IBM System Storage™

Data Center Fabric Manager v10.3.2 Release Notes

GC27-2234-03

CONTENTS

Overview

IBM Data Center Fabric Manager (DCFM) 10.3.2 release adds support for a new hardware platform, new software features, and enhancements to existing features as outlined below.

New Hardware Platforms

- IBM Converged Switch B32 (3758-B32)
- SAN06B-R (2494-R06)
- FX8-24 (8 Gbps routing blade for SAN384B and SAN768B)
- FCOE10-24 (24 port CEE 10GbE blade for SAN384B and SAN768B)

New Software Features

- FCoE / CEE Performance Management
  - Support for historical and realtime port statistics
  - CEE 10G Ethernet port statistics
    - Tx/Rx percentage utilization and MB/s
    - Received EOF
    - Underflow error
    - Overflow error
    - CRC error
    - Alignment error
    - Runtime Errors
    - Too long error
- End-to-end HBA-to-switch group management
  - Host-based Discovery (single host, or multiple via IP list or CSV import, requires HCM 2.0 or later)
  - Discovery of Brocade adapters (using JSON-RPC)
  - Host-based Topology views
  - Server-to-HBA automatic mapping
  - Properties
  - Events integration
  - Statistics collection and display
  - End-to-end configuration (host and switch ports) for FC-SP and Trunking
  - HBA SupportSave
  - Deep element management configuration via HCM Launch-in-Context
- Server Virtualization Support
  - Discovery of VMware ESX virtual machines via APIs
  - View virtual machines running on physical servers
  - Display of VM properties. Including end-to-end path from VM to LUN

Enhancements to existing features

- LDAP Enhancements
  - Administrator / root user has an option to select the condition on which the DCFM Authentication will fallback to the Secondary Auth i.e. Local DB.
    - When the LDAP Servers are Not Reachable.
    - When the user is not present in the configured LDAP Server.
- FCIP Enhancements
  - Support for new features introduced with the new extension platforms
  - Comprehensive FCIP Tunnels Configuration diaglog (replacement for existing FCIP Tunnel Wizard)
  - Enhancements for Circuit properties, Tunnel Properties, Connection Properties, Switch Properties, Flyovers and the Topology View
  - Support to view all tunnels discovered by DCFM across all fabrics
  - Introduced Circuit Configuration for the tunnels in the SAN06B-R and the FX8-24 blades.
  - Support to view performance statistics of FCIP tunnels in SAN06B-R and the FX8-24 blades.
- FICON Enhancements
  - Lossless DLS support in Configure Cascaded FICON and merge wizard
  - 'Cascaded FICON Merge' wizard conflict resolution
    - Data Field Size
    - VC Priority
  - 'Card Swap Function'
    - Allows a user to swap a failing card with a new one
    - Moves port address and port index of ports within blades over to new card
    - Enable all the ports on the blades once swap is completed successfully
  - PDCM Enhancements
    - Warn users when prohibiting E-E and E-F port connections
    - Ability to provision same PDCM updates to multiple switches
    - Usability enhancement to support direct entry of row + column for prohibit
    - PDCM dialog – Changed from Modal to Non-Modal dialog
- Reliability, Availability and Serviceability Enhancements
  - DCFM SupportSave improvements
    - Configure an interval at which SupportSaves will be captured from specified switches automatically
    - Include Brocade HBA SupportSave
    - Increased simultaneous switch SupportSave captures to 50 (from 10)
  - Policy Engine improvements
    - Added an action to capture switch SupportSave in the Event policy dialog
  - Facility to register switches in upload failure data capture destination
  - Facility to register DCFM as a tracedump destination

- Port Fencing policies for Class 3 frame drops
- Fault Management improvements
    - Receive syslog events from HBAs
    - Increase max number of events stored in DB to 20,000 (from 10,000) with a maximum of 50,000
- Added support to optionally back up the **FTP** folder, **Technical Support** folder and **Trace dump** folder
- System Monitor process improvements
    - Generate master log event when memory usage >= 80% and disk space usage >=90%
- Audit log improvements
    - All important user actions generate application events
- Debug logging improvements
    - Logging of messages at appropriate level to prevent rollover of logs
    - Increase default size of logfiles from 5MB to 10MB
    - Isolate failures to small grained tasks (e.g. failure to collect one piece of data due to errors will not prevent collection of remaining data)
    - Include data source name to avoid ambiguity (multiple data collection sources)

- Zoning Enhancements
    - Active TI Zone enhancements
        - Active TI Zone information collected by DCFM and persisted in DB
        - Displays differences between active TI zone and defined TI zone in zone DB
        - Active TI Zone members display in **Active Zone Config** tab
        - Active Status display for **TI Zones Properties** dialog
    - Policy to control number of zone db modifications
        - Set limits on number of editing operations (add / remove / modify) user can perform in zones, zone configs, alieases and on zone members before activation
        - Set policy by fabric as limits may vary (e.g. disk vs. tape)
        - Warn users when policy is exceeded and prevent user from proceeding further
    - Support for QoS D, I Zones
- Other Enhancements
    - RBAC Enhancements
        - In **Add/Edit Resource** group dialog, **Hosts** tab is added so that Resources can be assigned as a Fabric or Host.
        - New default user roles "Network Administrator", "Host Administrator" are added.
        - New User Privileges “Host Management, Active session management, FCoE Management, CEE Management, Zoning Set-Edit Limits” are added.
    - Event Storage Enhancements in **Options** Dialog
        - Increased default event count from 5000 to 20000 in DCFM Enterprise
        - The maximum configurable limit is 50000 in DCFM Enterprise
    - DCFM Active Sessions
        - Shows active client sessions logged into DCFM server

- Users with Read Write ‘Active Session Management’ privilege can disconnect active clients

- Switch Configuration Management
  - New column named “**Configuration Type**” has been introduced to notify that the configuration file is of the type CEE/FC.
- **HCM Upgrade** tab
  - New tab added to SMC to facilitate ugrading HCM in DCFM to a newer version of HCM
- Backup Dialog Enhancements
  - Three checkboxes added to the existing design
    - Include FTP Root Directory
    - Include Technical Support Directory
    - Include Upload Failure Data Capture Directory
- SNMP v3
  - Option to choose either v3 traps or Informs
  - Configure at fabric-level from standalone dialog (instead of Discovery dialog)
  - Only supported with FOS 6.3 or above
- Support for 239 DID mode and offsets display (native connectivity with M-series switches)
  - ‘Port Auto Disable’ policy for any of the following conditions
    - Loss Of Sync
    - Loss Of Signal
    - Non Operational Primitive Sequence
    - Loop Initialize Process
    - Offline Primitive Sequence
- Implemented main end user “requests for enhancement” (RFEs)

IBM DCFM 10.3.2 supports a seamless upgrade path from previous versions of IBM DCFM (10.0.x and 10.1.x) as well as EFCM 9.6.x/9.7.x and FM 5.4 / 5.5

IBM DCFM 10.3.2 supports use with IBM Tivoli Storage Productivity Center (TPC) 4.1.0.103 and later

Operating Systems Supported

DCFM 10.3.2 is supported on the following operating systems.

Table 1 Server / Client Operating System Support

Operating System	Versions
Windows	XP Professional SP2, SP3 (x86 32-bit) 2003 Server SP2 (x86 32-bit) Vista Business Edition (x86 32-bit) 2008 Server (x86 32-bit)
Linux	RedHat Enterprise Linux AS 4 (x86 32-bit) RedHat Enterprise Linux 5 Advanced Platform (x86 32-bit) SUSE Linux Enterprise Server 10 SP1 (x86 32-bit)

Switch Platform and Firmware Requirements

The following table lists the versions of Brocade software supported in this release. IBM and Brocade recommend using the latest software versions to get the greatest benefit from the SAN. IBM and equivalent Brocade hardware products are listed.

Operating System	IBM Switch/Director	Brocade Switch/Director
Switch (b-type and B-Model) Firmware Versions		
FOS 5.0.x, 5.1.x, 5.2.x, 5.3.x, 6.0.x, 6.1.x, 6.2.x, 6.3.x	SAN Switch F32 (2109-F32)	Brocade 3900
	SAN Switch H08 (2005-H08)	Brocade 3250
	SAN Switch H16 (2005-H16)	Brocade 3850
	SAN32B-2 (2005-B32, -32B)	Brocade 4100
	SAN04B-R (2005-R04)[1]	Brocade 7500E[1]
	SAN18B-R (2005-R18)[1]	Brocade 7500[1]
	SAN16B-2 (2005-B16, -16B)	Brocade 200E
	SAN64B-2 (2005-B64)[2]	Brocade 4900[2]
	SAN32B-3 (2005-B5K, -5KB)[3]	Brocade 5000[3]
	SAN24B-4 Express (2498-B24, -24E)[5]	Brocade 300[5]
	SAN40B-4 (2498-B40, -40E)[5]	Brocade 5100[5]
	SAN80B-4 (2498-B80)[5]	Brocade 5300[5]
	IBM Converged Switch B32 (3758-B32)[10]	Brocade 7800[10]
	SAN06B-R (2498-R06)[9]	Brocade 8000[9]
	SAN Switch M12 (2109-M12)	Brocade 12000
	SAN Switch M14 (2109-M14)	Brocade 24000
	SAN256B (2109-M48) with FC4-16, FC4-32 and FC4-48 blades[2]	Brocade 4800 with FC4-16, FC4-32 and FC4-48 blades[2]
	SAN256B (2109-M48) with FR4-18i blades[1]	Brocade 4800 with FR4-18i blades[1]
	SAN256B (2109-M48) with FC4-16IP blades[2]	Brocade 4800 with FC4-16IP blades[2]
	SAN256B (2109-M48) with FC10-6 blade[4]	Brocade 4800 with FC10-6 blades[4]
	SAN768B (2499-384) with FC8-16, FC8-32, and FC8-48 blades[6]	Brocade DCX with FC8-16, FC8-32, and FC8-48 blades[6]
	SAN768B (2499-384) with FR4-18i blades[6]	Brocade DCX with FR4-18i blades[6]
	SAN768B (2499-384) with FC10-6 blades[6]	Brocade DCX with FC10-6 blades[6]
	SAN768B (2499-384) with FX8-24 blades[10]	Brocade DCX with FX8-24 blades[10]
	SAN768B (2499-384) with FCoE10-24 blades[10]	Brocade DCX with FCoE10-24 blades[10]
	SAN384B (2499-192) with FC8-16, FC8-32, and FC8-48 blades[8]	Brocade DCX-4S with FC8-16, FC8-32, and FC8-48 blades[8]
	SAN384B (2499-192) with FR4-18i blades[8]	Brocade DCX-4S with FR4-18i blades[8]
	SAN384B (2499-192) with FC10-6 blades[8]	Brocade DCX-4S with FC10-6 blades[8]
	SAN384B (2499-192) with FX8-24 blades[10]	Brocade DCX-4S with FX8-24 blades[10]
	SAN384B (2499-192) with FCoE10-24 blades[10]	Brocade DCX-4S with FCoE10-24 blades[10]

[1] Requires FOS v5.1.0 or higher
[2] Requires FOS v5.2.0 or higher
[3] Requires FOS v5.2.1 or higher
[4] Requires FOS v5.3.0 or higher
[5] Requires FOS v6.1.0 or higher
[6] Requires FOS v6.0.0 or higher
[7] Requires FOS v6.1.1_enc or higher
[8] Requires FOS v6.2.x or higher
[9] Requires FOS v6.1.2_CEE or 6.3
[10] Requires FOS v6.3.0 or higher

Operating System	IBM Switch/Director	Brocade Switch/Director
Switch (m-type, M-Model) Firmware Versions		
M-EOSc 9.6.x, 9.7.x, 9.8.x, and 9.9.x	SAN12M-1 (2026-E12, -12E) SAN16M-2 (2026-416, -16E) SAN24M-1 (2026-224) SAN32M-1 (2027-232) SAN32M-2 (2027-432, -32E) SAN140M (2027-140)	Spheron 4300 Spheron 4400 Brocade M4500 Spheron 3232 Brocade M4700 Brocade M6140
M-EOSn 9.6.x, 9.7.x, 9.8.x, and 9.9.x	SAN256M (2027-256)	Brocade Mi10K

Important Notes

This section lists information that you should consider before you use DCFM v10.3.2 See the *DCFM User Manual* for full details on the following notes.

M-EOSc switches with SNMPv3 enabled cannot be managed through DCFM. SNMPv3 needs to be disabled.

If SNMPv3 is enabled on M-EOSc switches, SNMPv1 is automatically disabled. SNMPv3 and SNMPv1 cannot be enabled simultaneously. Since DCFM 10.3.2 uses only SNMPv1 to manage the M-EOSc switches, the manageability link will not get established, if SNMPv3 is enabled. It is recommended to disable SNMPv3 using CLI.

Issues with JRE v1.6.0 update not at 13

If the system JRE is not at update 1.6.0_13 then the following issues could be seen

Remote client fails to launch with java webstart exception

Remote client cannot be upgraded or downgraded

DCFM server / client and B-model Element Manager crashes on launch

Verify that the system JRE is at 1.6.0_13 by executing 'java --version' at the command prompt. If the version does not display as '1.6.0_13', it is recommended that you uninstall the current version and point a supported web browser to the DCFM Server IP address and download and install the correct version which is bundled with the DCFM Server. It is recommended that the JRE is not automatically updated as this will change the version.

Upgrade switches running FOS v5.2.1_NI to v6.0.0 or higher

To completely manage a fabric, in DCFM, where the seed switch is running FOS v52.1_NI, it is recommended to upgrade the switch to FOS v6.0.0 or higher. Failure to do so will limit the ability to manage fabric services such as Zoning. However, monitoring features suchas Status, Events, and Performance Monitoring should not be affected.

Creating tape pool in a mixed FOS version environment

If FOS versions 6.2.0 and 6.1.1_enc_X (where X is any released version) are deployed in an environment the user should not configure any Tape Pool information. If Tape Pool information is configured and a failover occurs where the 6.1.1_enc_X node becomes the group leader, the user will not be able to remove the created tape pool.

Event priority mismatch

Error-level policies can sometimes be triggered by warning-level events.

Config Download fails when all parameters are selected

When Configdownload is attempted from one virtual switch to another virtual switch and when all parameters are selected where the Fabric IDs are not identical, download will fail

Switch name update delay

When changing the name of a switch from outside of DCFM the new name for the switch will not be reflected within DCFM for up to 15 minutes, depending on SAN Size selection.

Element Manager fails to launch on SAN256M (Mi10k)

If the admin partition (partition 0) is removed and then reattached to a managed fabric the Element Manager will no longer be able to be launched from DCFM until the DCFM services are restarted.

Deleting Logical Switches with GbE ports causes errors

In order to delete a logical switch that contains Gigabit Ethernet ports, the GbE ports must be moved to the default logical switch prior to deleting the logical switch.

Event-based file actions fail

DCFM event-actions will fail to run scripts on remote-mounted filesystems under Windows.

EX-Port disabled when configuring Routing Domain IDs

In the Routing Domain IDs dialog, if a user adds the appropriate Domain IDs to the front and xlate domains, clicking OK will disabled the Ex_ports with the message "EX_PORT ISOLATE".

Removing Switches

If you plan to segment and remove multiple switches (more than 2) from a fabric and you have historical performance collection enabled, it is recommended that you 'accept changes' after each switch segmentation from the client rather than doing it together.

DCFM Clients

As a best practice it is recommended that the clients which are not being used actively should be shutdown. This will free up the server resources. In some scenarios, if **duplicate** entries are seen in the 'Product List', restart the client.

Secure FOS fabrics cannot be discovered from DCFM

DCFM doesn't support Secure FOS (SFOS), If user tries to discover the fabric, DCFM will show an error message that "Discovery Failed". User will have to remove the secure FOS settings and change it back to normal fabric before discovering it from DCFM

Performance Data Aging tab has been removed from Server Management Console (SMC)

User cannot configure the Performance Data Aging setting in DCFM 10.3.2, the tab has been removed from Server Management Console. The following are the default configuration

288 samples for 5 minute period

144 samples for 30 minute period

84 samples for 2 hour period

90 samples of 1 day period

Total number of samples – 606

During migration from earlier releases all the historical data will be truncated with respect to the default samples and the aging configuration will not be migrated to 10.3.2.

Unable to launch Element Manager for EOS switches after Migrating from EFCM.

EOS switches in dual mode when discovered using Ipv4 address from EFCM will not retain manageability when migrated to DCFM due to the preferred IP mechanism present in the DCFM, which discovers the switch using Ipv6 address and the previous session with Ipv4 is not released. To work around this issue, user can try any one of the following options

User can disable dual mode in EOS switches before migrating to DCFM
(OR)
After migration, user must delete and rediscover the fabric (In this case user will have to take backup of Zone information, Historical Performance Data(if applicable) and Names before doing this operation and import this data once the discovery operation is complete)

Encryption switch/blade public certificates exported using DCFM should be signed before the switches can connect to the Key Vault

Exported certificates using DCFM to do the setup on the encryption switches will have to be signed by the certificate autority that is trusted by the RKM before it can be imported into both the RKM and the switch/blade. This step is required only for RKM and not required for other key management systems.

To workaround this, use the CLI command to export the self signed public certificate:

Cryptocfg --export --scp –KACcert [scp server address] [scp server login id] [scp server path]

Encryption config has limited support and slow to register change for LUN provisioning

The current commit limitation of 25 is for the total tansactions which includes add, update and remove LUNs. To workaround this, please commit the transaction first before making further changes.

Inappropriate Discovery status displayed for VF enabled switches

During the Discovery of VF enabled switches if incorrect user ID is provided for the SNMP v3 user name, ”The SNMP user ID entered is not defined as fos switch user” message will be shown. After that if the user provide the correct user ID, the message will not show the correct status and it remains the same. It is recommended to give the correct user ID while discovering the VF enabled switches. TR:260884

M-i10k is not displayed under EMC call center in CMDCE after migration when it is assigned under EMC in CM

While migrating from EFCM to DCFM, SAN256M (Mi10k) is not assigned under EMC call home center. The workaround for the issue is the user has to manually assign SAN256M (Mi10k) to the EMC call home center.TR: 245270

Complete migration process (from installing DCFM to discovering all the switches) takes 35 minutes when migrating from 10.1.x to 10.3.x

The migration process can take an extended time when the ftproot folder size is more than 7GB. It is recommended to minimize the number of additional files saved in the ftproot folder, such as firmware and support data collection files in DCFM. TR- 259313.

Complete migration process (from installing DCFM to discovering all the switches) takes 46 minutes when migrating from EFCM

The migration process can take an extended time when the ftproot folder size is more than 7GB. It is recommended to minimize the number of additional files saved in the ftproot folder, such as firmware and support data collection files in EFCM. TR 259323 & 258791

Firmware Repositary select Latest option

When the user imports firmware in the repository there are two firmware versions, 6.2.0g and 6.1.2a. When “Select latest” button is used 6.1.2a is chosen instead of 6.2.0g. It is recommended to select the latest manually. TR 256603

Empty LAG creation

If a dot1x enabled port is assigned to a LAG, an empty LAG will be created. [If a couple of ports combination of dot1x and dot1x disabled are added to a LAG, here only the dot1x disabled ports will be added to the LAG] It is recommended to check for the dot1x status on the port before assigning it to a LAG. TR 254487

Duplicate tunnels are shown in the FCIP tunnel dialog after creating a new tunnel

After creating a new tunnel between two FCIP capable switches, duplicate tunnels are shown in the "FCIP tunnel" dialog. It is recommended to close, wait a short time, and then reopen the FCIP tunnel dialog. The duplicate tunnels will no longer be visible. TR261244

No operation performed when clicking the buttons present in the "FCIP Tunnel" dialog

Sometimes it happens when clicking the buttons (Add Tunnel, Edit Tunnel, Disable Tunnel, Enable tunnel) in the FCIP Tunnel dialog, that no operation takes place. It is recommended to Close and reopen the FCIP tunnel dialog to perform the same operations. TR 260012

In the "FCIP Tunnel" dialog after adding the new circuit in the 'Circuits' TAB, some fields are shown as EMPTY

In the "FCIP Tunnel" dialog after adding the new circuit in the '**Circuits**' tab, some fields are shown as EMPTY for the newly added circuit (Gateway, GigE ports, Administrative Status, Wrong MTU size value). It is recommended to Close and reopen the FCIP tunnel dialog after waiting a short time, to see the updated values. TR 260301

Error message thrown when deleting a circuit

While trying to delete a Circuit, the following error message displays: "The Operation has Failed error: Failed to remove FCIP circuit. Error issuing delete to port. Removing from config database. It is recommended to reboot, to clean up active port config", and does not allow deleting the circuit. It is recommended to Reboot the switch and try to delete the tunnel. TR 260445

IFL connection shown in topology after deleting all the VE-VEX tunnels present between the Spike switches

After deleting all the VE-VEX tunnels present between the SAN06B-R switches, sometimes the IFL connection is still shown in topology. It is recommended to Unmonitor and monitor the switch again. TR259685

When the switch is converted to AG an extra HBA icon is displayed in Topology

When the switch is convereted to AG mode, both HBA and AG are displayed in the Fabric with same WWN. It is recommended to unmonitor and remonitor the Fabric so that the HBA will be removed. TR251379

When the AG is converted to Switch it will still show as AG

In the Migrated server, when AG mode is disabled in the discovered fabric it will still appear as AG and End device connected to it will not be displayed. It is recommended to unmonitor and remonitor the Fabric. TR257257

AG to switch connection is not shown after the Fabric merge

When the fabrics are merged sometimes the AG to switch connection will not shown . It is recommended to unmonitor and monitor the fabric. TR 258998

F ports connected to Access Gateway are not shown as attached ports under the switch

If Access Gateway is connected to switch, F_ports connected to access gateway are not shown as attached virtual ports under the switch. It is recommended to launch a new client. TR253462

Quorum card options are enabled in mixed FOS Encryption Group

When the Encryption group is created one switch with FOS 6.3.0 and another switch with 6.2.0 or 6.1.1 encryption build in a same group, Quorum card option and system card options are enabled in security tab.

It is recommened to have the same FOS(6.3.0) in an encryption group for Quorum card and system card support. TR259628

Connection between AG and switch are not shown when F_port trunking is enabled on the AG

If switch is configured with F_port trunking which the AG is connected to the switch, F_port trunk group icon is not shown in the product tree and connection between switch and AG is also not shown in topology. It is recommended to disable F_port trunking on switch. TR253201

Zoning dialog opening fails when tried to open before the discovery completes

When the user try to open Zoning dialog before the discovery operation complete, an error message stating "Failed to load Zone DB" will be shown. It is recommended to open the zoning dialog after the discovery operation is completed. TR259665

SAN256M (MI10k) is not getting manageability in DCFM 10.3.x after migration when it is discovered using SNMPv3 with APIuser in DCFM 10.0.x / 10.1.x

After migration from DCFM 10.0.x / 10.1.x to DCFM10.3.x, Mi10k won't get manageability since "Configure for Intrepid 10k" checkbox is disabled and displayed user name as (API User | Administrator). It is recommended to check "Configure for Intrepid 10k" checkbox in SNMPv3 tab of Edit dialog. TR:265292

Users of DCFM and who use SysLog Host Configuration for events (Defect# 259950)

HCM Agent needs to be restarted if firewall settings on port# 514 changed in Vmware. Vmware (Esx 3.5 & 4) blocks the Syslog outgoing port 514 by default. We need to configure the firewall to allow outgoing port 514 for Syslog if you plan to use Syslog Host configuration or use HCM as part of DCFM. Use the command 'esxcfg-firewall -o 514,udp,out,syslog' to open the port 514 and use the command 'esxcfg-firewall -c 514,udp,out,syslog' to block outgoing traffic thru 514 port.

Failover restriction in Mixed Fabric

In case of Mixed Fabrics, only FOS switch can be the seed Switch. When the FOS Seed switch becomes unreachable and if there are no other manageable FOS switches in the fabric, Fail over to EOS seed switch will not happen. It is also not possible to manually change the seed switch to EOS. To manage this fabric,

a. Disconnect the ISL between FOS and EOS switches
b. Unmonitor/delete this fabric
c. Discover the Pure EOS Fabric by providing EOS seed switch IP Address

Failover can happen in the below mentioned cases

a. Same flavor of switches of B-Model to B-Model or M-Model to M-Model
b. M-Model to B-Model

Display of Logical switches

If Logical switches are created through the Logical Switch Dialog, it will be displayed under Undiscovered Logical Switch in the existing Logical Switches Panel. To manage, Discover the new logical Fabric

Documentation Updates

This section provides information on last-minute additions and corrections to the documentation. The most recent DCFM 10.3.x documentation manuals are available are available on the IBM SAN Support site: http://www.ibm.com/systems/support/storage/san

DCFM Installation, Migration, and Transition Guide

On page 8, in the **Scalability** requirements section, change the **Supported Limits** tables as follows:

Table 2 Enterprise Supported Limits by SAN size for Pure Fabric OS fabrics

Value	Small	Medium	Large
Number of Fabrics	8	16	24
Number of Domains	20	60	120
Number of Switch Ports	2000	5000	9000
Number of Device Ports	5000	10000	20000
Number of Access Gateways	20	30	40
Performance Monitoring Polling	5 minutes	5 minutes	5 minutes

Table 3 Supported Limits by SAN size for Mixed Fabrics with (FOS and M-EOS fabrics)

	Small	Medium	Large
Number of Fabrics	8	16	24
Number of Domains	10	30	60
Number of Switch Ports	1000	2500	5000
Number of Device Ports	2500	5000	10000
Number of AG's	20	30	40
Performance Monitoring Polling	5 min	5 min	5 min

On multiple pages, in the Installation procedure sections, in the Server Port Configuration step, use one of the following procedures (depending on your operation system,) to determine which process is running on the Syslog port and to stop the process.

Windows Operating Systems

Finding the process

1. Open a command window.
2. Type **netstat –anb | find /i "514"** and press **Enter**.

   The process running on port 514 displays.

   For example, UDP 127:0:0:1:514 *:* 3328.

Stopping the process

Type **taskkill /F /PID "<PID>"** and press **Enter**.

For example, **kill -9 “<3328>”**.

OR

1. Select CTRL + SHIFT + ESC to open Windows Task Manager.
2. Click the **Processes** tab.
3. Click the **PID** column header to sort the process by PID.
4. Select the process you want to stop and click **End Process**.

Linux Operating Systems

Finding the process

1. Open a command window.
2. Type **netstat –nap | grep 514** and press **Enter**.

   The process running on port 514 displays.

   For example, UDP 0 0 ::ffff:127:0:0:1:514 :::* 27397.

Stopping the process

Type **kill -9 “<PID>”** and press **Enter**.

For example, **kill -9 “<27397>”**.

On multiple pages, in the Pre-migration requirements on Windows systems and in the Pre-migration requirements on UNIX systems for DCFM migration, add the following option:

Make sure you manually delete any unwanted files in the DCFM directory to expedite the migration process. Files to remove include:

- Fabric OS firmware files located in <*Install_Home*>\data\ftproot\Firmware
- M-EOS firmware files located in <*Install_Home*>\data\em\eos_Raw
- Data collection files located in <*Install_Home*>\data\classicserver
- Switch supportSave files located in <*Install_Home*>\data\ftproot\technicalsupport

On page 38, in the ***Pre-migration requirements on Windows systems*** section, and on page 82, in the ***Pre-migration requirements on UNIX systems for*** EFCM migration, add the following option:

Make sure you manually delete any unwanted files in the EFCM directory to expedite the migration process. Files to remove include:

- M-EOS firmware files located in <Install_Home>\Server\Local_Root_Raw
- Fabric OS firmware files located in <Install_Home>\Server\ftproot

On page 38, in the ***Enterprise trial migration*** section, note that the referenced procedures should only be used when migrating from Enterprise trial 10.3.X to Enterprise trial or full edition 10.3.X.

When you are migrating from Enterprise trial 10.0.X or 10.1.X or 10.3.0 or 10.3.1 to Enterprise trial or full edition 10.3.X on Windows systems, use the following procedure:

Migrating from Enterprise trial 10.0.X or 10.1.X or 10.3.0 or 10.3.1 to Enterprise trial or full edition 10.3.X on Windows systems

Use the following procedure to migrate from Enterprise Trial edition 10.0.X or 10.1.X or 10.3.0 or 10.3.1 software to Enterprise Trial or Full edition 10.3.X software.

1. Insert the installation DVD into the DVD-ROM drive.

If autorun is enabled, the DVD Index page launches automatically. Click the **Enterprise Install** link.

If autorun is not enabled, open the following file: DVD_Drive>\DCFM\windows\install.exe

2. Click **Next** on the **Introduction** screen.
3. Read the agreement on the **License Agreement** screen, select **I accept the terms of the License Agreement** and click **Next**.
4. Select the usual location for your system's application files (for example, D:\Program Files\DCFM 10.3.X) on the **Select Install Folder** screen and click **Next**.

   Do not install to the root directory (for example, C:\).
5. Review the displayed installation summary on the **Pre-Installation Summary** screen and click **Install**.
6. Make sure the **Launch DCFM Configuration** check box is selected (default) on the **Installation Complete** screen and click **Done**.
7. Click **Next** on the **Welcome** screen.
8. Choose one of the following options to migrate data from a previous version.

   To migrate data from a previous management application, you must do so now.

   To migrate data from the previous version installed (automatically detected), select **Yes, from DCFM** in the following location.

   To browse to the previous version, select Yes, from **EFCM, FM, or DCFM installed in this machine or on network** and click **Browse** to browse to the installation directory.
9. Click **Next** on the **Copy Data and Settings** screen.

   An error message displays as "S "This is not a valid/supported EFCM/FM/DCFM installation directory"

   ", if invalid path is given.

   NOTE: If legacy EFCM or FM software exist in the system, an Uninstall screen displays. Click Yes to Uninstall services of legacy EFCM and FM software.
10. Click **Start** on the **Data Migration** screen.

    Data migration may take up to 30 minutes. When data migration is complete, the previous version is partially uninstalled.
11. Click **Next** on the **Data Migration** screen.
12. Select **Internal FTP Server** or **External FTP Server** on the **FTP Server** screen and click **Next**.

    The default selection reflects the previous Enterprise edition configuration.

    If port 21 is busy, a message displays. Click **OK** to close the message and continue. Once the Management application is configured make sure port 21 is free and restart the Server to start the FTP service.

    NOTE: If you select to use an FTP Server which is not configured on the same machine as DCFM, the Firmware Repository feature will not be available.
13. Complete the following steps on the **Server IP Configuration** screen.

    Select an address from the **Server IP Configuration** list.

    Select an address from the **Switch - Server IP Configuration Preferred Address** list.

    Click **Next**.

    If DNS is not configured for your network, do not select the 'hostname' option from either the Return Address or Preferred Address list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.

If you select a specific IP address from the Server IP Configuration screen and the selected IP address changes, you will not be able to connect to the server.

14. Complete the following steps on the **Server Port Configuration** screen.

    NOTE: Do not use port 2638 for any of these port numbers. Port 2638 is used internally by the server.

    a. Enter a port number in the **Syslog Port Number** field (default is 514).

       NOTE: If the default syslog port number is already in use, you will not receive any syslog messages from the device.

    b. Enable SSL by selecting the **SSL Enabled** check box.

    c. Enter a port number in the **Web Server Port Number** field (default is 443 if SSL Enabled is selected; otherwise, the default is 80).

    d. Enter a port number in the **SNMP Port Number** field (default is 162).

    e. Enter a port number in the **Starting Port Number** field (default is 24600).

       NOTE: The server requires 16 consecutive free ports beginning with the starting port number.

    f. Click **Next**.

       If you enter a Syslog port number already in use, a message displays. Click **OK** to close the message. Edit the Syslog port number and click **Next**.

       If you enter a port number already in use, a Warning displays beneath the associated port number field. Edit that port number and click **Next**.

15. Select one of the following options on the **SAN Size** screen (pure Fabric OS maximum numbers):

    Small (managing up to 2000 ports, 1-20 domains)

    Medium (managing up to 5000 ports, 21-60 domains)

    Large (managing up to 9000 ports, 61-120 domains)

16. Click **Next**.
17. Verify your configuration and license information on the **Server License Summary** screen and click **Next**.
18. Select the **Start Client** check box, if necessary, on the **Start Server** screen and click **Finish**.

    After all of the DCFM services are started, the Log In dialog box displays.

19. Enter your user name and password.

    The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

20. Click **Login**.
21. Click **OK** on the **Login Banner.**

When you are migrating from Enterprise trial 10.0.X or 10.1.X or 10.3.0 or 10.3.1 to Enterprise trial or full edition 10.3.X on UNIX systems, use the following procedure:

Migrating from Enterprise trial 10.0.X or 10.1.X or 10.3.0 or 10.3.1 to Enterprise trial or full edition 10.3.X on UNIX systems

Use the following procedure to migrate from Enterprise Trial edition 10.0.X or 10.1.X or 10.3.0 or 10.3.1 software to Enterprise Trial or Full edition 10.3.X software.

1. Insert the installation DVD into the DVD-ROM drive and open the following file.

   <DVD_Drive>\DCFM\<UNIX_Platform>\install.bin

2. Click **Next** on the **Introduction** screen.
3. Read the agreement on the **License Agreement** screen, select **I accept the terms of the License Agreement** and click **Next**.
4. Select the usual location for your system's application files (for example, opt/DCFM10_3_X) on the **Select Install Folder** screen and click **Next**.

   Do not install to the root directory (for example, /).
5. Review the displayed installation summary on the **Pre-Installation Summary** screen and click **Install**.
6. Make sure the **Launch DCFM Configuration** check box is selected (default) on the **Installation Complete** screen and click **Done**.
7. Click **Next** on the **Welcome** screen.
8. Choose one of the following options to migrate data from a previous version.

   To migrate data from a previous management application, you must do so now.

   To migrate data from the previous version installed (automatically detected), select **Yes, from DCFM** in the following location.

   To browse to the previous version, select Yes, from **EFCM, FM, or DCFM installed in this machine or on network** and click **Browse** to browse to the installation directory.
9. Click **Next** on the **Copy Data and Settings** screen.

   An error message displays as "This is not a valid /supported EFCM/FM/DCFM installation directory", if invalid path is given.

   NOTE: If legacy EFCM or FM software exist in the system, an Uninstall screen displays. Click Yes to Uninstall services of legacy EFCM and FM software.
10. Click **Start** on the **Data Migration** screen.

    Data migration may take up to 30 minutes. When data migration is complete, the previous version is partially uninstalled.
11. Click **Next** on the **Data Migration** screen.
12. Select **Enterprise** on the **Trial Editions** screen and click **Next**.
13. Select **Internal FTP Server** or **External FTP Server** on the **FTP Server** screen and click **Next**.

    The default selection reflects the previous Enterprise edition configuration.

    If port 21 is busy, a message displays. Click **OK** to close the message and continue. Once the Management application is configured make sure port 21 is free and restart the Server to start the FTP service.

    NOTE: If you select to use an FTP Server which is not configured on the same machine as DCFM, the Firmware Repository feature will not be available.
14. Complete the following steps on the **Server IP Configuration** screen.

    Select an address from the **Server IP Configuration Return Address** list.

    Select an address from the **Switch - Server IP Configuration Preferred Address** list.

    Click **Next**.

    If DNS is not configured for your network, do not select the 'hostname' option from either the Return Address or Preferred Address list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.

    If you select a specific IP address from the Server IP Configuration screen and the selected IP address changes, you will not be able to connect to the server.
15. Complete the following steps on the **Server Port Configuration** screen.

NOTE: Do not use port 2638 for any of these port numbers. Port 2638 is used internally by the server.

a) Enter a port number in the **Syslog Port Number** field (default is 514).

NOTE: If the default syslog port number is already in use, you will not receive any syslog messages from the device.

b) Enable SSL by selecting the **SSL Enabled** check box.

c) Enter a port number in the **Web Server Port Number** field (default is 443 if SSL Enabled is selected; otherwise, the default is 80).

d) Enter a port number in the **SNMP Port Number** field (default is 162).

e) Enter a port number in the **Starting Port Number** field (default is 24600).

NOTE: The server requires 16 consecutive free ports beginning with the starting port number.

f) Click **Next**.

If you enter a Syslog port number already in use, a message displays. Click **OK** to close the message. Edit the Syslog port number and click **Next**.

If you enter a port number already in use, a Warning displays beneath the associated port number field. Edit that port number and click **Next**.

16. Select one of the following options on the **SAN Size** screen (pure Fabric OS maximum numbers):

    Small (managing up to 2000 ports, 1-20 domains)

    Medium (managing up to 5000 ports, 21-60 domains)

    Large (managing up to 9000 ports, 61-120 domains)

17. Click **Next**.
18. Verify your configuration and license information on the **Server License Summary** screen and click **Next**.
19. Select the **Start Client** check box, if necessary, on the **Start Server** screen and click **Finish**.

    After all of the DCFM services are started, the Log In dialog box displays.

20. Enter your user name and password.

    The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.

21. Click **Login**.
22. Click **OK** on the **Login Banner.**

On page 72, in the **Migration** chapter, add the following procedure.

Restoring data to a new server

Use the following procedure to restore a data to the new Management application server.

1. Launch the Server Management Console
   On Windows systems, open the Server Management Console from the **Start** menu on the Management application server.
   On UNIX systems, go *to <Install_Home>*/bin on the Management application server, type /smc.sh and press **Enter**.
2. Stop the Management application services by completing the following steps:
   a. Click the **Services** tab.
   b. Click **Stop**.
3. Restore the data from the existing server to new server by completing the following steps:
   a. Click the **Restore** tab.

b. Click **Browse** to select the path (defined in the **Output Directory** field on the **Options** dialog box - **Backup** pane) to the database backup location.
c. Click **Restore**.

   Upon completion, a window displays the status of the restore operation.

4. Restore the client-server communication IP for the new server by completing the following steps:

   Note: <*New_IP_Address*> is the IP of the current DCFM Server

   If client-to-server communication IP address is configured as the 'host name' in the new server:
   1. Open the ftpd.properties file (located in the <Install_Home>\conf\ folder) in a text editor (such as Notepad).
   2. Edit the following variables:

      config.data-connection.active.local-address=<*New_IP_Address*>

      config.data-connection.passive.address=<*New_IP_Address*>

   3. Save and close the file.
   4. Update the FTP_SERVER table's IP column with the <*New_IP_Address*> in the database by completing the following steps.
      a. Click the **Services** tab.
      b. Click **Start**.
      c. Go to <*Install_Home*>\bin.
      d. Execute interactive SQA as follows:

         Windows systems:

         dbisql.bat <*user_name*> <*password*>

         UNIX systems:

         sh dbisql <*user_name*> <*password*>

         where the <*user_name*> is dcfm and the <*password*> is passw0rd

         Example: Type **dbisql dcfm passw0rd** and press **Enter**.

      e. Type update **FTP_SERVER set IP='**<*New_IP_Address*>**' where type=0** and press **Enter** to update IP column.
      f. Type **commit** press **Enter** to save the changes.
      g. Click the **Services** tab.
      h. Click **Stop**.

         This stops the database service as well

   If client-to-server communication IP address is configured as specific address in the new server:
   1. Open the ftpd.properties file (located in the <*Install_Home*>\conf\ folder) in a text editor (such as Notepad).
   2. Edit the following variables:

      config.data-connection.active.local-address=<*New_IP_Address*>

      config.data-connection.passive.address=<*New_IP_Address*>

   3. Save and close the file.
   4. Update the **IP** column in the **FTP_SERVER** table with the <*New_IP_Address*> in the database by completing the following steps.
      a. Click the **Services** tab.
      b. Click **Start**.
      c. Go to <*Install_Home*>\bin.
      d. Execute interactive SQA as follows:

         Windows systems:

dbisql.bat <*user_name*> <*password*>

UNIX systems:

sh dbisql <*user_name*> <*password*>

where the <*user_name*> is dcfm and the <*password*> is passw0rd

Example: Type **dbisql dcfm passw0rd** and press **Enter**.

e. Type update **FTP_SERVER set IP='**<*New_IP_Address*>**' where type=0** and press **Enter** to update IP column.
f. Type **commit** press **Enter** to save the changes.

5. Click the **Services** tab.
6. Click **Stop**.
7. Open the <*Management_Application_Name*>svc.conf file (located in the <*Install_Home*>\conf\ folder) in a text editor (such as Notepad).
8. Edit the following variable:
   set.BIND_ADDRESS=<*New_IP_Address*>
9. Save and close the file.
10. Open the <*Management_Application_Name*>.properties file (located in the <*Install_Home*>\conf\ folder) in a text editor (such as Notepad).
11. Edit the following variable:

    java.rmi.server.hostname=<*New_IP_Address*>

12. Save and close the file.

5. Start the Management application services by completing the following steps:
   a. Click the **Services** tab.
   b. Click **Start**.
6. Launch the Management application client from the **Start** menu.
7. Configure the Server IP by completing the following steps
   a. Select **SAN > Options**.

      The **Options** dialog box displays

   b. Click **IP Configuration**.

      The **Options** dialog box - **IP Configuration** pane displays

   c. Select the correct IP address from the **Switch - Server IP Configuration** list.
8. Restart the server to perform SNMP and Syslog auto registration with the new server IP address to all switches.

   NOTE: If the old server IP address displays in SNMP trap and Syslog recipient list, you must manually remove it from the list. The Management application server does not remove the old server IP address during auto-registration.

DCFM User Manual

On page 44, in the **Discovering Hosts by IP address or hostname** section, change the following step as follows:

4. Select **Network Name** from the list.

In the **Management server and client** section (starting on page 60), add the following information.

On multiple pages, in the **Call Home** section, remove all references to the EMC E-mail Call Home Center. The EMC E-mail Call Home Center is no longer available.

The SNMP (161), SNMP Traps (162), Syslog (514), and RADIUS (1812) services use UDP as transport. All other services use TCP as transport.

On page 101, in the **Configuring event storage** section, edit the procedure as follows:

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Event Storage** in the **Category** list.

3. Select the **Purge Events** check box.

   Events are purged at midnight (12:00 AM). For example, when the maximum number of events allowed limit is reached at 3:00 PM, the system purges the older events at midnight that day.

4. Enter the number of events (1 through 50000) in the repository in the **Maximum Historical Event** field.

   Older events are purged at midnight on the date the maximum event limit is reached regardless of the retention days.

5. Enter then number of days (1 through 30) you want to store events in the **Store Historical Event for <*number*> days** field.

   The events are purged at midnight on the last day of the retention period regardless of the number of maximum events.

6. Click **OK**.

On page 301, in the **Historical performance data** section, edit the third bullet as follows:

Store up to 606 records (maximum) for each port. Most ports require 600 KB disk space; however, the 256-Port Director requires 7GB disk space.

On page 597, in the **Troubleshooting** section, add the **Launch Client troubleshooting** information listed below.

Launch Client troubleshooting

The following section states a possible issue and the recommended solution if you are unable to launch the client.

Launch Client Issues

Problem	Resolution
Unable to log into the Client (the application does not launch when you use a valid user name and password and exceptions are thrown in the client side).	Use one the following procedures to configure the IP address in the host file. **Windows operating systems** 1. Log in using the 'Administrator' privilege. 2. Select **Start > Run**. 3. Type **drivers** in the **Open** field and press **Enter**. 4. Go to the ‘etc’ folder and open the ‘hosts’ file using a text editor. 5. Add the IP address and host name of the client and server in the following format: <IP_address> <Host_name>. For example: 102.54.94.97 rhino.acme.com # source server 38.25.63.10 x.acme.com # x client host 6. Save and exit the file. **Linux/Solaris operating systems** 1. Log in using the 'root' privilege. 2. Open the ‘/etc/hosts’ file using a text editor. 3. Add the IP address and host name of the client and server in the following format: <IP_address> <Host_name>. For example: 102.54.94.97 rhino.acme.com # source server 38.25.63.10 x.acme.com # x client host 4. Save and exit the file.

On page 597, in the **Troubleshooting** section, add the **Server Management Console troubleshooting** information listed below.

Server Management Console troubleshooting

The following section states a possible issue and the recommended solution for the Server Management Console (SMC).

Server Management Console issues

Problem	Resolution
Unable to launch the SMC on a Windows Vista system.	The Windows Vista system enables the User Access Control (UAC) option by default. When the UAC option is enabled, the SMC cannot launch. If the SMC does not launch, use one of the following options to disable the UAC option: The following are the various ways we can disable UAC in vista: Disable using msconfig by completing the following steps. 1. Select **Start > Run**. 2. Type msconfig on the **Run** dialog box and click **OK**. 3. Click the **Tools** tab on the **System Configuration Utility**. 4. Scroll down to and select the **Disable UAC** tool name. 5. Click **Launch**. A command window displays and runs the disable UAC command. When the command is complete, close the window. 6. Close the System Configuration Utility. 7. Restart the computer to apply changes. **Note:** You can re-enable UAC using the above procedure and selecting the **Enable UAC** tool name in step 4. Disable using regedit by completing the following steps. **Note:** Before making changes to the registry, make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes. 1. Select **Start > Run**. 2. Type regedit on the **Run** dialog box and click **OK**. 3. Navigate to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System 4. Right-click the **EnableLUA** value and select **Modify**. 5. Change the **Value data** field to 0 on the **Edit DWORD Value** dialog box and click **OK.** 6. Close the Registry Editor. 7. Restart the computer to apply changes. **Note:** You can re-enable UAC using the above procedure and changing the **Value data** field to 1 in step 5. Disable using the Group Policy by completing the following steps.

Problem	Resolution
	You can perform this procedure on you local machine using Local Group Policy editor or for many computers at the same time using the Active Directory-based Group Policy Object (GPO) editor. To disable using the Local Group Policy editor, complete the following steps. 1. On your local Vista computer, select **Start > Run**. 2. Type gpedit.msc on the **Run** dialog box and click **OK**. 3. Browse to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** in the Group Policy editor. 4. In the right pane scroll to the User Access Control policies (at the bottom of the pane). 5. Right-click the **Behavior of the elevation prompt for Administrators in Admin Approval Mode** policy and select **Properties**. 6. Select the **No Prompt** option and click **OK**. 7. Right-click the **Detect application installations and prompt for elevation** policy and select **Properties**. 8. Select the **Disabled** option and click **OK**. 9. Right-click the **Run all administrators in Admin Approval Mode** policy and select **Properties**. 10. Select the **Disabled** option and click **OK**. 11. Close the Group Policy editor. 12. Restart the computer to apply changes. To disable using the Active Directory-based GPO editor, complete the following steps. 1. On a Vista computer that is a member of a domain, select **Start > Run**. 2. Type gpedit.msc on the **Run** dialog box and click **OK**. 3. Browse to the required GPO that is linked to the OU or domain where the Vista computers are located, then edit it 4. Browse to **Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options** in the Group Policy editor. 5. In the right pane scroll to the User Access Control policies (at the bottom of the pane). 6. Right-click the **Behavior of the elevation prompt for Administrators in Admin Approval Mode** policy and select **Properties**. 7. Select the **No Prompt** option and click **OK**. 8. Right-click the **Detect application installations and prompt for elevation** policy and select **Properties**. 9. Select the **Disabled** option and click **OK**. 10. Right-click the **Run all administrators in Admin Approval Mode** policy and select **Properties**. 11. Select the **Disabled** option and click **OK**. 12. Close the Group Policy editor. 13. Restart the computer to apply changes.

On page 629, in the **About User Privileges** section, change the Configuration Management and Technical Support Data Collection privileges as follows:

Privilege	Description	No Privilege	Read-Only	Read/Write
Configuration Management	Allows you to access the **Configuration Management** dialog box and perform configuration upload and replication.	Disables **Save**, **Restore**, **Configuration Repository**, and **Schedule Backup** under **Configure > FC Switch** and the **Configuration** command under **Configure > FC Switch > Replicate**.	Enables **Configuration Repository** under **Configure > FC Switch**. Only viewing of saved configuration is supported. Configuration upload and replication are disabled.	Enables all commands under **Configure > FC Switch**. Allows you to perform configuration upload, download and restore.
Technical Support Data Collection	Allows you to capture support data from Fabric OS switches.	Disables the **SupportSave**, **Upload Failure Data Capture**, and **View Repository** commands from the **Monitor > Technical Support** menu and right-click menu.	Enables the **View Repository** command from the **Monitor > Technical Support** menu and right-click menu. Disables the **SupportSave** and **Upload Failure Data Capture** commands from the **Monitor > Technical Support** menu and right-click menu.	Enables the **SupportSave**, **Upload Failure Data Capture**, and **View Repository** commands from the **Monitor > Technical Support** menu and right-click menu. Enables all functions on the dialog boxes.

DCFM Online Help

In the **Address Properties** dialog box, **SNMP** tab section, change the field and component table as follows:

Field/Component	Description
Target Port text box	The target port number. The default value is 161.

In the **Options** dialog box, **Event Storage** pane section, change the field and component table as follows:

Field/Component	Description
Maximum Historical Event text box	Type in the maximum number of historical events you want to keep in the repository. The maximum number the repository holds is 50000. Default is 20000.

In the **FCIP tunnels** dialog box section, add the information as follows:

Edit FCIP tunnels dialog box

When you configure an FCIP extension connection, you create FCIP tunnels and FCIP circuits between two extension switches.

Opening the dialog box

1. Select **Configure > FCIP Tunnel**.

   The **FCIP Tunnels** dialog box display. All discovered fabrics with extension switches are listed under devices, and all existing FCIP tunnels are displayed.

2. Select the FCIP tunnel you want to edit under **Devices**.

3. Click **Edit Tunnel**.

   The **Edit FCIP Tunnel** dialog box displays. This dialog box allows you to configure settings for both switches on either end of the tunnel.

Fields and Components

Field/Component	Description
Switch One Settings **Switch Two Settings**	Settings for the switches on either end of the tunnel are configured and displayed under these two headings.
Select Switch Two button	Click to display the **Select Switch** dialog box. To create an FCIP tunnel, you must configure a switch on either end of the tunnel.
Switch	The name of the switch.
Fabric	The fabric that contains the switch.
Tunnel	A numeric ID assigned to the tunnel. Note that a tunnel ID cannot be applied until after a circuit is defined.
Description	A description of the tunnel.
Port Type	Specifies whether the port is a VEX port or a VE port. If VE ports are used for both switches, the fabrics are merged. If a VEX port type is chosen, the VEX port is assigned to switch one, and switch two remains a VE port. If a VEX port is used, the fabrics are not merged. If a VEX Port is chosen, you must supply a fabric ID and Interop mode.
Edit Circuit button	Click to display the **Edit Circuit** dialog box. At least one circuit must be created and added to implement an FCIP tunnel.
Advanced Settings button	Click to implement compression, FCIP fast write and tape pipelining, or FICON extension features.

Using the dialog box

Refer to the following topics for specific procedures using this dialog box.

Editing FCIP tunnels

Editing FCIP circuits

Configuring FCIP tunnel advanced settings

Defects Closed with Code Change in DCFM 10.3.2

This section lists the defects with High and Medium Technical Severity closed with a code change in DCFM 10.3.2.

Defect ID: DEFECT000264747	**Technical Severity**: High
Summary: Incorrect 'Source Name' for master log from virtual fabric enabled switches.	
Symptom: Master Log is showing incorrect Source Name for VF Switches	
Feature: FAULT MANAGEMENT	**Function**: NONE
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000264890	**Technical Severity**: High
Summary: Performance Management – Rx/Tx % Utilization is plotted incorrectly for xGE ports in Real Time Graph.	
Symptom: Graph will not reflect the actual data flowing.	
Feature: Performance Management	**Function**: RealTime Graph
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000264985	**Technical Severity**: High
Summary: Firmware upgrade via the Element Manager on a SAN32M-2 (M4700) never completes (according to the send firmware dialog box).	
Symptom: Element Manager will show that the firmware upgrade never completes, but actually the upgrade is success in the switch	
Feature: M-EOS Element Manager	**Function**: USABILITY
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265031	**Technical Severity**: High
Summary: Zoning: When normal zone and a TI zone is activated only the TI zone is shown as Active and the Active Zone configuration is not shown	
Symptom: Activated zone is not shown in the Active Zone Configuration after the Zone Activation	
Workaround: Wait until the Zone collection completes	
Feature: ZONING	**Function**: Online Zoning
Probability: High	**Risk of Fix**: High
Found in Release: DCFM10.3.1	

Closed with Code Change in DCFM 10.3.2

Defect ID: DEFECT000265033	**Technical Severity**: High
Summary: Zoning: When activating a new zone config, DCFM shows the old zone config as active	
Symptom: Active Zone Configuration tab is listing the old Active Zone when a New Config is activated	
Workaround: Wait until the Zone collection completes	
Feature: ZONING	**Function**: Online Zoning
Probability: High	**Risk of Fix**: High
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265293	**Technical Severity**: High
Summary: Zoning: The Redirection zones present in the zone Database vanishes when zoning activation done from DCFM	
Symptom: The Frame Redirection zones present in the Zone Database wiped out when zone activation is done.	
Feature: ZONING	**Function**: Online Zoning
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265451	**Technical Severity**: High
Summary: Webtool can not be launched from DCFM 10.3.1 with JRE 6u14 & above but DCFM webstart works fine.	
Symptom: User will not be able to launch Webtool proxy through DCFM if the JRE version is 1.6 update 14 and above.	
Feature: Proxy services	**Function**: Proxy services
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265487	**Technical Severity**: High
Summary: Except Services and Ports tabs, remaining tabs are not displayed under Server Management Console on migrating from FM to DCFM	
Symptom: Unable to see other tabs apart from services and ports.Operations like technical support information,changing Authentications are not possible.	
Feature: FM Migration	**Function**: USABILITY
Probability: High	**Risk of Fix**: Low
Found in Release: DCFM10.3.1	

Closed with Code Change in DCFM 10.3.2

Defect ID: DEFECT000257703	**Technical Severity**: Medium
Summary: FCIP: Duplicate circuits have been shown in the '**Circuits** tab' of '**FCIP Tunnels**' dialog when we create multiple circuits for the same tunnel.	
Symptom: Duplicate circuits have been shown in the '**Circuits** tab' of '**FCIP Tunnels**' dialog when we create multiple circuits for the same tunnel.	
Workaround: Close and reopen the '**FCIP Tunnels**' dialog and observe that now multiple circuits will not be shown to the user.	
Feature: FCIP	**Function**: CONFIGURATION
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000260396	**Technical Severity**: Medium
Summary: FCIP: "Failed to add IP interface, error: Configuration entry exists on a GigE port" error shown while clicking the "**Current Maximum Bandwidth**" button in the '**Edit Circuit**' dialog	
Symptom: When the user clicks the "**Current Maximum Bandwidth**" button in the **Edit Circuit** dialog, "Failed to add IP interface, error: Configuration entry exists on a GigE port" error shown, Instead of showing the IP perf result with the system suggested value. So u	
Feature: FCIP	**Function**: CONFIGURATION
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000262591	**Technical Severity**: Medium
Summary: FCIP: After creating a new tunnel, tunnel has not been shown at the "Switch-2" side. It has been shown only after relaunching the "**FCIP Tunnel**" dialog.	
Symptom: New tunnels are not shown in FCIP dialog immediately	
Workaround: Re-launch the **FCIP Tunnel** dialog	
Feature: FCIP	**Function**: CONFIGURATION
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000262947	**Technical Severity**: Medium
Summary: Not able to manage the switch in server A although the fabric is unmonitored in server B	
Symptom: User will not be able to manage the switch	
Feature: DISCOVERY	**Function**: Switch Discovery
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.2

Defect ID: DEFECT000263892	**Technical Severity**: Medium
Summary: SupportSave:No Support data are collected even after 35 minutes and empty zip folders were only created	
Symptom: User was not able to collect the Support Data for the switch	
Workaround: Restart the Server	
Feature: Technical Support	**Function**: Support Save
Probability: Medium	**Risk of Fix**: High
Found in Release: DCFM10.1.4	

Defect ID: DEFECT000264806	**Technical Severity**: Medium
Summary: Zoning: DCFM is not restricting when domain ID greater than 31 is added to the zone in Interopmode 2, which in turn cause the zone activation failure with inappropriate message	
Symptom: User will get inappropriate error message when domain ID greater than 31 is part of the Zone Database	
Workaround: User should not add members with Domain ID greater than 31 in Interopmode 2	
Feature: ZONING	**Function**: Zoning Dialog
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000264930	**Technical Severity**: Medium
Summary: In the Help content of '**Add FCIP Tunnel**' dialog, information about ' **Select Switch Two** ' button is missing	
Symptom: "**Select Switch Two**" button information is missing in the Online Help	
Feature: FCIP	**Function**: HELP
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265102	**Technical Severity**: Medium
Summary: Auto enclosure is not created in the Fabric view after discovering Host and wrong fabric WWN is shown in the Host view.	
Symptom: Auto enclosure is not seen in the fabric view though the Host connected to the fabric is discovered.	
Feature: HBA Management	**Function**: Desktop Changes
Probability: Medium	**Risk of Fix**: High
Found in Release: DCFM10.3.1	

Closed with Code Change in DCFM 10.3.2

Defect ID: DEFECT000265113	**Technical Severity**: Medium
Summary: Zoning:Error message is displayed and report is not generated while activating zone for a pure EOS fabric with report generation enabled	
Symptom: Report is not generated and error is displayed even after successfull activation of zone	
Feature: ZONING	**Function**: Zoning Dialog
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265114	**Technical Severity**: Medium
Summary: Fault Management : Master log event count is incremented with the old source name even when the switch name is changed.	
Symptom: Master Log Event is triggered with old Source Name when the Switch Name is updated	
Feature: FAULT MANAGEMENT	**Function**: USABILITY
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265223	**Technical Severity**: Medium
Summary: Renaming a host reflects only after client re-launch.	
Symptom: User will not be able to see the edited host name unless he re-launches the client.	
Workaround: Restart the client	
Feature: HBA Management	**Function**: Desktop Changes
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265230	**Technical Severity**: Medium
Summary: FCIP: When we edit the tunnel present between, SAN18B-R and SAN04B-R in the '**Advanced settings**' window, the **Transmission** tab is enabled. It gets disabled only when we move to other tabs.	
Symptom: In the '**Advanced settings**' window, the **Transmission** tab is enabled, When we edit the tunnel present between SAN18B-R and SAN04B-R, it should be in disabled state as SAN04B-R doesn't support it.	
Feature: FCIP	**Function**: CONFIGURATION
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Closed with Code Change in DCFM 10.3.2

Defect ID: DEFECT000265318	**Technical Severity**: Medium
Summary: After adding single side tunnel on SAN768B-[FR4-18i] or SAN256B[FR4-18i], VE port number not shown along with Tunnel ID. Upon adding second side tunnel for that one side tunnel error has been thrown in “FCIP Tunnel\Circuit Configuration Report” dialog.	
Symptom: User unable to add second side tunnel by selecting "SAN768B [FR4-18i] or SAN256B[FR4-18i]" as Remote Switch, for the one side tunnel exists in the "SAN768B [FR4-18i] or SAN256B[FR4-18i]" error has been thrown in “FCIP Tunnel\Circuit Configuration Report” dialog.	
Workaround: Add the double side tunnel between "Two SAN768B [FR4-18i] or Two SAN256B[FR4-18i],". We will be able to configure the tunnel.	
Feature: FCIP	**Function**: CONFIGURATION
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265376	**Technical Severity**: Medium
Summary: Zoning:An alert message is shown in the zoning dialog when the TI zone modification is done before activation	
Symptom: alert message is shown in zoning dialog though there is no changes in zone configuration	
Feature: ZONING	**Function**: Zoning Dialog
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.1	

Defect ID: DEFECT000265407	**Technical Severity**: Medium
Summary: After creating a third circuit, Horizontal scroll bar not shown in the “**Circuit** tab” of “**FCIP tunnel**” dialog.	
Symptom: After creating a third circuit, the user will not see the Horizontal scroll bar in the “**Circuit** tab” of “**FCIP tunnel**” dialog. It will be shown only after relaunching the "**FCIP Tunnel**" dialog.	
Workaround: Close and open the **FCIP tunnel** dialog. Horizontal scroll bar will be shown	
Feature: FCIP	**Function**: CONFIGURATION
Probability: Medium	**Risk of Fix**: Low
Found in Release: DCFM10.3.1	

Defects Closed with Code Change in DCFM 10.3.1

This section lists the defects with High and Medium Technical Severity closed with a code change in DCFM 10.3.1.

Defect ID: DEFECT000255806	**Technical Severity**: High
Summary: LSAN Zoning; Activated LSAN zone is not shown in the LSAN zoning dialog after reopening the dialog	
Symptom: LSAN zoning dialog is not showing the activated LSAN zone	
Workaround: Wait for 15 to 30 minutes	
Feature: FAULT MANAGEMENT	**Function**: NONE
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000256212	**Technical Severity**: High
Summary: PAD: Unable to unblock a automatically disabled port from PAD dialog	
Symptom: Not able to unblock a automatically disabled port.	
Workaround: Use CLI to unblock the port	
Feature: Port Auto Disable	**Function**: ENHANCEMENT
Probability: High	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000256371	**Technical Severity**: High
Summary: FCIP: Duplicate tunnels are shown in the **FCIP tunnel** dialog. After creating 4 tunnels , 4 more duplicate tunnels are shown, so unable to create 5th tunnel.	
Symptom: User will not be able to create more than 4 tunnels	
Feature: FCIP	**Function**: CONFIGURATION
Probability: High	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000256896	**Technical Severity**: High
Summary: Tunnel links are not being displayed in topology.	
Symptom: Switches in the Fabric are shown isolated without any link between them and also the user will not have the option to launch the **Connection properties** dialog.	
Feature: FCIP	**Function**: CONFIGURATION
Probability: High	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000258864	**Technical Severity**: High
Summary: Scalability: Client logs out observed in the Scalability server	
Symptom: client log out will be observed	
Feature: Client/Server Communication	**Function**: Client/Server Communication
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000258914	**Technical Severity**: High
Summary: Client lost connection to server on Linux server overnight. Local client	
Symptom: Client connectivity lost, need to re-login.	
Feature: Client/Server Communication	**Function**: Client/Server Communication
Probability: Medium	**Risk of Fix**: High
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000260437	**Technical Severity**: High
Summary: Host and storage connected to a fabric are shown isolated in the Host view when Host is rediscovered because of HCM agent connection failure	
Symptom: In the Host View, isolated HBA and the storage nodes are shown without any connections.	
Workaround: - Delete the newly discovered host - Monitor the old fabric - Delete and rediscover the host	
Feature: HBA Management	**Function**: Discovery (FC HBA & CNA)
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000260866	**Technical Severity**: High
Summary: Duplicate virtual NPIV ports are shown in device tree for m-type switch after migrating from EFCM to DCFM	
Symptom: Duplicate virtual NPIV ports are shown for m-type switch	
Feature: Client	**Function**: TOPOLOGY
Probability: High	**Risk of Fix**: High
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000261742	**Technical Severity**: High
Summary: DCFM reading CNA HCM Name into the DCFM Names database	
Symptom: Cannot use DCFM to set/change a CNA node or port name, must use HCM	
Feature: HBA Management	**Function**: Discovery (FC HBA & CNA)
Probability: High	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000262867	**Technical Severity**: High
Summary: SNMPv3 SHA authentication used in switch discovery fails	
Symptom: Switch cannot be discovered with SNMPv3 SHA	
Feature: DISCOVERY	**Function**: Switch Discovery
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000235540	**Technical Severity**: Medium
Summary: The "**vendor E-mail**" option is not necessary and having both the "**vendor**" and "**vendor E-mail**" options available will only create confusion.	
Symptom: The "**EMC E-mail**" option is not necessary and having both the "**vendor**" and "**vendor E-mail**" options available will only create confusion.	
Feature: other Dialog	**Function**: USABILITY
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.0.2	**Service Request ID**: 352329

Defect ID: DEFECT000241637	**Technical Severity**: Medium
Summary: Zone details missing in zone compare.	
Symptom: Zone details missing in zone compare. The panel is blank. Furthermore, it's not clear what the comparison would be. Is it the difference between the library and the fabric or vice versa?	
Feature: ZONING	**Function**: USABILITY
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.1.1	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000241638	**Technical Severity**: Medium
Summary: Zones Not Shown Correctly After Import	
Symptom: Zones not shown correctly after import. The names by adding the prefix "old_" so the zones no longer exist in the DB	
Feature: ZONING	**Function**: Zoning Dialog
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.1.1	

Defect ID: DEFECT000243353	**Technical Severity**: Medium
Summary: There are some issues found while configuring an end-to-end monitor pair.	
Symptom: Logic is reversed in case of end to end monitors	
Feature: Client	**Function**: TOPOLOGY
Probability: Medium	**Risk of Fix**: Low
Found in Release: DCFM10.1.1	**Service Request ID**: 370061

Defect ID: DEFECT000253184	**Technical Severity**: Medium
Summary: Fault Management – Switches discovered through v1 are getting listed in the **Informs** table in the "**snmp setup**" dialog listing	
Symptom: Customer will get confused when switches discovered via v1 are also listed in the table and only informs support is for FOS v6.3 discovered via v3.	
Feature: MISC	**Function**: SNMP INFORMS
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000256506	**Technical Severity**: Medium
Summary: Client: In Pure mEOS the Plus symbol is not removed from the device tree after giving accept changes	
Symptom: Topology will not properly reflect the changes to Users	
Workaround: Launch a new client	
Feature: Client	**Function**: Client Framework
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000256989	**Technical Severity**: Medium
Summary: Scalability Fabric: Local Client hangs when the total switch count is 10172 ports	
Symptom: Local client launched does not show the data	
Workaround: restart the client	
Feature: Client	**Function**: TOPOLOGY
Probability: Low	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000257467	**Technical Severity**: Medium
Summary: EOS: EOSc switches discovered as seed loses manageability and discovery status shows “Invalid protocol”.	
Symptom: User will not get manageability for EOS switches	
Feature: Mbean for Server	**Function**: Mbean for Server
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000257722	**Technical Severity**: Medium
Summary: Not able to make any zoning changes, works on b/u server	
Symptom: Zoning activation fails in case the port index greater than 255 is part of the zone Configuration in Interopmode 2	
Workaround: This would work fine, if only port index lesser than 256 are selected.	
Feature: ZONING	**Function**: USABILITY
Probability: Low	**Risk of Fix**: Medium
Found in Release: DCFM10.1.3	**Service Request ID**: 386917

Defect ID: DEFECT000258206	**Technical Severity**: Medium
Summary: Client crashes on launch when the system is at JRE 1.6.0_14	
Symptom: Client will not start	
Feature: Client	**Function**: Client Framework
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000259010	**Technical Severity**: Medium
Summary: Incorrect port number is displayed in the Topology for Switch to Switch connection	
Symptom: Link shows incorrect port information	
Feature: Client	**Function**: USABILITY
Probability: Medium	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000259163	**Technical Severity**: Medium
Summary: Discovery status for VF enabled switch is not getting updated in the Discovery dialog after changing its credentials from v1 to v3.	
Symptom: Appropriate Discovery status is not shown for VF enabled switches after modifying the SNMP credentials from v1 to v3.	
Feature: DISCOVERY	**Function**: Discovery Dialog
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000259605	**Technical Severity**: Medium
Summary: Discovery: Not able to discover the logical switch without deleting the existing one after changing the FID	
Symptom: Not able to manage the LS after changing the FID	
Workaround: Unmonitor/delete the unreachable LS	
Feature: DISCOVERY	**Function**: Switch Discovery
Probability: High	**Risk of Fix**: High
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000259674	**Technical Severity**: Medium
Summary: No ISL link is formed when port disable and enable is done in SAN Switch M14	
Symptom: Topology will not reflect properly to the user	
Feature: DISCOVERY	**Function**: ISL Discovery
Probability: Medium	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000260937	**Technical Severity**: Medium
Summary: FCIP: While disabling a tunnel between a SAN18B-R and a SAN04B-R, operation failed and invalid error has been thrown. Also the error message is not fully shown to the user.	
Symptom: Invalid error has been thrown, while disabling the tunnel there between the SAN18B-R and SAN04B-R switches, also the error message not fully shown to user. User has to maximize the window to see the full error message.	
Feature: FCIP	**Function**: CONFIGURATION
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000261014	**Technical Severity**: Medium
Summary: Web Tools is not launched for the switches in the SSL enabled server after migration	
Symptom: User will not be able to launch web tool some times.	
Feature: Proxy services	**Function**: Proxy services
Probability: Medium	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000261162	**Technical Severity**: Medium
Summary: Internal error is thrown on modifying the SNMP credentials from **Edit Discovery** dialog.	
Symptom: Internal error is observed when the SNMP credentials are modified for the Discovered switches after initial discovery.	
Feature: DISCOVERY	**Function**: Discovery Dialog
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000261163	**Technical Severity**: Medium
Summary: **FICON: Merge** wizard says merge operation success, but the master log says merge operation failed	
Symptom: User will not be sure whether the merge operation is success or failed	
Feature: FICON	**Function**: Cascaded FICON Merge
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000261422	**Technical Severity**: Medium
Summary: Yellow banner displayed in **ACL** tab of **Add LAG** dialog is not according tom FS.	
Symptom: Yellow banner displayed in the **ACL** tab of **Edit switch** isn't appropriate.	
Feature: FCoE/CEE Management	**Function**: Add/Edit CEE Port/LAG Dialog
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000261425	**Technical Severity**: Medium
Summary: Yellow banner displayed in **ACL** tab of **Edit port** dialog [LAG member] is not according to Functional Specification document	
Symptom: Yellow banner displayed in **ACL** tab will not be in sync with Functional Specification document	
Feature: FCoE/CEE Management	**Function**: Add/Edit CEE Port/LAG Dialog
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000261585	**Technical Severity**: Medium
Summary: When the Client is kept idle for some time, “unable to recover connection to server” error message is displayed.	
Symptom: Client suddenly lost its connection with the server and an error message "unable to recover connection to server" is displayed.	
Feature: Client	**Function**: USABILITY
Probability: Low	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000261645	**Technical Severity**: Medium
Summary: WT session got expired before the session time out value and also OutOfMemoryError Exception thrown when launched from DCFM	
Symptom: WT sessions gets expired before reaching the time out values	
Workaround: Launch WT via IE	
Feature: Other Dialogs	**Function**: USABILITY
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000261785	**Technical Severity**: Medium
Summary: Migration: After migration from EFCM, SAN256M is not getting manageability if it is discovered using APIuser in EFCM	
Symptom: SAN256M is not getting manageability after Migration	
Workaround: Give the proper SNMP credentials after migration or delete and rediscover the Fabric	
Feature: EFCM Migration	**Function**: USABILITY
Probability: High	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000261941	**Technical Severity**: Medium
Summary: Trap forwarding not allowing IP address addition	
Symptom: User will not be able to add the IP address of machine in which client is running.	
Workaround: Trap forwarding issue occurs only when the client IP matches the trap recipient IP, the workaround would be to try on a different client IP	
Feature: Other Dialogs	**Function**: USABILITY
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000262177	**Technical Severity**: Medium
Summary: Firmware Management – Import of firmware to repository fails with two different error messages that are not appropriate.	
Symptom: Misleads the user with incorrect error messages.	
Feature: FIRMWARE MANAGEMENT	**Function**: Firmware Repository Management
Probability: Medium	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000262526	**Technical Severity**: Medium
Summary: From a CMDCE to CMDCE migration, the call home that is enabled for EMC cannot be disabled.	
Symptom: EMC call home configuration cannot be disabled on a migrated server	
Feature: Advanced Call Home	**Function**: USABILITY
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Closed with Code Change in DCFM 10.3.1

Defect ID: DEFECT000262894	**Technical Severity**: Medium
Summary: Fabric changes cannot be accepted due to AG collector run before switch creation	
Symptom: When a AG capable device newly joins the fabric, the device type is not updated with an AG icon in the Connectivity Map and user will not be able to perform the 'Accept Changes' operation.	
Feature: Access Gateway	**Function**: Access Gateway
Probability: High	**Risk of Fix**: Medium
Found in Release: DCFM10.3.0	

Defect ID: DEFECT000262963	**Technical Severity**: Medium
Summary: Forbidden errors when doing the initial discovery in DCFM 10.1.4	
Symptom: User will not be able perform operations like Fabric Binding, Port Optics, Port Fencing etc.. when SSL is enabled & Port 80 is blocked.	
Feature: UNDETERMINED	**Function**: UNDER REVIEW
Probability: Low	**Risk of Fix**: Medium
Found in Release: DCFM10.1.4	**Service Request ID**: 396467

Defect ID: DEFECT000263418	**Technical Severity**: Medium
Summary: Improve LIC error message when there is no fabric being managed by DCFM, current message causes confusion	
Symptom: Error message doesn't give proper reason for the failure to launch certain dialogs	
Feature: LIC & SSO	**Function**: Launch in Context
Probability: Medium	**Risk of Fix**: Low
Found in Release: DCFM10.3.0	