	
Feature: 16G Platform Services	**Function:** FOS Kernel Drivers
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000345858	**Technical Severity:** High
Summary: FIPS firmware integrity check has gaps in coverage	
Symptom: None	
Feature: FOS-Infrastructure	**Function:** Firmware Download
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000346532	**Technical Severity:** High
Summary: Disable or shutdown BES causes the SVC nodes to go offline and service mode.	
Symptom: Disable or poweroff BES switch causes the SVC nodes to go offline. The SVC nodes reboot several times before it toggled between offline and services mode.	
Workaround: Issue affects SVC storage with BES going offline. Restart storage with VI/VT members (BES) online.	
Feature: FC Services	**Function:** Name Server
Probability: High	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0a

Defect ID: DEFECT000349012	**Technical Severity:** High
Summary: FICON: Active config is out of synch with FOS indicating a port is blocked after HA failover	
Symptom: Active configuration indicates port is not blocked. FOS indicates port is blocked.	
Feature: FICON	**Function:** Ficud
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000349150	**Technical Severity:** High
Summary: BES set to faulty, due to I/O sizes greater than 512KB starting at LBA 0 for a encrypted LUN	
Symptom: BES goes faulty without clear indication of the reason	
Feature: Data Security	**Function:** Disk Encryption
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000349589	**Technical Severity:** High
Summary: FICON: CE DE received by host 5 seconds after B1 CCW causing channel timeout	
Symptom: IFCC - CREJ Code of 00 until the implementation is completed in the patch branch, and the CCW is enabled. Until then, it is responded to as an "Invalid CCW Command"	
Feature: FICON	**Function:** Ficud
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000350136	**Technical Severity:** High
Summary: Encrypted/Compressed E-Port trunk goes down following CP failover	
Symptom: Encrypted link goes down after hafailover and gets stuck at G-Port.	
Workaround: Slotpoweroff /slotpoweron the blade.	
Feature: 16G ASIC Driver	**Function:** In-flight encryption/compression
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000350457	**Technical Severity:** High
Summary: Access Gateway N-port stuck in G-port after code upgrade	
Symptom: After upgrade fabric switch attached to AG switch with QoS enabled from 6.2.x to 6.3.x, N-port stuck in G-Port. Disable QoS on fabric switch port, port came up fine.	
Feature: Field Escalation	**Function:** Access Gateway
Probability: Low	
Found in Release: FOS6.3.1	**Service Request ID:** 610119

Closed with Code Change in Fabric OS v7.0.0a

Defect ID: DEFECT000350463	**Technical Severity:** High
Summary: Unable to configure ports as extended distance using CLI on 6510 10G ports without extended fabric license	
Symptom: The intention is that you should be able to configure any non-default Extended Fabric mode on a licensed 10G FC port without requiring the Extended Fabric license – non-10G ports still require the Extended Fabric license for this operation. On the 6510 pizza box, for 10G ports, from CLI you cannot configure anything but the default Extended Fabric modes without an Extended Fabric license present. On DCX8510 family CLI, the Extended Fabric configuration behaves as expected for licensed 10G ports (no Extended Fabric license is required for any extended distance modes).	
Feature: WebMgmt	**Function:** Switch Admin
Probability: High	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000350599	**Technical Severity:** High
Summary: FICON: Persistent state is not set in Portcfg when port is blocked in the IPL file	
Symptom: Ports are not blocked following switch POR, despite being blocked in the IPL file	
Feature: FICON	**Function:** Ficud
Probability: High	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000350660	**Technical Severity:** High
Summary: D-port failing when more than 4-ports are initiated simultaneously	
Symptom: D-port tests fail on some ports when run on more than 4 links simultaneously.	
Workaround: Toggle the port	
Feature: FC Services	**Function:** D-port
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000351469	**Technical Severity:** High
Summary: FICON: LPATH Reset flag not cleared on local paths if CUB is returned for first init IU after reset - path can't be assigned as CRP	
Symptom: Operational CUP logical path indicates "Reset" state and cannot be assigned as CRP. ____:FID21:root> ficoncupset crp 74fa00 08 Processing - set CRP Attempting to set Current Reporting Path to (74FA00:08) Error return from set CRP(-48) Specified Logical Path (74FA00:08) is not operational	
Feature: FICON	**Function:** Ficud
Probability: High	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0a

Defect ID: DEFECT000342412	**Technical Severity:** Medium
Summary: TPERF session may not be able to be restarted until all user disabled GE ports on the test tunnel are re-enabled.	
Symptom: If a user disables GE ports on a TPERF test tunnel while a TPERF session is in progress and the TPERF session is terminated, TPERF may not be able to be restarted until the disabled GE ports are re-enabled. When in this state, when the user attempts to re-start TPERF, they will get a message indicating that a TPERF session is already in progress.	
Feature: FCIP	**Function:** FCIP CLI
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000342738	**Technical Severity:** Medium
Summary: Enhancement to BE credit loss detection and recovery	
Symptom: When BE credit is lost, customer needs to reseat blade to recover. This release added options to generate link reset, port re-init, and blade fault depends on user configuration upon defect BE credit lose. Refer to bottleneck on man page: bottleneckmon --cfgcredittools -intport –recover [off | onLrOnly | onLrThresh]	
Feature: 8G ASIC Driver	**Function:** ASIC Driver
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000343519	**Technical Severity:** Medium
Summary: FICON: Local LPATHS not cleared from CUP LPATH db upon implicit logo for port disable	
Symptom: Potential inability for FICON channels to successfully establish logical paths to the CUP, in configurations where there are a large number of sub-channels defined to the CUP.	
Feature: FICON	**Function:** Ficud
Probability: High	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000344506	**Technical Severity:** Medium
Summary: Port fenced during supportsave	
Symptom: Port without errors are fenced during supportsave	
Feature: FABRIC WATCH	**Function:** PORT FENCING
Probability: Low	
Found in Release: FOS6.4.0	

Defect ID: DEFECT000349008	**Technical Severity:** Medium
Summary: DP panicked after modifying metric on FCIP Circuit using a crossport with IPSec enabled	
Symptom: Tunnels for DP complex go down do to FFDC for Soft Fault on DP after modifying the metric on a standby FCIP Circuit on a crossport with IPSec enabled.	
Workaround: Disable IPsec on FCIP tunnel.	
Feature: FCIP	**Function:** Other
Probability: Low	
Found in Release: FOS7.0.0	

Closed with Code Change in Fabric OS v7.0.0a

Defect ID: DEFECT000349010	**Technical Severity:** Medium
Summary: Component (ms) dropping HA data update during logical switch delete and moving of ports	
Symptom: FICON Database out of Sync between CP's HA failure	
Feature: FICON	**Function:** MS-FICON
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000349839	**Technical Severity:** Medium
Summary: DCX 8510-4 inundated with [PS-5011] internal messages	
Symptom: List of TopTalker flows will not be accurate since some flows are not being monitored.	
Feature: Performance Monitor	**Function:** Top Talker
Probability: Medium	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000350157	**Technical Severity:** Medium
Summary: pdmd memory increase seen on the standby CP of a DCX 8510-8 with max LS creation and fully populated EX-Ports after a long period of time with I/O running	
Symptom: pdmd memory usage may increase on the standby CP of 8510-8 with max LS creation and fully populated EX-Ports after a long period of I/O running..	
Feature: License	**Function:** License
Probability: Low	
Found in Release: FOS7.0.0	

Defect ID: DEFECT000350270	**Technical Severity:** Medium
Summary: FICON: Channel aborts I/O after presenting pending Attention status	
Symptom: Channel aborts I/O, Mainframe IOS000 messages indicating that there was a channel detected error.	
Workaround: Disable FICON Tape pipelining	
Feature: FCIP	**Function:** Emulation
Probability: Medium	
Found in Release: FOS6.4.2	

Defect ID: DEFECT000351031	**Technical Severity:** Medium
Summary: FIPS zeroization requires multiple prompting for DHCHAP clearing	
Symptom: Multiple prompts for zeroization function	
Feature: FOS Security	**Function:** Other
Probability: Medium	
Found in Release: FOS7.0.0	