



Citi Architecture and Technology Engineering

McData FC Switch Solutions Guide

GDSE-04046-SG

Solutions Guide

4.2

Version Control

Version	Date	Author	Reviewed	Comments
0.1	8-Jun-2004	Eliot A. Wilson		Draft
0.2	8-Sep-2004	Eliot A. Wilson		Mgmt network section added by Parul Jain
0.3	6-Dec-2004	Eliot A. Wilson	Robert Small	OpenTrunking section added by Quang Le
0.4	26-Jan-2005	Vivek Jain	Vivek Jain	Format change RFC
1.0	14-Mar-2005	Parul Jain	GDSE, Kery Hines	Release
1.1	16-Mar-2005	Parul Jain	-	Removed SANtegrity and OpenTrunking sections
1.2	21-June-2005	Parul Jain	-	Added WWDS access in section 9 . Changes made in section 10.5. Appendix B, C completely re-written. Added appendix D.
1.21	22-June-2005	Parul Jain	-	Changes to steps 4 and 5 in appendix B.
1.3	13-Jul-05	Kevin Hobaugh	-	Section 9 updated with eTrust Audit
1.31	25-Oct-05	Parul Jain	-	Section 9: added Master ID compliance
1.35	24-Oct-2005	Scott Torgerson	SANtegrity Global Stakeholders	Section 14 added for SANtegrity (RFC)
1.36	11-Nov-05	Kevin Hobaugh	SAN Global Stakeholders	Section 8 Added Security Standards Section 9 Added McData

Version	Date	Author	Reviewed	Comments
				secure build information Appendix E Added Connectrix Mgr Roles Appendix F Added Logs for Connectrix Mgr (RFC)
1.4	28-Nov-05	Scott Torgerson	SAN Global Stakeholders	Release to Production v1.35 and v1.36 revisions.
1.41	19-Dec-05	Quang Le	SAN Global Stakeholders	Section 10.6 Added Open Trunking (RFC)
1.42	23-Dec-05	Kevin Hobaugh	SAN Global Stakeholders	Removed references to specific E/OS versions. (RFC)
1.43	26-Jan-06	Quang Le	Peer Review by Kevin Hobaugh	Minor update to OpenTrunking implementation instructions.
1.44	31-Jan-06	Quang Le	SAN Global Stakeholders	Release to Production
1.45	21-Feb-06	Parul Jain	-	Updates to figures 13 and 14 to include WWDS
2.0	15-May-06	Kevin Hobaugh	Peer Review	Added Connectrix Mgr 8.7.1 references
3.0	31-July-06	Parul Jain, Kevin Hobaugh	SAN Global Stakeholders	Added ESS Monitoring Solution. Eliminated redundant information. Reorganized sections for flow. Please read the entire document.
3.1	14-August-06	Parul Jain	-	Minor update relating to enabling link alerts within the "Monitoring the Switch" section
3.2	27-Sep-06	Parul Jain	-	Fixed minor error in the "Known Issues with Monitoring" section
4.0	31-Jan-07	Kevin Hobaugh	San Global Stakeholders	Section 2.2: Extended Distance ISL table added Section 3: OpenTrunking Section 4: Added support

Version	Date	Author	Reviewed	Comments
				for Connectrix Mgr Server version 8.7.1 to run on a Citigroup owned SOE Server. Section 5: IP Network Architecture. Changed the location of Connectrix Mgr Server in the network.
4.1	12-Jul-07	Kevin Hobaugh	-	Minor update. - Added section 4.3.1 – “eTrust Audit - log collection” - Updated section 5 with reference to EMC Secure Remote Support Gateway
4.2	26-Oct-07	Kevin Hobaugh	SAN Stakeholders	Added: ISL Port Fencing NPIV Connectrix Manager 9.1.1

Legal Notice

Information contained herein is for Internal Use and may be used only for business purposes authorized by Citigroup.

CITI, CITIBANK, CITICORP, CITIGROUP and the Umbrella Device are trademarks and service marks of Citicorp and are used and registered throughout the world. Citibank, Citicorp, Citigroup and their subsidiaries also claim rights in certain other trademarks and service marks contained in these pages.

Contact

Please address any comments or questions regarding the information contained in this document via email to the “*GT PSE Storage Platforms and Services” distribution list or alternatively to gdse@citi.com.

Latest Versions

It is recommended that the latest version of the document be used from the Storage Platforms and Services website <http://engineering.citigroup.net/gdse>. Newer versions may include expanded scope, or comments on issues discovered after deployment.

Table Of Contents

1. INTRODUCTION.....	9
1.1. CERTIFIED MODELS AND VERSIONS	9
1.2. COMPONENTS.....	9
1.3. INFORMATION CLASSIFICATION CERTIFICATION	10
2. FABRIC TOPOLOGIES.....	10
2.1. LOCAL SAN	10
2.2. METRO SAN	12
3. SWITCH CONFIGURATION.....	13
3.1. PHYSICAL PLACEMENT.....	13
3.2. MANAGEMENT ACCESS.....	13
3.3. SWITCH IDENTIFICATION.....	13
3.4. OPERATING PARAMETERS	14
3.4.1. DOMAIN PARAMETERS (SWITCH).....	14
3.4.2. FABRIC PARAMETERS	14
3.5. PORT SETUP	15
3.6. ISL SETUP	15
3.6.1. ISL PORT FENCING	16
3.7. OPENTRUNKING (ISL PERFORMANCE).....	17
3.7.1. IMPLEMENTING OPENTRUNKING	18
3.7.2. ENABLING OPENTRUNKING ON THE SWITCH	18
3.8. ZONING	20
3.9. INCIDENT DETECTION AND RESPONSE	20
3.10. DISABLE DEFAULT CAPABILITIES.....	20
3.11. NPIV ON MCDATA SWITCH (N_PORT ID VIRTUALIZATION)	21
3.11.1. ENABLING NPIV FUNCTIONALITY	21
3.11.2. CONFIGURING LOGIN LIMITS	22
3.11.3. FINAL CONFIGURATION DISPLAY	23
4. CONNECTRIX MANAGER.....	24
4.1. MASTER ID COMPLIANCE	25
4.2. AUTHORIZATION AND ACCESS CONTROL	25
4.2.1. CONNECTRIX MANAGER DEFAULT SECURITY GROUPS	25
4.2.2. CITIGROUP CONNECTRIX MANAGER SECURITY GROUPS.....	26
4.2.3. CONNECTRIX MANAGER SECURITY PRIVILEGES	27
4.3. CONNECTRIX MANAGER VIEWS.....	28
4.4. INCIDENT DETECTION AND RESPONSE	30
4.4.1. ETRUST AUDIT - LOG COLLECTION	32
4.5. DISABLE DEFAULT CAPABILITIES.....	32
4.6. CONNECTRIX MANAGER BACKUP PROCESS	33
4.7. VIRUS SCAN	34
4.8. PERSISTENT FABRICS	34
4.9. ELEMENT MANAGER LICENSE KEY ENTRY	34

5. IP NETWORK ARCHITECTURE	35
5.1. FIREWALL RULES	36
5.2. VENDOR REMOTE ACCESS.....	36
5.3. VENDOR FUNCTIONAL USER ID	37
5.4. ADDITIONAL VENDOR FUNCTIONAL USER ID PERMISSIONS	37
6. SANTEGRITY	38
6.1. SANTEGRITY LICENSE KEY ENTRY.....	38
6.2. SANTEGRITY PORT BINDINGS	38
6.3. SANTEGRITY FABRIC BINDINGS.....	41
6.4. SANTEGRITY OPERATIONAL CHANGES.....	43
6.5. ADDING NEW STORAGE/SERVER CONNECTIONS TO A SWITCH	43
6.6. ADDING NEW SWITCHES TO THE FABRIC.....	44
6.7. ADDING ADDITIONAL ISLS FROM EXISTING SWITCHES.....	46
6.8. REMOVING HOSTS FROM SWITCHES.....	46
6.9. REMOVING ISLS FROM SWITCHES	46
6.10. REMOVING SWITCHES FROM A FABRIC.....	47
7. MONITORING THE SWITCH.....	47
7.1. COMPARISON OF MONITORING SOLUTIONS.....	48
7.2. IMPLEMENTATION STEPS.....	50
7.3. PREREQUISITES	51
7.3.1. FAULT MANAGEMENT PROCESS.....	51
7.3.2. E/OS VERSION.....	52
7.3.3. IP NETWORK REQUIREMENTS.....	52
7.4. MCDATA SNMP TRAP CAPABILITY OVERVIEW	52
7.4.1. PORT STATUS MONITORING.....	52
7.4.2. LINK STATUS MONITORING.....	53
7.4.3. FIELD REPLACEABLE UNIT MONITORING	53
7.4.4. LINK UTILIZATION THRESHOLD MONITORING	53
7.5. CONFIGURATION	53
7.5.1. SWITCH NAME.....	53
7.5.2. SWITCH SNMP AGENT	54
7.5.3. THRESHOLD SETTINGS	54
7.6. FILTERING RECOMMENDATIONS	55
7.6.1. FCEOS MIB (ENTERPRISE ID 1.3.6.1.4.1.289).....	55
7.6.2. FCMGMT V3.1 MIB (ENTERPRISE ID 1.3.6.1.2.1.8888).....	59
7.6.3. ENRICHMENT RECOMMENDATIONS.....	60
7.7. FIREWALL CHANGES.....	61
7.8. HEART BEAT MONITORING	61
7.9. TESTING.....	62
7.9.1. MONITORING TEST CASES.....	62
7.9.2. HEARTBEAT TEST CASE.....	62
7.10. KNOWN ISSUES WITH MONITORING.....	62
8. UPGRADE CONSIDERATIONS.....	63
8.1. STORAGE PORT SWAPS.....	63
9. REFERENCES AND RELATED DOCUMENTS	64

10.	APPENDIX A: CONNECTRIX MANAGER INSTALLATION.....	65
10.1.	CONNECTRIX MANAGER PACKAGES.....	65
10.2.	UPGRADING THE CONNECTRIX MANAGER SERVER.....	65
10.2.1.	INSTALLING CONNECTRIX MANAGER SERVER 9.1.0.....	65
10.2.2.	INSTALLING CONNECTRIX MANAGER SERVER 9.1.1.....	73
10.2.3.	INSTALLING CONNECTRIX MANAGER CLIENT 9.1.1.....	82

1. Introduction

Fibre channel (“FC”) networks provide highly scalable and reliable connectivity between servers and storage resources such as disk and tape libraries. The fibre channel network uses fibre cabling at the physical layer, and the fibre channel protocol at layer 2. The payload at layer 3 is usually the SCSI protocol.

The fibre channel network, also called “fabric”, is made up of one or more fibre channel switches, also called “directors”. Citigroup has selected McData switch products for building fibre channel networks.

1.1. Certified Models and Versions

To get a list of certified switch models and firmware versions, please see the “Storage Switches” section from

[GDSE Supported Storage Infrastructure Configuration Matrix](#)

1.2. Components

McData switch hardware needs several other hardware and software components to function within the Citigroup IT environment.

Name	Purpose	Documentation
McData Fibre Channel Switch	Hardware that switches fibre channel frames	This document
E/OS	Firmware that runs on McData switch	This document and certification documents located on the McData Product Page .
SANtegrity	Software that enables certain security features on McData switch	This document
OpenTrunking	Software that enables load balancing among inter switch links	This document
Connectrix Manager	Software used to manage McData Fibre Channel switches	This document and certification documents located on the McData Product Page .
IP Network Architecture	McData switches, Connectrix Manager and other components must be interconnected over a secure TCP/IP network	This document
ESRS - Vendor Remote Access	The fault management of McData switches is currently owned by the vendor. The vendor can remotely access the environment for this purpose.	Certification document: EMC Secure Remote Support - Solution Guide
SanScreen	Software for change monitoring. It	Documentation can be found on the Onaro

Name	Purpose	Documentation
	interfaces with Connectrix Manager.	SANscreen Product Page .
ECC FCC Agent ¹	EMC Control Center agent for monitoring and reporting. It interfaces with Connectrix Service Processor.	Documentation can be found on the EMC Control Center Product Page
eTrust Audit	Software used for capturing, processing and reporting audit logs from Connectrix Manager.	eTrust Audit document
ESS Monitoring	Switch faults are monitored via Enterprise System Services infrastructure.	This document

1.3. Information Classification Certification

The SAN is infrastructure, and thus will be managed towards a class ‘C’ certification. Therefore, the SAN can process and store information classified as “public”, “internal” and “confidential” only. Information classified as “restricted” or “highly confidential” cannot be processed on the SAN unless adequate controls, such as encryption, are built into the application.

The latest revision of the “Infrastructure Classification Ratings” document can be found at: <http://www.citigroup.net/informationsecurityservices/istg>.

2. Fabric Topologies

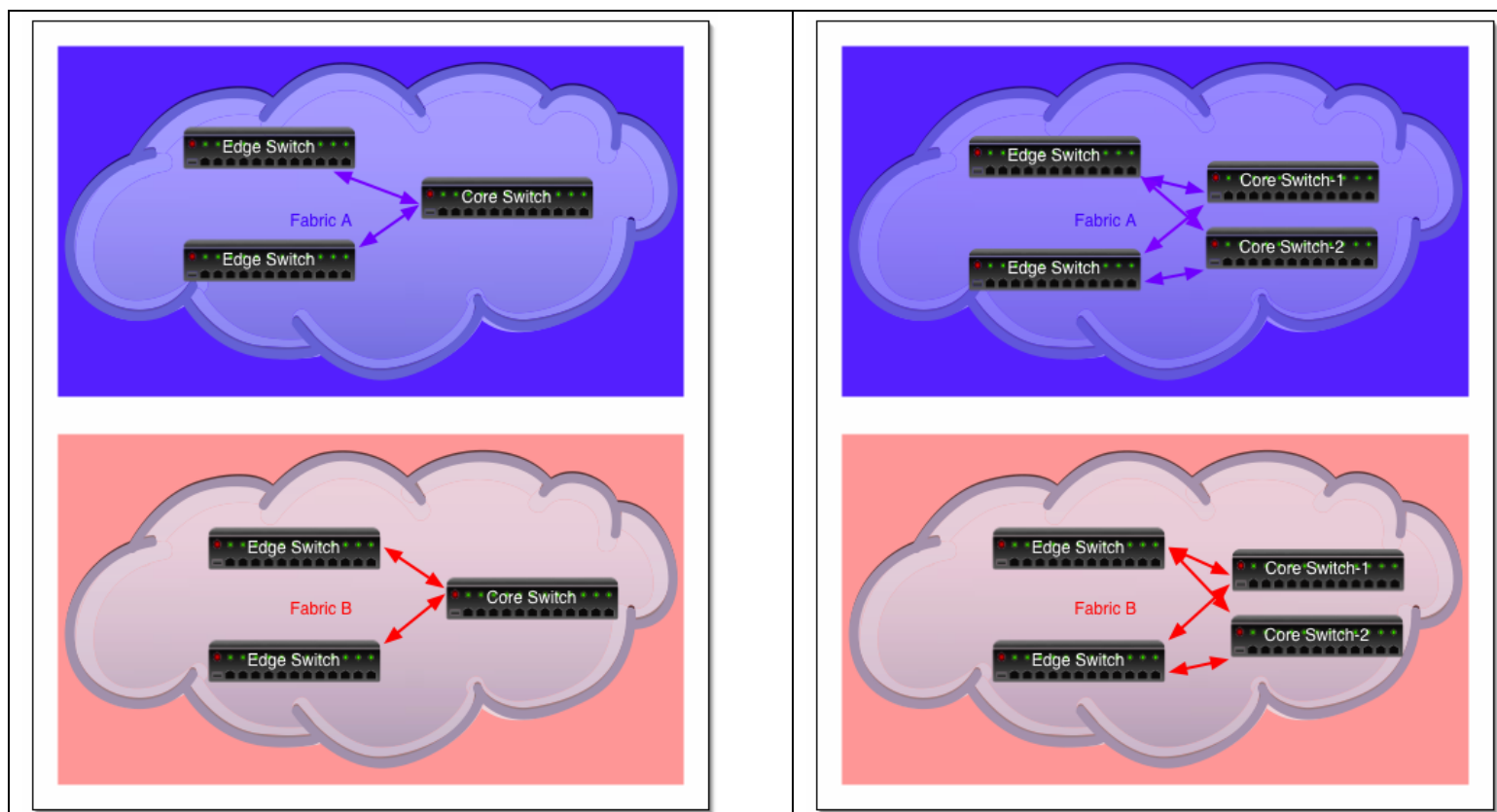
2.1. Local SAN

A “local” SAN fabric has all switches connected via Inter-Switch Links (ISL’s) which are all less than 5km in length and typically much shorter. Consult the latest network-planning guide from EMC or McData for cabling types and associated lengths supported for different bandwidths.

A core-to-edge fabric topology is recommended to provide any-to-any connectivity, evenly distribute traffic, maximize the ease of scalability and maintain a single hop between devices. In this topology, the core switch connects to tier 1 devices and to edge switches. The tier 1 devices are those requiring high bandwidth and availability such as storage arrays. Servers should be attached to the edge switches.

Dual fabrics should be implemented to provide high availability. Storage arrays and servers should be dual connected to each of the fabrics. This provides increased bandwidth and two independent data paths. There is also protection from single path failure (HBA, cable, switch) and allows for non-disruptive maintenance of the combined SAN. The fabrics should be configured symmetrically for ease of management.

¹ Pending certification



Large SAN environments where the highest port capacity core director will still not meet the connectivity requirements should consider a 2-tier dual core dual fabric architecture. In this design, ISL's from all edge switches are connected to a pair of dual core switches in each fabric. Storage ports are evenly distributed between the pair of dual core switches in each fabric. While this approach increases the total ISL requirements, it effectively doubles the number of core ports available and maintains a single hop architecture. In large environments such as this, consideration should be given to the increased operational risk of having twice as many servers attached to the same SAN fabrics. Change management policy and procedures may need to be enhanced to reduce the risk of change affecting both large fabrics at the same time.

Enterprise class SAN environments should use directors as core and edge devices. Directors provide a higher port count and uptime availability of 99.999%. Directors partially populated with port cards can provide an ideal building block for an easily expandable SAN fabric. Smaller deployments might initially build with a 1 or 2 tier switch configuration due to low port requirements but should consider future growth and the possible impacts of fabric expansion. Preliminary design considerations should take into account a manageable upgrade path to 2-tier fabrics with at minimum directors as core devices.

It is recommended that SAN fabrics and attached devices be located in a localized area less than 5km between connection points. Longer distance (extended) connections between switch and edge devices or ISL's between switches should be avoided in disk SAN's. This architecture helps avoid any impact to local storage access due to communications link failures and propagation delays between switches.

2.2. Metro SAN

Extended SAN's or Metro SAN's are only recommended for tape SAN's to provide offsite backup and for storage array replication such as EMC's SRDF over fibre channel. Metro SAN's should be dedicated to that traffic and local disk access should be maintained on separate SAN fabrics.

Dual fabrics should be implemented to provide high availability. Storage arrays should be connected to each of the dual fabrics. Tape devices and backup software that support dual attachment should connect to dual fabrics. Otherwise, tape devices should be evenly distributed across both fabrics to evenly distribute load. The projected fabric size and reliability required will be the determining factors in deciding whether to use switches or directors in an extended SAN. Extended ISL connections also require additional buffers (credits) to maintain full bandwidth over the longer distances. Some switch class products offer limited buffer credits and ports for extended ISL connections so this must be considered when designing the extended fabric.

Cable Type	62.5/125 micron multimode	50/125 micron multimode	9/125 micron single mode
Transmit Speed & Distance	300 meters (1.0625 Gbps) 150 meters (2.1250 Gbps) 33 meters (10.2000 Gbps)	500 meters (1.0625 Gbps) 300 meters (2.1250 Gbps) 150 meters (4.2500 Gbps) 82 meters (10.2000 Gbps)	10, 20, or 35 km, depending on transceiver type
SFP Port	Shortwave with 850 nm wavelength	Shortwave with 850 nm wavelength	Longwave with 1300 nm wavelength

Transmit Speed	1Gbps	2Gbps	4Gbps	10Gbps
BB Credit to distance ratio	1 credit per 2km	1 credit per 1km	2 credits per km	6 credits per km

Note: For detailed switch buffer to buffer credit information, please reference:

"McDATA Products in a SAN Environment - Planning Manual" from the McData website.

Refer to section "Product Features > Connectivity Features".

Extended ISL bandwidth between switches in a Metro SAN configuration needs to be carefully planned and maintained. This is especially true for SAN's carrying synchronous storage array replication traffic. Adequate bandwidth for peak load of all links through the extended switches plus a buffer of 25% should be planned. Additional bandwidth capacity should be considered to handle the increased load should one fabric fail and all traffic shifts to a single fabric.

The standard management environment for McData switches requires that switches at different sites connected via an extended ISL be managed by local Connectrix Manager

Servers as IP connectivity is not available between the private IP management subnets at each site. Since zoning information is stored on the CM Server, it is important to make changes to this information consistently from only one CM Server that manages a switch in the extended fabric. This CM Server should be designated as the primary Connectrix Manager for the extended fabric.

3. Switch Configuration

3.1. *Physical Placement*

Dual fabric environments should have switches from each fabric located in different physical cabinets and if possible, on different electrical circuits. Each fabric's cabinets should be physically separated as far apart as is reasonably possible to reduce the risk of a localized incident affecting both data paths.

3.2. *Management Access*

The switch can be managed with several interfaces. Some management interfaces, such as HTTP and TELNET, identify and authenticate users. Others, such as NMRU, do not identify users. To compensate for these weaknesses, the McData switch should only be managed with the Connectrix Manager application. The IP network architecture that enforces this is illustrated in the section called "IP Network Architecture".

The McData switch identifies devices connected to the N_PORT and the E_PORT with the World Wide Name ("WWN"). Although port and fabric bindings will be in place as a form of authentication, physical access to the switch should be controlled by installing the switch in a secure data center.

3.3. *Switch Identification*

It is suggested that a (WWN) nickname be defined for every switch and director with the device name and device model, for example "390G44MD ED-64M". It is also suggested that the description field be populated with the name of the switch, device model, and whether it is a core or edge switch, for example "390G44MD ED-64M Core". The location field should be set to the name of the fabric on which the switch resides and is the same as the active zone set, for example "390G_SAN1_a"².

² This is only a suggestion; regions should use a naming convention that works best for them.

3.4. Operating Parameters

3.4.1. Domain Parameters (Switch)

- ✓ The switch preferred domain ID should be set to a number between 1 and 31. It is suggested that the domain ID be derived from the switch IP address.
- ✓ The “Insistent” options should NOT be checked at this point³.
- ✓ Operating mode for the switch should be set to “Open Systems” for distributed server environments. The S/390 option should not be selected.
- ✓ The “Rerouting Delay” and “Domain RSCN's” should not be checked.
- ✓ The “Zoning RSCNs - Isolate on zone activation changes” checkbox should be checked.
Note: When enabled, only devices that require RSCN notification due to a zoning configuration change receive RSCNs.
- ✓ The “Node Port Virtualization” checkbox should be checked on edge switches that require NPort Virtualization. See Section 3.12 for more information.

3.4.2. Fabric Parameters

- ✓ Switch Priority should be set to the default of “Default”.
- ✓ Interop Mode should be set to “McData Fabric 1.0⁴”.
- ✓ The BB_credit should be set to the default of 16.
- ✓ The default values should be set for R_A_TOV and E_D_TOV to 100 and 20, respectively.

Note: Some non-director switches use buffer pools. In this case, the BB_credit for ISL's should be set to 16; the remainder of the buffer credits should be dispersed among the remaining ports.

³ The Insistent Domain ID option will get automatically enabled once fabric bindings are enabled.

⁴ At this time there are no applications in the fabric that require the “Open Fabric Mode”. GDSE might consider making “Open Fabric Mode” as the standard when sufficient incentives exist to do so. Mode switch requires downtime.

3.5. Port Setup

It is suggested that Port Names be assigned at a minimum to those used for ISL's and attached Tier 1 devices (storage arrays for example). ISL ports can be named⁵ using the source and destination switch and port such as "35E 3 – 36R 3". Storage array ports can be named with the array name and array port such as "OS7E 3BB".

The "10-100km" setting should only be enabled on ports operating over a distance greater than 10km. Switches on both ends of the connection need to support the additional buffering to fully utilize the link.

It is suggested that link incident alerts (LIN Alerts) be enabled for all ports used for ISL's, attached to storage arrays and other Tier 1 devices requiring high availability such as tape drives or SAN appliances.

Port type should be set to the default "G-port".

Port speed should be set to "negotiate" for all ports on switches supporting 1, 2 or 4Gb rates. Ports used for extended ISL connections over DWDM or similar links should be set to the actual link speed to avoid negotiation overhead during intermittent link outages.

Switches should be configured with at least 1 port open as spare so that a failed port's device can be re-connected to minimize any outage. Directors should be maintained with at least 1 port card open as spare to minimize the outage if a port card fails and also to allow for ISL growth.

[Port Bindings](#) should be enabled for all ports on the switch as soon as the switch is up and before any fiber cables are plugged in. Binding all empty ports will bind them to NULL so that nothing can be plugged into the switch and log into the fabric until the port is unbound.

3.6. ISL Setup

[Fabric Bindings](#) should be turned on a switch as soon as it is turned on but before any fiber cables are plugged into it. When fabric bindings are turned on for a new switch, that switch itself should be added to it's own fabric membership list.

The number of ISL links between switches should be well managed to provide expected fan-in ratios based upon port capacity and ISL bandwidth. At minimum there should be two ISL's between switches for high availability, but consideration must also be given to the situation where a single ISL loss would incur a loss in 50% of available bandwidth. For equal or greater link speeds for core to edge disk fabrics, the current rule of thumb

⁵ This is only a suggestion; regions should use a naming convention that works best for them.

is a 14 to 1 fan-in. A 32 port 1Gb/s edge would have 3 ISL's to a 1 or 2 Gb/s core. A 140 port 2Gb/s edge would have 10 ISL's to a 2Gb/s core. Expected traffic patterns of known applications should be considered when laying out ISL's to determine if a different ratio is needed⁶.

ISL connections should be spread across port cards in directors and ASIC's in switches when possible. Every ISL between the same two switches should be connected to a different port card or ASIC on each switch. This will minimize the impact of a failed component to the rest of the fabric.

3.6.1. ISL Port Fencing

Port Fencing is a feature that allows you to protect your SAN from repeated operational or security problems experienced by switch ports. Port Fencing allows you to set threshold limits on the number of specific port events permitted during a given time period. If the port generates more events during the specified time period, the Connectrix Manager (Port Fencing feature) blocks the port, disabling transmit and receive traffic until you have time to investigate, solve the problem, and manually unblock the port.

Use the "ISL Protocol Threshold" to block a port when one of the following ISL protocol errors meets the threshold:

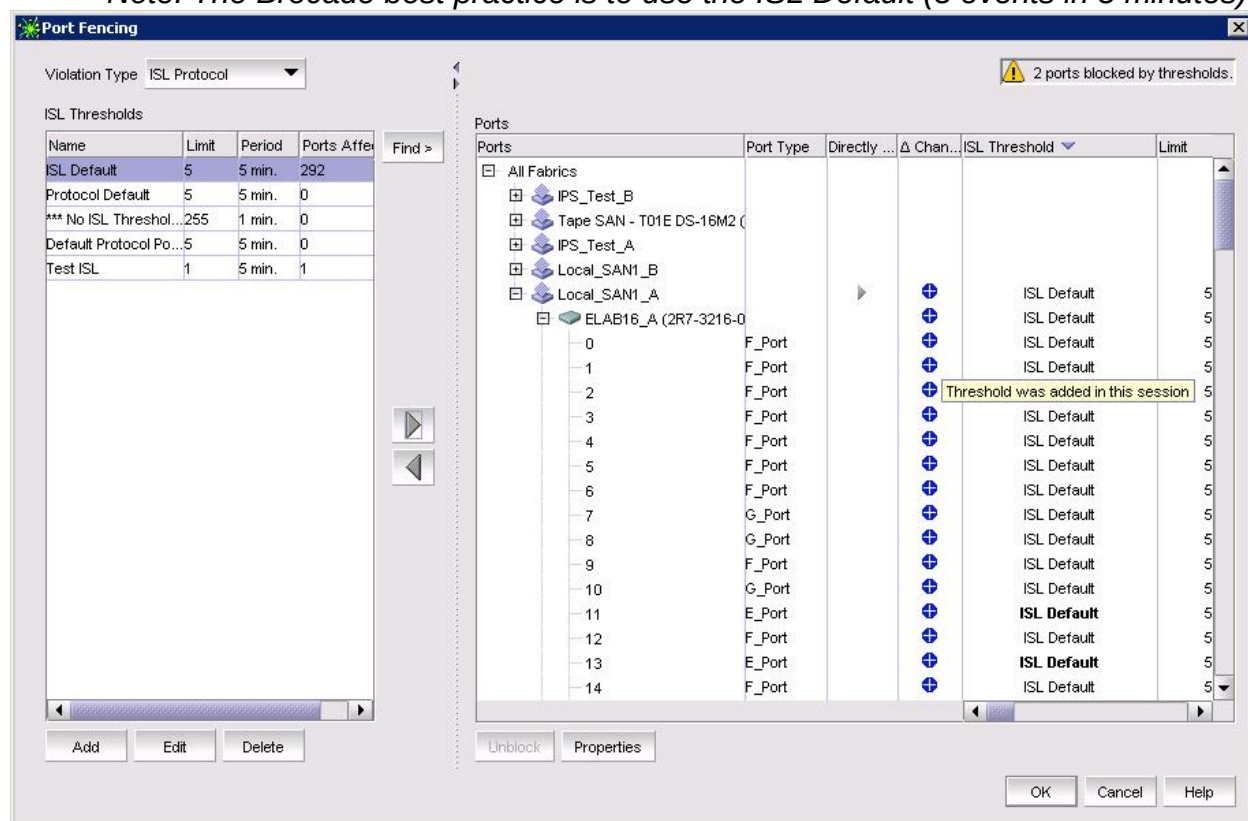
- ISL Bouncing—ISL has repeatedly become unavailable due to link down events.
- ISL Segmentation—ISL has repeatedly become segmented.
- ISL Protocol Mismatch—ISL has been repeatedly put into the Invalid Attachment state due to a protocol error.

From the Configure menu in Connectrix Manager, select "Port Fencing" (see dialog box below):

1. Select "ISL Protocol" from the Violation Type drop-down list.
2. In the Thresholds table, select the "ISL Default" threshold.
3. In the Ports table, select the Fabric or Switch you want to assign the threshold.
4. Click (right arrow). An icon appears next to the objects you selected in the Ports table to show that the threshold was applied. An icon appears next to every object in the tree to which the new threshold is applied (see figure below).
Note: The "ISL Default" will appear next to every port in the switch or fabric. This is okay. The setting will only apply to ISL ports. In the event that an ISL had to be moved to another port, it would automatically inherit the "ISL Default".
5. Click OK to apply the threshold and close the Port Fencing dialog box.

⁶ Please contact GDSE for alternative recommendations if this rule of thumb is inappropriate in your environment.

Note: The Brocade best practice is to use the ISL Default (5 events in 5 minutes).



3.7. OpenTrunking (ISL Performance)

OpenTrunking is a license-enabled feature available in McData directors and fabric switches that provide the capability to reroute traffic from over-utilized ISL's to more efficient ISL's. This technology can be used to resolve network congestion problems within the SAN. In order for OpenTrunking to be beneficial, ISL's with an appropriate amount of free bandwidth and BB Credits will need to be available to offload some of the traffic from over-utilized ISL's. GDSE has tested and certified OpenTrunking in disk SAN's. Although it was not specifically tested in SRDF and Tape environments, the vendor and GDSE support it.

Whenever traffic is rerouted, as a result of OpenTrunking or other infrequent fabric situations like the loss of an ISL, there is a possibility of out-of-order frame (OOOF) delivery. Therefore the algorithms used by OpenTrunking are extremely cautious and are based on long-term stable usage statistics. A significant change in traffic patterns must last for roughly a minute or longer, depending on the situation, before OpenTrunking can be expected to react to it.

E/OS firmware 6.0 and later includes optimizations to allow the original path to drain off any remaining queued frames prior to starting transmission on the new re-routed path.

In addition to a small delay to allow frames to drain from the current egress port, a small additional delay is included to allow the downstream switch some time to deliver the frames it has already received. This prevents OOOFs resulting from unknown downstream congestion when the re-route occurs.

McData highly recommends that OpenTrunking be utilized in single-hop configurations to reduce any incremental increase in the possibility of an OOOF. Their testing has also shown that these new enhancements have virtually eliminated the occurrence of OOOFs, even in extremely congested and dynamic fabric conditions.

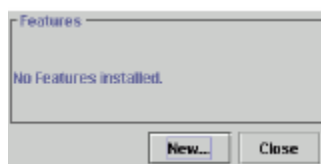
3.7.1. *Implementing OpenTrunking*

McData's OpenTrunking feature is only supported on switches that run E/OS versions 6.01 or later. Enabling OpenTrunking is a non-disruptive process but this feature should be enabled during a period of low-utilization. It is recommended that source and destination devices only have one hop between them to lower the risk of out-of-order frames when flows are rerouted to different ISL's. Assuming a dual-fabric configuration, OpenTrunking should be enabled using the following steps:

1. Ensure that hosts connected to the fabrics have both paths fully functional.
2. Enable OpenTrunking on the edge switches of the first fabric.
3. Enable OpenTrunking on the core switches of the first fabric.
4. Allow for a one-week break-in period before enabling OpenTrunking on the other fabric. If no issues are detected after one week, proceed to the next step.
5. Ensure that hosts connected to the fabrics have both paths fully functional.
6. Enable OpenTrunking on the edge switch of the second fabric.
7. Enable OpenTrunking on the core switches of the second fabric.

3.7.2. *Enabling OpenTrunking on the Switch*

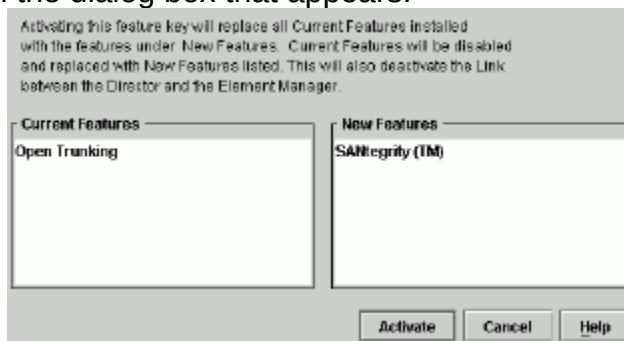
1. Refer to the [GDSE Supported Storage Infrastructure Configuration Matrix](#) to ensure that the switches are running a GDSE supported firmware version and a supported version of Connectrix Manager.
2. Obtain a feature key for the OpenTrunking feature.
3. Configure the feature key by doing the following:
 - a. Open the Element Manager view of the switch from Connectrix Manager.
 - b. From the **Configure** menu, select **Features**, and click **New** in the dialog box (Open Trunking would not be listed if the feature key has not been configured).



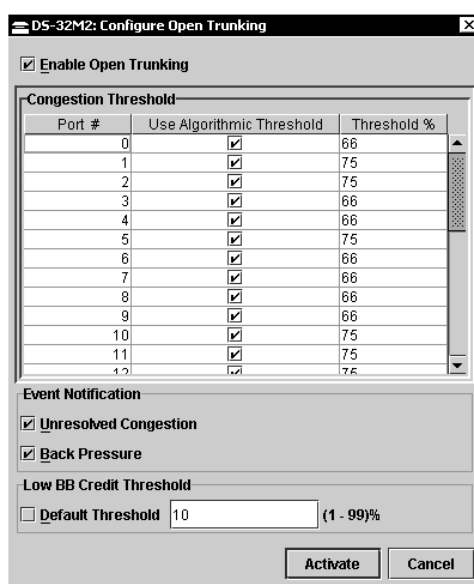
- c. Enter the feature key in the dialog box and Click **OK**.



- d. Click **Activate** in the dialog box that appears.



- e. The switch will IPL and all new features listed in the dialog box will become available. This should not disrupt any traffic within the SAN.
4. Once the feature key for OpenTrunking is configured, enable OpenTrunking by doing the following:
- Open Element Manager view of the switch from Connectrix Manager.
 - From the **Configure** menu, select **Open Trunking** and check the **Enable Open Trunking** checkbox. The **Use Algorithmic Threshold** checkbox should be checked so that the load-balancing algorithm will be used to reroute traffic. The **Unresolved Congestion** and **Back Pressure** checkboxes can also be checked for some additional logging.
 - Click **Activate**.



d. OpenTrunking is now enabled.

3.8. Zoning

Zoning is used to provide secure partitioning of devices connected to the SAN fabric. WWN zoning should be used instead of port zoning⁷. WWN zoning allows a device to be reconnected to a different port and continue access without requiring a zoning change⁸. Each zone can have only one initiator, and one or more targets from the same array type. Multiple array types in a single zone have not been tested by GDSE or recommended vendors. The “default” zone should be disabled; this zone is typically a catch all for devices not in any another zone. Unique zone sets should be maintained for each of the dual fabrics to minimize the total number of zones per zone set. Backup copies of the active zone set should be made prior to activating a modified zone set.

Note: Zoning is done based on WWPN (Port WWN) and not WWNN (Node WWN).

3.9. Incident detection and response

All logging is delegated to the Connectrix Manager application. Please see the Connectrix Manager section for a description of how logs are captured and processed.

3.10. Disable Default Capabilities

⁷ Port Bindings should always be used in conjunction with WWN Zoning.

⁸ When a cable is moved from an existing port, when port binding is enabled the new port will need to be unbound and then it needs to be rebound with the new WWN.

For security reasons, the telnet and web servers on every McData switch should be disabled. This can be done from Connectrix Manager, Element Manager GUI.

3.11. NPIV on McData Switch (N_Port ID Virtualization)

NPIV allows a single device port to support many virtual devices. Up to 256 virtual addresses per physical port (excluding ISLs) can be allocated without impacting the existing hardware implementation. Since the virtual N_port (called the NV_port) has the same properties as an N_port, it can register with all of the services in the fabric.

In order to support the HP C-Class Blade Servers and future Virtual Tape Library (VTL) products, NPIV must be enabled on the fabric switch before the server blade HBAs or any VTL product can log in to the fabric.

In the case of the HP C-Class Blade Servers, a Virtual Connect Fibre Channel (VC-FC) module is used to aggregate all the physical server HBA connections via a subset of 4 physical connections per module. This is done to reduce the number of physical fibre channel connections to the switch for the entire chassis.

Note: The configuration of the VC-FC is done strictly by the SA of the HP C-Class Blade Servers NOT by Storage Administrators.

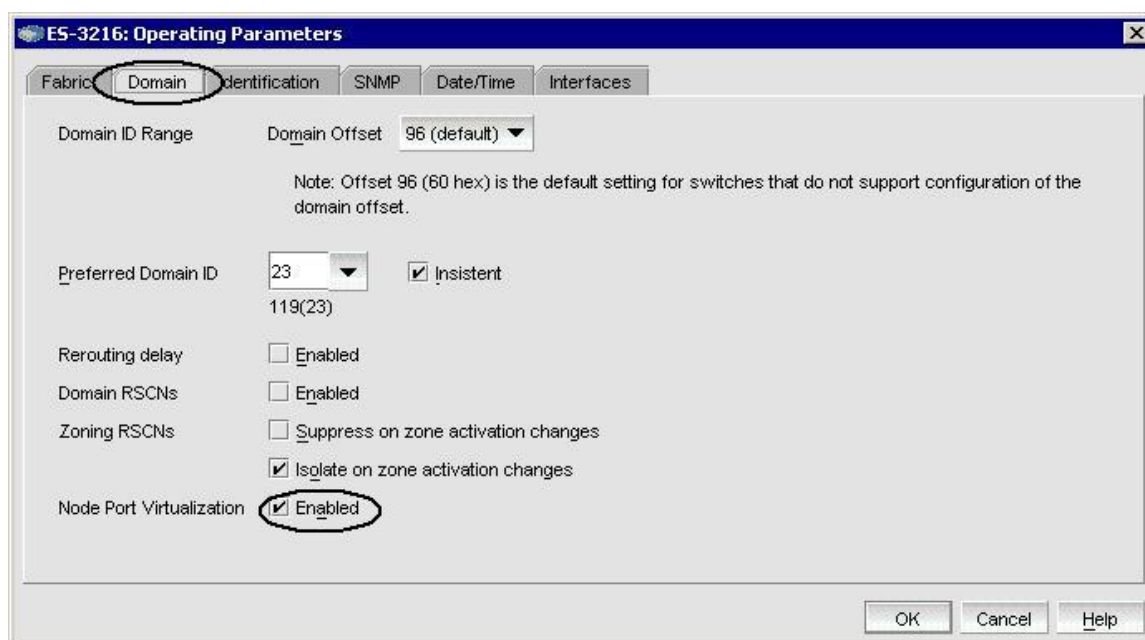
McDATA Fibre Channel switches with E/OS 8.0 or later will support NPIV. McDATA switches require an optional license to enable this function. Use the following procedure to apply this license and enable NPIV.

3.11.1. Enabling NPIV Functionality

1. From a browser, open the web user interface for the McDATA switch that is to be connected to the VC-FC module. The Node List view details the devices attached to the McDATA switch.
2. Although the license keys for NPIV functionality is provided a no cost by EMC, the serial number of the switch needs to be mailed to EMC for support confirmation in order to obtain the license key. (Or consult your local EMC representative)
 - a. Send an email containing the switch serial number to:
LicenseKeys@emc.com
3. To install the NPIV license, click **Maintenance**, and then select **Options Features**.
4. Enter the license key for NPIV in the **Feature Key** field. Select the key as the "N_Port ID Virtualization (NPIV)." Link from the window and apply the key by

clicking **OK**. A check mark in the left window indicates that the N_Port ID Virtualization key is installed.

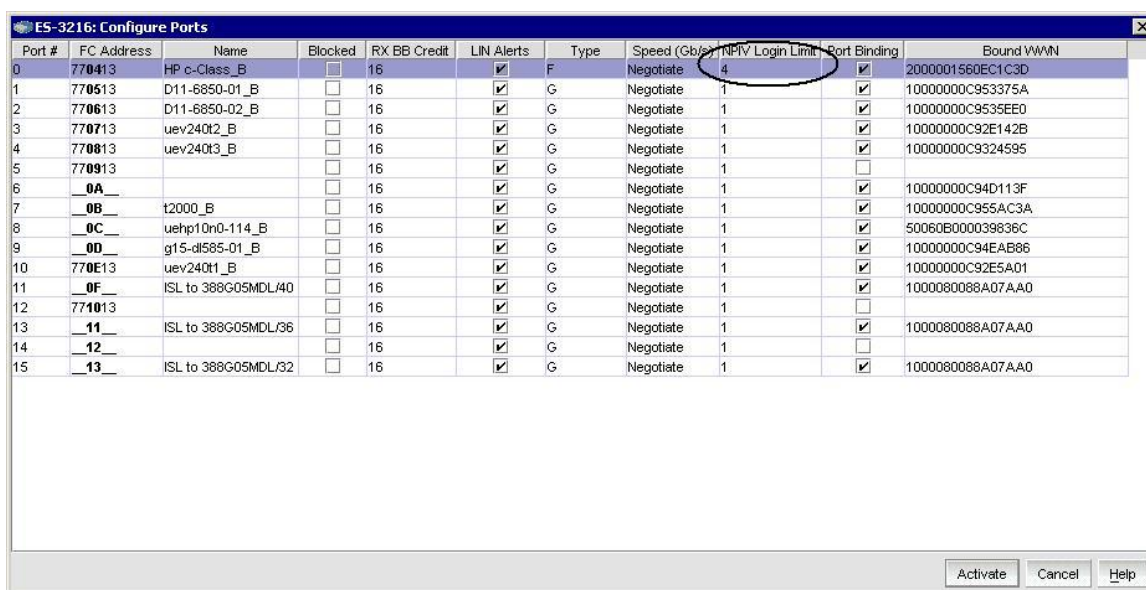
5. After launching the Element Manager menu for a particular switch, Click **Configure>Operating Parameters**, and then select the **Domain** tab.
6. Click **Enable** on the “Node Port Virtualization” option at the bottom of the menu.



7. At the prompt click **OK** if you are sure you want to enable NPV.

3.11.2. Configuring Login Limits

1. In the **Login** column, set the value to 17 or higher for each port connected to the VC-FC to ensure proper operation. (This example displayed “4”)



Port #	FC Address	Name	Blocked	RX BB Credit	LIN Alerts	Type	Speed (Gbit/s)	NPIV Login Limit	Port Binding	Bound WWN
0	770413	HP c-Class_B	☐	16	☒	F	Negotiate	4	☒	2000001560EC1C3D
1	770513	D11-6850-01_B	☐	16	☒	G	Negotiate	1	☒	10000000C953375A
2	770613	D11-6850-02_B	☐	16	☒	G	Negotiate	1	☒	10000000C9535EE0
3	770713	uev240t2_B	☐	16	☒	G	Negotiate	1	☒	10000000C92E142B
4	770813	uev240t3_B	☐	16	☒	G	Negotiate	1	☒	10000000C9324595
5	770913		☐	16	☒	G	Negotiate	1	☐	
6	0A		☐	16	☒	G	Negotiate	1	☒	10000000C94D113F
7	0B	t2000_B	☐	16	☒	G	Negotiate	1	☒	10000000C955AC3A
8	0C	uehp10n0-114_B	☐	16	☒	G	Negotiate	1	☒	50060B000039636C
9	0D	g15-df585-01_B	☐	16	☒	G	Negotiate	1	☒	10000000C94EAB86
10	770E13	uev240t1_B	☐	16	☒	G	Negotiate	1	☒	10000000C92E5A01
11	0F	ISL to 388G05MDL/40	☐	16	☒	G	Negotiate	1	☒	1000080088A07AA0
12	771013		☐	16	☒	G	Negotiate	1	☐	
13	11	ISL to 388G05MDL/36	☐	16	☒	G	Negotiate	1	☒	1000080088A07AA0
14	12		☐	16	☒	G	Negotiate	1	☐	
15	13	ISL to 388G05MDL/32	☐	16	☒	G	Negotiate	1	☒	1000080088A07AA0

2. Click **OK** to save changes.

3.11.3. Final Configuration Display

1. Under Element Manager for a particular switch, select **Node List** to view all the connected hosts. The proper configuration will display more than one WWN under a physical switch port. Each WWN numbers listed under the virtual switch port are hard coded on a physical HBA inside the Blade Server or any other device using this functionality.
2. The example below shows 1 physical connection with 2 virtual connections associated to it. This means there are 2 blade servers that are configured to see the switch ports.

Port #	Address	Class	BB Credit	Port WWN	Nickname
0	770413	Reserved	8	Unknown-2000001560EC1C3D	HP c-Class_B
0	770416	Reserved	16	Emulex-10000000C9566735	
0	77041E	Reserved	16	Emulex-10000000C95C99F3	d12-blade-01-slot-01_B
1	770513	Reserved	101	Emulex-10000000C953375A	g16-d1585-01_B(Sultan)
2	770613	Reserved	101	Emulex-10000000C9535EE0	g16-d1585-02_B(Sultan)
3	770713	Reserved	64	Emulex-10000000C92E142B	d8-v240-02_B
4	770813	Reserved	15	Emulex-10000000C9324595	d8-v240-03_B
5	770913	Reserved	15	Emulex-10000000C932437D	d8-v240-04_B
10	770E13	Reserved	64	Emulex-10000000C92E5A01	d8-v240-01_B
12	771013	Reserved	16	Emulex-10000000C955AB9F	

Note: The blade servers are configured to use the hardwired WWNs on each HBAs by default using the standard server build.

4. Connectrix Manager

McData switches and directors are managed using the Connectrix Manager, also known as “EFCM”, application software. The server communicates with the McData switches by using the SNMP (GET) and NMRU protocols over TCP/IP. Due to virus concerns on the vendor supplied Connectrix Manager Service Processor server (CSP), GDSE has re-architected the Connectrix Manager environment. This new architecture involves running the Connectrix Manager Server application on a Citigroup SOE server. The Connectrix Manager Server will reside on the Citigroup GDN. Having the Connectrix Manager environment running on a SOE server allows Citigroup to monitor for Antivirus fixes, OS updates, audit logins, hardware problem notifications and backup of the server.

For remote management access, the client portion of the Connectrix Manager application is automatically installed on the Connectrix Manager Server on SOE or can be loaded on a separate SOE server with IP connectivity to the Connectrix Manager Server on SOE.

For instructions on installing the Connectrix Manager application, please see the Appendix in this document. EMC will need to be engaged to assist in the migration of

Connectrix Manager Server from the vendor supplied 1U server to the Citi owned SOE server.

Note: Connectrix Manager Server can be co-located on the SANScreen Server.

4.1. Master ID Compliance

SOE IDs should be used as user IDs on the Connectrix Manager application. For example, if a user has been assigned SOE ID ol35678, their user ID on Connectrix Manager should also be ol35678.

Connectrix Manager 9.1.1 allows the user to manage their password. New IDs can be created with a default password (example: welcome). On their first login, the user can change their password.

4.2. Authorization and access control

With the release of Connectrix Manager 8.x, more granular security roles were incorporated into the product.

4.2.1. Connectrix Manager Default Security Groups

User Group	Read/Write Access	Read Only Access
System Administrator	All features.	
Security Administrator	Active Session Management Enterprise Fabric Mode Fabric Binding Remote Access Security Admin	

	User Management	
Maintenance	Backup, Call Home Event Notification Setup, Product Maintenance, E-mail Event Notification Setup	All other features except Product Administration, Product Operation.
Operator	Product Operation.	All other features except Product Administration, Product Maintenance.
Product Administrator	Backup Product Administration.	All other features except Product Maintenance, Product Operation.

4.2.2. **Citigroup Connectrix Manager Security Groups**

The default Connectrix Manager Security groups doesn't match our Citigroup security standards. Example, the Security Administrator has R/W access to Fabric Bindings. That access is not a requirement for the Citigroup Information Security Administration role. They only require log management. Therefore, customized Citigroup security groups and privileges will need to be created and used for user access. The following table details the groups and privileges that need to be created for the Citigroup environment. Use the default Administrator id to create the different groups. Add users per Master ID Compliance. Once this task is complete the default user groups in the above table can be removed.

User Group	Read/Write Access	Read Only Access
Citi Storage Administrator	All privileges <i>except</i> Log Management, User Management, Zoning Fabric Libraries (IPS zoning)	Log Management, User Management, Zoning Fabric Libraries (IPS zoning)
Citi Information Security Administrator	Group Manager - Create Event Log, Log Management, User Management	
Citi Auditor		Call Home Event Notification Setup, Product Administration, Product Operation, Email Event Notification Setup, Fabric Binding, Log Management, Properties, Server Access Control, SNMP Agent Configuration, Trap Forwarding, User Management
Vendor Maintenance	Product Maintenance, Call Home Event Notification Setup	
SANscreen Monitor		Active Session Management, Product Administration, Product Maintenance,

User Group	Read/Write Access	Read Only Access
		Product Operation, Enterprise Fabric Mode, Export, FabricBinding, License Update, Log Management, Monitor Ethernet Event, Persist Fabric, PortFencing, Properties, Security Admin, Server Access Control, Show Route, Shutdown, Trap Forwarding, View Management, Zoning
IPS Administrator	Product Administration Product Maintenance Product Operation Zoning Fabric Libraries (IPS zoning)	Reports

4.2.3. Connectrix Manager Security Privileges

Active Session Management	Add / Delete Properties Backup	Call Home Event Notification Setup
Discover On/Off	Discovery Setup	E-mail Event Notification Setup
Enterprise Fabric Mode	Event Management	Export
Fabric Binding	Frame Sniffer	Group Manager – Create Event Log
Group Manager – Firmware Install	Group Manager – Run Data Collection	Import
License Update	Log Management	Map Editing
Map Loop to Hub	Map Port to Storage	Monitor Ethernet Event
Nicknames	Performance	Persist Fabric
Planning	Port Fencing	Product Administration
Product Maintenance	Product Operation	Properties Edit
Remote Access	Reports	SAN Router Configuration
Security Admin	Servers	Setup Tools
Show Route	Shutdown	SNMP Agent Configuration
Software Configuration Parameters	Trap Forwarding	User Management
View Management	Virtual Fabric	Zoning Activation
Zoning Fabric Libraries (IPS)	Zoning Global Library (No IPS)	

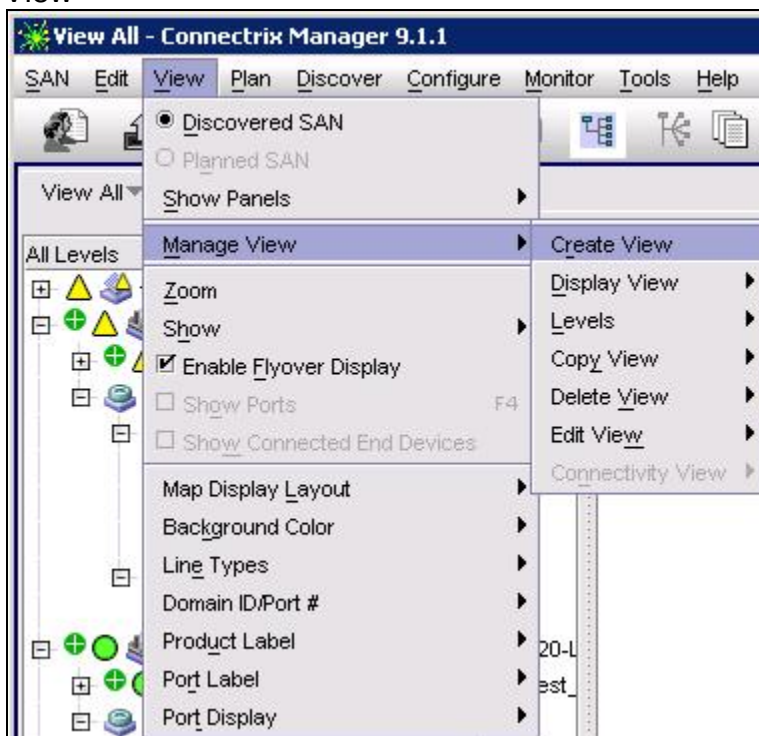
4.3. Connectrix Manager Views

In addition to creating security groups, Connectrix Manager allows for the creation of management views. These views are assigned to a security group and can be customized to provide specific views tailored to a particular group's function.

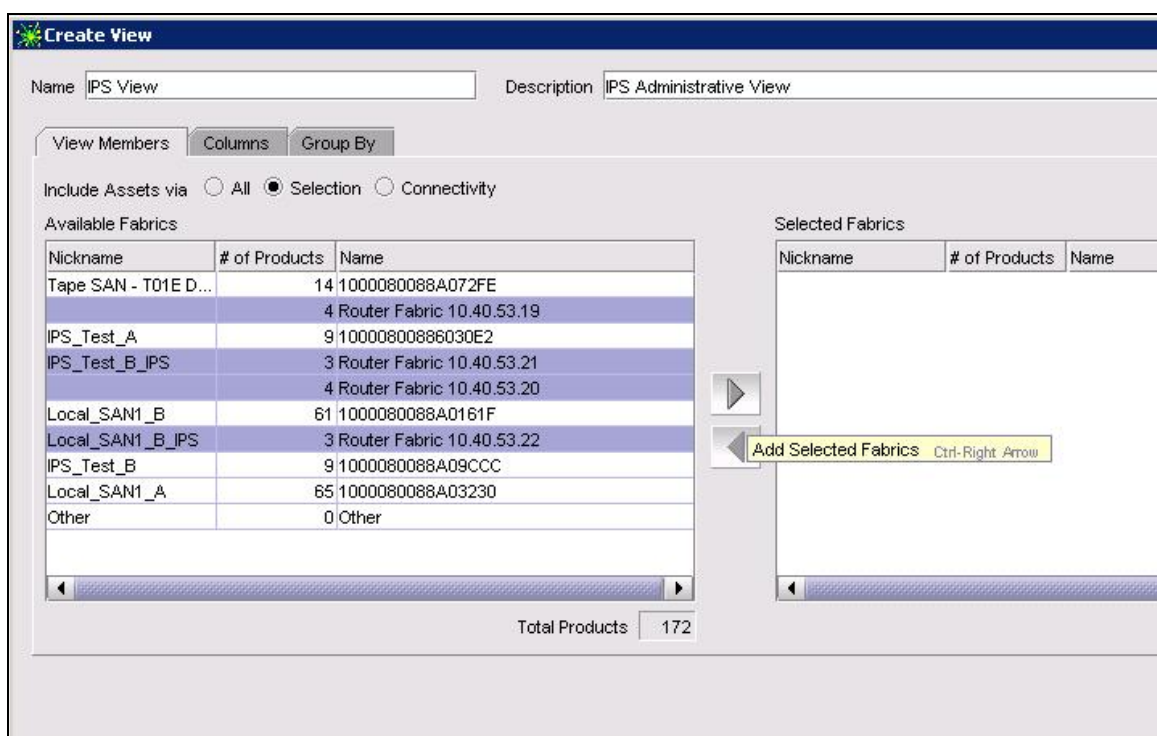
Example:

Create an IPS View, which would show IPS Administrators only the IPS Routers.

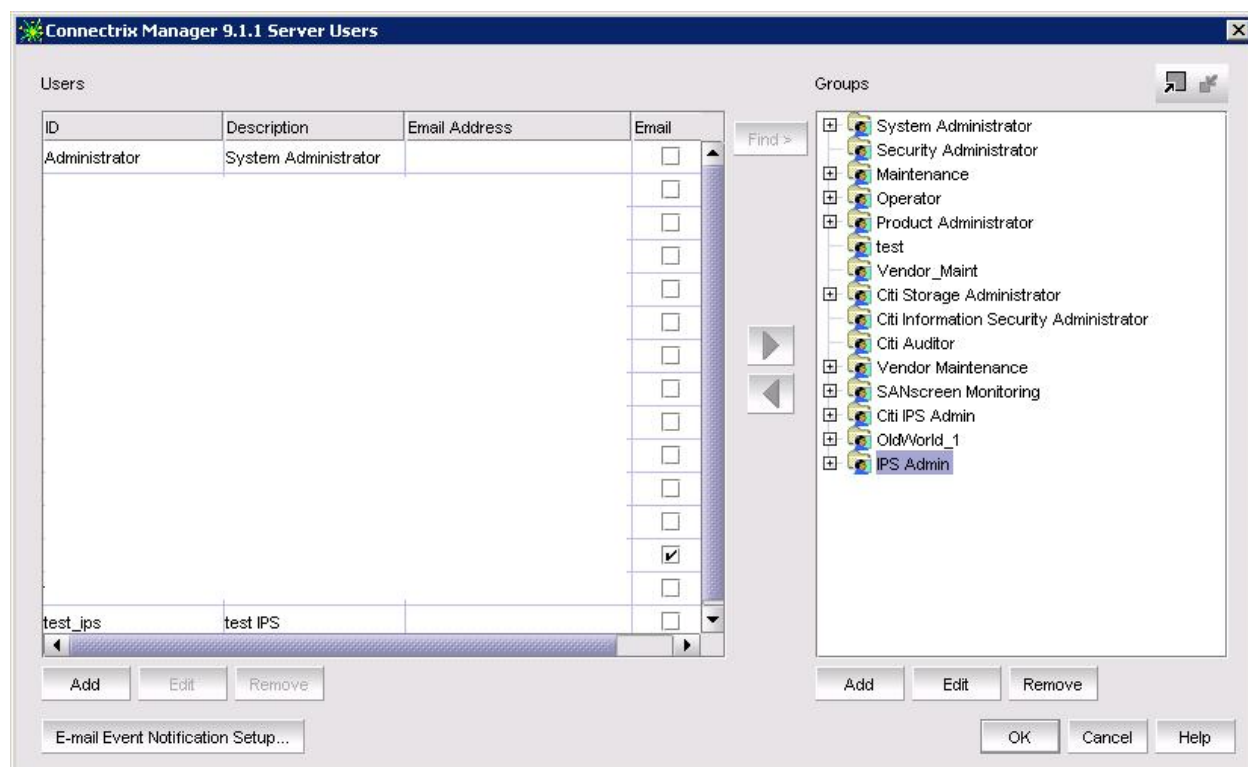
1. Select Create View



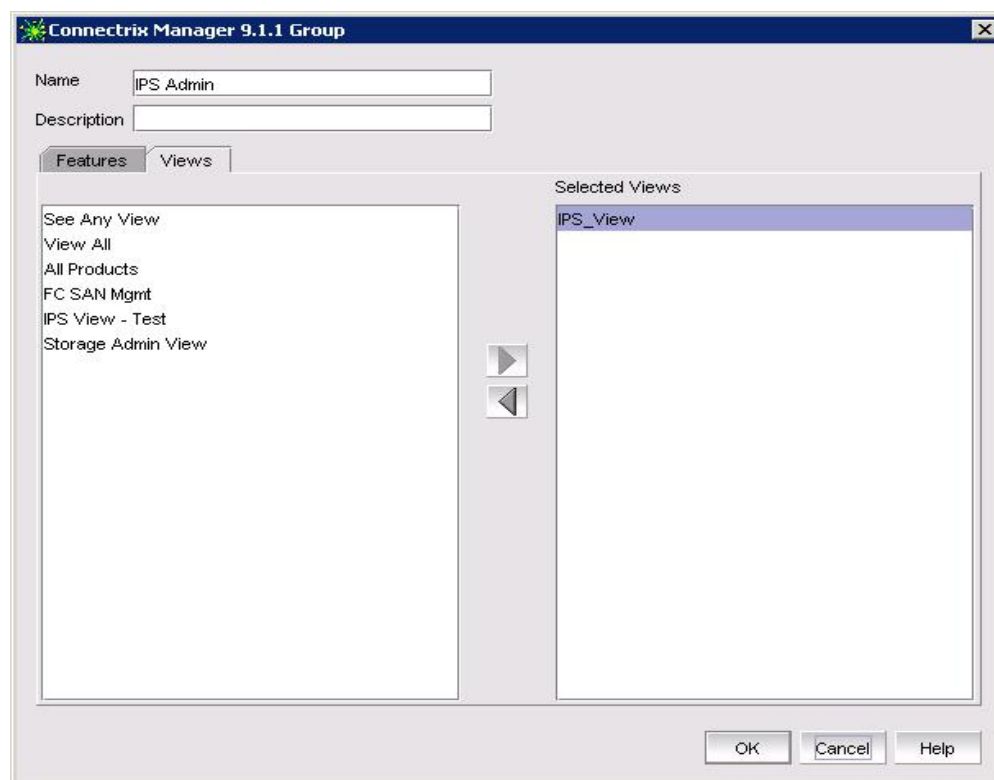
2. Name the view and click on the “Selection” radio button. From the list, select the “Router Fabrics” that the IPS Administrator will be managing. Add the selected fabrics and click “OK”.



3. Add the view to a security group.
From SAN/Users, select the Security group to add the view to and click on “Edit”.



4. Select the Views tab. Select the view from the left panel and add it to the right panel. Click 'OK' to complete.



NOTE: The above process can be used to create a FC Mgmt view, by selecting the FC switches only.

4.4. Incident detection and response

The Connectrix Manager application is capable of logging system and security events as illustrated below. The logs in Connectrix Manager are accessible from the Log menu, as illustrated below.



The Audit, Session, Product Status, and Fabric Logs store up to 1000 entries each and the Event Log stores up to 500 entries. Additional entries overwrite the oldest entries. The most recent entry appears at the top of a log.

From an Information Security perspective, the audit log is the one that is of interest. It displays a history of user actions performed through the Connectrix Manager. The following figure shows a sample audit log.

View Logs			
Audit Log		☐ Display in a new window	
Date/Time	Type	Parameter	User
2006/05/02 13:24:00	User Action Event	Updated Zone Set Z388G_SAN1L_B	System Administrator
2006/05/02 13:24:00	User Action Event	Succeeded Activate Zone Set Z388G_SAN1L_B in Fabric 1000080088A0161F	Administrator
2006/05/02 13:23:32	User Action Event	Updated Zone Set Z388G_SAN1L_A	System Administrator
2006/05/02 13:23:32	User Action Event	Succeeded Activate Zone Set Z388G_SAN1L_A in Fabric 1000080088A03230	Administrator
2006/05/02 13:23:01	User Action Event	Deleted Zone c11-d1585-02-388gx10hu_CL1A_A	System Administrator
2006/05/02 13:23:01	User Action Event	Succeeded Activate Zone Set Z388G_SAN1L_A in Fabric 1000080088A03230	Administrator
2006/05/02 13:22:27	User Action Event	Deleted Zone c11-d1585-02-388gx10hu_CL2C_B	System Administrator
2006/05/02 13:22:27	User Action Event	Updated Zone Set Z388G_SAN1L_A	System Administrator
2006/05/02 13:22:27	User Action Event	Updated Zone Set Z388G_SAN1L_B	System Administrator
2006/05/02 13:22:27	User Action Event	Succeeded Activate Zone Set Z388G_SAN1L_B in Fabric 1000080088A0161F	Administrator
2006/05/02 13:21:27	User Action Event	Succeeded Activate Zone Set Z388G_SAN1L_A in Fabric 1000080088A03230	Administrator
2006/05/02 10:57:31	User Action Event	Discovery Suspended	Administrator
2006/05/02 10:50:55	User Action Event	Nickname changed - FCSwitch 100008008860005D	Administrator
2006/05/02 10:50:55	User Action Event	Nickname changed - FCSwitch 100008008860005D	Administrator
2006/05/02 10:52:14	User Action Event	Nickname changed - FCSwitch 100008008860005D	Administrator
2006/05/02 10:49:07	User Action Event	Nickname changed - FCSwitch 1000080088A072FE	Administrator
2006/05/02 10:50:25	User Action Event	Nickname changed - FCSwitch 1000080088A072FE	Administrator
2006/05/02 10:49:07	User Action Event	Nickname changed - FCSwitch 1000080088A072FE	Administrator
2006/05/02 10:37:02	User Action Event	Updated Zone Set Z388G_SAN1L_B	System Administrator
2006/05/02 10:37:02	User Action Event	Succeeded Activate Zone Set Z388G_SAN1L_B in Fabric 1000080088A0161F	Administrator
2006/05/02 10:35:36	User Action Event	Updated Zone Set Z388G_SAN1L_A	System Administrator
2006/05/02 10:35:36	User Action Event	Succeeded Activate Zone Set Z388G_SAN1L_A in Fabric 1000080088A03230	Administrator
2006/05/02 10:34:51	User Action Event	Deleted Zone uelabhp7-020_388GX01ED_3ab_A	System Administrator
2006/05/02 10:34:51	User Action Event	Updated Zone Set Z388G_SAN1L_A	System Administrator

- The Date/Time column logs the date and time that the logged event took place

- The Parameter column describes the action that took place. Logged actions can include:
 - o Defining a new product
 - o Modifying product attributes
 - o Deleting product definitions
 - o Defining a new user
 - o Modifying user administration
 - o Deleting user administration
 - o Creating a zone set
 - o Modifying a zone set
 - o Modifying SNMP options
- The Parameter column describes the parameter affected by the event. For example, if a product is added or deleted, the product's network address is displayed.
- The User column identifies the user, which performed the logged action.

4.4.1. eTrust Audit - Log Collection

All Connectrix Manager Log events (Audit, Security, Event, etc) are collected in a Master Log. This log is available for viewing in Connectrix Manager 9.1.1 by selecting *Master Log* from the *View* menu. This log provides information on events that have occurred throughout the SAN. The data that populates the Master Log file is located in the Connectrix Manager directory on the Connectrix Manager server. If Connectrix Manager Server is installed on the vendor supplied server, Connectrix Manager files will be located in c:\program files. If Connectrix Manager Server is installed on a Citi SOE server, Connectrix Manager files will be located in c:\Program Files.

`\\ConnectrixManager9.1.1\\Server\\Universe_Home\\TestUniverse\\_Working\\EventStorage Provider`, in filename: Event_yyyymmdd.log.

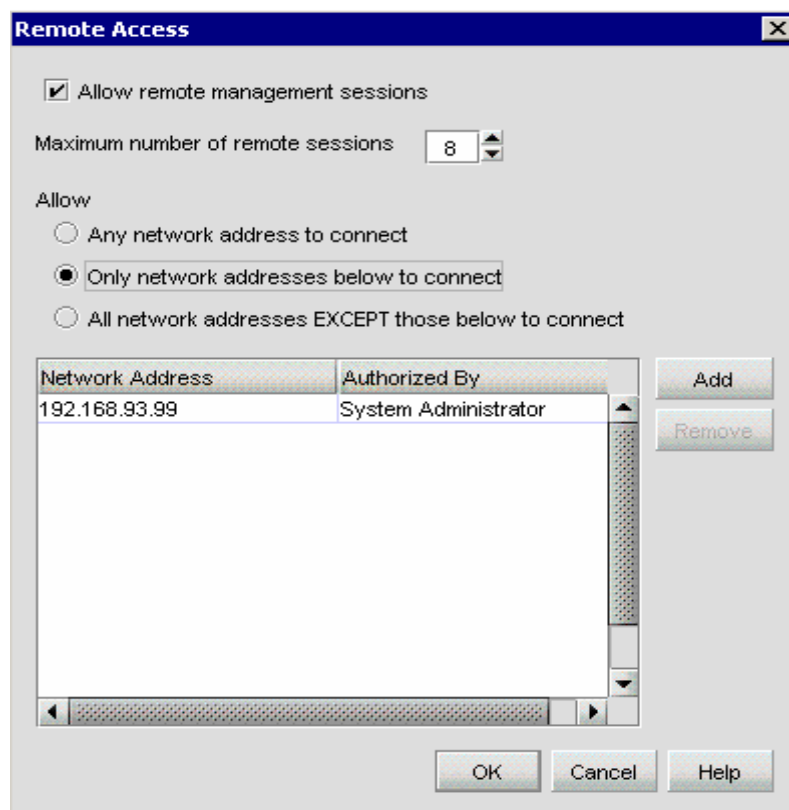
The Event files are created daily and are kept for 45 days or if total used space reaches 50mb. If these conditions are met they will roll off.

The Master Log should be archived on the eTrust Audit infrastructure. Details for implementing eTrust are available in the document "eTrust Audit - Storage Monitor Solutions Guide". The link for this document can be found in the [Reference](#) section.

4.5. Disable Default Capabilities

The following default capabilities should be disabled:

- The default password for the built in “Administrator” user ID should be changed at the time of install⁹
- Connections to the Connectrix Manager server should be limited to hosts that are authorized by Storage Management. Such servers would include any SOE server(s) hosting the Connectrix Manager client. The restriction can be enabled from the SAN -> Remote Access menu, as illustrated below.



- The logons on the SOE server hosting the Connectrix Manager client should be limited to users authorized by Storage Management.

4.6. Connectrix Manager Backup Process

Installing Connectrix Manager Server on a Citigroup owned SOE server provides Citigroup the ability to provide a backup of the Connectrix Manager configuration. A Citigroup approved SOE backup agent is required for backing up the fabric configuration.

⁹ The Connectrix Manager user and password database is stored on the Connectrix Manager Server. Any Connectrix Manager client instance can be used to change the password.

Connectrix Manager backs up data to two alternate folders. For example, if the backup directory location is *C:\CM911_Backup*, the backup service alternates between two backup directories, *C:\CM911_Backup\Backup* and *C:\CM911_Backup\BackupAlt*. The current backup is always *C:\CM911_Backup* and contains a complete backup of the system. The older backup is always *C:\CM911_Backup\BackupAlt*. Regional backup infrastructure process should be implemented for the Connectrix Manager Server.

Switch configuration backup is a manual process initiated from within the Element Manager for each particular product. The backup consists of multiple files and is stored in the “Connectrix Manager 9.1.1” directory. These files will be backed up through the Regional infrastructure backup process. GDSE recommends backing up the entire Connectrix Manager 9.1.1 directory.

4.7. Virus Scan

Running the Connectrix Manager Server application on a Citigroup owned SOE Server, allows for the installation of Citigroup approved virus-scanning software.

4.8. Persistent Fabrics

Connectrix Manager allows the fabric topology view to be persisted so that changes can be graphically highlighted in the application. When a fabric is persisted it must be given a name. This fabric name should match the name of the active zone set for ease of management. The topology view of a persistent fabric provides a “Fabric Log” which contains events that affected the state of the fabric and can be used for quick problem determination. After ISLs and/or switches are permanently added or removed from a persisted fabric the fabric should be re-persisted to take a new snapshot of the baseline topology.

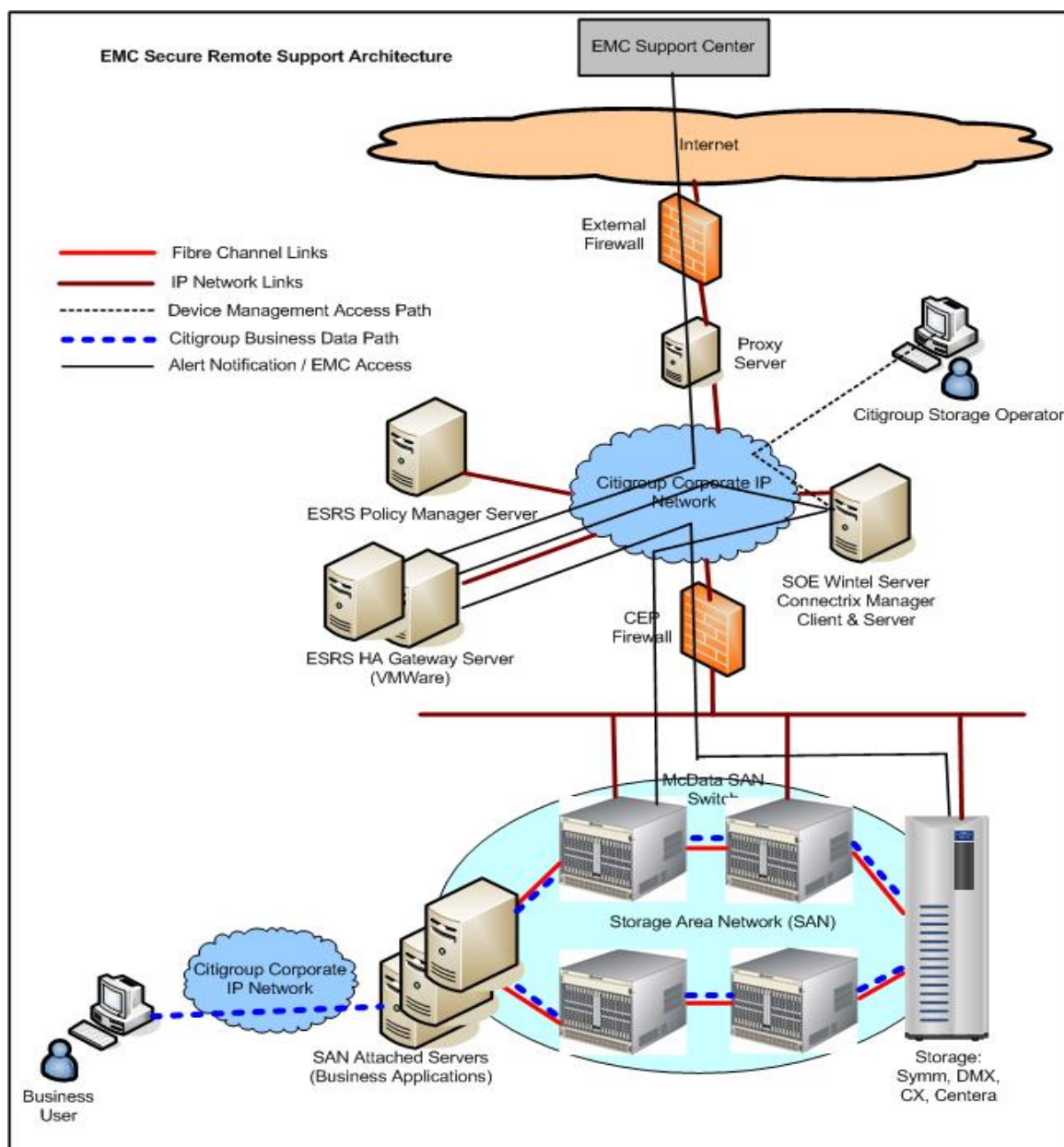
4.9. Element Manager License Key Entry

In order to enable Element Manager features, a license string must be entered. To enter the license key for the Element Manager, use the following steps:

- Go to the Element Manager view of the individual switch or switches that are being enabled. Use the Configure pull-down menu and select Features.
- Once the *Features* window is up, select *New* to add a new Feature. This will bring up the *New Feature Key* window so that the license key can be entered.
- After the Key has been entered, click the OK button.

5. IP Network Architecture

When the fibre channel switches are running E/OS 06.01.00 or higher, the fibre channel switches should be given routable IP addresses. This would allow management solutions to manage the environment through the Connectrix Manager. This topology is illustrated in the following figure.



5.1. Firewall Rules

With Connectrix Manager Server running on a Citi SOE Server on the Citi GDN, fewer CEP firewall rules are required.

1. For Connectrix Manager 9.1.1 running on an SOE server to communicate with the FC switches and IPS SAN routers, it must be able to communicate through the CEP firewall. Storage Operations must request a change in CEP firewall to allow Connectrix Mgr Server application traffic. Connectrix Mgr Server will require the following ports to be opened one-way to the target switches (Connectrix Mgr Server is the source):
 - o TCP port 2048 (Connectrix Mgr application)
 - o UDP port 161 (SNMP/Read)
 - o UDP port 123 (NTP/Read)

Note: If you're running Connectrix Manager Server on the EMC 1U CSP, not a Citi SOE build, then you'll need the following ports opened.

- o TCP port 5414 (EMCRemote/ Source: ESRS Gateway, Target: EMC 1U CSP)
 - o TCP port 51510/51511 (duplex traffic between CM Client and EMC 1U CSP)
2. SNMP TRAPs need to be permitted for monitoring. The required firewall rules are listed in the section "Monitoring the Switch".
 3. With Connectrix Manager Server running on an SOE server on the Citigroup GDN, there isn't a need for additional firewall settings for other SAN Management products such as SANScreen or ECC.

5.2. Vendor Remote Access

WWDS is no longer the preferred method for EMC to provide remote support to its storage devices. WWDS is being replaced with EMC Secure Remote Support Gateway. This product will provide Alert Notification, Vendor Remote Access and Audit Logging. The [ESRS Solution Guide](#) can be found on the GDSE [Vendor Remote Access](#) website.

EMC will use ESRS to connect to the Connectrix Manager Server (SOE) via EMCRemote. EMCRemote is required to be installed on the Citi Connectrix Manager Server (SOE).

A Process Control Manual ("PCM") will need to be developed by Regional Storage Operations teams to detail the vendor access process.

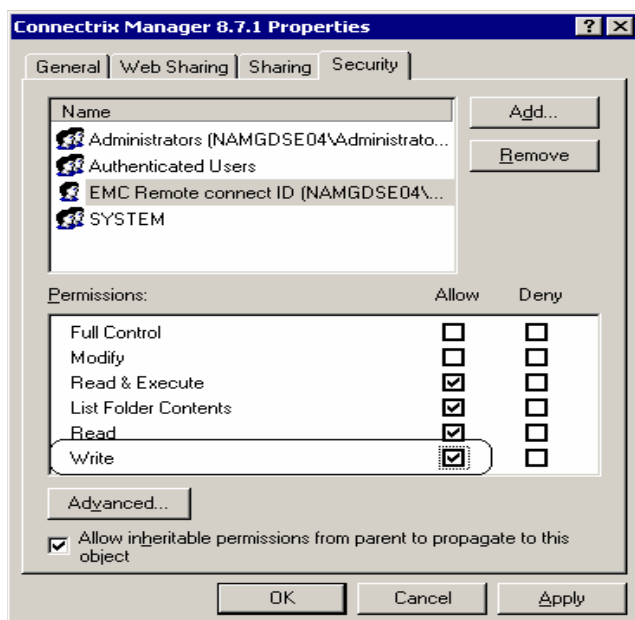
5.3. Vendor Functional User ID

The business owner, Storage Operations, is required to request a Local Functional ID from ISA for the vendor to use to login to the Connectrix Manager SOE Server for maintenance purposes. Use the [“Virtual Security Request”](#) system to request an ID from ISA. This ID should be the same for all Connectrix Manager SOE Servers and should reside in the default “User” group. It should have settings that disallow the user from changing the password and the password should never expire. Operations BISO approval may be required for this functional ID.

Detailed architecture for vendor remote access is described in Global Engineering’s “EMC Secure Remote Support Solution Guide” document. See [References](#) section for the location of this document.

5.4. Additional Vendor Functional User ID Permissions

The SPAC package installs the Connectrix Manager Server files in directory C:\Program Files\Connectrix Manager 9.1.1. The EMC vendor Local Functional User ID will need additional permissions for this directory, than the standard permissions that are default with an ID in the “User” group. The System Administrator is required to modify the permissions of the above folder, checking the “write” box. The default checked-boxes “read & exec”, “list folder contents” and “read” should remain checked (see below).



6. SANtegrity

The SANtegrity product is a licensed enabled feature in Connectrix Manager for enhancing the security of the McData FC switches. SANtegrity is designed to prevent both intentional and un-intentional problems from occurring on the fabric.

6.1. SANtegrity License Key Entry

In order to enable certain SANtegrity features (Fabric Bindings), a license string must be entered. To enter the license key for the SANtegrity product, use the following steps:

- Go to the Element Manager view of the individual switch or switches that are being enabled. Use the Configure pull-down menu and select Features.
- Once the *Features* window is up, select *New* to add a new Feature. This will bring up the *New Feature Key* window so that the license key can be entered.
- After the Key has been entered, click the *Ok* button.
- A new window will appear warning that the switch will IPL and have a momentary loss of LAN connectivity¹⁰. Select the *Yes* button on the warning screen.
- At this point the switch may quit responding (Ethernet only) for a few seconds and the status may show link down but it will come back to operational.

Once the license is entered, the switch will have SANtegrity binding license enabled so that fabric bindings can be configured.

6.2. SANtegrity Port Bindings

For a secure SAN environment, Port bindings should be enabled and configured on all McData FC switches in Citigroup. Port Bindings are a Base product in Connectrix Manager and therefore do not require a SANtegrity license key.

Port Bindings are designed to block unauthorized connections to the McData FC switches. When enabled, port binding authorizes a switch port to accept connections from only one designated WWN. If a different WWN is attached to the port, the device will not be allowed to log into the fabric. This eliminates the threat of obtaining unauthorized access to SAN resources by copying (“spoofing”) the WWPN from an authorized host. This also prevents failures related to accidental connection of devices to the wrong switch port (ex: incorrect cross fabric ISL).

To enable Port Bindings go to the Element Manager view of the individual switches in Connectrix Manager. The following high-level steps will be covered in detail below.

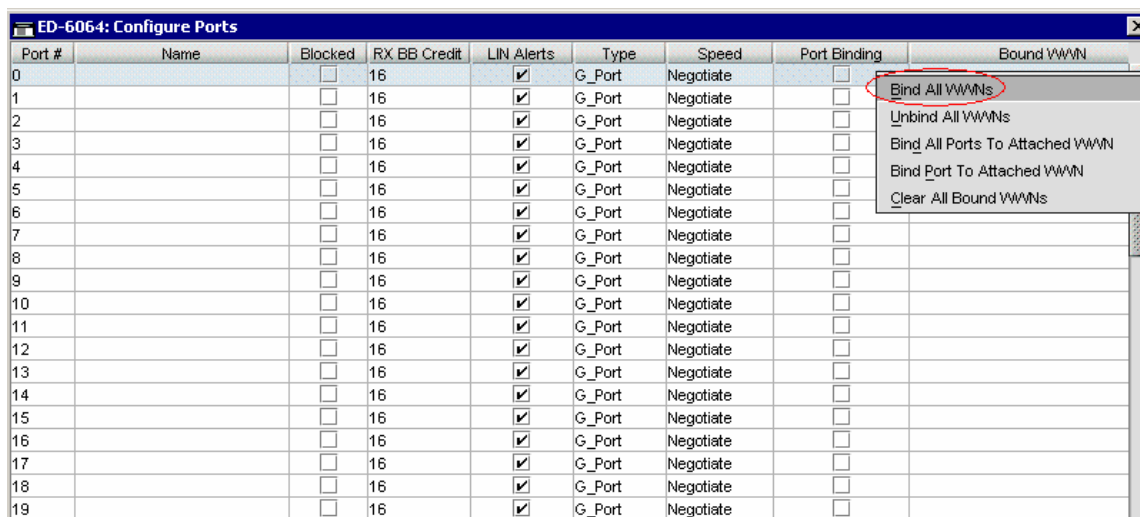
¹⁰ Only the Ethernet connection between the service processor and director is momentarily interrupted during an IPL. This will not disrupt Fibre Channel traffic like an IML would.

- Validate that all WWNs currently logged into the switch are valid.
- Validate that WWNs that are not currently logged into the switch that will (servers or storage that is down at the time bindings are enable) be enabled are valid.
- Bind all WWNs.
- Bind all ports to attached WWNs.
- Manually bind any WWNs of servers that may have been down when port bindings were enabled for the entire switch. (Optional)

A manual validation must be done before port bindings are initially enabled to make sure that an invalid WWN is not granted permanent access to the SAN. The administrator should validate that all WWNs that will attach (from servers or storage that is down), and that are currently attached to the switch, are WWNs that come from known servers, storage, or switches. The administrator should also validate that there are no duplicate WWNs (spoofed WWNs).

After the WWN validation is done for a switch, the administrator then needs to bind all WWNs on the switch to a port. To enable port bindings for all existing ports on the switch, the administrator needs to do the following:

- From the main view of Connectrix Manager, and call up the individual switch that will get the Port Bindings enabled.
- At the Element Manager view of the individual switch, click the Configure pull-down menu and select Ports.
- On the *Configure Ports* window (shown below), *right click* in the *Port Binding* column for port 0 outside of the port binding check box and then select Bind All WWNs from the pull-down menu as shown in figure below.



- After the Bind All WWNs option has been selected, the check box for each port in the *Port Binding* column will now be checked as shown in the figure below.

- Now *right click* in the port 0 *Port Binding* column again (outside the checkbox) and select *Bind All Ports To Attached WWN* from the pull-down menu.
- Now the *Bound WWN* column will have either a WWN or a WWN alias listed for all ports that have a fibre cable plugged in as shown in the figure below.
- If there is no cable plugged into a port, there will be nothing in the *Bound WWN* column as shown in figure below. In this case the port is actually bound to NULL and no cable would be allowed to plug into that port and log into the fabric until the port binding for that port is unbound.

Port #	Name	Blocked	RX BB Credit	LIN Alerts	Type	Speed	Port Binding	Bound WWN
22		☐	16	☒	G_Port	Negotiate	☒	
23		☐	16	☒	G_Port	Negotiate	☒	
24		☐	16	☒	G_Port	Negotiate	☒	50060482BFD22543
25		☐	16	☒	G_Port	Negotiate	☒	50060482BFD2254C
26		☐	16	☒	G_Port	Negotiate	☒	50060482BFD2254D
27	ISL to East Lab	☐	16	☒	G_Port	Negotiate	☒	10000000C94CAE48
28	388GX01ED_3A_P1	☐	16	☒	G_Port	Negotiate	☒	50060485C5EDBBE2
29		☐	16	☒	G_Port	Negotiate	☒	50060E800427D000
30		☐	16	☒	G_Port	Negotiate	☒	50060485C5EDBA32
31		☐	16	☒	G_Port	Negotiate	☒	1000080088A03230
32		☐	16	☒	G_Port	Negotiate	☒	5006016808202C90
33		☐	16	☒	G_Port	Negotiate	☒	5006048DC5EDBBCD
34		☐	16	☒	G_Port	Negotiate	☒	50060482BFD22543
35	isl1	☐	16	☒	G_Port	Negotiate	☒	1000080088A0D662
36		☐	16	☒	G_Port	Negotiate	☒	5006016108202C90
37		☐	16	☒	G_Port	Negotiate	☒	50060485C5EDBBCD
38		☐	16	☒	G_Port	Negotiate	☒	50060482C3A38E43
39	isl2	☐	16	☒	G_Port	Negotiate	☒	1000080088A0D662
40		☐	16	☒	G_Port	Negotiate	☒	50060161106005D9
41		☐	16	☒	G_Port	Negotiate	☒	5006048DC5EDBBC2

- At this point, press *Activate* and the bindings will take place and the *Configure Ports* screen will go away.

Now all ports that were logged in on the switch are bound to one of the following:

- A 64-bit WWPN (if no alias is assigned to the WWPN that is logged in)
- A WWPN Alias (if an alias is assigned to the WWPN that is logged in)
- NULL (if no cable is plugged into the switch port)¹¹
- A WWNN or WWNN Alias (if the port has an ISL plugged into it)

Even if the port has nothing plugged in, any attempt to plug in new cables without first unbinding the port will be denied. The port is bound to NULL, which will not match any WWPN that attempts to log into that port.

The administrator now needs to manually bind any server or storage that could have been down at the time the bindings were enabled. Failure to do this step would not allow any server or storage that was down during the time bindings were enabled, to log into the SAN when they come back. The steps for doing this are as follows:

¹¹ The Bound WWN column will not actually show the word "NULL", but at the E/OS level the port will be bound to nothing so that no WWN can be plugged in without unbinding the port.

- Call the *Configure Ports* screen up again and go to the port that has a fibre cable plugged in that is not logged in because the server or storage is currently down, and was down during the Port Bindings.
- Manually enter the WWPN or the WWPN alias in the *Bound WWN* column and hit the activate button as shown in figure below.

#	Name	Blocked	RX BB Credit	LIN Alerts	Type	Speed	Port Binding	Bound WWN
		☐	16	☒	G_Port	Negotiate	☒	
		☐	16	☒	G_Port	Negotiate	☒	
		☐	16	☒	G_Port	Negotiate	☒	50060482BFD22543
		☐	16	☒	G_Port	Negotiate	☒	50060482BFD2254C
		☐	16	☒	G_Port	Negotiate	☒	50060482BFD2254D
	ISL to East Lab	☐	16	☒	G_Port	Negotiate	☒	10000000C94CAE48
	388GX01ED_3A_P1	☐	16	☒	G_Port	Negotiate	☒	50060485C5EDBBE2
		☐	16	☒	G_Port	Negotiate	☒	50060E800427D000
		☐	16	☒	G_Port	Negotiate	☒	50060485C5EDBA32
		☐	16	☒	G_Port	Negotiate	☒	1000080088A03230
		☐	16	☒	G_Port	Negotiate	☒	5006016808202C90
		☐	16	☒	G_Port	Negotiate	☒	5006048DC5EDBBCD
		☐	16	☒	G_Port	Negotiate	☒	50060482BFD22543
	isl1	☐	16	☒	G_Port	Negotiate	☒	1000080088A0D662
		☐	16	☒	G_Port	Negotiate	☒	5006016108202C90
		☐	16	☒	G_Port	Negotiate	☒	50060485C5EDBBCD
		☐	16	☒	G_Port	Negotiate	☒	50060482C3A38E43
	isl2	☐	16	☒	G_Port	Negotiate	☒	1000080088A0D662
		☐	16	☒	G_Port	Negotiate	☒	50060161106005D9
		☐	16	☒	G_Port	Negotiate	☒	5006048DC5EDBBC2
		☐	16	☒	G_Port	Negotiate	☒	50060482C3A38E43

Now if this server were to come back online, the port would allow it to log into the SAN. If this step is not taken, the port will have to be unbound and then rebound once the server comes back up before it will be allowed to log into the SAN.

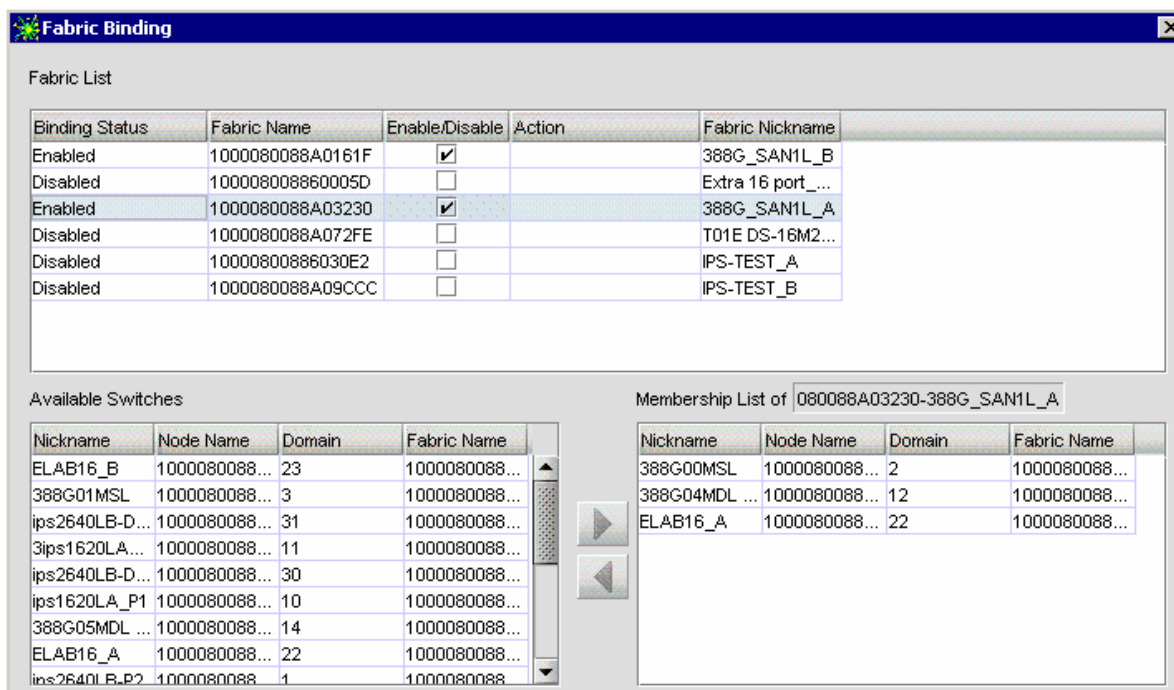
6.3. SANtegrity Fabric Bindings

For a secure SAN environment, Fabric Bindings should be enabled and configured on all McData FC switches. Before configuring fabric bindings for a fabric, the storage administrator must go to every switch in that fabric and [enter the SANtegrity license string](#).

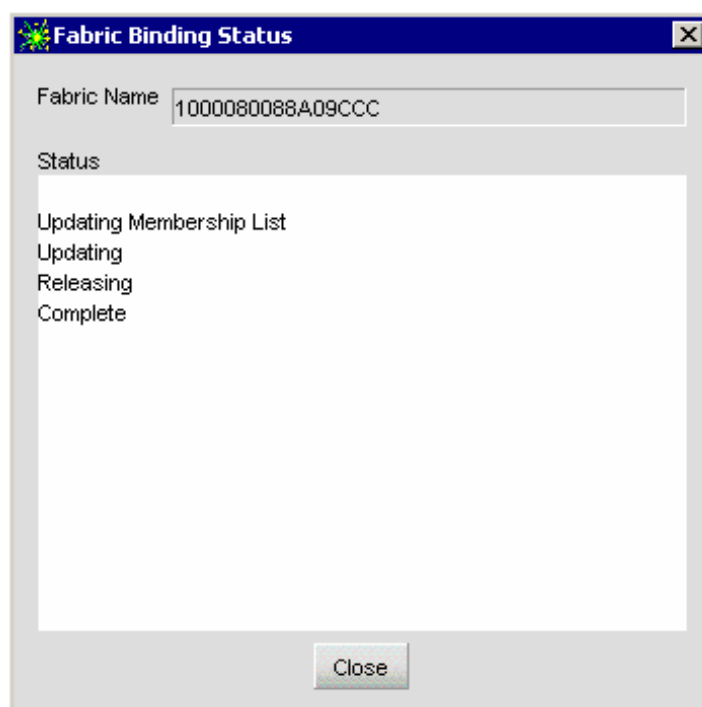
Fabric Bindings are designed to block unauthorized switches from joining an existing fabric via Inner Switch Links (E_Port Spoofing). Fabric bindings will also eliminate accidental fabric merges due to cabling mistakes. To enable Fabric Bindings, use the following steps:

- From the main Connectrix Manager window, Click on a persisted fabric that is going to have fabric bindings enabled.
- Select the *Configure* pull-down menu and select *Fabric Bindings*.
- When the *Fabric Binding* window appears, check the *Enable Fabric Binding* check box.

- The *Membership List* should contain all of the switches in the selected fabric, if not, then move them from the available switches to the membership list as shown in the figure below.



- Click OK. The *Fabric Binding Status* window will appear as shown in the figure below.



This process needs to be repeated for each fabric (multi or single switch) on the main Connectrix Manager view.

6.4. SANtegrity Operational Changes

Once SANtegrity Bindings are implemented at the port and fabric level, the normal Operations procedures for plugging new connections into the switch will change. The following sections will list and document these operational changes.

6.5. Adding New Storage/Server Connections to a Switch

Prior to SANtegrity when an administrator wanted to plug new storage or server connections into the SAN, the administrator only needed to plug the new cables into the switches and let the device login to the fabric. With port bindings enabled, if an administrator were to try and do this on an empty port, the connection would not login, and the port properties would show that there are binding errors as shown in the figure below.

ED-6064: Port Properties	
Port Number	41
Port Name	
Type	G_Port
Technology	Single mode 9 um ,Longwave Laser LC
Operating Speed	Not Established
Fibre Channel Address	__2D__
Port WWN	McDATA-202D080088A04C8A
Attached Port WWN	Not logged in
Block Configuration	Unblocked
10-100 km Configuration	Off
RX BB Credits Configured	16
NPIV Login Limit Configured	N/A
Logged in IDs	0
LIN Alerts Configuration	On
FAN Configuration	N/A
Beaconing	Off
Link Incident	None
Operational State	Invalid Attachment
Reason	Port binding violation - unauthorized wwn
Threshold Alert	

The new process for plugging a new server or storage fibre cable into the SAN will be as follows.

- Call up the *Element Manager* view of the switch, and select the Configure pull-down menu and then select Ports.
- Unbind the empty port by clearing the check box in the *Port Binding* column of the port in question, and then manually clearing any entry (if one exists) in the *Bound WWN* column, and then click the *Activate* button.
- Plug the new server or storage cable into the Port. With the bindings for that port turned off the connection should now log into the fabric.
- Manually validate the logged in WWN matches what is expected.
- Then *right click* in the *Port Binding column* for the port being bound and select *Bind Port to Attached WWN* from the pull down menu, then click the *Activate* button. This will only bind the port in question to the newly attached WWN.

6.6. Adding New Switches to the Fabric

The process of adding a new switch to an existing fabric will change with the additions of fabric bindings. Without fabric bindings, storage administrators only needed to add a new ISL from the new switch to the existing fabric, let the fabric rebuild, and then re-persist the fabric. If an administrator were to try this approach with Fabric and Port bindings enabled, the fabric would not merge and the ISL port would show a link alert with *Incompatible security attributes* for the *Reason* in the port properties as shown below.

ED-6064: Port Properties	
Port Number	41
Port Name	
Type	G_Port
Technology	Single mode 9 um ,Longwave Laser LC
Operating Speed	Not Established
Fibre Channel Address	_2D_
Port WWN	McDATA-202D080088A04C8A
Attached Port WWN	Not logged in
Block Configuration	Unblocked
10-100 km Configuration	Off
RX BB Credits Configured	16
NPIV Login Limit Configured	N/A
Logged in IDs	0
LIN Alerts Configuration	On
FAN Configuration	N/A
Beaconing	Off
Link Incident	None
Operational State	Invalid Attachment
Reason	Incompatible security attributes
Threshold Alert	
Zoning Enforcement	N/A

Close Help

The correct order for adding a new switch into an existing fabric with fabric and port bindings enabled is as follows.

- Add the new switch as a new managed object into the Connectrix Manager main view.
- Unbind the empty port on both the new and existing switch that will hold the ISL between the switches by clearing the check box in the *Port Binding* column on the *Configure Ports* screen, and clearing any entry in the *Bound WWN* Column.
- Call up the fabric bindings for the existing fabric where the new switch will be added and move the new switch into the fabric membership list.
- After the new switch is added into the existing fabric membership list, the administrator can now plug the new ISLs in and the fabric will merge with the new switch in the fabric.

- On both the new switch and the existing switch that holds the ISL from the new switch, a *Bind Port to Attached WWN* must be done on the ISL ports.
- Re-persist the fabric that should now include the new switch.

6.7. Adding Additional ISLs from Existing Switches

Adding an additional ISL from existing switches in a fabric would follow the same rules as adding new storage or server connections to the SAN except that the fabric would need to be re-persisted once the change is made. Adding a new ISL would not require any changes to the fabric bindings since the existing switches WWNs and Domain IDs would already be in the fabric membership lists. The steps would be as follows.

- Unbind the empty ports on each existing switch that will hold the new ISL by clearing the check box in the *Port Binding* column, and clearing any entries in the *Bound WWN* column.
- Plug the new ISL cable into the Ports on each switch. With the bindings for the ports turned off on both switches the connection should log into the fabric, and the fabric should rebuild.
- Then *Bind Port to Attached WWN* from the Port Bindings screen on each switch port that holds the new ISL. Bind only the port in question on each switch.
- Re-persist the fabric.

6.8. Removing Hosts from Switches

The procedure for removing a server from the SAN will change to include the port bindings functionality. Prior to SANtegrity, an administrator only needed to unplug a server from the SAN that would no longer require SAN connectivity. Due to the implementation of port bindings, the new procedure for removing servers from the SAN is as follows:

- Unbind the ports on each existing switch that currently holds the server or storage to be removed by clearing the check box in the *Port Binding* column, and clearing any entries in the *Bound WWN* column.
- Remove the server or storage fibre cable from the switch.
- Bind the switch port to nothing/NULL by checking the binding check box for the now empty port.

6.9. Removing ISLs from Switches

The following steps will explain how to remove an ISL from a switch that has multiple ISLs to the same location. If a source switch has multiple ISLs to a target switch and one needs to be removed, the fabric bindings will not come into play since the switch domain ID and WWN will still exist in the fabric membership list because of the ISLs that will not be removed.

Removing one of multiple ISLs to a target switch will only impact port bindings. To remove an ISL from a source switch that has multiple ISLs going to the same target switch follow these steps:

- Unbind the ports on each existing switch that currently hold the ISL that will be removed by clearing the check box in the *Port Binding* column, and clearing any entries in the *Bound WWN* column.
- Unplug the ISL cable on both the source and target switches. At this point the fabric should rebuild.
- Bind the now empty ports that held the ISL on both the source and target switches to nothing/NULL.
- Re-persist the fabric so that the fabric topology will be updated.

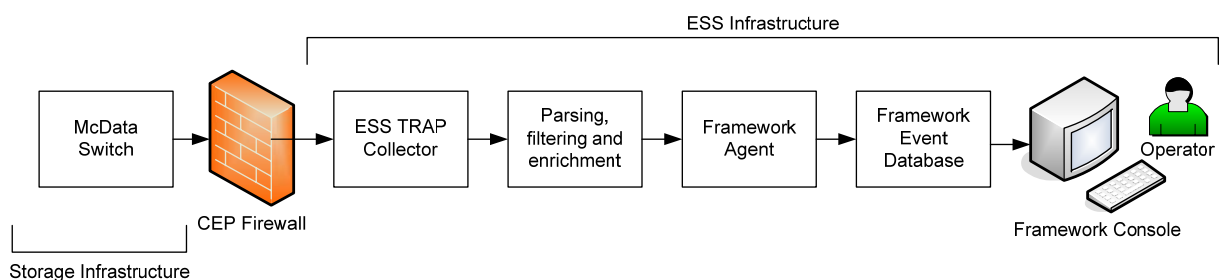
6.10. Removing Switches from a Fabric

The new process for removing a switch from a fabric will involve changes both in the Fabric and Port binding configurations. The new process for removing a switch from the fabric will be as follows:

- Unbind the ports on each existing switch that currently hold the ISL(s) that will be removed by clearing the check box in the *Port Binding* column, and clearing any entries in the *Bound WWN* column.
- Unplug the ISL(s) cable from both the associated switches. The fabric will rebuild at this point.
- Remove the switch from the fabric membership list in the Fabric Bindings for the fabric where the switch will be removed.
- Re-persist the fabric to update the topology for the fabric.
- Bind the now empty ports that held the ISL to nothing/NULL.
- On the switch that was removed, clear all of the switch names that are no longer in the fabric with it. Then disable Fabric Bindings on the switch by clearing the checkbox for that switch at the first Fabric Binding screen.

7. Monitoring the Switch

This section covers the installation, configuration and operation of a Simple Network Management Protocol ("SNMP") based monitoring solution for McData switches. The switches can be monitored 24x7 and problems such as exceptionally high utilization of links and hardware failures can be alerted to Storage Operations personnel in near real time that can help in preventing catastrophic failures. Citigroup standard monitoring framework called Enterprise Systems Services ("ESS") can be used to capture, process and display the alerts.



SNMP TRAPs generated by McData switches will be collected by an ESS TRAP collector server. These will then be parsed, filtered and enriched. The framework agent will then gather the processed events and report these to the console. The console will be monitored 24x7 by the Console Operator(s). A Process Control Manual (“PCM”) developed by Regional Storage Operations teams will direct the Console Operator to deal with alerts that show up on the console. Another PCM developed by Regional Storage Operations team will direct Storage Operator actions against all possible alerts.

7.1. Comparison of Monitoring Solutions

The overall goal of the solution is to increase the availability of the McData SAN environment. The following objectives must be met:

- ✓ Near real-time alerting of hardware failures
- ✓ Near real-time alerting of link utilization threshold exceeded
- ✓ Minimize the number of spurious alerts
- ✓ Maximize the information contained within the alert so that decisions can be made quickly

Monitoring via McData switch, Connectrix Manager, EMC Control Center and SANScreen were considered as alternatives.

Concern	Measure	SNMP traps to ESS from Connectrix Service Processor	SNMP traps to ESS from McData director or switch	SNMP traps to ESS from San Screen	SNMP traps to ESS from ECC Integration Gateway
How quickly will someone know of a problem?	Time between the occurring of an event within the device and showing up of an alert on an ESS console	Almost instantly	Almost instantly	San Screen polling cycle = 15 minutes	FCC agent polling cycle + repository polling cycle + integration gateway polling cycle. With default settings, this is around 1 hour.
How reliable is the	Number of systems that	Points of	Points of	Points of	Points of

Concern	Measure	SNMP traps to ESS from Connectrix Service Processor	SNMP traps to ESS from McData director or switch	SNMP traps to ESS from San Screen	SNMP traps to ESS from ECC Integration Gateway
monitoring going to be?	can fail and prevent events from being reported	failure = 1: Connectrix Service Processor	failure = 0 (Most reliable)	failure = 3: Connectrix Manager, RAU, San Screen	failure = 4: Connectrix Manager, FCC agent, repository, Integration gateway (least reliable)
What types of problems will be captured by this system?	FRU failures	Fan, Power	Fan, Power, CTP, Sbar	None	Unknown
	Port utilization exceeded a configurable threshold	No	Yes	Unknown	Yes
	Port failure	Yes	Yes	No	Yes
	Bit error rate on a link exceeded allowed threshold (this will catch failing optics or cabling)	No	Yes	No	No
	CTP failover	No	Yes	No	No
	Fibre channel primitive sequence errors	No	Yes	No	No
	Host to LUN logical path failure	No	No	Yes	Yes
	Performance problems based on collection and analysis of data over a period of time and comparison to baseline	No	No	No	Yes
	Engineering Effort	ESS engineering effort	ESS engineering effort	ESS engineering effort	ESS engineering effort + certify Fibrezone, FCC agent, Integration gateway (approx. 8 weeks for GDSE)

Concern	Measure	SNMP traps to ESS from Connectrix Service Processor	SNMP traps to ESS from McData director or switch	SNMP traps to ESS from San Screen	SNMP traps to ESS from ECC Integration Gateway
How fast can we implement this system?	Implementation Effort	ESS integration effort	ESS integration effort	ESS integration effort	ESS integration effort + install FibreZone on CSP + Deploy ECC + Deploy FCC agent + Deploy Integration Gateway + Configure data collection policies (approx. 12 weeks for NA)

From the above comparison, it is clear that using SNMP TRAPs from McData switches is the best option.

7.2. Implementation Steps

- ✓ Meet solution prerequisites
- ✓ Partner with regional ESS Engineering/Integration team. ESS will configure the TRAP collector server(s), parsing, filtering, enrichment and make sure that alerts are reported to the Console. At this time there is no global function for ESS; regions should engage their respective ESS team:

Region	ESS Technologies	Owner
APPC	BMC Patrol	Jit-Soon Koh
Mexico	HP Openview, MOM	Alfonso Diaz Jimenez
EMEA	Tivoli, Ice	Sean Lonegran
Japan	Tivoli, Ice	Carl Pickin
NA	Tivoli, Ice, NetIQ, MOM, HP Openview	Roger Kutchaver

Storage Engineering worked with Roger Kutchaver's team to develop this solution.

- ✓ Configure the CEP firewall
- ✓ Configure the McData Switches
- ✓ Test the System

Each step is detailed in the following sections.

7.3. Prerequisites

7.3.1. Fault Management Process

The fault management process for McData switches is currently owned and operated by the vendor. With the implementation of this solution, Citigroup would be required to own and staff a parallel process. Regional Storage Operations teams are expected to build, resource, operate and monitor the following. **These are recommendations only; Operations should implement what works best for them.**

1. A process to receive and act upon the alerts that will be seen by the Console Operator:
 - a. List of personnel that will be alerted
 - b. How they will be alerted (pager, email, etc.)
 - c. What happens if the paged person does not acknowledge the alert
 - d. What steps the person must follow on receiving the alert (log a trouble ticket, alert manager, call vendor, carry out diagnosis, etc.)
 - e. When and how will the alert be cleared from the Console
2. A SLA should be established with the Console Operator. This SLA will set expectations of both departments and provide justification for Console Operator resources. Example issues that can be addressed in this SLA include:
 - a. Operating hours – one, two or all three shifts
 - b. Response time - time from when the Operator sees the alert and paging of Storage person
 - c. Procedure to update contact lists and escalation path
 - d. Point person from each team responsible for the interaction
3. A SLA should be established with ESS Integration department. This should address things like adding devices, reconfiguring filtering or mapping, as well as availability and performance guarantee of ESS systems.
4. A process to periodically test the system by administratively triggering alerts
5. A process to periodically analyze historical fault data to comment on:
 - a. McData switch product reliability
 - b. Avoided outages (this would help justify the cost of the monitoring system)
 - c. Response performance of Storage Operations to faults
 - d. Response performance of vendor to faults

7.3.2. E/OS Version

All McData switches that will be monitored must be at E/OS level 6 or higher.

7.3.3. IP Network Requirements

Please refer to the “IP Network Architecture” section within this document. McData switches should be connected to a routable IP network such that UDP packets (SNMP TRAPS) can be sent to ESS TRAP collector server. If the McData switches are on a private IP network, Connectrix Manager 9.1.1 built-in TRAP forwarder can be used as a gap solution. This TRAP forwarder will capture TRAPS from the private IP network connected McData switches and forward these to the ESS TRAP collector over the corporate network. Use the Connectrix Manager GUI to enable TRAP forwarding. Provide the IP address of the ESS TRAP collector. Please note that having the McData switches on a private IP network reduces the benefits from monitoring as detailed in the “Known Issues with Monitoring” section, and therefore Operations should plan to move the switches to a routable IP network as soon as possible.

7.4. McData SNMP TRAP Capability Overview

McData switches are managed by Connectrix Manager software. Connectrix Manager has SNMP capabilities; it talks to McData switches using a proprietary protocol and generates SNMP v1 TRAPS that can be sent to ESS TRAP collector. Connectrix Manager version 8.x and 9.x implement the fcmgmt v3.1 (enterprise ID 1.3.6.1.2.1.8888) MIB and are capable of generating 5 specific TRAPS.

McData switches are themselves capable of generating SNMP v1 TRAPS in addition to Connectrix Manager without Connectrix Manager’s help. Switches running E/OS 6.x or higher implement the fceos (enterprise ID 1.3.6.1.4.1.289) MIB as well as the fcmgmt MIB. The fceos MIB defines 15 TRAPS. Combined with the 5 TRAPS defined within the fcmgmt v3.1 MIB, the McData switch produces 20 TRAPS in all.

7.4.1. Port Status Monitoring

Port status change, such as port going online or offline, is covered by both fceos and fcmgmt MIBs. However, fcmgmt provides a more detailed status. For example, unconnected ports are reported as “ready, offline” as compared to just “offline” reported by fceos. Fcmgmt also generates TRAP for administrative port shutdown through the “Block Port” feature of Connectrix Manager GUI, which can be used as a test tool in a production environment when used with unused ports.

Port status TRAPS cannot be enabled or disabled at the McData switch level. Because these TRAPS are also generated when hosts connected to the switch are powered

down or rebooted, Storage Engineering's recommendation is to filter out (or report as "Informational") all port status TRAPs within the ESS infrastructure.

7.4.2. *Link Status Monitoring*

Link status monitoring is only available within the fceos MIB, and therefore the McData switch only. Link status includes port status change notification. One notable event within the link status TRAP group is bit error rate exceeded threshold.

Link status monitoring is disabled by default. It cannot be enabled with Connectrix Manager, or even by using the switch command line interface. It can only be enabled by using third party SNMP manager software. Regions should contact their local EMC representative to have link alerts enabled for selected ports¹². Storage Engineering recommends that these alerts be enabled for all storage connected as well as ISL ports. As and when link alerts are enabled, these will start appearing on the Console without needing any other configuration changes within the storage, firewall or ESS infrastructure.

7.4.3. *Field Replaceable Unit Monitoring*

Field Replaceable Units ("FRU") are hardware components such as power supply, fan, CTP, etc. that can be replaced at the customer's premise. Fceos MIB provides full coverage of all FRUs, whereas the fcmgmt only monitors fan and power. Fceos monitoring includes administratively initiated actions such as CTP or SBAR failover and therefore can be used for testing.

7.4.4. *Link Utilization Threshold Monitoring*

Link utilization monitoring is only available within the fceos MIB, and therefore the McData switch. Per port receive, transmit or receive+transmit thresholds can be programmed using the Connectrix Manager, Element Manger GUI.

7.5. *Configuration*

7.5.1. *Switch Name*

Some fceos TRAPs report the name of the switch as programmed through the Connectrix Manager, Element Manager GUI, Configure Identification menu option, in addition to the IP address of the switch. Storage Operations should therefore program a unique name for every switch that will help locate the switch and/or its management station.

¹² Leaf 1113. 1.3.6.1.4.1.289.2.1.1.2.3.1.1.140 within the fceos MIB must be set to "1" for each port to enable its link alert. EMC representatives can contact GDSE for further clarification if required.

7.5.2. Switch SNMP Agent

Each switch must be configured to send SNMP TRAPs to the ESS TRAP collector using community “public” on port 162. If the switches are connected to a private IP network, the switch must be configured to send TRAPs to a TRAP forwarding station. A sample configuration is shown below.

Community Name	Write Authorization	Trap Recipient	UDP Port Number
public	☐	10.3.1.1	162
	☐		
	☐		
	☐		
	☐		
	☐		

7.5.3. Threshold Settings

The following table captures Storage Engineering’s recommendations for utilization alerts.

Port Type	Threshold Type	Utilization	For cumulative minutes or more	Notification Interval	Notes
Connected to host					Not used – covered by ISL alert since all host traffic will go over ISL
ISL	Receive and Transmit	90%	30 minutes	120 minutes	This can be fine tuned post implementation
Connected to storage					Not used – covered by ISL alert since all storage traffic will go over ISL

E/OS allows multiple threshold rules. Each threshold rule can service one or more ports. One TRAP is sent out for each port and for each rule. Thus if there were two rules, and each rule had five ports that were being monitored, a total of ten TRAPs will be sent when the conditions specified in the rules are met.

E/OS provides adequate controls to prevent alerting on traffic spikes. There are also controls to prevent repeating of alerts when condition persists. The “cumulative minutes” parameter specifies the time over which the traffic would be averaged, which helps eliminate alerting on spikes. TRAPs are generated as soon as the condition is met, but not repeated even if condition continues to persist for as long as the time specified in the “notification interval” parameter.

With Storage Engineering’s recommended settings, TRAPs will not be issued until utilization is in excess of 90% averaged over 30 minutes. TRAP(s) would be sent out immediately if this condition is met. TRAPs will not be sent for another 120 minutes. Thereafter TRAP(s) would be sent out again if the condition persists.

Each TRAP carries two parameters: the impacted port and the rule number that is triggering the TRAP. Please remember that the port numbering within the MIB starts from 1 as opposed to 0 within Connectrix Manager GUI. Thus “1” should be subtracted from the reported port number to match with Connectrix Manager. Alternatively, ESS TRAP processing can make the correction before presenting the alert on the Console.

7.6. Filtering Recommendations

A list of all possible TRAPs with categorization and filtering recommendations is provided below. These recommendations must be implemented within the ESS infrastructure.

7.6.1. FCEOS MIB (enterprise ID 1.3.6.1.4.1.289)

TRAP Specific Type	GDSE Filtering Recommendation	Trap Name	Description	Trap Variable	Variable OID	Type	Variable Values
1	Filter out: host ports will generate too many of these	fcEOSPortScn	Is generated whenever a Fc_Port changes its operational state. For instance, the Fc_Port goes from on-line to offline.	fcEOSPortOpStatus	1.3.6.1.4.1.289.2.1.1.2.3.1.1.3	Integer	1: online 2: offline 3: testing 4: faulty

TRAP Specific Type	GDSE Filtering Recommendation	Trap Name	Description	Trap Variable	Variable OID	Type	Variable Values
2	Filter out: covered by other TRAPs	fcEosFruScn	Generated when FRU operational state changes	fcEosFruStatus	1.3.6.1.4.1.289.2.1.1.2.2.1.1.3	Integer	0: unknown 1: active 2: backup - backup module is being used 3: update-busy 4: failed
3	Filter out: not aligned with availability goal	fcEosPortBindingViolation	Generated when a port binding violation occurs	fcEosPortAttachedWWN	1.3.6.1.4.1.289.2.1.1.2.4.1.1.4	Octet String	WWN of the device attached to the port. Example: 50 06 04 8d c5 ed bb c3
4	Critical	fcEosThresholdAlert	Generated when threshold is exceeded	fcEosPortIndex	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1	Integer	1 to max physical ports supported on the switch
				fcEosTALIndex	1.3.6.1.4.1.289.2.1.1.2.6.1.1.1	Integer	Not all McData switch models support this variable. For models that do support it, this is the rule number that is triggering the TRAP.
5	Critical	fcEosFruRemoved	Generated when a FRU is removed or its status changes to unknown	fcEosFruCode	1.3.6.1.4.1.289.2.1.1.2.2.1.1.1	Integer	FRU code of the device
				fcEosFruPosition	1.3.6.1.4.1.289.2.1.1.2.2.1.1.2	Index	1 to max cards on the device
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Name configured by user
				fcEosSysSwitchId	1.3.6.1.4.1.289.2.1.1.2.1.16	Octet String	WWN of the switch. Example: 10 00 08 00 88 60 30 e2
6	Inform	fcEosFruActive	Generated when a FRU status changes to active	fcEosFruCode	1.3.6.1.4.1.289.2.1.1.2.2.1.1.1	Integer	FRU code of the device
				fcEosFruPosition	1.3.6.1.4.1.289.2.1.1.2.2.1.1.2	Index	1 to max cards on the device
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Name configured by user
				fcEosSysSwitchId	1.3.6.1.4.1.289.2.1.1.2.1.16	Octet String	WWN of the switch. Example: 10 00 08 00 88 60 30 e2
7	Warning	fcEosFruBackup	Generated when a FRU status changes to backup	fcEosFruCode	1.3.6.1.4.1.289.2.1.1.2.2.1.1.1	Integer	FRU code of the device

TRAP Specific Type	GDSE Filtering Recommendation	Trap Name	Description	Trap Variable	Variable OID	Type	Variable Values
				fcEosFruPosition	1.3.6.1.4.1.289.2.1.1.2.2.1.1.2	Index	1 to max cards on the device
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Name configured by user
				fcEosSysSwitchId	1.3.6.1.4.1.289.2.1.1.2.1.16	Octet String	WWN of the switch. Example: 10 00 08 00 88 60 30 e2
8	Inform	fcEosFruUpdate	Generated when a FRU status changes to update/busy	fcEosFruCode	1.3.6.1.4.1.289.2.1.1.2.2.1.1.1	Integer	FRU code of the device
				fcEosFruPosition	1.3.6.1.4.1.289.2.1.1.2.2.1.1.2	Index	1 to max cards on the device
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Switch name configured by user
				fcEosSysSwitchId	1.3.6.1.4.1.289.2.1.1.2.1.16	Octet String	WWN of the switch. Example: 10 00 08 00 88 60 30 e2
9	Critical	fcEosFruFailed	Generated when a FRU status changes to failed	fcEosFruCode	1.3.6.1.4.1.289.2.1.1.2.2.1.1.1	Integer	FRU code of the device
				fcEosFruPosition	1.3.6.1.4.1.289.2.1.1.2.2.1.1.2	Index	1 to max cards on the device
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Name configured by user
				fcEosSysSwitchId	1.3.6.1.4.1.289.2.1.1.2.1.16	Octet String	WWN of the switch. Example: 10 00 08 00 88 60 30 e2
10	Critical	fcEosLinkBitErrorEvent	Generated when the bit error rate for a link exceeds threshold	fcEosPortIndex	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1	Integer	1 to max physical ports supported on the switch
				fcEosPortName	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1 52	String	The alias name assigned to the port by the user
				fcEosPortWWN	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1 53	Octet String	WWN of the switch port. Example: 20 04 08 00 88 60 30 e2
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Switch name configured by user
11	Critical	fcEosLinkNoSignalEvent	Generated when there is a loss of signal or sync	fcEosPortIndex	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1	Integer	1 to max physical ports supported on the switch
				fcEosPortName	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1 52	String	The alias name assigned to the port by the user

TRAP Specific Type	GDSE Filtering Recommendation	Trap Name	Description	Trap Variable	Variable OID	Type	Variable Values
				fcEosPortWWN	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.53	Octet String	WWN of the switch port. Example: 20 04 08 00 88 60 30 e2
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Switch name configured by user
12	Critical	fcEosLinkNOSEvent	Generated when a not operational primitive sequence is received	fcEosPortIndex	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1	Integer	1 to max physical ports supported on the switch
				fcEosPortName	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.52	String	The alias name assigned to the port by the user
				fcEosPortWWN	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.53	Octet String	WWN of the switch port. Example: 20 04 08 00 88 60 30 e2
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Switch name configured by user
13	Critical	fcEosLinkFailureEvent	Generated when a primitive sequence timeout occurs	fcEosPortIndex	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1	Integer	1 to max physical ports supported on the switch
				fcEosPortName	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.52	String	The alias name assigned to the port by the user
				fcEosPortWWN	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.53	Octet String	WWN of the switch port. Example: 20 04 08 00 88 60 30 e2
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Switch name configured by user
14	Critical	fcEosLinkInvalidEvent	Generated when an invalid primitive sequence is detected	fcEosPortIndex	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1	Integer	1 to max physical ports supported on the switch
				fcEosPortName	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.52	String	The alias name assigned to the port by the user
				fcEosPortWWN	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.53	Octet String	WWN of the switch port. Example: 20 04 08 00 88 60 30 e2
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Switch name configured by user
15	Filter out: not aligned with the availability goal	fcEosLinkAddedEvent	Generated when the firmware detects that a new connection has been established on a port	fcEosPortIndex	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1	Integer	1 to max physical ports supported on the switch

TRAP Specific Type	GDSE Filtering Recommendation	Trap Name	Description	Trap Variable	Variable OID	Type	Variable Values
				fcEosPortName	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.52	String	The alias name assigned to the port by the user
				fcEosPortWWN	1.3.6.1.4.1.289.2.1.1.2.3.1.1.1.53	Octet String	WWN of the switch port. Example: 20 04 08 00 88 60 30 e2
				fcEosSysSwitchName	1.3.6.1.4.1.289.2.1.1.2.1.15	String	Switch name configured by user

7.6.2. FCMGMT v3.1 MIB (enterprise ID 1.3.6.1.2.1.8888)

TRAP Specific Type	GDSE Filtering Recommendation	Trap Name	Description	Trap Variable	Variable OID	Type	Variable Values
1	Filter out	connUnitStatusChange	The overall status of the connectivity unit has changed	connUnitStatus	.mib-2.8888.1.1.3.1.6	Integer	1: unknown 2: unused - cannot report status 3: ok - available for meaningful work 4: warning - something needs attention 5: failed - something has failed
				connUnitState	.mib-2.8888.1.1.3.1.5	Integer	1: unknown 2: online - available for meaningful work 3: offline - unavailable for meaningful work, for example in self-test mode, configuration, etc.
2	Filter out	connUnitDeletedTrap	A connUnit has been deleted from this agent	connUnitGlobalID	.mib-2.8888.1.1.3.1.2	Integer	The unique identification for this connectivity unit among those within this proxy domain
3	Filter out	connUnitEventTrap	An event has been generated by the connectivity unit.	connUnitEventID	.mib-2.8888.1.1.7.1.1		The internal event ID. Incremented for each event, ranging between 1 and connUnitMaxEvents
				connUnitEventType	.mib-2.8888.1.1.7.1.5	Integer	1: unknown 2: other 3: status 4: configuration 5: topology
				connUnitEventObject	.mib-2.8888.1.1.7.1.6	OID String	This is used with connEventType to identify which object the event refers to. Examples are connUnitPortStatus, connUnitPortIndex,

TRAP Specific Type	GDSE Filtering Recommendation	Trap Name	Description	Trap Variable	Variable OID	Type	Variable Values
							connUnitStatus.commUnitId, etc.
				connUnitEventDescr	.mib-2.8888.1.1.7.1.7	String	The description of the event
4	Filter out	connUnitSensorStatusChange	An event has been generated by the connectivity unit.	connUnitSensorStatus	.mib-2.8888.1.1.5.1.3	Integer	1: unknown 2: other - the sensor indicates other than ok, warning or failure 3: ok - the sensor indicates ok 4: warning - the sensor indicates a warning 5: failed - the sensor indicates failure
5	Inform – used for test case (block/unblock port)	connUnitPortStatusChange	The overall status of the connectivity unit has changed	connUnitPortStatus	.mib-2.8888.1.1.6.1.6	Integer	1: unknown 2: unused - device cannot report this status 3: ready - FCAL loop of FCPH link reset protocol initialization has completed 4: warning - do not use 5: failure - do not use 6: not participating - loop not participating and does not have a loop address 7: initializing: protocol is proceeding 8: bypass - do not use 9: ols - FCP offline status
				connUnitPortState	.mib-2.8888.1.1.6.1.5	Integer	1: unknown 2: online - available for meaningful work 3: offline - not available for meaningful work 4: bypassed - no longer used 5: diagnostics

7.6.3. Enrichment Recommendations

Before the alert is displayed on an operator console and subsequently paged to Storage Operations personnel, it should be translated to an actionable message that is easily understood. The following are Storage Engineering recommendations for such translation. These would be implemented by ESS within the ESS infrastructure.

Object	TRAP Format	Recommended Console Format	Lookup Table
fcEosFruCode	FRU name is reported as an integer	Convert to FAN, POWER, CTP etc. by using a lookup table	1: Backplane 2: CTP 3: Sbar 4: Fan2 5: Fan 6: Power 12: Gsf2
Port Number	Switch port number is reported as an integer	Subtract 1 from the port number before reporting it to the console to match it with Connectrix Manager port number	

7.7. Firewall Changes

The firewall that isolates the McData switches and Connectrix Manager from the Corporate Network must be configured to allow the following:

Source IP	Destination IP	Protocol	Port	Traffic Description
McData switches and Connectrix Service Processor	ESS TRAP collector server(s)	UDP	162	SNMP TRAP
ESS TRAP collector server(s)	McData switches and Connectrix Service Processor	ICMP	Echo-request	PING

7.8. Heart Beat Monitoring

SNMP TRAPs are sent from the monitored device to the ESS infrastructure. If the device or the network connection between the device and the ESS infrastructure encounters a failure, no alerts will be received. To mitigate this risk, the ESS infrastructure should periodically ping each device that is being monitored, and alert if a reply is not received for a configurable number of retries.

If the McData switches are on a private network and TRAPs are being forwarded through the Connectrix Service Processor, ESS infrastructure will not be able to ping the switches. In this case, the ESS infrastructure should periodically ping the Connectrix Service Processor. Unfortunately, there is no way to heartbeat the switches; Connectrix Manager does not TRAP if it is not able to communicate with the switch for any reason. The only way to eliminate this gap in the monitoring solution is to move the McData switches to a routable IP network.

7.9. Testing

Because the TRAPs flow through several components, it is important that the regional Storage Operations team test the system as a part of the initial implementation. Thereafter, the test should be repeated every six months to assure continued operation of the system.

Testing in a production environment is a challenge because McData switches do not provide controls to generate TRAPs for testing purposes. Storage Engineering identified the following non-disruptive test cases that can be used during a scheduled maintenance window. One test case from each group (monitoring and heartbeat) is sufficient to fully test the integration.

7.9.1. Monitoring Test Cases

1. Identify an unconnected port on the switch. Block and unblock the port by using the Element Manager GUI. Alerts should show up on the ESS Console. Verify that the correct switch IP address is reported. Repeat this test for every switch.
2. Identify an E port that is carrying some traffic (use the performance view within the Element Manager). Set a low threshold that will trigger a utilization alert on that port. The alert should show up on the Console. Verify that the correct switch, switch port and rule number are reported. Repeat this test for every switch.

7.9.2. Heartbeat Test Case

This is only useful if the switches are on a routable IP network. Disconnect the switch from the IP network. A heart beat failed alert should be reported. Verify that the correct switch is reported.

7.10. Known Issues with Monitoring

- Port status change alerts are being categorized as “Informational” to prevent paging of Storage Personnel when SAN connected hosts are shutdown or rebooted¹³.
- If the switch is on a private network: Complete switch failure or IP network failure between Connectrix Service Processor and switch will be missed. This issue is resolved by moving the switch to a routable IP network.

¹³ ESS filters cannot distinguish between host connected ports and storage/ISL ports.

- If the switch is on a private network: Because private IP addresses may not be unique between SAN islands, alert message may fail to uniquely identify the problem switch¹⁴.
- OpenTrunking events are not a part of the fceos or fcmgmt MIB and will not be reported.
- Port numbering within the MIBs starts from 1 as opposed to 0 within Connectrix Manager. Please remember to subtract 1 from the reported port number to match with Connectrix Manager. Alternatively, ESS TRAP processing can subtract one from the port number before reporting it on the Console.

8. Upgrade Considerations

8.1. Storage Port Swaps

Upgrades to fabrics requiring that storage ports be moved from one switch to another must be carefully planned. This type of upgrade may be necessary when converting a 1-tier fabric to 2-tier, swapping a core switch for one with a higher port count, or when converting from a single to dual core fabric. Several server operating systems (AIX and HP-UX for example) may require a reboot to recover a path to a storage port that has been moved. These operating systems store the FC address as part of the disk device identification. The FC address is based on the switch port number and the switch domain ID, so if a storage port is moved to a different port on the same switch or to any port on a switch with a different domain ID, the FC address would change and the operating system would believe that access to the device had been lost¹⁵.

During these upgrades in environments with servers such as these and with varied change windows, it may not be possible to move all the storage ports required during a single change window. It may be necessary to temporarily connect sufficient ISL bandwidth between the existing and new core switches during the first change window so that a portion of edge ISL's and storage ports can be moved. Additional change windows should be planned to move the remaining connections and complete the fabric upgrade. It is not recommended that dual core switches be left interconnected with ISL's indefinitely as a means to increase fabric capacity.

¹⁴ Only the utilization threshold alert is impacted by this issue, because all other alerts in scope of this project also include the user configured switch name.

¹⁵ This limitation can be removed from AIX 5.2 by setting the "Dynamic Tracking of FC Devices" parameter on the fscsi* device

9. References and Related Documents

Document	Location
Connectrix Manager 9.1.1 Release Notes	http://engineering.citigroup.net/gdse/products/platforms/mcdatafc/releasenotes
Connectrix Manager Version 9.1.x User Guide	Available from EMC
E/OS 9.0.0 Release Notes	http://engineering.citigroup.net/gdse/products/platforms/mcdatafc/releasenotes
Global Distributed Storage Engineering Website	http://engineering.citigroup.net/gdse/
EMC Secure Remote Support Gateway (Alert Notification and Vendor Remote Access)	http://engineering.citigroup.net/gdse/products/services/VendorAccess/
eTrust Audit - Storage Monitoring Solution Guide	http://engineering.citigroup.net/gdse/products/platforms/symmetrix/stdsdocs/05023-sg.pdf
MIB files: fceos.mib and fcmgmt_v31.mib	Connectrix Service Processor
McData E/OS SNMP Support Manual P/N 620-000131-620 REV A	Available from http://www.mcdata.com
McData EFC Manager SNMP Agent User Manual P/N 620-000168-050 REV A	Available from http://www.mcdata.com
McData Intrepid 6140 and 6064 Directors Element Manager User Manual, P/N 620-000172-080 REV A	Available from http://www.mcdata.com

10. Appendix A: Connectrix Manager Installation

Note these cautions before upgrading to version 9.01.01:

- Backup the current Connectrix Manager 8.7.1 directory to CD or to a network share. This will be needed if migrating to a different server.
- Export Nicknames and ZoneSets
- **You will need to upgrade to Connectrix Manager 9.01.00, prior to upgrading to Connectrix Manager 9.01.01.**
- After installing Connectrix Manager 9.01.01, all remote clients running down-level versions of Connectrix Manager must install the 9.01.01 client application.
- Once running Connectrix Manager 9.01.01, any downgrade to a previous Connectrix Manager release will result in the loss of saved firmware files.
- All systems managing switches, including the Connectrix service processor and any remote systems running client software, must be offline before upgrading.
- Depending on the type of migration that will be performed, the Connectrix Manager Services may need to be stopped. Pay special attention to the instructions.
- Connectrix Manager Audit, Event, Session, Product Status, and Fabric log files are not migrated. As a safeguard, you should export and archived these logs in before migrating to Connectrix Manager 9.1.

10.1. *Connectrix Manager Packages*

- Connectrix Manager 9.1.0 Server (CSP): cnms9010
- Connectrix Manager 9.1.1 Server (CSP): cnms9110
- Connectrix Manager 9.1.1 Client: cnmgr910

10.2. *Upgrading the Connectrix Manager Server*

This procedure will assist the user with upgrading from Connectrix Manager 8.7.1 to Connectrix Manager 9.1.0 and then to Connectrix Manager 9.1.1. Connectrix Manager 8.7.1 and 9.1.0 is not removed during the Connectrix Manager 9.1.x upgrade process. It will need to be removed after you are sure everything has migrated successfully.

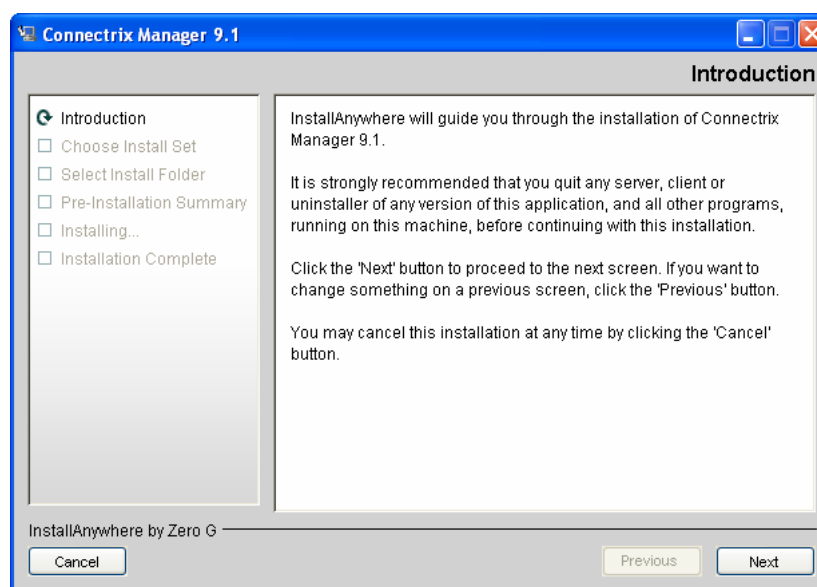
If this is a brand new SAN implementation (not an upgrade from 8.7.1), then it isn't necessary to install Connectrix Manager Server 9.1.0 first, you can go straight to version 9.1.1 (Section 10.2.2).

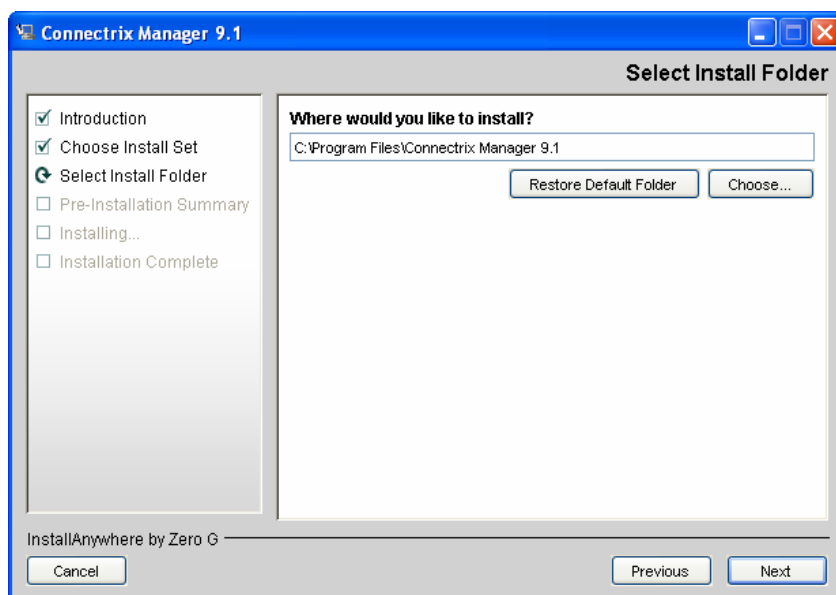
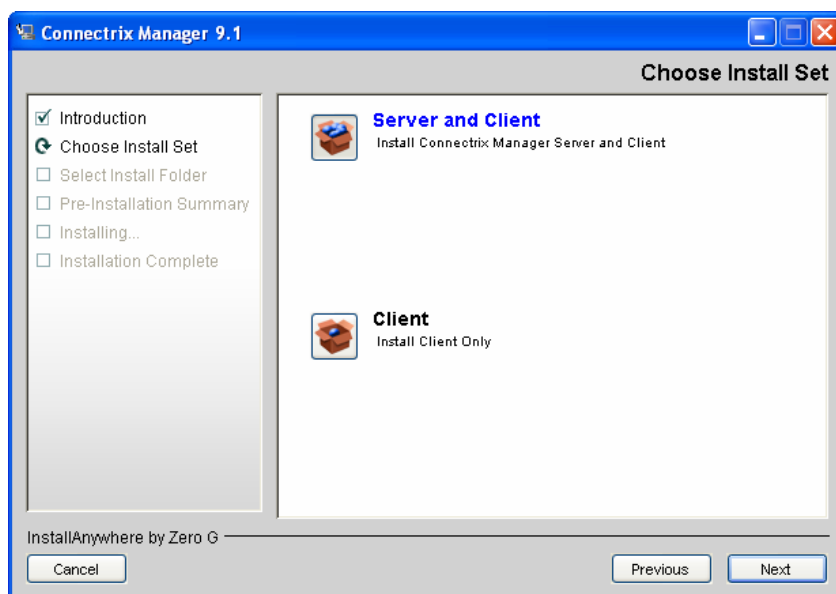
10.2.1. *Installing Connectrix Manager Server 9.1.0*

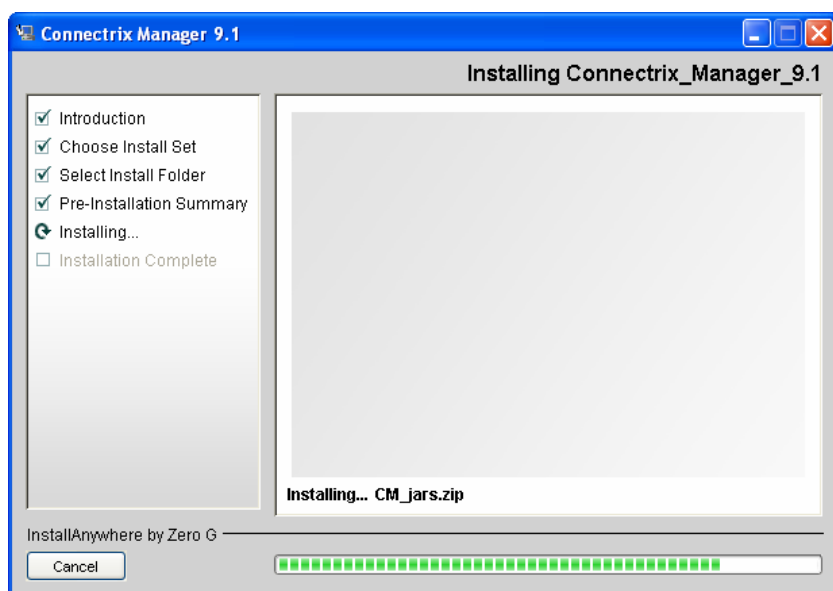
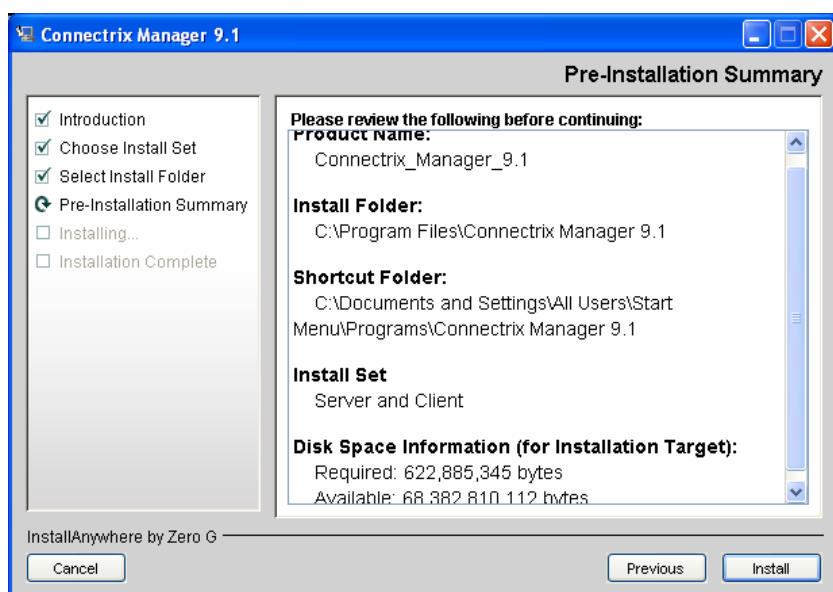
1. Backup the configuration of each director and switch.

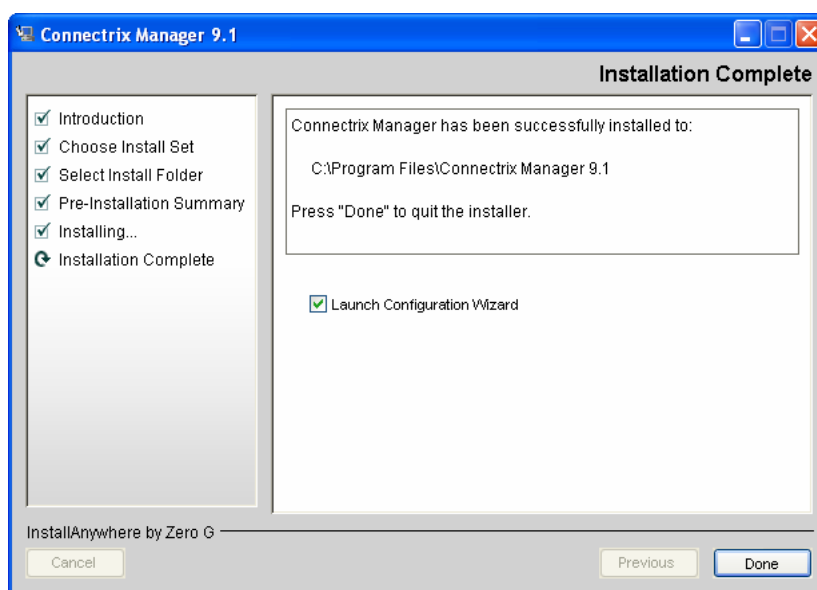
Note: IP addresses of unavailable Directors/Switches will not be fully migrated. Ensure all Directors/Switches are available using the Connectrix Manager 8.x application before proceeding with the upgrade.

- a. Select (double-click) the icon representing a director or switch for which the configuration file is to be backed up. The Hardware View for the selected product displays.
 - b. Select the Backup & Restore Configuration option from the Maintenance menu. The Backup and Restore Configuration dialog box for the product displays.
 - c. Click Backup. An Information dialog box is displayed, indicating the backup operation was initiated.
 - d. Click OK to complete the backup operation, close the dialog box, and return to the Hardware View.
 - e. Close the Hardware View by clicking close (X) at the upperright corner of the window.
 - f. Repeat step 1a through step 1e for each product (director and switch) managed by the Connectrix Manager server.
2. When the final product configuration file is backed up, close the Connectrix Manager application and stop the Connectrix Services.
 - a. Close any open Connectrix Manager Remote Clients.
 - b. Close the Connectrix Manager application on the Connectrix Manager server by selecting Exit from the SAN menu.
 3. Install Connectrix Manager 9.1.0 via the SPAC package (**cnms9010**).

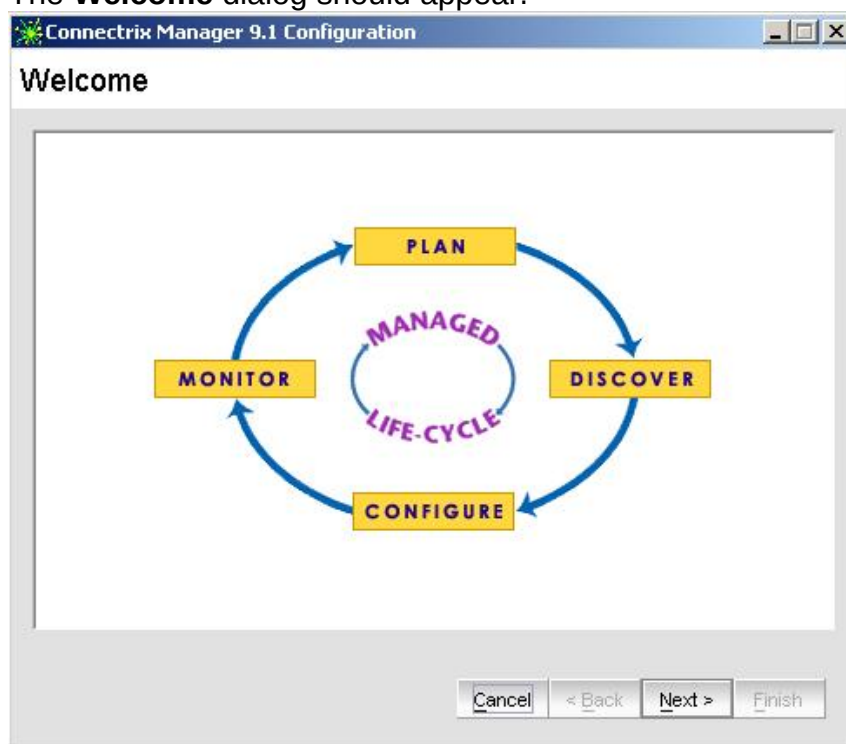






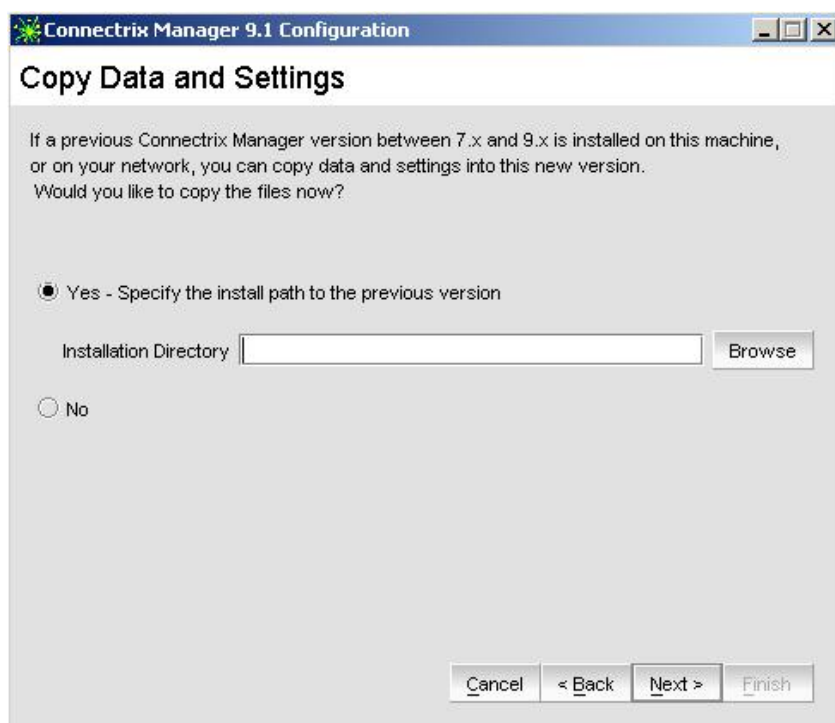


4. Perform the migration.
 - a. The **Welcome** dialog should appear.



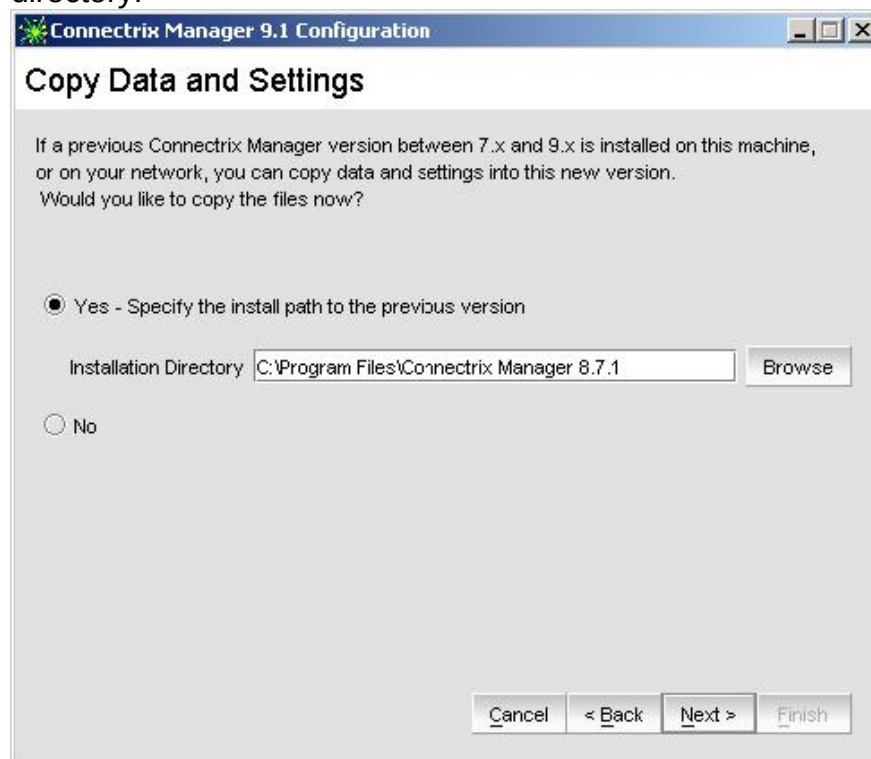
- b. On the **Welcome** dialog, click **Next**. The **License Agreement** dialog appears.
 - c. On the **License Agreement** dialog, if you agree with the license Agreement, select **Yes**, and click **Next**.

The **Copy Data and Settings** dialog displays.



- d. Accept the default setting of **Yes**, but change the Installation Directory to the location of Connectrix Manager 8.7.1 (C:\install directory\Connectrix Manager 8.7.1).

Using the **Browse** button, specify the path to the **Connectrix Manager 8.7.1** directory.



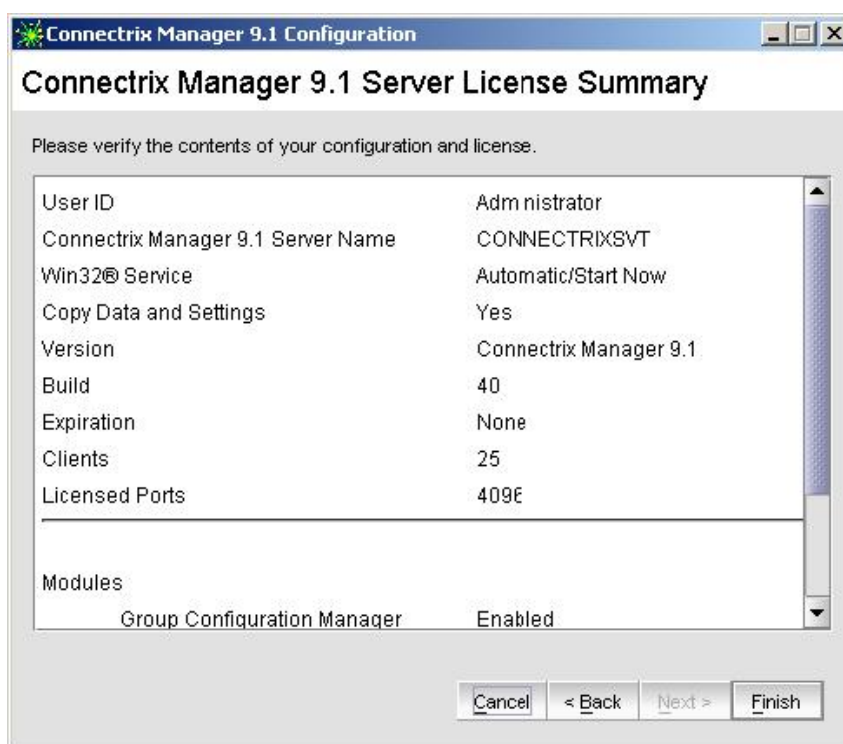
- e. Click Next. A **Connectrix Manager Message** window displays.



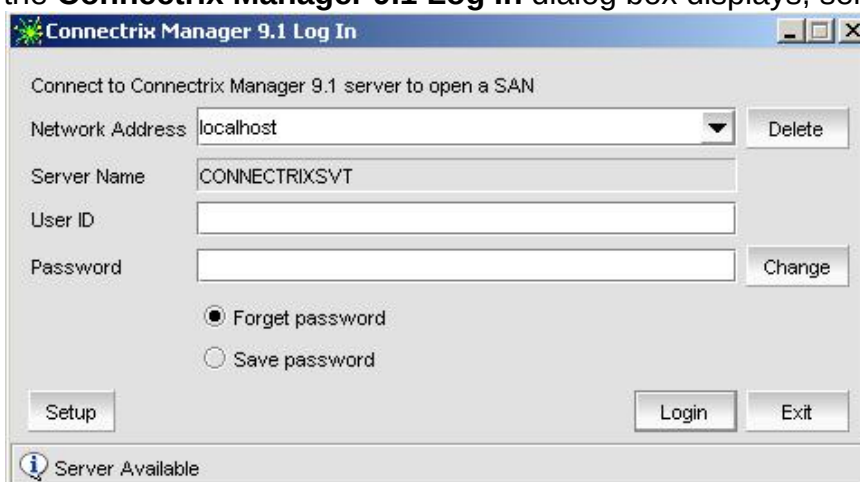
- f. Click OK. The Connectrix Manager 9.1 Server License panel displays. The serial number and license fields will NOT contain the values from the Connectrix Manager 8.7.1 installation. Type the Connectrix Manager serial number in the Serial Number field and the license key (obtained from EMC Powerlink) in the License Key field.

A screenshot of the "Connectrix Manager 9.1 Configuration" window, specifically the "Connectrix Manager 9.1 Server License" panel. The window has a blue header bar with the title and standard window controls. Below the header, the text "Please enter the Serial Number and License Key below." is displayed. There are two text input fields: "Serial Number" and "License Key". At the bottom right, there are four buttons: "Cancel", "< Back", "Next >", and "Finish".

- g. Type the Connectrix Manager serial number (obtained from the Connectrix Manager Documentation kit) in the Serial Number field and the license key (obtained from EMC Powerlink) in the License Key field. For more information, refer to *Getting a License Key* on page 2-15 in the *Connectrix Manager 8.7.1 User Guide*.
- h. Click **Next** to display the **Connectrix Manager 9.1 Server License Summary** dialog.

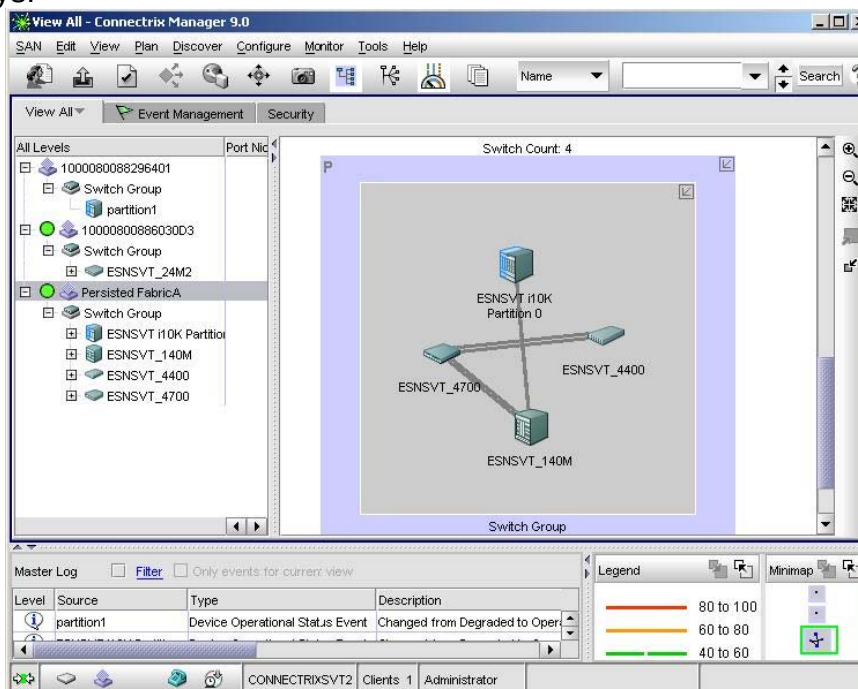


- i. Verify configuration and license information and click **Finish**.
- j. A **Connectrix Manager 9.1 Message** dialog will appear informing you to close the **Services** dialog. After you ensure it is closed, click **OK**. A message, *Applying user settings, please wait...* will appear until the migration process completes.
- k. When the **Connectrix Manager 9.1 Log In** dialog box displays, select **Exit**.



5. Reboot the server, and log in to Connectrix Manager.
 - a. On the server, go to **Start, Programs, Connectrix Manager 9.1**, and select **Connectrix Manager 9.1**.
 - b. On the **Connectrix Manager 9.1 Log In** dialog, type the Connectrix Manager user identification and password in the *User Id* and *Password* fields.

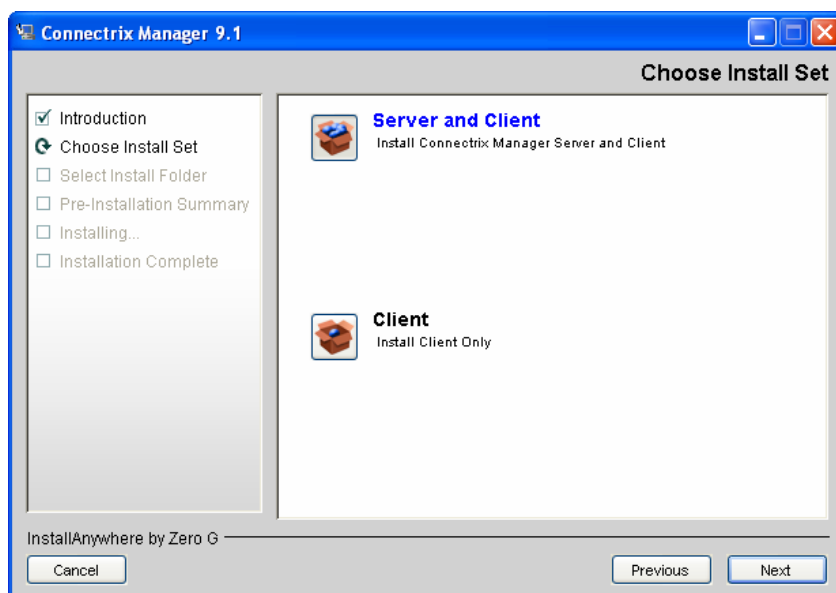
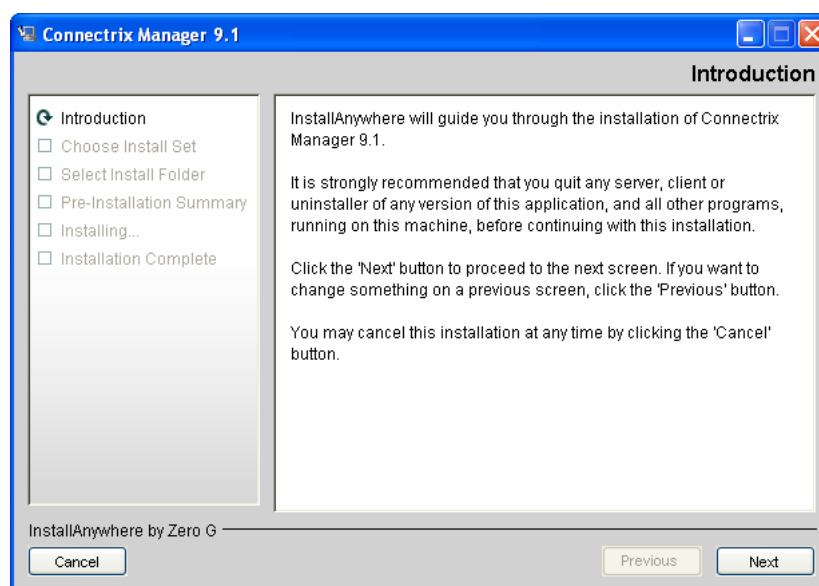
- c. Click **Login**. The application opens and the Connectrix Manager main window displays.

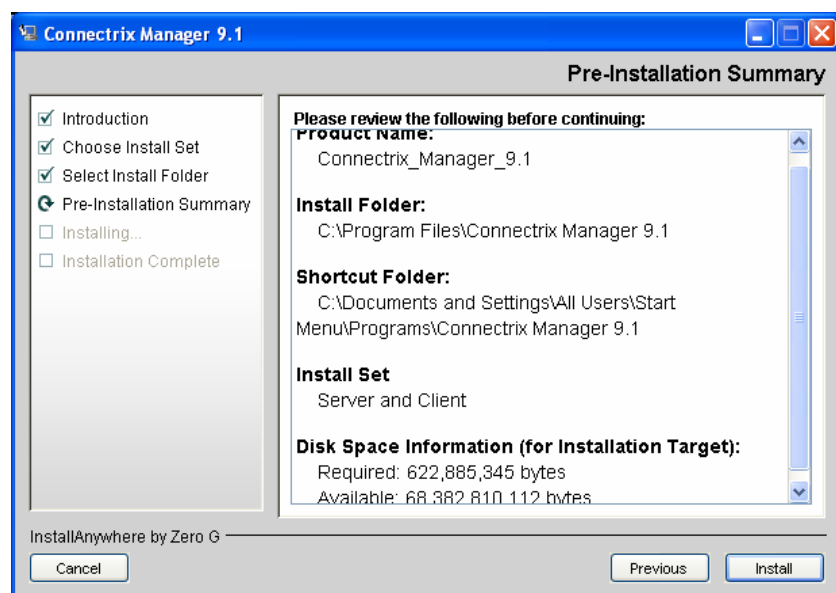
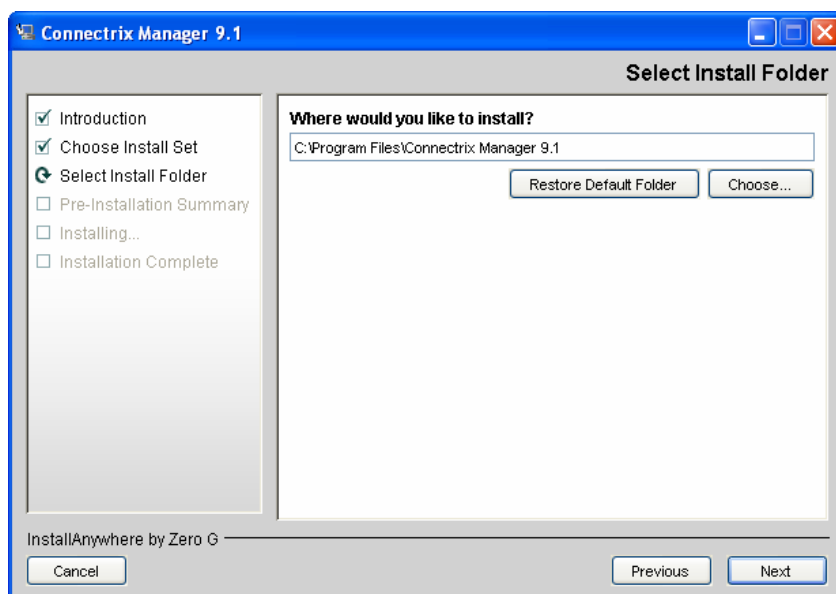


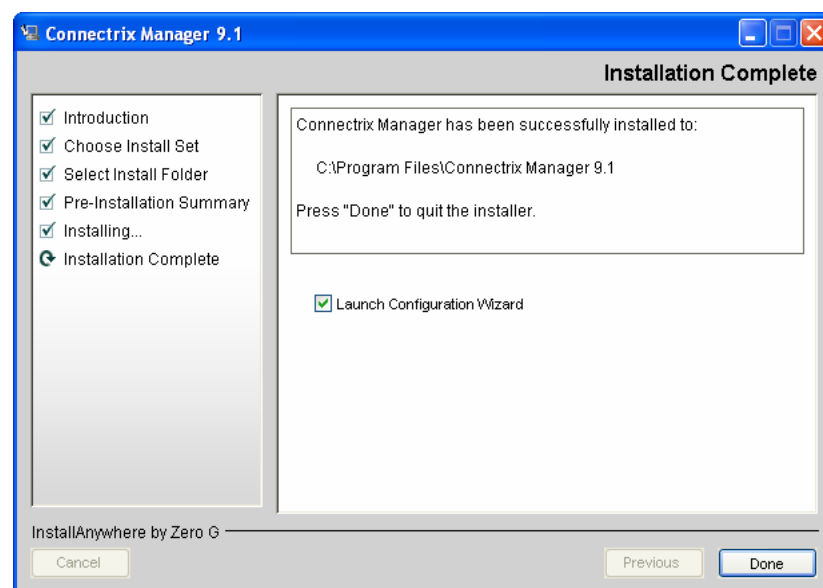
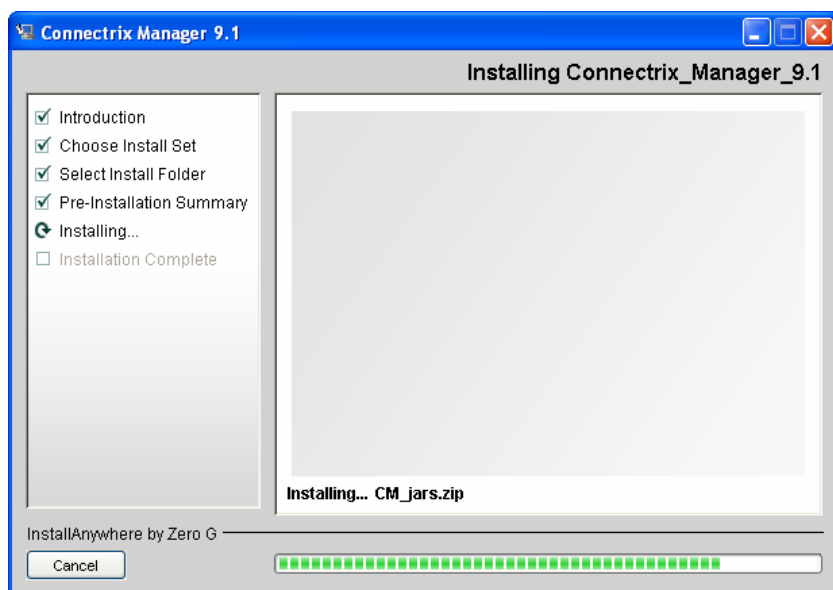
- d. At the Connectrix Manager's main window, inspect the shape and color of the status symbol associated with each product icon.
- e. Verify migration was successful. Information and settings for the following items should have migrated:
- Nickname Information
 - Zoning Library Information
 - User Information
 - Persisted Fabric Settings
 - Remote Access Settings
 - Event Notification Settings
 - SNMP Information
 - Trap Forwarding Information
 - Ethernet Notification Settings
- f. Verify that all director and switch products that were previously available are now managed by Connectrix Manager 9.1.

10.2.2. *Installing Connectrix Manager Server 9.1.1*

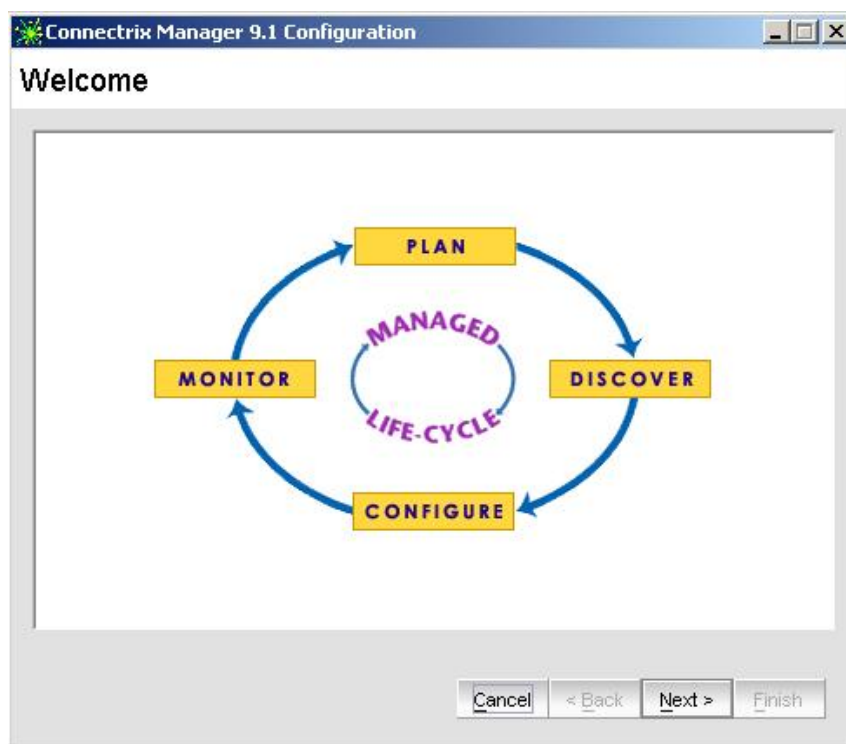
1. Install Connectrix Manager 9.1.1 via the SPAC package (**cnms9110**).







2. Perform the migration.
 - a. The **Welcome** dialog should appear.



- b. On the **Welcome** dialog, click **Next**. The **License Agreement** dialog appears.
- c. On the **License Agreement** dialog, if you agree with the license Agreement, select **Yes**, and click **Next**.

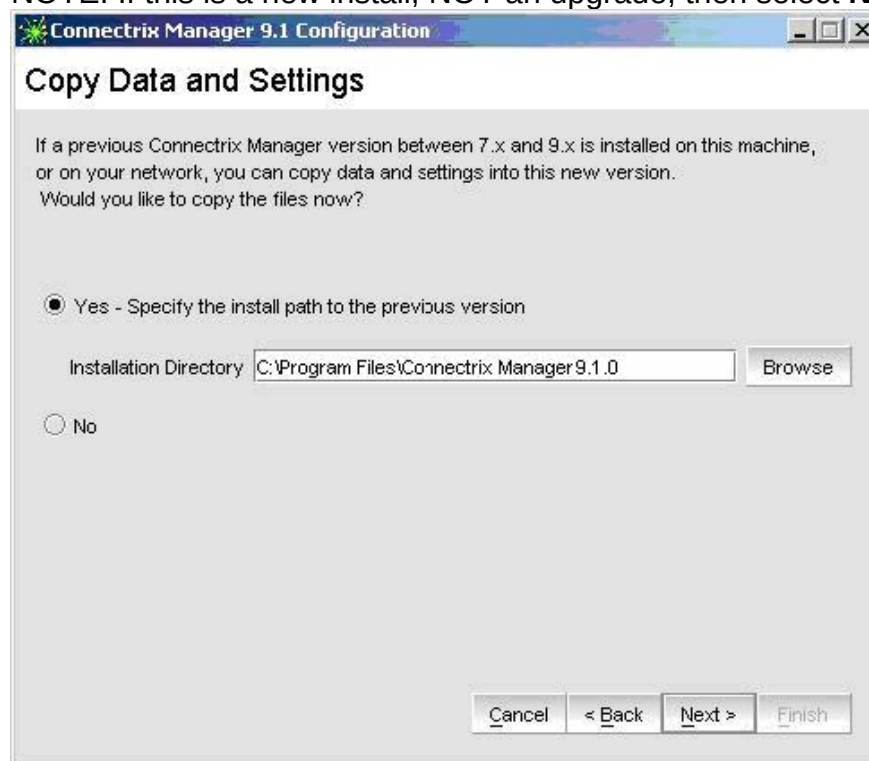
The **Copy Data and Settings** dialog displays.

The image shows the 'Connectrix Manager 9.1 Configuration' window with the 'Copy Data and Settings' tab selected. The dialog contains the following text: 'If a previous Connectrix Manager version between 7.x and 9.x is installed on this machine, or on your network, you can copy data and settings into this new version. Would you like to copy the files now?'. Below this text, there are two radio button options: 'Yes - Specify the install path to the previous version' (which is selected) and 'No'. The 'Yes' option is followed by a text field labeled 'Installation Directory' and a 'Browse' button. At the bottom of the window, there are four buttons: 'Cancel', '< Back', 'Next >', and 'Finish'.

- d. Accept the default setting of **Yes**, but change the Installation Directory to the location of Connectrix Manager 9.1.0 (C:\install directory\Connectrix Manager 9.1.0).

Using the **Browse** button, specify the path to the **Connectrix Manager 9.1.0** directory.

NOTE: If this is a new install, NOT an upgrade, then select **No** below.



- e. Click Next. A **Connectrix Manager Message** window displays.

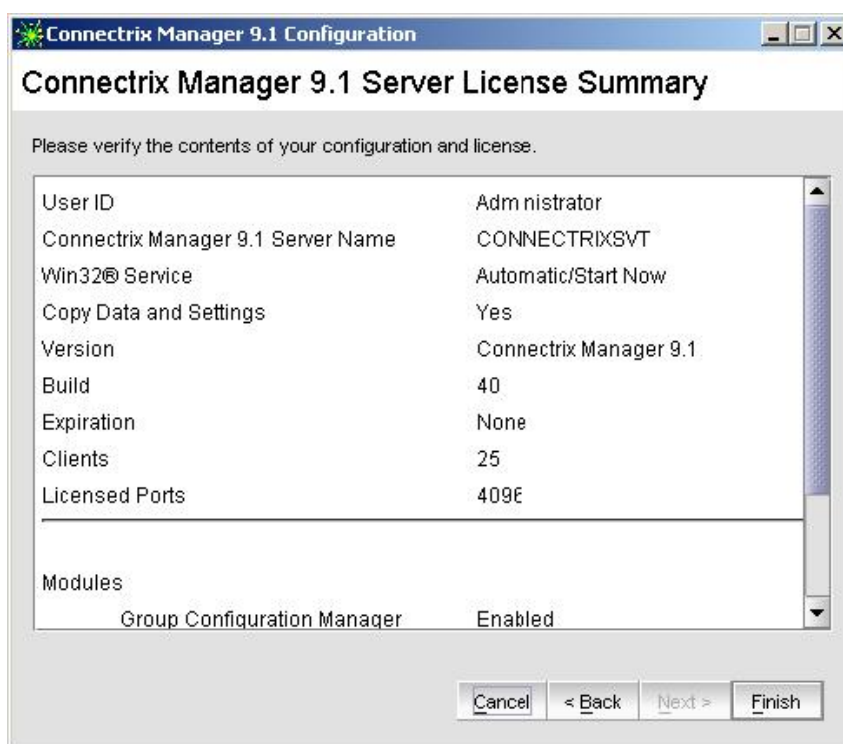


- f. Click OK. The Connectrix Manager 9.1.1 Server License panel displays. The serial number and license fields will contain the values from the Connectrix Manager 9.1.0 installation. Unless this is a new install, then type the Connectrix Manager serial number in the Serial Number field and the license key (obtained from EMC Powerlink) in the License Key field.

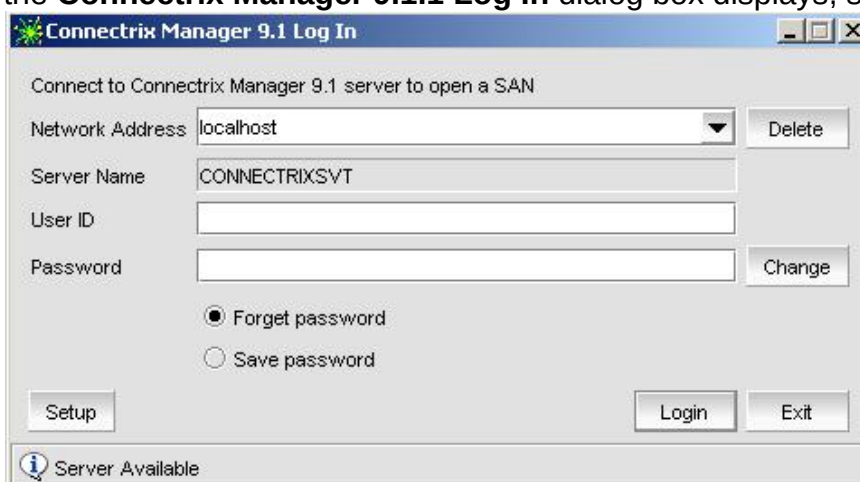


The image shows a Windows-style dialog box titled "Connectrix Manager 9.1 Configuration". The main heading inside is "Connectrix Manager 9.1 Server License". Below the heading, it says "Please enter the Serial Number and License Key below.". There are two text input fields: "Serial Number" and "License Key". At the bottom right, there are four buttons: "Cancel", "< Back", "Next >", and "Finish".

- g. Type the Connectrix Manager serial number (obtained from the Connectrix Manager Documentation kit) in the Serial Number field and the license key (obtained from EMC Powerlink) in the License Key field. For more information, refer to *Getting a License Key* on page 2-15 in the *Connectrix Manager 8.7.1 User Guide*.
- h. Click **Next** to display the **Connectrix Manager 9.1.1 Server License Summary** dialog.

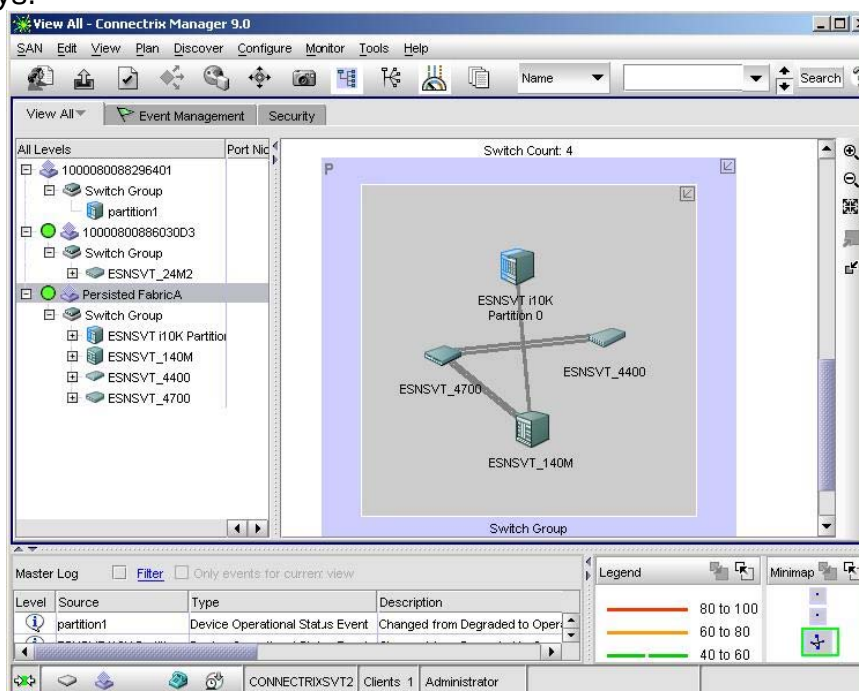


- i. Verify configuration and license information and click **Finish**.
- j. A **Connectrix Manager 9.1.1 Message** dialog will appear informing you to close the **Services** dialog. After you ensure it is closed, click **OK**. A message, *Applying user settings, please wait...* will appear until the migration process completes.
- k. When the **Connectrix Manager 9.1.1 Log In** dialog box displays, select **Exit**.



3. Reboot the server, and log in to Connectrix Manager.
 - a. On the server, go to **Start, Programs, Connectrix Manager 9.1.1**, and select **Connectrix Manager 9.1.1**.
 - b. On the **Connectrix Manager 9.1.1 Log In** dialog, type the Connectrix Manager user identification and password in the *User Id* and *Password* fields.

- c. Click **Login**. The application opens and the Connectrix Manager main window displays.



- d. At the Connectrix Manager's main window, inspect the shape and color of the status symbol associated with each product icon.
- e. Verify migration was successful. Information and settings for the following items should have migrated:
- Nickname Information
 - Zoning Library Information
 - User Information
 - Persisted Fabric Settings
 - Remote Access Settings
 - Event Notification Settings
 - SNMP Information
 - Trap Forwarding Information
 - Ethernet Notification Settings
- f. Verify that all director and switch products that were previously available are now managed by Connectrix Manager 9.1.1.
4. Upon completion of the upgrade the Connectrix Manager 8.7.1 and 9.1.0 services are no longer available, but the directory structure and desktop icons associated with the version remain. Therefore, once you have confirmed that the upgrade was successful you may want to proceed with the uninstall process to remove these items.
- a. From the Start menu, select Programs> Connectrix Manager 8.7.1 or 9.1.0, then Uninstall Connectrix Manager. The InstallShield Wizard will appear displaying three options.

- b. Select the Full Uninstall - Delete all files option, click Next.
 - c. After the maintenance operation completes, click Finish.
5. Engage EMC for the following:
 - a. Install ConnectEMC, and then configure it to send email alerts to the EMC Secure Remote Support Gateway server(s). Send a test alert, EMC should receive the alert in their CS database.

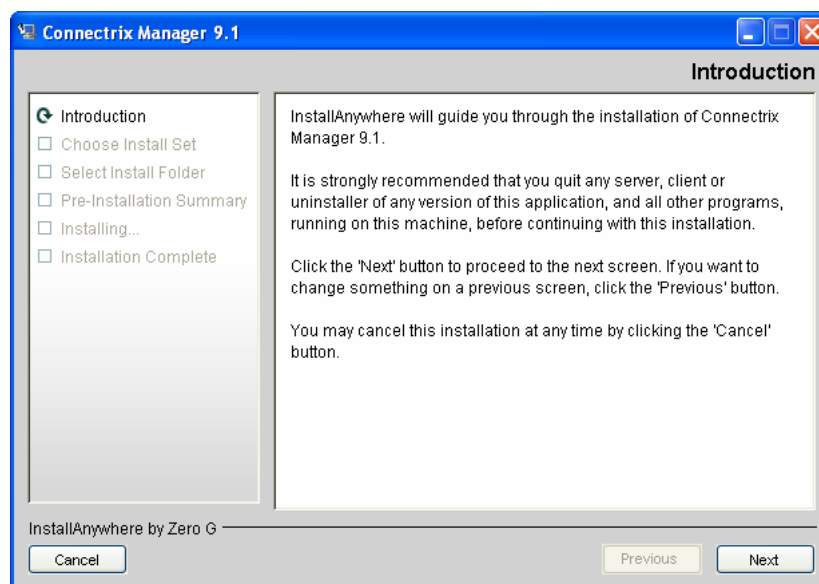
Note: EMC will need to assist in the installation and configuration of ConnectEMC.
 - b. Deploy the Connectrix Manager Server in EMC Secure Remote Support.
 - c. Install EMCRemote, and then configure and test the ability of EMC support to access the Connectrix Manager Server with EMCRemote via the EMC Secure Remote Support Gateway.

The installation of Connectrix Manager 9.1.1 is now complete.

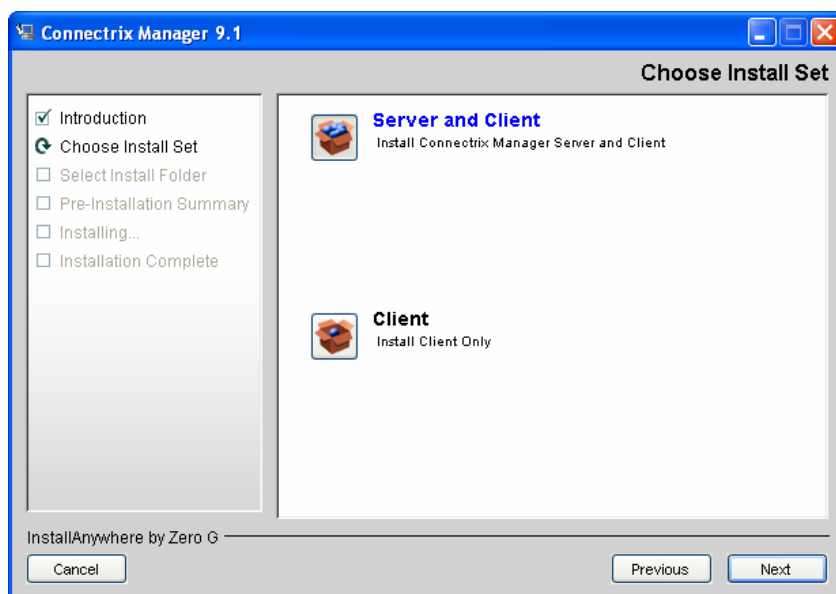
10.2.3. Installing Connectrix Manager Client 9.1.1

To access the Connectrix Manager Server from a Client running on a separate SOE server, will require the installation of the Connectrix Manager 9.1.1 Client package (**cnmgr910**).

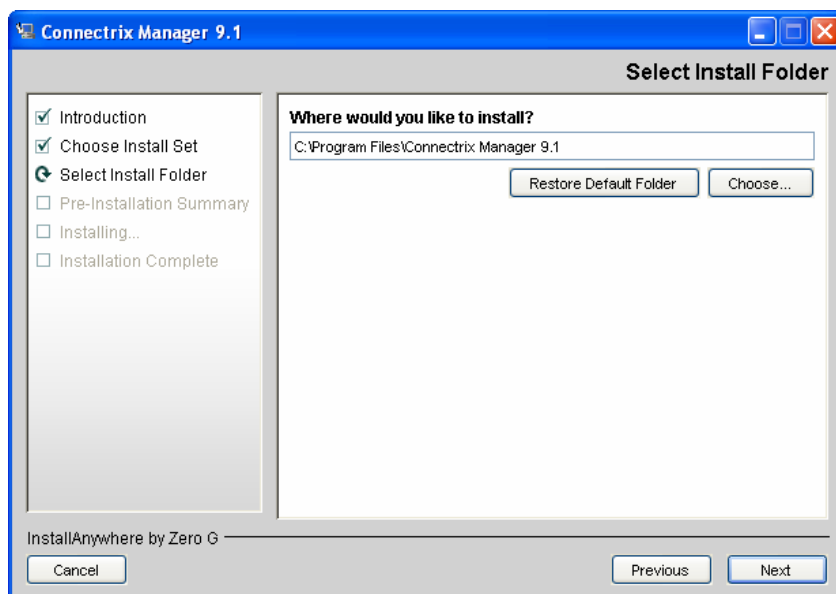
1. Start the Client package install. Click **Next**.



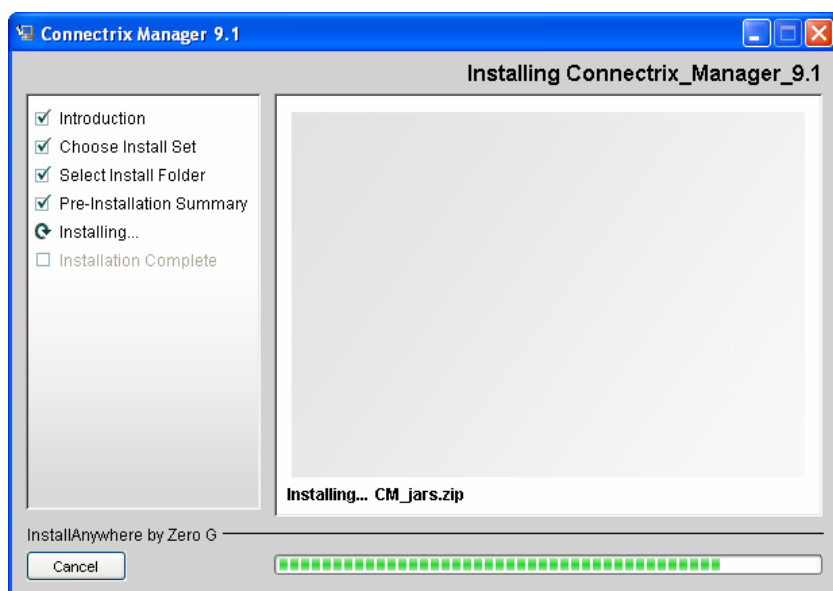
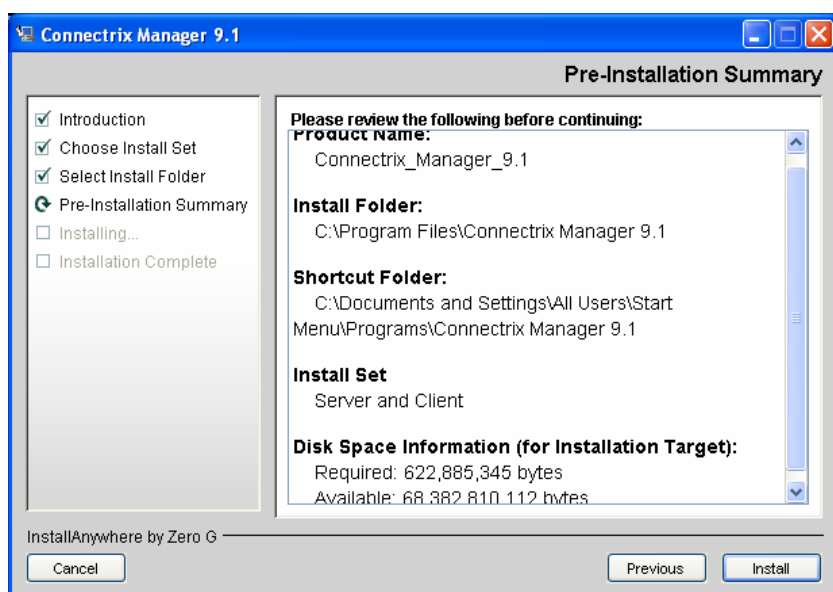
2. Select "**Client**" only. Click **Next**.



3. Allow the default directory and click **Next**.



4. At the Pre-Installation Summary dialog box, click **Next**.



5. Installation complete, click **Done**. Launch Connectrix Manager Client and verify it is working properly.

