



IBM System Storage™

# Data Center Fabric Manager v10.3.3

## Release Notes

Copyright © 2001-2010, Brocade Communications Systems, Incorporated.

Copyright © IBM Corporation 2008, 2010. All rights reserved.

Brocade, and Fabric OS are registered trademarks and the Brocade B-wing symbol and DCX, and are trademarks of Brocade Communications Systems, Inc., in the United States and/or in other countries. All other brands, products, or service names are or may be trademarks or service marks of, and are used to identify, products or services of their respective owners.

IBM, the IBM logo, and [ibm.com](http://www.ibm.com) are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

Notice: The information in this document is provided "AS IS," without warranty of any kind, including, without limitation, any implied warranty of merchantability, noninfringement or fitness for a particular purpose. Disclosure of information in this material in no way grants a recipient any rights under Brocade's patents, copyrights, trade secrets or other intellectual property rights. Brocade and IBM reserve the right to make changes to this document at any time, without notice, and assumes no responsibility for its use.

The authors, Brocade Communications Systems, Inc. , and IBM Corporation 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.....	5
New Hardware Platforms in DCFM 10.3.x.....	5
New Software Features .....	5
Enhancements to existing features.....	5
Switch Platform and Firmware Requirements.....	10
Management application server running in Windows 2008:.....	11
Important Notes.....	15
M-EOSc switches with SNMPv3 enabled cannot be managed through DCFM. SNMPv3 needs to be disabled.....	15
Issues with JRE v1.6.0 update not at 13 .....	15
Upgrade switches running FOS v5.2.1_NI to v6.0.0 or higher .....	15
Creating tape pool in a mixed FOS version environment.....	15
Event priority mismatch.....	15
Config Download fails when all parameters are selected.....	15
Switch name update delay.....	15
Element Manager fails to launch on SAN256M (Mi10k).....	15
Deleting Logical Switches with GbE ports causes errors .....	16
Event-based file actions fail.....	16
EX-Port disabled when configuring Routing Domain IDs .....	16
Removing Switches .....	16
DCFM Clients.....	16
Secure FOS fabrics cannot be discovered from DCFM .....	16
Performance Data Aging tab has been removed from Server Management Console (SMC).....	16
Unable to launch Element Manager for EOS switches after Migrating from EFCM.....	16
Encryption switch/blade public certificates exported using DCFM should be signed before the switches can connect to the Key Vault .....	17
Encryption config has limited support and slow to register change for LUN provisioning.....	17
Inappropriate Discovery status displayed for VF enabled switches .....	17
M-i10k is not displayed under EMC call center in CMDCE after migration when it is assigned under EMC in CM.....	17
Complete migration process (from installing DCFM to discovering all the switches .....	17
Complete migration process (from installing DCFM to discovering all the switches .....	17
Firmware Repository select Latest option.....	17
Empty LAG creation.....	17
Duplicate tunnels are shown in the FCIP tunnel dialog after creating a new tunnel .....	18
No operation performed when clicking the buttons present in the "FCIP Tunnel" dialog.....	18
In the "FCIP Tunnel" dialog after adding the new circuit in the 'Circuits' TAB, some fields are shown as EMPTY.....	18
Error message thrown when deleting a circuit.....	18
IFL connection shown in topology after deleting all the VE-VEX tunnels present between the SAN06B-R switches.....	18
When the switch is converted to AG an extra HBA icon is displayed in Topology.....	18
When the AG is converted to Switch it will still show as AG.....	18
AG to switch connection is not shown after the Fabric merge.....	18
F ports connected to Access Gateway are not shown as attached ports under the switch .....	18

Quorum card options are enabled in mixed FOS Encryption Group .....	19
Connection between AG and switch are not shown when F_port trunking is enabled on the AG .....	19
Zoning dialog opening fails when attempting to open before the discovery completes .....	19
SAN256M (MI10k) is not manageable in DCFM 10.3.x after migration when it is discovered using SNMPv3 with APluser in DCFM 10.0.x / 10.1.x .....	19
DCFM Users who use SysLog Host Configuration for events.....	19
Failover restriction in Mixed Fabric .....	19
Display of Logical switches .....	19
Device Port update in topology View .....	20
Procedure to update FTP IP address in db when there is a change in the Server IP address.....	20
Update the FTP SERVER table with the new IP Address .....	20
Documentation Updates .....	24
DCFM Installation, Migration, and Transition Guide .....	24
DCFM User Manual .....	32
Minimum CEE configuration for FCoE traffic.....	32
Creating the CEE map to carry the LAN and SAN traffic .....	32
Configuring LLDP for FCoE .....	33
Configuring the CEE interface with the CEE Map and Global LLDP profile.....	34
Create the FCoE VLAN to carry FCoE traffic .....	35
Creating VLAN classifiers and activating on the CEE interface .....	35
DCFM Online Help.....	39
Defects Closed with Code Change in DCFM 10.3.3 .....	42
Defects Closed with Code Change in DCFM 10.3.2 .....	45
Defects Closed with Code Change in DCFM 10.3.1 .....	50

## Overview

**IBM Data Center Fabric Manager (DCFM) 10.3.3** release adds support for a new hardware platform, new software features, and enhancements to existing features as outlined below.

### ***New Hardware Platforms in DCFM 10.3.x***

- 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)
- Brocade VA-40FC for 1410 SAN Switch Bundle and Brocade VA-40FC for iDataPlex SAN Switch Bundle

### ***New Software Features***

- FCoE / CEE Performance Management
  - Support for historical and real-time 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 3.5 virtual machines using centralized licensing 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 fall back 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 dialog (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 trace dump 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  $\geq 80\%$  and disk space usage  $\geq 90\%$
  - 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 log files 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, aliases 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 upgrading 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 10.3.3 supports a seamless upgrade path from previous versions of IBM DCFM (10.0.x, 10.1.x, and previous 10.3.x versions) 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 10.3.3 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
<b>Switch (b-type and B-Model) Firmware Versions</b>		
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) SAN Switch H08 (2005-H08) SAN Switch H16 (2005-H16) SAN32B-2 (2005-B32, -32B) SAN04B-R (2005-R04) <sup>1</sup> SAN18B-R (2005-R18) <sup>1</sup> SAN16B-2 (2005-B16, -16B) SAN64B-2 (2005-B64) <sup>2</sup> SAN32B-3 (2005-B5K, -5KB) <sup>3</sup> SAN24B-4 Express (2498-B24, -24E) <sup>5</sup> SAN40B-4 (2498-B40, -40E) <sup>5</sup> VA-40FC <sup>11</sup> SAN80B-4 (2498-B80) <sup>5</sup> IBM Converged Switch B32 (3758-B32) <sup>10</sup> SAN06B-R (2498-R06) <sup>9</sup> SAN Switch M12 (2109-M12) SAN Switch M14 (2109-M14) SAN256B (2109-M48) with FC4-16, FC4-32 and FC4-48 blades <sup>2</sup> SAN256B (2109-M48) with FR4-18i blades <sup>1</sup> SAN256B (2109-M48) with FC4-16IP blades <sup>2</sup> SAN256B (2109-M48) with FC10-6 blade <sup>4</sup> SAN768B (2499-384) with FC8-16, FC8-32, and FC8-48 blades <sup>6</sup> SAN768B (2499-384) with FR4-18i blades <sup>6</sup> SAN768B (2499-384) with FC10-6 blades <sup>6</sup> SAN768B (2499-384) with FX8-24 blades <sup>10</sup> SAN768B (2499-384) with FCoE10-24 blades <sup>10</sup> SAN384B (2499-192) with FC8-16, FC8-32, and FC8-48 blades <sup>8</sup> SAN384B (2499-192) with FR4-18i blades <sup>8</sup> SAN384B (2499-192) with FC10-6 blades <sup>8</sup> SAN384B (2499-192) with FX8-24 blades <sup>10</sup> SAN384B (2499-192) with FCoE10-24 blades <sup>10</sup>	Brocade 3900 Brocade 3250 Brocade 3850 Brocade 4100 Brocade 7500E <sup>1</sup> Brocade 7500 <sup>1</sup> Brocade 200E Brocade 4900 <sup>2</sup> Brocade 5000 <sup>3</sup> Brocade 300 <sup>5</sup> Brocade 5100 <sup>5</sup> VA-40FC <sup>11</sup> Brocade 5300 <sup>5</sup> Brocade 7800 <sup>10</sup> Brocade 8000 <sup>9</sup> Brocade 12000 Brocade 24000 Brocade 4800 with FC4-16, FC4-32 and FC4-48 blades <sup>2</sup> Brocade 4800 with FR4-18i blades <sup>1</sup> Brocade 4800 with FC4-16IP blades <sup>2</sup> Brocade 4800 with FC10-6 blades <sup>4</sup> Brocade DCX with FC8-16, FC8-32, and FC8-48 blades <sup>6</sup> Brocade DCX with FR4-18i blades <sup>6</sup> Brocade DCX with FC10-6 blades <sup>6</sup> Brocade DCX with FX8-24 blades <sup>10</sup> Brocade DCX with FCoE10-24 blades <sup>10</sup> Brocade DCX-4S with FC8-16, FC8-32, and FC8-48 blades <sup>8</sup> Brocade DCX-4S with FR4-18i blades <sup>8</sup> Brocade DCX-4S with FC10-6 blades <sup>8</sup> Brocade DCX-4S with FX8-24 blades <sup>10</sup> Brocade DCX-4S with FCoE10-24 blades <sup>10</sup>
	<sup>1</sup> Requires FOS v5.1.0 or higher <sup>2</sup> Requires FOS v5.2.0 or higher <sup>3</sup> Requires FOS v5.2.1 or higher <sup>4</sup> Requires FOS v5.3.0 or higher <sup>5</sup> Requires FOS v6.1.0 or higher <sup>6</sup> Requires FOS v6.0.0 or higher	<sup>7</sup> Requires FOS v6.1.1_enc or higher <sup>8</sup> Requires FOS v6.2.x or higher <sup>9</sup> Requires FOS v6.1.2_CEE or 6.3 <sup>10</sup> Requires FOS v6.3.0 or higher <sup>11</sup> Requires FOS v6.2.1_vfs

Operating System	IBM Switch/Director	Brocade Switch/Director
<b>Switch (m-type, M-Model) Firmware Versions</b>		
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

### ***Management application server running in Windows 2008:***

By default, when the Firewall is in “On” state in Windows 2008, it blocks all inbound connections to the host. You must select “Allow” in the **inbound connections** dropdown list to allow clients from other hosts to access the Management application server.

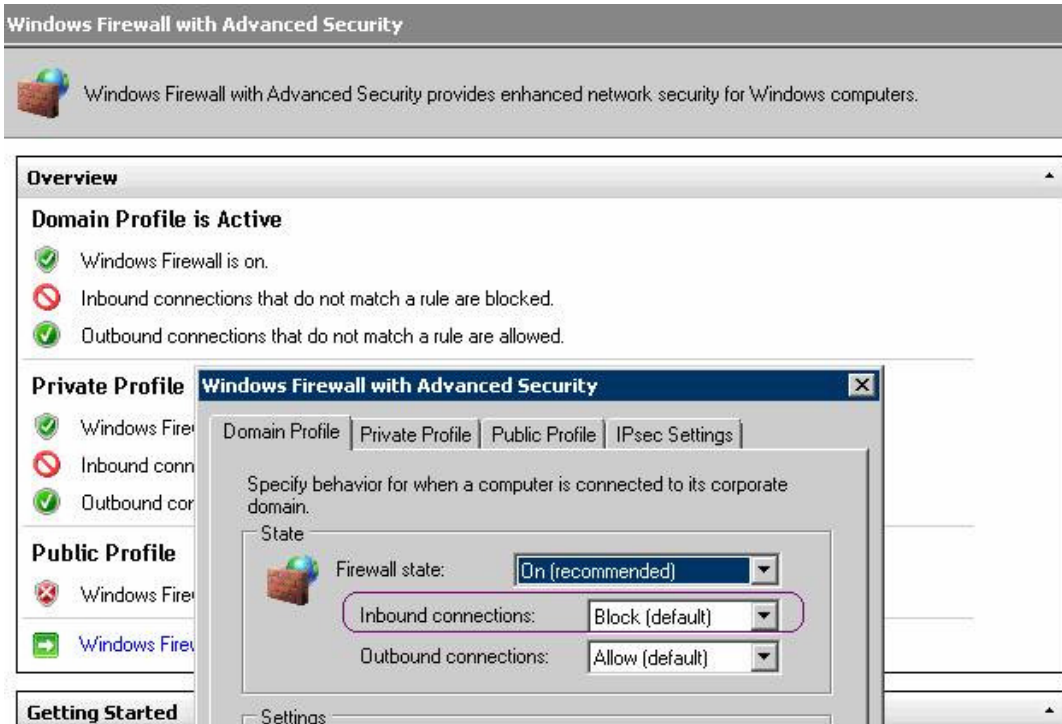
To change this setting, complete the following steps.

1. Select **Start > Administrative Tools > Server Manager**.
2. Click **Continue** on the **User Account Control** dialog box.
3. Under **Security Summary**, click **Go to Windows Firewall**.
4. Click **Windows Firewall Properties**. The **Windows Firewall with Advanced Security** dialog box displays.
5. On the **Windows Firewall with Advanced Security** dialog box, based on the Active Profile<sup>1</sup>, select **Allow** from the **Inbound Connections** list.

<sup>1</sup>**Note:** Windows Firewall with Advanced Security supports separate profiles (sets of firewall and connection security rules) for when computers are members of a domain, or connected to a private or public network.

6. Click **OK** to save the changes.

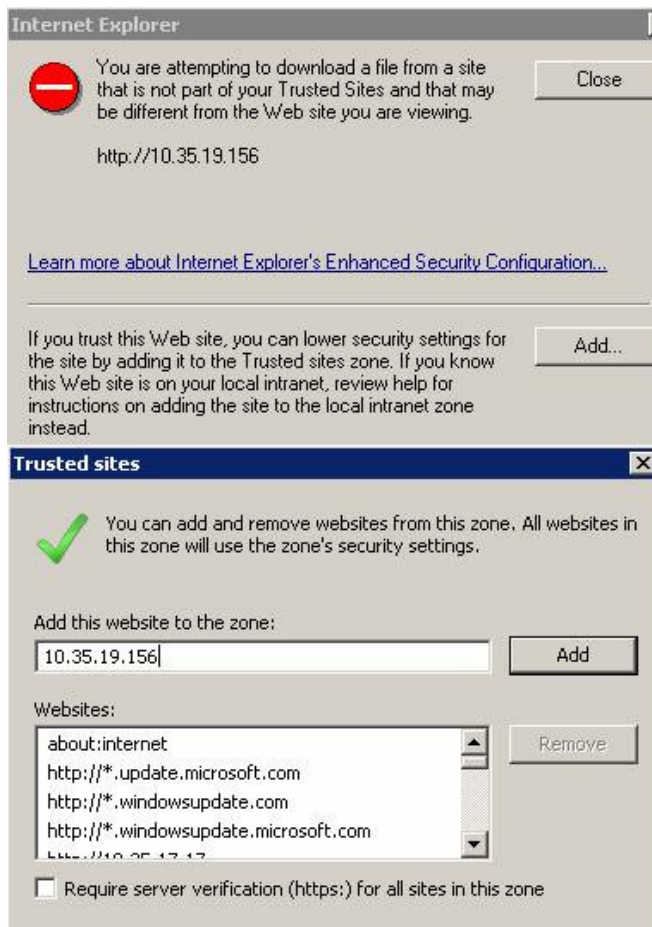
Once “Allow” option is selected in the **Inbound Connections** dropdown, user can launch client to the server running in 2008 host. In the snapshot below the Domain profile is Active.



For more information on Windows Firewall with Advanced Security, refer to [http://technet.microsoft.com/en-us/library/cc748991\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc748991(WS.10).aspx)

**To launch client from Windows 2008 host to Management application server:**

By default, Internet Explorer Enhanced Security Configuration (IE ESC) is enabled in Windows 2008. When you try to launch the client from the 2008 host to another host in which the Management application server is running, the following warning message displays. Click **Add** to add the site (Server IP) on which the Management application server is running to download the client.



If you do not want to see the warning message again, disable the IE ESE by completing the following steps.

1. Close all instances of Internet Explorer.
2. Select **Start > Administrative Tools > Server Manager**.
3. Click **Continue** on the **User Account Control** dialog box.
4. Under **Security Summary**, click **Configure IE ESC**.
5. Under **Administrators**, select the **Off** option.
6. Under **Users**, select the **Off** option.
7. Click **OK**.



## Important Notes

This section lists information that you should consider before you use DCFM v10.3.3. See the *DCFM User Manual* for full details on the following notes. See the *DCFM Installation, Migration, and Transition Guide* for installation or migration procedures.

### ***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 10.3.3 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 that is bundled with the DCFM Server. It is recommended that the JRE not be 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 v5.2.1\_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 such as 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 file systems 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 that are not being used actively should be shut down. 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 10.3.3, 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 except DCFM 10.1.4, all the historical data will be truncated with respect to the default samples and the aging configuration will not be migrated to 10.3.3.

### ***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 authority 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 transactions 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 provides 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. Defect: 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 requires that the user manually assign SAN256M (Mi10k) to the EMC call home center. Defect: 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 load a smaller number of firmware files and support saves into the ftproot folder in DCFM. Defect 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 load a smaller number of firmware and data collection files in ftproot folder in EFCM. Defect: 259323 & 258791

### ***Firmware Repository 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. Defect: 256603

### ***Empty LAG creation***

If a dot1x enabled port is assigned to an LAG, an empty LAG will be created. [If a couple of ports combination of dot1x and dot1x disabled are added to an 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 an LAG. Defect: 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. Defect:261244

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

Sometimes, when the buttons in the FCIP Tunnel dialog (**Add Tunnel, Edit Tunnel, Disable Tunnel, Enable Tunnel**) are clicked, no operation takes place. It is recommended to Close and reopen the FCIP tunnel dialog to perform the same operations. Defect: 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, GbE 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. Defect: 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. Defect: 260445

### ***IFL connection shown in topology after deleting all the VE-VEX tunnels present between the SAN06B-R 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 select **Unmonitor** and then select **Monitor** the switch again. Defect: 259685

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

When the switch is converted to AG mode, both HBA and AG are displayed in the Fabric with same WWN. It is recommended to select **Unmonitor** and then **Monitor** the fabric so that the HBA is removed. Defect: 251379

### ***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 select **Unmonitor** and then **Monitor** the fabric. Defect: 257257

### ***AG to switch connection is not shown after the Fabric merge***

When the fabrics are merged, sometimes the AG to switch connection is not shown. It is recommended to select **Unmonitor** and then **Monitor** the fabric. Defect: 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. Defect: 253462

### **Quorum card options are enabled in mixed FOS Encryption Group**

When the Encryption group is created for one switch with FOS 6.3.0 and another switch with 6.2.0 or 6.1.1 encryption build in a same group, the Quorum card option and system card options are enabled in **Security** tab. It is recommended to have the same FOS 6.3.0 in an encryption group for the Quorum card and system card support. Defect: 259628

### **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 and the AG is connected to the switch, the F\_port trunk group icon is not shown in the product tree and the connection between the switch and AG is also not shown in the topology. It is recommended that F\_port trunking is disabled on the switch. Defect: 253201

### **Zoning dialog opening fails when attempting to open before the discovery completes**

When the user attempts to open the **Zoning** dialog before the discovery operation is complete, an error message, "Failed to load Zone DB" will be shown. It is recommended to open the zoning dialog after the discovery operation is completed. Defect:259665

### **SAN256M (MI10k) is not manageable in DCFM 10.3.x after migration when it is discovered using SNMPv3 with APluser in DCFM 10.0.x / 10.1.x**

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

### **DCFM Users who use SysLog Host Configuration for events**

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 port 514. Defect# 259950

### **Failover restriction in Mixed Fabric**

In case of Mixed Fabrics, only a 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, failover to EOS Seed Switch will not occur. Also, it is not possible to manually change the Seed Switch to EOS. To manage this fabric,

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

Failover can happen in the cases mentioned below

- a. FOS to FOS switches
- b. EOS to EOS switches
- c. EOS to FOS switches

### **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 display properly, Discover the new logical Fabric.

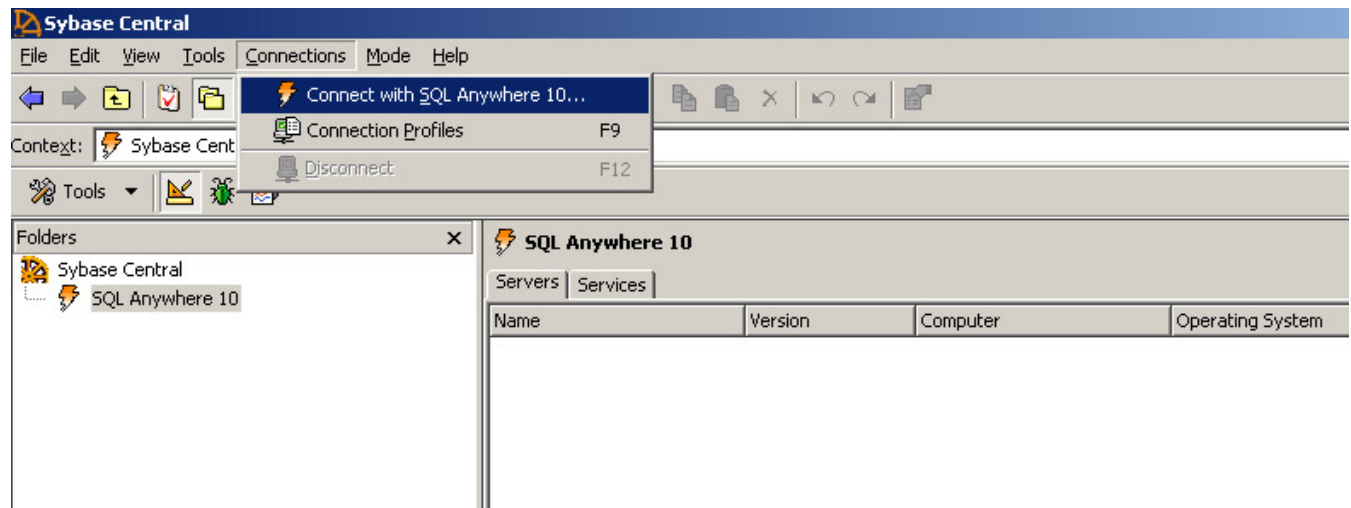
## Device Port update in topology View

In the case of a Non-VF environment, when the switches are discovered using SNMP V3, and if SSN (Soft Serial Number) is configured and if the EXT MIB is enabled, the device ports' status update would take 2 to 30 minutes (based on SAN size) to get updated in the GUI. In order to get updates within 1 to 3 minutes (based on SAN size) in these scenarios, disable EXT MIB.

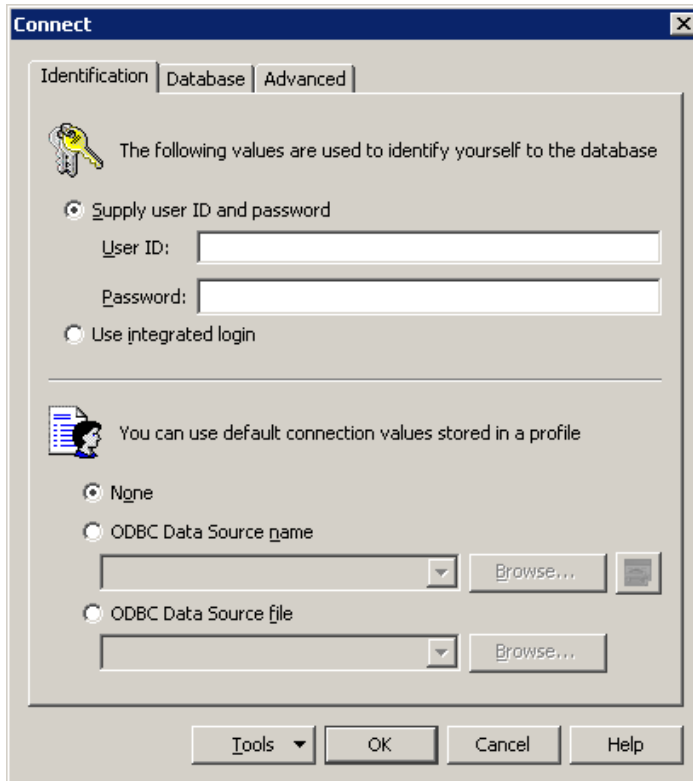
## Procedure to update FTP IP address in db when there is a change in the Server IP address

### Update the FTP SERVER table with the new IP Address

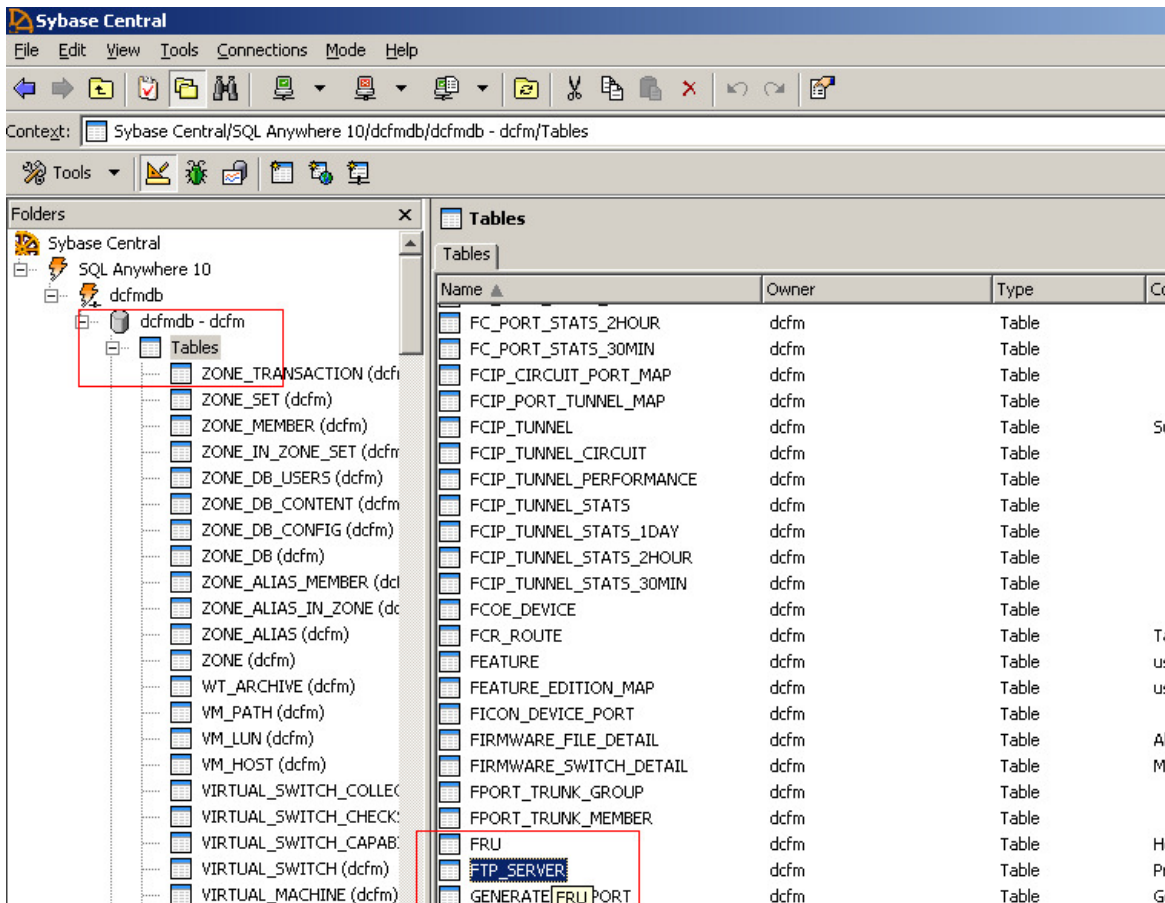
1. Go to <DCFM Home location>\db\Sybase Central 5.0.0\win32



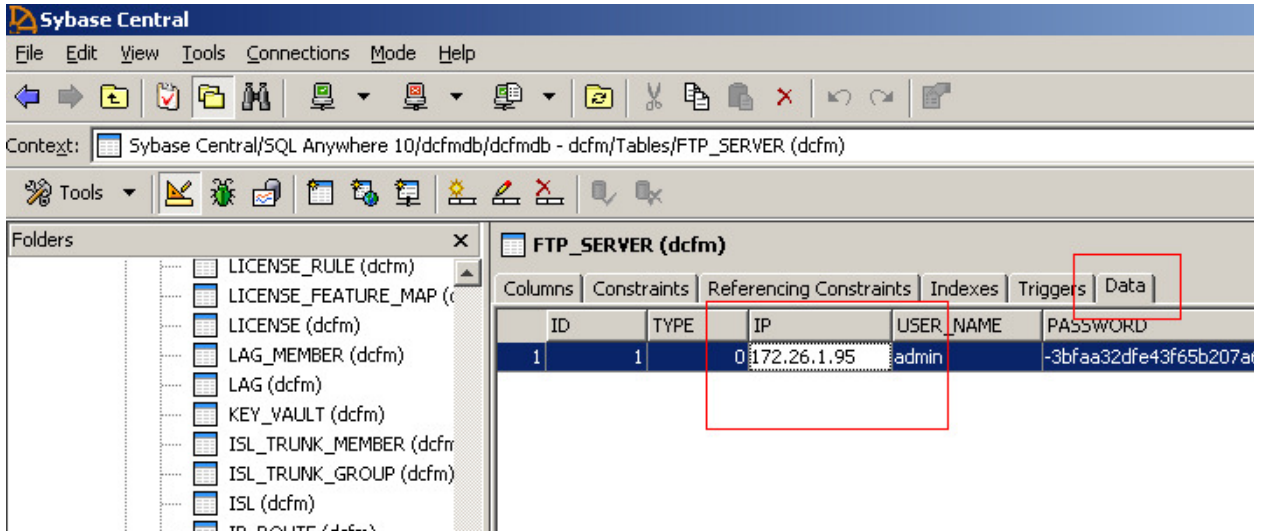
2. Launch the DB Application by clicking **scjview.exe**. Click on **Connections Menu > Connect with SQL Anywhere 10**.
3. Enter the username and password.



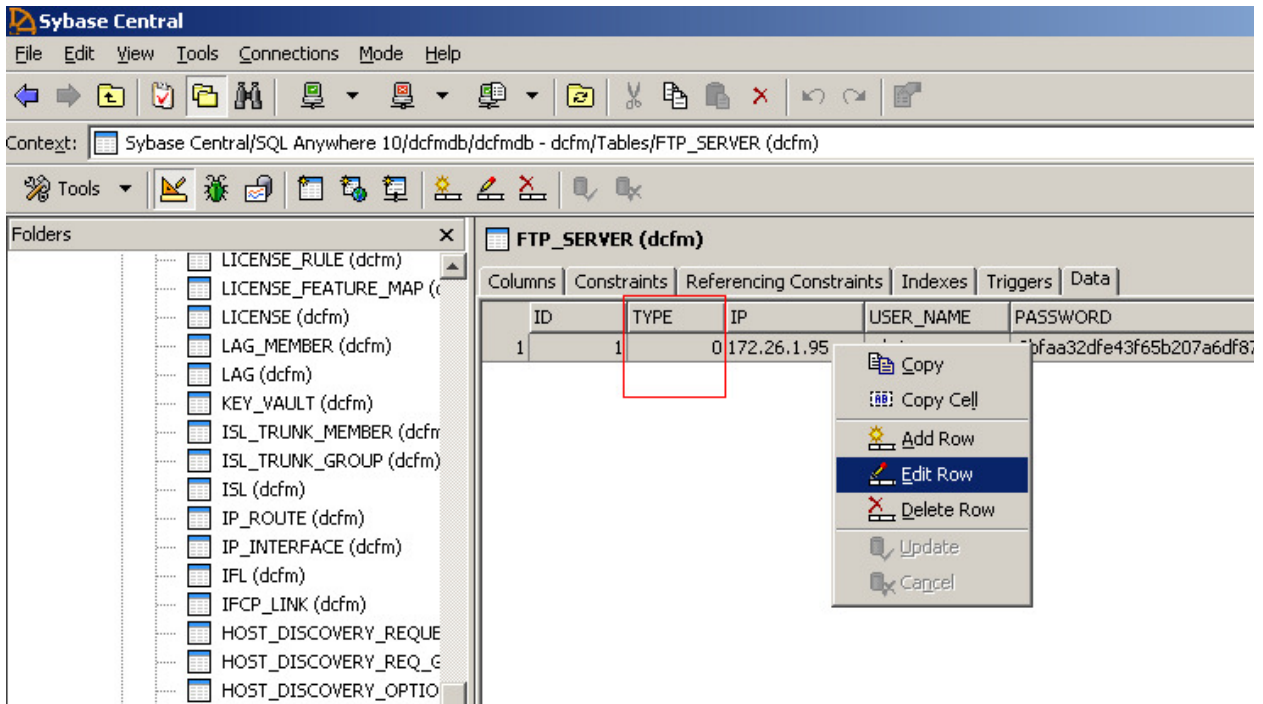
4. Click **Tables**, and then in the right pane, find and double click **FTP\_SERVER**.



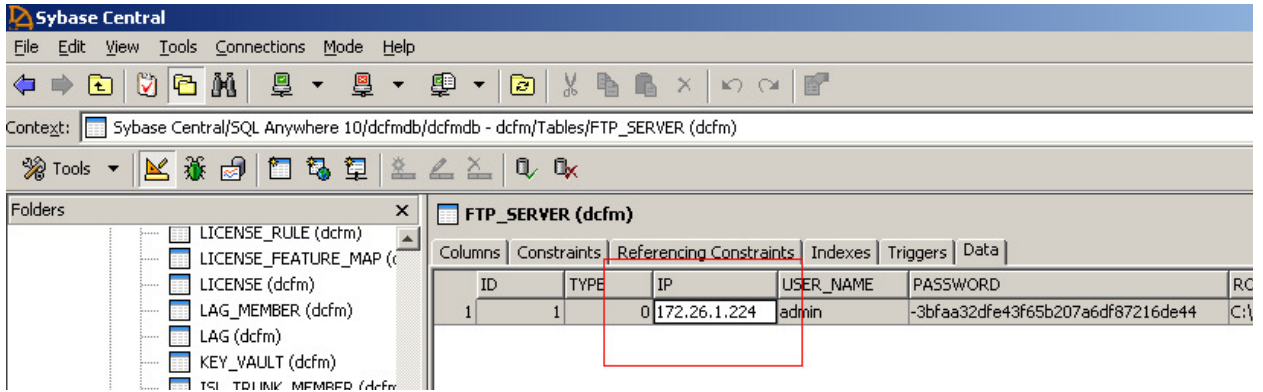
5. Click the **Data** tab



6. Right click on the record with Type=0 (i.e. Internal) and select **Edit Row**



7. Enter the new IP and click **Enter**. DO NOT modify any other column



8. Close the DB Connection and close the application

## 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 on the IBM SAN Support site: <http://www.ibm.com/systems/support/storage/san>

### DCFM Installation, Migration, and Transition Guide

On page 5, in the **System** requirements section, change SUSE Linux system requirements information as follows:

**TABLE 2** System Requirements

Operating System	Version	Installation Type	Small	Medium	Large
Linux®	AS5 ES4	Server plus 1 local client	Intel Core2 duo 2GHz or equivalent	Intel Dual CPU Core2 duo 2.4 GHz or equivalent	Intel Dual CPU Core2 duo 2.4 GHz or equivalent
		Remote client only	Intel Core2 duo 2GHz or equivalent	Intel Core2 duo 2GHz or equivalent	Intel Core2 duo 2GHz or equivalent

In the System Requirements section, For Solaris OS, the installation type

- 'Server' should be read as 'Server plus 1 local client'
- 'Client' should be read as 'Remote Client only'

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 CDefect:L + 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 10.3.3.

When migrating from Enterprise trial 10.0.X or 10.1.X, or previous 10.3.x versions to Enterprise trial or full edition 10.3.3 on Windows systems, use the following procedure:

**Migrating from Enterprise trial 10.0.X, 10.1.X, or previous 10.3.x versions to Enterprise trial or full edition 10.3.3 on Windows systems**

Use the following procedure to migrate from Enterprise Trial edition 10.0.X, 10.1.X, or previous 10.3.X software to Enterprise Trial or Full edition 10.3.3 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 10.3.3) 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 "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 that 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 , 10.1.X, or a previous version of 10.3.X to Enterprise trial or full edition **10.3.3** on UNIX systems, use the following procedure:

#### **Migrating from Enterprise trial 10.0.X, 10.1.X, or a previous 10.3.X version to Enterprise trial or full edition 10.3.3 on UNIX systems**

Use the following procedure to migrate from Enterprise Trial edition 10.0.X, 10.1.X , or a previous 10.3.X version software to Enterprise Trial or Full edition 10.3.3 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 an 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 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.
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**.

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:
      - a. `config.data-connection.active.local-address=<New_IP_Address>`
      - b. `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:
      - i. Windows systems:  
**dbisql.bat** <user\_name> <password>
      - ii. 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**, then 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:
      - a) config.data-connection.active.local-address=<New\_IP\_Address>
      - b) 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:
        - i. Windows systems:  
**dbisql.bat** <user\_name> <password>
        - ii. 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**, then 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:
  - 12) java.rmi.server.hostname=<New\_IP\_Address>
  - 13) 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 391 in the CEE configuration section, add the following procedure.

## **Minimum CEE configuration for FCoE traffic**

These are the procedures you must complete in order to create the basic configuration of CEE for FCoE traffic.

**Note:** The first two procedures in this section can be completed as a single procedure. They were divided into two separate procedures for clarity.

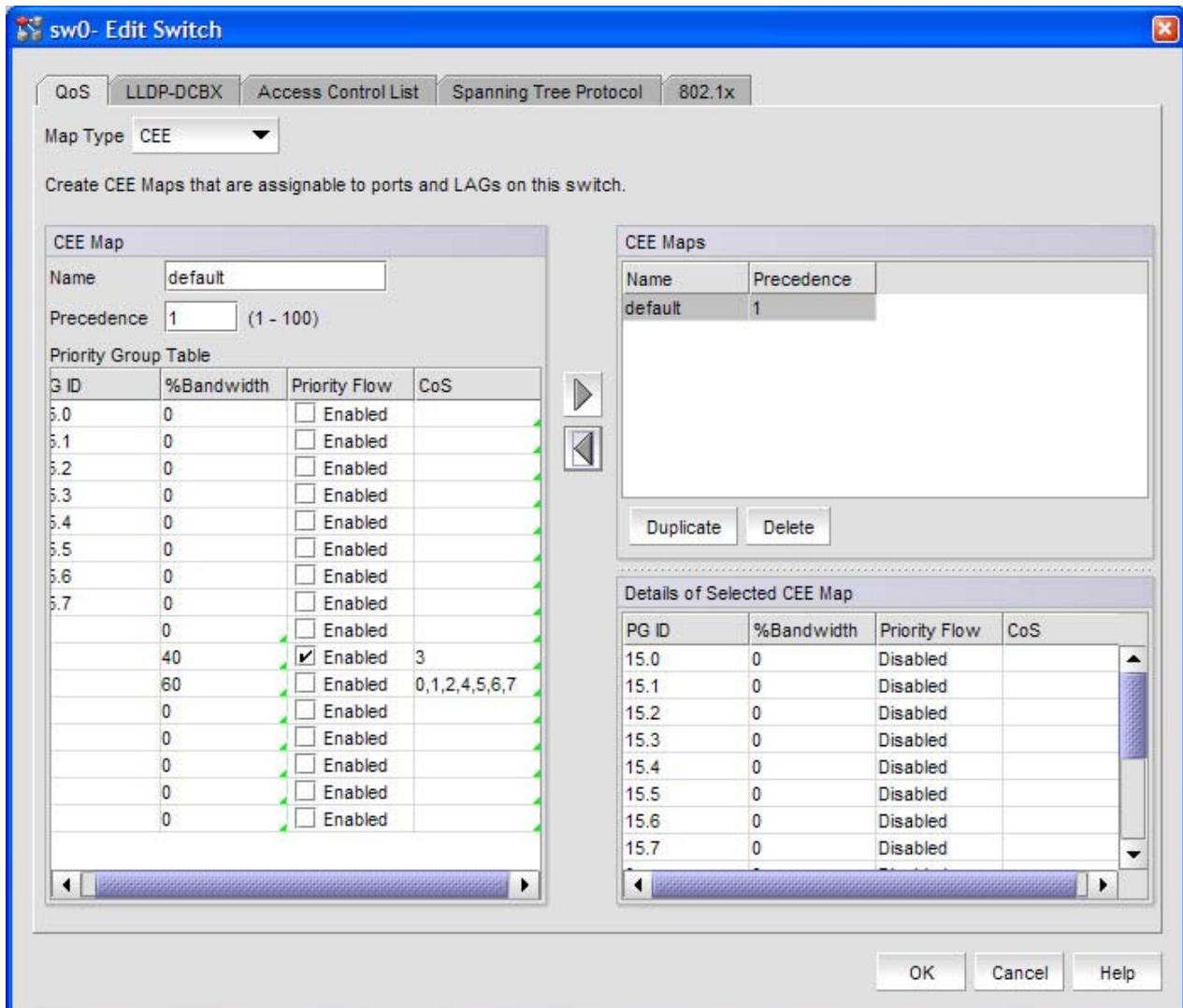
### ***Creating the CEE map to carry the LAN and SAN traffic***

Perform the following steps to create the CEE map:

1. Select **Configure > CEE Switch > CEE > CEE Configurations**. The **CEE Configuration** dialog displays.
2. Select your switch in the **CEE Configurations** tree table.
3. Click **Edit** to launch the **Edit Switch** dialog.
4. Select the **QOS** tab.



5. Create a new CEE Map to carry the traffic types as shown in the picture below.

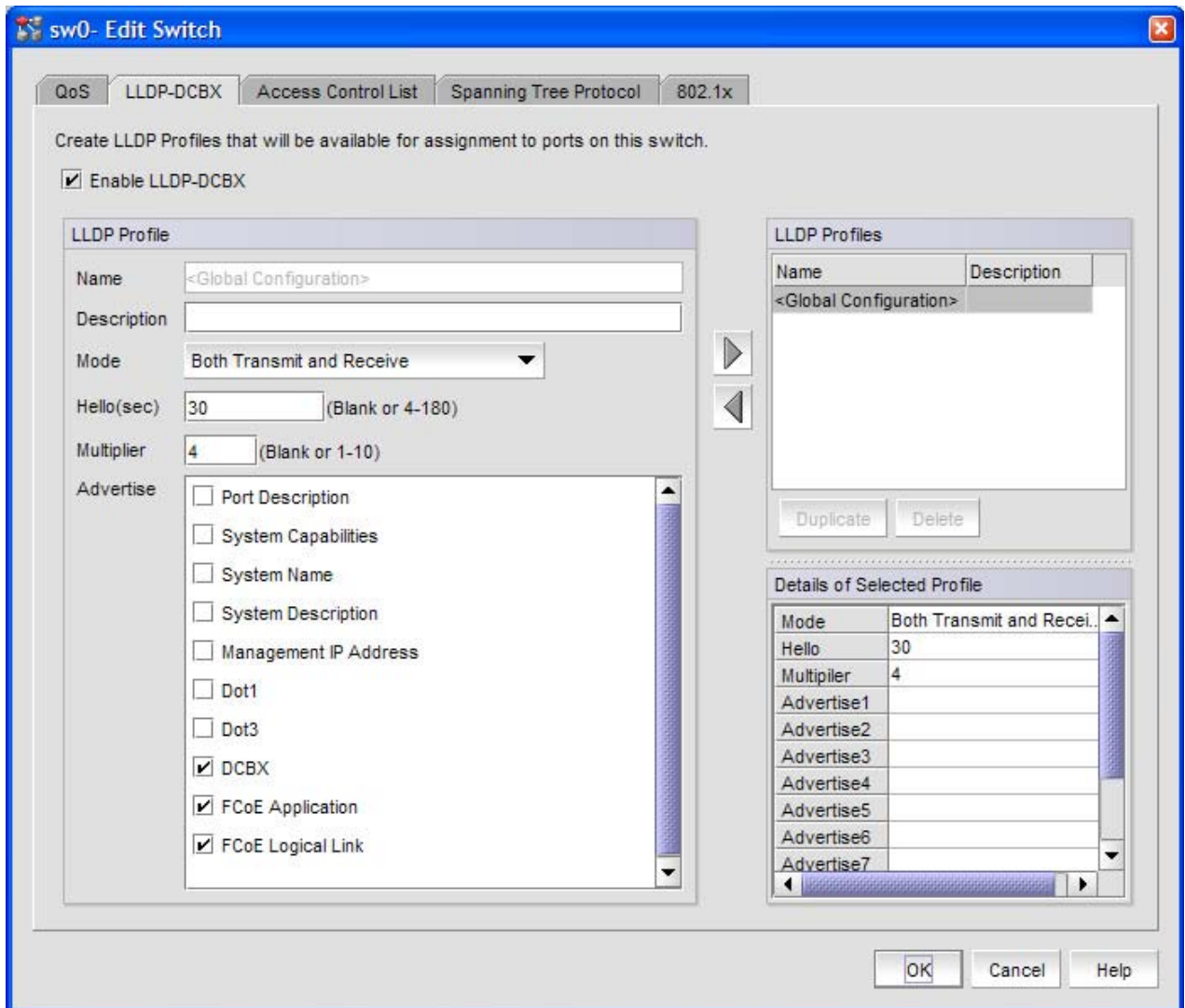


6. Click on the right arrow to save the CEE Map in the cache.
7. Click **OK**.
8. Click **Start** to save the changes to the switch.
9. Click **Close**.

### Configuring LLDP for FCoE

Perform these steps to configure LLDP for FCoE:

1. Select Configure > CEE Switch > CEE. The CEE Configuration dialog displays.
2. Select the switch in the CEE Configurations tree table.
3. Click Edit to launch the Edit Switch dialog.
4. Select the LLDP-DCBX tab.
5. Select the <Global Configuration> LLDP profile in the LLDP Profiles table.
6. Click on the left arrow button to edit.
7. Select the FCoE application and FCoE Logical Link TLVs to advertise them on the network.



8. Click **OK**.
9. Click **Start** to save the changes to the switch.
10. Click **Close**.

### **Configuring the CEE interface with the CEE Map and Global LLDP profile**

Perform these steps to configure the CEE interface:

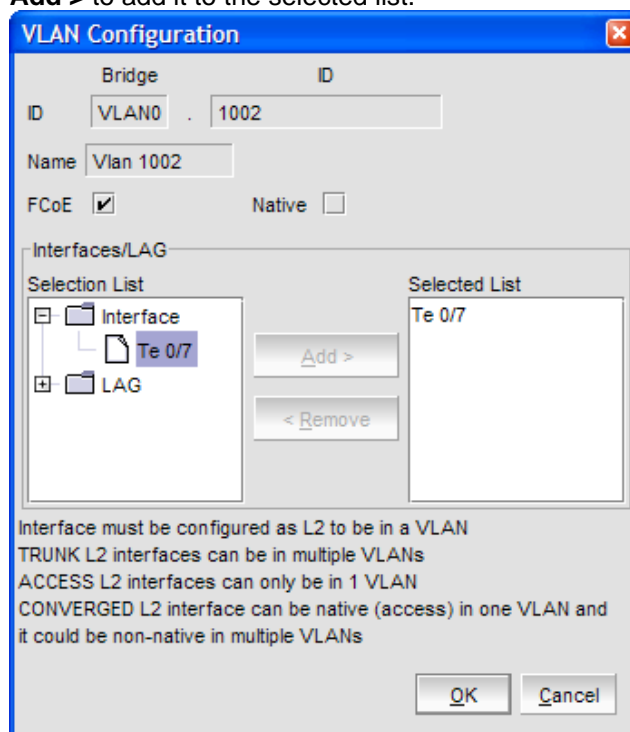
1. Select the Te port that is connected to the CNA in the CEE configuration tree table.
2. Click **Edit** to launch the **Edit port** dialog.
3. Select the **Port** tab and select the **Enable** option.
4. Select the **L2** option from the **Interface mode** list.
5. Select the **Converged** option for Brocade CNA, or the **Access** option for QLogic CNA in the **L2 Mode** list.
6. Select the **QOS** tab and select the **Assign a map to <port #>** option.
7. Select **Map Type > CEE**.
8. Open the **Available CEE Maps** list and select the CEE map 'default' created in Edit switch dialog above.
9. Select the **LLDP-DCBX** tab and select **Enable LLDP-DCBX on <port#>**.
10. Select the **Assign the Global Configuration** option.

11. Click **OK**. The **CEE Ports - Confirmation & Status** dialog displays.
12. Click **Start** to save the changes.

### **Create the FCoE VLAN to carry FCoE traffic**

Perform these steps to create the FCoE VLAN:

1. Select the FCoE switch in the Product Tree or Map.
2. Select **Configure > Element Manager > Admin**.
3. Select the **CEE** tab.
4. Select the **VLAN** tab.
5. Click **Add...** to launch the VLAN configuration dialog.
6. Enter the VLAN ID.
7. Click **OK**.
8. Select the VLAN you created and then click **Edit...** to convert it to an FCoE VLAN.
9. Select the **FCoE** option.
10. Select the **CEE** interface to carry the FCoE traffic from the **Selection List** tree and then click **Add >** to add it to the selected list.



11. Click **OK** to save your changes.
12. Close the Element Manager.

### **Creating VLAN classifiers and activating on the CEE interface**

**Note:** These steps are performed using the CLI

Perform these steps to create and activate the VLAN classifiers on the CEE interface:

1. Login to the switch and enter global configuration mode.  
**Example**  
switch:<userid>>cmsh  
switch#configure terminal
2. Create and apply VLAN Classifiers to the CEE interface to classify Ethernet frames on an untagged interface to VLAN.

**Example**

```
switch(config)#vlan classifier rule 1 proto fip encap ethv2
switch(config)#vlan classifier rule 2 proto fcoe encap ethv2
switch(config)#vlan classifier group 1 add rule 1
switch(config)#vlan classifier group 1 add rule 2
```

3. Apply the VLAN classifier Group to the CEE interface:

**Example of activating VLAN classifier on the interface Te 0/7**

```
switch(conf-if-te-0/7)#vlan classifier activate group 1 vlan 1002
```

4. Save running-config file to the startup-config file:

**Example**

```
switch#copy running-config startup-config
```

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. <b>Windows operating systems</b> <ol style="list-style-type: none"> <li>1. Log in using the 'Administrator' privilege.</li> <li>2. Select <b>Start &gt; Run</b>.</li> <li>3. Type <b>drivers</b> in the <b>Open</b> field and press <b>Enter</b>.</li> <li>4. Go to the 'etc' folder and open the 'hosts' file using a text editor.</li> <li>5. Add the IP address and host name of the client and server in the following format: &lt;IP_address&gt; &lt;Host_name&gt;.</li> </ol> For example: <pre>102.54.94.97 rhino.acme.com # source server 38.25.63.10 x.acme.com # x client host</pre> <ol style="list-style-type: none"> <li>6. Save and exit the file.</li> </ol> <b>Linux/Solaris operating systems</b> <ol style="list-style-type: none"> <li>1. Log in using the 'root' privilege.</li> <li>2. Open the '/etc/hosts' file using a text editor.</li> <li>3. Add the IP address and host name of the client and server in the following format: &lt;IP_address&gt; &lt;Host_name&gt;.</li> </ol> For example: <pre>102.54.94.97 rhino.acme.com # source server 38.25.63.10 x.acme.com # x client host</pre> <ol style="list-style-type: none"> <li>4. Save and exit the file.</li> </ol>

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
<p>Unable to launch the SMC on a Windows Vista system.</p>	<p>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:</p> <p>The following are the various ways we can disable UAC in vista:</p> <ul style="list-style-type: none"> <li>• Disable using msconfig by completing the following steps. <ol style="list-style-type: none"> <li>1. Select <b>Start &gt; Run</b>.</li> <li>2. Type msconfig on the <b>Run</b> dialog box and click <b>OK</b>.</li> <li>3. Click the <b>Tools</b> tab on the <b>System Configuration Utility</b>.</li> <li>4. Scroll down to and select the <b>Disable UAC</b> tool name.</li> <li>5. Click <b>Launch</b>.</li> </ol> <p>A command window displays and runs the disable UAC command. When the command is complete, close the window.</p> <ol style="list-style-type: none"> <li>6. Close the System Configuration Utility.</li> <li>7. Restart the computer to apply changes.</li> </ol> <p><b>Note:</b> You can re-enable UAC using the above procedure and selecting the <b>Enable UAC</b> tool name in step 4.</p> </li> <li>• Disable using regedit by completing the following steps. <p><b>Note:</b> 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.</p> <ol style="list-style-type: none"> <li>1. Select <b>Start &gt; Run</b>.</li> <li>2. Type regedit on the <b>Run</b> dialog box and click <b>OK</b>.</li> <li>3. Navigate to the following registry key:  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System</li> <li>4. Right-click the <b>EnableLUA</b> value and select <b>Modify</b>.</li> <li>5. Change the <b>Value data</b> field to 0 on the <b>Edit DWORD Value</b> dialog box and click <b>OK</b>.</li> <li>6. Close the Registry Editor.</li> <li>7. Restart the computer to apply changes.</li> </ol> <p><b>Note:</b> You can re-enable UAC using the above procedure and changing the <b>Value data</b> field to 1 in step 5.</p> </li> <li>• Disable using the Group Policy by completing the following steps. <p>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.</p> <p>To disable using the Local Group Policy editor, complete the following steps.</p> <ol style="list-style-type: none"> <li>1. On your local Vista computer, select <b>Start &gt; Run</b>.</li> <li>2. Type gpedit.msc on the <b>Run</b> dialog box and click <b>OK</b>.</li> </ol> </li> </ul>

Problem	Resolution
	<ol style="list-style-type: none"> <li>3. Browse to <b>Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Local Policies &gt; Security Options</b> in the Group Policy editor.</li> <li>4. In the right pane scroll to the User Access Control policies (at the bottom of the pane).</li> <li>5. Right-click the <b>Behavior of the elevation prompt for Administrators in Admin Approval Mode</b> policy and select <b>Properties</b>.</li> <li>6. Select the <b>No Prompt</b> option and click <b>OK</b>.</li> <li>7. Right-click the <b>Detect application installations and prompt for elevation</b> policy and select <b>Properties</b>.</li> <li>8. Select the <b>Disabled</b> option and click <b>OK</b>.</li> <li>9. Right-click the <b>Run all administrators in Admin Approval Mode</b> policy and select <b>Properties</b>.</li> <li>10. Select the <b>Disabled</b> option and click <b>OK</b>.</li> <li>11. Close the Group Policy editor.</li> <li>12. Restart the computer to apply changes.</li> </ol> <p>To disable using the Active Directory-based GPO editor, complete the following steps.</p> <ol style="list-style-type: none"> <li>1. On a Vista computer that is a member of a domain, select <b>Start &gt; Run</b>.</li> <li>2. Type gpedit.msc on the <b>Run</b> dialog box and click <b>OK</b>.</li> <li>3. Browse to the required GPO that is linked to the OU or domain where the Vista computers are located, then edit it</li> <li>4. Browse to <b>Computer Configuration &gt; Windows Settings &gt; Security Settings &gt; Local Policies &gt; Security Options</b> in the Group Policy editor.</li> <li>5. In the right pane scroll to the User Access Control policies (at the bottom of the pane).</li> <li>6. Right-click the <b>Behavior of the elevation prompt for Administrators in Admin Approval Mode</b> policy and select <b>Properties</b>.</li> <li>7. Select the <b>No Prompt</b> option and click <b>OK</b>.</li> <li>8. Right-click the <b>Detect application installations and prompt for elevation</b> policy and select <b>Properties</b>.</li> <li>9. Select the <b>Disabled</b> option and click <b>OK</b>.</li> <li>10. Right-click the <b>Run all administrators in Admin Approval Mode</b> policy and select <b>Properties</b>.</li> <li>11. Select the <b>Disabled</b> option and click <b>OK</b>.</li> <li>12. Close the Group Policy editor.</li> <li>13. Restart the computer to apply changes.</li> </ol>

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 <b>Configuration Management</b> dialog box and perform configuration upload and replication.	Disables <b>Save</b> , <b>Restore</b> , <b>Configuration Repository</b> , and <b>Schedule Backup</b> under <b>Configure &gt; FC Switch</b> and the <b>Configuration</b> command under <b>Configure &gt; FC Switch &gt; Replicate</b> .	Enables <b>Configuration Repository</b> under <b>Configure &gt; FC Switch</b> . Only viewing of saved configuration is supported. Configuration upload and replication are disabled.	Enables all commands under <b>Configure &gt; FC Switch</b> . 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 <b>SupportSave</b> , <b>Upload Failure Data Capture</b> , and <b>View Repository</b> commands from the <b>Monitor &gt; Technical Support</b> menu and right-click menu.	Enables the <b>View Repository</b> command from the <b>Monitor &gt; Technical Support</b> menu and right-click menu. Disables the <b>SupportSave</b> and <b>Upload Failure Data Capture</b> commands from the <b>Monitor &gt; Technical Support</b> menu and right-click menu.	Enables the <b>SupportSave</b> , <b>Upload Failure Data Capture</b> , and <b>View Repository</b> commands from the <b>Monitor &gt; Technical Support</b> 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
<b>Target Port</b> 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
<b>Maximum Historical Event</b> 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
<b>Switch One Settings</b> <b>Switch Two Settings</b>	Settings for the switches on either end of the tunnel are configured and displayed under these two headings.
<b>Select Switch Two</b> button	Click to display the <b>Select Switch</b> dialog box. To create an FCIP tunnel, you must configure a switch on either end of the tunnel.
<b>Switch</b>	The name of the switch.
<b>Fabric</b>	The fabric that contains the switch.
<b>Tunnel</b>	A numeric ID assigned to the tunnel. Note that a tunnel ID cannot be applied until after a circuit is defined.
<b>Description</b>	A description of the tunnel.
<b>Port Type</b>	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.
<b>Edit Circuit</b> button	Click to display the <b>Edit Circuit</b> dialog box. At least one circuit must be created and added to implement an FCIP tunnel.
<b>Advanced Settings</b> 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 10.3.3

This section lists the defects with High and Medium Technical Severity closed with a code change in DCFM 10.3.3.

<b>Defect ID:</b> DEFECT000265815	<b>Technical Severity:</b> High
<b>Summary:</b> Unable to launch Web Tools from DCFM	
<b>Symptom:</b> When trying to launch Web Tools pages from within DCFM, the operation fails with errors.	
<b>Feature:</b> Client	<b>Function:</b> Client
<b>Probability:</b> Medium	
<b>Found in Release:</b> DCFM10.3.0	<b>Service Request ID:</b> 404189

<b>Defect ID:</b> DEFECT000267386	<b>Technical Severity:</b> High
<b>Summary:</b> Configuration changes made to the FCIP tunnel cannot be saved.	
<b>Symptom:</b> Edit FCIP tunnel' dialog is not dismissed when OK button is selected after making changes in the Advanced Settings and hence configuration changes are not saved.	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> Medium	
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> DEFECT000268762	<b>Technical Severity:</b> High
<b>Summary:</b> Management application services stopped due to a memory leak.	
<b>Symptom:</b> Management application services - Web Server, Built In FTP and main server stopped due to memory leak.	
<b>Feature:</b> MISC	<b>Function:</b> USABILITY
<b>Probability:</b> High	
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> DEFECT000268928	<b>Technical Severity:</b> High
<b>Summary:</b> An encryption switch in an EG configured with KV1 initially but later changed to KV2 yet 'Management application still shows KV1 as the key vault	
<b>Symptom:</b> When a new key vault is registered for the Encryption group, the change is not reflected in Management application	
<b>Feature:</b> Encryption	<b>Function:</b> CONFIGURATION
<b>Probability:</b> High	
<b>Found in Release:</b> DCFM10.3.2	

<b>Defect ID:</b> DEFECT000268929	<b>Technical Severity:</b> High
<b>Summary:</b> Management application service that processes the SNMP traps was stuck.	
<b>Symptom:</b> 'Management application service that processes the SNMP traps got stuck, resulting in collectors not getting triggered.	
<b>Feature:</b> FAULT MANAGEMENT	<b>Function:</b> NONE
<b>Probability:</b> High	
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> DEFECT000268996	<b>Technical Severity:</b> High
<b>Summary:</b> Null Pointer Exception is thrown in Server Console when Fusion is connected to DCFM10.3.2.	
<b>Symptom:</b> User will not be able to fetch the Fabric details when Fusion 2.7 is connected with DCFM 10.3.2	
<b>Feature:</b> Client/Server Communication	<b>Function:</b> Client/Server Communication
<b>Probability:</b> High	
<b>Found in Release:</b> DCFM10.3.2	

<b>Defect ID:</b> DEFECT000265426	<b>Technical Severity:</b> Medium
<b>Summary:</b> PDCM – Copied Configuration is not listed in the Product/port tree but successfully saved in the switch.	
<b>Symptom:</b> Sometimes Product Tree will not be updated immediately after the configuration is copied.	
<b>Workaround:</b> Close the Configure Allow / Prohibit matrix and open it again.	
<b>Feature:</b> PDCM	<b>Function:</b> USABILITY
<b>Probability:</b> Low	
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> DEFECT000265573	<b>Technical Severity:</b> Medium
<b>Summary:</b> When a logical switch is edited through DCFM, the GUI takes a long time to update.	
<b>Symptom:</b> When moving ports from the default switch to the logical switch or vice-versa, DCFM takes a long period to reflect these changes in the GUI and this time period varies from 5 minutes to over 40 minutes.	
<b>Feature:</b> Virtual Fabrics	<b>Function:</b> USABILITY
<b>Probability:</b> Medium	
<b>Found in Release:</b> DCFM10.3.0	<b>Service Request ID:</b> 403185

<b>Defect ID:</b> DEFECT000267539	<b>Technical Severity:</b> Medium
<b>Summary:</b> FCIP: Wrong GbE port format has been mentioned in the “Delete Progress” dialog, when we delete the tunnel.	
<b>Symptom:</b> When we delete the tunnel, wrong GbE port format has been mentioned in the “Delete Progress” dialog. That is for the IBM Converged Switch B32 (Brocade 7800) [slot/port] format shown, for the FR4-18i and FX8-18; the wrong slot number is displayed.	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> Medium	
<b>Found in Release:</b> DCFM10.3.2	

<b>Defect ID:</b> DEFECT000268766	<b>Technical Severity:</b> Medium
<b>Summary:</b> 'Logical Switches' dialog displays unmonitored chassis.	
<b>Symptom:</b> After unmonitoring a VF enabled chassis, the still name appears in configure 'Logical Switches' dialog.	
<b>Feature:</b> Virtual Fabrics	<b>Function:</b> USABILITY
<b>Probability:</b> high	
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> DEFECT000269137	<b>Technical Severity:</b> Medium
<b>Summary:</b> Default sort column is incorrect for configure/CEE dialog.	
<b>Symptom:</b> The first time the user opens the Configure/CEE dialog, the display sorts the MAC Address column instead of Port number column.	
<b>Feature:</b> FCoE/CEE Management	<b>Function:</b> CEE Switch/Port Properties Dialog
<b>Probability:</b> high	
<b>Found in Release:</b> DCFM10.3.2	

## 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.

<b>Defect ID:</b> Defect:000264747	<b>Technical Severity:</b> High
<b>Summary:</b> Incorrect 'Source Name' for master log from virtual fabric enabled switches.	
<b>Symptom:</b> Master Log is showing incorrect Source Name for VF Switches	
<b>Feature:</b> FAULT MANAGEMENT	<b>Function:</b> NONE
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000264890	<b>Technical Severity:</b> High
<b>Summary:</b> Performance Management – Rx/Tx % Utilization is plotted incorrectly for xGE ports in Real Time Graph.	
<b>Symptom:</b> Graph will not reflect the actual data flowing.	
<b>Feature:</b> Performance Management	<b>Function:</b> RealTime Graph
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000264985	<b>Technical Severity:</b> High
<b>Summary:</b> Firmware upgrade via the Element Manager on a SAN32M-2 (M4700) never completes (according to the send firmware dialog box).	
<b>Symptom:</b> Element Manager will show that the firmware upgrade never completes, but actually the upgrade is success in the switch	
<b>Feature:</b> M-EOS Element Manager	<b>Function:</b> USABILITY
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265031	<b>Technical Severity:</b> High
<b>Summary:</b> 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	
<b>Symptom:</b> Activated zone is not shown in the Active Zone Configuration after the Zone Activation	
<b>Workaround:</b> Wait until the Zone collection completes	
<b>Feature:</b> ZONING	<b>Function:</b> Online Zoning
<b>Probability:</b> High	<b>Risk of Fix:</b> High
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265033	<b>Technical Severity:</b> High
<b>Summary:</b> Zoning: When activating a new zone config, DCFM shows the old zone config as active	
<b>Symptom:</b> Active Zone Configuration tab is listing the old Active Zone when a New Config is activated	
<b>Workaround:</b> Wait until the Zone collection completes	
<b>Feature:</b> ZONING	<b>Function:</b> Online Zoning
<b>Probability:</b> High	<b>Risk of Fix:</b> High
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265293	<b>Technical Severity:</b> High
<b>Summary:</b> Zoning: The Redirection zones present in the zone Database vanishes when zoning activation done from DCFM	
<b>Symptom:</b> The Frame Redirection zones present in the Zone Database wiped out when zone activation is done.	
<b>Feature:</b> ZONING	<b>Function:</b> Online Zoning
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265451	<b>Technical Severity:</b> High
<b>Summary:</b> Webtool can not be launched from DCFM 10.3.1 with JRE 6u14 & above but DCFM webstart works fine.	
<b>Symptom:</b> User will not be able to launch Webtool proxy through DCFM if the JRE version is 1.6 update 14 and above.	
<b>Feature:</b> Proxy services	<b>Function:</b> Proxy services
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265487	<b>Technical Severity:</b> High
<b>Summary:</b> Except Services and Ports tabs, remaining tabs are not displayed under Server Management Console on migrating from FM to DCFM	
<b>Symptom:</b> Unable to see other tabs apart from services and ports.Operations like technical support information,changing Authentications are not possible.	
<b>Feature:</b> FM Migration	<b>Function:</b> USABILITY
<b>Probability:</b> High	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000257703	<b>Technical Severity:</b> Medium
<b>Summary:</b> FCIP: Duplicate circuits have been shown in the 'Circuits tab' of 'FCIP Tunnels' dialog when we create multiple circuits for the same tunnel.	
<b>Symptom:</b> Duplicate circuits have been shown in the 'Circuits tab' of 'FCIP Tunnels' dialog when we create multiple circuits for the same tunnel.	
<b>Workaround:</b> Close and reopen the 'FCIP Tunnels' dialog and observe that now multiple circuits will not be shown to the user.	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000260396	<b>Technical Severity:</b> Medium
<b>Summary:</b> FCIP: “Failed to add IP interface, error: Configuration entry exists on a GigE port” error shown while clicking the “ <b>Current Maximum Bandwidth</b> ” button in the ‘ <b>Edit Circuit</b> ’ dialog	
<b>Symptom:</b> When the user clicks the “ <b>Current Maximum Bandwidth</b> ” button in the <b>Edit Circuit</b> 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	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000262591	<b>Technical Severity:</b> Medium
<b>Summary:</b> FCIP: After creating a new tunnel, tunnel has not been shown at the “Switch-2” side. It has been shown only after relaunching the “ <b>FCIP Tunnel</b> ” dialog.	
<b>Symptom:</b> New tunnels are not shown in FCIP dialog immediately	
<b>Workaround:</b> Re-launch the <b>FCIP Tunnel</b> dialog	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000262947	<b>Technical Severity:</b> Medium
<b>Summary:</b> Not able to manage the switch in server A although the fabric is unmonitored in server B	
<b>Symptom:</b> User will not be able to manage the switch	
<b>Feature:</b> DISCOVERY	<b>Function:</b> Switch Discovery
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000263892	<b>Technical Severity:</b> Medium
<b>Summary:</b> SupportSave:No Support data are collected even after 35 minutes and empty zip folders were only created	
<b>Symptom:</b> User was not able to collect the Support Data for the switch	
<b>Workaround:</b> Restart the Server	
<b>Feature:</b> Technical Support	<b>Function:</b> Support Save
<b>Probability:</b> Medium	<b>Risk of Fix:</b> High
<b>Found in Release:</b> DCFM10.1.4	

<b>Defect ID:</b> Defect:000264806	<b>Technical Severity:</b> Medium
<b>Summary:</b> 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	
<b>Symptom:</b> User will get inappropriate error message when domain ID greater than 31 is part of the Zone Database	
<b>Workaround:</b> User should not add members with Domain ID greater than 31 in Interopmode 2	
<b>Feature:</b> ZONING	<b>Function:</b> Zoning Dialog
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000264930	<b>Technical Severity:</b> Medium
<b>Summary:</b> In the Help content of 'Add FCIP Tunnel' dialog, information about 'Select Switch Two' button is missing	
<b>Symptom:</b> "Select Switch Two" button information is missing in the Online Help	
<b>Feature:</b> FCIP	<b>Function:</b> HELP
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265102	<b>Technical Severity:</b> Medium
<b>Summary:</b> Auto enclosure is not created in the Fabric view after discovering Host and wrong fabric WWN is shown in the Host view.	
<b>Symptom:</b> Auto enclosure is not seen in the fabric view though the Host connected to the fabric is discovered.	
<b>Feature:</b> HBA Management	<b>Function:</b> Desktop Changes
<b>Probability:</b> Medium	<b>Risk of Fix:</b> High
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265113	<b>Technical Severity:</b> Medium
<b>Summary:</b> Zoning:Error message is displayed and report is not generated while activating zone for a pure EOS fabric with report generation enabled	
<b>Symptom:</b> Report is not generated and error is displayed even after successful activation of zone	
<b>Feature:</b> ZONING	<b>Function:</b> Zoning Dialog
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265114	<b>Technical Severity:</b> Medium
<b>Summary:</b> Fault Management : Master log event count is incremented with the old source name even when the switch name is changed.	
<b>Symptom:</b> Master Log Event is triggered with old Source Name when the Switch Name is updated	
<b>Feature:</b> FAULT MANAGEMENT	<b>Function:</b> USABILITY
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265223	<b>Technical Severity:</b> Medium
<b>Summary:</b> Renaming a host reflects only after client re-launch.	
<b>Symptom:</b> User will not be able to see the edited host name unless he re-launches the client.	
<b>Workaround:</b> Restart the client	
<b>Feature:</b> HBA Management	<b>Function:</b> Desktop Changes
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	



<b>Defect ID:</b> Defect:000265230	<b>Technical Severity:</b> Medium
<b>Summary:</b> FCIP: When we edit the tunnel present between, SAN18B-R and SAN04B-R in the 'Advanced settings' window, the <b>Transmission</b> tab is enabled. It gets disabled only when we move to other tabs.	
<b>Symptom:</b> In the 'Advanced settings' window, the <b>Transmission</b> 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.	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265318	<b>Technical Severity:</b> Medium
<b>Summary:</b> 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.	
<b>Symptom:</b> 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.	
<b>Workaround:</b> Add the double side tunnel between "Two SAN768B [FR4-18i] or Two SAN256B[FR4-18i],". We will be able to configure the tunnel.	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265376	<b>Technical Severity:</b> Medium
<b>Summary:</b> Zoning:An alert message is shown in the zoning dialog when the TI zone modification is done before activation	
<b>Symptom:</b> alert message is shown in zoning dialog though there is no changes in zone configuration	
<b>Feature:</b> ZONING	<b>Function:</b> Zoning Dialog
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.1	

<b>Defect ID:</b> Defect:000265407	<b>Technical Severity:</b> Medium
<b>Summary:</b> After creating a third circuit, Horizontal scroll bar not shown in the "Circuit tab" of "FCIP tunnel" dialog.	
<b>Symptom:</b> 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.	
<b>Workaround:</b> Close and open the <b>FCIP tunnel</b> dialog. Horizontal scroll bar will be shown	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> 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.

<b>Defect ID:</b> Defect:000255806	<b>Technical Severity:</b> High
<b>Summary:</b> LSAN Zoning; Activated LSAN zone is not shown in the LSAN zoning dialog after reopening the dialog	
<b>Symptom:</b> LSAN zoning dialog is not showing the activated LSAN zone	
<b>Workaround:</b> Wait for 15 to 30 minutes	
<b>Feature:</b> FAULT MANAGEMENT	<b>Function:</b> NONE
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000256212	<b>Technical Severity:</b> High
<b>Summary:</b> PAD: Unable to unblock a automatically disabled port from PAD dialog	
<b>Symptom:</b> Not able to unblock a automatically disabled port.	
<b>Workaround:</b> Use CLI to unblock the port	
<b>Feature:</b> Port Auto Disable	<b>Function:</b> ENHANCEMENT
<b>Probability:</b> High	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000256371	<b>Technical Severity:</b> High
<b>Summary:</b> FCIP: Duplicate tunnels are shown in the <b>FCIP tunnel</b> dialog. After creating 4 tunnels , 4 more duplicate tunnels are shown, so unable to create 5th tunnel.	
<b>Symptom:</b> User will not be able to create more than 4 tunnels	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> High	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000256896	<b>Technical Severity:</b> High
<b>Summary:</b> Tunnel links are not being displayed in topology.	
<b>Symptom:</b> Switches in the Fabric are shown isolated without any link between them and also the user will not have the option to launch the <b>Connection properties</b> dialog.	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> High	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000258864	<b>Technical Severity:</b> High
<b>Summary:</b> Scalability: Client logs out observed in the Scalability server	
<b>Symptom:</b> client log out will be observed	
<b>Feature:</b> Client/Server Communication	<b>Function:</b> Client/Server Communication
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000258914	<b>Technical Severity:</b> High
<b>Summary:</b> Client lost connection to server on Linux server overnight. Local client	
<b>Symptom:</b> Client connectivity lost, need to re-login.	
<b>Feature:</b> Client/Server Communication	<b>Function:</b> Client/Server Communication
<b>Probability:</b> Medium	<b>Risk of Fix:</b> High
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000260437	<b>Technical Severity:</b> High
<b>Summary:</b> Host and storage connected to a fabric are shown isolated in the Host view when Host is rediscovered because of HCM agent connection failure	
<b>Symptom:</b> In the Host View, isolated HBA and the storage nodes are shown without any connections.	
<b>Workaround:</b> - Delete the newly discovered host - Monitor the old fabric - Delete and rediscover the host	
<b>Feature:</b> HBA Management	<b>Function:</b> Discovery (FC HBA & CNA)
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000260866	<b>Technical Severity:</b> High
<b>Summary:</b> Duplicate virtual NPIV ports are shown in device tree for m-type switch after migrating from EFCM to DCFM	
<b>Symptom:</b> Duplicate virtual NPIV ports are shown for m-type switch	
<b>Feature:</b> Client	<b>Function:</b> TOPOLOGY
<b>Probability:</b> High	<b>Risk of Fix:</b> High
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261742	<b>Technical Severity:</b> High
<b>Summary:</b> DCFM reading CNA HCM Name into the DCFM Names database	
<b>Symptom:</b> Cannot use DCFM to set/change a CNA node or port name, must use HCM	
<b>Feature:</b> HBA Management	<b>Function:</b> Discovery (FC HBA & CNA)
<b>Probability:</b> High	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000262867	<b>Technical Severity:</b> High
<b>Summary:</b> SNMPv3 SHA authentication used in switch discovery fails	
<b>Symptom:</b> Switch cannot be discovered with SNMPv3 SHA	
<b>Feature:</b> DISCOVERY	<b>Function:</b> Switch Discovery
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000235540	<b>Technical Severity:</b> Medium
<b>Summary:</b> The "vendor E-mail" option is not necessary and having both the "vendor" and "vendor E-mail" options available will only create confusion.	
<b>Symptom:</b> The "EMC E-mail" option is not necessary and having both the "vendor" and "vendor E-mail" options available will only create confusion.	
<b>Feature:</b> other Dialog	<b>Function:</b> USABILITY
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.0.2	<b>Service Request ID:</b> 352329

<b>Defect ID:</b> Defect:000241637	<b>Technical Severity:</b> Medium
<b>Summary:</b> Zone details missing in zone compare.	
<b>Symptom:</b> 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?	
<b>Feature:</b> ZONING	<b>Function:</b> USABILITY
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.1.1	

<b>Defect ID:</b> Defect:000241638	<b>Technical Severity:</b> Medium
<b>Summary:</b> Zones Not Shown Correctly After Import	
<b>Symptom:</b> Zones not shown correctly after import. The names by adding the prefix "old_" so the zones no longer exist in the DB	
<b>Feature:</b> ZONING	<b>Function:</b> Zoning Dialog
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.1.1	

<b>Defect ID:</b> Defect:000243353	<b>Technical Severity:</b> Medium
<b>Summary:</b> There are some issues found while configuring an end-to-end monitor pair.	
<b>Symptom:</b> Logic is reversed in case of end to end monitors	
<b>Feature:</b> Client	<b>Function:</b> TOPOLOGY
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.1.1	<b>Service Request ID:</b> 370061

<b>Defect ID:</b> Defect:000253184	<b>Technical Severity:</b> Medium
<b>Summary:</b> Fault Management – Switches discovered through v1 are getting listed in the <b>Infirms</b> table in the " <b>snmp setup</b> " dialog listing	
<b>Symptom:</b> 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.	
<b>Feature:</b> MISC	<b>Function:</b> SNMP INFORMS
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000256506	<b>Technical Severity:</b> Medium
<b>Summary:</b> Client: In Pure mEOS the Plus symbol is not removed from the device tree after giving accept changes	
<b>Symptom:</b> Topology will not properly reflect the changes to Users	
<b>Workaround:</b> Launch a new client	
<b>Feature:</b> Client	<b>Function:</b> Client Framework
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000256989	<b>Technical Severity:</b> Medium
<b>Summary:</b> Scalability Fabric: Local Client hangs when the total switch count is 10172 ports	
<b>Symptom:</b> Local client launched does not show the data	
<b>Workaround:</b> restart the client	
<b>Feature:</b> Client	<b>Function:</b> TOPOLOGY
<b>Probability:</b> Low	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000257467	<b>Technical Severity:</b> Medium
<b>Summary:</b> EOS: EOSc switches discovered as seed loses manageability and discovery status shows "Invalid protocol".	
<b>Symptom:</b> User will not get manageability for EOS switches	
<b>Feature:</b> Mbean for Server	<b>Function:</b> Mbean for Server
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000257722	<b>Technical Severity:</b> Medium
<b>Summary:</b> Not able to make any zoning changes, works on b/u server	
<b>Symptom:</b> Zoning activation fails in case the port index greater than 255 is part of the zone Configuration in Interopmode 2	
<b>Workaround:</b> This would work fine, if only port index lesser than 256 are selected.	
<b>Feature:</b> ZONING	<b>Function:</b> USABILITY
<b>Probability:</b> Low	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.1.3	<b>Service Request ID:</b> 386917

<b>Defect ID:</b> Defect:000258206	<b>Technical Severity:</b> Medium
<b>Summary:</b> Client crashes on launch when the system is at JRE 1.6.0_14	
<b>Symptom:</b> Client will not start	
<b>Feature:</b> Client	<b>Function:</b> Client Framework
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000259010	<b>Technical Severity:</b> Medium
<b>Summary:</b> Incorrect port number is displayed in the Topology for Switch to Switch connection	
<b>Symptom:</b> Link shows incorrect port information	
<b>Feature:</b> Client	<b>Function:</b> USABILITY
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000259163	<b>Technical Severity:</b> Medium
<b>Summary:</b> Discovery status for VF enabled switch is not getting updated in the Discovery dialog after changing its credentials from v1 to v3.	
<b>Symptom:</b> Appropriate Discovery status is not shown for VF enabled switches after modifying the SNMP credentials from v1 to v3.	
<b>Feature:</b> DISCOVERY	<b>Function:</b> Discovery Dialog
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000259605	<b>Technical Severity:</b> Medium
<b>Summary:</b> Discovery: Not able to discover the logical switch without deleting the existing one after changing the FID	
<b>Symptom:</b> Not able to manage the LS after changing the FID	
<b>Workaround:</b> Unmonitor/delete the unreachable LS	
<b>Feature:</b> DISCOVERY	<b>Function:</b> Switch Discovery
<b>Probability:</b> High	<b>Risk of Fix:</b> High
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000259674	<b>Technical Severity:</b> Medium
<b>Summary:</b> No ISL link is formed when port disable and enable is done in SAN Switch M14	
<b>Symptom:</b> Topology will not reflect properly to the user	
<b>Feature:</b> DISCOVERY	<b>Function:</b> ISL Discovery
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000260937	<b>Technical Severity:</b> Medium
<b>Summary:</b> 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.	
<b>Symptom:</b> 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.	
<b>Feature:</b> FCIP	<b>Function:</b> CONFIGURATION
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261014	<b>Technical Severity:</b> Medium
<b>Summary:</b> Web Tools is not launched for the switches in the SSL enabled server after migration	
<b>Symptom:</b> User will not be able to launch web tool some times.	
<b>Feature:</b> Proxy services	<b>Function:</b> Proxy services
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261162	<b>Technical Severity:</b> Medium
<b>Summary:</b> Internal error is thrown on modifying the SNMP credentials from <b>Edit Discovery</b> dialog.	
<b>Symptom:</b> Internal error is observed when the SNMP credentials are modified for the Discovered switches after initial discovery.	
<b>Feature:</b> DISCOVERY	<b>Function:</b> Discovery Dialog
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261163	<b>Technical Severity:</b> Medium
<b>Summary:</b> <b>FICON: Merge</b> wizard says merge operation success, but the master log says merge operation failed	
<b>Symptom:</b> User will not be sure whether the merge operation is success or failed	
<b>Feature:</b> FICON	<b>Function:</b> Cascaded FICON Merge
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	



<b>Defect ID:</b> Defect:000261422	<b>Technical Severity:</b> Medium
<b>Summary:</b> Yellow banner displayed in <b>ACL</b> tab of <b>Add LAG</b> dialog is not according tom FS.	
<b>Symptom:</b> Yellow banner displayed in the <b>ACL</b> tab of <b>Edit switch</b> isn't appropriate.	
<b>Feature:</b> FCoE/CEE Management	<b>Function:</b> Add/Edit CEE Port/LAG Dialog
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261425	<b>Technical Severity:</b> Medium
<b>Summary:</b> Yellow banner displayed in <b>ACL</b> tab of <b>Edit port</b> dialog [LAG member] is not according to Functional Specification document	
<b>Symptom:</b> Yellow banner displayed in <b>ACL</b> tab will not be in sync with Functional Specification document	
<b>Feature:</b> FCoE/CEE Management	<b>Function:</b> Add/Edit CEE Port/LAG Dialog
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261585	<b>Technical Severity:</b> Medium
<b>Summary:</b> When the Client is kept idle for some time, "unable to recover connection to server" error message is displayed.	
<b>Symptom:</b> Client suddenly lost its connection with the server and an error message "unable to recover connection to server" is displayed.	
<b>Feature:</b> Client	<b>Function:</b> USABILITY
<b>Probability:</b> Low	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261645	<b>Technical Severity:</b> Medium
<b>Summary:</b> WT session got expired before the session time out value and also out of Memory Error Exception thrown when launched from DCFM	
<b>Symptom:</b> WT sessions gets expired before reaching the time out values	
<b>Workaround:</b> Launch WT via IE	
<b>Feature:</b> Other Dialogs	<b>Function:</b> USABILITY
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261785	<b>Technical Severity:</b> Medium
<b>Summary:</b> Migration: After migration from EFCM, SAN256M is not getting manageability if it is discovered using APIuser in EFCM	
<b>Symptom:</b> SAN256M is not getting manageability after Migration	
<b>Workaround:</b> Give the proper SNMP credentials after migration or delete and rediscover the Fabric	
<b>Feature:</b> EFCM Migration	<b>Function:</b> USABILITY
<b>Probability:</b> High	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000261941	<b>Technical Severity:</b> Medium
<b>Summary:</b> Trap forwarding not allowing IP address addition	
<b>Symptom:</b> User will not be able to add the IP address of machine in which client is running.	
<b>Workaround:</b> 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	
<b>Feature:</b> Other Dialogs	<b>Function:</b> USABILITY
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000262177	<b>Technical Severity:</b> Medium
<b>Summary:</b> Firmware Management – Import of firmware to repository fails with two different error messages that are not appropriate.	
<b>Symptom:</b> Misleads the user with incorrect error messages.	
<b>Feature:</b> FIRMWARE MANAGEMENT	<b>Function:</b> Firmware Repository Management
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000262526	<b>Technical Severity:</b> Medium
<b>Summary:</b> From a CMDCE to CMDCE migration, the call home that is enabled for EMC cannot be disabled.	
<b>Symptom:</b> EMC call home configuration cannot be disabled on a migrated server	
<b>Feature:</b> Advanced Call Home	<b>Function:</b> USABILITY
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000262894	<b>Technical Severity:</b> Medium
<b>Summary:</b> Fabric changes cannot be accepted due to AG collector run before switch creation	
<b>Symptom:</b> 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.	
<b>Feature:</b> Access Gateway	<b>Function:</b> Access Gateway
<b>Probability:</b> High	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.3.0	

<b>Defect ID:</b> Defect:000262963	<b>Technical Severity:</b> Medium
<b>Summary:</b> Forbidden errors when doing the initial discovery in DCFM 10.1.4	
<b>Symptom:</b> User will not be able perform operations like Fabric Binding, Port Optics, Port Fencing etc.. when SSL is enabled & Port 80 is blocked.	
<b>Feature:</b> UNDETERMINED	<b>Function:</b> UNDER REVIEW
<b>Probability:</b> Low	<b>Risk of Fix:</b> Medium
<b>Found in Release:</b> DCFM10.1.4	<b>Service Request ID:</b> 396467

<b>Defect ID:</b> Defect:000263418	<b>Technical Severity:</b> Medium
<b>Summary:</b> Improve LIC error message when there is no fabric being managed by DCFM, current message causes confusion	
<b>Symptom:</b> Error message doesn't give proper reason for the failure to launch certain dialogs	
<b>Feature:</b> LIC & SSO	<b>Function:</b> Launch in Context
<b>Probability:</b> Medium	<b>Risk of Fix:</b> Low
<b>Found in Release:</b> DCFM10.3.0	