Copyright © 2004, 2007 EMC Corporation. All rights reserved.

Published: February, 2007

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED "AS IS." EMC CORPORATION MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

All other trademarks used herein are the property of their respective owners.
Preface ........................................................................................................................... 31

Chapter 1  Introduction to Connectrix Manager
  Connectrix Manager overview ................................................................. 36
  Connectrix Manager components ................................................... 37
  Access method .................................................................................. 38
  Connectrix service processor ........................................................... 39
  Automatic Data Backup (update to CD-RW) ................................. 39

Chapter 2  Getting Started
  Overview ....................................................................................................... 42
  Client system requirements ................................................................. 42
  Product licensing overview ................................................................. 43
    License keys ..................................................................................... 43
    Feature keys (switch or director Element Managers) ................ 48
  Getting a license key ........................................................................... 49
    Getting a license key for new software........................................... 49
    Where to start ................................................................................. 49
  Starting the application ...................................................................... 50
  Starting Connectrix Manager for Windows Systems .................. 50
  Backing up and restoring data ............................................................. 57
    What is backed up? ...................................................................... 57
    Management server backup .......................................................... 58
    Configuring backup to a writable CD ......................................... 59
    Configuring backup to a hard drive ............................................ 60
    Configuring backup to a network drive .................................. 61
    Enabling backup .......................................................................... 62
    Disabling backup ......................................................................... 62
Viewing the backup status........................................................ 63
Changing the backup interval .................................................. 63
Starting immediate backup..................................................... 64
Reviewing backup events....................................................... 64
Restoring data ..................................................................... 65
Restoring data from the EMC-supplied rack mount management server.................................................. 66
Restoring data from CD.......................................................... 67
Restoring data from the hard drive........................................ 67
Restoring data from a network drive .................................... 68
Formatting and archiving CD-RW disks.............................. 69
Closing the application.......................................................... 72
Searching the online help .................................................... 72
Icon legends......................................................................... 73
Keyboard shortcuts .............................................................. 74

Chapter 3 Software Overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>The life cycle of a SAN</td>
<td>76</td>
</tr>
<tr>
<td>Overview</td>
<td>77</td>
</tr>
<tr>
<td>View tab</td>
<td>78</td>
</tr>
<tr>
<td>Product list</td>
<td>79</td>
</tr>
<tr>
<td>Master log</td>
<td>82</td>
</tr>
<tr>
<td>Minimap</td>
<td>83</td>
</tr>
<tr>
<td>Anchoring or floating the Minimap</td>
<td>83</td>
</tr>
<tr>
<td>Resizing the Minimap</td>
<td>84</td>
</tr>
<tr>
<td>Menu bar</td>
<td>85</td>
</tr>
<tr>
<td>Toolbar</td>
<td>92</td>
</tr>
<tr>
<td>Toolbox</td>
<td>92</td>
</tr>
<tr>
<td>Status bar</td>
<td>93</td>
</tr>
</tbody>
</table>

Chapter 4 Setting Up the Connectrix Manager

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring the Connectrix Manager server</td>
<td>96</td>
</tr>
<tr>
<td>Logging in to a server</td>
<td>96</td>
</tr>
<tr>
<td>Changing your password</td>
<td>97</td>
</tr>
<tr>
<td>Logging out of a server</td>
<td>98</td>
</tr>
<tr>
<td>Adding a server</td>
<td>98</td>
</tr>
<tr>
<td>Configuring HBAs and servers</td>
<td>99</td>
</tr>
<tr>
<td>Renaming a server</td>
<td>100</td>
</tr>
<tr>
<td>Deleting a server</td>
<td>100</td>
</tr>
<tr>
<td>Removing a server</td>
<td>100</td>
</tr>
<tr>
<td>Configuring options</td>
<td>101</td>
</tr>
</tbody>
</table>
Configuring backup settings ................................................... 101
Configuring domain ID and port number display .......... 102
Configuring end node display ................................................ 103
Configuring flyover settings ................................................... 103
Configuring nickname settings ............................................... 104
Editing duplicate nicknames ................................................ 105
Configuring reset display settings .......................................... 106
Configuring software settings ................................................. 107
Managing users ............................................................................... 113
Viewing the list of users ........................................................... 113
Adding a user account ............................................................. 113
Changing a user account .......................................................... 114
Removing a user account ......................................................... 115
Filtering event notifications for a user ................................... 115
Managing user groups .................................................................... 117
Creating a user group ............................................................... 117
Editing a user group ................................................................. 120
Removing a user group ............................................................ 121
Assigning users to groups ....................................................... 122
Removing a user from a group ............................................... 122
Finding a user’s groups ............................................................ 123
Configuring remote access ............................................................. 124
Viewing active user sessions ......................................................... 125
Partitioned switch support ............................................................ 126
Viewing the logical configuration of devices ................. 127
Customizing the main window .................................................... 128
Zooming in and out of the physical map ....................... 128
Showing levels of detail on the physical map ............... 129
Turning flyovers on or off ....................................................... 129
Viewing flyovers ....................................................................... 129
Exporting and importing ............................................................... 130
Exporting data to disk or email .............................................. 130
Defining filters for export ........................................................133
Exporting data to a database ................................................... 133
Importing data ........................................................................... 136
Importing SANvergence Manager Data ......................... 139
Accessing third-party tools ............................................................. 141
Adding a tool ............................................................................. 141
Adding an option to the Tools menu ....................... 143
Changing an option on the Tools menu ..................... 144
Removing an option from the Tools menu ............... 144
Adding an option to a device’s Shortcut menu ............ 145
Changing an option on a device’s Shortcut menu ... 146
Chapter 5   Discovering a SAN

How discovery works .............................................................. 150
Out-of-band discovery .......................................................... 150
Manager of Manager discovery ............................................. 151
    Discovering data from another Connectrix Manager server .................................................. 153
License discovery ................................................................. 154
Setting up discovery ............................................................ 156
Setting the polling delay ........................................................ 160
Setting the Polling Delay ....................................................... 160
Configuring address properties ............................................. 161
    Adding an IP address ...................................................... 161
    Editing an IP address .................................................. 163
    Removing an IP address ............................................. 164
    Configuring a SNMP community string ......................... 164
    Reverting to a default SNMP community string ............. 167
    Configuring the product type and access ................. 168
Turning discovery on and off ................................................ 170
Determining the discovery state ........................................... 171
Troubleshooting discovery .................................................... 171
Configuring Storage Port Mapping ....................................... 175
    Adding storage ports to a storage array ........................ 176
    Removing storage port and storage array associations ...... 176
    Reassigning mapped storage ports .............................. 177
    Creating a storage array ............................................ 177
    Editing storage array properties ................................ 178
    Deleting a storage array .......................................... 179
    Viewing storage port properties .................................. 180
    Viewing storage array properties .............................. 180

Chapter 6   Group Configuration Management

Overview ................................................................. 184
    Group management of virtual switches ......................... 184
Select group action tab .................................................... 185
Creating a group event log .............................................. 185
    Accessing the Create Group Event Log dialog box .......... 186
Chapter 7 Configuring User Groups

About user groups and access levels........................................... 194
Creating a user group ................................................................. 195
Changing a user group ............................................................... 197
Removing user groups ............................................................... 198

Chapter 8 Administering User Groups

Assigning users to groups.......................................................... 200
Removing users from groups ..................................................... 200
Finding a user's groups............................................................. 202

Chapter 9 Configuring SAN Products and Fabrics

Managing products................................................................. 204
  Opening a product's Element Manager ....... 204
  Searching for products in a SAN .............. 204
  Changing product properties .................. 205
  Determining a product's operational status .. 206
  Deleting an offline product .................... 207
  Showing routes between two end-products ...... 207
  Hiding routes between two end-products .......... 209
  Viewing properties of routes between two end-products ... 209
  Changing a fabric's properties ............... 209
Configuring nicknames ........................................................... 210
  Viewing nicknames ........................................... 210
  Assigning a nickname to an existing device .. 210
  Adding a nickname to a new device ........... 211
  Importing nicknames ......................................... 211
  Exporting nicknames .......................................... 212

Selecting switches and directors............................................. 186
Creating a group log................................................................. 187
Installing E/OS firmware .......................................................... 188
  Select Firmware tab ........................................... 188
  Execution Options tab ....... 189
  Install tab ........................................... 189
  History tab ........................................... 190
Running data collection ............................................................. 191
  Output Options tab ........................................... 191
  Execution Options tab ........................................... 191
  Run Data Collection tab ........................................... 192
# Chapter 10 Monitoring SAN Products and Fabrics

Event monitoring ................................................................. 246  
Viewing logs ....................................................................... 247  
Exporting log data ............................................................... 247  
Viewing the fabric log .......................................................... 248  
Filtering events in the master log .......................................... 248  
Copying log entries .............................................................. 250  
Using event notification features .......................................... 251  
  Configuring email notification ............................................ 251  
  Configuring Call Home notification .................................... 252  
  Enabling Ethernet events .................................................... 252  
Creating reports ................................................................. 254  
  Generating reports ............................................................ 255  
  Viewing reports ............................................................... 256  
  Printing reports ............................................................... 257  
  Printing a Physical Map report .......................................... 257  
  Deleting reports .............................................................. 258

# Chapter 11 Zoning

Assigning zone properties .................................................. 261  
Comparing zone sets .......................................................... 262  
Copying a zone to a library .................................................. 264  
Copying a zone set to a library ............................................ 265  
Deleting a fabric and its zone library ................................... 267  
Deleting a zone ................................................................. 268  
Deleting a zone set ............................................................ 269  
Duplicating a zone ............................................................ 270  
Duplicating a zone set ........................................................ 271  
Exporting zones and zone sets ........................................... 272  
Finding a member in one or more zones ............................... 273  
Finding a zone member in the potential member list ............. 274  
Finding zones in a zone set ................................................ 275  
Finding a zone set member in the zones list .......................... 275  
Importing a zone set .......................................................... 276  
Listing zone members ....................................................... 277  
Removing zone members .................................................... 279  
Removing a zone from a zone set ....................................... 280  
Renaming a zone .............................................................. 281  
Renaming a zone set .......................................................... 282  
Replacing a zone set from history ...................................... 282  
Replacing zone members .................................................... 284  
Saving the active zone set to a zone library ......................... 286
Searching for a zone member by WWN or nickname........... 288
Setting the zoning delay ................................................. 289
Viewing properties for iFCP links................................. 290
Viewing properties for zones and zone sets .................. 291
Viewing zoning reports............................................... 292
Configuring zoning...................................................... 294
Accessing zoning ........................................................ 294
Zoning limits ............................................................... 295
Zoning naming conventions ......................................... 295
Administrator zoning privileges ................................. 295
Configuring zoning ...................................................... 297
Creating a new zone..................................................... 299
Adding members to a zone .......................................... 299
Creating a new member in a zone ................................. 300
Creating a zone set....................................................... 302
Adding zones to zone sets ........................................... 303
Activating a zone set ................................................... 304
Enabling or disabling the default zone for fabrics .......... 307
Enabling or disabling safe zoning mode for fabrics ......... 308
Removing a member from a zone ................................. 309
Removing a zone from a zone set ................................. 310
Deactivating a zone set ............................................... 311

Chapter 12 Monitoring Performance

Monitoring connection utilization ............................... 314
   Turning on connection utilization ............................ 315
   Turning off connection utilization .......................... 315
Monitoring switch performance ............................... 316
Monitoring HBA performance .................................. 317
Gathering and viewing performance data .................. 318
   Storing performance data ..................................... 318
   Exporting performance data .................................. 318
   Setting up automatic exports ............................... 322
Importing performance data .................................... 324
Monitoring port performance .................................. 326
Monitoring latency .................................................. 328
Viewing ISL and end-node performance in the Topology ..... 329
Setting performance thresholds ............................... 330
Chapter 13  Virtual Fabrics

Feature description ................................................................. 332
Feature benefits ................................................................. 332
Creating fabrics ................................................................. 332
Virtual switches .............................................................. 333
Core switches ................................................................. 335
Virtual switch ports .......................................................... 335
Virtual fabrics feature and zoning ..................................... 336
Creating virtual switches — overview .................................. 338
Virtual switch display and function in the Physical Map ....... 339
Connecting virtual switches to existing fabrics ................. 342
Creating a virtual switch ................................................... 343
Configuring a new virtual switch ....................................... 344
Assigning ports to virtual switches .................................... 351
Assigning ports to a new virtual switch ............................... 351
Important notes for assigning ports ................................... 352
Editing virtual switch parameters ....................................... 353
Using the right-click menu ................................................ 353
Removing virtual switches ................................................ 354
Managing virtual switches ............................................... 355
Connectrix Manager application ........................................ 355
Element Manager ............................................................ 360

Chapter 14  Event Management

Event Management components ......................................... 368
Event types ................................................................. 368
About Triggers .............................................................. 369
Event Management actions .............................................. 369
Event Management page description .................................. 371
Turning the Event Management feature on or off ............... 373
Configuring Event Management rules ............................... 373
Defining an event trigger ................................................ 374
Trigger phrases ............................................................. 376
Specifying time limits for an event trigger ......................... 377
Defining a schedule trigger ............................................ 378
Specifying a rule’s actions ............................................... 379
Specifying an e-mail action ............................................ 379
Specifying an export action .......................................... 380
Specifying a launch action .......................................... 380
Specifying a log action .................................................. 381
Specifying a message action ....................................... 382
Specifying a pause action ............................................ 382
Specifying a report action ........................................................ 383
Specifying a send SNMP trap action ..................................... 383
Specifying a sound action .................................................... 383
Editing a rule ............................................................................. 384
Copying a rule ............................................................................ 388
Deleting a rule .......................................................................... 388
Activating an existing rule ...................................................... 389
Deactivating rules .................................................................... 390
Event trigger properties ........................................................... 391
Common property sets ............................................................ 392
  Product property set .............................................................. 392
  Port property set .................................................................. 394
  System property set ............................................................. 395
Event types ............................................................................... 397
  Device operational status event property set ................. 397
  Ethernet event property set ................................................. 398
  Fabric event property set ..................................................... 399
  Performance event property set ........................................ 399
  Product audit event property set ....................................... 400
  Product event property set .................................................. 401
  Product hardware event property set ............................. 401
  Product link incident event property set ...................... 402
  Product state event property set ......................................... 402
  Product threshold alert event property set .................... 403
  Security event property set ................................................ 404
  Session event property set ................................................ 405
  SNMP trap event property set .......................................... 405
  User action event property set .......................................... 406
Writing Event Management macros ...................................... 407
  Event context property set ................................................. 408
  Product context property set ............................................. 409
  Port context property set .................................................. 410
  TIME context property set ................................................ 412
  System context property set .............................................. 413
  User context property set ................................................ 414
  FILE Macro ........................................................................ 414
  EXEC context property set ................................................. 414
  Specifying arguments to the Internet Launcher scripts ....... 415
Advanced event filtering .......................................................... 417
# Chapter 15  SAN Routing

- What is SAN routing? ................................................................. 420
- SAN routing definitions .......................................................... 420
- SAN routing groups ................................................................. 423
- Discovering a SAN router ......................................................... 426
- Router port configuration .......................................................... 427
  - Assigning a fabric to an R_port ............................................. 428
  - Setting an insistent domain ID for an R_port ....................... 428
  - Establishing or changing a preferred domain ID for an R_port ................................................................. 429
  - Setting port binding for an R_port ...................................... 430
  - Displaying the status of an R_port ..................................... 431
  - Editing the port binding for an R_port ................................... 431
  - Displaying all fabric switches assigned to an R_port ........... 432
- Finding an R_port in a router fabric configuration .................... 432
- Zoning scopes ........................................................................ 434
  - Router fabric zone configuration properties ....................... 434
  - Editing the router fabric name ............................................ 435
  - Changing the interop mode ............................................... 435
  - Changing the zone policy .................................................. 435
  - Enabling or disabling fabric binding ................................... 436
  - Viewing proxy node WWNs and Domain IDs ....................... 436
- SAN router configuration ......................................................... 437
  - Assigning a cluster ID ....................................................... 438
  - Enabling SNTP .................................................................. 439
  - Setting the date and time .................................................. 440
  - Assigning SNMP traps ....................................................... 441
  - Removing an SNMP trap ................................................... 442
  - Assigning an iFCP ID ........................................................ 442
  - Reviewing and confirming SAN router configuration changes ................................................................. 443
- Configuration archive ............................................................... 444
  - Archiving files and reports .................................................. 444
  - TFTP root path ................................................................. 446
- Applying properties for router consistency ................................. 447
- Creating a log file .................................................................. 448
- Saving changes to Flash memory ............................................. 448
Chapter 16  Customizing the Topology Layout

Topology overview ................................................................................. 450
  Mapping and unmapping hubs ........................................................... 451
Customizing the layout of devices on the topology ......................... 452
Customizing the layout of connections on the topology ............... 453
Changing a group’s background color ............................................. 453
Changing the product label ............................................................... 455
Changing the port label ................................................................... 456
Changing the port display ................................................................. 456
Viewing ports and port properties ................................................. 457
Viewing port types ............................................................................. 458
Showing connected ports ................................................................. 459
Determining inactive iSCSI devices ............................................... 459
Determining port status ................................................................. 459

Appendix A  Configuring Remote Workstations

System requirements ........................................................................... 462
Installing the Connectrix Manager .................................................. 462
Uninstalling the Connectrix Manager ............................................. 466
  Windows systems ........................................................................... 466
  Solaris and Linux systems ........................................................... 466

Appendix B  Upgrading to Connectrix Manager 9.1

Prerequisites ....................................................................................... 468
Upgrade considerations ...................................................................... 469
Getting started ................................................................................... 470
Upgrade/migration from a laptop running v7.1 ............................... 471
  Replacing the Connectrix Service processor ................................. 471
  Migrating from a laptop running Connectrix Manager 7.1
    (Donor) to a new 1U server running Connectrix Manager 9.1
    (Recipient) ................................................................................... 472
Upgrading a 1U server from v7.2 to v9.1 ....................................... 489
Upgrading a 1U server from v8.x or v9.0 to v9.1 ............................ 504
  Upgrade procedure for remote clients .......................................... 519
  Migrating data after initializing Connectrix Manager 9.1 .............. 520
Data migrated .................................................................................... 522
  User information .......................................................................... 522
  Zoning ......................................................................................... 522
  Email event configuration ........................................................... 522
  Switch identification .................................................................... 523
  FAF libraries ................................................................................ 523
Sessions configuration............................................................. 523
SNMP configuration.............................................................. 523
Firmware library .................................................................... 523
Logs...................................................................................... 524
Nicknames ............................................................................. 524
Threshold alert configurations................................................. 524
Data not migrated ................................................................. 525
Post-upgrade configuration tasks .............................................. 526
User configuration ................................................................. 526
Call Home ............................................................................ 526
Event notification .................................................................. 526
Configuring SAN devices ....................................................... 526
Ethernet event notification .................................................... 526
Connectrix EC-1500 cabinet installation ..................................... 527

Appendix C Connectrix Service Processor SNMP Agent

Downloading MIB information................................................... 530
Fibre Channel Management MIB support................................... 533
Notes on current support.......................................................... 533
Connectrix service processor agent MIB objects ...................... 533
Director/switch agent MIB objects ........................................... 574
MIB-II support ....................................................................... 605
Generic traps.......................................................................... 605

Appendix D Editing Configuration Properties Files

Specifying a host IP address in multi-NIC networks ............... 608
Editing master log settings ..................................................... 609

Appendix E SANtegrity Security Center

SANtegrity Security Center features ......................................... 612
Accessing the Security Center ............................................... 614
Security window components ............................................... 615
Fabrics list ............................................................................ 615
Authentication table .............................................................. 615
Security tabs ........................................................................ 616
Master Log ........................................................................... 616
Security Log ......................................................................... 616
Managing updates to security data .......................................... 617
About the security tabs ......................................................... 618
Using the Security tabs ......................................................... 619
Working with virtual fabrics ................................................... 621
Setting authentication methods ................................................................. 622
CHAP secrets ............................................................................................ 623
Accessing the Users tab ............................................................................ 624
Security Authentication Users tab .............................................................. 625
  Opening the User tab ............................................................................ 625
  Overview of tasks to be completed ..................................................... 626
  Configuring Web server and Telnet security .................................... 628
  Using the Apply To button .................................................................. 629
Accessing the Software tab ...................................................................... 631
Security Authentication Software tab ...................................................... 632
  Opening the Software tab ................................................................. 632
  Overview of tasks to be completed ..................................................... 633
  Configuring software authentication .................................................. 634
  Editing the CHAP secret for the current server ............................... 636
  Adding an additional software ID ....................................................... 637
  Editing the CHAP secret for another API user ................................. 638
  Removing another Server ................................................................. 638
  Specifying the Authentication Method for API users ..................... 638
  Enabling OSMS authentication ....................................................... 638
  Defining OSMS CHAP secret ............................................................ 639
  Applying changes and confirmation .................................................. 639
Accessing the Devices tab ........................................................................ 640
Security Authentication Devices tab ....................................................... 641
  Opening the Devices tab .................................................................... 641
  Components of the Devices tab .......................................................... 643
  Overview of tasks to be completed ..................................................... 644
  Configuring device authentication ..................................................... 645
Accessing the IP Access Control tab ....................................................... 650
Security Authentication IP Access Control tab ..................................... 651
  Opening the IP Access Control tab .................................................... 651
  Overview of tasks to be completed ..................................................... 652
  Configuring the IP Access Control feature ....................................... 652
Accessing Radius Servers tab ................................................................. 655
Security Authentication Radius Servers tab ........................................... 656
  Opening the Radius Servers tab .......................................................... 656
  Overview of tasks to be completed ..................................................... 657
  Configuring RADIUS servers ............................................................ 658
Accessing the Security Log ..................................................................... 661
Viewing the Security Log ......................................................................... 662
Appendix F Troubleshooting
Problems with addresses ......................................................... 666
Problems with discovery .......................................................... 667
  Determining the discovery state ......................................... 667
Problems with fabric binding .................................................. 670
Problems with LUNs .............................................................. 671
Problems with products ......................................................... 672
Miscellaneous problems ....................................................... 673

Appendix G Call Home Setup Procedure
Configure Call Home notification ............................................. 678
  Get information from the DialEMC Configuration dialog box ............................................. 678
Set Call Home Configuration ................................................ 679
Install ConnectEMC ............................................................ 681
Configure ConnectEMC ...................................................... 684
Enable and test Call Home notification ................................ 692
Test remote access ............................................................ 695

Appendix H Configuring Connectrix Manager for Firewall Access
Introduction ............................................................................. 698
  Document nomenclature .................................................. 698
Secure Socket Layer (SSL) ...................................................... 698
  Disabling SSL ................................................................. 699
Default Server Ports ............................................................ 699
  Default port numbers ...................................................... 699
  Modifying the default Connectrix Manager Server Ports .................................................... 700
Configuring the application to use dual network cards ........... 700
Polling client function .......................................................... 702
  Configuring for faster logins ............................................. 702
Configuring TCP port numbers to allow firewall access ....... 704
  Connectrix Manager with RMI at TCP port level .......... 704
  Forcing port in RMI registry .......................................... 706
  Forcing server and client export port number ................. 706

Appendix I Customer-Supplied Service Processor Requirements
Platform requirements .......................................................... 710
Automatic backup device ..................................................... 711
EMC Call Home and remote support ..................................... 712
Recommended operating system modifications .................. 713
  Windows active desktop ............................................... 713
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Connectrix service processor and remote workstation configuration</td>
<td>37</td>
</tr>
<tr>
<td>2 License dialog box</td>
<td>46</td>
</tr>
<tr>
<td>3 License dialog box</td>
<td>47</td>
</tr>
<tr>
<td>4 Connectrix Manager 9.1 Configuration dialog box (Welcome)</td>
<td>51</td>
</tr>
<tr>
<td>5 Connectrix Manager configuration dialog box (copy data and settings)</td>
<td>52</td>
</tr>
<tr>
<td>6 Connectrix Manager configuration serial number and license key dialog box</td>
<td>53</td>
</tr>
<tr>
<td>7 Connectrix Manager configuration verification dialog box</td>
<td>54</td>
</tr>
<tr>
<td>8 Connectrix Manager Log In dialog box</td>
<td>55</td>
</tr>
<tr>
<td>9 The life cycle of a SAN</td>
<td>76</td>
</tr>
<tr>
<td>10 Minimap</td>
<td>83</td>
</tr>
<tr>
<td>11 Toolbox</td>
<td>92</td>
</tr>
<tr>
<td>12 Status bar</td>
<td>93</td>
</tr>
<tr>
<td>13 Log In dialog box</td>
<td>97</td>
</tr>
<tr>
<td>14 Define Filter dialog box</td>
<td>116</td>
</tr>
<tr>
<td>15 Define Filter Dialog Box</td>
<td>116</td>
</tr>
<tr>
<td>16 Group features dialog box</td>
<td>118</td>
</tr>
<tr>
<td>17 Export dialog box</td>
<td>131</td>
</tr>
<tr>
<td>18 Import dialog box</td>
<td>138</td>
</tr>
<tr>
<td>19 Setup Tools dialog box (Tools Menu tab)</td>
<td>141</td>
</tr>
<tr>
<td>20 Discover Setup Dialog Box (General Tab)</td>
<td>156</td>
</tr>
<tr>
<td>21 Discover setup dialog box</td>
<td>157</td>
</tr>
<tr>
<td>22 Discover Setup Dialog Box (Out-of-Band Tab)</td>
<td>161</td>
</tr>
<tr>
<td>23 Address Properties Dialog Box (IP Address Tab)</td>
<td>162</td>
</tr>
<tr>
<td>24 Address Properties dialog box (IP Address tab)</td>
<td>162</td>
</tr>
<tr>
<td>25 Address Properties dialog Box (SNMP tab)</td>
<td>165</td>
</tr>
<tr>
<td>26 Address Properties dialog box (Community strings tab)</td>
<td>165</td>
</tr>
<tr>
<td>27 Address Properties dialog Box (SNMP Tab)</td>
<td>167</td>
</tr>
<tr>
<td>28 SNMP settings in SAN Pilot or Connectrix Manager Basic</td>
<td>172</td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>29</td>
<td>Product type in SAN Pilot or Connectrix Manager Basic ............... 173</td>
</tr>
<tr>
<td>30</td>
<td>Product properties dialog box (Basic) ....................................... 205</td>
</tr>
<tr>
<td>31</td>
<td>Enterprise Fabric Mode dialog box ............................................ 215</td>
</tr>
<tr>
<td>32</td>
<td>Persisted fabric icon on physical map ........................................ 232</td>
</tr>
<tr>
<td>33</td>
<td>Persisted fabric icon on product list .......................................... 232</td>
</tr>
<tr>
<td>34</td>
<td>Product added to persisted fabric ............................................. 233</td>
</tr>
<tr>
<td>35</td>
<td>Product removed from persisted fabric ......................................... 233</td>
</tr>
<tr>
<td>36</td>
<td>Removed connection in a persisted fabric ..................................... 233</td>
</tr>
<tr>
<td>37</td>
<td>Product removed from persisted fabric ......................................... 234</td>
</tr>
<tr>
<td>38</td>
<td>Product removed from persisted fabric ......................................... 235</td>
</tr>
<tr>
<td>39</td>
<td>Export dialog box .......................................................................... 319</td>
</tr>
<tr>
<td>40</td>
<td>Export Dialog Box .......................................................................... 320</td>
</tr>
<tr>
<td>41</td>
<td>Directors containing virtual switches .......................................... 334</td>
</tr>
<tr>
<td>42</td>
<td>Physical map .................................................................................. 340</td>
</tr>
<tr>
<td>43</td>
<td>The Virtual Switches dialog box displays. .................................... 344</td>
</tr>
<tr>
<td>44</td>
<td>Event Management tab ..................................................................... 371</td>
</tr>
<tr>
<td>45</td>
<td>Router Port Configuration dialog box ............................................ 427</td>
</tr>
<tr>
<td>46</td>
<td>SAN Router Configuration dialog box ............................................. 437</td>
</tr>
<tr>
<td>47</td>
<td>Choose a background color dialog box ............................................ 453</td>
</tr>
<tr>
<td>48</td>
<td>The port Properties dialog box displays.Port Properties dialog box ... 457</td>
</tr>
<tr>
<td>49</td>
<td>Connectrix Manager web page ....................................................... 463</td>
</tr>
<tr>
<td>50</td>
<td>Internet Explorer security warning ............................................... 464</td>
</tr>
<tr>
<td>51</td>
<td>Netscape security warning ............................................................. 464</td>
</tr>
<tr>
<td>52</td>
<td>Backup and Restore Configuration dialog box .................................. 473</td>
</tr>
<tr>
<td>53</td>
<td>Information dialog box ................................................................... 473</td>
</tr>
<tr>
<td>54</td>
<td>Connectrix: Configure Sessions dialog box ...................................... 474</td>
</tr>
<tr>
<td>55</td>
<td>DialEMC Configuration dialog box ................................................... 475</td>
</tr>
<tr>
<td>56</td>
<td>Local Area Connection 2 Properties dialog box ............................... 476</td>
</tr>
<tr>
<td>57</td>
<td>Map Network Drive dialog box ....................................................... 477</td>
</tr>
<tr>
<td>58</td>
<td>Connectrix Manager 9.1 Configuration, Welcome dialog .................... 479</td>
</tr>
<tr>
<td>59</td>
<td>Connectrix Manager 9.1 Configuration, copy data and settings with defaults ................................................................................. 480</td>
</tr>
<tr>
<td>60</td>
<td>Copy Data and Settings showing the Installation Directory ................ 481</td>
</tr>
<tr>
<td>61</td>
<td>Copy and Data Settings (continued) showing the Data Directory ....... 482</td>
</tr>
<tr>
<td>62</td>
<td>Connectrix Manager Server License dialog box ................................. 483</td>
</tr>
<tr>
<td>63</td>
<td>Connectrix Manager Configuration 9.1, Server License Summary dialog box ....................................................................................... 484</td>
</tr>
<tr>
<td>64</td>
<td>Connectrix Manager 9.1 Log In dialog box ....................................... 485</td>
</tr>
<tr>
<td>65</td>
<td>Main window (Connectrix Manager) .................................................. 486</td>
</tr>
<tr>
<td>66</td>
<td>Backup and Restore Configuration dialog box .................................... 489</td>
</tr>
<tr>
<td>67</td>
<td>Information dialog box .................................................................... 490</td>
</tr>
<tr>
<td>68</td>
<td>Connectrix Configure Sessions dialog box ........................................ 491</td>
</tr>
<tr>
<td>69</td>
<td>DialEMC Configuration dialog box ................................................... 493</td>
</tr>
<tr>
<td>Page</td>
<td>Description</td>
</tr>
<tr>
<td>------</td>
<td>-------------</td>
</tr>
<tr>
<td>70</td>
<td>Connectrix Manager 9.1 Configuration, Welcome dialog box .......... 494</td>
</tr>
<tr>
<td>71</td>
<td>Connectrix Manager 9.1 Configuration, Copy Data and Settings with defaults dialog box ................................................. 495</td>
</tr>
<tr>
<td>72</td>
<td>Copy Data and Settings with Installation Directory shown ................ 496</td>
</tr>
<tr>
<td>73</td>
<td>Copy Data and Settings (continued) with Data Directory shown .......... 497</td>
</tr>
<tr>
<td>74</td>
<td>Connectrix Manager 9.1 Server License dialog box .......................... 498</td>
</tr>
<tr>
<td>75</td>
<td>Connectrix Manager 9.1 Server License Summary dialog box ............... 499</td>
</tr>
<tr>
<td>76</td>
<td>Connectrix Manager 9.1 Log In dialog box ........................................... 500</td>
</tr>
<tr>
<td>77</td>
<td>Main window (Connectrix Manager) ................................................ 501</td>
</tr>
<tr>
<td>78</td>
<td>Connectrix Manager 9.1 Configuration, Welcome dialog box ............... 507</td>
</tr>
<tr>
<td>79</td>
<td>Connectrix Manager 9.1 Configuration, Copy Data and Settings dialog box ........................................................................ 508</td>
</tr>
<tr>
<td>80</td>
<td>Copy Data and Settings for Connectrix Manager 8.1 ...................... 509</td>
</tr>
<tr>
<td>81</td>
<td>Copy Data and Settings for Connectrix Manager 8.6.1 .................... 510</td>
</tr>
<tr>
<td>82</td>
<td>Copy Data and Settings for Connectrix Manager 8.7.1 .................... 511</td>
</tr>
<tr>
<td>83</td>
<td>Copy Data and Settings for Connectrix Manager 8.9.1 .................... 512</td>
</tr>
<tr>
<td>84</td>
<td>Copy Data and Settings for Connectrix Manager 9.1 .................... 513</td>
</tr>
<tr>
<td>85</td>
<td>Nickname message ........................................................................ 513</td>
</tr>
<tr>
<td>86</td>
<td>Connectrix Manager 9.1 Server License dialog box ......................... 514</td>
</tr>
<tr>
<td>87</td>
<td>Connectrix Manager 9.1 Server License Summary dialog box ............ 515</td>
</tr>
<tr>
<td>88</td>
<td>Connectrix Manager 9.1 Log In dialog box ........................................... 516</td>
</tr>
<tr>
<td>89</td>
<td>Main window (Connectrix Manager) ................................................ 517</td>
</tr>
<tr>
<td>90</td>
<td>Connectrix Management web page .................................................. 518</td>
</tr>
<tr>
<td>91</td>
<td>SNMP MIB files download area .......................................................... 531</td>
</tr>
<tr>
<td>92</td>
<td>DialEMC Configuration dialog box .................................................. 678</td>
</tr>
<tr>
<td>93</td>
<td>Call Home Configuration dialog box ................................................ 679</td>
</tr>
<tr>
<td>94</td>
<td>Call Home Configuration dialog box with example data .................. 680</td>
</tr>
<tr>
<td>95</td>
<td>ConnectEMC Installation dialog box .................................................. 681</td>
</tr>
<tr>
<td>96</td>
<td>Installing dialog box .................................................................... 682</td>
</tr>
<tr>
<td>97</td>
<td>Installation complete dialog box .................................................... 682</td>
</tr>
<tr>
<td>98</td>
<td>View All – Connectrix Manager window ........................................... 683</td>
</tr>
<tr>
<td>99</td>
<td>ConnectEMC Console dialog box ....................................................... 684</td>
</tr>
<tr>
<td>100</td>
<td>New Dialup Connection dialog box .................................................. 685</td>
</tr>
<tr>
<td>101</td>
<td>New Dialup Connection – First Call Home number .......................... 686</td>
</tr>
<tr>
<td>102</td>
<td>New Dialup Connection – Second Call Home number .......................... 687</td>
</tr>
<tr>
<td>103</td>
<td>Completed setup ............................................................................. 688</td>
</tr>
<tr>
<td>104</td>
<td>New Email Connection dialog box .................................................... 689</td>
</tr>
<tr>
<td>105</td>
<td>New Email Connection dialog box (completed) ............................... 690</td>
</tr>
<tr>
<td>106</td>
<td>ConnectEMC Console (Setup completed) .............................................. 691</td>
</tr>
<tr>
<td>107</td>
<td>Connectrix Manager server and client communications .................... 704</td>
</tr>
<tr>
<td>108</td>
<td>Run&gt;regedit .................................................................................... 717</td>
</tr>
<tr>
<td>109</td>
<td>Registry Editor&gt;My Computer, HKEY_LOCAL_MACHINE ...................... 717</td>
</tr>
<tr>
<td>110</td>
<td>Registry Editor Parameters ............................................................. 718</td>
</tr>
<tr>
<td></td>
<td>Description</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>111</td>
<td>Registry Editor, New, Key, DWORD Value</td>
</tr>
<tr>
<td>112</td>
<td>Registry Editor&gt; DisableDHCPMediaSense</td>
</tr>
<tr>
<td>113</td>
<td>Edit DWORD Value</td>
</tr>
<tr>
<td>114</td>
<td>Registry Editor&gt; DisableDHCPMediaSense Modified</td>
</tr>
<tr>
<td>Title</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>1 Linux system requirements for the client</td>
<td>42</td>
</tr>
<tr>
<td>2 Connectrix Manager software features</td>
<td>43</td>
</tr>
<tr>
<td>3 Steps</td>
<td>45</td>
</tr>
<tr>
<td>4 Backup icons</td>
<td>63</td>
</tr>
<tr>
<td>5 Product icons</td>
<td>73</td>
</tr>
<tr>
<td>6 Product status icons</td>
<td>73</td>
</tr>
<tr>
<td>7 Event icons</td>
<td>74</td>
</tr>
<tr>
<td>8 Keyboard shortcuts</td>
<td>74</td>
</tr>
<tr>
<td>9 Event icons</td>
<td>82</td>
</tr>
<tr>
<td>10 Connectrix Manager Classic display settings</td>
<td>106</td>
</tr>
<tr>
<td>11 Manager of Manager ECC-API discovery</td>
<td>152</td>
</tr>
<tr>
<td>12 Product status icons</td>
<td>206</td>
</tr>
<tr>
<td>13 Fields and descriptions</td>
<td>261</td>
</tr>
<tr>
<td>14 Administrator zoning privileges</td>
<td>296</td>
</tr>
<tr>
<td>15 Utilization legend description</td>
<td>314</td>
</tr>
<tr>
<td>16 Comparing fabrics created from virtual switches and partitions</td>
<td>333</td>
</tr>
<tr>
<td>17 Comparing fabrics created from virtual switches and zoning</td>
<td>336</td>
</tr>
<tr>
<td>18 Fields and description</td>
<td>371</td>
</tr>
<tr>
<td>19 Operators and values</td>
<td>376</td>
</tr>
<tr>
<td>20 Type of edit</td>
<td>385</td>
</tr>
<tr>
<td>21 Product property set</td>
<td>392</td>
</tr>
<tr>
<td>22 Post property set</td>
<td>394</td>
</tr>
<tr>
<td>23 System property set</td>
<td>395</td>
</tr>
<tr>
<td>24 Device operational status even property set</td>
<td>397</td>
</tr>
<tr>
<td>25 Ethernet event property set</td>
<td>398</td>
</tr>
<tr>
<td>26 Fabric event property set</td>
<td>399</td>
</tr>
<tr>
<td>27 Performance event property set</td>
<td>399</td>
</tr>
<tr>
<td>28 Product audit event property set</td>
<td>400</td>
</tr>
<tr>
<td>29 Product event property set</td>
<td>401</td>
</tr>
<tr>
<td>30 Product hardware event property set</td>
<td>401</td>
</tr>
<tr>
<td>Page</td>
<td>Section</td>
</tr>
<tr>
<td>------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>31</td>
<td>Product link incident event property set</td>
</tr>
<tr>
<td>32</td>
<td>Product state event property set</td>
</tr>
<tr>
<td>33</td>
<td>Product threshold alert event property set</td>
</tr>
<tr>
<td>34</td>
<td>Security event property set</td>
</tr>
<tr>
<td>35</td>
<td>Session event property set</td>
</tr>
<tr>
<td>36</td>
<td>SNMP trap event property set</td>
</tr>
<tr>
<td>37</td>
<td>User action event property set</td>
</tr>
<tr>
<td>38</td>
<td>User property set</td>
</tr>
<tr>
<td>39</td>
<td>Event context property set</td>
</tr>
<tr>
<td>40</td>
<td>Product context property set</td>
</tr>
<tr>
<td>41</td>
<td>Port context property set</td>
</tr>
<tr>
<td>42</td>
<td>TIME context property set</td>
</tr>
<tr>
<td>43</td>
<td>System context property set</td>
</tr>
<tr>
<td>44</td>
<td>User context property set</td>
</tr>
<tr>
<td>45</td>
<td>Configuration reports</td>
</tr>
<tr>
<td>46</td>
<td>Port types</td>
</tr>
<tr>
<td>47</td>
<td>Connectrix Service Processor Connectivity Group table</td>
</tr>
<tr>
<td>48</td>
<td>Connectrix Service Processor ConnUnit table</td>
</tr>
<tr>
<td>49</td>
<td>Connectrix Service Processor Firmware table</td>
</tr>
<tr>
<td>50</td>
<td>Connectrix Service Processor Sensor table</td>
</tr>
<tr>
<td>51</td>
<td>Connectrix Service Processor Port table</td>
</tr>
<tr>
<td>52</td>
<td>Connectrix Service Processor Event table</td>
</tr>
<tr>
<td>53</td>
<td>Connectrix Service Processor Link table</td>
</tr>
<tr>
<td>54</td>
<td>Connectrix Service Processor Port Statistics table</td>
</tr>
<tr>
<td>55</td>
<td>Name Server table</td>
</tr>
<tr>
<td>56</td>
<td>SNMP Trap Registration Group table</td>
</tr>
<tr>
<td>57</td>
<td>Trap Registration table</td>
</tr>
<tr>
<td>58</td>
<td>Trap type table</td>
</tr>
<tr>
<td>59</td>
<td>Director/Switch type definition table</td>
</tr>
<tr>
<td>60</td>
<td>Connectivity Unit Group table</td>
</tr>
<tr>
<td>61</td>
<td>fcConnUnit table</td>
</tr>
<tr>
<td>62</td>
<td>Firmware table</td>
</tr>
<tr>
<td>63</td>
<td>Sensor table</td>
</tr>
<tr>
<td>64</td>
<td>Port table</td>
</tr>
<tr>
<td>65</td>
<td>Event table</td>
</tr>
<tr>
<td>66</td>
<td>Link table</td>
</tr>
<tr>
<td>67</td>
<td>Port Statistics table</td>
</tr>
<tr>
<td>68</td>
<td>Name Server table</td>
</tr>
<tr>
<td>69</td>
<td>Trap Registration Group table</td>
</tr>
<tr>
<td>70</td>
<td>SNMP Trap Registration table</td>
</tr>
<tr>
<td>71</td>
<td>Trap type table</td>
</tr>
<tr>
<td>72</td>
<td>Supported MIB-II Objects</td>
</tr>
<tr>
<td>73</td>
<td>Master log parameters</td>
</tr>
<tr>
<td>Page</td>
<td>Section</td>
</tr>
<tr>
<td>------</td>
<td>-------------------------------------------------------------------------</td>
</tr>
<tr>
<td>74</td>
<td>Security Log handling</td>
</tr>
<tr>
<td>75</td>
<td>RMI protocol level</td>
</tr>
<tr>
<td>76</td>
<td>Privileges</td>
</tr>
<tr>
<td>77</td>
<td>User groups</td>
</tr>
<tr>
<td>78</td>
<td>User groups and assigned privileges for fresh install</td>
</tr>
<tr>
<td>79</td>
<td>Element Manager privileges and access control (For managed products)</td>
</tr>
<tr>
<td></td>
<td>other than an ED-10000M</td>
</tr>
<tr>
<td>80</td>
<td>Access control for ED-10000M products</td>
</tr>
<tr>
<td>81</td>
<td>Product icons</td>
</tr>
<tr>
<td>82</td>
<td>Product status icons</td>
</tr>
<tr>
<td>83</td>
<td>Event icons</td>
</tr>
<tr>
<td>84</td>
<td>Keyboard shortcuts</td>
</tr>
</tbody>
</table>
As part of an effort to improve and enhance the performance and capabilities of its product line, EMC from time to time releases revisions of its hardware and software. Therefore, some functions described in this document may not be supported by all revisions of the software or hardware currently in use. For the most up-to-date information on product features, refer to your product release notes.

If a product does not function properly or does not function as described in this document, please contact your EMC representative.

Note: Any reference in text and/or screen shots in this manual regarding Connectrix Manager version 9.0. or 9.1 can be used interchangeably; they are all one in the same.

Audience
This publication is intended for data center administrators, LAN administrators, operations personnel, and customer support personnel who administer user access to the Connectrix Manager application.

Related documentation
Related documents include:

- *Connectrix DS-16M2 and DS-32M2 Fibre Channel Switch User Guide*, P/N 300-001-471
- *Connectrix DS-24M2 Fibre Channel Switch User Guide*, P/N 300-001-775
- *Connectrix Enterprise Director ED-10000M User Guide*, P/N 300-002-400
Conventions used in this Guide

EMC uses the following conventions for notes, cautions, and warnings.

A note presents information that is important, but not hazard-related.

CAUTION

A caution contains information essential to avoid data loss or damage to the system or equipment. The caution may apply to hardware or software.

WARNING

A warning contains information essential to avoid a hazard that can cause severe personal injury, death, or substantial property damage if you ignore the message.

Typographical conventions

EMC uses the following type style conventions in this guide:

In running text:

- Interface elements (for example, button names, dialog box names) outside of procedures
- Items that user selects outside of procedures
- Java classes and interface names
- Names of resources, attributes, pools, Boolean expressions, buttons, DQL statements, keywords, clauses, environment variables, filenames, functions, menu names, utilities
- Pathnames, URLs, filenames, directory names, computer names, links, groups, service keys, file systems, environment variables (for example, command line and text), notifications

- User actions (what the user clicks, presses, or selects)
- Interface elements (button names, dialog box names)
- Names of keys, commands, programs, scripts, applications, utilities, processes, notifications, system calls, services, applications, and utilities in text
EMC Connectrix Manager User Guide

Preface

Where to get help

EMC support, product, and licensing information can be obtained as follows.

Product information — For documentation, release notes, software updates, or for information about EMC products, licensing, and service, go to the EMC Powerlink website (registration required) at:

http://Powerlink.EMC.com

Technical support — For technical support, go to EMC WebSupport on Powerlink. To open a case on EMC WebSupport, you must be a WebSupport customer. Information about your site configuration and the circumstances under which the problem occurred is required.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Please send your opinion of this guide to:

techpub_comments@EMC.com
This chapter presents an overview of Connectrix Manager.

- Connectrix Manager overview ....................................................... 36
- Connectrix service processor ............................................................ 39
**Connectrix Manager overview**

*Note:* Any reference in text and/or screen shots in this manual regarding Connectrix Manager version 9.1 or 9.1.0 can be used interchangeably; they are all one in the same.

The EMC® Connectrix® Management system is a client/server application that runs on the Connectrix service processor. The client can also run on remote workstations on the network. Up to twenty-five concurrent remote users (in addition to the local Connectrix service processor user) can log in to the Connectrix Manager application.

For details on configuring remote workstations, refer to Appendix A, “Configuring Remote Workstations”.

Subsequent references in this document to the Connectrix Manager imply the Connectrix Manager client application whether running locally on the service processor or a remote client unless otherwise noted.

When logging into Connectrix Manager at the 1U service processor, you are actually using a local Connectrix Manager client. The Connectrix Management services run in the background on the 1U rackmount service processor.

*Note:* Connectrix Manager 8.x on the 1U server supports a limited number of managed switches. For more information, please refer to the latest version of the Connectrix Manager Release Notes.
Connectrix Manager components

The Connectrix Management system is a Java-based graphical user interface (GUI) that provides local access to managed products. The management system is composed of the Connectrix Manager and Element Manager.

The Connectrix Manager and Element Manager are separate applications; however, the Element Manager is accessible only through the Connectrix Manager.
Access method

Only one Connectrix service processor can manage any given fabric. You cannot have more than one Connectrix service processor attempt to manage the same directors/switches and/or fabrics. Attempting to do this will yield inconsistent results; errors will occur in zoning, discovery, and monitoring of products.

The recommended access method to the Connectrix Manager application on the service processor is by logging in locally on the service processor and launching the client application or by launching a Connectrix Manager client on a remote workstation. The remote workstation client application would communicate with the service processor using the public LAN interface on the service processor, identified below as Adapter 1.

- Adapter 1 can be connected to the customer’s ethernet LAN providing remote management via Connectrix Manager clients installed on remote workstations.

Note: This is optional and dependant upon how the customer wishes to manage their Connectrix environment.

It is recommended that the network segment used for remote access be configured as a semi-private network for use by remote management workstations. Each customer will have to determine how they want to manage the service processor and how open the network is to which they connect the service processor.

- Adapter 2 links the Connectrix directors and switches with the Connectrix service processor over a private network.

The Connectrix cabinet ships from the factory with this configuration, which should not be changed unless absolutely necessary. If this is a requirement, contact your EMC Global Services Representative for further information.

Figure 1 on page 37 shows an example of the dual Ethernet configuration.
Connectrix service processor

The Connectrix service processor is a rackmount platform (with a separate keyboard/video assembly) that provides a central point of control for managed Fibre Channel products. The service processor is required for installing, configuring, and managing these products.

Although products can perform normal operations without a Connectrix service processor, the service processor should operate at all times to monitor product operations, report failures, log event and configuration changes, and call home to the EMC Support Center.

Automatic Data Backup (update to CD-RW)

Automatic Data Backup is accomplished using the CD-RW drive in the 1U rackmount service processor.

The directories that contain the Connectrix Manager data are $<Install_Home>/Server$, $<Install_Home>/Client$, $<Install_Home>/Backup$, and $<Install_Home>/Call Home$ directories (where $<Install_Home>$ is the C:\Program Files\Connectrix Manager 9.1 directory where the Connectrix Manager application is installed).

Whenever you make a configuration change, add or remove a managed product, or make any other changes through the Connectrix Manager or Element Manager, the data is backed up automatically.
This chapter contains the following information.

- Overview ............................................................................................. 42
- Client system requirements .............................................................. 42
- Product licensing overview .............................................................. 43
- Getting a license key ........................................................................ 49
- Starting the application ..................................................................... 50
- Closing the application .................................................................... 72
- Searching the online help .................................................................. 72
- Icon legends ........................................................................................ 73
- Keyboard shortcuts ............................................................................ 74
Overview

The Connectrix Manager services and application run on the EMC 1U service processor. Remote Connectrix Manager client applications run on a customer workstation. A maximum of twenty-five (25) client applications can be logged into the Connectrix Manager services on the 1U service processor at any given time, including the local Connectrix Manager application running on the 1U service processor.

Connectrix Manager Release 9.1 is available for installation on a management server supplied by EMC or your own management server.

Client system requirements

The Connectrix Manager remote client application has the following system requirements shown in Table 1.

Note: A maximum of 25 Clients are allowed per Connectrix Manager Enterprise edition Server.

Table 1 Linux system requirements for the client

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Requirement Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>1 GHz Intel Pentium III and up</td>
</tr>
<tr>
<td>Hardware</td>
<td>CD-ROM</td>
</tr>
<tr>
<td>Operating system</td>
<td>Red Hat Enterprise Linux ES 3.0</td>
</tr>
<tr>
<td></td>
<td>Redhat 9.0 kernel v. 2.4.20-8</td>
</tr>
<tr>
<td></td>
<td>Redhat 8.0 kernel v. 2.4.18-14</td>
</tr>
<tr>
<td>Memory</td>
<td>512 MB RAM (minimum)</td>
</tr>
<tr>
<td>Disk space</td>
<td>350 MB disk space</td>
</tr>
<tr>
<td>Video requirements</td>
<td>8 MB Video RAM</td>
</tr>
<tr>
<td>Resolution</td>
<td>256 colors</td>
</tr>
</tbody>
</table>
Product licensing overview

License and feature keys are unique strings of alphanumeric characters that verify ownership of the Connectrix Manager application software and additional software modules as well as software features within the switches or directors that you purchased.

License keys

License keys allow you to access the features that you purchase with the Connectrix Manager application software package. Depending on the software package you purchase, you may have any of the following features:

<table>
<thead>
<tr>
<th>Features</th>
<th>Enterprise Edition</th>
<th>Enterprise Edition Optional Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Module</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Event Management</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Group Configuration</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auto - Discovery</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Backup</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Call Home</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Export to Database</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Planning</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Remote Discovery Connector</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SAN Routing</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>SNMP Agent</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Topology Layout Customization</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>User Group Management</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>View Management</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Virtual Fabrics</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Zoning</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>
Note the following items regarding the Connectrix Manager software application for this release:

- In the **License** dialog box, the **Licensed Ports** field indicates the number of ports for which you have licenses, for the optional software modules.

- The number of ports in the licensed optional software modules must be equal to or greater than the number of currently discovered ports.

- All of the software modules that are port-based must have the same number of ports activated. For example, if you have 128 ports for Performance and want to add the Event Management module, you must purchase 128 ports for Event Management.

- The serial number cannot be changed without reinstalling the software.

Depending on whether you are installing for the first time, adding additional features, adding ports, or upgrading to a new version, you need to complete the following steps:

- Obtain the license key
- Enter the license key
- Enter the software serial number
Table 3 details which steps you need to perform to complete the installation or upgrade process.

Table 3  Steps

<table>
<thead>
<tr>
<th>Obtain license key</th>
<th>Enter serial number</th>
<th>Enter license key</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing the software application for the first time</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Purchasing Additional Software Modules</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Purchasing Ports</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Upgrading Connectrix Manager</td>
<td>X*</td>
<td>X</td>
</tr>
</tbody>
</table>

* a. You will need to enter the license key and serial number when upgrading from Connectrix Manager 8.1, 8.6.1, 8.7.1, or 8.9.1.

To obtain the license key, follow instructions provided:

1. Type the management application’s 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. See “Getting a license key” on page 49.

2. To access the License dialog box in the application, click Help and License.
3. Enter the serial number in the **Serial Number** field and enter the license key into the **License Key** field.

![License dialog box](image)

**Figure 2** License dialog box

Following are important notes about the Connectrix Manager software application for this release.

- In the **License** dialog box, the **Licensed Ports** field indicates the number of ports that you are licensed for the optional software modules.
- The number of ports in the optional software module licensed must be equal to or greater than the number of currently discovered ports.
- All of the software modules that are port-based must have the same number of ports activated. For example, if you have 128 ports of Performance and want to add the Event Management module, you must purchase 128 ports of Event Management.
- The serial number cannot be changed without reinstalling the software.

**Entering a license key**

A license key is required to run the application. The key specifies the maximum number of switch ports you can monitor as well as any licensed optional features or modules.
1. In the application, select **License** from the **Help** menu.

The **License** dialog box displays (Figure 3).

![License dialog box](image)

**Figure 3** License dialog box

2. In the **License Key** field, enter the license key.

   **Note:** The **License Key** field is not case-sensitive.

3. Click **Update** and ensure that the information is accurate.

   **Note:** The **License** dialog box displays the license information for the Server to which the Client is currently connected. When you click **Update**, the dialog box will decode the key you entered and display the new license information without setting a new license on the Server. The information will be set on the Server only when you click **OK**.

4. Click **OK** to enable the software.

   The application will automatically log out and the **Log In** dialog box will display. Log in using the instructions in “Logging in to a server” on page 96.

**Retrieving lost keys**

If you have lost your license key:

1. Go to the URL listed on the transaction code certificate.
2. Click the **Unit Information** menu.
3. Enter your product’s serial number or key.
4. Click Next.

The product information will display.

**Ordering additional features**

To order new features or increase managed port capabilities, contact your sales representative.

**Feature keys (switch or director Element Managers)**

Feature keys verify ownership of the Element Manager and optional feature, and allows you to access the software features that you have purchased in the switch or director. The feature key, which is encoded with a switch or director’s serial number, can only be configured on the switch or director to which it is assigned. Here are some important notes about the Element Manager feature key for this release.

- Enabling the Reset Configuration option through the Element Manager Maintenance menu clears all features that were enabled through the Configure Feature Key dialog box. When you attempt to re-install features using a feature key assigned for version E/OS 5, a warning displays that the feature key is not installed. You must contact customer support to get a feature key re-assigned.

- For directors with E/OS 6.0 or greater installed, feature keys for all purchased software features are activated automatically.

- For each switch with E/OS 6.0 or greater installed, you need a feature key to enable the Element Manager and any other additional software features within the switch.

- When you purchase additional software features for a director or switch, you receive a new feature key that includes existing features purchased previously. Use the Configure Feature Key dialog box in the Element Manager to activate the new features.
Getting a license key

In order to activate the application, you will need to request a license key.

Getting a license key for new software

If you just purchased the application, use these instructions to obtain your license key.

1. Go to the URL listed on the transaction code certificate.
2. In the Serial Number field, type the serial number.
   You can find the serial number on the back of the software CD case.
3. In the Transaction Code fields, type the transaction code(s) shipped with the software.
4. Click Next.
5. Confirm the existing and new features to be enabled.
6. Click Next.
   The license key and all enabled features will display.
7. Print or email the information to retain a copy for your records.
   You will need to enter this key during the installation process.

Where to start

If you are installing the Connectrix Manager application for the first time and you are not upgrading from a previous release, then proceed to “Starting the application” on page 50.

If you are upgrading a Laptop running Connectrix Manager v7.01 to a 1U Server running Connectrix Manager v9.1, then proceed to Appendix B, “Upgrading to Connectrix Manager 9.1”.

If you are upgrading an existing 1U Server from Connectrix Manager v7.02, v8.01, v8.06.01, v8.07.01, v8.09.01, or v9.0 to Connectrix Manager v9.1, refer to Appendix B, “Upgrading to Connectrix Manager 9.1”.

Getting a license key
Starting the application

The procedure outlined below for starting Connectrix Manager for the first time is for a new installation ONLY without any upgrade or data migration.

If you need to perform and upgrade from Connectrix Manager v7.02, v8.01, v8.06.01, 8.07.01 v8.09.01, or v9.0 on a 1U rack mount server or migrate data from a laptop-based service processor to a new 1U rack mount server, refer to Appendix B, “Upgrading to Connectrix Manager 9.1”.

Note: If upon powering up the EMC-Supplied 1u service processor for the first time you are prompted to input the Microsoft Windows 2003 “Product ID”, the Certificate of Authenticity containing the 25 character Product ID or License is located atop the right-hand corner of the 1u server.

Once the license has been entered it must then be activated by contacting Microsoft either via the Internet or by phone. If the customer fails to activate within 30 days upon entering the license, services will continue to work but they will no longer be able to log in.

They will then be forced to contact Microsoft in order to re-gain access to Windows. For more information, refer to the following Microsoft web site: http://www.microsoft.com/windowsserver2003/techinfo/overview/activation.mspxr.

Starting Connectrix Manager for Windows Systems

The 1U server should have shipped from the factory with the Connectrix Manager application pre-installed. If not, proceed to the first step. If it is already installed, proceed to Step 2.

1. Install Connectrix Manager 9.1 on the 1U server.
   a. Insert the Software distribution CD provided with your kit into the CD-ROM drive. If autorun is enabled, the installer begins automatically. If it is not enabled, double-click the setup.exe file on the CD. The InstallAnywhere wizard will take you through the installation process.
   b. The Connectrix Manager 9.1 splash screen is briefly displayed followed by the Introduction screen. Click Next.
c. The Choose Install Set screen is displayed. Select Server and Client, and click Next.

d. The Select Install Folder screen is displayed. Click Next to accept the default Destination Folder C:\Program Files\Connectrix Manager 9.1.

e. On the Pre-Installation Summary screen, review the your installation settings and click Install.

f. On the Installation Complete screen, make sure the Launch Configuration Wizard checkbox is selected (default), and click Done.

2. Complete the installation.

a. The Welcome page should appear (Figure 4). If not, on the 1U server, go to Start, Programs, Connectrix Manager 9.1 and select Connectrix Manager 9.1.

Figure 4  Connectrix Manager 9.1 Configuration dialog box (Welcome)
b. Click Next. The License Agreement panel displays.

c. Select Yes and click Next. The Copy Data and Settings dialog box displays (Figure 5).

![Connectrix Manager 9.1 Configuration dialog box](image)

**Copy Data and Settings**

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?

- Yes - Specify the install path to the previous version
- No

![Figure 5](image)

**Figure 5** Connectrix Manager configuration dialog box (copy data and settings)

d. Click No, and then click Next. The Connectrix Manager 9.1 Server Name dialog displays.

e. Enter the name you want to assign the server. Enter a name of fewer than 20 characters for the server.
f. Click Next. The Connectrix Manager 9.1 Server License dialog displays (Figure 6).

![Connectrix Manager 9.1 Configuration](image)

Connectrix Manager 9.1 Server License

Please enter the Serial Number and License Key below.

Serial Number

License Key

Figure 6 Connectrix Manager configuration serial number and license key dialog box

g. Type the management application’s 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 49.
h. Click Next. The second Connectrix Manager 9.1 License panel displays (Figure 7).

![Connectrix Manager 9.1 Configuration]

Connectrix Manager 9.1 Server License Summary

Please verify the contents of your configuration and license.

- User ID: Administrator
- Connectrix Manager 9.1 Server Name: CONNECTRIX/SVT
- Win32® Service: Automatic/Start Now
- Copy Data and Settings: Yes
- Version: Connectrix Manager 9.1
- Build: 40
- Expiration: None
- Clients: 25
- Licensed Ports: 4096
- Modules
  - Group Configuration Manager: Enabled

Figure 7  Connectrix Manager configuration verification dialog box

i. Verify configuration and license information and click Finish.

j. A Connectrix Manager 9.1 Message window will appear informing you to close the Services window. After you ensure it is closed, click OK. A message, Applying user settings, please wait…., will appear until the installation process completes.
k. When the installation completes, the **Connectrix Manager 9.1 Log In** dialog box displays (Figure 8).

![Figure 8 Connectrix Manager Log In dialog box](image)

1. At the **Connectrix Manager 9.1 Log In** dialog box, type the Connectrix Manager application user identification and password in the **User ID** and **Password** fields. Default User ID for Connectrix Manager is **Administrator**, the default password is **password**. Network address should be left at **localhost**.

m. Click **Login**. The application opens and the **Connectrix Manager** main window appears.

n. Insert a blank **pre-formatted** CD-RW disk into the CD-RW drive on the 1U service processor. The Connectrix Manager data contained in the `C:\Program Files\Connectrix Manager 9.1` directory is automatically backed up to the CD-RW drive as long as a formatted CD-RW disk remains in the drive.

**Note:** Three options are available for backing up the management server: Writable CD, Hard drive, and Network drive. In addition, Connectrix Manager 9.1 has a "Backup Now" feature which will perform an immediate backup to any one of these three options.
Getting Started

**Important:** Do not format a blank CD-RW disk while the Connectrix Manager application is running. Ensure the Connectrix Manager Services have been stopped before proceeding. For more information, refer to EMC Knowledgebase solution emc96761.

3. Connect the modem to the COM1 port on the 1U server. Using the new modem cable supplied with the 1U server, connect the DB9 end to the COM1 port on the 1U server and the DB25 end to the modem port.

4. Reboot the 1U server. Login to Connectrix Manager.
   a. On the 1U server, go to **Start, Programs, Connectrix Manager 9.1** and select **Connectrix Manager 9.1**.
   b. At the **Connectrix Manager 9.1 Login In** dialog box, type the Connectrix Manager application user identification and password in the **User ID** and **Password** fields. Default User ID for Connectrix Manager is **Administrator**, the default password is **password**. Network address should be left a **localhost**.
   c. Click **Login**. The application opens and the Connectrix Manager main window displays.

5. Install ConnectEMC and then configure and test the Call-home feature. For more information, refer to Appendix G, “Call Home Setup Procedure”.

6. If required, load the FibreZoneBridge/Connectrix Bridge to support EMC ControlCenter. The FibreZoneBridge/Connectrix Bridge and the installation notes are available for download from the Powerlink website at http://Powerlink.emc.com.

7. It is the customer’s responsibility to load any Microsoft patches and anti-virus protection software.
Backing up and restoring data

The Connectrix Manager application helps you to protect your SAN data by backing it up automatically. The data can then be restored, as necessary.

Backup occurs, if needed, approximately every six hours and may take as long as six hours and 15 minutes maximum. However, the backup cycle interval can be adjusted. The minimum value is 15 minutes and the maximum value is 360 minutes.

Note: Backing up data takes some time. It is possible that, in a disaster recovery situation, configuration changes made after the last backup interval will be missing from the backup.

The Connectrix Manager application allows you to view the backup status at a glance, initiate immediate backup, enable or disable automatic backup, reconfigure the backup directory, interval, and start time, and retrieve backup events.

What is backed up?

The backed up data is contained in the following directories:

- `<Install_Home>\Backup`
- `<Install_Home>\Call Home`
- `<Install_Home>\Client`
- `<Install_Home>\Server`

Note: `<Install_Home>` refers to the directory where the Connectrix Manager application is installed.

The data in those directories is automatically backed up to disk. The data includes the following items:

- All data saved through the Export function.
- All log files.
- All plans saved through the Planning function.
- All reports generated.
- Application configuration data.
- Backup configuration.
Getting Started

- Call-home configuration (including phone numbers and dialing options). Note that Call-home functions may be optional, depending on your purchased software package.
- License information.
- Performance data.
- User-defined sounds.
- User-launched scripts.
- Zoning library (all zones sets and zone definitions) saved through the Zoning function.

**Important:** Firmware files are NOT backed up.

Management server backup

There are three options for backing up data to the management server:
- “Configuring backup to a writable CD”
- “Configuring backup to a hard drive”
- “Configuring backup to a network drive”

The rack-mount Management Server is backed up to a rewritable (CD-RW) compact disk, by default. Make sure you have a CD-RW disk in the CD recorder drive to ensure that backup can occur. Critical information from the Connectrix Manager application is automatically backed up to the CD-RW when the data directory contents change or when you restart the Connectrix Manager application.

Note that backing up to CD is not the recommended method. The usable capacity of a CD is approximately 700 MB and needs to be replaced when full. Also, CD media has a limited number of re-writes before the medium is exhausted, and write errors occur. It is recommended that you configure the backup system to target a hard drive or a network drive as described in the procedures below.

Back up directory structure overview

Connectrix Manager Connectrix Managerbacks up data to two alternate folders. For example, if the backup directory location is D:\Backup, the backup service alternates between two backup directories, D:\Backup and D:\BackupAlt. The current backup is
always D:\Backup and contains a complete backup of the system. The older backup is always D:\BackupAlt.

If a backup cycle fails, the cause is usually a full CD-RW. When the backup cycle fails, there may only be one directory, D:\Backup. There may also be a D:\BackupTemp directory. Ignore this directory since it may be incomplete.

### Configuring backup to a writable CD

**Note:** This is not recommended on a permanent basis. CDs have a limited life, and may only last a month. An error message occurs if your Connectrix Manager application can no longer back up to the disc.

To configure the backup function to a writable CD, complete the following steps:

1. Select **SAN > Options**.
   
   The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.
   
   The currently defined directory displays in the **Backup Output Directory** field.

3. Select the **Enable backups** check box, if necessary.

4. In the **Next Backup Start Time Hours** and **Minutes** fields, enter the time (using a 24-hour clock) you want to backup process to begin.

5. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.

6. Verify that the CD backup directory is correct (default directory is D:\Backup).
   
   It is assumed that drive D is a CD-RW drive.
   
   You can change the directory or use the **Browse** button to select another directory.

7. Install the formatted disc into the CD drive.
   
   To back up to a writable CD, you must have CD-writing software installed. The disc must be formatted by the CD-writing software so that it behaves like a drive.
8. Click **Apply** or **OK**.

   The application verifies that the backup device exists and that the server can write to it. If the device does not exist or is not writable, an error message displays that says you have entered an invalid device. Click **OK** to go back to the **Options** dialog box and fix the error.

   Backup occurs, if needed, at the interval you specified.

---

**Configuring backup to a hard drive**

*Note: This requires a hard drive. The drive should not be the same physical drive on which your Operating System or Connectrix Manager Connectrix Manager is installed.*

To configure the backup function to a hard drive, complete the following steps:

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. Select **Backup** in the **Category** list.

   The currently defined directory displays in the **Backup Output Directory** field.

3. Select the **Enable backups** check box, if necessary.

4. In the **Next Backup Start Time Hours** and **Minutes** fields, enter the time (using a 24-hour clock) you want to backup process to begin.

5. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.

6. Click **Browse** to choose the hard drive and directory to which you want to backup your data.

7. Click **Apply** or **OK**.

   The application verifies that the backup device exists and that the server can write to it.

   If the device does not exist or is not writable, an error message displays that states you have entered an invalid device. Click **OK** to go back to the **Options** dialog box and fix the error.
Backup occurs, if needed, at the interval you specified.

**Configuring backup to a network drive**

*Note:* To back up to a network drive, your workstation can be either in the same domain or in the same workgroup. However, you must have rights to copy files for the network drive. Also, the user account name and password on the IU Server must match the user account name and password on the customer's server that is sharing the network drive.

*Note:* It is recommended that this configuration be completed on the Local client (the client application running on the Server) so that the backup path and location can be confirmed (step 5).

To configure the backup function to a network drive, complete the following steps:

1. Select **SAN > Options**. The **Options** dialog box displays.
2. Select **Backup** in the **Category** list. The currently defined directory displays in the **Backup Output Directory** field.
3. Select the **Enable backups** check box, if necessary.
4. In the **Next Backup Start Time Hours** and **Minutes** fields, enter the time (using a 24-hour clock) you want to backup process to begin.
5. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
6. In the Output Directory field, enter the path of the network drive. Do not click **Browse**, but rather enter the full network path to your destination directory, such as: `\network-server-name\shared-folder-name\Backup`. Do not use the drive letter format (C:\directory).

Where **Backup** = the name of a sub-folder in the shared folder on the network share.

You must have this sub-folder created and entered in the full Backup Output Directory path statement.
7. In the **Domain Workgroup** field, enter the name of the **Windows** domain or workgroup in which you are defined.

   **Note:** You must be authorized to write to the network device.

8. In the **User Name** field, enter your **Windows** login name.

9. In the **Password** field, enter your **Windows** password.

10. Click **Apply** or **OK**.

    The application verifies that the device is accessible and that the server can write to it.

    If the device does not exist or you are not authorized to write to the network drive, an error message displays that states you have entered an invalid device path or invalid network credentials. Click **OK** to go back to the **Options** dialog box and fix the error.

    Backup occurs, if needed, at the interval you specified.

---

**Enabling backup**

To enable the backup function, complete the following steps:

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. In the **Category** list, select **Backup**.

3. Select the **Enable backups** check box.

4. Click **Apply** or **OK** to save your changes.

---

**Disabling backup**

Backup is enabled by default. If you want to stop the backup process, you need to disable backup. To disable the backup function, complete the following steps:

1. Select **SAN > Options**.

   The **Options** dialog box displays.

2. In the **Category** list, select **Backup**.

3. Clear the **Enable backups** check box.

4. Click **Apply** or **OK** to save your changes.
Viewing the backup status

The Connectrix Manager application enables you to view the backup status at a glance by providing a backup status icon on the Status Bar. The following icons show the current status of the backup function:

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Backup in Progress" /></td>
<td>Backup in Progress—displays the following tooltip: “Backup started at hh:mm:ss, in progress... XX files in &lt;directory_name&gt; are backed up.”</td>
</tr>
<tr>
<td><img src="image2" alt="Countdown to Next Scheduled Backup" /></td>
<td>Countdown to Next Scheduled Backup—displays the following tooltip: “Next backup scheduled in XX minutes.”</td>
</tr>
<tr>
<td><img src="image3" alt="Backup Disabled" /></td>
<td>Backup Disabled—displays the following tooltip: “Backup is disabled.”</td>
</tr>
<tr>
<td><img src="image4" alt="Backup Failed" /></td>
<td>Backup Failed—displays the following tooltip: “Backup failed at hh:mm:ss mm/dd/yyyy.”</td>
</tr>
</tbody>
</table>

Changing the backup interval

Once the backup feature is enabled, your SAN is protected by automatic backups. The backups occur every six hours (360 minutes) by default. However, you can change the interval at which backup occurs.

**Important:** Do NOT modify the backup.properties file.

To change the backup interval, complete the following steps:

1. Select **SAN > Options**.
   The **Options** dialog box displays.
2. In the **Category** list, select **Backup**.
3. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
4. Click **Apply** or **OK** to save your changes.
   - The minimum value is 15 minutes and the maximum value is 24 hours.

**Starting immediate backup**

---

**Note:** You must have Backup privileges to use the Backup Now function.

To start the backup process immediately, complete one of the following procedures:

**Using the backup icon**

1. Right-click the **Backup** icon and select **Backup Now**.
   - The backup process begins immediately. There is no confirmation message.

**Using the SAN menu**

1. Select **SAN > Options**.
   - The **Options** dialog box displays.
2. In the **Category** list, select **Backup**.
3. Click **Backup Now**.
   - The backup process begins immediately. There is no confirmation message. However, the SAN menu will display the time when the last backup completed.

---

**Reviewing backup events**

The Master Log, which displays in the lower left area of the main window, lists the events that occur on the SAN.

If you do not see the Master Log, select **View > All Panels**.

The following backup events appear in the Master Log:
- **Backup started**
- **Backup ended**
- **Backup error**
• Backup enabled
• Backup disabled
• Backup destination change
• Backup interval change
• Backup start time change
• Domain workgroup change
• User name change
• User password change

---

**Restoring data**

*Note:* You cannot restore data from a previous version of the Connectrix Manager application.

The backed up data is contained in the following directories:

• `<Install_Home>\Backup`
• `<Install_Home>\Call Home`
• `<Install_Home>\Client`
• `<Install_Home>\Server`

*Note:* `<Install_Home>` refers to the directory where the Connectrix Manager application is installed.

In a disaster recovery situation, it is possible that configuration changes made less than 45 minutes before Server loss (depending on the backup interval you set) could be missing from the backup.

**Important:** Firmware files are NOT backed up.

The data in those directories is automatically backed up and can be restored from your disk, network folder, or CD. The data includes the following items:

• All log files.
• All plans saved through the **Planning** function.
• All reports generated.
Getting Started

- Application configuration data.
- Backup configuration.
- Call-home configuration (including phone numbers and dialing options). Note that Call-home functions may be optional, depending on your purchased software package.
- License information.
- Performance data.
- User-defined sounds.
- User-launched scripts.
- Zoning library (all zones sets and zone definitions) saved through the Zoning function.

Restoring data from the EMC-supplied rack mount management server

To restore data to the server platform, follow these instructions.

1. Reinstall the application.
2. Open the Connectrix Manager application and go through the steps in the configuration wizard.
3. Log back into the application.
4. Stop the Connectrix Manager application Services by selecting Start > Programs > Connectrix Manager 9.1 > Stop Services. A DOS window displays messages of services being shut down.
5. Go to C:\Program Files\Connectrix Manager 9.1\bin.
7. At the Command Prompt, enter the path to the backup source directory and press Enter. The default is D:\Backup.
8. At the Command Prompt, enter the path to the destination directory and press Enter. The default is C:\Program Files\Connectrix Manager 9.1.
9. When you receive the “Restore completed” message, press any key to close the DOS window.
10. Restart the Connectrix Manager services and application.
11. Log back into the application.
12. Make sure discovery is turned on. If it is not, select Discover > On.

**Restoring data from CD**

1. Reinstall the application.
2. Open the Connectrix Manager application and complete the configuration wizard.
3. Stop the Connectrix Manager Services by selecting Start > Programs > Connectrix Manager 9.1 > Stop Services.
   A DOS window displays messages of services being shut down.
4. Go to C:\Program Files\Connectrix Manager 9.1\bin.
5. Double-click restore.bat.
   A DOS window opens.
6. At the Command Prompt, enter the path to the backup source directory and press Enter.
   The default is D:\Backup.
7. At the Command Prompt, enter the path to the destination directory and press Enter.
   The default is C:\Program Files\Connectrix Manager 9.1.
8. When you receive the “Restore completed” message, press any key to close the DOS window.
9. Restart the Connectrix Manager services and application.
10. Log back into the application.
11. Make sure discovery is turned on. If it is not, select Discover > On.

**Restoring data from the hard drive**

1. Reinstall the application.
2. Open the Connectrix Manager application and complete the configuration wizard.
3. Stop the Connectrix Manager Services by selecting Start > Programs > Connectrix Manager 9.1 > Stop Services.
   A DOS window displays messages of services being shut down.
4. Go to C:\Program Files\Connectrix Manager 9.1\bin.
5. Double-click restore.bat.
   A DOS window opens.
6. At the Command Prompt, enter the path to the backup source directory and press Enter.
   The default is D:\Backup.
7. At the Command Prompt, enter the path to the destination directory and press Enter.
   The default is D:\Backup.
8. When you receive the “Restore completed” message, press any key to close the DOS window.
9. Restart the Connectrix Manager services and application.
10. Log back into the application.
11. Make sure discovery is turned on. If it is not, select Discover > On.

**Restoring data from a network drive**

1. Reinstall the application.
2. Open the Connectrix Manager application and complete the configuration wizard.
3. Stop the Connectrix Manager Services by selecting Start > Programs > Connectrix Manager 9.1 > Stop Services.
   A DOS window displays messages of services being shut down.
4. Go to C:\Program Files\Connectrix Manager 9.1\bin.
5. Double-click restore.bat.
   A DOS window opens.
6. At the Command Prompt, enter the full network path of the backup source directory, such as: \\network-server-name\shared-folder-name\Backup) and press Enter. Do not use the drive letter format (C:\directory).

   The default is D:\Backup.

7. At the Command Prompt, enter the path to the destination directory and press Enter.

   The default is C:\Program Files\Connectrix Manager 9.1.

8. When you receive the “Restore completed” message, press any key to close the DOS window.

9. Restart the Connectrix Manager services and application.

10. Log back into the application.

11. Make sure discovery is turned on. If it is not, select Discover > On.

**Multiple network interface cards**

A second Ethernet NIC card may be desirable in the PC to isolate the switches in your SAN from the public network. If there are any connection issues with the dual NICs, modify the configuration file (<Install_Home>\resources\Server\config.properties) to force the server to look at a specific IP address. To force the server to look at a specific IP address, add the following parameter to the file:

```
ServerRmIpAddress=xxx.xxx.xxx.xxx
```

where xxx.xxx.xxx.xxx is the IP of the NIC card on which they want the client connections to come in.

**Formatting and archiving CD-RW disks**

The Connectrix M-Series 1U server and FRUs ship with blank pre-formatted 700 MB CD-RW disks. During normal operation, a formatted CD-RW disk should remain in the CD-RW drive at all times. For customer service personnel when taking a data collection, use the blank CD-RW disk provided with the FRU. Do not overwrite the CD-RW disk that is used for normal backups for data collection purposes to be returned with FRUs. Place the blank CD-RW disk provided with the FRU into the CD-RW disk and perform the data collection(s) as required. Customer Service personnel refer to CON-CSP-03/A Customer Service Procedure Connectrix Data Collection.
Procedure. After the data collection is complete, put the original CD-RW disk back into the CD-RW drive.

If the customer wants to archive the CD-RW backup disks, they need to provide blank 700 MB CD-RW media, format it, and archive the media per their archiving schedule. Archiving is optional to the customer; however, it is required that a CD-RW disk be in the CD-RW drive at all times for normal automatic backup operations. If you (customer) want to archive the backup CD-RW disks, follow the procedures below to format a CD-RW disk.

Note: EMC personnel can obtain the latest InCD driver and upgrade instructions from the Global Services Internal website (http://www.cs.isus.EMC.com), under Application Download Area, ESN Product Information, InCD CleanTool & Driver.

To format a CD-RW in the 1u service processor shipped from the factory with Connectrix Manager v9.1, use the following procedure:

1. Right-click the CD Drive in **My Computer** and select **InCD Format**.
The **Format** dialog box appears.

2. Type in a label for the CD-RW Disk and click **Start**.

   **Note:** Formatting will take several minutes.

3. Click **OK** when the formatting is complete.
Closing the application

**Note:** Only a controlled application shutdown guarantees the last 10 minutes of data entry. Do not enter any data into the application 10 minutes prior to shutdown.

To close the Connectrix Manager Client, select **Exit** from the **SAN** menu.

To close the Connectrix Manager Client and Server, select **Shutdown** from the **SAN** menu.

Searching the online help

To find all the help topics that contain a particular word or phrase:

1. On the **Help** window, click the tab with the magnifying glass icon.
2. In the **Find** field, enter the word or phrase for which you want to search.
3. Press **Enter**.

If any matches are found, a list of topics will display in the panel. The number of times the word or phrase occurs in the topic will display next to the name. Click the name to display that topic.
Icon legends

Table 5 lists icons and descriptions for Connectrix M products.

Table 5  Product icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DS-16M</td>
<td></td>
<td>DS-32M</td>
<td></td>
</tr>
<tr>
<td>DS-16M2</td>
<td></td>
<td>DS-32M2</td>
<td></td>
</tr>
<tr>
<td>DS-24M2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DS-4400M</td>
<td></td>
<td>DS-4700M</td>
<td></td>
</tr>
<tr>
<td>Generic Switch or Director</td>
<td></td>
<td>ED-10000M</td>
<td></td>
</tr>
<tr>
<td>ED-64M</td>
<td></td>
<td>ED-140M</td>
<td></td>
</tr>
</tbody>
</table>

Product status icons

Table 6 lists product status icons.

Table 6  Product status icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>No icon</td>
<td>Operational</td>
</tr>
<tr>
<td>▲</td>
<td>Degraded</td>
</tr>
<tr>
<td>◆</td>
<td>Failed</td>
</tr>
<tr>
<td>❌</td>
<td>Unknown/Link Down</td>
</tr>
</tbody>
</table>
**Event icons**

Table 7 lists event icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>📘</td>
<td>Informational</td>
</tr>
<tr>
<td>🚧</td>
<td>Warning</td>
</tr>
<tr>
<td>🛑</td>
<td>Fatal</td>
</tr>
</tbody>
</table>

**Keyboard shortcuts**

You can use the keystrokes shown in Table 8 to perform common functions.

**Note:** To open a menu using keystrokes, press ALT + the underlined letter. To open a submenu, release the ALT key first, then press SHIFT + the key for the underlined letter of the submenu option.

<table>
<thead>
<tr>
<th>Menu item or function</th>
<th>Keyboard shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>CTRL + C</td>
</tr>
<tr>
<td>Cut</td>
<td>CTRL + X</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete All</td>
<td>CTRL + Delete</td>
</tr>
<tr>
<td>Help</td>
<td>F1</td>
</tr>
<tr>
<td>Paste</td>
<td>CTRL + V</td>
</tr>
<tr>
<td>Properties</td>
<td>CTRL + P</td>
</tr>
<tr>
<td>Select All</td>
<td>CTRL + A</td>
</tr>
<tr>
<td>Select Connections</td>
<td>CTRL + T</td>
</tr>
<tr>
<td>View Physical Map</td>
<td>F7</td>
</tr>
</tbody>
</table>
This chapter describes the user interface and includes the following information:

- The life cycle of a SAN ................................................................. 76
- Overview ..................................................................................... 77
- ................................................................................................. 77
- Product list .................................................................................. 79
- Master log .................................................................................... 82
- Minimap ....................................................................................... 83
- Toolbar ........................................................................................ 92
- Status bar ..................................................................................... 93
Software Overview

The life cycle of a SAN

The application enables you to proceed through the managed life cycle of the SAN with confidence.

The first stage of a SAN’s life cycle is to Plan the SAN. Use paper and pen or a software application to plan the SAN.

The second stage of the life cycle is to Discover the SAN. The Connectrix Manager application establishes contact with many SAN devices, gathers embedded information, and then depicts it in the Physical Map, or topology. The application discovers the devices attached to the SAN and presents an intuitive visual map of devices and their connections.

The third stage of the life cycle is to Configure the SAN, during which you should configure SAN devices and fabrics.

The final and longest stage of the life cycle is to Monitor the SAN. The application generates events and messages about product and property status. The user interface features an animated display of the data flow and error rates over the entire topology. The application’s self-monitoring, event-logging, and event notification features allow you to stay informed about the state of the SAN.

At any point, a discovered SAN can be used as a starting point to plan a new SAN, completing the life cycle.
Overview

The main window comprises of various areas, discussed in this chapter.

<table>
<thead>
<tr>
<th>Product list</th>
<th>Lists the devices discovered in the SAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology / Physical map</td>
<td>Displays the SAN topology, including discovered and monitored devices and connections.</td>
</tr>
<tr>
<td>Master log</td>
<td>Displays all events that have occurred on the SAN.</td>
</tr>
<tr>
<td>Menu bar</td>
<td>Lists commands you can perform on the SAN.</td>
</tr>
<tr>
<td>Minimap</td>
<td>Displays a “bird’s-eye” view of the entire SAN.</td>
</tr>
<tr>
<td>Status bar</td>
<td>Displays data regarding the Server, connection, device, and fabric.</td>
</tr>
<tr>
<td>Toolbar</td>
<td>Provides buttons that enable quick access to dialog boxes and functions.</td>
</tr>
<tr>
<td>View tab</td>
<td>Displays the Master Log, Utilization Legend, Minimap, Physical Map (topology), and Product List.</td>
</tr>
<tr>
<td>Event Management tab</td>
<td>Displays the tools you need to automate tasks performed on the SAN. You can configure the application to perform any of the following functions automatically:</td>
</tr>
<tr>
<td></td>
<td>• Sending an e-mail message when events or errors occur</td>
</tr>
<tr>
<td></td>
<td>• Exporting data</td>
</tr>
<tr>
<td></td>
<td>• Playing sound to notify you of specific events</td>
</tr>
<tr>
<td>Security tab</td>
<td>Displays the tools you need to manage the authentication settings of all SANtegrity-capable switches and directors in the installation.</td>
</tr>
<tr>
<td>Master log</td>
<td>Displays all events that have occurred on the SAN.</td>
</tr>
<tr>
<td>Utilization legend</td>
<td>Indicates the percentage ranges represented by the colored, dashed lines on the Physical Map.</td>
</tr>
</tbody>
</table>
View tab

The View tab displays the Master Log, Physical Map (topology), and Product List.

To easily open all areas of the View window, select All Panels from the View menu or press F12.

You can change the default size of the display by placing the cursor on the divider until a double arrow displays. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.
The Product list, located on the View tab, displays an inventory of all discovered devices and ports. The Product List is a quick way to look up product and port information, including serial numbers and IP addresses. To display the Product List, select Product List from the View menu, or press F9.

**Note:** Nicknames of attached end-nodes also display in the Product List.

You can edit information in the Product list by double-clicking in a field marked with a green triangle. You can sort the Product List by clicking a column heading.

The following columns are included in the Product List.

- **All Levels.** Displays all discovered fabrics, groups, devices, and ports.
- **Nickname.** Displays the nickname of the product. This field is editable at the fabric, group, and device level.
- **Name (Product).** Displays the name of the product.
- **Device Type.** Displays the type of device.
- **Class.** Displays the class to which the product belongs.
- **Tag #.** Displays the tag number of the product.
- **Node WWN.** Displays the node world wide name of the product.
- **IP Address.** Displays the IP address of the product. This field is editable at the device level.
- **Domain ID.** Displays the Domain ID for the product in the format xx(yy), where xx is the Connectrix M normalized value and yy is the actual value on the wire.
- **Vendor.** Displays the name of the product’s vendor. This field is editable at the device level.
- **Model #.** Displays the model number of the product. This field is editable at the device level.
- **Serial #.** Displays the serial number of the product. This field is editable at the device level.
- **Port Count.** Displays the number of ports on the product.
Software Overview

- **Firmware.** Displays the firmware version of the product. This field is editable at the device level.
- **Location.** Displays the physical location of the product. This field is editable at the fabric and device level.
- **Contact.** Displays the name of the person or group you should contact about the product. This field is editable at the fabric and device level.
- **Description.** Displays the description of the product. This field is editable at the fabric and device level.
- **Comments.** Displays any comments about the product. This field is editable at the fabric and device level.
- **Management Link.** Displays whether the management link for the product is up or down.
- **Operation Status.** Displays the operational status of the product.
- **Alert.** Displays any alerts on the product.
- **Enclosure.** Displays the enclosure of the product. This field is editable at the device level.
- **Port Nickname.** Displays any nickname for the port. This field is editable at the port level.
- **Port Name.** Displays the name of the port.
- **Port #.** Displays the number of the port.
- **Address.** Displays the address of the port.
- **OS Device Name.** Displays the device name of the operating system.
- **Symbolic Name.** Displays the symbolic name of the product.
- **Port WWN.** Displays the world wide name of the port.
- **FC Address.** Displays the Fibre Channel address of the port.
- **Fabric Nickname.** Displays the fabric nickname of the port.
- **Max Frame Size (bytes).** Displays the maximum frame size in bytes of the port.
- **Port State.** Displays the state of the port (online or offline).
- **Port Type.** Displays the type of port (for example, expansion port, node port, or NL port).
- **Active FC4 Types.** Displays the active Fibre Channel 4 types of the port.
- **Supported FC4 Types.** Displays the Fibre Channel 4 types supported by the port.
- **Speed Configured (Gbps).** Displays the actual speed of the port in Gb/s.
- **Speed Supported (Gbps).** Displays the supported speed of the port in Gb/s.
- **Class of Service.** Displays the class of service for the port.
- **VFID.** Displays the Virtual Fabric ID of the port.
- **Transmit % Utilization.** Displays the transmit percentage utilization of the port.
- **Receive % Utilization.** Displays the receive percentage utilization of the port.
- **Blocked Configuration.** Displays the blocked configuration of the port.
- **Operational State.** Displays the operational state of the port.
- **Port Blocked Reason.** Displays the reason why the port is blocked.
- **Block configuration.** Displays the blocked configuration of the port.
- **Driver.** Displays the product's driver
- **Driver Version.** Displays the product's driver version.
- **Fabric.** Displays the fabric nickname of the port.
- **iSCSI Alias.** Displays the name of the alias target.
- **iSCSI Node Name.** Displays the node name of the product.
- **iSCSI Node Type.** Displays the node type of the product.
- **OS.** Displays the operating system running on the product.
The Master log, which displays in the lower left area of the main window, lists the events that occurred on the SAN. If you do not see the Master log, select All Panels from the View menu or press F5.

Two daily files are maintained: one that contains events and one that contains summary information. The format of the daily event log file name is Event_YYYYMMDD.log, where YYYYMMDD is the date that the events took place and the log was created. The daily summary file name format is Event_YYYYMMDD.sum.

By default, event history are kept for 45 days, or until 1000 MB of disk space is taken up. Log files (and summary files) that are older than 45 days are deleted from the system. In addition, when the total disk space used by all the daily log files exceeds the allowable disk quota, the oldest daily log and the associated summary file are deleted from the system. This check is performed hourly to ensure optimal performance. The default locations for the log files are

<Install_Home>\Server\Universe_Home\TestUniverse\_Working\EventStorageProvider\event.log and <Install_Home>\Server\Local_Root\EventStorageProvider\event.log.

Note: <Install_Home> refers to the C:\Program Files\Connectrix Manager 8.9.1 directory where the Connectrix Manager application is installed.

The following fields and columns are included in the Master Log.

- **Level.** The severity of the event.

  **Table 9 Event icons**

<table>
<thead>
<tr>
<th>Event icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Informational" /></td>
<td>Informational</td>
</tr>
<tr>
<td><img src="image" alt="Warning" /></td>
<td>Warning</td>
</tr>
<tr>
<td><img src="image" alt="Fatal" /></td>
<td>Fatal</td>
</tr>
</tbody>
</table>

- **Source.** The product on which the event occurred.
- **Type.** The type of event that was performed (for example, client/server communication events).
Minimap

The Minimap, which displays in the lower right-hand corner of the main window, is useful for getting a bird’s-eye view of the SAN, or to quickly jump to a specific place on the Physical Map. To jump to a specific location on the Physical Map, click that area on the Minimap. A close-up view of the selected location will display on the Physical Map.

Use the Minimap to view the entire SAN and to navigate more detailed map views. This feature is especially useful if you have a large SAN.

Anchoring or floating the Minimap

You can anchor or float the Minimap to customize your main window.

Floating the Minimap

To float the Minimap and view it in a separate window, click the Detach button ( ) in the upper right-hand corner of the Minimap.
Anchoring the Minimap

To return the Minimap to its original location on the main window, do one of the following:

- Click the Attach button (_attach_icon) in the upper right-hand corner of the Minimap.
- Click the Close button (_close_icon) in the upper right-hand corner of the Minimap.
- Click the logo in the upper left-hand corner of the Minimap and select Close (ALT + F4).

Resizing the Minimap

On an anchored Minimap, place the cursor on the left border of the Minimap until a double-pointed arrow displays. Click and drag the adjoining divider.

On a floating Minimap, place the cursor on a border of the Minimap until a double-pointed arrow displays. Click and drag to change the window size.
**Menu bar**

The menu bar is located at the top of the main window.

**SAN Menu.** The SAN menu provides the following commands:

- **Log Out.** Select to log off the Connectrix Manager application.
- **Shutdown.** Select to close the Connectrix Manager Client and Server.
- **Users.** Select to configure users and user groups.
- **Active Sessions.** Select to display all active sessions on the server.
- **Remote Access.** Select to configure remote access.
- **Server Properties.** Select to display the Server properties.
- **Options.** Select to configure the Connectrix Manager application options.
- **Export.** Select to export files.
- **Import.** Select to import files.
- **New Plan.** Select to configure a new planned SAN.
- **Open Plan.** Select to open an existing planned SAN.
- **Save Plan.** Select to save a planned SAN with the same name.
- **Save Plan As.** Select to save a planned SAN with a new name.
- **Exit.** Select to close the Connectrix Manager Client.

**Edit Menu.** The Edit menu provides the following commands:

- **Cut.** Select to cut information and move it to another location.
- **Copy.** Select to copy information and move it to another location.
- **Paste.** Select to paste information in another location.
- **Delete.** Select to delete the selected information.
- **Delete All.** Select to delete all information in a specific dialog box.
- **Clear ISL Alert(s).** Select to remove ISL alerts from the selected object.
- **Show Connections.** Select to show connections in a group.
- **Select Connections.** Select to select a connection.
- **Select Attached Devices.** Select to show all devices attached to the selected object.
- **Select Connected Set.** Select to select two connected objects.
- **Select All.** Select to select all object in the physical map.
- **Properties.** Select to display the selected objects properties.

**View Menu.** The View menu provides the following commands:

- **Discovered SAN.** Select to display the discovered SAN.
Software Overview

- **Planned SAN.** Select to display a planned SAN.
- **Show Panels.** Select to select which panels to display.
  - **All Panels.** Select to show all panels.
  - **Connectivity Map.** Select to only show the connectivity map.
  - **Product List.** Select to only show the product list.
  - **Event Management.** Select to only show the Event Management tab.
  - **Security Center.** Select to only show the Security tab.
  - **Master Log.** Select to only show the master log.
- **Manage View.** Select to set up the Connectrix Manager application view.
  - **Create View.** Select to create a new view.
  - **Display View.** Select to display by View All or by a view you create.
  - **Levels.** Select to display by All Levels, Products and Ports, Product Only, or Ports Only.
  - **Copy View.** Select to copy a view.
  - **Delete View.** Select to delete a view.
  - **Edit View.** Select to edit a view.
  - **Connectivity View.** Select to configure a connectivity view.
- **Zoom.** Select to configure the zoom percentage.
- **Show.** Select to determine what products display.
  - **Fabrics Only.** Select to displays only fabrics.
  - **Groups Only.** Select to displays only groups.
  - **All Products.** Select to displays all products.
  - **All Ports.** Select to displays all ports.
- **Enable Flyover Display.** Select to
- **Show Ports.** Select to show utilized ports on the selected device.
  - Show Ports is not active when
- **Show Connected.** Select to show all connected devices.
- **Map Display Layout.** Select to customize a group’s layout to make it easier to view the SAN and manage its devices.
  - **Default For Group.** Select to display the devices in the default format.
  - **Custom Grid.** Select to drag and drop device or group icons. Devices can only be moved within a group and groups can only be moved within a fabric. After selecting Custom Grid, click device or a group and drag it to the desired location.
- **Square.** Select to display the device icons in a square configuration.
- **Vertical.** Select to display the device icons vertically.
- **Horizontal.** Select to display the device icons horizontally.
- **Most Connected at Center.** Select to display the node that has the most connections at the center of the topology.
- **Directional.** Select to display the internal nodes in a position where they mirror the external groups to which they are connected.

- **Background Color.** Select to customize the topology by changing background color.
  - **Default.** Select to select the default background color.
  - **Custom.** Select to select a background color.

- **Line Types.** Select to determine the way inter-device connections display on the topology.
  - **Straight.** Select to display connections using straight lines.
  - **Orthogonal.** Select to display connections in orthogonal grid lines.
  - **None.** Select to hide the connections between devices.

- **Domain ID/Port #.** Select to set the display domain IDs and port numbers in decimal or hex format.
  - **Decimal.** Select to display all domain IDs and port numbers in decimal format.
  - **Hex.** Select to display all domain IDs in hex format. Port numbers only display in hex format in the Element Managers.

- **Product Label.** Select to configure which product labels display.
  - **Name.** Select to display the product name as the product label.
  - **Nickname.** Select to display the nickname as the product label.
  - **Node WWN.** Select to display the node name as the product label.
  - **IP Address.** Select to display the IP Address as the product label.
  - **Domain ID.** Select to display the domain ID as the product label.

- **Port Label.** Select to configure which port labels display.
  - **Nickname.** Select to display the nickname as the port label.
  - **Name.** Select to display the name as the port label.
Software Overview

- **Port Number.** Select to display the port number as the port label.
- **Port Address.** Select to display the port address as the port label.
- **Port Name.** Select to display the port name as the port label.

- **Port Display.** Select to configure how ports display.
  - **Occupied Product Ports.** Select to display the ports of the devices in the fabrics (present in the physical map) that are connected to other devices.
  - **UnOccupied Product Ports.** Select to display the ports of the devices (shown in the physical map) that are not connected to any other device.
  - **Attached Ports.** Select to display the attached ports of the target devices.

**Plan Menu.** The Plan menu is only active when you are in the Planned SAN view. To display a planned SAN, select Planned SAN from the View menu. The Plan menu provides the following commands:

  - **Set Rules.** Select to specify planning rules.
  - **Evaluate.** Select to evaluate the plan.
  - **Insert Device.** Select to insert a device such as an HBA, bridge, or server.
  - **Insert Devices.** Select to add multiple devices to your plan.
  - **Planned Device.** Select to change the selected icon to identify either a planned or an installed device.

**Discover Menu.** The Discover menu provides the following commands:

  - **On.** Select to turn on Discovery.
  - **Off.** Select to turn off Discovery.
  - **Setup.** Select to set up Discovery.
  - **Servers.** Select to create servers and assign HBAs.
  - **Storage Port Mapping.** Select to manually map Storage Ports to a Storage Device or other Storage Ports.
  - **Map to Hub.** Select to place each hub in the appropriate location of the topology.

**Configure Menu.** The Configure menu provides the following commands:

  - **Group Manager.** Select to manage a group of switches and directors
• **Virtual Switches.** Select to configure virtual switches in the SAN. Virtual switches are created from multiple directors.

• **Nicknames.** Select to provide familiar simple names to products and ports in your SAN.

• **SAN Routing.** Select to interconnect storage area network (SAN) islands (separately designated logical portions of a SAN) within a larger network.

• **Router Port Configuration.** Select to view the R_Ports on a SAN router.
  • **SAN Router Configuration.** Select to configure the Cluster ID, SNTP, Date and Time, SNMP Traps, or iFCP ID for an individual SAN Router or a group of SAN Routers.
  • **Configuration Archive.** Select to archive files and reports, which help customer service troubleshoot problems, as well as configure TFTP root path properties.

• **Router Consistency.** Select to display the router’s properties.

• **Log Viewer.** Select to generate a log file.

• **Save To Flash.** Select to save changes to the Router Port Configuration or SAN Router Configuration to flash memory.

• **Zoning.** Select to configure zones in SANs.

• **List Zone Members.** Select to display all members in a zone.

• **LUN Management.** Select to configure logical unit numbers (LUNs) for your SANs.

• **Port Fencing.** Select to configure port fencing to protect your SAN from repeated operational or security problems experienced by ports.

• **Enterprise Fabric Mode.** Select to activate Enterprise Fabric Mode, which enables Fabric Binding, Switch Binding, Domain RSCNs, and Insistent Domain ID.

• **Fabric Binding.** Select to configure whether switches can merge with a selected fabric, which provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

**Monitor Menu.** The Monitor menu provides the following commands:

• **Performance.** Select to monitor SAN devices.
  • **Setup.** Select to start performance monitoring.
  • **Latency Graphs.** Select to monitor the time it takes for data to go from an HBA to a device’s LUN and back to the HBA.
• **Switch Graphs.** Select to monitor a switch’s performance through a performance graph, which displays transmit and receive data. The graphs show persisted data.

• **View Utilization.** Select to display the connection utilization.

• **Event Notification.** Select to configure the Connectrix Manager application to send event notifications at specified time intervals.
  - **Email.** Select to configure the Connectrix Manager application to send event notifications through e-mail.
  - **Call Home.** Select to configure the Connectrix Manager Server to automatically dial-in to a support center to report system problems.

• **SNMP Agent.** Select to configure the Connectrix Manager application to act as a translator of information stored on the Server into a form usable by SNMP management stations.
  - **On.** Select to turn on SNMP Agent.
  - **Off.** Select to turn off SNMP Agent.
  - **Setup.** Select to configure community strings and trap recipients.

• **Ethernet Event.** Select to configure the application to send notification of Ethernet events.

• **Trap Forwarding.** Select to configure the Connectrix Manager application to send SNMP traps to other computers.

• **Frame Sniffer.** Select to configure the Connectrix Manager application to count frames passed by a switch port that meet user-specified criteria.

• **Reports.** Select to generate reports about the SAN.
  - **Generate.** Select to determine which reports to run.
  - **View.** Select to view reports through the application or through an internet browser.
  - **Consistency.** Select to view the Consistency Report.
  - **iFCP Connections and Zones.** Select to view the iFCP Connections and Zone Report.

• **LUN Mapping.** Select to view the LUN Mapping Report.

• **Name Server.** Select to view the Name Server Report.

• **R Port.** Select to view the R Port Report.

• **Router Configuration.** Select to view the Router Configuration Report.

• **Zone Library.** Select to view the Zone Library Report.

• **Logs.** Select to display logs.
Software Overview

- **Audit.** Select to display a history of user actions performed through the application (except login/logout).
- **Event.** Select to display errors related to SNMP traps and Client-Server communications.
- **Fabric.** Select to display the events related to the selected fabric.
- **Group.** Select to display the event logs defined on the Group Management screen.
- **Product Status.** Select to display operational status changes of managed products.
- **Session.** Select to display the users who have logged in and out of the Server.
- **Security.** Select to display security information.
- **Persist Fabric.** Select to takes a “snapshot” of the current products and connections in the fabric as a reference point for comparison to future fabric changes.
- **Unpersist Fabric.** Select to unpersist a fabric.
- **Unpersist Product.** Select to unpersist a single product in a persisted fabric if the product is no longer part of the fabric.
- **Show Route.** Select to view the path that Fibre Channel frames must take between two end-products in a multi-switch fabric.

**NOTE:** Show Route is only available when your Fabric contains two or more Switches.

- **Hide Route.** Select to hide routes that Fibre Channel frames must take between two end-products in a multi-switch fabric.

**Tools Menu.** The **Tools** menu provides the following commands:

- **Setup.** Select to set up the applications that display on the **Tools** menu.
- **Product Menu.** Select to access the tools available on a device’s shortcut menu.
- **Tools (determined by user settings).** Select to open a software application. You can configure **Tools** menu to display different software application. Recommended tools to include in this menu include an internet browser, the command prompt application, and Notepad.

**Help Menu.** The **Help** menu provides the following commands:

- **Contents.** Select to open the Online Help.
- **Find.** Select to search the Online Help.
Software Overview

- **License.** Select to view or change your License information.
- **About.** Select to view the Connectrix Manager application information, such as release number.

**Toolbar**

The toolbar is located at the top of the main window and provides icons to perform various functions.

**Toolbox**

The toolbox is located at the top right-hand side of the View window and provides tools to zoom in and out of the Physical Map, collapse and expand groups, and fit the topology to the window.

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoom In</td>
<td>Use to zoom out of the Physical Map.</td>
</tr>
<tr>
<td>Zoom Out</td>
<td>Use to zoom out of the Physical Map.</td>
</tr>
<tr>
<td>Fit in View</td>
<td>Use to scale the map to fit within the Physical Map area.</td>
</tr>
<tr>
<td>Expand</td>
<td>Use to expand the map to show all ports in use on a device.</td>
</tr>
<tr>
<td>Collapse</td>
<td>Use to collapse the map to show only devices (hides ports).</td>
</tr>
</tbody>
</table>
The status bar displays at the bottom of the main window. The status bar provides a variety of information about the SAN and the application. The icons on the status bar change to reflect different information such as current status of products, fabrics, and backup.

**Figure 12 Status bar**

*Note:* The icons on your status bar will vary based on the licensed features on your system.

<table>
<thead>
<tr>
<th>1. <strong>Connection status</strong></th>
<th>Displays the Server-Client connection status.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. <strong>Product status</strong></td>
<td>Displays the status of the most degraded device in the SAN. For example, if all devices are operational except one (which is degraded), the Product Status will display as degraded. Click this button to open the Product State Log. Refer to “Determining a product’s operational status” on page 206 for more information.</td>
</tr>
<tr>
<td>3. <strong>Fabric status</strong></td>
<td>Displays the state of the fabric that is least operational, based on ISL status. The possible states are: operational, unknown, degraded, or failed. Select a product or fabric from the Physical Map or Product List and click this button to open the related Fabric Log (only available for persisted fabrics). Refer to “Viewing the fabric log” on page 248 for more information.</td>
</tr>
<tr>
<td>4. <strong>Attention indicator</strong></td>
<td>This icon displays when at least one EMC product in the SAN requires attention. Click the icon to open the Service Request dialog box, which lists all managed EMC switches and directors that need attention.</td>
</tr>
</tbody>
</table>
5. Call Home status
Displays if the Call Home service is enabled. If Call-Home has been enabled on all managed EMC switches and on the management application, the icon appears as enabled. If Call-Home is disabled on any one of the EMC switches or on the management application, the icon appears as disabled. Click the icon to open the Call Home Settings Summary dialog box, to determine whether the Call Home feature is enabled on the management application and on each managed EMC switch or director.

Note: Call Home support for managed switches and/or directors refers to M-Series switches/directors purchased from EMC with valid EMC service contracts.

6. Backup status
Displays a backup status icon, which allows you to determine the current backup status. Let the pointer pause on the backup status icon to display the following information in a tooltip:
- Backup in Progress icon. Backup started at hh:mm:ss, in progress... XX files in <directory_name> are backed up.
- Countdown to Next Scheduled Backup icon. Waiting for next backup to start.
- Backup Disabled icon. Backup is disabled.
- Backup Failed icon. Backup failed at hh:mm:ss mm/dd/yyyy.

7. Server name
Displays the name of the Server to which you are connected.

8. Total users
Displays the number of clients logged into the server.

9. User’s ID
Displays the user ID of the logged in user.
This chapter provides instructions for setting up and customizing the application.

- Configuring the Connectrix Manager server ........................................ 96
- Managing users .................................................................................. 113
- Customizing the main window ......................................................... 128
- Exporting and importing ................................................................. 130
Setting Up the Connectrix Manager

Configuring the Connectrix Manager server

The application is comprised of two parts: the Server and the Client. The Server is installed on one machine and stores SAN-related information; it does not have a user interface. To view SAN information through a user interface, you must log in to the Server through a Client.

Note: The Server and Client(s) may reside on the same machine, or on separate machines.

In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between Servers and Clients. In other words, a Client can find a Server, appear to log in, but will immediately be logged out because the Server cannot reach the Client. To resolve this issue, the application will automatically detect the network configuration and run the Client in “polling mode” when necessary.

When the Client is not running in polling mode, the Server calls the Client whenever it has new data. When the Client is running in polling mode, the Server will queue up the data and the Client will periodically check in (approximately every 5 or 10 seconds) and get the data.

Logging in to a server

You must log in to a Server to monitor a SAN.

Note: You must have an established login and password account on the Server in order to log in.

1. The Connectrix Manager Log In dialog box displays automatically when you open the application.
Figure 13  Log In dialog box

2. The Server’s address displays in the Network Address field. You may specify a new address by typing it in the field, or selecting one from the drop-down list.

   Note: Localhost is the default value. The application automatically determines the local IP address and uses that value as the local host address.

   The Server’s name displays in the Server Name field.

3. Enter your user ID and password.

4. Click Forget password or Save password to select whether you want the application to remember your password the next time you log in.

5. Click Login.

Changing your password

1. Select Start > Programs > Connectrix Manager 9.1 > Connectrix Manager 9.1 to open the application.

   The Connectrix Manager 9.1 Log In dialog box displays.

2. Enter your user name in the User ID field.

3. Enter your password in the Password field.

4. Click Change.

   The Change Password dialog box displays.
5. Enter your new password in the Secure Password and Retype Password fields and click OK.

6. Click Login.

### Logging out of a server

To log into a different Server, you must first log out of the current Server.

1. Select Log Out from the SAN menu.

   You will be logged out of the current Server and the Connectrix Manager Log In dialog box will display (Figure 13 on page 97).

Refer to “Logging in to a server” on page 96 for instructions on logging in to a new Server.

### Adding a server

1. Select Log Out from the SAN menu.

   The Connectrix Manager Log In dialog box displays (Figure 13 on page 97).

2. To add a new Server, enter the Server’s network address in the Network Address field.

   **Note:** You must have an established login and password account on the new Server.

3. The Server’s name displays in the Server Name field.

4. Enter your user ID and password.

5. Click Forget password or Save password to select whether you want the application to remember your password the next time you log in.

6. Click Login.

   The application will log into the Server located at the specified network address.
Configuring HBAs and servers

Associating an HBA to a server

Note: Discovered information overwrites your user settings.

1. On the Physical Map, right-click an HBA icon and select Server HBA Mapping from the menu.

2. The Create servers and assign HBAs dialog box displays. In the Servers table, select the server to which you want to assign HBAs.

   Note: To add or remove servers, click Create or Delete. To rename a server click the server name once, wait, then click it again. Type the new name over the old name.

3. Select the HBA from the table on the left and click the right arrow.

   The HBA displays in the Servers table. The HBA is now associated with the selected server.

4. Click OK to save your changes and close the Create servers and assign HBAs dialog box.

   On the Physical Map, the HBA displays in the server.

Unassociating an HBA from a server

1. On the Physical Map, right-click an HBA icon and select Server HBA Mapping from the menu.

   The Create servers and assign HBAs dialog box displays.

2. Select the HBA from the Servers table on the right and click the left arrow.

   The HBA you selected is removed from the Servers table and the HBA is longer associated with the server.

3. Click OK to save your changes and close the Create servers and assign HBAs dialog box.

   On the Physical Map, the HBA displays on its own.

Toggling between viewing HBAs and servers

Note: An HBA must be associated with a server before you can toggle views.
On the Physical Map, right-click a server icon and select HBA from the menu.

If the option is selected, the associated HBA displays. If the option is not selected, the server displays.

### Renaming a server

You can rename Servers that display on the Physical Map.

1. On the Physical Map, right-click an HBA icon and select Server HBA Mapping from the menu.
   
   The Create servers and assign HBAs dialog box displays.

2. Click once on the Server name in the Servers table on the right.

3. Edit the Server name.

4. Press Enter.

   The Server’s new name displays on the Physical Map.

### Deleting a server

You can delete Servers that display on the Physical Map.

1. On the Physical Map, right-click an HBA icon and select Server HBA Mapping from the menu.

   The Create servers and assign HBAs dialog box displays.

2. From the Servers table on the right, select the Server you want to delete.

3. Click Delete.

   The Server is deleted.

4. Click OK to save your changes and close the Create servers and assign HBAs dialog box.

### Removing a server

You can remove Servers from the list in the Connectrix Manager 9.1 Log In dialog box.

1. From the Network Address list, select the Server you want to remove.
2. Click **Delete**.
   A confirmation message displays to confirm you want to delete the selected server.

3. Click **OK**.

---

### Configuring options

Connectrix Manager **Connectrix Manager** enables you to configure the following options:

- Backup
- End Node Display
- Domain ID
- Flyovers
- Nicknames
- Reset Display
- Software Configuration

---

### Configuring backup settings

**Note:** You must have Backup Read/Write privileges to configure Backup settings.

To configure backup settings, complete the following steps.

1. Select **SAN > Options**.
   The **Options** dialog box displays.

2. In the **Category** list, select **Backup**.

3. Select the **Enable backups** check box.

4. In the **Next Backup Start Time Hours** and **Minutes** fields, enter the time (using a 24-hour clock) you want to backup process to begin.

5. Select an interval from the **Backup Interval** list to set how often backup occurs.

6. In the **Output Directory** field, enter the path for the backup directory.
Setting Up the Connectrix Manager

**Note:** If you set your backup directory to a network drive, you must specify the directory in a share format (for example, \\server\share\). You must also supply user credentials for a user that is authorized to write to the network device.

You can change the directory or use the **Browse** button to select another directory.

7. Set the Network Drive Credentials, if necessary.
   a. In the **Domain or Workgroup** field, enter the domain or workgroup name.
   b. In the **User Name** field, enter the user name.
   c. In the **Password** field, enter the password.

8. Click **Apply** or **OK** to save your work.
   The application verifies that the backup device exists and that the server can write to it.

   If the device does not exist or is not writable, an error message displays that says you have entered an invalid device. Click **OK** to go back to the **Options** dialog box and fix the error.

   Backup occurs, if needed, at the interval you specified.

---

**Configuring domain ID and port number display**

To display the domain ID and port numbers in either decimal or hex format, complete the following steps.

1. Select **View>Domain ID/Port #**.

2. Select one of the following display formats:
   - Select **Decimal** to display the domain ID and port numbers in decimal format.
     Decimal is the default format. The domain IDs and port numbers display in the decimal format in both Connectrix Manager and the Element Managers.
   - Select **Hex** to display the domain ID and port numbers in hex format.

3. **(Hex only)** Click **OK** on the Connectrix Manager message.
The domain ID displays in the hex format in both Connectrix Manager and the Element Managers. However, the port number only displays in the hex format in the Element Managers. The port number always displays in the decimal format in Connectrix Manager.

---

**Configuring end node display**

To display end nodes when discovering a new fabric, complete the following steps.

1. Select **SAN > Options**.
   
   The Options dialog box displays.

2. In the **Category** list, select **End Node Display**.

3. Select the **Show connected end nodes when new fabric is discovered** check box to display end nodes on your system.

   **Note:** Before changes can take effect, the topology must be rediscovered.

4. Click **Apply** or **OK** to save your work.

---

**Configuring flyover settings**

You can configure your system to display product information for products and connections in a pop-up window on the Physical Map.

To display product information in a pop-up window, complete the following steps.

1. Select **SAN > Options**.
   
   The Options dialog box displays.

2. In the **Category** list, select **Flyovers**.

3. Select the **Enable flyover display** check box to enable flyover display on your system.

4. Select the **Include labels** check box to include labels on flyover displays.

5. To set the products to display on flyover, select the **Product** tab and complete the following steps.
Setting Up the Connectrix Manager

a. In the Available Properties table, select each product you want to display.

b. Click the right arrow to move the selected products to the Selected Properties table.

c. Use the Move Up and Move Down buttons to reorder the products in the Selected Properties table, if necessary.

Items in the Selected Properties table appear in the flyover display.

6. To set the connections to display on flyover, click the Connection tab and complete the following steps.

a. In the Available Properties table, select all the products you want to display.

b. Click the right arrow to move the selected products to the Selected Properties table.

c. Use the Move Up and Move Down buttons to reorder the products in the Selected Properties table.

Items in the Selected Properties table appear in the flyover display.

7. Click Apply or OK to save your work.

---

Configuring nickname settings

The Connectrix Manager application allows you to configure nicknames to be either unique or non-unique.

To configure nicknames, complete the following steps.

1. Select SAN > Options.

   The Options dialog box displays.

2. In the Category list, select Nicknames.

3. Select one of the following options.

   a. Select Set nicknames to be unique to require that nicknames be unique on your system.

   b. Select Set nicknames to be non-unique to allow duplicate nicknames on your system.

4. Click Apply or OK to save your work.
### Editing duplicate nicknames

The SAN Management application allows you to edit duplicate nicknames so that each device has a unique nickname.

**Note:** This dialog box only displays when you set nicknames to be unique and there are duplicate nicknames in the system.

To edit duplicate nicknames, complete the following steps:

1. Select **SAN>Options**.
   - The **Options** dialog box displays.
2. In the **Category** list, select **Nicknames**.
3. Select **Set nicknames to be unique** to require that nicknames be unique on your system.
4. Click **OK** in the **Options** dialog box.
   - The **Duplicate Nicknames** dialog box displays.
5. Select one of the following options:
   - If you select **Append Incremental numbers for all repetitive nicknames**, the nicknames are edited automatically using incremental numbering.
   - If you select **I will fix them myself**, edit the nickname in the **Nickname** field.
6. Select **OK**.
Configuring reset display settings

You can reset your system to display the following Connectrix Manager classic display settings.

<table>
<thead>
<tr>
<th>Settings</th>
<th>Default State</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch and device show port mode</td>
<td>Set to not show ports.</td>
</tr>
<tr>
<td>Show connected end device node</td>
<td>Set to not show end devices.</td>
</tr>
<tr>
<td>Show connected end device node for newly discovered fabrics</td>
<td>Set to not show end device.</td>
</tr>
<tr>
<td>Fabric Map Layout</td>
<td>Set to default for Fabric.</td>
</tr>
<tr>
<td>Device Group Layout</td>
<td>Set to Free Form.</td>
</tr>
<tr>
<td>Fabric Line Types</td>
<td>Set to Straight.</td>
</tr>
<tr>
<td>Device Group Line types</td>
<td>Set to Straight.</td>
</tr>
<tr>
<td>Routed Products Virtual Group</td>
<td>Set to Collapse.</td>
</tr>
<tr>
<td>Port Display</td>
<td>Set to Attached Ports only.</td>
</tr>
<tr>
<td>Product Flyover</td>
<td>Set to include the only following properties: Nickname, Name, WWN, IP Address, and Domain ID.</td>
</tr>
<tr>
<td>Connection Flyover</td>
<td>Set to include the following properties: Nickname, IP Address, WWN, Port Number Hex, Port Address, and Port WWN.</td>
</tr>
<tr>
<td>Master Log Events</td>
<td>Set to not select “Extended Events”.</td>
</tr>
<tr>
<td>Table columns in the Product List</td>
<td>Set to only display columns displayed in Connectrix Manager 8.9.1.</td>
</tr>
<tr>
<td>Number of panels displayed on the main panel</td>
<td>Set to display all panels including Product List, Topology Map, Master Log, Legend, and Mini Map; as well as display product information for products and connections in a pop-up window on the Physical Map.</td>
</tr>
</tbody>
</table>

To reset Connectrix Manager to the default Connectrix Manager display and view settings, complete the following steps.

1. Select **SAN > Options**.
The Options dialog box displays.

2. In the Category list, select Reset Display.
3. Click Reset Display.
4. Click Yes on the reset confirmation message.
   The display and view settings are immediately reset to the default Connectrix Manager classic display settings (as detailed in the Table 10 on page 106).
5. Click Apply to save your work and leave the dialog box open.
6. Click OK to save your work and close the dialog box.

**Configuring software settings**

The Connectrix Manager application allows you to configure the following software settings:
- Client Export Port—Configure a port for communication between the client and server.
- Element Management—Configure the element management method.
- IP Configuration—Configure the Ethernet ports.
- Memory Allocation—Configure memory allocation for the client and server.
- Server Connection—Configure client-server connectivity settings.
- SNMP Discovery—Configure the SNMP time-out and retry settings.
  - SNMP Trap Listening—Allows you to configure the SNMP Trap port.
  - Support Mode—Allows you to configure support settings to allow enhanced diagnostics.

**Configuring element management settings**

To configure element management settings, complete the following steps.

1. Select SAN > Options.
   The Options dialog box displays.
2. In the Category list, select Software Configuration.
3. Select **Element Management**.

4. Select the **SNMP and discovery** option to allow discovery and monitoring by this server and not allow element management capability from other servers.

5. Select the **SNMP Discovery Only** option to allow discovery and monitoring without overriding the element management capability from another server.

6. Click **Apply** or **OK** to save your work.

   **Note:** Changes to this option take effect after an application restart.

---

**Configuring client export port settings**

To configure client export port settings, complete the following steps.

1. Select **SAN > Options**.
   
   The **Options** dialog box displays.

2. In the **Category** list, select **Client Export Port** to assign a communications port between the client and server.

3. In the **Client Export Port #** field, enter the client export port number to set a fixed port number for the client.

4. Click **Apply** or **OK** to save your work.

   **Note:** Changes to this option take effect after an application restart.

---

**Configuring IP configuration settings**

To configure the IP address and subnet mask to override the default Ethernet ports used by the server for client-server communications, complete the following steps.

1. Select **SAN > Options**.
   
   The **Options** dialog box displays.

2. In the **Category** list, select **IP Configuration** to set the IP address and subnet mask.

3. If you select the default from the **Server IP Configuration** list, the application sets the default as the Ethernet port for the server.

4. If you select **Automatic** from the **Server IP Configuration** list, the application automatically sets the Ethernet port for the server.
5. If you select **Manual** from the **Server IP Configuration** list, you must manually set the Ethernet port for the server.
   a. In the **Subnet Mask** field, enter the subnet mask address for the server.
   b. In the **Return Address** field, enter the return address for the server.
6. Click **Apply** or **OK** to save your work.

   **Note:** Changes to this option take effect after an application restart.

**Configuring the application to use dual network cards**

Issues with Client-to-Server connectivity can be due to different causes. Some examples are:

- The computer running the Server has more than one network interface card (NIC) installed.
- The computer running the Server is behind a firewall that performs network address translation.

To make sure that Clients can connect to the Server, you may need to edit the IP configuration setting in the Options dialog to manually specify the IP address that the Server should use to communicate to its Clients.

To configure the IP address and subnet mask to override the default RMI server host IP address, complete the following steps.

   **Note:** This configuration option replaces the -Djava.rmi.server.hostname value used in previous releases.

1. Select **SAN > Options**.
   The **Options** dialog box displays.
2. In the **Category** list, select **IP Configuration** to set the IP address and subnet mask.
3. Select **Manual** from the **Server IP Configuration** list.
4. In the **Subnet Mask** field, enter the subnet mask address for the server.
5. In the **Return Address** field, enter the return address (RMI server host name) for the server.
Setting Up the Connectrix Manager

6. Click **Apply** or **OK** to save your work.
   
   **Note:** Changes to this option take effect after an application restart.

**Configuring memory allocation settings**

To configure memory allocation settings, complete the following steps.

1. Select **SAN > Options**.
   
   The **Options** dialog box displays.
2. In the **Category** list, select **Memory Allocation** to set the memory allocation for the server and client.
3. In the **Client Memory Allocation** field, enter the memory allocation (MB) for the client.
4. In the **Server Memory Allocation** field, enter the memory allocation (MB) for the server.
5. Click **Apply** or **OK** to save your work.
   
   **Note:** Changes to this option take effect after an application restart.

**Configuring server connection settings**

Allows you to configure client-server connectivity settings so that you can assign a server connection port for the initial contact from the client, assign a server export port from communications between server and client, and set the server export port to be SSL enabled.

To configure server connection settings, complete the following steps.

1. Select **SAN > Options**.
   
   The **Options** dialog box displays.
2. In the **Category** list, select **Server Connection** to configure client-server connectivity settings.
3. In the **Server Connection Port #** field, enter a port number for the initial contact from the client.
4. In the **Server Export (SSL) Port #** field, enter a port number for communications between the client and the server.
5. Click **Enable SSL** to SSL enable the server export port.
6. Click **Apply** or **OK** to save your work.
Configuring SNMP discovery settings
To configure SNMP discovery settings, complete the following steps.

1. Select SAN > Options.
   The Options dialog box displays.
2. In the Category list, select SNMP Discovery to set the number of retries and timeout for SNMP discovery between the client and server.
3. In the SNMP Timeout field, enter a timeout value (default=5) for discovery between the application and the managed products (switches and directors).
4. In the SNMP Retry field, select the number of retries for discovery between the application and the managed products (switches and directors).
5. Select the Apply settings to all currently defined IP addresses check box.
6. Click Apply or OK to save your work.

Configuring SNMP trap listening settings
To configure SNMP trap listening settings, complete the following steps.

1. Select SAN > Options.
   The Options dialog box displays.
2. In the Category list, select SNMP Trap Listening.
3. In the SNMP Listening Port # field, enter a SNMP listening port number to assign a port to retrieve SNMP traps.
4. Click Apply or OK to save your work.

   Note: Changes to this option take effect after an application restart.

Configuring support mode settings
To configure support mode settings, complete the following steps.

1. Select SAN > Options.
The Options dialog box displays.

2. In the Category list, select Support Modes to enable or disable support modes.

   Note: Only use this option when directed to by customer support.

3. Select the Client Support Mode check box to enable the support mode for the client.

4. Select the Server Support Mode check box to enable the support mode for the server.

5. Click Apply or OK to save your work.
Managing users

When you set up users and user groups, you can add, change, or remove users. By adding a user, you assign privileges to certain features and/or views in the application, enhancing the security of your SAN.

Viewing the list of users

From the SAN menu, select Users.

Adding a user account

**Note:** You must have the User Management privilege to perform this task.

1. From the SAN menu, select Users.
   
   The Server Users dialog box displays.

2. Click the Add button located below the Users table.
   
   The Add User dialog box displays.

3. In the Name field, type the name of the user.

4. In the Email Address field, type the users’ email addresses, separating multiple addresses with a semicolon (:) or comma (,).

5. Select the Enable option to enable email notification for the user.
   
   A message may display stating that you must enable event notification for the SAN. Click Yes.

6. Click the Filter link to specify the event types for which to send email notification to this user.
Refer to “Filtering event notifications for a user” on page 115 for detailed instructions.

7. In the User ID field, type a unique user name for the user.
8. In the Secure Password field, type the user’s password.
9. In the Retype Password field, confirm the password by retyping it.
10. Click OK to close the Add User dialog box.

   The new user will display on the Server Users dialog box.
11. Click OK to close the Server Users dialog box.

---

**Changing a user account**

*Note:* You must have the User Management privilege to perform this task.

1. From the SAN menu, select Users.

   The Server Users dialog box displays.
2. In the Users table, select the user whose information you want to edit.
3. Click the Edit button located below the Users table.

   The Edit User dialog box displays.

4. Edit the information as necessary.
5. Click OK to close the Edit User dialog box.

   The edited information will display on the Server Users dialog box.
6. Click OK to close the Server Users dialog box.
Removing a user account

**Note:** You must have the User Management privilege to perform this task.

**Note:** You will not be prompted for confirmation before the user’s account is removed. If the user is logged in when you remove his account, he will not be affected until he logs out and tries to log in again.

1. From the **SAN** menu, select **Users**.
   
The **Server Users** dialog box displays.
2. Select the user account you want to remove.
3. Click **Remove**.
4. Click **OK**.

Filtering event notifications for a user

The application provides notification of many different types of SAN events. If a user only wants to receive notification of certain events, you can filter the events specifically for that user.

**Note:** The email filter in Connectrix Manager is overridden by the firmware email filter. When the firmware determines that certain events do not receive email notification, an email is not be sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box.

1. From the **SAN** menu, select **Users**.
   
The **Server Users** dialog box displays.
2. In the **Email** column, click the **Filter** link associated with the user for whom you want to filter events.
The Define Filter dialog box displays (Figure 14). The Selected Events table includes the events of which this user will be notified. The Available Events table includes all other events.

![Figure 14 Define Filter dialog box](image1)

### Figure 14 Define Filter dialog box

3. Move events between the tables by selecting the event and clicking the appropriate arrow button.

4. Click **OK**.

5. On the Server Users dialog box, turn on event notification for the user by selecting the check box next to Filter.

6. Click **OK** to close the Server Users dialog box.
Managing user groups

Creating a user group

Note: You must be a System Administrator or Security Administrator to perform this task.

You can create a user group and specify access to certain features and/or views in the application, enhancing the security of your SAN.

1. Select SAN > Users.

   The Connectrix Manager Server Users dialog box displays.

2. Connectrix Manager Connectrix Manager Click the Add button.

   The Features tab of the Group dialog box displays, and lists the available features (Figure 16 on page 118).
3. Enter a name and description for the group in the fields provided.

4. To assign Read/Write or Read Only permissions to selected features, click the Features tab. Otherwise, skip to step 5.

   **Note:** You must assign a feature to the Read/Write or Read Only list for the new group to have access to a selected feature.

   a. In the left-hand list, select features to which you want to allow “read and write” access. Press CTRL and click to select multiple features.
Setting Up the Connectrix Manager

Note: Depending on your licensed modules, the list of features may differ.

b. Click the right arrow next to the Read/Write list.
   The features is moved to the Read/Write list.

c. In the left-hand list, select features to which you want to allow “read only” access. Press CTRL and click to select multiple features.

d. Click the right arrow next to the Read Only list.
   The features are moved to the Read Only list.

5. To assign Read/Write or Read Only permissions to selected views, click the Views tab. Otherwise, skip to step 6.

   a. In the left-hand list, select views to which you want the user group to have access. Press CTRL and click to make multiple selections.

   b. Click the right arrow next. The views are moved to the Selected Views List.

6. Click OK to save the new group and close the Group dialog box.

   The new group displays in the Groups list of the Connectrix Manager Server Users dialog box. To add users to this group, follow the instructions in “Assigning users to groups” on page 122.
7. To configure email event notification for the group, click **Email Event Notification Setup**.

   **For instructions on setting up event notifications**, refer to the Event Monitoring section of the *Connectrix Manager Software User Manual*.

8. Click **OK** to save your changes and close the *Connectrix Manager Server Users* dialog box.

---

**Editing a user group**

---

**Note:** You must have the User Management privilege to perform this task.

You can change a user group’s permissions to use certain features and views. This provides added security for your SAN as well as your management application.

1. Select **SAN > Users**.

   The *Connectrix Manager Server Users* dialog box displays.

2. Select a user group in the **Groups** list.

3. Click **Edit** located below the **Groups** list.

   The **Group** dialog box displays.

4. To change permissions to use certain features, click the **Features** tab. Otherwise, skip to step 5.

   a. In the Read/Write list, select the features to which you want to remove “read and write” access.

      Press CTRL and click to select multiple features.

   b. Click the left arrow next to the **Read/Write** list.

      The features are moved to the left-hand list.

   c. In the **Read Only** list, select the features to which you want to remove “read only” access.

      Press CTRL and click to select multiple features.

   d. Click the left arrow next to the **Read Only** list.

      The features are moved to the left-hand list.
5. To change permissions to use certain views, click the Views tab. Otherwise, skip to step 6.
   a. In the Selected Views list, select the views to which you want to remove access.
      Press CTRL and click to make multiple selections.
   b. Click the left arrow to move the selection(s) to the left-hand list.
6. Click OK on the Group dialog box to save your edits and close the dialog box.
7. Click OK to save your changes and close the Connectrix Manager Server Users dialog box.

Removing a user group

Note: You must have the User Management privilege to perform this task.

Important: After completing these steps, the user group is removed without confirmation.

You can remove a user group regardless of whether a user is assigned to the group.
1. Select SAN > Users.
   The Connectrix Manager Server Users dialog box displays.
2. In the Groups list, select the group you want to remove.
3. Click Remove.
4. Click OK to save your changes and close the dialog box.
Assigning users to groups

Note: You must have the User Management privilege to perform this task.

You can assign users to groups to assign them permissions for features and topology views. If you assign one user to multiple groups, the user has the user rights specified in all the groups.

Note: If users are logged in when you reassign their group, they are not affected until they log out and try to log in again.

1. Select SAN > Users.

2. The Connectrix Manager Server Users dialog box displays. Connectrix Manager In the Users list, select a user.

3. In the Groups list, select the group(s) to which you want to assign the user. Press CTRL and click to make multiple selections.

4. Click the right arrow. The user is assigned to the selected groups.

5. Click OK.

Removing a user from a group

Note: You must have the User Management privilege to perform this task.

You can remove users from groups to take away permissions for features and topology views.

Note: If users are logged in when you reassign their group, they are not affected until they log out and try to log in again.

1. Select SAN > Users.

   The Connectrix Manager Server Users dialog box displays.

2. In the Groups list, select the group(s) from which you want to remove the user. Press CTRL and click to make multiple selections.

3. Click the left arrow.
The user is removed from the selected groups.

4. Click OK to save your changes and close the dialog box.

---

Finding a user’s groups

*Note:* Any user with User Management read-only privileges can find a user’s group.

You can determine the groups to which a user belongs through the Connectrix Manager Server Users dialog box.

1. Select SAN > Users.
   
The Connectrix Manager Server Users dialog box displays.

2. Select a user from the Users list.

3. Click the Find button.
   
The groups to which the user belongs is highlighted in the Groups list.

4. Click OK to save your changes and close the dialog box.
## Configuring remote access

You can specify the network addresses that can have access to the Server.

1. From the SAN menu, select **Remote Access**.

   The **Remote Access** dialog box displays.

2. Select the **Allow remote management sessions** checkbox to allow others to access the Server remotely.

3. Enter the maximum number of remote sessions you want to allow.

4. From the **Allow** options, choose whether to allow all or some network addresses to connect.

5. (Optional) If you selected **Only network addresses below to connect** or **All network addresses EXCEPT those below to connect**, add and remove addresses in the table at the bottom of the dialog box.
   - To add an address, click **Add**, enter a network address, and click **OK**.
   - To remove an address, select the address from the table and click **Remove**.

6. Click **OK**.
Viewing active user sessions

Since more than one Client can access a Server at a time, monitoring Clients can be an important part of maintaining the SAN. View active user sessions to determine which Clients are logged into the Server.

1. From the SAN menu, select Active Sessions.

   The Active Sessions dialog box displays. The Active Sessions dialog box lists the connected users, their network addresses, and the date and time of when they logged in. If a user is logged in from more than one location, there will be a separate entry for each session.

2. View users and the network addresses from which they connected.

3. (Optional) Select a user and click Disconnect User to disconnect the user from the Server.

   The Server will immediately shut down the Server-Client connection. The status bar on the Client will display that the Server connection was lost. All products and connections on the Physical Map will stay in the condition they were in when the session ended; they will not turn grey. The Client will display a message stating that a user disconnected the Client from the Server.

Note: To prevent this user from reconnecting, remove the user account through the Connectrix Manager Server Users dialog box. Refer to “Removing a user account” on page 115 for instructions.
Partitioned switch support

Release 9.1 displays the logical configurations of partitioned switches. Remember the following when viewing logical configurations on the topology:

- The physical set of Cisco switches display in isolated switches.
- All current view settings are used when displaying logical configurations.
- Partitioned switches are identified by their logical WWNs, not their physical WWNs.
- Cisco switch element managers provide the physical information about the switches and fabrics.
- All port information is equivalent to the physical port information.
Viewing the logical configuration of devices

You can view the logical configuration (virtual SANs) of devices on the Topology (Physical Map) and Product List.

1. Locate the virtual SAN on the topology or the Product List.
2. View switches, ISLs, and end nodes in the virtual SAN.
3. View the switch’s properties using the Properties dialog box or the Product List.
4. View the VSAN’s name and principle switch’s WWN through the Fabric Properties dialog box.

Fibre Channel networks use World Wide Names to uniquely identify nodes and ports within nodes. For many devices, the 64-bit WWNs are fixed, and their assignment follows conventions established by the IEEE. For other devices, the WWNs may be set or modified by the user. World Wide Names are a special concern for the Connectrix Manager application because:

- WWNs are used as the primary keys to identify network elements;
- Experience has been that an ill-formed WWN is evidence of a malfunctioning device.

Proper operation with the Connectrix Manager application requires that WWNs be unique within the network and well-formed (they must be 64 bits in length and the first byte cannot be zero).
Customizing the main window

You can customize the main window to display only the data you need by displaying different levels of detail on the Physical Map (topology) or Product List.

Zooming in and out of the physical map

You can zoom in or out of the Physical Map to see products and ports.

**Zooming in**

To zoom in on the Physical Map, use one of the following methods:

- Click the zoom-in icon on the toolbox
- 1. From the View menu, select Zoom.
   - The Zoom dialog box displays.
   - 2. Select a zoom percentage.
   - 3. Click OK.

**Zooming out**

To zoom out of the Physical Map, use one of the following methods:

- Click the zoom-out icon on the toolbox
- 1. From the View menu select Zoom.
   - The Zoom dialog box displays.
   - 2. Select a zoom percentage.
   - 3. Click OK.
Showing levels of detail on the physical map

You can view different levels of detail on the Physical Map, making Connectrix Manager easier.

**View fabrics**
To view only fabrics, without seeing groups, product or ports:
Select View > Show > Fabrics Only.

**View groups**
To view only groups and fabrics, without seeing products or ports:
Select View > Show > Groups Only.

**View products**
To view products, groups, and fabrics:
Select View > Show > All Products.

**View ports**
To view all ports:
Select View > Show > All Ports.

Turning flyovers on or off

Flyovers display when you place the cursor on a product. They provide a quick way to view a product’s properties.

To turn flyovers on or off, select Enable Flyover Display from the View menu.

Viewing flyovers

On the Physical Map, rest the pointer over a product icon, port, or connection.

The pop-up window containing the product, port, or connection information displays.
Setting Up the Connectrix Manager

Exporting and importing

The import and export features are important functions of the application. You can import and export data for many reasons, including to communicate issues to the support center, and capture network status.

Note: Currently, you can only export to and import from the same releases of the application (for example, export from release 8.9.1 and import to release 8.9.1).

Exporting data to disk or email

The Export dialog box displays a list of file types that can be exported, along with their sizes. You can export various SAN files to a disk or email.

You can also export to database, such as MySQL or DB2. For instructions for exporting to database, refer to “Exporting data to a database” on page 133.

1. From the SAN menu, select Export.

   The Export dialog box displays a list of file types that can be exported, along with their sizes (Figure 17 on page 131).
2. From the Export To drop-down list, select one of the following options:

To export to both Disk and EMail at the same time, complete steps 2 through 5 (as needed) for each option.

- **Disk.** Saves the exported zip files to a user-specified directory.
- **EMail.** Mails the exported files as an email attachment

_Note:_ Connectivity XML cannot be exported to email.

To export to a database, such as MySQL or DB2, refer to “Exporting data to a database” on page 133.

3. Select the types of files you want to export.

_Note:_ Some file types may not be available based on the export destination you selected in the previous step.

- **SAN Files.** Exports the SAN files.
• **Performance Data.** Exports the performance data. This is an optional feature. Contact your sales representative to purchase this module.

  **Note:** When exporting to Disk or E-mail, this option is subordinate to SAN Files. When exporting to MySQL or DB2 it is independent of SAN Files.

• **Master log.** Exports the Event files.

• **Connectivity Map.** Exports the Connectivity Map (topology) as a graphic JPG file.

• **Connectivity XML.** Exports description of all fabric topologies in XML format, including online and persisted product and connection information.

  **Note:** Connectivity XML cannot be exported to email.

• **Product List.** Exports the Product List in tab-delimited format. To view the product list in table format, open it in Microsoft Excel.

  **Note:** The Product List cannot be imported back into the Connectrix Manager application.

• **Reports.** Exports SAN reports.

• **Nicknames.** Exports nicknames.

• **Status.** Exports SAN status data used by technical support.

• **Zone set activation history.** Exports the zone set activation history.

4. If you are exporting to disk, skip to step 6. Otherwise, continue to step 5.

5. If you are exporting to email, enter information in the following fields:

  • **Mail To.** Enter the recipient’s email address.
  
  • **Mail List** button. Click to select from a list of email addresses.
  
  • **From.** Enter your email address.
  
  • **Subject.** Enter a subject for the email message.
  
  • **Message.** Enter content for the email message.

6. Click OK to export the files and close the dialog box.
7. If you exported to disk, make a note of the file location and name. Click OK at the confirmation window.

---

**Defining filters for export**

The SAN Management application enables you to filter the events included in the export of the Master Log.

1. Select SAN > Export.
   
   The Export dialog box displays.

2. Select Master log.

3. Click Select Events.

4. The Define Filter dialog box displays. Select the Include extended events checkbox to include extended events.

5. Select the Only events in the current view checkbox to only include events in the current view.

6. To add an event type to the filter, select the event from the Available Events table and click the right arrow.

7. To remove an event type from the filter, select the event from the Selected Events table and click the left arrow.

8. Click OK.

---

**Exporting data to a database**

*Note:* You can only export SAN files and Performance data to a third-party database, such as MySQL or DB2.

*Note:* Export to a DB2 database is only supported on the Windows platform.

You can also export to disk or e-mail. For instructions for exporting to disk or e-mail, refer to “Exporting data to disk or email” on page 130.

1. Configure your Connectrix Manager application for exporting to a database.

   For more information, refer to “Setting up for exporting to a MySQL database” on page 135 and “Setting up for exporting to a DB2 database” on page 135.
2. Select **SAN > Export**.

   The Export dialog box displays a list of file types that can be exported, and their size.

3. From the **Export To** list, select:
   - **MySQL.** Exports data to a MySQL database. You must have a MySQL database set up to use this feature. For instructions, refer to “Setting up for exporting to a MySQL database” on page 135.
   - **DB2.** Exports data to a DB2 database. You must have a DB2 database set up to use this feature. For instructions, refer to “Setting up for exporting to a DB2 database” on page 135.

4. Select the types of files you want to export.

   **Note:** Some file types may not be available based on the export destination you selected in the previous step.

   - **SAN Files.** Exports the SAN files.
   - **Performance Data.** Exports the performance data. This is an optional feature. Contact your sales representative to purchase this module.

   **Note:** When exporting to Disk or E-mail, this option is subordinate to SAN Files. When exporting to MySQL or DB2 it is independent of SAN Files.

5. Enter information in the following fields:

   - **Instance Name (DB2 only).** DB2 instance name.
   - **Host IP (MySQL only).** The IP address where the MySQL database resides.
   - **Port (MySQL only).** The port number used to connect to the MySQL database.
   - **DB Driver.** The location of the database driver.
   - **User ID.** User ID for the database.
   - **Password.** Password for the database.
   - **Save Password.** Saves the database password.
   - **DB Name.** Enter a name for the database export.
   - **Auto generated.** Select to have the application generate a database name for the database export.
Note: If Auto generated is cleared without giving a database name, a database name is automatically created.

6. Click Apply or OK to export the files.

7. Click OK at the confirmation window.

Setting up for exporting to a MySQL database

You can export files from the Connectrix Manager application to a MySQL database. Use these instructions to set up for exporting to a MySQL database.

Note: Your MySQL account must have a password for the export feature to work correctly.

1. Create a new folder on your computer.

2. Download the supported version of the JDBC driver from the MySQL website to the folder you created. Note the full path.

   Note: You must download the appropriate driver for the MySQL server version in your environment.

3. Follow the MySQL documentation for extracting the JDBC driver into the created folder.

4. To export files to a MySQL database, follow the instructions in “Exporting data to a database” on page 133.

Setting up for exporting to a DB2 database

You can export files from the Connectrix Manager application to a DB2 database. Use these instructions to set up for exporting to a DB2 database.

Note: Export to a DB2 database is only supported on the Windows platform.

1. Set up the DB2 client on the machine running the Server.

   Verify that the DB2 client is in the path before the Server is started.

   If the database happens to be a remote database, configure the DB2 Client to access the instance that you want to use.
Setting Up the Connectrix Manager

The Connectrix Manager application uses the JDBC application driver (db2java.zip) to connect to DB2.

The driver can be found in the Java folder after the DB2 Client is installed.

2. To export files to a MySQL database, follow the instructions in “Exporting data to a database” on page 133.

Importing data

You can choose to import the following information to the application:

- **SAN File (zip)**. Imports an entire SAN in zip format.
- **SANvergence Manager Data**. Imports an mSAN List (created using SANvergence Manager) which contains the discovered mSAN IDs, user-defined labels, SAN Router details, and Zoning files, as well as other information.

**Note:** You must exit SANvergence Manager before starting an import from the Connectrix Manager application. SANverage Manager only stores the contents of the discovered devices after you exit the application. Therefore, if SANvergence Manager is running during the Connectrix Manager import, you may not receive all IP addresses from the mSAN list.

**Note:** SANvergence Manager has a different zone data structure than the Connectrix Manager application; therefore, it must be converted into a data structure that can be re-used by Connectrix Manager application. When using Connectrix Manager application to import zones, Connectrix Manager application only converts the data into the Connectrix Manager application data structure and stores the data (xml files) in the <Install_Home>\Client\Data\Zoning directory (<Install_Home>\Client\Data\Zoning) where you can access them using the Import button on the Zoning dialog box to save them into the current Zone Library. For more information, refer to Chapter 11, “Zoning”.

- **Nicknames**. Imports the nicknames that were assigned using the Connectrix Manager and displays them on the Physical Map and Product List as product labels. Nicknames must have been defined in the Node List View of the Connectrix Manager. Nicknames defined in the Configure Ports area will not be imported.
If the WWN identifies a port or both a port and a node:

- The nickname will always be given to the port.
- If special handling is selected for the port’s node (either HBA or Storage-Tape-Bridge) the nickname will also be given to the node.

**Note:** The Storage-Tape-Bridge special handling selection may not work if you use LUN Management.

- If the node has multiple ports, the nickname from the first port on the device will be given to the node.

If the WWN identifies a node of any kind, the nickname will always be given to the node (never to the node’s ports).

- **Properties (csv).** Imports properties of products and ports, including nicknames and IP addresses. The general format for this import is in comma-separated value (CSV) ASCII format. The first line defines the kind of import (Node or Port) and lists the properties and columns in the Product List. The first column must be either **Node Name** or **Port Name**. Subsequent columns contain property (column) names. These properties may be standard (for example, **Label**), or user-defined (for example, **Cabinet Color**). Non-editable properties will not be imported (for example, **Port Count**). Non-existent columns will be ignored. The format is space-sensitive (only commas are used as separators) so trim leading or trailing spaces unless you want to import them as part of the data. To import port properties, use the **Port Name** column header. Port import will only allow the **Port Nickname** property to be set.

**Note:** You cannot import fabric type user-defined properties because both the Fabric WWN and the Switch WWN share the same WWN. When a WWN is imported using the CSV format, the WWN refers to the Switch rather than the Fabric. You can edit the user-defined properties at the Fabric Level in the Connectrix Manager application.

- **Server HBA Mappings (csv).** Imports Server HBA Mappings into the existing Fabric Map. The general format for this import is in comma-separated value (CSV) ASCII format. The first row contains the header for the file, which does not effect the import process; however, text must be present. The first two fields must be the WorldWideNodeName (WWNN), then the Server Nickname. If either of these fields (WWNN or Server Nickname)
have no text in them, the Server HBA Mapping entry is considered null and is not imported. All additional fields are ignored during the import process. The format is space-sensitive (only commas are used as separators) so trim leading or trailing spaces unless you want to import them as part of the data.

- **Storage Port Mappings (csv).** Imports Storage Port Mappings into the existing Fabric Map. The general format for this import is in comma-separated value (CSV) ASCII format. The first row contains the header for the file, which does not affect the import process; however, text must be present. The first two fields must be the WorldWidePortName (WWPN), then the Storage Array Nickname. If either of these fields (WWPN or Storage Array Nickname) have no text in them, the Storage Port Mapping entry is considered null and is not imported. All additional fields are ignored during the import process. The format is space-sensitive (only commas are used as separators) so trim leading or trailing spaces unless you want to import them as part of the data.

- **Zone set activation history.** Imports zone set files in zip format.

To import files:

1. From the **SAN** menu, select **Import**. The **Import** dialog box displays ([Figure 18](#)).

   ![Figure 18 Import dialog box](image)

2. Select the type of file you want to import from the **Import From** list.
   
   - SAN File (zip)
   - SANvergence Manager Data
   - Nicknames
   - Properties (csv)
   - Server HBA Mappings (csv)
   - Storage Port Mappings (csv)
   - Zone set activation history (zip)

3. In the **File Name** field, enter the path and file name or Browse to the file.
Note: The default path is: \Install_Home\ClientData\san<date>\san*.zip. Be sure to select the san*.zip file for import. Importing the rep*.zip file will cause errors.

The default path for the nicknames file is C:\EfcData\EmsData\EfcServices\WwnNicknames.

4. (Optional) If you selected Connectrix Manager Nicknames, select one of the following options to set special handling for nicknames assigned to ports:
   - For HBA ports, also apply the nickname to the HBA product
   - For Storage* ports, apply one of the nicknames to the Storage product
     *includes product types of Storage, Tape, and Bridge

5. Click OK.
   - If you selected SAN File, Connectrix Manager Nicknames, or Properties, continue with step 6.
   - If you selected Server HBA Mappings or Storage Port Mapping, go to step 7.

6. A message displays, stating that imported data will replace corresponding data on the server.
   - If you are sure you want to replace the data on the server, click OK.
   - If you are importing a SAN file or a properties file, the client will be logged out and the Log In dialog box will display. Log back into the application.

Important: When discovery is on, the discovered SAN will be replaced with the imported data. Only one SAN can be viewed at a time. For instructions about turning on discovery, refer to “Setting up discovery” on page 156.

7. On the Imported Results dialog box, click OK to close.

Importing SANvergence Manager Data

Connectrix Manager 9.1 allows you to import your SANvergence Manager data. The SANvergence Manager data includes discovery information (mSAN and SAN Router details), user-defined labels,
SNMP traps, TFTP paths, and Zoning files, as well as other information.

**Note:** You must exit SANvergence Manager before starting an import from the Connectix Manager. SANvergence Manager only stores the contents of the discovered devices after you exit the application. Therefore, if SANvergence Manager is running during the SAN Management import, you may not receive all IP addresses from the mSAN list.

**Note:** SANvergence Manager has a different zone data structure than the Connectix Manager; therefore, it must be converted into a data structure that can be re-used by the Connectix Manager. When importing SANvergence Manager zones, the Connectix Manager only converts the data into the Connectix Manager data structure and stores the data files (xml files) in the <Install_Home> directory (<Install_Home>\Client\Data\Zoning). You can then access them using the Import function on the Zoning dialog box to save them into the current Zone Library.

For more information, refer to Chapter 11, “Zoning” or Zoning Online Help.

To import SANvergence Manager Data files, complete the following steps.

1. Select **SAN > Import**.
2. The **Import** dialog box displays. From the **Import From** list, select **SANvergence Manager Data**.
3. In the **Installation Path** field, enter the path to the SANvergence Manager directory or Browse to the directory.

   The default path is: C:\Program Files\McDATA\SANvergence Manager 4.7.
4. Click **OK**.

   When the import is complete and successful, an User Action Event entry is created in the Master Log.
Accessing third-party tools

You can add third-party tools to the Tools menu or shortcut menus to open other software products you frequently use.

Adding a tool

You can specify third-party tools so they appear on the Setup Tools dialog box. From there, you can add them to the Tools menu and then open the tools directly from the management application.

1. Select Tools > Setup.

   The Setup Tools dialog box displays.

2. Click the Tools Menu tab

   ![Setup Tools dialog box (Tools Menu tab)](image)

   Figure 19   Setup Tools dialog box (Tools Menu tab)

3. Click Define.

   The Define Tools dialog box displays.
4. In the **Tool Name** field, type the tool’s name as you want it to appear on the **Setup Tools** dialog box.

5. In the **Path** field, type or browse to the path of the executable file.

6. In the **Working Folder** field, type or browse to the path of the folder that you want to set as your working folder.

7. To add the tool, click **Add**.
   
   The **Setup Tools** dialog box displays with the new tool added to the **Tools Menu Item** table.

   **Note:** You must click **Add** before clicking **OK**; otherwise, your changes will be lost.

8. Click **OK** to save your work and close the **Setup Tools** dialog box.

**Removing a tool**

You can remove a tool from the third-party tool list.

1. Select **Tools > Setup**.
   
   The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.

3. Click **Define**.
   
   The **Define Tools** dialog box displays.

4. In the **Tools** table, select the row of the tool you want to remove.
5. Click Remove. If the tool is not being utilized, no confirmation message displays.

**Note:** You must click Remove before clicking OK; otherwise, your changes will be lost.

6. Click OK to save your work and close the Setup Tools dialog box.

### Adding an option to the Tools menu

You can add options to the Tools menu to launch tools directly from the application.

2. Click the Tools Menu tab. The Tool Menu Items table displays all configured tools, along with the text as it displays on the Tools menu, parameters, and keystroke shortcuts.
3. In the Menu Text field, type a label for the option as you want it to appear on the Tools menu.
4. Select the application from the Tool list, or click Define if you want to specify a new tool.
   For instructions, refer to “Adding a tool” on page 141.
5. (Optional) In the Parameters field, enter parameters, such as a URL.
6. (Optional) In the Keystroke list, select a keyboard shortcut.

**Note:** You must click Add before clicking OK; otherwise, the new menu option is not created.

8. Click OK to save your work and close the Setup Tools dialog box. The tool you configured now displays on the Tools menu.
**Changing an option on the Tools menu**

You can edit parameters for third-party tools that display on the Tools menu.

1. Select **Tools > Setup**.
   The Setup Tools dialog box displays.

2. Click the **Tools Menu** tab
   The Tool Menu Items table displays all configured tools, along with the text as it displays on the Tools menu, parameters, and keyboard shortcuts.

3. In the Tool Menu Items table, select the tool you want to edit.
   The settings for the selected tool displays in the fields at the top of the dialog box.

4. Edit the fields as desired.

5. Click **Edit**.

   **Note:** You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

6. If you changed the name of a tool, you are prompted to verify the change. Accept the change.

7. Click **OK** to save your work and close the Setup Tools dialog box.

**Removing an option from the Tools menu**

You can remove a third-party tool that is listed on the Tools menu.

1. Select **Tools > Setup**.
   The Setup Tools dialog box displays.

2. Click the **Tools Menu** tab.

3. Select the tool you want to remove from the Tool Menu Items table.
   The settings for the selected tool displays in the fields at the top of the dialog box.
4. Click Remove.

   Note: You must click Remove before clicking OK; otherwise, your changes will be lost.

5. Click OK to save your work and close the Setup Tools dialog box.

---

**Adding an option to a device’s Shortcut menu**

You can add an option to a device’s shortcut menu.

1. Select Tools > Setup.
   The Setup Tools dialog box displays.

2. Click the Device Menu tab.
   The Device Popup Menu Items table displays all configured shortcut menu options.

3. In the Menu Text list, type or select the text as you want it to appear on the menu.

4. Select Match Conditions or All.
   - Select Match Conditions to display the menu option only for devices that meet the conditions listed.
   - Select All to display the menu option on the shortcut menus for all devices.

   If you selected All, skip to step 7. Otherwise, continue to step 5.

5. Select a Property name and Value for Condition 1.

6. (Optional) To define a second condition to be simultaneously true, enter the Property name and Value for Condition 2 (Condition 1 AND Condition 2 must be true).

   Note: To set up a condition where Condition 1 OR Condition 2 must be true, define two menu items, one for each condition.

7. From the Tool list, select the tool that you want to launch, or click Define to add a tool.

   For more information, refer to “Adding a tool” on page 141.

8. Click Append device ID to specify the parameter used when opening the tool.
Setting Up the Connectrix Manager

- Select **IP Address** to specify that the device’s IP address should be used when opening the tool.
- Select **Node WWN** to specify that the device’s Node WWN should be used when opening the tool.

9. Click **Add** to add the new menu item.

   It displays in the **Device Popup Menu Items** table.

   **Note:** You must click **Add** before clicking **OK**; otherwise, your changes will be lost.

10. Click **OK** to save your work and close the **Setup Tools** dialog box.

---

**Changing an option on a device’s Shortcut menu**

You can change the parameters for a tool that displays on a device’s shortcut menu.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Device Menu** tab.

   The **Device Popup Menu Items** table displays all configured shortcut menu options.

3. In the **Device Popup Menu Items** table, select the menu item you want to change.

   The settings for the selected menu item displays in the fields at the top of the dialog box.

4. Edit the fields, as necessary.

5. Click **Edit**.

   **Note:** You must click **Edit** before clicking **OK**; otherwise, your changes will be lost.

6. Click **OK** to save your work and close the **Setup Tools** dialog box.

---

**Removing an option from a device’s Shortcut menu**

You can remove a tool that displays on a device’s shortcut menu.
1. Select Tools > Setup.
   The Setup Tools dialog box displays.
2. Click the Device Menu tab.
   The Device Popup Menu Items table displays all configured menu options.
3. In the Device Popup Menu Items table, select the menu item you want to remove.
4. Click Remove.

   Note: You must click Remove before clicking OK; otherwise, your changes will be lost.
5. Click OK to save your work and close the Setup Tools dialog box.

Launching a Telnet session

You can use Telnet to log in and issue command line-based commands to a switch.

1. On the Physical Map, select the switch to which you want to connect.

   Note: The switch must have a valid IP address. If the device does not have a valid IP address, the Telnet selection will not be available on the Tools menu or the shortcut menu. You must right-click the device icon, select Properties, and enter the device’s IP address before you can open a Telnet session.

2. Select Tools > Device Menu > Telnet.
   The Telnet session window displays.

   Note: On Linux systems, you must use CTRL + BACKSPACE to delete text in the Telnet session window.

Launching an Element Manager

Element Managers are used to manage Connectrix M EMC Fibre Channel switches and directors. You can open a device’s Element Manager directly from the application.
On the Physical Map, right-click the Connectrix M EMC device you want to manage and select **Element Manager**.

The Element Manager displays.

**Starting third-party tools from the application**

You can open third-party tools from the **Tools** menu or a device’s shortcut menu. Remember that you cannot open a tool that is not installed on your computer. You must install the tool on your computer and add the tool to the **Tools** menu or device’s shortcut menu.

To open an application, choose from the following steps.

1. Select the device.
2. Use either of the following techniques:
   - Select **Tools > Product Menu > available tool**.
   - Right-click the device, and select the tool from the menu.
Invisible Body Tag

Connectrix Manager discovers products, fabrics, and connections in a SAN. Through this powerful tool, you can manage and monitor your SAN in realtime, ensuring that issues are resolved immediately. This chapter provides instructions for configuring the discovery feature.

- How discovery works ................................................................. 150
- Setting up discovery .................................................................. 156
- Setting the polling delay ........................................................... 160
- Configuring address properties ................................................ 161
- Turning discovery on and off .................................................... 170
- Determining the discovery state ............................................. 171
- Configuring Storage Port Mapping ......................................... 175
Discovering a SAN

How discovery works

Discovery is the process by which the application contacts the devices in your SAN. When you log in to a Server, the local network is automatically discovered and displayed on the Physical Map. When you configure and turn on discovery, the application discovers products connected to the SAN. The application illustrates each product and its connections on the Physical Map (topology). For details, refer to “Setting up discovery” on page 156 for details. During the discovery process, the status bar at the bottom of the main window displays “Discovery.” When discovery is turned off, the status bar displays “Discovery Off.”

During the discovery process, the status bar at the bottom of the main window displays “Discovery.” When discovery is turned off, the status bar displays “Discovery Off.”

The Connectrix Manager application enables you to discover devices using Out-of-Band and In-Band discovery.

Out-of-band discovery

When performing out-of-band discovery, the application connects to the switches through the IP network and product information is copied from the SNS database on the switch to the Server.

To correctly discover all SAN products, you must specify each product’s IP address or a subnetor subnet in the Discover Setup dialog box’s Out-of-Band tab. If you do not configure the application to directly discover the devices, the connections and attached devices may not display correctly. Only fabrics that have Connectrix-M switches as the principal switch display. If a switch is being directly managed, but exists in a fabric where the principal switch is a third-party device, another Server will not be allowed to connect to and manage those devices.

Note: Ensure that your SNMP communication parameters are set correctly in order to discover switches. Otherwise, the discovery may fail.

Note: Only one copy of the application should be used to monitor and manage the same devices in a subnet.
Manager of Manager discovery

Connectrix Manager (9.0 and higher) provides a Manager of Managers (MoM) feature that enables you to discover data from other servers (target servers) in the SAN and manage Connectrix Manager switches through the discovered target servers. The discovering server (MoM server) can be used to communicate and access multiple versions of Connectrix Manager, view performance across fabrics, and perform select management actions such as zoning. This allows you to create a consolidated “single pane” view across multiple fabrics and locations managed by multiple Connectrix Manager server instances.

Once the MoM server discovers the target server, it obtains the basic discovery information through SNMP, such as the target server description and sysObjectID. The rest of the basic discovery information is from the Connectrix Manager switches currently being managed by the target server. The management of the target server and its attached switches is through ECC-API discovery. The following table details the features which are available for this mode of discovery. For the sake of simplicity the server being discovered is referred to as the target server and the server discovering other servers is referred to as MoM server.

Table 11 on page 152 is applicable only to the switches discovered by the target server. Switches directly managed by the MoM server, have all the capabilities.
### Discovering a SAN

<table>
<thead>
<tr>
<th>MoM server</th>
<th>Target server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only MPI managed switches (see below) display in the topology with the generic icon.</td>
<td>All managed switches display in the topology with the specific icons.</td>
</tr>
<tr>
<td>• EMC DS-16M</td>
<td>All switches connected to the managed switches display with the generic icons.</td>
</tr>
<tr>
<td>• EMC DS-32M</td>
<td></td>
</tr>
<tr>
<td>• EMC DS-16M2</td>
<td></td>
</tr>
<tr>
<td>• EMC DS-32M2</td>
<td></td>
</tr>
<tr>
<td>• EMC DS-4400M</td>
<td></td>
</tr>
<tr>
<td>• EMC DS-24M2</td>
<td></td>
</tr>
<tr>
<td>• EMC DS-4700M</td>
<td></td>
</tr>
<tr>
<td>• EMC ED-64M</td>
<td></td>
</tr>
<tr>
<td>• EMC ED-140M</td>
<td></td>
</tr>
<tr>
<td>• EMC ED-10000M</td>
<td></td>
</tr>
<tr>
<td>All switches connected to the managed switches display with the generic icons.</td>
<td></td>
</tr>
<tr>
<td>Devices display as unmanaged switches (gray).</td>
<td></td>
</tr>
<tr>
<td>The MoM server displays a consolidated view of the discovered servers.</td>
<td></td>
</tr>
<tr>
<td>Call Home is not available.</td>
<td>Call home is available.</td>
</tr>
<tr>
<td>Element Manager cannot be launched for devices discovered through a target server.</td>
<td>Element Manager can be launched.</td>
</tr>
<tr>
<td>Enterprise Fabric Mode is not available.</td>
<td>Enterprise Fabric Mode is available.</td>
</tr>
<tr>
<td>Events are not passed back to the MoM server.</td>
<td>Events are available.</td>
</tr>
<tr>
<td>Fabric Binding is not available.</td>
<td>Fabric Binding is available.</td>
</tr>
<tr>
<td>Firmware code loads are not available.</td>
<td>Firmware code loads are available.</td>
</tr>
<tr>
<td>Nicknames are not available.</td>
<td>Nicknames are available.</td>
</tr>
<tr>
<td>Performance information displays in the topology (for example, marching ants, real time performance graphs, and historical performance graphs).</td>
<td>Performance information displays in the topology (for example, marching ants, real time performance graphs, and historical performance graphs).</td>
</tr>
<tr>
<td>Port Fencing is not available.</td>
<td>Port Fencing is available.</td>
</tr>
<tr>
<td>Security Center is not available.</td>
<td>Security Center is available.</td>
</tr>
<tr>
<td>Show Route supported for the managed switches.</td>
<td>No Show Route support for the switches discovered via the target server.</td>
</tr>
</tbody>
</table>
Discovering a SAN

To discover another server and manage a SAN with remote sites, complete the following steps.

1. Select Discover > Setup.
   
   The Discovery Setup dialog box displays.

2. Click the Out-of-Band tab.

3. Click Add.
   
   The Address Properties dialog box displays.

4. Specify the IP addresses you want to discover.
   
   a. On the IP Address tab, enter a description for the device at the new IP address.
   
   b. In the IP Address field, enter the IP address.
   
   c. In the Subnet Mask field, enter the subnet mask associated with the IP address.

5. Click the SNMP tab and edit the default settings, if needed.
   
   To change the SNMP default settings, refer to “Configuring a SNMP community string” on page 164.

6. Click the Product Type and Access tab.
   
   a. From the Product Type list, select Ctx Mgr Server.
   
   b. In the User ID field, enter a user ID.

### Table 11 Manager of Manager ECC-API discovery (continued)

<table>
<thead>
<tr>
<th>MoM server</th>
<th>Target server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual Fabrics are discovered and displayed but cannot be configured from the MoM server.</td>
<td>Virtual Fabrics is available.</td>
</tr>
<tr>
<td>Zoning is available. Zoning Scope and Zoning Library contains selections for all discovered fabrics as well as the discovered target servers.</td>
<td>Zoning is available. Zoning Scope and Zoning Library contains selections for all discovered fabrics.</td>
</tr>
<tr>
<td>For all other features the MoM server has the same level of support as the Target server.</td>
<td></td>
</tr>
</tbody>
</table>

Discovering data from another Connectrix Manager server

To discover another server and manage a SAN with remote sites, complete the following steps.

1. Select Discover > Setup.
   
   The Discovery Setup dialog box displays.

2. Click the Out-of-Band tab.

3. Click Add.
   
   The Address Properties dialog box displays.

4. Specify the IP addresses you want to discover.
   
   a. On the IP Address tab, enter a description for the device at the new IP address.
   
   b. In the IP Address field, enter the IP address.
   
   c. In the Subnet Mask field, enter the subnet mask associated with the IP address.

5. Click the SNMP tab and edit the default settings, if needed.
   
   To change the SNMP default settings, refer to “Configuring a SNMP community string” on page 164.

6. Click the Product Type and Access tab.
   
   a. From the Product Type list, select Ctx Mgr Server.
   
   b. In the User ID field, enter a user ID.
Discovering a SAN

**Note:** Do not confuse the Server ID with the Connectrix Manager login ID.

c. In the **Password** and **Retype Password** fields, enter the password.

7. Click **OK** on the **Address Properties** dialog box.

8. Repeat steps 1 through 16 for each device that you want to discover.

9. From the **Available Addresses** table, select the IP address you want to add to discovery.

10. Click the right arrow button next to the **Selected Individual Address** table.

    The selected addresses display in the **Selected Individual Address** table.

11. Click **OK** on the **Discover Setup** dialog box.

    The selected devices display in the Connectrix Manager main window, indicated by the Server icon.

---

**License discovery**

License discovery is only available with the Connectrix Manager 9.1 server. If you discover a Connectrix Manager 7.X or 8.X server, their licenses will not affect the MoM server license.

When configured correctly, the MoM server obtains the license key and serial number from the target server and then updates its license information with any target server licensed port count and additional modules. To configure the MoM server to obtain license information, refer to “Generating an aggregate licensed port count” on page 155.

The MoM server license updates every time a target server is added or removed from the active discovery list. However, the state of the target server (offline/online) does not affect the license. Note that when the MoM server detects a change in the licensed port count or modules, it forces the clients connected to the MoM server to logout (same behavior as license updates).
Discovering a SAN

Generating an aggregate licensed port count

To discover the license keys from managed Connectrix Manager servers and update the Manager of Manager (MoM) server license, complete the following steps.

1. Select Help > License.
   The License dialog box displays.
2. Select the Aggregate licensed port counts from all managed Connectrix Manager servers checkbox.
3. Click OK.
   A message displays, warning you that you have changed the aggregate port count setting, click Yes to continue.

   After the next discovery cycle, the MoM server updates the licensed port count and modules list to include information from all discovered managed Connectrix Manager servers. Clients connected to the MoM server are logged out automatically and must log in again.
### Setting up discovery

Discovery is the process by which the application contacts the devices in your SAN. When you log in to a Server, the local network is automatically discovered and displayed on the Physical Map. To discover specific IP addresses or subnets, you need to set up discovery.

To discover specific IP addresses or subnets, set up discovery.

Only one copy of the application should be used to monitor and manage the same devices in a subnet.

**Note:** Only one copy of the application should be used to monitor and manage the same devices in a subnet.

1. From the **Discover** menu, select **Setup**.
2. The **Discover setup** dialog box displays (Figure 20) (Figure 21). Click the **General** tab.

![Discover Setup Dialog Box (General Tab)](image)
3. Click the **General** tab.
4. Change the polling delay, if necessary.
   For details, refer to “Setting the polling delay” on page 160.
5. Select the discovery method you want to use.
   - Select the **Out-of-Band Discovery Enable** check box to perform out-of-band discovery. Continue with step 6. For more information, refer to “Out-of-band discovery” on page 150.
   - Select the **In-Band Discovery Enable** check box to perform in-band discovery. Go to step 6.

   **Important:** In-Band discovery is not supported by EMC.

   **Note:** To perform in-band discovery, an HBA must be physically installed in the Server. Download the vendor’s HBA drivers and libraries from the vendor’s website.

   - Select both options to perform both in-band and out-of-band discovery. Continue with step 6.
6. If you selected **In-Band Discovery**, in the **Available HBAs** table, select the **Active** check box for each HBA you want to use to discover the SAN.
7. Select **Clear current SAN devices before starting new discovery** to start discovery with a clean desktop.
8. Select the Rebuild Discovery Schedule check box to reset the discovery engine and rebuild the discovery catalog.

- If you selected Out-of-Band Discovery, continue with step 16.
- If you only selected In-Band Discovery, go to step 20.
- Click the Out-of-Band tab.

9. Change the polling delay, if necessary.
Refer to “Setting the polling delay” on page 160 for details.

10. Select the discovery methods you want to use.

  Refer to “How discovery works” on page 150 for background information about out-of-band discovery.
- Select In-Band to perform in-band discovery. Go to step 6.
  
  **Note:** To perform in-band discovery, an HBA must be physically installed in the Server. Download the vendor’s HBA drivers and libraries from the vendor’s website.

- Select both options to perform both in-band and out-of-band discovery. Go to step 5.

11. In the SNMP Timeout field, enter the amount of time after which the application times out.
   If you only selected Out-of-Band, go to step *.
   If you also selected In-Band, go to step 6.

12. If you selected In-Band, in the Available HBAs table, select the Active check box for each HBA you want to use to discover the SAN.

13. Select Clear current SAN devices before starting new discovery to start discovery with a clean desktop.

14. Select the Rebuild Discovery Schedule check box to reset the discovery engine and rebuild the discovery catalog.
   If you selected Out-of-Band, continue with step *.
   If you only selected In-Band, go to step 20.

15. Click the Out-of-Band tab.
16. Specify the IP addresses you want to discover through out-of-band discovery.

You can add, change, and remove IP addresses as necessary. Refer to “Configuring address properties” on page 161 for instructions.

**Note:** To correctly discover all SAN products, you must specify each product’s IP address or a subnet in the Discover Setup dialog box Out-of-Band tab. If you do not configure the application to discover the devices directly, the connections and attached devices may not display correctly.

17. Select IP addresses from the Available Addresses table and add them to the Selected Subnets table or Selected Individual Addresses table by clicking the right arrow (\(\rightarrow\)) buttons.

18. Click **Add** to specify the IP addresses you want to discover through out-of-band discovery.

You can add, change, and remove IP addresses as necessary. Refer to “Configuring address properties” on page 161 for instructions.

19. Select the Selected Subnets or Selected Individual Addresses table entries that you do not want to discover now, and move them back to the Available Addresses table by clicking the corresponding left arrow (\(\leftarrow\)) button.

20. Click **OK**.

21. Turn discovery on or off by selecting **On** or **Off** from the Discover menu.
Setting the polling delay

The polling delay allows you to configure a delay between polling cycles.

1. Select Discover > Setup.
   The Discover Setup dialog box displays.
2. Click the General tab.
3. Edit the values in the Polling Delay field.

   Note: To make sure performance data is accurate, set the polling delay below two minutes. If you set the polling delay to greater than two minutes, it may produce inaccurate performance data.
4. Click OK on the Discover Setup dialog box.

Setting the Polling Delay

The polling delay allows you to configure a delay between polling cycles.

1. Select Setup from the Discover menu.
   The Discover Setup dialog box displays (Figure 20).
2. Click the General tab.
3. Edit the values in the Polling Delay field.
4. Click OK.
Configuring address properties

You can configure IP addresses, SNMP community strings, as well as product type and access through which the application can perform discovery and communication functions and set password authentication.

Adding an IP address

You can add IP addresses and subnets through which the SAN can be discovered.

1. From the Discover menu, select Setup.

   The Discover Setup dialog box displays (Figure 21 on page 157).

2. Click the Out-of-Band tab (Figure 22).

   ![Figure 22 Discover Setup Dialog Box (Out-of-Band Tab)](image)

3. Click Add.

   The Address Properties dialog box displays (Figure 24)
Discovering a SAN

Figure 23  Address Properties Dialog Box (IP Address Tab)

Figure 24  Address Properties dialog box (IP Address tab)

Note: The dialog box may display more fields or tabs depending on your licensed features.
4. On the **IP Address** tab, enter a description for the product at the new IP address.

5. In the **IP Address** field, enter the IP address.

6. In the **Subnet Mask** field, enter the subnet mask associated with the IP address.

7. **(Optional)** To generate a sequence of IP addresses, complete the following:
   - This eliminates the need to add each IP address individually.
   - a. In the **Add Multiple** field, click the **Generate a sequence of IP addresses** option.
   - b. In the **Last IP** field, enter the last IP address in the sequence.

   All IP addresses in a sequence must be on the same subnet and have the same first three octets.

8. Click **OK** on the **Address Properties** dialog box.

9. Click **OK** on the **Discover Setup** dialog box.

---

**Editing an IP address**

You can edit IP addresses or associated subnets that are listed on the **Discover Setup** dialog box.

1. From the **Discover** menu, select **Setup**.

   The **Discover Setup** dialog box displays (Figure 21 on page 157).

2. Click the **Out-of-Band** tab.

3. Click the **Out-of-Band** tab (Figure 22).

4. In the **Available Addresses** table, select the IP address to edit.

5. Click **Edit**.

   If the IP Address you want to edit is in the **Selected Individual Addresses** tab of the **Discovery Setup** dialog box, then an **Editing Domain Information** message displays asking whether to proceed with changes. Click **OK** to continue edit.

   The **Address Properties** dialog box displays (Figure 24 on page 162).

6. Click the **IP Address** tab.
7. In the **Description** field, enter a description for the device at the new IP address.
8. In the **IP Address** field, enter the IP address.
9. In the **Subnet Mask** field, enter the subnet mask associated with the IP address.
10. Click **OK** on the **Address Properties** dialog box.
11. Click **OK** on the **Discover Setup** dialog box.

### Removing an IP address

You can remove IP addresses from the **Discover Setup** dialog box.

1. From the **Discover** menu, select **Setup**.
   
The **Discover Setup** dialog box displays (Figure 21 on page 157).
2. Click the **Out-of-Band** tab.
3. Click the **Out-of-Band** tab.
4. From the **Available Addresses** table, select the IP address you want to remove.

**Important:** When you click the **Remove** button, the IP address will be removed without confirmation.

5. Click **Remove**.

   If the IP Address you want to remove is in the **Selected Individual Addresses** tab of the **Discovery Setup** dialog box, an **Editing Domain Information** message displays asking whether to proceed with removal. Click **OK** to close this message.

   Remove the IP Address from the **Selected Individual Addresses** tab of the **Discovery Setup** dialog box, then repeat step 5 to remove the IP Address.

6. Click **OK** to close the **Discover Setup** dialog box.

### Configuring a SNMP community string

You can specify SNMP community strings used to communicate with products.

1. From the **Discover** menu, select **Setup**.
1. Click the Out-of-Band tab.
2. Click the Out-of-Band tab (Figure 22).
3. Click Add.
4. The Address Properties dialog box displays.
5. Click the SNMP tab (Figure 25).

![Address Properties Dialog Box (SNMP tab)](image1)

![Address Properties dialog box (Community strings tab)](image2)
6. In the **Target Port** field, enter the target port.

7. In the **Time-out (sec)** field, enter the duration (in seconds) after which the application times out.

8. In the **Retries** field, enter the number of times to retry the process.

9. From the **SNMP Version** drop down list, select the SNMP version.
   - If you selected v1 or v2, continue with step 14.
   - If you select v3, the SNMP tab displays the v3 required parameters. Go to step 13.

10. In the **Target Port** field, enter the target port.

11. In the **SNMP Timeout** field, enter the duration (in seconds) after which the application times out.

12. In the **Retries** field, enter the number of times to retry the process.

13. From the **SNMP Version** drop down list, select the SNMP version.
   - If you select v1 or v2, continue with step 14.
   - If you select v3, the SNMP tab displays the v3 required parameters. Go to step 26.

14. At the **Read** option, select **Default ‘public’** or **Custom**.

15. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

16. At the **Write** option, select **Default ‘private’** or **Custom**.

17. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.
   - Go to step 32.

18. In the **User Name** field, enter a user name.

19. In the **Context Name** field, enter a context name.

20. In the **Auth Protocol** field, select the authorization protocol.

21. In the **Auth Password** field, enter the authorization password.

22. In the **Retype Password** field, re-enter the authorization password.
   - If you selected , go to step 32.
23. In the **Priv Protocol** field, select the privacy protocol.

24. In the **Priv Password** field, enter the privacy password.

25. In the **Retype Password** field, re-enter the privacy password. Go to step 32.

26. In the **User Name** field, enter a user name.

27. In the **Context Name** field, enter a context name.

28. In the **Auth Protocol** field, select the authorization protocol.

29. In the **Auth Password** field, enter the authorization password.

30. In the **Priv Protocol** field, select the privacy protocol.

31. In the **Priv Password** field, enter the privacy password.

32. Click **OK** on the **Address Properties** dialog box.

33. Click **OK** on the **Discover Setup** dialog box.

---

**Reverting to a default SNMP community string**

1. From the **Discover** menu, select **Setup**.

   The **Discover Setup** dialog box displays (Figure 21 on page 157).

2. Click the **Out-of-Band** tab.

3. Click the **Out-of-Band** tab (Figure 22).
Discovering a SAN

4. Select an IP address from the Available Addresses table.
5. Click Edit.
   The Address Properties dialog box displays.
6. Click the SNMP tab (Figure 25) (Figure 26 on page 165).
7. Click Default ‘public’ and Default ‘private.’
8. Click OK on the Address Properties dialog box.
9. Click OK on the Discover Setup dialog box.

Configuring the product type and access

You can specify the product type and set a user name and password for the address.

Note: The Product Type and Access tab may not be available in all situations.

1. From the Discover menu, select Setup.
   The Discover Setup dialog box displays.
2. Click the Out-of-Band tab.
3. Click the Out-of-Band tab.
4. Click Add.
   The Address Properties dialog box displays.
5. On the Address Properties dialog box, click the Product Type and Access tab.

![Address Properties dialog box with product type and access options]
6. Select the type of device from the **Product Type** drop-down list.
   - If you selected *<not specified>* from the **Product Type** list, go to step 16.
   - If you selected **Switch** from the **Product Type** list, go to step 14.
   - If you selected **IBM ESS Storage** from the **Product Type** list, go to step 14.
   - If you selected **HDS** from the **Product Type** list, go to step 14.
   - If you selected **Clariion** from the **Product Type** list, go to step 16.
   - If you selected **CIM/WBEM Services** from the **Product Type** list, enter a name in the **Name Space** field, and go to step 14.
   - If you selected **Symmetrix** from the **Device Type** list, go to step 16.

7. If you select **IBM ESS Storage** from the **Product Type** drop-down list, go to step 14.

8. If you select **HDS** from the **Product Type** drop-down list, go to step 14.

9. If you select **Clariion** from the **Product Type** drop-down list, go to step 16.

10. If you select **CIM/WBEM Services** from the **Product Type** drop-down list, enter a name in the **Name Space** field, and go to step 14.

11. If you select **Symmetrix** from the **Device Type** drop-down list, go to step 16.

12. If you select **NetApp DFM** from the **Product Type** drop-down list, complete the following:
   a. From the **Protocol** drop-down list, select the product protocol.
   b. In the **DFM Port** field, enter the product DFM port number.
   c. Go to step 14.

13. If you select **HP XP Storage** from the **Product Type** drop-down list, continue with step 14.

14. In the **User ID** field, enter a user ID.

15. In the **Password** and **Retype Password** fields, enter the password.
16. Click OK.
17. Select the DataFabric Manager server you just added and move it to the Selected Individual Address list.
18. Click OK.

**Turning discovery on and off**

To turn discovery on, select On from the Discover menu.
To turn discovery off, select Off from the Discover menu.
Determining the discovery state

Note: The Product List panel may be hidden by default. To view all panels, select All Panels from the View menu, or press F12.

You can determine the discovery status of products by looking at the Status column in the Product List. Additionally, the operational status called “Unknown” is equivalent to the discovery state named “Offline.” The operational statuses, “Operational,” “Degraded,” and “Failed,” are equivalent to a discovery state of “Online.”

Troubleshooting discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly:

1. Verify IP connectivity by pinging the switch.
   • Open the command prompt.
   • From the Server, type ping <switch IP address>.
   If the switch/director is running E/OS v7.01 or earlier, proceed with steps 2 and 3. If the switch/director is running E/OS v8.0 or later, skip steps 2 and 3 and proceed to steps 4 and 5.

2. Verify the SNMP settings using SANpilot.
   • Launch SANpilot by opening a web browser application and entering the IP address of the product as the Internet uniform resource locator (URL).
     For example, http://10.1.1.11.
   • Log in and click OK.
   • Select Configure from the navigation panel.
   • Select the Management tab.
     The Management and SNMP tab views display (Figure 28 on page 172).
Discovering a SAN

Figure 28  SNMP settings in SAN Pilot or Connectrix Manager Basic

- Verify that the **Enable SNMP Agent** option is selected.
- Verify that the **Community Name** field displays “public” or matches the Connectrix Manager configuration.

3. Verify the product data using SANpilot.
   - Select **View** from the navigation panel.
   - Select the **Unit Properties** tab (Figure 29 on page 173).
     The **Unit Properties** tab view displays showing product properties.

If the switch/director is not running E/OS v8.0 or later, skip steps 4 and 5 and proceed to step 6.
Discovering a SAN

Troubleshooting discovery

1. Verify that the type number is one of the following:
   - 003016
   - 003032
   - 003216
   - 003232
   - 004300
   - 004500
   - 005000
   - 006064
   - 006140


3. Verify SNMP connectivity.
   - Use a third-party MIB browser to verify the SNMP connection.
   - Change SNMP default timeout.
   - Stop the Server.
Discovering a SAN

- Increase the default SNMP settings. If the device is running heavy traffic or is known to have slow SNMP response time, moderately increase the SNMP timeout (default timeout is one second) and retry count (default count is one retry).

These two values are controlled by two VMParameters residing in the bin\CtxMgrService.ini file when the application is running as a Windows service: smp.snmp.timeout and smp.snmp.retries. For example, specifying “-Dsmp.snmp.timeout=5” and “-Dsmp.snmp.retries=1” instructs the server to use five seconds as the SNMP timeout and one retry as the retry count.

**Note:** The higher the values, the longer discovery will spend waiting for a SNMP response. This translates into slower system performance.

- Restart the server.
Configuring Storage Port Mapping

The Connectrix Manager application enables you to see multiple ports on your storage devices in a SAN. It also displays the relationship between multiple ports and represents them as attached to a storage array (device) in the Device Tree, Topology, and Fabric views. Occasionally, there are cases where the Connectrix Manager application cannot see the relationship between ports attached to the same storage device. Therefore, the Connectrix Manager application allows you to manually associate the connections that the system is unable to make using the Storage Port Mapping dialog box.

The Connectrix Manager application allows you to create and assign properties to a Storage Device during the mapping process using the Storage Port Mapping dialog box. Once a Storage Device has multiple ports assigned to it you cannot change the device type. While in the Storage Port Mapping dialog box, Discovery is turned off. When you close the Storage Port Mapping dialog box, Discovery restarts.

During Discovery, if a previously mapped Storage Port is found to have a relationship with a port just discovered, the Connectrix Manager application automatically reassigns the Storage Port to the proper mapping. The two Ports are grouped together. This grouping is visually represented as a Storage Device. This Storage Device contains Node information from the discovered port and populates default information where available.

The Connectrix Manager application allows you to change the Device Type of a discovered device. Isolated Storage Ports are represented as Storage Devices. Using the Storage Port Mapping dialog you cannot change the device type to an HBA, JBOD, and so on. However, once a device has been identified as type Storage with ports assigned, you can no longer change its type.
Discovering a SAN

Adding storage ports to a storage array

1. To open the Storage Port Mapping dialog box, choose from one of the following steps.
   - Select a storage port icon in the topology view, then select Discover > Storage Port Mapping.
   - Right-click any storage port icon in the topology view and select Storage Port Mapping.
   - Right-click any storage port in the Device Tree and select Storage Port Mapping.

2. The Storage Port Mapping dialog box displays. Select a storage port from the Storage Ports table.
   
   To select more than one port, hold down the CTRL key while selecting multiple storage ports.
   
   A storage array in the Storage Array list is highlighted.

3. Click the right arrow.
   
   The selected storage port is added to the Storage Array.

4. Click OK.

Removing storage port and storage array associations

1. To open the Storage Port Mapping dialog box, choose from one of the following approaches.
   - Select a storage port icon in the topology view, then select Discover > Storage Port Mapping.
   - Right-click any storage port icon in the topology view and select Storage Port Mapping.
   - Right-click any storage port in the Device Tree and select Storage Port Mapping.
   
   The Storage Port Mapping dialog box displays.

2. Select a storage port from the Storage Array list and click the left arrow button.
   
   The selected storage port is removed from the Storage Array list and added to the Storage Ports table.

3. Click OK.
Reassigning mapped storage ports

1. To open the Storage Port Mapping dialog box, choose from one of the following approaches.
   - Select a storage port icon in the topology view, then select Discover > Storage Port Mapping.
   - Right-click any storage port icon in the topology view and select Storage Port Mapping.
   - Right-click any storage port in the Device Tree and select Storage Port Mapping.
   The Storage Port Mapping dialog box displays.

2. Select a storage port from the Storage Array list and click the left arrow button.
   The selected storage port is removed from the Storage Array list and added to the Storage Ports table.

3. Make sure that the storage port you want to reassign is still selected.

4. Select the storage array to which you want to reassign the storage port and click the right arrow button.
   The storage port moves from the Storage Ports table to the selected storage array.

5. Click OK.

Creating a storage array

1. To open the Storage Port Mapping dialog box, choose from one of the following approaches.
   - Select a storage port icon in the topology view, then select Discover > Storage Port Mapping.
   - Right-click any storage port icon in the topology view and select Storage Port Mapping.
   - Right-click any storage port in the Device Tree and select Storage Port Mapping.
   The Storage Port Mapping dialog box displays.

2. Click Create.
Discovering a SAN

A new storage array displays in the **Storage Array** list.

3. Double-click on the new array to rename the new storage array and press **Enter**.

4. Add storage ports to the new storage array.
   
   For step-by-step instructions about adding port to an array, refer to “Adding storage ports to a storage array” on page 176.
   
   **Note:** You must add storage ports to the new storage array to save the new array in the system.

5. Click **OK**.

---

**Editing storage array properties**

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
   
   - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
   - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
   - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.
     
     The **Storage Port Mapping** dialog box displays.

2. Select the storage array in the **Storage Array** list and click **Properties**.

3. The **Properties** dialog box appears. In the **Nickname** field, edit the storage array nickname, if necessary.

4. In the **Enclosure** field, enter an enclosure for the storage array.

5. In the **IP Address** field, enter the IP address for the storage array.

6. In the **Vendor** field, enter the vendor name for the storage array.

7. In the **Model #** field, enter a model number for the storage array.

8. In the **Serial #** field, enter a serial number for the storage array.

9. In the **Firmware** field, enter the firmware for the storage array.

10. In the **Location** field, enter a location for the storage array.

11. In the **Contact** field, enter a contact name for the storage array.
12. In the **Description** field, enter a description for the storage array.

13. In the **Comments** field, enter any comments.

14. Click **OK** on the **Properties** dialog box to save the storage array properties.

15. Click **OK** on the **Storage Port Mapping** dialog box.

### Deleting a storage array

1. To open the **Storage Port Mapping** dialog box, choose from one of the following approaches.
   
   - Select a storage port icon in the topology view, then select **Discover > Storage Port Mapping**.
   
   - Right-click any storage port icon in the topology view and select **Storage Port Mapping**.
   
   - Right-click any storage port in the Device Tree and select **Storage Port Mapping**.
     
     The **Storage Port Mapping** dialog box displays.

2. Select a Storage Array icon in the **Storage Array** list.

3. Click **Delete**.
   
   The selected Storage Array and all Storage Ports assigned to the array are removed from **Storage Array** list. All Storage Ports assigned to the device are moved to the **Storage Ports** table.

4. Click **OK**.
Discovering a SAN

Viewing storage port properties

1. To open the Storage Port Mapping dialog box, choose from one of the following approaches.

   • Select a storage port icon in the topology view, then select Discover > Storage Port Mapping.
   • Right-click any storage port icon in the topology view and select Storage Port Mapping.
   • Right-click any storage port in the Device Tree and select Storage Port Mapping.

   The Storage Port Mapping dialog box displays.

2. Select a storage port from the Storage Array list.

3. Click Properties.

   The Properties dialog box displays.

4. Review the properties.

5. Click OK on the Properties dialog box.

6. Click OK on the Storage Port Mapping dialog box.

Viewing storage array properties

1. To open the Storage Port Mapping dialog box, choose from one of the following approaches.

   • Select a storage port icon in the topology view, then select Discover > Storage Port Mapping.
   • Right-click any storage port icon in the topology view and select Storage Port Mapping.
   • Right-click any storage port in the Device Tree and select Storage Port Mapping.

   The Storage Port Mapping dialog box displays.

2. Select a storage array from the Storage Array list.

3. Click Properties.
4. The Properties dialog box displays. Review the properties.
5. Click OK on the Properties dialog box.
6. Click OK on the Storage Port Mapping dialog box.
This chapter provides instructions for using the Group Configuration Management feature and contains the following information.

- Overview ................................................................. 184
- Select group action tab ........................................... 185
- Creating a group event log ....................................... 185
- Installing E/OS firmware ........................................ 188
- Running data collection .......................................... 191
Overview

Group Configuration Management lets you perform selected changes related to the configuration and monitoring tasks to multiple devices at the same time. These tasks are as follows:

- Set up a group event log for display.
- Install E/OS firmware on a group of switches and directors.
- Initiate data collections on multiple switches.
- Remove the previous firmware installation and install new or previously installed firmware.

The Group Configuration Management feature tasks are accessible through the Select Group Manager option on application menus.

Group management of virtual switches

Note: This information only applies if virtual switches are configured on Directors discovered through your Connectrix Manager application.

When virtual switches are configured on fabric directors, the virtual switches, in addition to the core switches, display in the Select Switches tab. The virtual switches can be selected for any Group Manager function, but not all functions are applicable to virtual switches. Note the following differences:

- Install E/OS firmware – Firmware can only be installed on a core switch. If you include virtual switches in the group, they will not be sent the firmware upgrade.
- Run data collection – Data collections are done for both core and virtual switches. Data collected for a core switch contains parameters for the core switch and all virtual switches configured in the switch. Data collected for a virtual switch contains data for the core switch where the virtual switch is configured and data for the virtual switch. If multiple virtual switches on the same core switch are included in the group, duplicate data is collected. Therefore, you should include either the core switch in the group or one virtual switch to represent the core switch.
Select group action tab

To perform any action from the Group Manager, the following conditions must exist:

- The Connectrix Manager application must be set up to manage the switch or director.
- The switch or director must support the Element Manager option.

After your Connectrix Manager application meets these conditions, complete the following steps to use the Group Manager options.

1. Select Configure > Group Manager.
2. Select the option to use. Group Manager initially displays with the Select Group Action tab selected and with the following options available.

- **Create Group Event Log** – Set up a group event log for display.
- **Install E/OS firmware** – Installs compatible firmware on a group of products.
- **Create Run data collection** – Displays information that lets you confirm group membership and run data collection.

Creating a group event log

The Create Group Event Log option enables you to create a log that lists all events that are associated with any of the products in the specified group.

Use the Group Log feature to view or change the definition of the group event log. For instructions, see “Viewing and editing the group log” on page 187.
Group Configuration Management

**Accessing the Create Group Event Log dialog box**

1. Select Configure > Group Manager.
2. Select the Create Group Event Log button, and the following tabs display on the left side:
   - Select Switches
   - Create Log

**Selecting switches and directors**

The Select Switches/Directors dialog box displays all switches and directors that are discovered by the server and enables you to select any set of those products for use in the Group Manager.

1. On the main window, select the discovered switches and directors you want to add to the Available Switches/Directors table.
   Press Shift or CTRL and click to make multiple selections.
2. Select Configure > Group Manager.
3. Select one of the three group management options: Create Group Event Log, Install E/OS Firmware, or Run data collection.
4. Click the Select Switches tab.

   The Select Switches/Directors dialog box displays, and the switches and directors you selected in Step 1 display in the Available Switches/Director table.
5. To add a switch or director, select it in the Available Switches/Directors table and move it to the Selected Switches/Directors table using the right arrow.

**Adding a group**

1. To add a group, select and click a switch or director from the Available Switches/Directors table and click the right arrow to move it to the Selected Switches/Directors table.
2. Click Save.
3. Type a name into the Group name text box and click OK.
4. Click Next.
Creating a group event log

If you attempt to add a group name that already exists, a warning message displays. You are prompted to confirm the group definition. Click Yes to change the group definition.

5. If a group is already configured, select the Use Group down-down list and select a group from the list, and click Next.

If you select an already-configured group, a list of all the devices in that group displays in the Select Switches/Director table.

6. To remove a switch or director, select it in the Selected Switches/Directors table and move it to the Available Switches/Directors table using the left arrow.

Creating a group log

1. From the upper right section of the Group Manager - Create Group Event Log dialog, click Start.

When the group event log has completed running, a message is displayed indicating the group event log has been created.

2. If you want to cancel the group event log once it has started running, click Halt.

A message is displayed at the bottom of the dialog, indicating the group event log was not created.

3. Click Finish.

4. See “Viewing and editing the group log” on page 187 to view, edit, or delete the group event log.

Viewing and editing the group log

The group log enables you to view and delete the event logs that were created using Create Group Event Log.

1. Select Monitor > Logs > Group.

2. To save the group log, click Export.

You are prompted to name the group log.

3. After you have named the group log, select a file type.

The default file type is .txt. The default location to where the group log is saved is the local C:\ drive.

4. To delete the group log, click the Delete Log tab.

5. To exit the group log, click Close.
Installing E/OS firmware

The Install E/OS firmware option installs firmware on a group of products (either switches or directors).

To access the Install E/OS Firmware dialog box:

1. Select Configure > Group Manager.
2. Select the Install E/OS firmware button, and the following tabs display on the left side:
   - Select Switches
   - Select Firmware
   - Execution Options
   - Install
   - History

Select Firmware tab

The Select Firmware option lists all firmware that can be installed on a product in the selected products list. Use this tab to add, revise and delete firmware.

**Note:** You will receive an error message if no firmware is found in the library that is applicable to any one of the selected switches.

1. From the Install E/OS Firmware dialog box, click the Select Firmware tab. The Select Firmware dialog box displays.
2. Click Add.
   
   The Add Firmware dialog box displays.
   
   If you attempt to load firmware that already exists in the library, an error message displays.

   **Note:** After the addition of new firmware, a message, which states the firmware is successfully filed in the library, is displayed.

3. Click Modify to display the Edit Firmware Description dialog box.
4. Type a new or change an existing Description for the firmware.
5. Type a **Path** or click **Browse** to select a path for the firmware.
6. Click **OK**.
   The **Select Firmware** dialog box displays.
7. Click **Next** to advance to the next tab.

### Execution Options tab

When you select execution options, you can pause the firmware installation or halt the installation in the event of an error.

From the **Install E/OS Firmware** dialog box, click the Select Execution Options tab.

#### Enabling execution options

1. Perform the following actions sequentially until all the firmware is installed on the selected products.
   - Click the **Pause before starting each action** button to enable a **Continue** button on the **Install** tab. This gives you more control over the installation process.
   - Click the **Halt on error** button if you want to be notified if an error occurs during an installation. If there is an error, the process stops and the action will not be started on the remaining selected products.
2. Click **Next** to advance to the next tab.

### Install tab

The **Confirm Firmware Installation Parameters** dialog box lets you confirm group membership and install firmware.
1. Click Start to begin the firmware installation.
   During firmware installation, the status is displayed. The status can be one of the following:
   - Not started
   - In Progress
   - Failed
   - Completed

2. Click Halt to cancel the installation.

3. Click Next to advance to the next tab.

Note: If the Switch Properties dialog box does not reflect the E/OS firmware update immediately, use the Element Manager to confirm the firmware upgrade.

History tab

The Firmware Install History dialog box displays historic installation information and, if necessary, revert to previous firmware versions, both for individual products or for a group of products.

Reverting to previous firmware installations

1. Select the row in the firmware install history log that corresponds to the product or group of products you will revert to the previous firmware version.
   You will receive an error message if no firmware is found in the library that is applicable to any one of the selected switches.

2. To go back to the previously-installed firmware, click Revert.
   - If you need to revert the firmware installation to a previous version for an individual product, select the row that corresponds to the product, and then click Revert.
   - If you need to revert the firmware installation to a previous version for the entire group, select multiple rows until all the products in the group are highlighted, and then click Revert.

3. After you have assigned the correct firmware to the product or group of products, click Finish.
Running data collection

Use the Run data collection tab to collect maintenance data about a group of switches or directors.

Note: As tasks are completed, you will be able to select and complete options that were previously greyed out.

1. Select Configure > Group Manager.
2. Click Group Manager.
3. Select the Run data collection button, and the following tabs display on the left side.
   - Select Switches
   - Output Options
   - Execution Options
   - Data Collection

Output Options tab

Using the Output File Options tab, you can select whether your data will be combined into a zip file or placed into a designated folder for later retrieval.

Selecting output file options

1. Select one of two output types:
   - Zip the files into a single file.
   - Place the files into a folder.
2. If you elect to place the files into a folder, browse to find the location of the folder or file name where the files will be saved.
3. Click Next to advance to the Select Execution Options dialog box.

Execution Options tab

When you select execution options, you can pause or halt the data collection in the event of an error.
The Select Execution Options dialog box is displayed.

1. Perform the following actions sequentially on the selected products.
   - Click the Pause before starting each action button to enable a Continue button on the Run Data Collection dialog. This gives you more control over the installation process.
   - Click the Halt on error button if you want to be notified if an error occurs during the process. If there is an error, the process stops and the action will not be started on the remaining selected products.

2. Click Next to advance to the next tab.

Run Data Collection tab

The Run Data Collection dialog box displays information that lets you confirm group membership and run data collection with the pause execution option selected.

Running data collection

Manage data collection by performing one of the following steps.
- Click Start to run the first data collection.
- Click Continue to continue the data collection after a pause.
- Click Halt to cancel the data collection process.
- Click Finish to advance to the next tab.
This chapter provides an overview of user groups and their access levels and describes how to set up a user group.

- About user groups and access levels ............................................ 194
- Creating a user group ................................................................. 195
- Changing a user group ............................................................. 197
- Removing user groups ............................................................... 198
**About user groups and access levels**

A user with administrative privileges can assign users to user groups. Five preconfigured user groups are available with the application; however, System Administrators can also create user groups manually. Refer to “Creating a user group” on page 195 for instructions.

<table>
<thead>
<tr>
<th>User group</th>
<th>Read/Write access</th>
<th>Read-only access</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator</td>
<td>All features.</td>
<td></td>
</tr>
<tr>
<td>Maintenance</td>
<td>Call Home Event Notification Setup, Device Maintenance, and Email Event Notification Setup.</td>
<td>All other features, except Device Administration and Device Operation.</td>
</tr>
<tr>
<td>Operator</td>
<td>Device Operation.</td>
<td>All other features, except Device Administration and Device Maintenance.</td>
</tr>
<tr>
<td>Product Administrator</td>
<td>Device Administration.</td>
<td>All other features, except Device Maintenance and Device Operation.</td>
</tr>
</tbody>
</table>
Creating a user group

Note: You must be an System Administrator or Security Administrator to perform this task.

You can create a user group and specify access to certain features and/or views in the application, enhancing the security of your SAN.

1. From the SAN menu, select Users.
2. The Connectrix Manager 8.9 Connectrix Manager Server Users dialog box displays. Connectrix Manager 8.9 Connectrix Manager
   Click the Add button located below the Groups list.
   The Group dialog box displays.
3. Type a name and description for the group.
4. To assign permissions to use certain features, click the Features tab. Otherwise, skip to step 5.

   Note: You must assign a feature to the Read/Write or Read Only list for the new group to have access to that feature.

   a. In the left-hand list, select the features to which you want to allow “read and write” access.
   Press CTRL and click to select multiple features.

   Note: Depending on your licensed modules, the list of features may differ.

   b. Click the right arrow next to the Read/Write list.
   The features will be moved to the Read/Write list.

   c. In the left-hand list, select the features to which you want to allow “read only” access.
   Press CTRL and click to select multiple features.

   d. Click the right arrow next to the Read Only list.
   The features will be moved to the Read Only list.

5. To assign permissions to use certain views, click the Views tab. Otherwise, skip to step 6.
configuring User Groups

a. In the left-hand list, select the views to which you want the user group to be allowed access. Press CTRL and click to make multiple selections.

b. Click the right arrow to move the selection(s) to the Selected Views list.

6. Click OK on the Connectrix Manager Group dialog box to save the new group and close the dialog.

The new group displays in the Groups list of the Connectrix Manager 8.9 Connectrix Manager Server Users dialog box. To add users to this group, follow the instructions in “Assigning users to groups” on page 200.

7. To configure email event notification for the group, click Email Event Notification Setup.

8. Click OK to close the Connectrix Manager 8.9 Connectrix Manager Server Users dialog box.
Changing a user group

Note: You must be a System Administrator or Security Administrator to perform this task.

You can change a user group’s permissions to use certain features and views. This provides added security for your SAN as well as your Connectrix Manager.

1. From the SAN menu, select Users.
   
   The Connectrix Manager 8.9 Connectrix Manager Server Users dialog box displays.

2. Select a user group in the Groups list.

3. Click Edit located below the Groups list.
   
   The Group dialog box displays.

4. To change permissions to use certain features, click the Features tab. Otherwise, skip to step 5.
   
   a. In the Read/Write list, select the features to which you want to remove “read and write” access.
      
      Press CTRL and click to select multiple features.

   b. Click the left arrow next to the Read/Write list.
      
      The features will be moved to the left-hand list.

   c. In the Read Only list, select the features to which you want to remove “read only” access.
      
      Press CTRL and click to select multiple features.

   d. Click the left arrow next to the Read Only list.
      
      The features will be moved to the left-hand list.

5. To change permissions to use certain views, click the Views tab. Otherwise, skip to step 6.
   
   a. In the Selected Views list, select the views to which you want to remove access.
      
      Press CTRL and click to make multiple selections.

   b. Click the left arrow to move the selection(s) to the left-hand list.
Configuring User Groups

6. Click OK on the Group dialog box to save your edits and close the dialog.

7. Click OK to close the Connectrix Manager 8.9 Connectrix Manager Server Users dialog box.

Removing user groups

**Note:** You must be a System Administrator or Security Administrator to perform this task.

**Important:** After completing these steps, the user group will be removed without confirmation.

You can remove a user group regardless of whether a user is assigned to the group.

1. From the SAN menu, select Users.
   
   The Connectrix Manager 8.9 Connectrix Manager Server Users dialog box displays.

2. In the Groups list, select the group you want to remove.

3. Click Remove located below the Groups list.

4. Click OK.
This chapter describes how to assign users to groups and how to determine the groups to which a user belongs.

- Assigning users to groups .............................................................. 200
- Removing users from groups ......................................................... 200
- Finding a user’s groups ................................................................. 202
Assigning users to groups

Note: You must be a System Administrator or Security Administrator to perform this task.

You can assign users to groups to assign them permissions for features and topology views. If you assign one user to multiple groups, the user will have the user rights specified in all the groups.

Note: If the user is logged in when you reassign his group, he will not be affected until he logs out and tries to log in again.

1. From the SAN menu, select Users.
2. The Connectrix Manager 8.9 Connectrix Manager Server Users dialog box displays. Connectrix Manager 8.9 Connectrix Manager
In the Users list, select a user.
3. In the Groups list, select the group(s) to which you want to assign the user.
   Press CTRL and click to make multiple selections.
4. Click the right arrow.
   The user will be assigned to the selected groups.
5. Click OK.

Removing users from groups

Note: You must be an System Administrator or Security Administrator to perform this task.

You can remove users from groups to take away permissions for features and topology views.

Note: If the user is logged in when you reassign his group, he will not be affected until he logs out and tries to log in again.

1. From the SAN menu, select Users.
   The Connectrix Manager 8.9 Connectrix Manager Server Users dialog box displays.
2. In the **Groups** list, select the group(s) from which you want to remove the user.

   Press **CTRL** and click to make multiple selections.

3. Click the left arrow.

   The user will be removed from the selected groups.

4. Click **OK**.
Finding a user’s groups

Note: You must be a System Administrator or Security Administrator to perform this task.

You can determine the groups to which a user belongs through the Connectrix Manager 8.9 Connectrix Manager Server Users dialog box.

1. From the SAN menu, select Users.
   The Connectrix Manager 8.9 Connectrix Manager Server Users dialog box displays.
2. Select a user from the Users list.
3. Click the Find button.
   The groups to which the user belongs will be highlighted in the Groups list.
4. Click OK.
This chapter contains information on configuring SAN products and fabrics.

- Managing products ................................................................. 204
- Configuring nicknames .......................................................... 210
- Configuring Fabric Binding .................................................... 216
- Configuring Port Fencing ......................................................... 219
- Configuring trap forwarding .................................................. 236
Managing products

You can use the application to manage discovered products. You can search for a product, change its properties, and perform other configuration and maintenance tasks.

Opening a product’s Element Manager

You can open an Element Manager to manage Connectrix M EMC switches and directors directly from the application.

Opening the Element Manager from the interface

To open an Element Manager from the user interface, perform one of the following steps:

- Right-click a switch icon, and select Element Manager or Element Management (HTML).
- Double-click a switch icon.

Note: If you encounter problems, ensure that only one copy of the application is being used to monitor and manage the device. Only one copy of the application should be used to monitor and manage the same devices in a subnet.

Searching for products in a SAN

You can search a discovered SAN for a specific product by its properties, such as name or IP address.

1. Enter the search parameter in the Search box on the toolbar.

2. Click the up or down arrow to search forward or backward through the Physical Map.

3. Click the Search button to find each product.

Note: When the application finds a product on the Physical Map, it will highlight the product on the Physical Map as well as on the Product List.
Changing product properties

You can change some of the properties for online products.

**Note:** This process does not change the configuration of the product. It only changes the information that is stored on the local Server.

1. On the Physical Map, right-click a product icon and select **Properties** from the menu.
   
   The product’s **Properties** dialog box displays.

2. Click the **Properties** tab (Figure 30).

   ![Product properties dialog box (Basic)](image)

   **Figure 30**  **Product properties dialog box (Basic)**

   **Note:** If the product you selected is offline, you will not be able to edit this information.

3. Edit information as necessary.

4. When finished, click **OK** to update the product’s properties on the local Server.
Determining a product’s operational status

You can determine a product’s operational status by looking at the Physical Map or the Product List. On both the Physical Map and the Product List, you can determine a product’s operational status by looking at the associated icons.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>No icon</td>
<td>Operational</td>
</tr>
<tr>
<td>🔄</td>
<td>Attention</td>
</tr>
<tr>
<td>🔴</td>
<td>Degraded</td>
</tr>
<tr>
<td>🟢</td>
<td>Device Added</td>
</tr>
<tr>
<td>🔴</td>
<td>Device Removed</td>
</tr>
<tr>
<td>🔴</td>
<td>Failed</td>
</tr>
<tr>
<td>➡️</td>
<td>Routed In</td>
</tr>
<tr>
<td>⬅️</td>
<td>Routed Out</td>
</tr>
<tr>
<td>🚭</td>
<td>Unknown/Link Down</td>
</tr>
<tr>
<td>📰</td>
<td>Virtual Switch</td>
</tr>
</tbody>
</table>

Table 12 Product status icons

To see a list of all products requiring attention, click the Attention Indicator icon (⚠️) on the Status bar at the bottom of the main window. The Service Request dialog box displays the names and IP addresses of devices needing attention. Click a product name hyperlink to jump to the product on the Physical Map. The list will update dynamically.
Deleting an offline product

You can delete offline products from the Physical Map to make monitoring online products easier. If communication with a deleted product is re-established, the product displays again on the Physical Map.

Note: The delete command is only available for offline objects (displaying with an exclamation symbol). In other words, you can only delete products that have been physically removed or that have failed.

Deleting a single offline product

1. Delete a single product using one of the following methods:
   - Right-click the product icon and select Delete from the menu.
   - Click a product icon and select Delete from the Edit menu.
   - Click a product icon and press DEL.
2. On the message that displays, click Yes.
   The product is deleted from the Physical Map.

Deleting multiple offline products

1. Select Delete All from the Edit menu (or CTRL + DEL).
2. If there is more than one offline product, the number of offline products is listed in a confirmation message.
3. Click Yes.
   The offline product(s) and connections are removed from the Physical Map.

Showing routes between two end-products

Note: This feature is only available for fabrics consisting solely of Connectrix-M products.

You can use the Show Route feature to view the path that Fibre Channel frames must take between two end-products in a multiswitch fabric. If you intend to show a different route within the same fabric, the previous route will automatically be hidden.
**Requirements**

To view the route between two products, the following conditions must be met:

- All switches or directors in the route must be managed by the application and attached to the same Server.
- All switches or directors in the route must be Connectrix-M models and must be running firmware version E/OS 4.0 or higher.
- All attached products in the route must be in the same zone.

**Procedure**

To show the route for two specific ports on the end nodes, perform the following steps:

1. Right-click a node port and select **Show Route**.
2. The **Show Route** dialog box displays. Select a destination node port from the **Destination Port** table.
3. Click **OK**. The route between the nodes port displays on topology.
Hiding routes between two end-products

Note: This feature is only available for fabrics consisting solely of Connectrix-M products.

You can use the Hide Route feature to hide routes that Fibre Channel frames must take between two end-products in a multiswitch fabric. You must show routes before you can hide routes. Refer to “Showing routes between two end-products” on page 207 for instructions on showing routes.

To hide the route, right-click the route (line between end-nodes), or the fabric that includes the route you want to hide and select Hide Route.

Viewing properties of routes between two end-products

1. To view the properties of a route, right-click the route and select Properties. The Route Properties dialog box displays.
2. Review the source and destination ports, as well as route details.
3. Click Close to close the dialog box.

Changing a fabric’s properties

You can view and change a fabric’s properties.

1. On the Physical Map, right-click a fabric icon or the background of an expanded fabric and select Properties from the menu.
   The Fabric Properties dialog box displays.
2. View the fabric’s information and edit the nickname, if desired.
   Note: If you segment a fabric, the fabric’s nickname follows the assigned principal switch.
3. When finished, click OK to update the fabric’s properties.
Configuring nicknames

The Connectrix Manager allows you to use Nicknames as a method of providing familiar simple names to products and ports in their SAN. Using your Connectrix Manager, you can:

◆ Associate a nickname with a product or port WWN currently being discovered.
◆ Add a WWN and an associated nickname for a product or port that is not yet being discovered.
◆ Remove or disassociate a nickname from a WWN.

Viewing nicknames

The Connectrix Manager allows you to view devices by the device nickname.

4. Select Nicknames from the Configure menu. The Configure Nicknames dialog box displays. To display all devices with a nickname assigned, select All Nicknames from the Device list.

Only devices with a nickname display. The table displays the Nickname, WWN, Operational Status, and Type of the device.

Assigning a nickname to an existing device

The Connectrix Manager allows you to assign a nickname to an existing device.

1. Select Configure > Nicknames.
   The Configure Nicknames dialog box displays.
2. From the Device list, select how you want to display devices.
   You can display devices by All Nicknames, All WWNs, Only Fabrics And mSANs, Only Products, Only Ports, or Switch and N Ports.
   All discovered devices display.
3. In the Display table, select the device to which you want to assign a nickname.
4. Double-click in the **Nickname** column for the selected device and enter a nickname for the device.

   If you set nicknames to be unique on the **Options** dialog box and the nickname you entered already exists, the entry is not accepted.

   **Note:** If you segment a fabric, the fabric’s nickname follows the assigned principal switch.

---

### Adding a nickname to a new device

The Connectrix Manager allows you to add a new device.

1. Select **Nicknames** from the **Configure** menu.

   The **Configure Nicknames** dialog box displays.

2. Enter the WWN of the device in the **Detached WWN** field.

3. Enter the Nickname for the device in the **Nickname** field.

   If you set nicknames to be unique on the **Options** dialog box and the nickname you entered already exists, the entry is not accepted.

4. Click **Add**.

   The new device displays in the table.

---

### Importing nicknames

This procedure provides step-by-step instructions for importing nicknames from the **Configure Nicknames** dialog box.

If you need to add a single (') or a double (") quotation mark to a nickname, you must edit the `<Nickname>.csv` file using a text editor (such as Notepad). However, note that if you add a single or double quotation mark to the `<Nickname>.csv` file in an editor other than a text editor, the quotation marks will not display correctly in the Connectrix Manager application.

You can also import nicknames from the Import dialog box, for more information, refer to “Importing data” on page 136.

1. Select **Nicknames** from the **Configure** menu.

   The **Configure Nicknames** dialog box displays.
2. Click Import.  
   A message displays informing you that “Importing a nickname for a WWN that already has a nickname will overwrite the existing nickname” and asking if you want to continue.  
3. Click Yes to continue.  
   The Import dialog box displays.  
4. From the Import From list, select Nicknames.  
5. In the File Name field, enter or browse to the nickname file you want to import.  
6. (Optional) Select one of the following options to set special handling for nicknames assigned to ports:  
   • For HBA ports, also apply the nickname to the HBA product  
   • For Storage* ports, apply one of the nicknames to the Storage product  
      *includes product types of Storage, Tape, and Bridge  
7. Click OK.  
   The Imported Results dialog box displays.  
8. Click OK to close the Imported Results dialog box.  
   The file is imported and assigned.  

---  

**Exporting nicknames**  

1. Select Nicknames from the Configure menu.  
   The Configure Nicknames dialog box displays.  
2. Select All Nicknames or All WWNs from the Device list.  
   You can display devices by All Nicknames, All WWNs, Only Fabrics And mSANs, Only Products, Only Ports, or Switch and N Ports.  
3. Click Export.  
   The Save dialog box displays.  
4. Browse to the folder where you want to save the file and type a file name in the File Name field.  
5. Click Save.
Configuring nicknames

Removing a nickname

1. Select **Nicknames** from the **Configure** menu.
   The **Configure Nicknames** dialog box displays.
2. In the **Display** table, select the nickname of the device you want to remove.
3. Click **Remove**.
   An application message displays asking if you are sure you want to clear the selected nickname.
4. Click **Yes**.
5. Click **OK** on the Configure Nicknames dialog box.

The file is exported to the selected folder.
Configuring Enterprise Fabric Mode

The Enterprise Fabric Mode option is available on the Configure menu. This option automatically enables features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. When Enterprise Fabric Mode is enabled, each switch in the fabric automatically enforces a number of security-related features including Fabric Binding, Switch Binding, Insistent Domain IDs, Domain Register for State Change Notifications (RSCNs), and Rerouting Delays.

About Enterprise Fabric Mode

Activating Enterprise Fabric Mode enables the following:

- **Fabric Binding.** Allows or prohibits switches from merging with a selected fabric.

6. **Switch binding.** This feature, enabled through a product’s Element Manager, allows or prohibits switches from connecting to switch E_Ports and products from connecting to F_Ports.

- **Rerouting delay.** This feature, enabled through a product’s Element Manager, ensures that frames are delivered through the fabric in order to their destination. If there is a change to the fabric topology that creates a new path (for example, a new switch is added to the fabric), frames may be routed over this new path if its hop count is less than a previous path with a minimum hop count. This may result in frames being delivered to a destination out of order since frames sent over the new, shorter path may arrive ahead of older frames still in route over the older path.

- **Domain RSCNs.** This feature, enabled through a product’s Element Manager, indicates that an event occurred to a switch in a fabric. The only cause would be a switch entering or leaving the fabric. Notifications are sent fabric-wide and are not constrained by a zone set. Domain RSCNs are not sent between end-products.

- **Insistent Domain ID.** This feature, enabled through a product’s Element Manager, sets the domain ID as the active domain identification when the fabric initializes. Insistent Domain ID is enabled, the switch will isolate itself from the fabric if the preferred Domain ID is not assigned as the switch’s Domain ID.
Configuring SAN Products and Fabrics

**Configuring Enterprise Fabric Mode**

1. From the **Configure** menu, select **Enterprise Fabric Mode**.
   The **Enterprise Fabric Mode** dialog box displays (Figure 31).

   ![](image)

   **Figure 31** **Enterprise Fabric Mode** dialog box

   2. From the **Fabric Name** list, select the fabric for which you want to configure Enterprise Fabric Mode.

   3. The fabric’s current status will display in the **Enterprise Fabric Mode** field.

   4. To **activate Enterprise Fabric Mode** on the selected fabric, click the **Activate** button; or

      To **deactivate Enterprise Fabric Mode** on the selected fabric, click the **Deactivate** button.

      You must be managing the fabric in order to set this option.
The Fabric Binding feature enables you to configure whether switches can merge with a selected fabric. This provides security from accidental fabric merges and potential fabric disruption when fabrics become segmented because they cannot merge.

**Note:** Fabric Binding is only supported on Connectrix M switches and fabrics.

**Note:** You cannot disable Fabric Binding if Enterprise Fabric Mode is enabled. However, if Enterprise Fabric Mode is disabled, you can disable Fabric Binding.

### Enabling Fabric Binding

Fabric Binding is enabled through the Fabric Binding dialog box. After you have enabled Fabric Binding, use the Fabric Membership List to add switches that you want to allow into the fabric.

1. From the Configure menu, select Fabric Binding.

The Fabric Binding dialog box displays.
2. In the Fabric List table, click the Enable/Disable checkbox for fabrics for which you want to configure Fabric Binding.

Refer to “Adding switches to the Fabric Binding membership list” on page 217 for instructions on adding and removing switches from the membership list.

**Disabling Fabric Binding**

Fabric Binding can be disabled while Enterprise Fabric Mode is active if the switch is offline. This disables fabric binding and Enterprise Fabric Mode on the switch, but not the rest of the fabric. Disabled switches segment from the fabric. Fabric Binding is disabled through the Fabric Binding dialog box.

*Note:* Fabric Binding is only supported on Connectrix M switches and fabrics.

1. Select Configure > Fabric Binding.

   The Fabric Binding dialog box displays.

2. In the Fabric List table, clear the Enable/Disable check box for fabrics for which you want to disable fabric binding.

**Adding switches to the Fabric Binding membership list**

Once you have enabled Fabric Binding (refer to “Enabling Fabric Binding” on page 216), you can add and remove switches from the membership list.

*Note:* Fabric Binding is only supported on Connectrix M switches and fabrics.

1. Select Configure > Fabric Binding.

   The Fabric Binding dialog box displays.

2. Select the switches you want to add to the selected fabrics’ Fabric Membership List (FML) in the Available Switches table.

3. Click the right arrow to move the switches to the Membership List table.

4. To add a switch that does not have physical connection to the fabric:
5. Click Add Detached Switch.
   The Add Detached Product dialog displays.

6. Select Switch or SANRouter from the Device list.
   a. If you selected Switch, specify the Domain ID and Node WWN of the switch.
   b. If you selected SANRouter, specify the RPort Domain ID, RPort WWN, Node WWN for Domain ID 30, and Node WWN for Domain ID 31 of the switch.
   c. Click OK to save your changes and close the Add Detached Product dialog box.

7. Click OK to save your changes and close the Fabric Binding dialog box.

---

**Removing switches from Fabric Binding membership**

Once you have enabled Fabric Binding (refer to “Enabling Fabric Binding” on page 216), you can remove switches from the membership list.

**Note:** Fabric Binding is only supported on Connectrix M switches and fabrics.

1. Select Configure > Fabric Binding.
   The Fabric Binding dialog box displays.

2. Select the switches you want to remove from the selected fabrics’ Fabric Membership List (FML) in the Membership List table.

3. Click the left arrow to move the switches to the Available Switches table.

   **Note:** If you segment a fabric, the Fabric’s nickname follows the assigned principal switch.

4. Click OK to save your changes and close the dialog box.
Configuring Port Fencing

Port Fencing is a policy-based 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.

The Port Fencing dialog box displays any existing thresholds discovered on Connectrix-M directors and switches running E/OS 7.0fj and 8.0fj. The Port Fencing feature allows you to name a threshold, set the limit and time period for the threshold, and select objects to which to apply the threshold.

The Port Fencing dialog box can display any of the following objects:

- Fabrics
- Directors
- Switches (physical)
- Virtual Switches
- Port Types (E Port, F Port, and Fx Port)
- Ports

Physical fabrics, directors, switches, port types, and ports display in the Port Fencing dialog box when you have the privileges to manage that object. These objects are indicated by the standard product icons.

Using Port Fencing, you can directly assign a threshold to any of these physical objects. If a switch does not support Port Fencing, the Threshold field in the Ports table displays a Port Fencing Not Supported message.

However, virtual switches display when you have the privileges to manage the fabric that contains the virtual switch and are indicated by the virtual icon.
You can only directly assign thresholds to ports on a virtual switch. To assign a threshold to the virtual switch or its port types, you must assign the threshold to the associated physical switch or to another object above it in the hierarchy. If no thresholds are set above the virtual switch in the hierarchy, the ISL Protocol, Link, or Security Threshold field in the Ports table displays a Limited Fencing Support message.

**Requirements**

To configure port fencing, the following requirement must be met:

- All switches and directors must be running firmware E/OS 7.0 or higher.
  - 12-Port
  - 16-Port, 1 GB
  - 16-Port, 2 GB
  - 16-Port, 4 GB
  - 24-Port, 2 GB
  - 32-Port, 4 GB
  - 64-Port
  - 140-Port
- E/OS 7.x only supports ISL Protocol fencing.
- All switches must be discovered directly using MPI.higher.

**Thresholds**

You can create ISL Protocol, Link, and Security thresholds, which you can then assign to available objects in the tree. Thresholds are prioritized using the following policies:

- Port List policies, which have top priority, are assigned to a set of port numbers on a switch and operate no matter what other policies are assigned to the switch.
- Port Type (E_Port Type, F_Port Type, FL_Port Type) policies, which have secondary priority, apply to any port of the Port List policy.
- Default policies, which have the lowest priority, only apply to ports not governed by Port List or Port Type policies.
During the dynamic operation of a SAN, any port could be any type. For example, a technician could disconnect a port from a switch and reconnect that port to a storage port, or the port could change from an E Port to an F Port. Therefore, when calculating the Affected Ports value the SAN Management application does not look for the current port type, but looks at the policy priority level in relation to the other policies currently assigned to this switch.

When there are two or more policies on a switch, the total number of Affected Ports may be more than the total number of ports on the switch (the same port may adopt different policies depending on changes in the port’s port type).

**ISL Protocol thresholds**

Use ISL Protocol thresholds to block a port when one of the following ISL protocol errors meet 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.

**Link thresholds**

Use this type of threshold to block a port when a Link Level (Hot I/O) error meets the threshold.

- Link Level (Hot I/O) — Active Loop port repeatedly received LIP. Active non-loop port repeatedly received LR, OLS or NOS.

**Security thresholds**

Use this type of threshold to block a port when one of the following security violations occur:

- Authentication — The switch has repeatedly become unavailable due to authentication events.
- Fabric Binding — The switch has repeatedly become unavailable due to fabric binding events.
- Switch Binding — The switch has repeatedly become unavailable due to switch binding events. Switch Binding is enabled through a product’s Element Manager.
- Port Binding — The switch has repeatedly become unavailable due to port binding events.
Configuring SAN Products and Fabrics

- ISL Security — (Generic Security Error) the switch on the other side of the ISL detected a specific security violation, but is only able to tell us that a generic security violation has occurred or a security configuration mismatch was detected.
- N_Port Connection Not Allowed — The switch has repeatedly become unavailable due to N_Port connection not allowed events.

Adding thresholds

The Connectrix Manager allows you to manage ISL Protocol, Link, and Security thresholds.

Adding ISL protocol thresholds

Use this type of threshold to block a port when one of the following ISL protocol errors meet 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.

To add ISL Thresholds, complete the following:

1. From the Configure menu, select Port Fencing.
   The Port Fencing dialog box displays.
Configuring SAN Products and Fabrics

Adding link thresholds

Use this type of threshold to block a port when a Link Level (Hot I/O) error meets the threshold.

- Link Level (Hot I/O) – Active Loop port repeatedly received LIP. Active non-loop port repeatedly received LR, OLS, or NOS.
To add Link Thresholds, complete the following:

1. From the **Configure** menu, select **Port Fencing**.
   
   The **Port Fencing** dialog box displays.

2. Select **Link** from the **Violation Type** drop-down list.

3. Click **Add**.

4. The **Add Link Threshold** dialog box displays. Enter a name for the threshold in the **Name** field.

5. Select the number of port events allowed for the threshold from the **Threshold errors** drop-down list.

6. Select the time period for the threshold from the **Threshold Seconds** drop-down list.

7. Click **OK** to add the Link threshold to the table and close the **Add Link Threshold** dialog box.

8. To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 225.

9. Click **OK** to close the **Port Fencing** dialog box.

**Adding security thresholds**

Use this type of threshold to block a port when one of the following security violations occur:

- Authentication – the switch has repeatedly become unavailable due to authentication events.
- Fabric binding – the switch has repeatedly become unavailable due to fabric binding events.
- Switch binding – the switch has repeatedly become unavailable due to switch binding events.
- Port binding – the switch has repeatedly become unavailable due to port binding events.
- ISL Security – (Generic Security Error) the switch on the other side of the ISL detected a specific security violation, but is only able to tell us that a generic security violation has occurred or a security configuration mismatch was detected.
- N Port Connection Not Allowed – the switch has repeatedly become unavailable due to N port connection not allowed events.

To add Security Thresholds, complete the following:
1. From the Configure menu, select Port Fencing. The Port Fencing dialog box displays.
2. Select Security from the Violation Type drop-down list.
3. Click Add.
4. The Add Security Threshold dialog box displays. Enter a name for the threshold in the Name field.
5. Select the number of port events allowed for the threshold from the Threshold errors drop-down list.
6. Select the time limit for the threshold from the Threshold Minutes drop-down list.
7. Click OK to add the Security threshold to the table and close the Add Security Threshold dialog box.
8. To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 225.
9. Click OK to close the Port Fencing dialog box.

**Assigning thresholds**

You can assign thresholds to any active object in the Ports table. If you assign a threshold to a switch, director, or fabric object, or to the All Fabrics object, the threshold is assigned to all subordinate objects (which do not have a directly assigned threshold) in the tree.

However, if an object inherits a threshold from another object above it in the hierarchy, you cannot remove that inherited threshold directly from the subordinate object. You must either remove the threshold from the higher object to which it was directly assigned or directly assign a different threshold to the subordinate object.

To assign an existing threshold to fabric, director, switch, port type, and port objects, complete the following steps.

1. From the Configure menu, select Port Fencing. The Port Fencing dialog box displays.
2. Select a threshold type from the Violation Type drop-down list.
3. In the Thresholds table, select the threshold you want to assign.
4. In the **Ports** table, select the objects (All Fabrics, Fabric, Switch, Port Type (Security only), and/or Port) to which you want to assign the threshold.

5. Click ➤ (right arrow).

   An ➤ icon appears next to the objects you selected in the **Ports** table to show that the threshold was applied at this level and was inherited by every object below it in the tree (if not affected by lower level direct assignments).

   An ➡ icon appears next to every object in the tree to which the new threshold is applied.

6. Click **OK** to apply the threshold to the selected ports and close the **Port Fencing** dialog box.

---

### Turning off port fencing inheritance

When you directly assign a threshold to an object, the threshold is inherited by all subordinate objects (unless it already has a directly assigned threshold) in the tree. You can not remove an inherited threshold from a subordinate object. However, the Connectrix Manager application allows you to effectively turn off inheritance for individual subordinate objects while maintaining inheritance for other subordinate objects. To turn off inheritance for an individual subordinate object, you must create a new threshold with a maximum limit of events allowed and a minimum time period, then assign the new threshold to the subordinate object.

To turn off port fencing inheritance, complete the following steps.

1. Select **Configure > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.

3. In the **Name** field, type a name for the new threshold (for example, TurnOffISL).

4. From the **Threshold errors/violations** list, select the maximum number of errors or violations allowed.

5. From the **Threshold minutes/seconds** list, select the minimum time period available.

6. Click **OK** to close the **Add Threshold** dialog box.
7. Click OK to close the Port Fencing dialog box.

**Editing link thresholds**

1. From the Configure menu, select Port Fencing. The Port Fencing dialog box displays.
2. Select Link from the Violation Type drop-down list.
3. Click Edit.
4. The Edit Link Threshold dialog box displays. Change the name for the threshold in the Name field, if necessary.
5. Change the number of port events allowed for the threshold from the Threshold errors drop-down list, if necessary.
6. Change the time period for the threshold from the Threshold Seconds drop-down list, if necessary.
7. Click OK to accept the changes and close the Edit Link Threshold dialog box.

If the threshold has already been assigned to ports, a “this edit will apply to affected switches” message displays. Click OK to close.

8. To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 225.
9. Click OK to close the Port Fencing dialog box.

**Editing security thresholds**

1. From the Configure menu, select Port Fencing. The Port Fencing dialog box displays.
2. Select Security from the Violation Type drop-down list.
3. Select the threshold you want to change and click Edit.
4. The Edit Security Threshold dialog box displays. Change the name for the threshold in the Name field, if necessary.
5. Change the number of port events allowed for the threshold from the Threshold errors drop-down list, if necessary.
6. Change the time period for the threshold from the Threshold Minutes drop-down list, if necessary.
7. Click OK to accept the changes and close the *Edit Security Threshold* dialog box.

   If the threshold has already been assigned to ports, a “this edit will apply to affected switches” message displays. Click OK to close.

8. To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 225.

9. Click OK to close the *Port Fencing* dialog box.

---

**Finding assigned thresholds**

The Connectrix Manager allows you to find all ports with a specific threshold applied.

1. From the Configure menu, select Port Fencing.

   The *Port Fencing* dialog box displays.

2. Select a threshold type from the *Violation Type* drop-down list.

3. Select a threshold from the *Threshold* table.

4. Click Find.

5. Every port that uses the selected threshold is highlighted in the *Ports* table.

6. Click OK to close the *Port Fencing* dialog box.

---

**Viewing thresholds**

1. From the Configure menu, select Port Fencing.

   The *Port Fencing* dialog box displays.

2. Select a threshold type from the *Violation Type* drop-down list.

3. Review the *Thresholds* and *Ports* tables.

4. Repeat steps 2 and 3, as necessary.

5. Click OK to close the *Port Fencing* dialog box.
Removing thresholds

When you assign a new threshold to an object, the threshold that was active on that object is automatically removed. The Connectrix Manager also allows you to remove thresholds from an individual Fabric, Switch, or Switch Port, from all Fabrics, Switches, and Switch Ports at once, as well as from the Threshold table.

To remove thresholds from the All Fabrics object, an individual Fabric, Switch, or Switch Port, complete the following:

1. From the Configure menu, select Port Fencing.
   
   The Port Fencing dialog box displays.

2. Select a threshold type from the Violation Type drop-down list.

3. In the Ports table, select the object with the threshold you want to remove.

4. Click (left arrow).

   **Note:** If the selected object inherits a threshold assignment from an object higher in the tree, you cannot remove the threshold. You may assign a different threshold directly to the selected objects or change the assignment on the higher object.

   A icon displays next to every instance where the threshold was removed from an object, if there was another threshold higher in the tree that is now inherited by the object.

   A icon displays next to the affected objects.

To remove thresholds from all Fabrics, Switches, and Switch Ports as well as the Threshold table, complete the following:

1. From the Configure menu, select Port Fencing.

   The Port Fencing dialog box displays.

2. Select a threshold type from the Violation Type drop-down list.

3. In the Thresholds table, select the threshold you want to remove.

4. Click Remove.
Note: If the selected object inherits a threshold assignment from an object higher in the tree, you cannot remove the threshold. You may assign a different threshold directly to the selected objects or change the assignment on the higher object.

A ++ icon displays next to every instance where the threshold was removed from an object, if there was another threshold higher in the tree that is now inherited by the object.

A − icon displays next to the each object affected and does not inherit a threshold from higher in the tree.

5. Click OK to accept the changes and close the Port Fencing dialog box.
Persisting and unpersisting fabrics

Persisting fabrics takes a “snapshot” of the current products and connections in the fabric as a reference point for comparison to future fabric changes. You can export the topology, including persisted fabric information. Refer to “Exporting data to disk or email” on page 130.

Note: If the fabric’s principal switch changes, the new fabric must be manually persisted. Persistence does not follow the new fabric even if only one switch is removed from the original fabric. The principal switch should always be managed. Also, the principal switch must be a Connectrix-M switch or director in order to manage the devices in the fabric.

Persisting a fabric

To persist a fabric:

- Select a fabric in the Physical Map or Product List, then select Persist Fabric from the Configure menu.
- Right-click the fabric in the Product List or Physical Map and select Persist Fabric from the pop-up menu.
- Select a fabric in the Physical Map or Product List, then click the Persist Fabric button on the toolbar.

Unpersisting a fabric

To unpersist a fabric:

- Select a fabric in the Physical Map or Product List, then select Monitor>Unpersist Fabric.
- Right-click the fabric in the Product List or Physical Map and select Unpersist Fabric from the pop-up menu.
Unpersisting a single product

You can unpersist a single product in a persisted fabric if the product is no longer part of the fabric.

When a product is unpersisted, the connections associated with that product will also be removed. The persisted fabric’s data will be updated with the changes.

To unpersist a product, click the product icon and select Unpersist Product from the Configure menu, or right-click the product and select Unpersist Product from the menu.

Graphic indicators related to persisted fabrics

There are various ways to determine the status of persisted fabrics and persisted products. Real-time changes to the fabric display on the Physical Map and the Product List and are listed in the Fabric Log.

Determining a persisted fabric’s status

The fabric’s status is reflected by the indicator that displays on the fabric icon on the Physical Map and in the Product List (Figure 32 and Figure 33, respectively). Refer to Table 12 on page 206 for a list of status icon definitions.

Figure 32 Persisted fabric icon on physical map

<table>
<thead>
<tr>
<th>Product List</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="" /></td>
<td></td>
</tr>
</tbody>
</table>

Figure 33 Persisted fabric icon on product list

You can also determine changes to the persisted fabric through the Fabric Log.

To display the log, follow these steps:

1. Select a persisted fabric in the Physical Map or Product List.
2. From the Monitor menu, select Logs, then Fabric Log.
For more details on the Fabric Log, refer to “Creating reports” on page 254.

**Determining status of a product in a persisted fabric**

When a product is added to a persisted fabric, it displays with a “plus” icon (Figure 34).

![](image1)

**Figure 34 Product added to persisted fabric**

When a product is removed from a persisted fabric, it displays with a “minus” icon (Figure 35).

![](image2)

**Figure 35 Product removed from persisted fabric**

**Determining the status of connections in a persisted fabric**

If more than one connection exists between products and all connections are disconnected, the connections change to yellow, dashed lines. If one or some of the connections are disconnected (but not all), the enabled connections will appear as black lines and the disable connections will display as yellow, dashed lines with an interswitch link (ISL) alert (Figure 36). To remove an ISL alert, right-click the connection and select **Clear ISL Alert(s)**. If an ISL is added, the ISL appears as a black line.

![](image3)

**Figure 36 Removed connection in a persisted fabric**
Clearing ISL alerts

To clear a single ISL alert, right-click the ISL and select **Clear ISL Alert(s)**.

To clear all ISL alerts, select **Clear All ISL Alerts** from the **Edit** menu.

Merging persisted fabrics

When you merge two persisted fabrics, the fabric whose principal switch will be the principal switch in the merged fabric will become the “real” fabric. It will include the switches of both fabrics in the Physical Map and the Product List. The other fabric will become a “ghost” fabric.

On the Physical Map, the ghost fabric will display its original products with “minus” symbols (**Figure 37**). On the Product List, the fabric will display as offline and no products will display under the fabric. The ghost fabric will not be updated. The Fabric Log will be reset after the fabric merge.

**Figure 37**  Product removed from persisted fabric

Splitting persisted fabrics

When you split persisted fabrics, the principal switch determines which fabric is mapped to the persistent fabric. The fabric that includes the principal switch will be mapped to the persistent fabric.

Layout changes in persisted fabrics

When you move a product in a persisted fabric’s topology, the new positions will be stored on the Client. If you log in to the Server from a different Client, you will lose the layout of the products if the fabric is not persisted with the layout changes.
**Finding devices in a persisted fabric**

When a product is removed from a persisted fabric, it displays a “ghost” image with a minus icon (Figure 38). Right-click the icon and select **Find Product**. The focus will jump to the online item that corresponds to the “ghost” image from the original fabric.

![Figure 38](image)

**Figure 38  Product removed from persisted fabric**
Configuring Trap Forwarding

Trap forwarding is the process by which you can configure the application to send SNMP traps to other computers. To correctly configure trap reporting, you must configure the target computer’s IP address and SNMP ports in the Configure Trap Forwarding dialog box.

To configure trap forwarding

1. Select Trap Forwarding from the Monitor menu.
   
   The Configure Trap Forwarding dialog box displays.
   
   ![Configure Trap Forwarding dialog box]

2. If necessary, add or remove trap recipients.
   
   Refer to “To add trap recipients” on page 236 and “To remove trap recipients” on page 237 for instructions.

3. In the Configure Trap Forwarding dialog box, select the recipient from the Available Recipients table and add it to the Selected Recipients table by clicking the button.

4. To forward all traps received by the application to the recipients listed in the Selected Recipients table, select the Enable Trap Forwarding option.

5. Click OK.

To add trap recipients

1. Select Trap Forwarding from the Monitor menu.
   
   The Configure Trap Forwarding dialog box displays.
2. Click **Add**.

   The **Add Trap Recipient** dialog box displays.

   ![Add Trap Recipient dialog box]

3. (Optional) In the **Description** field, enter a description of the trap recipient.

4. In the **IP Address** field, enter the trap recipient’s IP address.

5. In the **Port** field, enter the trap recipient’s TCP/IP port number.

   **Note:** The Connectrix Manager interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label.

   Be aware that third-party applications may not correctly interpret the information.

6. Click **OK**.

7. Click **OK** to close the **Configure Trap Forwarding** dialog box.

---

**To remove trap recipients**

1. Select **Trap Forwarding** from the **Monitor** menu.

   The **Configure Trap Forwarding** dialog box displays.

2. In the **Available Recipients** table, select the recipient you want to remove.

3. Click **Remove**.

4. Click **OK**.
Configuring the SNMP agent

The following sections provide instructions for configuring the SNMP agent.

Setting up the SNMP agent

The simple network management protocol (SNMP) agent instruments the objects defined in the Fibre Channel Management (FCMGMT) Management Information Base (MIB) Version 3.1 and a small number of objects defined in MIB II. Through instrumentation of these MIB objects, the agent acts as a translator of information stored on the Server into a form usable by SNMP management stations.

You can configure network addresses and community names for up to 12 SNMP trap recipients, which receive messages through SNMP for specific events that occur on the Server.

To configure the SNMP agent that runs on the Server and implements the Fibre Alliance MIB, use the following steps:

1. Select Monitor > SNMP Agent > Setup.

   The SNMP Agent Setup dialog box displays.

2. In the SNMP Agent Setup dialog box, click the Community String tab. Choose from the following.
   - To add a new community string, click Add. Refer to “Adding community strings” on page 242 for more instructions.
   - To edit an existing community string, click the recipient’s row in the table and then click Edit. Refer to “Editing community strings” on page 242 for more instructions.
   - To remove an existing community string, click the community string row in the table and then click Remove.

3. In the SNMP Agent Setup dialog box, click the Trap Recipient tab.

4. To enable or disable authorization traps to be sent when unauthorized management stations try to access SNMP information through the Server, select the Enable Authentication Traps check box.
5. Choose from one of the following.
   - To add a new trap recipient, click **Add**.  
     Refer to “Adding trap recipients” on page 239 for more instructions.
   - To edit an existing trap recipient, click the recipient’s row in the table and then click **Edit**.  
     Refer to “Editing Trap Recipients” on page 240 for more instructions.
   - To remove a trap recipient, click the recipient’s row in the table and then click **Remove**.
6. Click **OK** to save your changes and close the dialog box.

### Turning on the SNMP agent

Select **Monitor > SNMP Agent > On**.

### Turning off the SNMP agent

Select **Monitor > SNMP Agent > Off**.

### Adding trap recipients

To add a trap recipient during SNMP agent configuration, complete the following steps.

1. Select **Monitor > SNMP Agent > Setup**.  
   The **SNMP Agent Setup** dialog box displays.
2. Click the **Trap Recipient** tab. In the **Trap Recipient** tab, click **Add**.  
   The **Add Trap Recipient** dialog box displays.
3. Select the **Activate** option to activate the trap recipient.
4. In the **IP Address** field, enter the IP Address of the trap recipient.
5. To override the default User Datagram Protocol (UDP) port number for a trap recipient with any legal, decimal UDP number, enter the UDP port number in the **UDP Port** field.

**Note:** The Connectrix Manager application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the...
varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label. Third-party applications may not correctly interpret the information.

6. In the Community String field, select or enter the trap recipient community.

7. Click OK to save your changes and close the dialog box.

**Editing Trap Recipients**

To edit an existing trap recipient during SNMP agent configuration, use the following steps:

1. In the SNMP Agent Setup dialog box, click the Trap Recipients tab.
2. Select the trap recipient you want to edit and click Edit.
3. The Edit Trap Recipient dialog box displays. Edit the trap recipient, as necessary.
   a. Clear the Activate check box to deactivate the trap recipient.
   b. In the IP Address field, edit the IP Address of the trap recipient.
   c. To override the default User Datagram Protocol (UDP) port number for a trap recipient with any legal, decimal UDP number, enter the UDP port number in the UDP Port field.

**Note:** The Connectrix Manager application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label. Third-party applications may not correctly interpret the information.

   d. In the Community String field, change the trap recipient community.
4. Click OK to save your changes and close the dialog box.
Changing the UDP Port

You can change the User Datagram Protocol (UDP) port number to a trap recipient with any legal, decimal UDP number. To change the UDP port number, complete the following steps.

1. Select **Monitor > SNMP Agent > Setup**.
   
   The **SNMP Agent Setup** dialog box displays.

2. Click the **Trap Recipient** tab.

3. In the **Trap Recipient** tab, click **Edit**.
   
   The **Edit Trap Recipient** dialog box displays.

4. In the **UDP Port** field, enter a new UDP port number.
   
   **Note:** The Connectrix Manager application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label.
   
   Third-party applications may not correctly interpret the information.

5. Click **OK** to save your changes and close the dialog box.

Removing trap recipients

To remove an existing trap recipient during SNMP agent configuration, use the following steps:

**CAUTION**

This procedure removes trap recipients without asking for confirmation.

1. In the **SNMP Agent Setup** dialog box, select the trap recipient you want to remove and click **Remove**.

   The trap recipient is removed without confirmation.

2. Click **OK** to close the dialog box.
Adding community strings

To add a community string during SNMP agent configuration, complete the following steps.

3. Select Monitor > SNMP Agent > Setup.
   The SNMP Agent Setup dialog box displays. In the SNMP Agent Setup dialog box, click the Community Strings tab, if necessary.

4. On the Community Strings tab, click Add.
   The Add Community String dialog box displays.

5. Enter a name for the community string in the Community String field.

6. Select the appropriate Privileges option.
   When you select Read and Write, an administrator at an SNMP management station has write permissions for writable MIB objects on the Server.

7. Click OK to save your changes and close the dialog box.

Editing community strings

To edit an existing community string during SNMP agent configuration, use the following steps:

1. Select Monitor > SNMP Agent > Setup.
   The SNMP Agent Setup dialog box displays.

2. In the SNMP Agent Setup dialog box, click the Community Strings tab, if necessary.

3. Select the community string you want to edit and click Edit.
   The Edit Trap Recipient dialog box displays.

4. Edit the fields as necessary.
   Refer to “Adding community strings” on page 242 for more details.

5. Click OK to save your changes and close the dialog box.
Removing community strings

To remove an existing community string during SNMP agent configuration, use the following steps:

CAUTION

This procedure removes community string without asking for confirmation.

1. In the SNMP Agent Setup dialog box, select the community string you want to remove and click Remove. The community string is removed without confirmation.
2. Click OK to save your changes and close the dialog box.

Changing the TCP/IP port for SNMP trap events

1. Select SAN > Options.
   The Options dialog box displays.
2. In the Category list, select SNMP Trap Listening.
   The SNMP Trap Listening fields display to the right of the Category list.
3. In the Server SNMP Trap Listening Port field, enter the TCP/IP port number.

   Note: The Connectrix Manager application interprets trap data and displays the proper port value for all firmware levels. When traps are generated on the switch, for firmware versions 4.X and below the varbind shows the correct port number (0) as the first port; however, for firmware versions 5.X and above the varbind shows port number 1 as the first port and the label for the first port is 0, so you need to subtract 1 from the port number extracted from the varbind to correctly match the label.
   Third-party applications may not correctly interpret the information.
4. Click Apply or OK to save your work.
5. Restart the application for your changes to take effect.
This chapter provides instructions for monitoring SAN products using the application.

- Event monitoring ................................................................. 246
- Using event notification features ........................................ 251
- Creating reports ............................................................... 254
Event monitoring

The application provides a variety of logs through which you can monitor the SAN. Two daily files are maintained: one that contains events and one that contains summary information. The format of the daily event log file name is `Event_YYYYMMDD.log`, where YYYYMMDD is the date that the events took place and the log was created. The daily summary file name format is `Event_YYYYMMDD.sum`.

You can view all events that take place in the SAN through the Master Log at the bottom of the main window. You can also view a specific log by selecting an option from the Monitor menu’s Logs submenu. The available logs include:

- **Audit log.** Displays a history of user actions performed through the application (except login/logout).
- **Event log.** Displays errors related to SNMP traps and Client-Server communications.
- **Fabric log.** Displays the events related to the selected fabric. The event types may include but are not limited to:
  - ISL added to fabric
  - ISL removed from fabric
  - Switch added to fabric
  - Switch removed from fabric
  - Fabric renamed
  - Fabric persisted
  - Fabric status changed
  - Device unpersisted
- **Group log.** Displays the event logs defined on the Group Management dialog.
- **Product state log.** Displays operational status changes of managed products.
- **Security log.** Displays the following security information:
  - Severity
  - User
  - Reason
  - Description
  - Date and Time
  - Count
  - Category
Monitoring SAN Products and Fabrics

Event monitoring

- IP
- Role
- Interface

- **Session log.** Displays the users who have logged in and out of the Server.

The application also has an event notification feature. By configuring event notification, you can specify when the application should alert you of an event. Refer to “Using event notification features” on page 251 for details. For information about the Master Log interface, fields, and icons, refer to “Master log” on page 82.

### Viewing logs

You can view log data through the Master Log on the main window. However, if you want to see only certain types of events, for example only login/logout events (session events), open a specific log through the View Logs dialog box.

To view a log, follow these instructions:

1. From the **Monitor** menu, select **Logs**, then one of the log options.
2. The **View Logs** dialog box displays (Optional) Perform one of the following actions:
   - To clear the log, click the **Clear** button.
   - To export log entries, click **Export** and refer to “Exporting log data” on page 247.
3. Click **Close** to close the **View Logs** dialog box.

### Exporting log data

You can export the Connectrix Manager log data in tab-delimited format. This feature is useful for providing the data to a third-party or including it in a report.

1. From the **Monitor** menu, select **Logs**, then one of the log options.

   The **View Logs** dialog box displays the log for the fabric you selected.

2. Click the **Export** button.

   The **Save** dialog box displays.
3. Browse to the folder where you want to save the file and type a file name in the file name field.

4. Click Save.
   The file will be exported in tab-delimited format. To view it in table format, open the file in Microsoft Excel.

**Viewing the fabric log**

You can view persisted fabric data through the Fabric Log dialog box. For more details on the Fabric Log, refer to “Event monitoring” on page 246. To display the Fabric Log:

1. Select a persisted fabric in the Physical Map or Product List.
2. From the Monitor menu, select Logs, then Fabric Log.
   The Fabric Log dialog box displays.
3. Click Close to close the Fabric Log dialog box.

**Filtering events in the master log**

You can filter the events that display in the Master Log on the main window. For more information, refer to “Master log” on page 82.

---

**Note:** The email filter in Connectrix Manager Connectrix Manager is overridden by the firmware email filter. When the firmware determines that certain events do not receive email notification, an email is not sent for those events even when the event type is added to the Selected Events table in the Define Filter dialog box.

1. On the Master Log, click the Filer hyperlink.
   The Define Filter dialog box displays.
2. Select the **Include extended events** check box to include extended events in the log.

3. Include or exclude event types.
   - To include an event type in the filter, select the event from the **Available Events** table and click the right arrow.
   - To exclude an event type from the filter, select the event from the **Selected Events** table and click the left arrow.

4. Click **OK**.

5. On the Master Log, perform one of the following actions.
   - **Select Filter** to view only the events specified in the **Define Filter** dialog box, regardless of the current view.
   - Select **Only events in current view** to view only the events specified in the **Define Filter** dialog box for products in the current view.
   - Clear both the **Filter** and **Only events in current view** check boxes to turn off the filter and view all events.

*Note:* Selecting these options only filters product-specific events.
Copying log entries

You can copy data and column headings from logs to other applications. Use this function to analyze or store the data using another tool.

Note: When using the View Logs dialog box, you can only copy one row at a time. To copy multiple rows of data, copy the data from the Master Log on the main window.

Copying rows

1. In the log window, select the row(s) you want to copy.
   • To select contiguous rows, select the first row you want to copy and Shift-click in the last contiguous row you want to copy.
   • To select noncontiguous rows, select the first row you want to copy and CTRL-click every additional row you want to copy.
2. Press CTRL+C to copy the selected information on the clipboard in tab-delimited format.
3. Open the application you want to paste the data into.
4. Click where you want to paste the data.
5. Press CTRL+V (or select the paste command from the other application).
   All data and column headings will be pasted.

Copying the entire master log

1. In the Master Log window, click in the list.
2. Choose Select All from the Edit menu (CTRL+A).
   All Master Log rows will be selected.
3. Press CTRL+C to copy the selected information in tab-delimited format.
4. In another application, click where you want to paste the data.
5. Press CTRL+V (or select the paste command from the other application).
   All data and column headings will be pasted.
Using event notification features

The application records the SAN events in the Master Log. You can configure the application to send event notifications to email addresses at certain time intervals. This is a convenient way to keep track of events that occur on the SAN. You can also configure products to “call home” for certain events, notifying the service center of product problems.

Configuring email notification

You can configure the application to send notification of events to users.

1. From the Monitor menu, select Event Notification, then Email.

   The Email Event Notification Setup dialog box displays.

2. To enable email notification, select Enable Email Event Notification.

3. In the Email Server field, enter the IP address or the name of the SMTP mail server that the server can use to send the email.

4. In the Reply Address field, enter the recipient’s email address.

5. In the Summary Interval field and drop-down list, enter the length of time the application should wait between notifications. Notifications are combined into a single email and sent at each interval setting. An interval setting of zero will cause notifications to be sent immediately.

   Important: Setting too short of an interval can cause the recipient’s email inbox to fill very quickly.
6. Select one of the following options:
   - Select **Send to** and enter an email address for a user to send a test email to a specific user.
   - Select **Send to all users enabled for notification** to send a test email to all user already set to receive notification.

7. Click the **Send Test Email** button to test the email server.
   
   A message displays whether the server was found. If the server was not found, verify that the server address was entered correctly and that the server is running.

8. To specify which users will receive email notification, click the **User List** button.
   
   The **Connectrix Manager 9.1 Connectrix Manager Server Users** dialog box displays.
   
   a. Select the **Filter** checkbox in the **Email** column for each user.
   b. Click **OK** on the **Connectrix Manager 9.1 Connectrix Manager Server Users** dialog box to save your selections and close the dialog.

9. Click **OK** on the **Email Event Notification Setup** dialog box to save your selections and close the dialog.

---

**Configuring Call Home notification**

To set up the call home feature, you first specify the support center information through the call home configuration (call home icon in the Connectrix Manager desktop). You must also enable call home notification through the **Event Notification** option under the **Monitor** menu. If you are upgrading from a previous release of the application, all of your call home settings will be preserved.

---

**Enabling Ethernet events**

*Note: This feature is only available for managed M-Series switches.*

An Ethernet event occurs when the Ethernet link between the Server and the managed product is lost. You can configure the application to send notification of Ethernet events.

1. From the **Monitor** menu, select **Ethernet Event**.
The **Configure Ethernet Event** dialog box displays.

2. To be notified when the Ethernet link between the Server and the managed product is lost, select **Enable Ethernet Event**.

3. In the **Ethernet Time Out** field, enter the length of time the application should wait before notifying you of the event.

4. Click **OK** to save your changes and close the **Configure Ethernet Event** dialog box.
Creating reports

Presenting and archiving data about a SAN is equally as important as gathering the data. Through the application, you can generate reports about the SAN. You can send the reports to network administrators, support consultants, and others interested in the SANs architecture, or archive them for future reference.

The following report type is available:

- **Product List.** Lists the Product List, which has detailed information about the products in the SAN.

- **Operating Status Change.** Lists status change for products in the SAN, including the number of products online and offline, the product with the most downtime, and details about each product’s status. Note that this report only looks at the events from the event log for the last 30 days. To save space, the log may be truncated and events lost, resulting in an inaccurate summary. The generation time for the Operating Status Report depends on the size of the event logs for the past 30 days.

- **Performance Data.** Displays the performance data. The Performance feature is an optional feature. Contact your sales representative to purchase this feature.

- **Physical Map.** Displays a graphic of the SAN’s topology.

- **Port Usage.** Lists the number of connected ports in the SAN as well as detailed usage information for each port. Since only E_Ports are displayed in the topology, they are the only ports displayed in this report.

- **Fabric Ports.** Lists fabric details including port and director utilization and individual product data.

- **Zone Library.** Lists the active zone set in the discovered zone library.
Generating reports

You can generate various reports of the SAN. Generated reports are saved to `<Install_Home>\Server\Reports\`.

1. From the Monitor menu, select Reports, then Generate. The Select Template dialog box displays.

   **Note:** You can also generate a report of the Physical Map by clicking the Generate Reports button (or **CTRL**+**G**) on the right-hand toolbox while viewing a discovered SAN.

2. Select the type(s) of reports you want to generate.
   - Product List
   - Operating Status Change
   - Performance Data
   - Physical Map
   - Port Usage
   - Fabric Ports

3. Click OK.

   The generated reports will automatically display in the Reports dialog box.

   **Note:** Hyperlinks in reports will only be active as long as the source data is available.
Viewing reports

You can view reports through the application, or through an internet browser. Reports are stored in `<Install_Home>\Server\Reports`.

1. From the Monitor menu, select Reports, then View.

   The Reports dialog box displays.

2. In the left-hand pane, select the report you want to view.

   If you don’t see the report you want to view, generate it first by following the instructions in “Generating reports” on page 255.

   - Product List
   - Operating Status Change
   - Performance Data
   - Physical Map
   - Port Usage
   - Fabric Ports

   Note: Hyperlinks in reports will only be active as long as the source data is available.

3. To view the report in your Web browser window, click Show in Browser.

   The selected report displays in your default Web browser.

4. Click the Close button in the View Reports window to close it.
Printing reports

You can print reports through an internet browser. Reports are stored in `<Install_Home>\Server\Reports\`.

1. Select Monitor > Reports > View.
   The View Reports dialog box displays.
2. Select the report you want to view in the left pane of the dialog box.
   If you do not see the report you want to view, generate it first by following the instructions in “Generating reports” on page 255.

   Note: Hyperlinks in reports are active only as long as the source data is available.

3. Click Show in Browser.
   The selected report displays in your default Web browser.
4. Select File > Print (in the Web browser).
   The Print dialog box displays.
5. Select the printer to which you want to print and click Print.
6. Click the Close button in the Web browser to close.
7. Click the Close button in the View Reports dialog box to close.

Printing a Physical Map report

You can print a Physical Map report through a photo editor application.

1. Browse to `<Install_Home>\Server\Reports\` and select the Physical Map report you want to print.
2. Open the folder of the Physical Map report you want to print.
3. Open the image (san.jpg) in a photo editor application.
4. Select File > Print.
   The Print dialog box displays.
5. Select the printer to which you want to print and click Print.
6. Click the Close button in the photo editor to close.
7. Click the Close button in the View Reports dialog box to close.
Deleting reports

You can delete reports using the View Reports dialog box.

1. From the Monitor menu, select Reports, then View. The Reports dialog box displays.

2. Select the report(s) you want to delete in the left pane of the dialog box.

   **Important:** Once you click Delete Reports, the report will be deleted without confirmation.

3. Click Delete Reports.

4. Click the Close button in the View Reports dialog box to close it.
This chapter provides instructions for performing administrative functions with zoning. You can rename, duplicate, delete, and perform other tasks on zones and zone sets.

- Assigning zone properties .............................................................. 261
- Comparing zone sets .................................................................. 262
- Copying a zone to a library ......................................................... 264
- Copying a zone set to a library ..................................................... 265
- Deleting a fabric and its zone library .......................................... 267
- Deleting a zone ........................................................................... 268
- Deleting a zone set ..................................................................... 269
- Duplicating a zone ...................................................................... 270
- Duplicating a zone set ................................................................. 271
- Exporting zones and zone sets..................................................... 272
- Finding a member in one or more zones ..................................... 273
- Finding a zone member in the potential member list .................. 274
- Finding zones in a zone set .......................................................... 275
- Finding a zone set member in the zones list ............................... 275
- Importing a zone set ................................................................... 276
- Listing zone members ................................................................. 277
- Removing zone members ............................................................. 279
- Removing a zone from a zone set ............................................... 280
- Renaming a zone ....................................................................... 281
- Renaming a zone set .................................................................. 282
- Replacing a zone set from history .............................................. 282
- Replacing zone members ............................................................ 284
- Saving the active zone set to a zone library ............................... 286
- Searching for a zone member by WWN or nickname ............... 288
- Setting the zoning delay .............................................................. 289
Zoning

- Viewing properties for iFCP links ................................................. 290
- Viewing properties for zones and zone sets ................................. 291
- Viewing zoning reports ................................................................. 292
- Configuring zoning ..................................................................... 294
- Accessing zoning ........................................................................ 294
- Zoning limits ................................................................................ 295
- Zoning naming conventions ......................................................... 295
- Administrator zoning privileges .................................................. 295
- Configuring zoning ..................................................................... 297
- Creating a new zone ..................................................................... 299
- Adding members to a zone ........................................................... 299
- Creating a new member in a zone ................................................. 300
- Creating a zone set ...................................................................... 302
- Adding zones to zone sets ............................................................ 303
- Activating a zone set .................................................................... 304
- Enabling or disabling the default zone for fabrics ...................... 307
- Enabling or disabling safe zoning mode for fabrics .................... 308
- Removing a member from a zone ............................................... 309
- Removing a zone from a zone set ................................................. 310
- Deactivating a zone set ............................................................... 311
Assigning zone properties

The content and format of the Zone Properties dialog box vary slightly based on whether it is being displayed for an FC fabric, Router fabric, or mSAN. All three contain the fields in Table 13.

### Table 13 Fields and descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zone name</td>
<td>Displays the name of the zone</td>
</tr>
<tr>
<td>Zone sets containing this zone</td>
<td>Displays the number of zone sets containing the selected zone.</td>
</tr>
<tr>
<td>Total zone members</td>
<td>Lists the number of zone member in the selected zone.</td>
</tr>
<tr>
<td>Status</td>
<td>Lists the status of the selected zone.</td>
</tr>
</tbody>
</table>

However, the versions of the dialog box for Router Fabrics and mSANs contain the following three additional fields:

- **Zone ID** — Every router zone has a unique ID that is assigned to it automatically and sequentially. The IDs are used by routers to identify the zones. Zone IDs are particularly important when devices must be shared between mSANs over an iFCP link. For devices to be able to communicate, their zones must be exported from each of the link using identical zone IDs. The valid range of zone IDs is 1 to 512.

- **Min Guaranteed Bandwidth** — The minimum guaranteed bandwidth for the zone.

- **Max Allowed Bandwidth** — The maximum allowed bandwidth for the zone.

The minimum guaranteed and maximum allowed bandwidth values vary with the level of operating system firmware. When the firmware level is less than 4.7, the bandwidth range is 150 to 1 million Kb/s; when the firmware level is equal to or greater than 4.7, the range is 1 to 125 MB/s.

Note that when a zone is copied and saved from one Router fabric or mSAN with one level of firmware to another Router fabric or mSAN with a different level of firmware, the system converts the bandwidth accordingly.
A new zone name can be assigned to any zone in an FC fabric, Router fabric, or mSAN. The zone ID and bandwidth properties only apply to Router fabrics and mSANs.

Note that specifying a new zone name on the Zone Properties dialog box has the same result as using the Rename command on a shortcut menu. For information about this command, refer to the procedure “Renaming a zone” on page 281.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. In the Zones list, right-click the zone whose properties you want to assign and select Properties.
   The Zone Properties dialog box displays.

4. Key in the new value for the desired property.
   If you key in an incorrect zone ID or bandwidth value, a message displays informing you of this. Click OK to reset the value in the Zone Properties dialog box. Key in a correct value or proceed to Step 5.

5. Click Close to exit the Zone Properties dialog box.

6. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.

Comparing zone sets

You can compare zone sets against one another to identify any and all differences between the two sets. You can compare the active zone set with an inactive zone set, or you can compare any two inactive zone sets.
Comparing zone sets

Remember that for mSANs, when the active zone set is compared to an inactive one, fabrics in the mSAN are not individually compared. Instead, the aggregate zone set, which contains all the zones in all the fabrics in the mSAN active zone set, are compared to the inactive zone set.

1. Select Configure > Zoning.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Perform one of the following actions based on the kind of comparison you want to do:

   • To compare the active zone set to an inactive zone set, click the Active Zone Set tab, then click Compare. The Select a Zone Set dialog box displays.

   • To compare any zone set with any other zone set, right-click one of the zone sets in the Zone Sets list and select Compare With. The Select a Zone Set dialog box displays.

   The Select a Zone Set dialog box lists all the existing zone sets in the selected zone library.

4. Select the zone set to which you want to compare the previously selected zone set and click OK.

   When the two zone sets have the same zones and zone members, a message box informing you that the two sets are identical is displayed.

   When the two zone sets have different zones or zone members, the Compare Zone Sets dialog box displays. By default, the dialog box shows both what the two zone sets have in common and what is different between the zone sets. To view only the differences, click the Changes Only check box.

5. Review the comparison information. Click Close to dismiss the Compare Zone Sets dialog box.

6. Click OK to close the Zoning dialog box.

   If you have made any changes in addition to comparing zone sets, a message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and
warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.

### Copying a zone to a library

As with a save operation, when you copy a zone a comparison is automatically performed to ensure there are no conflicts between the zone being copied and existing zones in the destination zone library. The specific items compared are as follows:

- For FC fabrics, the zone names and contents are compared.
- For Router fabrics, the zone ID of the zone being copied is compared to the IDs of all existing zones, in addition to zone names and contents being compared.
- For mSANs, the zone name and contents of the zone being copied are compared to the names and contents of all the zones in all the fabrics in the mSAN.

1. Select Configure > Zoning.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Select the destination library to which you want to copy the zone in the Zone Library list.

4. Right-click the zone you want to copy in the Zones list and select Copy Into.

   When successful, the zone you want to copy is compared to the zones in the destination zone library. If no conflicts are found, the selected zone is copied. However, note the following exceptions:

   - If the destination library contains a zone that is identical (in ID, name, and contents) to the one being saved, a message informs you that a copy will overwrite the zone in the destination library and asks whether you want to proceed. Click Yes to continue and overwrite the existing zone with the one being copied, or, click No to cancel the copy operation.
• If the destination library contains a zone with the same name as the one being copied but different contents, a message displays informing you of this, warning you that continuing will overwrite the existing zone, and asking whether you want to proceed. Click **Detail** for a list of differences between the zones, click **Yes** to overwrite the existing zone, or click **No** to cancel the copy operation.

• If the destination library contains a zone with a different name or zone ID, a message displays informing you of the conflict and asking whether you want to overwrite the zone with the name conflict and assign it the next available zone ID. Click **Detail** for a list of differences between the zones, click **Yes** to overwrite the existing zone, or click **No** to cancel the copy operation.

5. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the **Zoning** dialog box, or click **Cancel** to stop your exit from the **Zoning** dialog box.

**Copying a zone set to a library**

As with a save operation, when you copy a zone set a comparison is automatically performed to ensure there are no conflicts between the zone set being copied and existing zone sets in the zone library. The specific items compared are as follows:

- For FC fabrics, the zone set name and its zones and their contents are compared.
- For Router fabrics, the zone IDs of the zones in the zone set being copied are compared to the IDs of all existing zones, in addition to zone set names and contents being compared.
- For mSANs, the name and the zones and the contents of the zone set being copied are compared to the names and contents of all the zone sets in all the fabrics of the mSAN.
Important: If you are running a QLogic switch in a fabric and it is the principal switch, turn the switch’s auto-save feature off before you configure zoning. The feature will store zone libraries on the QLogic switch. This is not only redundant, but will eventually cause a failure because zone member limits will be exceeded.

1. Select Configure > Zoning.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the zone set you want to copy in the Zone Sets list and select Copy Into.

   When successful, the zone set you want to copy is compared to the zone sets in the destination zone library. If no conflicts are found, the selected zone set is copied. However, note the following exceptions:

   • If the destination library contains a zone set that is identical (in ID, name, and contents) to the one being saved, a message informs you that a copy will overwrite the zone set in the destination library and asks whether you want to proceed. Click Yes to continue and overwrite the existing zone set with the one being copied, or, click No to cancel the copy operation.

   • If the destination library contains a zone set with the same name as the one being copied but different contents, a message is displayed informing you of this, warning you that continuing will overwrite the existing zone, and asking whether you want to proceed. Click Detail for a list of differences between the zones, click Yes to overwrite the existing zone, or click No to cancel the copy operation.

   • If the destination library contains a zone with a different name or zone ID, a message displays informing you of the conflict and asking whether you want to overwrite the zone with the name conflict and assign it the next available zone ID. Click Detail for a list of differences between the zones, click Yes to overwrite the existing zone, or click No to cancel the copy operation.
Deleting a fabric and its zone library

Use this procedure to delete a fabric and its associated zone library. Note that you can only delete a fabric that is no longer being discovered. Furthermore, you cannot delete the Global Library.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected fabric.
   The name of the library for the fabric displays in the Zone Library field.

3. Click Delete.
   A message box displays asking you to confirm the deletion.

4. Click Yes to delete the selected fabric.
   The message box closes and, when successful, the fabric is removed from the Potential Members list and the library is removed from the Zone Library list.

5. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Deleting a zone

Use this procedure to delete a zone.

1. Select Configure > Zoning.
   
The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the zone you want to delete in the Zones list and select Delete.

   A message box displays asking you to confirm the deletion.

4. Click Yes to delete the selected zone.

   The message box closes and, when successful, the zone is removed from the Zones list.

   However, if the zone you selected contains routed devices, a message displays informing you that such a zone must be unexported from the iFCP link before it can be deleted. Click OK to close the message box. Take the appropriate steps to unexport the zone and then retry this delete procedure.

   **Important:** If you select “Don’t show me this again.” on the confirmation message box, the next time you delete a zone, the zone is deleted without requesting confirmation from you. If you delete something in error, click Cancel on the Zoning dialog box to restore it.

5. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Deleting a zone set

Use this procedure to delete a zone set.

1. Select Configure > Zoning.
   
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the zone set you want to delete in the Zone Sets list and select Delete.
   
   A message box displays asking you to confirm the deletion.

4. Click Yes to delete the selected zone set.
   
   The message box closes and, when successful, the zone set is removed from the Zone Sets list.

   However, if the zone set you selected contains routed devices, a message displays informing you that such a zone set must be unexported from the iFCP link before it can be deleted. Click OK to close the message box. Take the appropriate steps to unexport the zone and then retry this delete procedure.

   **Important:** If you select “Don’t show me this again.” on the confirmation message box, the next time you delete a zone set, it will be deleted without requesting confirmation from you. If you delete something in error, click Cancel on the Zoning dialog box to restore it.

5. Click OK or Apply to save your changes.
   
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Duplicating a zone

When you duplicate a zone, you make a copy of it in the same zone library. The first time a zone is duplicated, the duplicate is automatically given the name <zonelabel>_copy. On subsequent times, a sequential number is assigned to the zone name, such as <zonelabel>_1, <zonelabel>_2, and <zonelabel>_3.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Right-click the zone you want to duplicate in the Zones list and select Duplicate.
   The duplicated zone displays in the Zones list.
4. Key in a new name for the zone, if desired. If not, proceed to Step 5.
   If you key in a new name, press Enter to save the name.
   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click Yes to continue, or No to cancel the renaming. (For zone name requirements and limitations, refer to “Zoning naming conventions” on page 295.)
5. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
**Duplicating a zone set**

When you duplicate a zone set, you make a copy of it in the same zone library. The first time a zone set is duplicated, the duplicate is automatically given the name `<zonesetlabel>_copy`. On subsequent times, a sequential number is assigned to the zone name, such as `<zonesetlabel>_1`, `<zonesetlabel>_2`, and `<zonesetlabel>_3`.

Note that these naming conventions apply both to duplicate and deep duplicate operations.

1. Select Configure > Zoning.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the zone set you want to duplicate in the Zone Sets list and select one of the following options:

   - **Duplicate** - to duplicate the zone set
   - **Deep Duplicate** - to duplicate the zone set and all its zones

   The duplicated zone set displays in the Zone Sets list.

4. Key in a new name for the zone set if desired. If not, proceed to Step 5.

   If you key in a new name, press Enter to save the name.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click Yes to continue, or No to cancel the renaming. (For zone set name requirements and limitations, refer to “Zoning naming conventions” on page 295.)

5. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Zoning

Exporting zones and zone sets

You can export zone sets as an XML file and then import them into another Server’s zone set library, or to a different zone set library on the current Server.

Note that for devices in a local mSAN to be visible to a remote mSAN and vice versa, the zones containing the devices must be exported over an iFCP link. The exporting is performed by adding the zones with identical zone IDs under the same iFCP link on the Zone Sets lists of both the local and remote mSANs. The router zones may have different names, but if the zone IDs do not match, the zones are not exported over the iFCP link; an information message is displayed informing you that the local zone needs the same ID as that of a remote zone before it can be exported over the iFCP link. When performed correctly, the zones merge during zone set activation. An exported zone can be unexported by removing it from the iFCP link.

In addition to the requirement for identical zone IDs, note the following configuration requirements:

◆ A zone cannot be exported over two or more iFCP links to the same remote mSAN.
◆ A device cannot be exported over two or more iFCP links to the same mSAN.
◆ A fabric port cannot be exported over an iFCP link. Stated another way, an F or FL_port cannot be added to a zone that is exported over an iFCP link.

If any of these export operations are performed and then followed by an attempt to activate the zone set, the activation fails and the configuration violation is identified in an activation failure message.

Note: You can only export one zone set at a time.

1. Select Configure > Zoning.

The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Select the zone set you want to export in the Zone Sets list.
4. Click Export.
   The Export Zone Set dialog box displays.
5. Browse the Look in field and find the folder to which you want to export the zone set.
6. Type a name for the file in the File name field.
7. Click Export Zone Set.
   The file is saved to the location you specified and the Export Zone Set dialog box is closed.
   When attempting to export the zone set and add it under an iFCP link, various messages may display to inform you of the condition of the export operation. Click OK to close any of the message boxes. If the condition reports an error, particularly a mismatch in zone IDs, correct the mismatch and retry the export operation.
8. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.

**Finding a member in one or more zones**

Use this procedure to locate all instances of a member in the Zones list on the Zone Library tab.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Perform one of the following actions based on the selection you made for the Zoning Scope.
   - For FC fabrics, select Display All to show all network objects in your fabric group in the Potential Members list.
For Router fabrics and mSANs, go to step 4.

4. Select the device or port you want to find in the Potential Members list.

5. Click Find > between the Potential Members list and Zones list.
   • If the member is found, all instances of the zone member found are highlighted in the Zones list.
   • If the member is not found, a message displays informing you of this. Click OK to close the message box.

Finding a zone member in the potential member list

Use this procedure to locate a zone member in the Potential Members list on the Zone Library tab.

1. Select Configure > Zoning.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Select the zone member in the Zones list that you want to find in the Potential Member list.

4. Click Find < between the Potential Members list and the Zones list.
   • If the member is found, it is highlighted in the Potential Members list.
   • If the member is not found, a message displays informing you of this. Click OK to close the message box.
   • If there are no ports listed in the Potential Members list, a message displays informing you that additional action is required. Right-click within the list panel and select Port Display from the shortcut menu to display ports.
Finding zones in a zone set

Use this procedure to locate all instances of a zone in the Zone Sets list on the Zone Library tab.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Select the zone you want to find in the Zones list.
4. Click Find > between the Zones list and the Zone Sets list.
   - If the zone is found, all instances of the zone are highlighted in the Zone Sets list.
   - If the zone is not found, a message displays informing you of this. Click OK to close the message box.

Finding a zone set member in the zones list

Use this procedure to locate a zone set member in the Zones list on the Zone Library tab.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Select the zone set member (i.e., the zone) in the Zone Sets list that you want to find in the Zones list.
4. Click Find < between the Zones list and the Zone Sets list.
   - If the zone is found, it is highlighted in the Zones list.
   - If the zone is not found, a message displays informing you of this. Click OK to close the message box.
**Importing a zone set**

Use this procedure to import a zone set (file) into a selected zone library.

When importing a zone set, the set and its zones are compared with all the existing zone sets and zones in the destination library to ensure there are no conflicts. Consequently, the results of the comparison determine whether the zone set is automatically imported or you are prompted to overwrite an existing zone set with the zone set being imported.

The specific items compared are the same as those when an active zone set is saved to a selected zone library. For a list of the items, refer to the procedure “Saving the active zone set to a zone library” on page 286.

1. Select **Configure > Zoning**.
   The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Click **Import**.
   The Import dialog box displays.
4. Browse the Look in field and find the file you want to import.
5. Click **Import**.
   The zone set you want to import is compared to zone sets in the destination zone library. If no zone name or zone ID conflicts are found, the zone set is successfully imported and the Import dialog box closes. However, note the following exceptions:

   - If the destination library contains a zone set that is identical to the one being imported, a message is displayed informing you of this and asking whether you want to proceed. Click Yes to continue and overwrite the existing zone set with the one being imported, or click No to cancel the import operation.
   - If the destination library contains a zone set with the same name as the one being imported but different contents, a message is displayed informing you of this, warning you that
continuing will overwrite the existing zone set, and asking whether you want to proceed. Click Yes to overwrite the existing zone set, or click No to cancel the import operation.

- If the destination library contains a zone set that is identical to the one being imported but with a different name, a message displays informing you of the conflict and asking whether you want to proceed. Click Yes to import the zone set with its name and assign a new name to the existing zone set. The existing zone set in the library will be renamed by appending copy to the name. For example, zonesetFinance would be renamed zonesetFinance_copy. Any subsequent copies would be renamed zonesetFinance_1, zonesetFinance_2, zonesetFinance_3, and so forth. Click No to cancel the import operation.

6. Click OK or Apply to save your changes.

A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.

Listing zone members

Use this procedure to identify the zone to which an individual port belongs and the other zone members in that zone.

Note that the procedure is performed from the main view of the Connectrix Manager application.

1. On the product device list of the Connectrix Manager application, expand the list of products to show the ports.
2. Right-click a port and select **List Zone Members from the shortcut menu**.

   If **List Zone Members** is not included on the shortcut menu, the port cannot be zoned. Keep in mind that only attached device ports can be zoned. If desired, select another port.

   If the port is not a member of a zone, a message displays informing you of this. Click **OK** to close the message.

   If the port is a member of a zone, the **List Zone Members** dialog box displays. The fabric’s nickname, the port’s name, and all zone members display.

3. Click **Close** to exit the **List Zone Members** dialog box.
Removing zone members

The following procedure explains one way to remove one or more members from a zone. For alternative instructions that make use of arrow buttons on the Zone Library tab, refer to “Removing a member from a zone” on page 309.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the name of the zone member you want to remove in the Zones list and select one of the following options from the shortcut menu that displays:

   • Remove — to remove the zone member from the selected zone.
   • Remove All — to remove the zone member from all zones to which it belongs.

   When successful, the zone member is removed from the Zones list. Note that the zone member will no longer appear in the Zone Sets list either.

   However, if the zone member you selected is a routed device, a message displays informing you that such a device must be unexported from the iFCP link before it can be removed from the zone. Click OK to close the message box. Take the appropriate steps to unexport the zone member and then retry this remove procedure.

4. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Removing a zone from a zone set

The following procedure explains one way to remove a zone from a zone set. For alternative instructions that make use of arrow buttons on the Zone Library tab, refer to “Removing a zone from a zone set” on page 310.

1. Select Configure > Zoning.
   
The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the name of the zone you want to remove in the Zone Sets list and select Remove.
   
   When successful, the zone is removed from the Zone Sets list.

   However, if the zone you selected contains routed devices, a message displays informing you that such a zone must be unexported from the iFCP link before it can be removed from the zone set. Click OK to close the message box. Take the appropriate steps to unexport the zone and then retry this remove procedure.

4. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Renaming a zone

Use this procedure to assign a new name to a zone.

1. Select **Configure > Zoning**.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the name of the zone you want to change in the **Zones** list and select **Rename**.

4. Key in the new name for the zone.

   For zone name requirements and limitations, refer to “Zoning naming conventions” on page 295.

5. Press **Enter** to save the new name.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the renaming and consider your options.

6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the Zoning dialog box, or click **Cancel** to stop your exit from the Zoning dialog box.
Renaming a zone set

Use this procedure to assign a new name to a zone set.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Right-click the name of the zone set you want to change in the Zone Sets list and select Rename.
4. Key in the new name for the zone set.
   For zone set name requirements and limitations, refer to “Zoning naming conventions” on page 295.
5. Press Enter to save the new name.
   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click Yes to continue, or No to cancel the renaming and consider your options.
6. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.

Replacing a zone set from history

Because a zone set file is saved every time a zone set is activated, over time it is possible to accumulate a number of versions of a particular zone set. These historical versions can be viewed on a dialog box with the date and time that each one was activated. Furthermore, you can use the following procedure to replace a current version of a zone set with one of the historical versions.
1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the zone set you want to replace in the Zone Sets list and select Replace from History.
   The Replace Zone Set from History dialog box displays with a list of previous versions of the zone set identified by the date and time each version was activated.

   OR

   If the zone set has never been activated before, there are no previous versions to list. Consequently, a message box displays instead of the Replace Zone Set from History dialog box, informing you there is no activation history for the zone set. Click OK to dismiss the message box and return to the Zoning dialog box.

4. Select the zone set you want as the replacement for the current zone set and click OK.
   If the name of the replacement zone set is the same as a zone set in the destination library, a message box displays informing you of the naming conflict and asking whether you want to overwrite the zone set in the destination library.
   - If you select Yes, the zone set is overwritten, the Replace Zone Set from History dialog box is closed, and the Zone Library tab displays.
   - If you select No, the zone set is not overwritten and the Replace Zone Set from History dialog box displays. Click Cancel to close the dialog box and return to the Zone Library tab.

5. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Replac ing zone members

A zone member can be replaced in a specific, selected zone, or, if it is the member of more than one zone, it can be replaced in all the zones to which it belongs.

1. Select Configure > Zoning.
   
The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   
This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Right-click the zone member you want to replace in the Zones list and select one of the following options from the shortcut menu that displays:
   • Replace - to replace the zone member in a selected zone
   • Replace All - to replace all instances of the selected zone member

When you select Replace, the Replace Zone Member dialog box displays. When you select Replace All, the same dialog box displays, but with the title Replace Zone Member (all instances).
4. Select the option from the Method list that you want to use to identify the replacement zone member.
5. Enter the WWN, nickname, domain and port numbers, or fabric address—whichever is appropriate for the method you chose in step 4.

When you choose the WWN method, the Assign Nickname field is available; you may define a nickname for the replacement zone member. If a nickname was previously assigned to the potential member, a message displays informing you of this and asking whether you want to overwrite the existing nickname. Click Yes to continue and assign a new nickname, or No to decline and dismiss the message box.
6. Click **OK**.

   If you have entered more than one port name or zoning method, a message displays informing you of the error. Click **OK** to close the message, correct your entry, and click **OK** again.

   If no entry error was made, the new zone member replaces the old zone member in the **Zones** list and the Replace Zone Member dialog box closes.

7. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the **Zoning** dialog box, or click **Cancel** to stop your exit from the **Zoning** dialog box.
Saving the active zone set to a zone library

You can save a copy of an FC or Router fabric active zone set into a selected zone library. For an mSAN, this procedure will gather all the active zone sets in all the fabrics in the mSAN into a single zone set, and save that zone set to the designated zone library. (If active zone sets in different fabrics of the mSAN have identical names, the zone sets will be renamed in the format <zonelabel>_<fabriclabel>.)

When saving the active zone set, the set and its zones are compared with all the existing zone sets and zones in the destination library to ensure there are no conflicts. Consequently, the results of the comparison determine whether the active zone set is automatically saved or you are prompted to overwrite an existing zone set or rename the zone set being saved.

The specific items compared are as follows:

- For FC fabrics, the name of the active zone set, plus its zones and their contents are compared.
- For Router fabrics, the zone IDs of the zones in the zone set being saved are compared to the IDs of all existing zones, in addition to zone set names and contents being compared.
- For mSANs, the name and the zones and the contents of the zone set being copied are compared to the names and contents of all the active zone sets in all the fabrics of the mSAN.

1. Select Configure > Zoning.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Click the Active Zone Set tab and select the active zone set.

4. Click Save To.

   The Save Active Zone Set As dialog box displays with the current name of the zone set.
5. Key in a new name for the active zone set, if desired, and click OK.

If you click OK without any zone set name in the Save Active Zone Set As dialog box, a message displays prompting you to key in a name. Click OK to close the message box, then key in a name for the zone set and click OK to proceed with the save operation.

6. Click OK to begin the save operation.

The active zone set you want to save is compared to zone sets in the destination zone library. If no zone name or zone ID conflicts are found, the active zone set is successfully saved. However, note the following exceptions:

- If the destination library contains a zone set that is identical to the one being saved, a message is displayed informing you of this and asking whether you want to proceed. Click Yes to continue and overwrite the existing zone set with the one being saved. Or, click No to return to the Save Active Zone Set As dialog box where you can key in a different name for the zone set you are saving.

- If the destination library contains a zone set with the same name as the one being saved but different contents, a message is displayed informing you of this, warning you that continuing will overwrite the existing zone set, and asking whether you want to proceed. Click Detail for a list of differences between the zone sets, click Yes to overwrite the existing zone set, or click No to return to the Save Active Zone Set As dialog box and key in a different name for the zone set.

- If the destination library contains a zone set that is identical to the one being saved but with a different name, a message displays informing you of the conflict and asking whether you want to proceed. Click Yes to save the zone set with its name and assign a new name to the existing zone set. The existing zone set in the library will be renamed by appending copy to the name. For example, zonesetFinance would be renamed zonesetFinance_copy. Any subsequent copies would be renamed zonesetFinance_1, zonesetFinance_2, zonesetFinance_3, and so forth. Click No to cancel the save operation and close the Save Active Zone Set As dialog box.
7. Click **OK** or **Apply** to save your changes.

A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the **Zoning** dialog box, or click **Cancel** to stop your exit from the **Zoning** dialog box.

---

### Searching for a zone member by WWN or nickname

This procedure describes how you conduct the following three kinds of searches:

- Searching for a specific member in the **Potential Members** list.
- Searching for a zone member in a specific zone.
- Searching for all instances of a zone member in all zones.

Regardless of the kind of search, a **Search** dialog box displays and enables you to specify the WWN or nickname of the member.

1. Select **Configure > Zoning**.

   The **Zone Library tab of the Zoning** dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Perform one of the following actions based on the specific nature of your search:

   - In the **Potential Members** list, right-click anywhere in the list box (without clicking a member name) and select **Search** from the shortcut menu. The **Search** dialog box displays.
   - In the **Zones** list, right-click the name of the zone in which you want to search for the zone member and select **Search** from the shortcut menu. The **Search** dialog box displays.
   - In the **Zones** list, right-click anywhere in the list box (without clicking a zone name) and select **Search** from the shortcut menu. The **Search** dialog box displays.

4. Key in the WWN or nickname of the member you want to search for in the field provided on the **Search** dialog box.
5. Click **OK** to begin the search.

   - If the member is found, its name is highlighted in the **Potential Members** or **Zones** list. If you searched for all instances of the member in all zones, each instance is highlighted in the **Zones** list.
   - If the member is not found, a message displays informing you of this. Click **OK** to close the message box.

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

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the **Zoning** dialog box, or click **Cancel** to stop your exit from the **Zoning** dialog box.

---

### Setting the zoning delay

Edit the batch file to set the application to configure zoning. If a response is not received within the amount of time specified here, the application will end the operation and report that it failed. If the flag is not set, the timeout returns to its default setting of 180000ms (180sec).

**Note:** Setting large zone sets through Telnet can take a long time — approximately six seconds for each zone within a zone set.

**Windows**

1. Open the `<Install_Home>/bin/Connectrix ManagerService.ini` file using a text editor (for example, Notepad).
2. Edit the `-Dsmp.zoning.wait.timeout` entry as desired. Be sure to add a space after your entry.
3. Save and close the file.

**UNIX**

1. Open the `<Install_Home>/bin/Connectrix Manager_MgrConnectrixManager` file using a text editor (for example, vi).
2. Edit the `-Dsmp.zoning.wait.timeout` entry as desired. Be sure to add a space after your entry.
3. Save and close the file.
Viewing properties for iFCP links

Use this procedure to view basic information and status for iFCP links.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Right-click the link you want to review in the Zone Sets list and select Properties.
   The iFCP Link Properties dialog box displays.
4. Review the properties information. For descriptions of the fields on the properties dialog box, refer to .
5. Click Close to exit the properties dialog box.
6. Click OK to close the Zoning dialog box.
**Viewing properties for zones and zone sets**

Use this procedure to view basic information and status for zones and zone sets.

1. Select **Configure > Zoning**.
   
   The **Zone Library tab of the Zoning** dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the **Zoning Scope** list.
   
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Right-click the zone in the **Zones** list, or the zone set in the **Zone Sets** list, that you want to review and select **Properties**.
   
   The **Zone Properties** dialog box or the **Zone Set Properties** dialog box displays.

4. Review the properties information. For descriptions of the fields on each properties dialog box, refer to .

5. Click **Close to exit** the properties dialog box.

6. Click **OK** to close the **Zoning** dialog box.
Viewing zoning reports

The zoning feature provides the following three reports:

- Fabric Zone Library Report
  This report outlines the zoning information in a zone library; it can be the library associated with a particular fabric or the Global Library (FC fabrics only). It identifies the zone sets in the library, the zones in the zone sets, and the members in each zone. For each of these items, the report provides a variety of information, such as whether a zone set is active and the number of member zones it has, the properties of both WWN and routed members in a zone, and information about each member’s WWN, name, nickname, and whether the member is currently logged in. (The information in the report varies slightly with the type of fabric selected.)

- Active Zone Set Report
  This report lists the zones in the active zone set, and the members in each zone. For zones in the active zone set, the report gives the minimum and maximum rates of traffic (in MB/sec), the number of members in the zone, and the number of members currently logged in. For each member in the zones, the report provides the same information as the Fabric Zone Library Report. Note that for mSANs, the report reflects that there may be more than one fabric and, consequently, provides information for each active zone set from all fabrics in the mSAN.

- iFCP Connections and Zones Report
  This report identifies the IP addresses of the local and remote routers at the ends of the connection, and the names of any zones under the link. It also gives the status of the connection, its minimum and maximum bandwidth (in MB/sec), and the number of sessions.

Generating the reports

The Fabric Zone Library Report is generated and displayed when you click the Report button on the Zone Library tab of the Zoning dialog box.

The Active Zone Set Report is generated and displayed when you click the Report button on the Active Zone Set tab of the Zoning dialog box.
Note that after you click either of these **Report** buttons, a message displays informing you that any changes made to zones or zone sets will be saved before the report is generated and displayed. Click **OK** to continue or **Cancel** to stop the report generation.

The iFCP Connections and Zones Report is generated by accessing Monitor > Reports > View from the Connectrix Manager application main menu. When the **View Reports** dialog box displays, select the iFCP report in the **All Reports** list.

**Managing the reports**

All three reports are automatically saved and can be viewed again by accessing Monitor > Reports > View from the Connectrix Manager application main menu. By default, a report is displayed in the **Reports** dialog box. However, this dialog box provides a **Show in Browser** button that allows you to change the display to a browser window.

If you want to print a report, click **Show in Browser** to change the display, and use the browser’s print command to print the report.

If you do not want to retain the report, click **Delete Report** on the **Reports** dialog box.

Whether you are viewing the report in the **Reports** dialog box or a browser window, click the red X button in the upper right corner to close the report.
Zoning

Configuring zoning

Zoning defines the communication paths in a fabric. A zone is comprised of a collection of initiator and target ports within the SAN. The ports in a zone can only communicate with other ports in that zone. However, ports can be members of more than one zone.

In order to zone devices in a fabric, the fabric’s principal switch must be an M-Series switch and must be discovered and managed through the application.

Note: The application performs zoning discovery once at startup, and then once every two hours during routine discovery. If the Zoning dialog box is open, zoning discovery will be performed during every polling cycle. It will continue to discover at the increased speed for 30 minutes before it returns to the default value. For best results, wait for five discovery cycles after starting the Server before performing zoning.

Accessing zoning

You can access the Zoning feature from the main screen of the Connectrix Manager application in any of the following ways:

- Select Configure > Zoning.
- Right-click a device (SAN router, switch, or director) or fabric name in the device list and select Zoning from the resulting menu.
- Right-click a device or fabric in the physical map and select Zoning from the resulting menu.

However, if you are also implementing the Virtual Fabrics feature, you may experience a small variation to the last of these methods. When you have virtual switches configured on directors that are discovered through the Connectrix Manager application, the Zoning command will not appear on the shortcut menu when you right-click a physical switch on the physical map, but will appear on the shortcut menu when you right-click a virtual switch on the physical map. Furthermore, you can only add to zones the WWNs for the ports assigned to the virtual switch and for detached ports. You must also enable active zone sets on individual virtual switches.
Zoning limits

Refer to the E/OS release notes for the specific zoning limits relative to a particular E/OS release.

Your Connectrix Manager application imposes a limit of total zone members in a zone set. There are no limits on the number of zones, members per zone, zone sets, and number of end ports that you can configure in the Zoning Library. Limits are imposed by the firmware release and hardware product where this firmware is installed.

During zone set activation, the total number of zone members in each zone and in the zone set are checked against the limits imposed by the firmware and hardware product. If the limits are exceeded, a message is displayed informing you of this. Click OK to close the message box, and take appropriate action to meet the limits.

Zoning naming conventions

The following naming rules apply for zone names and zone set names:

- Names are case insensitive.
- Names cannot begin with “SANav_” or “SMP_”. These prefixes are reserved.
- Names cannot begin with a numeric character.
- Recommended character limit: 60 characters.
- No duplicate names are allowed across the zone libraries or between zones and zone sets.

Administrator zoning privileges

You can set read only or read/write access for the following zoning components:

- Zoning Global Library (FC fabric only)
- Zoning Fabric Libraries
- Zoning Activation (and deactivation)

When read/write privileges are defined for all three components, an administrator can perform all zoning-related operations provided by
dialog boxes and shortcut menus. The following table summarizes the functions permitted for other privilege level settings.

Table 14   Administrator zoning privileges

<table>
<thead>
<tr>
<th>Privilege Level per Zoning Components</th>
<th>Accessible Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read only</td>
<td>Zone Library tab</td>
</tr>
<tr>
<td></td>
<td>• Find</td>
</tr>
<tr>
<td></td>
<td>• Export</td>
</tr>
<tr>
<td></td>
<td>Active Zone Set tab</td>
</tr>
<tr>
<td></td>
<td>• Compare</td>
</tr>
<tr>
<td></td>
<td>Potential Members list shortcut menu</td>
</tr>
<tr>
<td></td>
<td>• All commands</td>
</tr>
<tr>
<td></td>
<td>Zones list shortcut menu</td>
</tr>
<tr>
<td></td>
<td>• Port Label</td>
</tr>
<tr>
<td></td>
<td>• Search</td>
</tr>
<tr>
<td></td>
<td>• Properties</td>
</tr>
<tr>
<td></td>
<td>Zone Sets list shortcut menu</td>
</tr>
<tr>
<td></td>
<td>• Properties</td>
</tr>
<tr>
<td>Read/write</td>
<td>All functions except activating and deactivating the active zone set.</td>
</tr>
<tr>
<td></td>
<td>Global Library</td>
</tr>
<tr>
<td></td>
<td>(FC fabric only)</td>
</tr>
<tr>
<td></td>
<td>Fabric Libraries</td>
</tr>
<tr>
<td></td>
<td>Activation</td>
</tr>
</tbody>
</table>

Note the following items about setting zoning privileges:

- If no privilege level is set for any of the components, zoning is disabled at the Connectrix Manager application main menu and the Zoning dialog box cannot be opened.
- If a privilege level is set for Activation without levels being set for the Global or Fabric Libraries, the Zoning dialog box can be opened, but it will not display the zone library.
- If a privilege level is set for the Global or Fabric Libraries, or for both, without a level being set for Activation, the Zoning dialog box can be opened and the functions outlined in the table for read/write and read only settings for the libraries will be accessible. (Activating and deactivating active zone sets will not be possible.)
To set the privilege levels, in the Connectrix Manager application select SAN > Users. Then select Security Administrator in the Groups list and click Edit. The Features tab of the Connectrix Manager application Group dialog box displays. Select the desired zoning component in the Features list and click the appropriate right arrow to move the component to the Read/Write or Read Only list.

**Configuring zoning**

The application performs zoning discovery once at startup, and then once every two hours during routine discovery. If the Zoning dialog box is open, zoning discovery will be performed during every polling cycle. It will continue to discover at the increased speed for 30 minutes before it returns to the default value. For best results, wait for five discovery cycles after starting the Server before performing zoning.

**Important:** To zone non-Connectrix M products, you must have an Open Fabric license key. This key enables you to discover WWNs connected to non-Connectrix M products and then zone the products. Contact your sales representative to purchase this key.

**Note:** If you are not going to use the default zone, you must enter a password on the Address Properties dialog box to enable zoning.

The following procedure provides an overview of the steps you must perform to configure zoning for the SAN.

Note that for any Zoning-related procedure, changes to a zone library will not be saved unless you click **OK** or **Apply** on the Zoning dialog box. If you click **Cancel** or the close button (X), only changes made to the active zone set will be saved. These changes are saved because they have been activated and saved on the switch.

1. Select **Configure > Zoning**.

   The **Zone Library tab of the Zoning** dialog box displays.

2. Select an FC fabric, Router fabric or mSAN from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Perform one of the following actions based on the selection you made for the Zoning Scope.
   - For FC fabrics, select Display All to show all network objects in your fabric group in the Potential Members list.
   - For Router fabrics and mSANs, go to step 4.
4. Create the desired zones. For specific instructions, refer to “Creating a new zone”.
5. Add members to each zone. For specific instructions, refer to “Adding members to a zone” and “Creating a new member in a zone”.
6. Create a zone set. For specific instructions, refer to “Creating a zone set”.
7. Activate the zone set. For specific instructions, refer to “Activating a zone set” on page 304.
8. Set zoning policies for FC and Router fabrics, if necessary. For specific instructions, refer to “Enabling or disabling the default zone for fabrics” on page 307 and “Enabling or disabling safe zoning mode for fabrics” on page 308.
9. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Creating a new zone

Use this procedure to create a new zone.

1. Select Configure > Zoning.  
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.  
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Click New Zone.  
   A new zone displays in the Zones list.

4. Key in the desired name for the zone.  
   For zone name requirements and limitations, refer to “Zoning naming conventions” on page 295.

5. Click OK or Apply to save your changes.  
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.

Adding members to a zone

Use this procedure to add a member to a zone when the member is listed in the Potential Members list of the Zone Library tab.

For instructions to add a member to a zone when the member is not listed in the Potential Members list, refer to the procedure “Creating a new member in a zone” on page 300.

1. Select Configure > Zoning.  
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.  
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Perform one of the following actions based on the selection you made for the Zoning Scope.
   • For FC fabrics, select Display All to show all network objects in your fabric group in the Potential Members list.
   • For Router fabrics and mSANs, go to step 4.

4. Select one or more zones to which you want to add members in the Zones list. (Press SHIFT or CTRL and click each zone name to select more than one zone.)

5. Select an option from the Method list.
   You can list potential zone members by World Wide Name, Domain/Port, or Fabric Address.

6. Select one or more members to add to the zone in the Potential Members list. (Press SHIFT or CTRL and click each member to select more than one member. To add all ports on a device, select the device.)

7. Click the right arrow between the Potential Members list and Zones list to add the selected member(s) to the zone.
   A message may display informing you that one or some of the selected potential members cannot be zoned. Click OK to close the message box. Reconsider your selections and make corrections as appropriate.

8. Click OK or Apply to save your changes.
   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.

Creating a new member in a zone

Use this procedure to add a member to a zone when the member is not listed in the Potential Members list of the Zone Library tab.

For instructions to add a member to a zone when the member is listed in the Potential Members list, refer to the procedure “Adding members to a zone” on page 299.
1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Select one or more zones to which you want to add members in the Zones list. (Press SHIFT or CTRL and click each zone name to select more than one zone.)

4. Click New Member.
   The Add New Zone Member dialog box displays.

5. Select the option from the Method list that you want to use to create the new member. (WWN is the only possible method for Router fabrics.)

6. Enter the WWN, nickname, domain and port numbers, or fabric address—whichever is appropriate for the method you chose in step 5.
   If you enter a WWN that has been used by a discovered device, a message displays informing you of this and instructing you to enter a port WWN. Click OK to close the message box and key in an appropriate WWN.
   When you choose the WWN method, the Assign Nickname field is available; you may define a nickname for the new member. If a nickname was previously assigned, the nickname appears in the field and a message displays asking whether you want to overwrite the existing name. Click Yes to continue and assign a new nickname, or No to decline and close the message box.

   **Note:** If you add an invalid WWN, domain/port value, fabric address, or device nickname and then activate the zone set, the application may initially indicate that the zone has been configured properly; however, a zoning mismatch message will display on the Zoning dialog box after the next discovery pass.
7. Click **OK** to save your changes and close the **Add New Zone Member** dialog box.

   OR

   Click **Apply** to save your changes and keep the **Add New Zone Member** dialog box open so you can add more new members. Repeat steps 5, 6 and 7 as many times as needed, and proceed to step 8 when appropriate.

8. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the **Zoning** dialog box, or click **Cancel** to stop your exit from the **Zoning** dialog box.

---

**Creating a zone set**

Use this procedure to create a new zone set.

1. Select **Configure > Zoning**.

   The **Zone Library tab of the Zoning** dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Click **New Set**.

   A new set displays in the **Zone Sets** list.

4. Key in the desired name for the zone set.

   For zone name requirements and limitations, refer to “**Zoning naming conventions**” on page 295.

5. Press **Enter**.

   Depending on the characters included in the name you enter, a message may display informing you the name contains characters that are not accepted by some switch vendors, and asking whether you want to proceed. Click **Yes** to continue, or **No** to cancel the zone creation.
6. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.

**Adding zones to zone sets**

Use this procedure to add one or more zones to a zone set.

1. Select Configure > Zoning.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Select one or more zone sets to which you want to add zones in the Zone Sets list. (Press SHIFT or CTRL and click each zone set name to select more than one zone set.)

4. Select one or more zones to add to the zone set(s) in the Zones list. (Press SHIFT or CTRL and click each zone name to select more than one zone.)

5. Click the right arrow between the Zones list and Zone Sets list to add the zone(s) to the zone set(s).

6. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Activating a zone set

When a zone set is active (activated), its members can communicate with one another. Only one zone set can be active at any given time.

When you initiate activation of a zone set, a number of checks are performed on the zone set. These checks are performed before the Activate Zone Set dialog box is displayed, and look for the following problems:

◆ Zone and zone set name violations
◆ Total zone and zone member limit violations
◆ Zoning configuration violations

When a zone set is activated, only the selected zone set’s data is sent to the fabric; zone libraries are never sent to the fabric.

Note: Only one Server should be run at a time (actual servers performing discovery) or log on conflicts may occur. Also, activation speeds may differ depending on the hardware vendor and type of zoning used.

If you do not have access privileges to activate zone sets, the Activate button on the Zone Library tab will be unavailable. You will not be able to activate a zone set unless your access privileges are redefined.

1. Select Configure > Zoning.

The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Select the zone set you want to activate in the Zone Sets list.

4. Click Activate.

The Connectrix Manager application begins performing various checks. Note the following events that may occur:

• For FC fabrics, and depending on the characters included in the name you gave to this zone set, a message may display informing you the name contains characters that are not accepted by some switch vendors and asking whether you
want to proceed. Click **Yes** to continue and proceed to the **Activate Zone Set** dialog box, or click **No** to cancel the activation and consider your naming options.

- For FC fabrics, when the total number of zones and zone members defined exceeds the limit recommended for the system firmware, a warning message displays informing you of this fact and asking whether you want to proceed. Consider carefully whether you want to continue with the zone set activation. The limits are set to ensure stable fabrics; if you proceed, you may undermine the stability of your fabric. Click **Yes** to continue and proceed to the **Activate Zone Set** dialog box, or click **No** to cancel the activation. (You can then click **Cancel** to close the **Activate Zone Set** dialog box, reduce the number of zones or zone members on the Zone Library tab, and then return to this procedure to activate the zone set.

- For Router fabrics and mSANs, a table may display listing configuration violations found in the zone set, such as limits being surpassed, invalid or mismatched zone IDs, or inappropriate attempts at exporting over iFCP links. Click **OK** to close the message box. Such errors halt the activation process; you must correct the configuration violations before you can activate the zone set.

- When the checks find no violations, the **Activate Zone Set** dialog box displays.

5. Review the information in this dialog box and make sure the selected zone set is the one you want to activate. Also, select or clear the **Generate a report** and **Store a Copy** check boxes as desired. For Router fabrics, select or clear the **Save to flash** check box as desired.

6. Click **OK** to activate the zone set.

A message box displays informing you that the zones and zone sets you change will be saved in the zone library and asking whether you want to proceed. Click **Yes** to confirm the activation, or **No** to cancel the activation.

When you click **Yes**, a busy window displays indicating the activation is in progress. A status field informs you whether the activation succeeded or failed. When it succeeds, icons for the active zone set and its zones display green. When it fails, the message includes the reason for the failure.
7. Click **OK** to continue. The **Activate Zone Set** dialog box is closed and the **Zone Library** tab displays.

8. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the **Zoning** dialog box, or click **Cancel** to stop your exit from the **Zoning** dialog box.
Enabling or disabling the default zone for fabrics

Use this procedure to enable or disable the default zone for FC and Router fabrics.

1. Select Configure > Zoning.
   
   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric or Router fabric from the Zoning Scope list.
   
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Click Zoning Policies.
   
   The Zoning Policies dialog box displays.

   **Note:** The format and content of this dialog box vary slightly with the firmware level installed on your switch or director, the target selected in the Zoning Scope list, and whether safe zoning mode is enabled. If safe zoning mode is enabled and you want to enable the default zone, the Default Zone buttons may be unavailable (dimmed) and you may need to disable safe zoning mode before you can enable the default zone.

4. Make sure the appropriate fabric is named on the Zoning Policies dialog box.

5. Perform one of the following actions based on the task you want to complete:
   
   • To enable the default zone, click Enable, and then click OK.
   
   • To disable the default zone, click Disable, and then click OK.

   The Zoning Policies dialog box closes and the Zone Library tab displays.

6. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click OK to continue and close the Zoning dialog box, or click Cancel to stop your exit from the Zoning dialog box.
Enabling or disabling safe zoning mode for fabrics

Use this procedure to enable or disable Safe Zoning Mode for FC and Router fabrics.

1. Select Configure > Zoning.
   The Zone Library tab of the Zoning dialog box displays.
2. Select an FC fabric or Router fabric from the Zoning Scope list.
   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.
3. Click Zoning Policies.
   The Zoning Policies dialog box displays.
   
   Note: The format and content of this dialog box vary slightly with the firmware level installed on your switch or director and the target selected in the Zoning Scope list.

4. Make sure the appropriate fabric is named on the Zoning Policies dialog box.

5. Perform one of the following actions based on the task you want to complete:
   - To enable safe zoning mode, click the Enable check box to add a check mark to the box.
   - To disable safe zoning mode, click the Enable check box to remove the check mark from the box.

6. Click OK to save your changes and close the Zoning Policies dialog box.

   If the default zone is enabled when you attempt to enable safe zoning mode, a message box displays informing you that default zone must be disabled for safe zoning mode to be enabled, and asking whether you want to continue.
   - If you click Yes, the default zone is disabled, safe zoning mode is enabled, the Zoning Policies dialog box closes, and the Zone Library tab displays.
   - If you click No, the default zone is not disabled, safe zoning mode is not enabled, and the Zoning Policies dialog box displays. Click Cancel to close the dialog box and return to the Zone Library tab.
Removing a member from a zone

The following procedure explains one way to remove one or more members from a zone. For alternative instructions that make use of a shortcut menu, refer to “Removing zone members” on page 279.

1. Select Configure > Zoning.

   The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Click the plus sign (+) by the appropriate zone in the Zones list to expand the listing and show the zone’s members.

4. Select one or more members to be removed from the zone. (Press SHIFT or CTRL and click each member name to select more than one member.)

5. Click the left arrow between the Potential Members list and the Zones list to remove the selected member(s) from the zone.

   When successful, the selected member is removed from the Zones list and appears in the Potential Members list. Note that the member is not deleted, only removed from the zone.

   However, if the member you selected is a routed device, a message displays informing you that such a member must be unexported from the iFCP link before it can be removed from the zone. Click OK to close the message box. Take the appropriate steps to unexport the member and then retry this remove procedure.
6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the **Zoning** dialog box, or click **Cancel** to stop your exit from the **Zoning** dialog box.

---

### Removing a zone from a zone set

The following procedure explains one way to remove one or more zones from a zone set. For alternative instructions that make use of a shortcut menu, refer to “Removing a zone from a zone set” on page 280.

1. Select **Configure > Zoning**.

   The **Zone Library tab of the Zoning** dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Click the plus sign (+) by the appropriate zone set in the **Zone Sets** list to expand the listing and show the zone set members.

4. Select one or more zones to be removed from the zone set. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)

5. Click the left arrow between the **Zones** list and the **Zone Sets** list to remove the selected zone(s) from the zone set.

   When successful, the selected zone is removed from the **Zone Set** list and appears in the **Zones** list. Note that the zone is not deleted, only removed from the **zone set**.

   However, if the zone you selected contains routed devices, a message displays informing you that such a zone must be unexported from the iFCP link before it can be removed from the zone set. Click **OK** to close the message box. Take the appropriate steps to unexport the zone and then retry this remove procedure.
Deactivating a zone set

Use this procedure to deactivate the active zone set.

If you do not have access privileges to deactivate zone sets, the Deactivate button on the Zone Library tab will be unavailable. You will not be able to deactivate the zone set unless your access privileges are redefined.

1. Select Configure > Zoning.

The Zone Library tab of the Zoning dialog box displays.

2. Select an FC fabric, Router fabric, or mSAN from the Zoning Scope list.

This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

3. Click Deactivate.

The Deactivate Zone Set dialog box displays.

4. Review the information in this dialog box and make sure you want to deactivate this zone set.

   Note: If you want to fully disable zoning, check the default zone setting. If the default zone is enabled and the active zone set is deactivated, members of the default zone may still be able to communicate with each other. To fully disable zoning, you must also disable the default zone.

5. Click the check boxes at the bottom of the dialog box to generate a report with the deactivation and store a copy of the zone set for possible use later, if desired. If not, proceed to Step 6.

For more information about available reports, refer to “Viewing zoning reports” on page 292. For more information about using stored copies of zone sets, refer to “Replacing a zone set from history” on page 282.
6. Click **OK** to deactivate the zone set.

   If the active zone set has never been saved to the zone library, and if you did not select the **Store a copy** check box in Step 5, a message displays informing you of this fact, warning you that it will be lost on deactivation, and asking whether you want to proceed. Click **Yes** to continue or **No** to cancel the deactivation.

   When the deactivation process is finished, a message displays informing you whether it succeeded or failed. Perform the appropriate action based on the content of the message:

   • When deactivation succeeded, proceed to Step 7.
   • When the deactivation failed, the message includes the reason for the failure. Click **OK** to close the message box and proceed to Step 7.

7. Click **OK** to continue.

   The **Deactivate Zone Set** dialog box is closed and the **Zone Library** tab displays.

   When the deactivation succeeded, the icons for the zone set and its zones no longer display as green.

   When the deactivation failed, the icons for the zone set and its zones still display as green.

8. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone sets you have changed will be saved in the zone library, and warning you to make sure no other user is making changes to the same areas. Click **OK** to continue and close the **Zoning** dialog box, or click **Cancel** to stop your exit from the **Zoning** dialog box.
This chapter includes the following information:

- Monitoring connection utilization ................................................. 314
- Monitoring switch performance .................................................... 316
- Monitoring HBA performance .................................................... 317
- Gathering and viewing performance data ................................ 318
- Monitoring port performance .................................................... 326
- Monitoring latency ................................................................. 328
- Viewing ISL and end-node performance in the Topology .......... 329
- Setting performance thresholds ............................................... 330
Monitoring connection utilization

Note: Monitoring performance requires the Performance Monitoring Feature Key to be purchased and installed into the Connectrix Manager server application.

To display the connection utilization, from the Monitor menu, select View Utilization (or CTRL + U). The application displays the percentage of utilization on the trunks as well as on the utilization legend. To turn utilization off, select View Utilization from the Monitor menu.

In the utilization legend, the color and the length of the lines indicate the bandwidth utilization, as shown in Table 15.

<table>
<thead>
<tr>
<th>Line color</th>
<th>Utilization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red line</td>
<td>80% to 100% utilization</td>
</tr>
<tr>
<td>Orange line</td>
<td>60% to 80% utilization</td>
</tr>
<tr>
<td>Light green line</td>
<td>40% to 60% utilization</td>
</tr>
<tr>
<td>Dark purple line</td>
<td>20% to 40% utilization</td>
</tr>
<tr>
<td>Blue line</td>
<td>0% to 20% utilization</td>
</tr>
<tr>
<td>Gray line</td>
<td>0% utilization</td>
</tr>
</tbody>
</table>
Monitoring connection utilization

**Turning on connection utilization**

To display the connection utilization, select Monitor > View Utilization (or CTRL + U).

**Turning off connection utilization**

To turn utilization off, select Monitor > View Utilization.
Monitoring switch performance

You can monitor a switch’s performance through a performance graph, which displays transmit, receive, and error data from the switch ports to the connected devices. The graphs show persisted data. The graphs can be sorted by the Time Range, Transmit, and Receive data.

Note: Ports are labeled with the first available of these fields: Port #, Nickname, Name, WWPN in the Physical Map (show ports) and Performance Graph dialog box. In other words, even if nicknames are selected, the port number takes precedence.

1. Right-click a switch icon and select Performance Graphs.
2. The Performance Graph screen displays. From the Data drop-down list, select the type of data to display in the performance graph.
3. From the Time Range drop-down list, select the time range to display.
   For example, if you select hourly, the graph dynamically updates. The update period is based on when a performance event is received for the selected switch. A performance event is typically received every discovery cycle. When the event is received, the hourly data is updated and the graph is repainted.
4. To change the height of a row, move the Row Height slider right and left.
   You can adjust the height of all the rows in the table. You can adjust the column size to any value between 50 to 300 pixels. The size values for the columns do not display.
5. Click the Close (X) button to close the window.
Monitoring HBA performance

You can monitor an HBA’s performance through a performance graph, which displays transmit and receive data. The graphs show persisted data. The graphs can be sorted by the Time Range, Transmit, and Receive data.

**Note:** Ports are labeled with the first available of these fields: Port #, Nickname, Name, WWPN in the Physical Map (show ports) and Performance Graph dialog box. In other words, even if nicknames are selected, the port number takes precedence.

1. Right-click an HBA icon in the physical map and select Performance Graphs.

   The Performance Graph screen displays.

2. From the Data list, select the type of data to display in the performance graph.

3. From the Time Range list, select the time range to display.

   For example, if you select hourly, the graph dynamically updates. The update period is based on when a performance event is received for the selected switch. A performance event is typically received every discovery cycle. When the event is received, the hourly data is updated and the graph is repainted.

4. To change the height of a row, move the Row Height slider right and left.

   You can adjust the height of all the rows in the table. You can adjust the column size to any value between 50 and 300 pixels. The size values for the columns do not display.

5. Click the Close (X) button in the upper right corner of the Reports window to close it.
Gathering and viewing performance data

You can collect performance data about your SAN and then export it and distribute the data to others. For more information, refer to “Storing performance data” on page 318 and “Exporting performance data” on page 318.

Note: Performance data export files created using the Performance Data Setup dialog box cannot be imported back into the Connectrix Manager application using the Import dialog box.

Storing performance data

You can specify whether you want the application to store performance information.

1. Select Monitor > Performance > Setup.
   The Performance Data Setup dialog box displays.
2. Select the Store Data check box.
3. Click OK to save the setting and close the Performance Data Setup dialog box.

Exporting performance data

You can export SAN performance data to communicate issues to the support center, capture network status, and archive historical data. You can export performance data to various outputs. You also can export performance data on an as-needed basis (see below) or set up your application to export automatically approximately every 15 minutes. For more information about exporting, refer to the Connectrix Manager User Guide or Connectrix Manager Connectrix Manager Online Help.

Note: Performance data export files created using the Performance Data Setup dialog box cannot be imported back into the Connectrix Manager application using the Import dialog box.

Note: Currently, you can only export to the same versions of the application.
To export performance data as needed, complete the following steps.

1. From the SAN menu, select Export.

   The Export dialog box displays a list of file types that can be exported, along with their sizes (Figure 39).

   ![Export dialog box](image)

   **Figure 39** Export dialog box
Monitoring Performance

Figure 40 Export Dialog Box

2. From the Export To drop-down list, select one of the following options:

   **Note:** Some file types may not be available based on the export destination you selected in the previous step.

To export to both **Disk** and **E-mail** at the same time, complete steps 2 through 6 (as needed) for each option.

**Note:** Connectivity XML cannot be exported to e-mail.

- **DB2.** Exports data to a DB2 database. You must have a DB2 database set up to use this feature.
- **Disk.** Saves the exported files to the disk in <\.
- **E-mail.** Mails the exported files as an e-mail attachment from the application.
- **MySQL.** Exports data to a MySQL database. You must have a MySQL database set up to use this feature.

3. Select the **Performance Data** checkbox.

   Select other types of files to export, if desired.
4. If you want to export performance data for only specific switches, click the **Select Switches** button and select the switches for which you want to export performance data.

5. If you are exporting to disk, skip to step 9. Otherwise, continue to step 6.

6. If you are exporting to **email**, complete the following fields:
   a. Enter the recipient’s email address in the **Mail To** field.
   b. Click **Mail List** to select from a list of email addresses.
   c. Enter your email address in the **From** field.
   d. Enter a subject for the email message in the **Subject** field.
   e. Enter content for the email message **Message** field.

7. If you are exporting to **MySQL**, use the following fields:
   a. Enter the host IP address in the **Host IP** field.
   b. Enter the port name/number in the **Port** field.
   c. Enter the DB driver in the **DB Driver** field. Click Browse to browse to the DB driver.
   d. Enter a user ID in the **User ID** field.
   e. Enter the password in the **Password** field.
   f. (Optional) To save the password, select the **Save Password** check box.
   g. Enter the DB name in the **DB Name** field.
   h. (Optional) To automatically generate a DB name, select the **Auto Generated** check box.

8. If you are exporting to **DB2**, use the following fields and buttons.
   a. Enter the name in the **Instance Name** field.
   b. Enter the DB driver in the **DB Driver** field. Click Browse to browse to the DB driver.
   c. Enter a user ID in the **User ID** field.
   d. Enter the password in the **Password** field.
   e. (Optional) To save the password, select the **Save Password** check box.
   f. Enter the DB name in the **DB Name** field.
Monitoring Performance

9. Click OK to export the files and close the Export dialog box.

10. Click OK at the confirmation window.

Setting up automatic exports

You can configure your application to export performance data automatically to a disk or a database (MySQL or DB2).

Note: Performance data export files created using the Performance Data Setup dialog box cannot be imported back into the Connectrix Manager application using the Import dialog box.

To set up automatic performance data exports, complete the following steps.

1. Select Monitor > Performance > Setup.

   The Performance Data Setup dialog box displays.

2. Select the Store Data check box.

3. Select the High resolution continuous export check box.

4. In the Select Switches table, select the appropriate check boxes for the switches you want to include in the export.

   To select all switches, click Select All. To clear all check boxes, click Select None.

5. From the Export To list, select the export format.

6. If you selected Disk, complete the following steps.

   a. In the File Naming field, enter a file name, then select a naming convention from the drop-down list.

      Note: If you select yymmdhhnns or yymmd+{time in long integer} from the File Naming drop-down list and the system time changes (for example, daylight savings time change), some data may be lost.
Gathering and viewing performance data

Note: If you select 0000n (grow by 1) from the File Naming drop-down list and the naming convention count cycles completely (00001 through 99999), the new 00001 file overwrites the old file.

b. In the Directory field, enter the path to the folder where you want to export the data.

7. If you selected MySQL, complete the following steps.
   a. In the Host IP field, enter the IP address where the MySQL database resides.
   b. In the Port field, enter the port number used to connect to the MySQL database.
   c. In the DB Driver field, enter the location of the database driver.
   d. In the User ID field, enter the User ID for the database.
   e. In the Password field, enter the Password for the database.
   f. Select the Save Password check box to save the database password.
   g. In the DB Name field, enter a name for the database export.
   h. Select the Auto generated check box to have the application generate a name for the database export.

   Note: If the Auto generated check box is cleared without giving a database name, a database name is automatically created.

i. In the Table Name field, enter a name for the export.

8. If you selected DB2, complete the following steps.
   a. In the Instance Name field, enter the DB2 instance name.
   b. In the DB Driver field, enter the location of the database driver.
   c. In the User ID field, enter the User ID for the database.
   d. In the Password field, enter the Password for the database.
   e. Select the Save Password check box to save the database password.
   f. In the DB Name field, enter a name for the database export.
Monitoring Performance

- Select the **Auto generated** check box to have the application generate a name for the database export.

  **NOTE:** If the **Auto generated** check box is cleared without giving a database name, a database name is automatically created.

- In the **Table Name** field, enter a name for the export.

9. Click **OK** to save your changes and close the **Performance Data Setup** dialog box.

---

**Importing performance data**

Performance data may not always be available.

**Note:** Importing or installing performance data may overwrite performance files on the server if the target Server has discovered the same switches as those contained in import file.

**Important:** Importing performance data may overwrite performance files on the Server if the target Server has discovered the same switches as those contained in the imported file.

To import performance data, complete the following steps.

1. Select **SAN > Import**.
   - The **Import** dialog displays.
2. From the Import list, select **SAN File (zip)**.
3. In the **File Name** field, enter or browse to the file you want to import.
4. Select the **Install Performance Data** checkbox.
   - This is only available when importing SAN files.
5. Click **OK**.
6. Click **OK** on the “imported data will replace corresponding data on the server” message.
   - The Client is logged out and the **Connectrix Manager Connectrix Manager 9.1 Log In** dialog box displays. Log back into the application.
**Important**: Turning on discovery replaces the imported data with the discovered data, unless the imported data was user-specified. Only one SAN can be viewed or saved at a time.
Monitoring port performance

You can monitor the performance of individual switch ports in the SAN through a port performance graph. The Performance Graph displays the performance of the switch and any connected devices. It also displays information about transmit and receive performance.

1. Right-click a switch icon and select Performance Graphs.
   
The Port Performance Graph dialog box displays.

2. Select a port row and click the History/Events button, or double-click a port row.
   
The Performance Graph screen displays.

3. Apply graph settings.
   
   • To change the unit of measure for the graph, select an option from the Data drop-down list.
   
   • To change the time range for the graph, select an option from the Time Range drop-down list.
   
   • To display the percentage of utilization over a period of time, select the Histogram Display checkbox.
     
     To change the period of time, slide the Histogram slide-bar to the appropriate times. As you move the slide-bars, the display updates automatically.

4. To view a linear average of the trunk utilization, select the Linear Display checkbox.
   
   The application predicts potential threshold crossings. This function provides a forward-looking trend analysis and is intended to notify the user of resource modeling problems.

5. To configure both high and low usage performance warnings and critical thresholds, select the appropriate Set Event Threshold checkboxes.
   
   If Running Average Display is selected, threshold are only triggered if the running average crosses the threshold.

6. To apply an averaging algorithm to the display, select the Running Average Display checkbox.
   
   This display can be smoothed on a varying percentage of an hour. To change the display, move the slider left or right.
7. (Optional) To apply your changes to all ports on the device, select the **Apply to All Ports** checkbox.

8. Click **OK**.
Monitoring latency

You can monitor a device’s latency, which is the time it takes for data to go from an HBA to a device’s LUN and back to the HBA.

**Note:** In-band discovery is required for this task.

1. Open the Latency Graph dialog box using one of the following methods:
   - On the Physical Map, select an HBA icon, then select Monitor > Performance > Latency Graphs.
   - Right-click an HBA icon and select Latency Graphs from the menu.
   - Right-click an HBA icon and select Show Ports from the menu, then right-click a port and select Latency Graphs from the menu.

   The Latency Graph dialog box displays.

2. Review the device latency.

   The Latency Graph shows the response time for each LUN communicating with the HBA.
   - The LUN Nickname column displays the LUN with which the HBA is communicating.
   - The Graph column displays the graph of the data, over time.
   - The Response column displays the y-axis data values, in microseconds (μs).
   - The Mount Path column is the logical drive letter (e.g., D, E, F,…) that a LUN is associated with on the Host computer.
   - The Storage Nickname column is the Nickname of the storage system containing the LUN.
   - At the bottom of the dialog box, the x-axis displays the label Time (seconds).
   - Current Polling Delay specifies the polling delay which can be edited on the Discover Setup dialog box.
   - Client Server Offset specifies the difference between the Server’s computer time and the Client’s computer time to synchronize them for the real-time performance data.
Viewing ISL and end-node performance in the Topology

You can view the ISL and end-node performance in logical configurations (virtual SANs) on the Topology (Physical Map). The total ISL performance (the combined utilization for all virtual SAN traffic) is shown in each virtual SAN that uses the ISL.

1. Select Monitor > View Utilization (CTRL + U).
2. Observe the percent (%) utilization on terminal nodes and ISLs.


Setting performance thresholds

Through the application, you can configure both high- and low-usage performance warnings and critical thresholds.

**Note:** Discovery must be turned on to view threshold values. Select On from the Discover menu.

1. Right-click a switch icon and select Performance Graphs.
   
   The Performance Graph screen displays the performance of the switch and the devices connected to it. It also displays information about transmit and receive performance.

2. Double-click a port row or select a port row and click the History/Events button.
   
   The Port Performance Graph displays.

3. To configure both high- and low-usage performance warnings and critical thresholds, select the appropriate Set Event Thresholds checkboxes.

4. (Optional) Select the Apply to All Ports checkbox to apply your changes to all ports on the device.

5. Click OK.

**Note:** Switch performance data and thresholds are indexed by their node name. This means if you move a switch from one location to another, it “brings” its performance data and thresholds with it. Additionally, if a threshold is set in one SAN file and the same switch is discovered in a different SAN file, the threshold will be defined in both files.
This chapter includes instructions for creating virtual switches through the Connectrix Manager application.

- Feature description .......................................................... 332
- Virtual switch ports ............................................................ 335
- Virtual fabrics feature and zoning ....................................... 336
- Creating virtual switches — overview ................................. 338
- Virtual switch display and function in the Physical Map ....... 339
- Connecting virtual switches to existing fabrics ................. 342
- Creating a virtual switch .................................................... 343
- Configuring a new virtual switch ....................................... 344
- Assigning ports to virtual switches .................................... 351
- Editing virtual switch parameters ...................................... 353
- Using the right-click menu ................................................ 353
- Removing virtual switches ................................................ 354
- Managing virtual switches ............................................... 355
- Connectrix Manager application ....................................... 355
- Element Manager ............................................................ 360
Virtual Fabrics

Feature description

The virtual fabrics feature allows you to divide Fibre Channel ports belonging to a single fabric into multiple virtual fabrics using the fabric’s existing hardware and physical infrastructure. Each of these fabrics, though virtual, can employ unique fabric services, such as name server and policies, and have unique management access.

Feature benefits

Fabrics created from virtual switches can provide the following benefits:

- Isolation from disruptions or errors that occur on other fabrics. For example, activation of a zone set on one fabric will not affect another fabric. Fabric service failures and events, such as build fabric or reconfigure fabric, are also isolated on each fabric.
- Fabrics interconnected, but with traffic specific to each fabric remaining isolated.
- Different applications isolated on separate fabrics.
- Better use of existing hardware. If one fabric contains many underused ports, these can be quickly and non-disruptively assigned to fabrics requiring additional ports.
- Increased scalability of a single fabric that has limits on the number of domains to multiple fabrics with the same limits.
- Replication of fabric services to multiple virtual fabrics.
- Duplication of fabrics on the same SAN to ensure redundancy in case of fabric failure.
- Isolation of devices to individual fabrics so that user groups are separated.
- More efficiency in moving devices to a new fabric by reassigning ports through the software application and not by physically moving devices.

Creating fabrics

You create fabrics by grouping ports into “virtual switches.” By assigning a 12-bit virtual fabric identifier (VF ID) to the virtual switch, you assign it to a specific fabric. For example, you can assign a unique VF ID to one virtual switch to create a fabric consisting of one switch, or assign the same VF ID to multiple virtual switches to create a fabric consisting of many switches.
A VF ID is a decimal number (such as 1, 2, 3) within the range of valid VF IDs for the partition where the port resides.

This feature is only supported on 256-port Directors. If this Director is partitioned, you can create multiple virtual switches by assigning virtual fabric identifiers to groups of ports on each partition. If not partitioned, you can create multiple virtual switches by assigning virtual fabric identifiers to groups of ports throughout the Director.

**Virtual switches**

A virtual switch can consist of any number of ports on a Director or Director partition that are configured with the same VF ID and operating parameters, such as Preferred Domain ID, Interop Mode, and Domain ID Range. Each virtual switch is assigned a unique world wide name (WWN). You can configure multiple groups of ports on the same Director or partition into multiple virtual switches with unique VF IDs. You assign ports to virtual switches and configure common operating parameters for these switches using the Connectrix Manager application and Element Manager dialog boxes.

Creating virtual switches can be compared to partitioning ports on a Director. In the Director, line module (LIM) cards contain Fibre Channel ports. You “partition” the Director by assigning entire Line Module (LIM) cards to one of up to four partitions. Each partition functions like a separate Director with common Fibre Channel service subsystems. Creating virtual switches is like creating virtual partitions from a single physical Fibre Channel fabric. Each virtual partition functions as a separate fabric with common Fibre Channel services and fabric operating parameters. These fabrics can span across multiple partitions or multiple Directors.

*Table 16* compares partitioning and virtual switches.

<table>
<thead>
<tr>
<th>Partition</th>
<th>Fabrics with Virtual Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>LIM-level granularity.</td>
<td>Port-level granularity.</td>
</tr>
<tr>
<td>Partition ID local to Director.</td>
<td>VF ID sent across the fabric.</td>
</tr>
<tr>
<td>Multiple IP addresses.</td>
<td>Single IP address. One management interface per virtual switch.</td>
</tr>
</tbody>
</table>
Virtual Fabrics

Table 16 Comparing fabrics created from virtual switches and partitions

<table>
<thead>
<tr>
<th>Partition</th>
<th>Fabrics with Virtual Switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operates with firmware code installed in Director where partition is located.</td>
<td>Virtual switches operate with firmware code installed on core switches where virtual switches are located.</td>
</tr>
<tr>
<td>Not upgradable. Maximum of four partitions per Director.</td>
<td>Scalable. Multiple virtual switches per partition. Refer to the Connectrix Manager Release Notes.</td>
</tr>
<tr>
<td>Complete fault and traffic isolation.</td>
<td>No fault isolation (limited ones like adding device in 1 VF doesn't cause problem in other VF) but only traffic isolation</td>
</tr>
</tbody>
</table>

Figure 41 is an illustration of how ports located on multiple partitions can be grouped into multiple virtual switches and then combined into multiple fabrics.

![Figure 41 Directors containing virtual switches](image)

In Figure 41, ports are combined on partitions on each Director into groups labeled 1 through 5. Each group of ports labeled ‘1’ is assigned to VF ID 1. Note that any decimal number could be used as
Virtual switch ports

A port assigned to a virtual switch will inherit the VF ID assigned to that switch. This VF ID may be displayed for virtual switch ports in screens, tables, and dialog boxes in your management application.

Note that you cannot assign a port to more than one virtual switch on a Director or partition at the same time. However, you can always reassign a port to another virtual switch. Or, you can take ports assigned to existing virtual switches on the partition or Director and create a new virtual switch just by grouping the ports under a new VF ID using the Virtual Switches dialog box.
An isolated port is a core switch port that is in the pool of core switch ports not currently assigned to a virtual switch. These ports are disabled and cannot be enabled until assigned to a virtual switch.

**Virtual fabrics feature and zoning**

In zoning, devices attached to Directors and fabric switches are partitioned into restricted-access groups called zones. Devices in the same zone can recognize and communicate with each other through switched port-to-port connections. Devices in separate zones cannot recognize name server or route table information and therefore cannot communicate with each other.

System administrators create zones to control the discovery process of HBAs to increase network security measures, differentiate between operating systems, and prevent data loss or corruption by controlling access between devices (such as servers and data storage units), or between separate user groups (such as engineering or human resources).

Zoning has limitations, however. For example, because zoning is configured throughout the fabric, changes in zoning configuration may disrupt the entire fabric. The Virtual Fabrics feature allows you to divide the existing hardware in an existing fabric into separate fabrics, each with a unique set of Fibre Channel fabric services. Zoning works in harmony with virtual fabrics by applying more security to the separate fabrics that meets the requirements of each fabric.

The following table outlines differences between fabrics created with virtual switches and zones.

<table>
<thead>
<tr>
<th>Fabrics Created from Virtual Switches</th>
<th>Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain individual Fibre Channel route tables, name servers, as well as zoning information and protocol.</td>
<td>Fabric services are not maintained per zone.</td>
</tr>
<tr>
<td>Can contain multiple zones with one zone set active.</td>
<td>Zones are contained within a fabric created by virtual switches and cannot span across this fabric.</td>
</tr>
<tr>
<td>May limit other than Unicast traffic.</td>
<td>Limit unicast traffic only.</td>
</tr>
</tbody>
</table>
**Table 17** Comparing fabrics created from virtual switches and zoning (continued)

<table>
<thead>
<tr>
<th>Fabrics Created from Virtual Switches</th>
<th>Zones</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain zone membership by mapping the VF ID to the port number</td>
<td>Maintain membership by port number or WWN.</td>
</tr>
<tr>
<td>Enforce membership at each E_Port and each source and destination port.</td>
<td>Enforce membership only at source and destination port.</td>
</tr>
</tbody>
</table>
Creating virtual switches — overview

You can create virtual switches through either the Connectrix Manager application or the Director’s Element Manager. Both software components provide a **Virtual Switches** dialog box that you can use to not only create, but also view and maintain, virtual switches in your SAN.

You access the **Virtual Switches** dialog box by selecting **Configure > Virtual Switches**. This dialog box allows you to create virtual switches on all discovered core switches in the SAN and assign them to specific fabrics. The left panel displays a tree structure of all core switches in the SAN discovered in the physical map, and the ports in each switch. Click the “+” to the left of a core switch to display ports on that switch. If a port is assigned to a virtual switch, it is identified by a virtual fabric identification (VF ID) in the VF ID column. Note that the name of the core switch at the top of the tree identifies the “physical” switch in the Core Switch Group on the Physical Map.

The right panel displays a tree structure of all configured virtual switches arranged under SAN fabrics where they are assigned. Click the “+” next to a fabric to display virtual switches. Click the “+” next to a virtual switch to display ports assigned to that switch. Note that the VF ID for assigned ports matches the number in parenthesis following the fabric name at the top of the tree.

This table is populated by selecting the destination fabric in the right panel, selecting ports in the left panel, and selecting the right arrow button to move the ports to selected fabrics.

You access the Element Manager **Virtual Switches** dialog box by right-clicking the core switch on the Physical Map and selecting **Virtual Switches**. This dialog box allows you to create virtual switches on specific core switches and assign them to specific fabrics. The left panel displays a table of information on the ports available in the core switch represented by the Element Manager. The right panel displays a table of configured virtual switches and the numbered ports assigned to these switches. This table is populated by selecting the destination virtual switch in the right panel, selecting ports in the left panel, then selecting the right arrow button to move the ports under selected virtual switches.
Virtual Fabrics

**Fabric template**

Each virtual switch in a fabric will inherit fabric, domain, and other parameters from the fabric’s principal core switch. If the core switch does not support virtual switches, parameters are inherited from the default virtual switch on the first core switch discovered that does support virtual switches.

When you configure a new virtual switch using the Virtual Switches Operating Parameters dialog box and assign a unique VF ID to the switch, you are in effect, creating a template of fabric and domain parameters for subsequent virtual switches that get the same VF ID. Each time that you create a switch with a unique VF ID, a fabric line and icon will be added to the Virtual Switches tree on the right side of the Virtual Switches dialog box. Each virtual switch created with the same VF ID will display under this fabric line.

The following parameters are inherited from the fabric template:

- Switch priority
- Interop mode
- ISL cost
- Domain ID range
- Preferred domain ID, insistent domain ID
- Domain and zoning RSCNs
- Node port virtualization enablement
- Default zone enablement

**Virtual switch display and function in the Physical Map**

When a Director or partition is first discovered and no one has created virtual switches, the Director displays in the Connectrix Manager application’s Physical Map as the icon in . The icon is labeled as `partition0` (administration partition) or the name configured for the partition. Note that if Director properties are not
configured, the same icon displays with an *undefined* label, instead of *partition0*.

When you create a new virtual switch and assign it a VF ID other than 1, the Physical Map appears as in *Figure 42*.

---

**Note:** A default virtual switch with VF ID of 1 always exists on the Director. You cannot remove this virtual switch. It contains all ports on the core switch that are not assigned to other virtual switches.
Note the following characteristics of the Physical Map when you create the first virtual switch for the Director or partition with a VF ID other than 1:

- A Director icon appears inside a colored rectangle labeled **Core Switch Group**. This group contains all core switches where virtual switches are created. The icon is labeled *partition0* or the name configured for the partition.

- Two Director icons with a “V” (virtual) badge appear inside a colored rectangles. These icons will be labeled with the names configured for the virtual switches.

- Two director icons with a “V” (virtual) badge appear inside colored rectangles.
  - One icon represents the new virtual switch created with a VF ID other than 1.
  - One icon represents the default virtual switch (with VF ID of 1) that contains all ports not yet assigned to virtual switches.

The **All Ports** list (left panel of the window) lists and identifies the discovered virtual switches and their assigned ports under the appropriate fabric icon. Core switches, from where the ports are assigned to virtual switches, are listed under the Core Switch Group icon. Clicking on a switch or fabric in the All Ports list highlights the corresponding switch or fabric in the Physical Map.
Connecting virtual switches to existing fabrics

Note that connecting a virtual switch port to a fabric through an ISL connection is the same as connecting a Director port to a fabric. You must coordinate fabric, domain, zoning, and other parameters configured on the switch with parameters set on other fabric elements.

Configuring virtual switches through the Virtual Switches and Virtual Switches Operating Parameters dialog boxes in the Connectrix Manager application, rather than through the Element Manager, is the preferred method for configuring virtual switches when you are merging them into existing fabrics. This is because new virtual switches “inherit” fabric, domain, and other parameters from the fabric template established for the initial virtual switch configured in the fabric. This helps ensure that the new virtual switch can merge without fabric segmentation or other problems. For details on the fabric template and parameters that are inherited, refer to “Fabric template” on page 339.
Creating a virtual switch

You can configure virtual switches through your Connectrix Manager application or your hardware product’s Element Manager application. When you want to configure virtual switches on multiple Directors, use the Connectrix Manager application, and when you want to configure virtual switches on one Director, use the Element Manager.

A virtual switch is a group of ports on a core switch that is configured with a common virtual fabric identification (VF ID) and common operating parameters (such as Preferred Domain ID, Interop Mode, and Domain ID Range). Each virtual switch has a unique worldwide name (WWN).

Several virtual switches can be configured on a single partition, each with a unique VF ID. A virtual switch with the same VF ID can be configured on different partitions on a single Director and on partitions on multiple Directors to form a single fabric. These virtual switches can be configured with common operating parameters or with unique operating parameters as desired.

All Directors are shipped with one virtual switch configured with VF ID=1. This virtual switch includes all ports on the Director. This allows the Director to participate in a standard fabric with no additional configuration. Only configure virtual switches when defining switches for multiple fabrics on the Director or partition.
Configuring a new virtual switch

Use this procedure to create a template for the virtual switches using the Virtual Switches and Virtual Switch Parameters dialog boxes, then assign ports to the template to create virtual switches.

If you want to assign ports to an existing virtual switch, follow steps under

1. Select Configure > Virtual Switches.

2. Click New Fabric.

   The Virtual Switches dialog box displays.

   Figure 43

   The Virtual Switches dialog box displays.

   Parameters entered into the Virtual Switches Operating Parameters dialog box provide a “template” for other virtual switches. Multiple virtual switches created in different core switches will “inherit” these parameters to ensure consistent fabric-level parameters.

   The Edit version of this dialog box is exactly the same as the New version, except that the VF ID field cannot be edited. You can only change this value by creating a new fabric and assigning all ports to the new fabric’s VF ID.

   Configuring these parameters requires that the switch be taken offline. After configuring these parameters and selecting OK in the dialog box, a dialog box will prompt you to set the switch offline.

   Some options in this dialog box may not be available if they require configuration through the Element Manager. Reasons for unavailability are explained in tool-tip messages.

3. VF ID — Enter a unique virtual fabric identification (VF ID) number for the fabric within the range of valid VF IDs allowed. This, in effect, creates a new fabric.

   Note: This field is not available if you selected the Edit button on the Virtual Switches dialog box.
4. **VS Name** — Enter a short (maximum 64 characters), descriptive name for the virtual switch. This is a name for the switch stored in the Director.

5. **RA TOV and ED TOV.** Resource Allocation Time Out Value and Error Detect Time Out Value — These values can only be set through an Element Manager opened from core switch icon in the Core Switch Group.

6. **Switch Priority** — Select Principal (highest priority), Default, or Never Principal (lowest priority) from drop-down list. Setting these priority values determines the principal switch selected for the multiswitch fabric.
   - If three virtual switches are in the fabric and one is set as Principal, one as Default, and one is Never Principal, the switch set to Principal becomes the principal switch in the fabric.
   - If each switch is set to Principal or Default, the switch with the highest priority becomes the principal switch.
   - Note that at least one switch in a fabric needs to be set as Principal or Default. If each switch is set to Never Principal, all of the interswitch links (ISLs) will segment. If all but one switch is set to Never Principal and the switch that was principal goes offline, then all of the other ISLs will segment.

7. **Interop Mode** — Select an interop mode as follows:
   - Open Fabric 1.0. This is the default mode. Select this mode if the fabric contains McDATA or EMC switches and Directors, as well as other open-fabric compliant switches. Select this mode for managing heterogeneous fabrics.
   - McDATA Fabric 1.0. Select this mode if the fabric contains only McDATA or EMC Switches and Directors that are operating in McDATA Fabric 1.0 mode.

8. **ISL Cost** — Select By Port Speed or Ignore Port Speed.

Fabric shortest path first (FSPF) uses a cost metric to determine interswitch paths used in a fabric to route traffic. By default, the firmware assigns a cost of 1000 to 1 Gbps and 2 Gbps ISLs (interswitch links) and 100 to 10 Gbps ISLs. The formula for determining the cost is based on the speed of the ISL, as specified by FC-SW-2. Since FSPF uses only minimum cost paths to route interswitch traffic, these default costs mean that if a user adds a
10 Gbps ISL in parallel with an existing 2 Gbps ISL, the switch will use only the 10 Gbps ISL because the 10G ISL is the minimum cost path between the switches. To allow users to upgrade to higher speed ISLs, all ISLs can be assigned an equal cost so both ISLs are used, but more traffic goes to the 10 Gbps ISL.

**Note:** Set the switch offline to change the ISL cost.

- **By Port Speed** - Select if you want FSFP routing selection to account for port speed when assigning traffic to ISLs. Traffic skews to the higher speed ISL until it is at or near capacity, then it routes some traffic to the lower speed ISL.

9. **Ignore Port Speed** - Select if you want FSFP routing selection to not account for port speed when assigning traffic to ISLs. All ISLs will have equal cost. Set the Domain tab. Set the Domain ID Range.

The domain identification (Domain ID) number is a unique identification for the switch in a fabric. A distinct ID is automatically allocated to each switch in the fabric by the principal switch. A switch cannot contain the same domain ID as another switch or their E_Ports will segment when they try to join as a fabric. The Domain ID Range options allow you to configure or expand the range of possible domain IDs in a fabric from the legacy range of 96-127 IDs.

You can configure one of three modes:

- **239 Domain ID** — Selecting 239 Domain ID Range, allows a Domain ID range from 1 to 239. This mode has no offset. If the switch does not support 239 domain IDs, this option does not display. This setting may not be compatible with switches that do not support this range or are not configured for 239 Domain ID.

- **Domain ID Offset** — Selecting the Domain ID Offset option and value from the drop-down list, allows you to configure the domain offset values. Domain IDs minus the offset are still in the 1-31 range. Values available in the drop-down list are 0, 32, 64, 96 (default), 128, 160, and 192.

**Note:** This option is not compatible with Switches or Directors using 239 Domain ID or Legacy Domain ID modes.
• **Legacy Domain ID** — Selecting the default value (96) from the Domain Offset drop-down list, sets the Domain ID range at 96-127. This also makes the switch compatible with switches using earlier firmware versions.

**Important Notes:**

• The switch must be offline to change these options. If it is not, when you click **OK** on the tab to change the options, a dialog box displays prompting you to set the unit offline immediately. You can also select an option in the dialog box to set the switch back online after configuration changes are made.

  **Note:** Setting the switch offline terminates all Fibre Channel connections.

• All switches in a fabric must be have the same setting for the domain ID range.

10. Set the Preferred Domain ID.

Use this field to set a unique domain ID for the virtual switch. The default value is 1. Set a value between 1 and 31. When the switch comes online with a preferred ID, it requests an ID from the fabric’s principal switch (indicating its preferred value as part of the request). If the requested domain ID is not allocated to the fabric, the domain ID is assigned to the requesting switch. If the requested domain ID is already allocated, an unused domain ID is assigned.

The preferred domain ID must be unique for each virtual switch in a fabric. If two switches have the same preferred domain ID and Insistent Domain ID is enabled, the E_Ports segment, causing the fabric to segment.

  **Note:** The switch must be offline to change some of these options. If it is not, when you click **OK** on the tab to change the options, a dialog box displays prompting you to set the unit offline immediately. You can also select an option in the dialog box to set the switch back online after configuration changes are made. Setting the switch offline terminates all Fibre Channel connections.

11. Enable or disable Domain RSCN:
If enabled, domain register for state change notifications (domain RSCNs) are sent between end devices in a fabric to provide additional connection information to host bus adapters (HBA) and storage devices. As an example, this information might be that a logical path has been broken because of a physical event, such as a fiber optic cable being disconnected from a port. Consult with your HBA and storage device vendor to determine if enabling Domain RSCNs will cause problems with your HBA or storage products. For example, some HBAs may log out and then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic.

**Note:** Enabling Domain RSCNs is required if Enterprise Fabric Mode (optional SANtegrity Binding feature) is enabled.

12. Select Zoning RSCNs options.

Fabric format domain RSCNs are sent to switch ports following any change to the fabric’s active zone set. These changes include activating and deactivating the zone set, or enabling and disabling the default zone. When a device receives an RSCN, this can disrupt normal activity because the device must then determine status of other devices. RSCNs can also cause some devices to write messages to error logs.

- **Suppress on zone set activations** — When enabled, fabric format RSCNs are not sent for zone changes to the attached devices on the switch. This option, in most cases, should be enabled so that attached devices can receive notification of zoning changes in the fabric. However, some HBAs may log out and then log back into the fabric when they receive an RSCN, thereby disrupting Fibre Channel traffic.

- **Isolate on zone set activations** — When enabled, only devices that require RSCN notification for a zoning configuration change receive RSCNs. Note that this option does not need to be enabled if Suppress on zone set activations is enabled, since RSCNs will not be sent to attached devices.

13. Node Port Virtualization

This feature allows you to assign multiple Fibre Channel addresses to a single N_Port. Enable this feature mainly for systems that support multiple images behind a single node port.
Note that this check box does not display for a Director that is not at the correct firmware level. If a user activates the Node Port Identification Virtualization (NPIV) feature and the Director is at the correct firmware level, but the feature key is not installed, then an error message displays.

Multiple NPIVs on a single N_Port are sometimes referred to as virtual N_Ports, or virtual ports. Virtual N_Ports can perform the same functions as a traditional N_Port, but may be subject to switch resource limitations and performance issues.

The permanent name for the virtual port is the world wide port name (WWPN) of the device that initiates a fabric login (FLOGI) to the virtual port. Because each virtual N_Port has a unique WWPN, it can be zoned through WWN zoning.

The first device to log into a port initiates a FLOGI and subsequent login requests use the FDISC command. FDISC is an extended link service command sent from an attached device to request an additional port identification. The N_Port that originally sent the FLOGI may log out, using the LOGO command, without affecting operation of other N_Ports on the physical port. The F_Port associated with these requests remains active until a link-resetting event occurs or all of the N_Ports log out. Thus, logout of any single virtual N_Port does not deactivate the link as long as at least virtual N_Port is present.

**Constraints**

- Loop ports (FL_Ports) cannot participate in NPIV.
- Interswitch links (via E_Ports) cannot participate in NPIV.
- Authentication resources are scaled to support at least one N_Port authentication, but not necessarily subsequent N_Ports.
- Port binding and switch binding lists can also support one N_port per physical port but not subsequent N_ports.

**Note:** Modify **Rerouting Delay** through the Element Manager **Operating Parameters** dialog box when accessing the Element Manager from the switch icon in the Core Switch Group. Note that you cannot change this value when accessing the Element Manager through the virtual switch icon.

14. Click **OK** to save all parameter values and close the dialog box.
The Virtual Switches dialog box displays. If this is the initial virtual switch that you have assigned to a VF ID, a new fabric branch based on the new VF ID is included in the Virtual Switches table. It will display as [New] VS name (VF ID). For example: [New] vs156 (2).

**Note:** If you do not specify a name for the virtual switch in the operating parameters dialog box or if the switch branch is automatically created, the virtual switch name is provided from the name of the fabric where the switch is located.

15. Assign ports to the new virtual switch through the Virtual Switches dialog box. Follow steps under “Assigning ports to virtual switches” on page 351.
Assigning ports to virtual switches

Use these steps to assign ports to new or existing virtual switches.

1. Select a port in the All Ports panel of the Virtual Switches dialog box. You may select a range of ports by pressing down the Shift or CTRL key while using the left mouse button to select the ports.

2. Select a virtual switch in the right panel.

3. Click the right arrow button.

4. The port moves from the left to the right panel, and is positioned following the virtual switch.

   A message similar to the following may display if you are reassigning a port from an existing virtual switch.

   Moving ports to the selected virtual switch removes these ports from their original virtual switch.

   Select OK to confirm the move. Select the Don’t show me this again check box to not display this message in the future when assigning ports.

5. Click OK on the Virtual Switches dialog box.

Assigning ports to a new virtual switch

When you assign ports to a new virtual switch and click OK on the Virtual Switches dialog box, a message box displays to explain that creating a virtual switch is similar to introducing new hardware to the network. It provides a list of core switch options that may not be carried forward to the virtual switch with desired values. Note that you might need to configure these options through the new virtual switches Element Manager and your Connectrix Manager application to meet network requirements. Select OK on this dialog box to continue creating the switch.

After you assign ports the a new virtual switch, an icon for the virtual switch displays in the Virtual Switches table in the Virtual Switches dialog box and assigned ports display under the switch icon. An icon for the virtual switch also displays in the Physical Map of your Connectrix Manager application.
Note: If this is the first virtual switch that you have defined other than the default virtual switch, a virtual switch icon will display for both the new switch and the default virtual switch.

Important notes for assigning ports

Remember this information when assigning ports to virtual switches.

- If you select a port to assign to a switch, then select a destination virtual switch that is located on a core switch different from where the port resides, clicking the right-arrow button will place the port in the virtual switch that is created on the same core switch where the port resides.

- For example, if you try to move port 32 from a core switch “PDirector 2” to virtual switch “VSwitch3” under the fabric “Payroll (2),” but VSwitch3 is created from ports on core switch “PDirector 1,” port 32 will be placed under “VSwitch4,” which was created from ports located on PDirector2. If a virtual switch has not been created in the fabric from PDirector2, a new virtual switch is created using the parameters from the fabric.

- When you assign a port to a virtual switch, the maximum number of virtual fabrics for the core switch is verified and an error message displays if this number is exceeded.

- If you try to select more than one fabric in the Virtual Switches table, then assign a port to these fabrics, the right-arrow button disables.

- If you try to reassign ports from the same core switch to two different fabrics with the same VF ID, an error message displays. The action is not allowed.

- You can reassign ports from one virtual switch to another, regardless of their current assignment. Just select the ports to be reassigned from the ports list, select the new destination virtual switch in the Virtual Switches table, then click the right arrow button to move the ports under the new switch.

- If you reassign all ports from a virtual switch, the switch is deleted from the Virtual Switches table when you click OK on the Virtual Switches dialog box.
When you create a new virtual switch, the maximum number of virtual switches for the core switch is verified and an error message displays if this number is exceeded.

If you try to reassign ports from the same core switch to two different fabrics with the same VF ID, an error message displays. The action is not allowed.

**Editing virtual switch parameters**

Use these steps to edit operating parameters for an existing virtual switch.

1. Select **Configure >Virtual Switches**. The **Virtual Switches** dialog box displays.
2. Select the switch that you want to edit in the **Virtual Switches** table.
3. Click **Edit**. The **Edit Virtual Switches Operating Parameters** dialog box displays. This dialog box is the same as the dialog box displayed when you select the **New Fabric** button, except that you cannot edit the virtual fabric identification (VF ID).
4. Use steps under “Configuring a new virtual switch” on page 344 to modify any parameters except the VF ID.
5. Click **OK** when finished.

Parameters are changed for the switch.

**Using the right-click menu**

Right click on a virtual switch in the **Virtual Switches** dialog box to display a menu with the following options:

- **Expand All** — Expands all ports under all virtual switches.
- **Collapse All** — Collapses all ports under virtual switches so that only the virtual switches (top-level) display.
- **Delete** — Sets the VF ID for all ports assigned to the virtual switch as “Isolated” and removes the virtual switch from the **Virtual Switches** table. Note that the virtual switch for VF ID 1 cannot be deleted.
Removing virtual switches

There are two methods for removing virtual switch configurations. You can reassign all ports from the virtual switch to other virtual switches or you can use the Delete option from the virtual switch’s right-click menu.

**Note:** You cannot delete the virtual switch with a VF ID = 1.

**Method 1: Reassign Ports**

1. Select **Configure > Virtual Switches** to display the **Virtual Switches** dialog box.
2. Determine which ports are assigned to the virtual switch by expanding the list of ports for the switch in the **Virtual Switches** table.
3. Select ports assigned to the switch in the **All Ports** list.
4. Select virtual switches in the **Virtual Switches** table where you want to assign these ports.
5. Click the arrow key to reassign the ports.
6. When the message displays warning you that moving ports from the selected switch removes ports from the original virtual switch, click **OK**.
7. Click **OK** on the **Virtual Switches** dialog box.
   The following message displays:
   
   *The following virtual switch definitions have no ports assigned. Continuing will remove the virtual switch definitions.*

8. Click **OK**.
   The virtual switch is removed from the **Virtual Switches** table in the **Virtual Switches** dialog box. In addition, the icon for the virtual switch is removed from the physical map in your Connectrix Manager application.

**Note:** If you remove all switches except the default virtual switch with VS ID of 1, only the Core Switch icon appears in the Physical Map. You cannot remove the default virtual switch.
Method 2: Delete Option on Popup Menu

Note: Using this method, the VF IDs for any ports still assigned to the virtual switch will be set to “Isolated.” These isolated ports, if not reassigned, are maintained offline and cannot log into attached devices.

1. Right click on a virtual switch in the Virtual Switches table of the Virtual Switches dialog box and select Delete.

   A dialog box displays warning that all of the ports on the virtual switch will become isolated and that the Element Manager for the switch will be closed.

2. Click Yes to continue.

   The switch is removed from the Virtual Switches dialog box and the Physical Map in your Connectrix Manager application. All ports that were assigned to the switch will be isolated.

Managing virtual switches

Virtual switches are managed through the Connectrix Manager application and the Director’s Element Manager application. Be aware that when virtual switches are configured, various management tasks and features in these applications are affected. For example, indicators such as a ‘v’ enclosed by a small circle may be added to window elements to indicate that they relate to virtual switches. Also, options in various menus and dialog boxes may be greyed out and unavailable, depending upon virtual switch configuration, your access rights, and how you opened the management application. Position the mouse cursor over unavailable items to view messages about why the option is not available.

This chapter explains how management functions and features are affected in your Connectrix Manager application and the Element Manager applications so that you can be aware of them when managing switches at the physical and virtual level.

Connectrix Manager application

This provides information about how to use the Connectrix Manager application to manage virtual switches. Specifically, it describes the variations you will see in Connectrix Manager Connectrix Manager menus, dialog boxes, and features when virtual switches are...
configured. (Figure 1 on page 37 in Chapter 1 illustrates the Connectrix Manager main application window with virtual switches.)

This section describes variations in Connectrix Manager feature, dialog box, and menu functions when virtual switches are configured in the SAN.

---

**Note:** This information only applies if virtual switches are configured on Directors discovered through your Connectrix Manager application.

When virtual switches are configured on fabric directors, the virtual switches, in addition to the core switches, display in the Select Switches tab. The virtual switches can be selected for any Group Manager function, but not all functions are applicable to virtual switches. Note the following differences:

- **Install E/OS firmware** – Firmware can only be installed on a core switch. If you include virtual switches in the group, they will not be sent the firmware upgrade.

- **Run data collection** – Data collections are done for both core and virtual switches. Data collected for a core switch contains parameters for the core switch and all virtual switches configured in the switch. Data collected for a virtual switch contains data for the core switch where the virtual switch is configured and data for the virtual switch. If multiple virtual switches on the same core switch are included in the group, duplicate data is collected. Therefore, you should include either the core switch in the group or one virtual switch to represent the core switch.

---

**Note:** This information only applies if virtual switches are configured on Directors discovered through your Connectrix Manager application.

Review these notes when setting port fencing thresholds and virtual switches are configured.

- You cannot set a threshold on a fabric that contains a virtual switch and that threshold has not been configured on the core switch where the virtual switch is located.

- You cannot set a threshold on a core switch when same threshold has not been set on fabrics where one or more of virtual switches reside that are on the core switch.
Virtual Fabrics

- You cannot set a threshold on a core switch when the threshold is different than assigned to one or more virtual switches on that core switch.
- You can directly assign thresholds to ports on a virtual switch. To assign a threshold to the virtual switch or its port types, you must assign the threshold to the associated core switch or to another object above it in the hierarchy. If no thresholds are set above the virtual switch in the hierarchy, the ISL Protocol, Link, or Security Threshold field in the Ports table displays a Limited Fencing Support message.

**Dialog box function when virtual switches are configured**

Both core and virtual switches display in the Port Fencing dialog box. You can only assign thresholds for Port Fencing to the core switches; virtual switches inherit port fencing configuration from the core switch. If thresholds are configured on a core switch, the thresholds apply to all virtual switches configured for the core switch.

- Both core and virtual switches display in the Port Fencing dialog box. You can only assign thresholds to the core switches; virtual switches inherit port fencing configuration from the core switch. If thresholds are configured on a core switch, the thresholds apply to all virtual switches configured for the core switch.
- Physical fabrics, directors, switches, port types, and ports display in the Port Fencing dialog box when you have the privileges to manage that object. These objects are indicated by the standard product icons.
- Using Port Fencing, you can directly assign a threshold to any of these physical objects. If a switch does not support Port Fencing, the Threshold field in the Ports table displays a Port Fencing Not Supported message.
- Virtual switches display when you have privileges to manage the fabric that contains the virtual switch and are indicated by the virtual icon ('v' enclosed by circle).
- The core switch displays when you have privileges to manage the core switch.

If you enable Enterprise Fabric Mode, the Rerouting Delay parameter is disabled. Note that since rerouting delay is a core switch parameter, multiple fabrics containing virtual switches configured in the same core switch may be affected. We recommend that the Rerouting Delay parameter be identical on all fabrics in the SAN.
The Port tab of the Properties dialog box contains a virtual fabric identifier (VF ID) field for each port. If the Director supports virtual switches, this will be the VF ID of the virtual switch where the port is assigned. Note that if you select a virtual switch, only those ports assigned to the switch display in the Port tab. If you select a core switch, all ports display.

**Note:** This information only applies if virtual switches are configured on Directors discovered through your Connectrix Manager application.

The Fabrics list displays fabrics and core switches. Select a fabric in this panel to display all fabric switches in the Product Configuration table. Virtual switches, highlighted with a “V” icon, and core switches that do not contain virtual switches both display in the table.

Selecting the Core Switch Group entry in the Fabrics list to display available core switches discovered by the Connectrix Manager application. Core switches are the “physical” Director or partition where the virtual switches are configured. Be aware that actions performed on a core switch may affect multiple virtual switches.

If you select a virtual switch in the Product Configuration table, only those Security tabs are available that contain configuration parameters allowed for virtual switches. Options and display on available tabs are modified for virtual switches.

- On the Devices tab, ports that display in the Port Authentication List table are those assigned to the virtual switch. A VF ID column displays the virtual fabric identifier for the virtual fabric where the port is assigned. If you select a core switch in the Product Configuration panel, options are not available on the Devices tab, such as Edit Secret, Enable E_Port Authentication, and Enable N_Port Authentication.

- On the Software tab, OSMS options are only available if a virtual switch is selected. The remaining options (Enable Authentication, Method, Include Current Server, and Permitted Software, are only available if a core switch is selected.

The fabric Properties dialog box includes a virtual fabric identifier (VF ID) field to identify the fabric. If the Switch or Director does not support virtual switches, the field will be blank.

The **Group** dialog box of the Connectrix Manager application includes **Virtual Fabrics** in the list of features for which read/write
permissions can be specified. Access SAN > Users > Add (under the Groups panel) to access the Group dialog box and set permissions for the Virtual Fabrics feature to read/write or read-only for a group of users.

**Note:** This information only applies if virtual switches are configured on Directors discovered through your Connectrix Manager application.

If virtual switches are configured for a Director, the Zoning option is not available when you right-click a core switch in the physical map. Zoning is available on the right-click menu for a virtual switch, however. Since zoning is configured and active zone sets are stored on individual fabrics, you must enable active zone sets on individual virtual switches. You can only add WWNs to zones for the ports assigned to the virtual switch. You can also add a detached port’s WWN to a zone.
Virtual Fabrics

**Element Manager**

This section provides information about how to use the Element Manager application to manage virtual switches. Generally, virtual switch versus core switch management depends on how you open the Element Manager from the Connectrix Manager application Physical Map.

However, variations in Element Manager functions and features can also depend on the following conditions:

- Whether the product supports or does not support virtual switches.
- Whether you have configured virtual switches on a product that supports them.
- Whether the switch or its ports are offline vs. online.

To manage the physical Director and partitions, you must open the Element Manager through the core switch icon in the Core Switch Group. You can access all ports, configure all standard options, and perform any task as you would for any physical Director. You cannot perform tasks that affect virtual switch function in a fabric.

*Note:* Performing actions through the core switch Element Manager may disrupt virtual switch operations. Make sure that you coordinate configuration changes and other actions with virtual switch administrators.

In contrast, when you open the Element Manager through a virtual switch icon in the Physical Map, you can only access virtual switch ports and configuration options relating to the virtual switch’s operation in the fabric. You cannot perform tasks that disrupt the core switch. For example, you cannot load firmware to the firmware library, change partitioning, and configure ports not assigned to the virtual switch.

When you display the Director graphic in the Hardware tab through an Element Manager opened from a virtual switch icon, ports on the line module are dimmed if they do not belong to the virtual switch that you have selected. If all ports on a line module belong to another virtual switch, the entire line module is dimmed. Ports are also dimmed in the Line Module or Line Module Quad window.

To access port properties, configuration, and other port functions for these ports you must open the Element Manager for the virtual
switch where the ports are assigned. Access to line module properties is always available, however. When you open an Element Manager from the core switch icon in the Core Switch Group, functions for all installed ports are available.

Offline and online state function and display behave differently when virtual switches are configured. For details, refer to the Director’s user guide.

Display of tabs and options on tabs in the Operating Parameters dialog box varies according to how you access the Element Manager. Also, tabs and tab options may not be available, depending on user authorization. Reasons for unavailability are explained in tool-tip messages.

For example, if you launch the Element Manager from a virtual switch, you can only configure specific parameters in the Fabric and Domain tabs of the Operating Parameters dialog box. As another example, if you launch the Element Manager from the core switch, you can configure parameters on all tabs, but only specific parameters on the Fabric and Domain tabs. For detailed information, refer to the Director’s user guide or the online help.

This section outlines considerations for the security feature when virtual switches are configured in the fabric.

Different functions available in the Authentication tab depend on whether you open the virtual switch and the core switch element manager.

If you open the Element Manager from the virtual switch icon:

- Options are only available on the Devices tab.
- Ports that display in the Port Authentication List table on the Devices tab are those assigned to the virtual switch only. A VF ID column displays the virtual fabric identifier for the virtual fabric where the port is assigned.
- If you open the Element Manager from the virtual switch icon, only OSMS options are available on the Software tab,

If you open the Element Manager from a core switch icon, options are available on all tabs, however:
Some options are not available on the Devices tab, such as Edit Secret, Enable E_Port Authentication, and Enable N_Port Authentication. These are available if you open the Element Manager from the virtual switch icon.

OSMS options are not available on the Software tab.

You cannot enable FICON Management Server from the Element Manager launched through the core switch or virtual switch if virtual switches are configured. To enable, you must first assign all ports on the Director to the virtual switch with VF ID = 1.

Configure virtual switches using the Virtual Switches dialog box. For details, refer to the Director’s user guide. This option is only available when the Element Manager is launched from the core switch icon.

The Port Properties dialog box contains a VF ID field for each port. If the Director supports virtual switches, this will be the VF ID of the virtual switch where the port is assigned. Note that if you select a virtual switch, only those ports assigned to the switch display in the Port tab. If you select a core switch, all ports display.

In the Port List view, a VF ID column identifies the virtual fabric identifier for the port. This column does not display if you launch the Element Manager from the core switch icon. All ports on a virtual switch have the same VF ID. Options in the right-click menu in this view may be unavailable depending on whether you launch the Element Manager from the core switch or virtual switch icon. For example, the Port Binding option is not available from the core switch Element Manager.

In the Node List tab, a VF ID column identifies the virtual fabric identifier associated with the node. If you launch the Element Manager from the virtual switch icon, all ports will have the same VF ID. Options in the right-click menu in this tab may be unavailable depending on whether you launch the Element Manager from the core switch or virtual switch icon. For example, Port Binding is not available when you launch the Element Manager from a core switch icon.

If you launch the Element Manager from a virtual switch icon, you can only block ports assigned to the virtual switch. You cannot block All Ports on an optical paddle or LIM card unless all ports on these field replaceable units (FRUs) are all assigned to the virtual switch.
Isolated ports only display in the **Configure Ports** dialog box if you launch the Element Manager from the core Switch icon. Although you can configure these ports, they are not available until you assign them to a virtual Switch. Also, configuration options, such as **BB_Credit** and **Port Binding**, are not available.

If you launch the Element Manager from the virtual Switch icon, only those ports assigned to the Switch display.

If you launch the Element Manager from a virtual switch icon, you can only perform port diagnostics on ports assigned to the virtual switch. You cannot perform port diagnostics on **All Ports** on an optical paddle or LIM card unless all ports on these field replaceable units (FRUs) are all assigned to the virtual switch.

If you initiate this option in the Element Manager launched from a core switch, **Data Collection** generates one file containing data for the core switch and one file for each virtual switch configured in the core switch. Each virtual switch file contains information specific to that switch.

If you initiate this option in the Element Manager launched from a virtual switch, **Data Collection** generates one file containing data for the core switch and one file containing information for the selected virtual switch.

If virtual switches are configured in the Director, the offline and online state have different meanings depending on whether you open the Element Manager through a core switch or a virtual switch icon. Refer to the Director’s user guide for details about online state and offline state meanings.

If swapping ports through the **Swap Ports** dialog box in a core switch Element Manager, you can only swap ports not assigned to a virtual switch. If swapping ports through a virtual switch Element Manager, you can only swap ports assigned to that virtual switch.

If you initiate this option in the Element Manager launched from a core switch, the report contains data for the core switch and each virtual switch configured in the core switch.

If you initiate this option in the Element Manager launched from a virtual switch, the report contains data for the core switch and the selected virtual switch.
The **Director Properties** dialog box identifies virtual switches configured on the Director and associated virtual fabric identifiers (VF ID).

If you configure **Preferred Path** through the Element Manager launched from a virtual switch icon, you can only configure paths using ports assigned to the virtual switch.

If you configure **Preferred Path** through the Element Manager launched from a core switch icon, you can configure paths using all ports on the core switch.

You can configure **Port Binding** for a virtual switch or core switch. For the virtual switch, you can only configure ports assigned to that switch.

You can only configure **Open Trunking** through the Element Manager launched from a virtual switch icon. Ability to configure **Open Trunking** is not available through the core switch Element Manager.

When virtual switches are configured in the Director, you cannot configure switch binding in the Element Manager launched from the core switch icon. You can configure switch binding for ports assigned to a specific virtual switch by opening the Element Manager through the specific virtual switch icon.

If virtual switches are configured, logs will include a virtual fabric identifier (VF ID) entry. The VF ID is a decimal number (such as 1, 2, 3) within the range of valid VF IDs for the partition where the port assigned to a virtual switch resides. The VF ID identifies the fabric that the virtual switch or port belongs to.

When you launch the Element Manager from a core switch icon and select **Configure > Threshold Alerts**, the Threshold Alerts dialog box displays data on threshold alerts received and transmitted. It also provides full ability to activate, deactivate, create, edit, and delete threshold alerts.

When the Element Manager is launched from a virtual switch icon and you select **Configure > Threshold Alerts**, the Threshold Alerts dialog box displays data on threshold alerts received and transmitted. However, function buttons are replaced with only a View button. You cannot activate, deactivate, create, edit, or delete threshold alerts. Selecting the View button displays the Threshold
Alerts dialog box, but you can only view configuration settings for current threshold alerts. You cannot change any of these settings.

If you open the Element Manager from a virtual switch icon, you can only clear link incidents for ports that are assigned to the virtual switch. You can clear link incidents on all ports on the Director if you open the Element Manager from the core switch icon.

The following Element Manager features and options are only available if you open the Element Manager from the core switch icon. They are not available through a virtual switch Element Manager.

◆ Allow/Prohibit Matrix
◆ Backup and Restore Configuration
◆ Clear System Error Light
◆ Configure Feature Key
◆ Configure FICON Management Server
◆ Configure Partitions
◆ Configure Virtual Switch
◆ Enable Call Home Notification
◆ Enable E-Mail Notification
◆ Install Firmware (Firmware Library)
◆ Specific Operation Parameters
◆ Reset Configuration
◆ Threshold Alerts

**Note:** When you open the Element Manager from a virtual switch icon, you can only view alerts and details.

The following Element Manager features and options are only available if you open the Element Manager from the virtual switch icon. They are not available through a core switch Element Manager.

◆ Open Systems Management Server
◆ Open Trunking
◆ Switch Binding
◆ API Password
This chapter contains the following information.

- Event Management components ................................................... 368
- Event Management page description ........................................... 371
- Turning the Event Management feature on or off ....................... 373
- Configuring Event Management rules ........................................ 373
- Specifying a rule’s actions.......................................................... 379
- Editing a rule .............................................................................. 384
- Copying a rule ........................................................................... 388
- Deleting a rule ........................................................................... 388
- Activating an existing rule......................................................... 389
- Deactivating rules .................................................................... 390
- Event trigger properties ............................................................. 391
- Common property sets............................................................... 392
- Event types................................................................................ 397
- Writing Event Management macros............................................ 407
- Advanced event filtering.............................................................. 417
Event Management

Event Management components

Note: Enterprise Edition only. Event Management is a feature of the Advanced Module, which is an optional module. Please contact your sales representative to order the Advanced Module.

With Event Management, you can create rules for events you want to monitor. A rule is the mechanism defined by the user that identifies the response to specific event types. You can customize the event management rule using triggers and actions, which are explained in this section.

Event types

The event types for which you can customize the event management rule using triggers and actions are listed below.

- SNMP Trap Event
- Performance Event
- Product State Event
- Device Operational Status Event
- User Action Event
- Session Event
- Fabric Event
- Product Audit Event
- Product Event
- Product Hardware Event
- Product Link Incident Event
- Product Threshold Alert Event
- Ethernet Event
- Security Event

“Reference” on page 761 provides descriptions of the properties and their values that you can set for event triggers.
About Triggers

An event trigger or a schedule trigger is a logical filter that determines which conditions will initiate a set of predefined actions. You can set multiple triggers.

**Event triggers**

Event triggers are filters that define which events, of all the possible events listed in “Event types”, should initiate, or trigger, a set of actions. You can select or add values that correspond to one of the event type’s event, product, port, or system properties. Refer to “Event trigger properties” on page 391 for event type property descriptions.

Event triggers also allow you to set time limits so that the trigger will only occur if the event happens within a specified start and end time.

**Schedule triggers**

Schedule triggers monitor the system clock and fire when the specified time and date conditions are met. For information about how to set up a schedule trigger, see “Defining a schedule trigger” on page 378.

Event Management actions

You can use Event Management to automate tasks that you perform on the SAN by configuring multiple actions to be performed when an associated trigger is fired. The following actions are available:

- **E-mail.** Sends an e-mail message to specified recipients.
- **Export.** Exports data to a designated location.
- **Launch.** Launches the specified application using a script.
- **Log.** Adds an entry to the master log file and screen display.
- **Message.** Displays a message to all open Clients.
- **Pause.** Inserts a pause between actions.
- **Report.** Generates a report.
- **Send SNMP Trap.** Sends an SNMP trap containing information about the triggering event to the receiving system.
- **Sound.** Plays a sound.

You can write macros for the Event Management feature to insert relevant data into the text fields of some action phrases.
The following actions allow macros. Left-click to place the blinking cursor into one of the text fields indicated below.

- E-mail / Export – subject field and message field
- Launch – arguments field
- Log – description field
- Message – message field

Note: Refer to “Writing Event Management macros” on page 407 for instructions.
To view the Event Management user interface, click the Event Management tab on the main window of the Connectrix Manager application. Initially, you use this tab to access the Add Rule dialog box where you can define rules for your SAN environment. Once rules are defined, all configured rules display on the Event management tab. You can then activate, deactivate, edit, copy, or delete rules on this page, as well as create more new rules. You also turn the Event Management feature on or off on this tab. Refer to “Configuring Event Management rules” on page 373 for instructions on writing rules.

Table 18 describes the fields.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Buttons</td>
<td></td>
</tr>
<tr>
<td>Activate</td>
<td>Click to activate the selected rules.</td>
</tr>
<tr>
<td>Change</td>
<td>Click to change the reset interval.</td>
</tr>
<tr>
<td>Copy</td>
<td>Click to duplicate the selected rule.</td>
</tr>
<tr>
<td>Deactivate</td>
<td>Click to deactivate the selected rules.</td>
</tr>
<tr>
<td>Delete</td>
<td>Click to delete the selected rule.</td>
</tr>
</tbody>
</table>

Figure 44 Event Management tab
### Event Management

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit button</td>
<td>Click to edit the selected rule.</td>
</tr>
<tr>
<td>New button</td>
<td>Click to add a new rule.</td>
</tr>
<tr>
<td>OFF button</td>
<td>Click to turn the feature off. The flag on the Event Management tab will turn gray and be crossed out.</td>
</tr>
<tr>
<td>ON button</td>
<td>Click to turn the feature on. The flag on the Event Management tab will turn green.</td>
</tr>
</tbody>
</table>

**Columns**

<table>
<thead>
<tr>
<th># column</th>
<th>Specifies the auto-assigned rule number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active column</td>
<td>Specifies whether the rule is on.</td>
</tr>
<tr>
<td>Date Modified column</td>
<td>Lists the date and time that the rule was last edited.</td>
</tr>
<tr>
<td>Description column</td>
<td>Specifies the user-defined rule description.</td>
</tr>
<tr>
<td>Group column</td>
<td>Lists the group to which the rule belongs.</td>
</tr>
<tr>
<td>Name column</td>
<td>Specifies the user-defined rule name.</td>
</tr>
<tr>
<td>User column</td>
<td>Specifies the last user to modify the rule.</td>
</tr>
</tbody>
</table>

**Lists**

<table>
<thead>
<tr>
<th>Actions list</th>
<th>Lists the actions to be performed when the rule’s triggers are met.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description list</td>
<td>Lists the description of the selected rule.</td>
</tr>
<tr>
<td>Trigger list</td>
<td>Lists the trigger for the selected rule.</td>
</tr>
</tbody>
</table>

### Table 18 Fields and description (continued)
Turning the Event Management feature on or off

The color of the flag on the Event Management tab shows whether Event Management is turned on or off.

- If Event Management is turned on, the flag is green.
- If Event Management is turned off, the flag is gray and crossed out.

To turn Event Management on or off:
1. Click the Event Management tab on the main window.
2. Click the On or Off button in the top right corner of the page.
   If you click the Off button, any existing rules are disabled.

Configuring Event Management rules

When you write a rule, you must begin by specifying a trigger that will initiate an action.

There are two types of triggers:

- Event triggers – filters that define which events, of all the possible events, should initiate, or trigger, a set of actions.
- Schedule triggers – monitors the system clock and fires when the specified time and date conditions are met.

**TIP:** If you plan to use event macros in any of your actions, it is a good practice to define your trigger first and then define your actions and their macros. When you define the trigger first, the macro menus are filtered to give you choices that are appropriate to the event type of the event trigger. If you do not redefine the trigger, you will get a generic set of macro choices, some of which might not be appropriate for the event type you choose later when you define your trigger. See Appendix K, “Reference,” for complete information about event macros.
Defining an event trigger

1. Click the Event Management tab on the main window.
2. Click New.
   The Add Rule dialog box displays.
3. Type a name for the rule in the Name field.
4. Select or enter a group name in the Group field.
5. Select the Active check box if you want to activate the rule after you are finished creating it.
6. Type a description for the rule in the Description field.
7. From the Trigger list on the bottom left of the dialog box, select Event or Schedule.
8. Filter the trigger by selecting an option from the Type list. The Event types, with a brief description, are listed below.
   • SNMP Trap Event – SNMP trap events occur when the Connectrix Manager application Server receives an SNMP trap.
   • Performance Event – Performance events occur when the performance at a switch port crosses a user-defined threshold.
   • Product State Event – Product state events occur when a device or connection changes to Up or Down.
   • Device Operational Status Event – Device operational status events notify you of the operational status of SAN products.
   • User Action Event – User action events occur when you change a setting in the Server.
   • Session Event – Session events notify you of session changes.
   • Fabric Event – Fabric events notify you of fabric changes.
   • Product Audit Event – Product audit events occur when a target product is audited.
   • Product Event – Product events notify you when the product status changes.
   • Product Hardware Event – Product hardware events notify you of errors that occur on the product hardware.
   • Product Link Incident Event – Product link incident events notify you of changes to the link status.
• Product Threshold Event – Product threshold events notify you when a threshold alert has been reached.
• Ethernet Event – Ethernet events notify you when the Ethernet link between the Server and the managed product is lost.
• Security Event – Security events notify you when a product’s security level changes.

See Appendix K, “Reference,” for descriptions of the properties you can set for event triggers.

9. Select or enter data in the Property, Operator, and Value fields, as required. See “Trigger phrases” on page 376 for information about the Property, Operator, and Value fields.

**Important:** Once you have selected a trigger type and have added the first phrase, click Add to avoid losing your work.

10. Click **Add**.

The first line of the trigger you specified displays in the Trigger table in the top half of the dialog box.

11. Select a blank line in the Trigger table and repeat steps 9 and 10 to add additional phrases to the rule trigger.

12. Click AND in the Trigger table to choose a different logical relationship between phrases, if necessary. Otherwise, go to Step 13.

13. Add opening and closing parentheses, as needed, to construct complicated logical triggers. If you are constructing simple triggers, go to “Trigger phrases”, next.

To remove an opening or closing parenthesis, select a row and highlight a parenthesis bracket by clicking and dragging across it. The bracket becomes highlighted by a darker color than the background row selection color. You can then remove the parenthesis bracket by selecting the Delete or Backspace button.
The two types of triggers (event and schedule) are constructed from logically-related phrases, and each phrase contains the following three parts:

- **Property.** A property is a variable for which you set values. Properties are generally one of four types: Event, Product, Port, or System. For descriptions of the event properties, refer to “Event trigger properties” on page 391.

- **Operator.** An operator is a logical or string function that you use to define the relationship between a property type and its values. For details, see “Trigger operators” on page 376.

- **Value.** A value is a text string or time reference that you define for a specific property. Values are either presented in a list or entered by the user.

### Trigger operators

Operators define the relationship between properties and their values. The list of available operators varies depending on whether the value is a string or a number. Table 19 shows the full list of operators.

#### Table 19  Operators and values

<table>
<thead>
<tr>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>==</td>
<td>Number or String</td>
</tr>
<tr>
<td>!=</td>
<td>Number or String</td>
</tr>
<tr>
<td>&lt;</td>
<td>Number</td>
</tr>
<tr>
<td>&lt;=</td>
<td>Number</td>
</tr>
<tr>
<td>&gt;</td>
<td>Number</td>
</tr>
<tr>
<td>&gt;=</td>
<td>Number</td>
</tr>
<tr>
<td>Contains</td>
<td>String</td>
</tr>
<tr>
<td>Does Not Contain</td>
<td>String</td>
</tr>
<tr>
<td>Starts With</td>
<td>String</td>
</tr>
</tbody>
</table>
Configuring Event Management rules

**Phrase operators**

The phrases in the Trigger table are related using the following operators:

- **AND**
- **OR**
- **AND NOT**
- **OR NOT**

Each phrase, except the first one, starts with a logical operator. The default operator is AND.

**Specifying time limits for an event trigger**

Time limit triggers are used to specify times during which an event trigger should be fired. For example, you may specify that all offline events between 5:00 PM and 8:00 AM will trigger e-mail messages and log entries to occur. Thus, the application will send an e-mail message to notify recipients that the event occurred, and will add a second, more detailed entry to the master log.

1. From the Add Rule or Edit Rule Trigger table, select an existing trigger.
2. Select *Time Limits* from the *Trigger* list at the left.
3. Select *Daily Time Limits* or *Weekly Time Limits* from the *Type* list.
4. Enter the appropriate information in the *Values* fields based on the type of limits you selected.
   - If you selected *Daily*, enter the start time and end time in military time format.
   - If you selected *Weekly*, enter the start time and end time in military time format. Then select an option from the *Start Day* and *End Day* lists.

---

**Table 19 Operators and values (continued)**

<table>
<thead>
<tr>
<th>Operator</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ends With</td>
<td>String</td>
</tr>
<tr>
<td>Changed From</td>
<td>String'</td>
</tr>
<tr>
<td>Changed To</td>
<td>String</td>
</tr>
</tbody>
</table>
5. Click Add.
6. Click OK to save your changes and close the Edit Rule dialog box.

   The system returns to the Event Management dialog box. Click the Edit button to return to the Edit Rule Trigger table and verify the time limit setting.

---

**Defining a schedule trigger**

You can add a schedule trigger to specify the time and date that an action should be performed.

1. Click the Event Management tab on the main window.
2. Click New.
   The Add Rule dialog box displays.
3. Type a name for the rule in the Name field.
4. Select or enter a group name in the Group field.
5. Select the Active check box if you want to make the rule active after you are finished creating it.
6. Type a description for the rule in the Description field.
7. Select Schedule from the Trigger list at the bottom left of the dialog box.
8. Select an option from the Type list. From the Type list, you can specify the trigger to fire daily, weekly, monthly, one time, or hourly.
9. Enter the time values into the Value fields.
10. Click Add.
    The first line of the trigger you configured displays in the Trigger table in the top half of the dialog box.

   **Note:** You cannot combine two schedule triggers in a single rule.

11. Repeat steps 8-10 to add additional phrases to the schedule trigger.
Specifying a rule’s actions

After specifying a rule’s triggers, you can add actions that the application will perform when trigger conditions are met.

◆ “Specifying an e-mail action”
◆ “Specifying an export action”
◆ “Specifying a launch action”
◆ “Specifying a log action”
◆ “Specifying a message action”
◆ “Specifying a pause action”
◆ “Specifying a report action”
◆ “Specifying a send SNMP trap action”

Specifying an e-mail action

You can configure the application to send an e-mail message when the specified trigger is fired.

1. Select Email from the Actions list at the bottom left corner of the Add Rule dialog box.
2. Enter the recipients’ e-mail addresses in the To field, separating multiple addresses with semicolons (required).
3. Enter your e-mail address in the From parameter field (required).
4. Enter a subject for the e-mail in the Subject parameter field.
   To insert a macro for values from the trigger’s content, click in the Value column and then right-click and select an argument. To write a macro, see “Writing Event Management macros” on page 407.
5. Enter the body of your e-mail message in the Message parameter field.
   To insert a macro for values from the trigger’s context, click in the Value column and then right-click and select an argument. To write a macro, see “Writing Event Management macros” on page 407.
6. Click Add.
Event Management

7. When you have finished configuring the rule, click **OK** to save your work and close the **Add Rule** dialog box.

**Specifying an export action**

You can configure Event Management to export data, such as SAN files, performance data, reports, or zoning information, when the specified trigger is fired. By default, on Windows-based systems, the data is exported to the following directory: 

<Install_Path>\Server\Data\Export.

On Unix-based systems, the exported data from the Server/Data/Export is transferred to the Client/Data directory: 

${INSTALL_DIR}/Server/Data/Export.

1. Select **Export** from the **Actions** list at the bottom left of the **Add Rule** dialog box.

2. Select the destination from the **Type** list for the export (for example, Disk, E-mail, MySQL, or DB2).

3. Select the types of information you want to export in the **Files** area.
   
   The options may differ depending on the export destination.

4. Select the switches for which you want to export performance data in the **Switches** area.

   If you are not exporting performance data, proceed to Step 5.

5. Click **Add**.

6. Click **OK** to save your work and close the **Add Rule** dialog box.

**Specifying a launch action**

You can configure the Event Management feature to launch an application when the specified trigger is fired.

1. Select **Launch** from the **Actions** list at the bottom left of the **Add Rule** dialog box.

2. Select an option in the **Script File** parameter field.

   You can add script files to this list by copying them to 

   <Install_Home>\Server\LaunchScripts\.

3. Enter the script arguments in the **Arguments** parameter field.

**TIP:** Before configuring the Event Management feature to launch a script, verify that the script launches the application successfully on the Server.
Specifying a rule’s actions

i. To insert a macro for values from the trigger’s content, click in the Value column and then right-click and select an argument.

j. To write a macro, see “Writing Event Management macros” on page 407.

4. Click Add.

5. Click OK to save your work and close the Add Rule dialog box.

Specifying a log action

You can configure an additional master log entry that includes a custom description of events.

1. Select Log from the Actions list at the bottom left of the Add Rule dialog box.

2. Select the location for the log entry in the To parameter field. The options are Log File and Screen and Log File.

3. Select a severity level for the log entry in the Level parameter field. The options are Informational, Warning, and Fatal.

4. Enter a description for the log entry action in the Description parameter field.

5. To insert a macro for values from the trigger’s content, click in the Value column and then right-click and select an argument. To write a macro, see “Writing Event Management macros” on page 407.

6. Click Add.

7. Click OK to save your work and close the Add Rule dialog box.
Specifying a message action

You can configure the application to display a pop-up message on all open Clients when the specified trigger is fired. You can choose to display either informational, warning, or fatal icons in the message. The title bar will display the rule number, rule name, and “message” (for example, “Rule 23 Switch Offline Message”). The time and date is inserted automatically. Multiple messages display in a single pop-up window.

1. Select Message from the Actions list at the bottom left of the Add Rule dialog box.
2. Select a severity level for the message in the Severity Level parameter field. The options are Information, Warning, and Fatal.
3. Enter the text of the desired message in the Message parameter field.
4. To insert a macro for values from the trigger’s contextual data, click in the Message Value column and then right-click and select an argument. To write a macro, see “Writing Event Management macros” on page 407.
5. Click Add.
6. Click OK to save your work and close the Add Rule dialog box.

Specifying a pause action

You can configure the application to delay the execution of the next action in the Actions list by the time period specified in the pause action.

1. Select Pause from the Actions list at the bottom left of the Add Rule dialog box.
2. Select a time unit for the pause from the Type list. The options are seconds, minutes, and hours.
3. Enter the length of time for the pause in the Value field.
4. Click Add.
5. Click OK to save your work and close the Add Rule dialog box.
Specifying a report action

You can configure the application to generate a report when the specified trigger is fired.

1. Select **Report** from the **Actions** list at the bottom left of the **Add Rule** dialog box.
2. Select the types of reports to generate by clicking each report’s corresponding check box.
   
   For detailed information about various report types, refer to the *Connectrix Manager User Guide*.
3. Click **Add**.
4. Click **OK** to save your work and close the **Add Rule** dialog box.

Specifying a send SNMP trap action

You can send an SNMP Trap to a specified receiving system.

1. Select **Send SNMP Trap** from the **Actions** list at the bottom left of the **Add Rule** dialog box.
2. Enter the IP address and the port number of the receiving system into the **Destination IP Address** and **Port Number** fields.
3. Click **Add**.
4. Click **OK** to save your work and close the **Add Rule** dialog box.

Specifying a sound action

You can configure the application to play a sound when the specified trigger is fired.

The sound card and driver must be installed on the same server for the sound action to work.

1. Select **Sound** from the **Actions** list at the bottom left of the **Add Rule** dialog box.
2. Select a sound in the **File** parameter field.
   
   Note that you can add sounds to this list.
3. Click **Add**.
4. Click **OK** to save your work and close the **Add Rule** dialog box.

**Editing a rule**

After you add a rule and configure its triggers and actions, you can edit the rule.

*Note:* The Add Rule and Edit Rule dialog boxes are identical.

Steps 1 through 5 provide basic instructions for editing a rule. For instructions on specific editing tasks, refer to . This table lists the kinds of edits you can make to a rule and provides additional instructions for performing the edit.

1. Click the **Event Management** tab on the main window of the Connectrix Manager application.
2. Select the rule you want to edit in the **Rules** table.
3. Click **Edit.**
   
The **Edit Rule** dialog box displays.
4. Edit the rule as needed. For instructions on specific kinds of edits, refer to .
5. Click **OK** to save your changes and close the **Edit Rule** dialog box.
<table>
<thead>
<tr>
<th>Type of edit</th>
<th>Additional instructions for editing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change from Schedule Trigger to Event Trigger</td>
<td>1. Select the Schedule trigger you want to change from the <strong>Trigger</strong> table.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Event</strong> from the <strong>Trigger</strong> list at the bottom left of the dialog box.</td>
</tr>
<tr>
<td></td>
<td>3. Filter the event trigger by selecting an option from the <strong>Type</strong> list.</td>
</tr>
<tr>
<td></td>
<td>4. Enter the appropriate values in the <strong>Property</strong>, <strong>Operator</strong>, and <strong>Values</strong> fields.</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>The Schedule trigger is changed to an Event trigger.</td>
</tr>
<tr>
<td>Change from Event Trigger to Schedule Trigger</td>
<td>1. Select the Event trigger you want to change from the <strong>Trigger</strong> table.</td>
</tr>
<tr>
<td></td>
<td>2. Select <strong>Schedule</strong> from the <strong>Trigger</strong> list at the bottom left of the dialog box.</td>
</tr>
<tr>
<td></td>
<td>3. Select a schedule option from the <strong>Type</strong> list.</td>
</tr>
<tr>
<td></td>
<td>4. Select or enter appropriate information in the <strong>Value</strong> field(s).</td>
</tr>
<tr>
<td></td>
<td>5. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>The Event trigger is changed to a Schedule trigger.</td>
</tr>
<tr>
<td>Change the Event type</td>
<td>1. Select the Event trigger you want to change from the <strong>Trigger</strong> table.</td>
</tr>
<tr>
<td></td>
<td>2. Filter the event trigger by selecting a different option from the <strong>Type</strong> list.</td>
</tr>
<tr>
<td></td>
<td>3. Enter the appropriate values in the <strong>Property</strong>, <strong>Operator</strong>, and <strong>Values</strong> fields.</td>
</tr>
<tr>
<td></td>
<td>4. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>The event type is changed.</td>
</tr>
<tr>
<td>Change the Schedule type</td>
<td>1. Select the Schedule trigger you want to change from the <strong>Trigger</strong> table.</td>
</tr>
<tr>
<td></td>
<td>2. Select a different schedule option from the <strong>Type</strong> list. The options are <strong>Daily</strong>, <strong>Weekly</strong>, <strong>Monthly</strong>, <strong>One Time</strong>, and <strong>Hourly</strong>.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>The schedule type is changed.</td>
</tr>
<tr>
<td>Change an existing Property/Operator/Value</td>
<td>1. Select the Event trigger you want to change from the <strong>Trigger</strong> table.</td>
</tr>
<tr>
<td>combination of an exiting phrase</td>
<td>2. Select or enter the desired value in the <strong>Property</strong>, <strong>Operator</strong>, or <strong>Value</strong> fields.</td>
</tr>
<tr>
<td></td>
<td>3. Click <strong>Add</strong>.</td>
</tr>
<tr>
<td></td>
<td>The value is changed.</td>
</tr>
</tbody>
</table>
## Event Management

### Table 20  Type of edit (continued)

<table>
<thead>
<tr>
<th>Type of edit</th>
<th>Additional instructions for editing</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the logical relationships between phrases and any of the following:</td>
<td>• Click AND in the Trigger table to choose a different logical relationship between phrases.</td>
</tr>
<tr>
<td>• Adding or removing parentheses</td>
<td>• Select a phrase in the Trigger table and click the opening or closing parenthesis button.</td>
</tr>
<tr>
<td>• Changing logical operators at the beginning of phrases</td>
<td>• Use the up and down arrow keys to change the order of phrases.</td>
</tr>
<tr>
<td>• Changing the phrase order by moving phrases up and down in the Trigger table.</td>
<td></td>
</tr>
<tr>
<td>Change an existing action</td>
<td>1. Select the trigger from the Trigger table for which you want to change the action.</td>
</tr>
<tr>
<td></td>
<td>2. Select a different action for the trigger from the Actions list in the lower left corner of the dialog box.</td>
</tr>
<tr>
<td></td>
<td>3. Perform all steps required by the type of action you selected. For specific instructions, refer to the individual procedures in this section for specifying different kinds of actions.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add.</td>
</tr>
<tr>
<td></td>
<td>The action is changed.</td>
</tr>
<tr>
<td>Add new phrases</td>
<td>1. Select Event or Schedule from the Trigger list in the lower left corner of the dialog box.</td>
</tr>
<tr>
<td></td>
<td>2. Select the appropriate event or schedule type in the Type list.</td>
</tr>
<tr>
<td></td>
<td>3. Select or enter appropriate Property, Operator, and Value information for the new phrase.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add.</td>
</tr>
<tr>
<td></td>
<td>The new phrase is added to the Trigger table.</td>
</tr>
<tr>
<td>Add a new action</td>
<td>1. Select the trigger from the Trigger table for which you want to add the new action.</td>
</tr>
<tr>
<td></td>
<td>2. Select a new action to add to the trigger from the Actions list in the lower left corner of the dialog box.</td>
</tr>
<tr>
<td></td>
<td>3. Perform all steps required by the type of action you selected. For specific instructions, refer to the individual procedures in this section for specifying different kinds of actions.</td>
</tr>
<tr>
<td></td>
<td>4. Click Add.</td>
</tr>
<tr>
<td></td>
<td>The new action is added to the Actions table.</td>
</tr>
</tbody>
</table>
Table 20 Type of edit (continued)

<table>
<thead>
<tr>
<th>Type of edit</th>
<th>Additional instructions for editing</th>
</tr>
</thead>
</table>
| Change the order of Actions              | 1. Select the action you want to move in the **Actions** table.  
2. Use the up and down arrow keys to change the order of the actions.                                           |
| Delete existing Trigger Phrases or Actions| 1. Select a trigger phrase from the **Trigger** table, or an action from the **Actions** table.  
2. Click the appropriate **Delete** button (for triggers, the one to the right of the **Trigger** list; for actions, the one to the right of the **Actions** list). |
| Change the Reset Interval of a Rule       | 1. In the **Interval** field, type the number of time units to wait between rule firings.  
2. From the list, select the size of the time units (**seconds**, **minutes**, or **hours**).  
3. Click **OK**.                                                                                          |
**Copying a rule**

By copying a rule, you can retain previously-configured triggers and actions from an existing rule. You can then edit the rule as needed, rather than creating a new rule.

1. Click the **Event Management** tab on the main window of the Connectrix Manager application.

   The **Event Management** dialog box displays.

2. Click the rule that you want to copy in the **Rules** table.

3. Click **Copy**.

   The word “Copy” is added to the front of the rule name, and a copy of the selected rule is assigned a new rule number and displays in the **Rules** table.

**Deleting a rule**

You can permanently remove a rule from the Rules table by deleting it.

1. Click the **Event Management** tab on the main window of the Connectrix Manager application.

   The **Event Management** dialog box displays.

2. Select one or more rules you want to delete in the **Rules** table.

   - To select multiple rules in sequence, press **Shift** as you click the first and last rules in the group.
   - To select a non-contiguous group of rules, press **CTRL** as you click each rule.

   **Note:** To select a non-contiguous set of rules, press **CTRL** and click each rule.

3. Click **Delete**.

   A message box displays a list of the rules to be deleted and a request that you confirm the deletion.

4. Make sure the appropriate rules are listed. Click **Yes** to continue or **No** to cancel the deletion.
When you click Yes, the rules are deleted and no longer display in the Rules table of the Event Management dialog box.

Activating an existing rule

You can manually activate one or multiple rules by following these steps.

1. Click the Event Management tab on the main window of the Connectrix Manager application.
   The Event Management dialog box displays.
2. Click the row for each rule you want to activate.
   • To select multiple rules in sequence, press Shift as you click the first and last rules in the group.
   • To select a non-contiguous group of rules, press CTRL as you click each rule.
3. Click Activate.
   A message box lists the selected rule(s) and a request for you to confirm the activation.
4. Make sure the appropriate rules are listed. Click Yes to continue or No to cancel the activation.
   When you click Yes, the rules are activated. A green flag displays by each active rule in the Active column.

Note: For new rules, select the Active check box to activate the rule after you finish creating it.
Deactivating rules

You can manually deactivate one or multiple rules by following these steps.

1. Click the **Event Management** tab on the main window of the Connectrix Manager application.

   The **Event Management** dialog box displays.

2. Click the row for each rule you want to deactivate.

   - To select multiple rules in sequence, press **Shift** as you click the first and last rules in the group.
   - To select a non-contiguous group of rules, press **CTRL** as you click each rule.

3. Click **Deactivate**.

   A message box lists the selected rule(s) and a request for you to confirm the deactivation.

4. Make sure the appropriate rules are listed. Click **Yes** to continue or **No** to cancel the deactivation.

   When you click **Yes**, the rules are deactivated. A green flag disappears by each deactivated rule in the **Active** column.

   **Note:** For new rules, verify that the **Active** check box, just to the right of the rule name, is clear after you finish creating it.
Event trigger properties

Event trigger properties belong to one of four groups:

- Event Properties
- Product Properties
- Port Properties
- System Properties

**Note:** The one exception is with the User Action Event type, which has User properties.

Refer to the information in the following sections for descriptions of the Event properties and their values that you can set for event triggers.
Common property sets

Each Event type has its own Event property set. The following property sets are common to all Event types:

- “Product property set”
- “Port property set”
- “System property set”

Note: The one exception is with the User Action Event type, which has User properties.

Product property set

The product property set includes properties about a product in the SAN.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Enter the FICON class to which the node belongs.</td>
</tr>
<tr>
<td>Comments</td>
<td>Enter strings that would be contained in the Comments field of the Properties dialog box of target products.</td>
</tr>
<tr>
<td>Contact</td>
<td>Enter the name of person to contact if problems occur on the product.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description of the product.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Select the type of device. The options are HBA, Storage, Switch, Bridge, Hub, NAS, Tape, and Manager.</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Enter the product’s domain identifier.</td>
</tr>
<tr>
<td>Enclosure Name</td>
<td>Enter the name that has been given to an enclosure for a particular set of products.</td>
</tr>
<tr>
<td>Firmware</td>
<td>Enter the product’s firmware level.</td>
</tr>
<tr>
<td>Firmware (in-band)</td>
<td>Enter the firmware level for in-band devices.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product’s IP address.</td>
</tr>
<tr>
<td>Location</td>
<td>Enter the location of the product.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Managed By</td>
<td>Enter the name of the hardware product that manages the device.</td>
</tr>
<tr>
<td>Management Link</td>
<td>Select the management link status (down, up, or discovery failed).</td>
</tr>
<tr>
<td>Model Number</td>
<td>Enter the product’s model number.</td>
</tr>
<tr>
<td>Model Number (in-band)</td>
<td>Enter the model number for in-band devices.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the product’s name, as specified in the Properties dialog box.</td>
</tr>
<tr>
<td>Name (in-band)</td>
<td>Enter the name for the in-band device.</td>
</tr>
<tr>
<td>Nickname</td>
<td>Enter the product’s label, as shown on the physical map.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the product’s world wide name (WWN).</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Select the product’s status (operational, degraded, failed, or unknown).</td>
</tr>
<tr>
<td>Port Count</td>
<td>Enter the number of ports on the product.</td>
</tr>
<tr>
<td>Port Count (in-band)</td>
<td>Enter the number of in-band ports.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Enter the product’s serial number.</td>
</tr>
<tr>
<td>Serial Number (in-band)</td>
<td>Enter the serial number for in-band devices.</td>
</tr>
<tr>
<td>Tag Number</td>
<td>Enter the tag number of the product.</td>
</tr>
<tr>
<td>Text1 through Text4</td>
<td>Enter values into the Text1 through Text4 value fields.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Enter the product’s vendor.</td>
</tr>
<tr>
<td>Vendor (in-band)</td>
<td>Enter the vendor for in-band devices.</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Enter the vendor’s identification information.</td>
</tr>
</tbody>
</table>
The port property set includes properties about the port.

### Table 22  Port property set

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active FC4 Types</td>
<td>Enter the active Fibre Channel 4 types; for example, SCSI or IP.</td>
</tr>
<tr>
<td>Blocked Configuration</td>
<td>Enter the blocked configuration of the port.</td>
</tr>
<tr>
<td>Blocked Reason</td>
<td>Enter the reason why the port is blocked.</td>
</tr>
<tr>
<td>Class of Service</td>
<td>Enter the port’s class of service (CoS) value. The CoS value, which ranges between zero (low priority) and seven (high priority) determines how the frame is handled as it is transmitted from the switch.</td>
</tr>
<tr>
<td>Fabric Nickname</td>
<td>Enter the name of the fabric’s string that is associated with the fabric’s world wide name (WWN).</td>
</tr>
<tr>
<td>FC Address</td>
<td>Enter the Fibre Channel address. Each FC port has both an address identifier and a world wide name (WWN).</td>
</tr>
<tr>
<td>Max. Frame Size (bytes)</td>
<td>Enter the port’s maximum frame size, in bytes.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the name of the port that was specified through the Switch Element Manager.</td>
</tr>
<tr>
<td>OS Device Name</td>
<td>Enter the operating system's product name.</td>
</tr>
<tr>
<td>Port Address</td>
<td>Enter the address of the port.</td>
</tr>
<tr>
<td>Port Nickname</td>
<td>Enter a label to associate the port to its world wide name (WWN).</td>
</tr>
<tr>
<td>Port Number</td>
<td>Enter the number of the port whose properties display.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Select the port type. The options are N, NL, E, F, FL, T100, GigE, G, and R.</td>
</tr>
<tr>
<td>Port WWN</td>
<td>Enter the world wide name of the port.</td>
</tr>
<tr>
<td>Speed Configured (Gb/s)</td>
<td>Enter the current speed of the port, in gigabits per second.</td>
</tr>
<tr>
<td>Speed Supported (Gb/s)</td>
<td>Enter the maximum speed of the port, in gigabits per second.</td>
</tr>
<tr>
<td>State</td>
<td>Select the port state. The options are Up or Down.</td>
</tr>
</tbody>
</table>
**Common property sets**

**Event Management**

**System property set**

The system property set includes properties about the operating system and the server.

### Table 22 Post property set (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supported FC4 Types</td>
<td>Enter the Fibre Channel 4 types that the port supports; for example, SCSI or IP</td>
</tr>
<tr>
<td>Symbolic Name</td>
<td>Enter the product’s symbolic name for the discovered port. The symbolic name has a six-character limit.</td>
</tr>
<tr>
<td>VF ID</td>
<td>Enter the virtual fabric ID for the switch.</td>
</tr>
</tbody>
</table>

### Table 23 System property set

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Count</td>
<td>Enter the number of Clients that are logged into the SAN.</td>
</tr>
<tr>
<td>Discovery Off</td>
<td>Select true or false to indicate whether discovery is turned on.</td>
</tr>
<tr>
<td>Event Notification Off</td>
<td>Select true or false to indicate whether event notification is turned on.</td>
</tr>
<tr>
<td>Free Memory</td>
<td>Enter how much physical memory is available.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the Server’s IP address.</td>
</tr>
<tr>
<td>OS Architecture</td>
<td>Enter the architecture of the operating system.</td>
</tr>
<tr>
<td>OS Name</td>
<td>Select the operating system name. The options are Sun, Linux, HP-UX, AIX, and Windows, 98, NT, 2000, 2003, and XP.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Enter the version of the operating system.</td>
</tr>
<tr>
<td>Region</td>
<td>Enter the region of the world where the user is located.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Enter the name of the Server.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Enter the number of the discovered subnet mask.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Enter the user’s time zone.</td>
</tr>
</tbody>
</table>
### Table 23 Event Management

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total Memory</td>
<td>Enter the amount of total physical memory.</td>
</tr>
<tr>
<td>Trap Forwarding Off</td>
<td>Select true or false to indicate whether SNMP trap forwarding is enabled.</td>
</tr>
<tr>
<td>User Count</td>
<td>Enter the number of users.</td>
</tr>
<tr>
<td>VM Name</td>
<td>Enter the name of the Java Virtual Machine.</td>
</tr>
<tr>
<td>VM Vendor</td>
<td>Enter the vendor of the Java Virtual Machine.</td>
</tr>
<tr>
<td>VM Version</td>
<td>Enter the version of the Java Virtual Machine.</td>
</tr>
</tbody>
</table>
The event types for which you can customize the event management rule using triggers and actions are listed below.

- “Device operational status event property set”
- “Ethernet event property set”
- “Fabric event property set”
- “Performance event property set”
- “Product audit event property set”
- “Product event property set”
- “Product hardware event property set”
- “Product link incident event property set”
- “Product state event property set”
- “Product threshold alert event property set”
- “Security event property set”
- “Session event property set”
- “SNMP trap event property set”
- “User action event property set”

### Device operational status event property set

Device operational status events occur to notify you of the operational status of products in the SAN.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the device operational status events you want to target.</td>
</tr>
<tr>
<td>Device Operational Status</td>
<td>Select the product’s current operational status. The options are operational, degraded, failed, and unknown.</td>
</tr>
<tr>
<td>Element Type</td>
<td>Select the element type. The options are Device or Link.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, or fatal.</td>
</tr>
</tbody>
</table>
Event Management

Table 24  Device operational status even property set (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the product that encountered an event.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the world wide name of the product that encountered an event.</td>
</tr>
<tr>
<td>Previous Device</td>
<td>Select the product’s previous operational status. The options</td>
</tr>
<tr>
<td>Operational Status</td>
<td>are operational, degraded, failed, and unknown</td>
</tr>
<tr>
<td>Source</td>
<td>Enter a string for the target source’s cause of the event (for example, user ID or device label).</td>
</tr>
</tbody>
</table>

Table 25  Ethernet event property set

An Ethernet event occurs when the Ethernet link between the Server and the managed product is lost. You can configure the application to send notification of Ethernet events.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the ethernet events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product’s IP address.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Type the product’s world wide name (WWN).</td>
</tr>
<tr>
<td>Source</td>
<td>Enter a string for the target source’s cause of the event. The options are user ID or device label.</td>
</tr>
</tbody>
</table>
Fabric event property set

Fabric events occur to notify you of fabric changes.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the fabric events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>Fabric Nickname</td>
<td>Enter the nickname of the fabric on which the event occurred.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product’s IP address.</td>
</tr>
</tbody>
</table>

Performance event property set

Performance events occur when the performance at a switch port crosses a user-defined threshold.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select a severity level. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>Fabric Nickname</td>
<td>Enter the nickname of the selected zone set’s fabric.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the product that encountered an event.</td>
</tr>
<tr>
<td>Measure Type</td>
<td>Select a performance measurement unit. The options are Transmit, Receive, CRC errors, Loss of Sync Errors, and Loss of Signal Errors.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the world wide name (WWN) of the product that encountered an event.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Enter the port number that encountered an event.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Select the port type. The options are N, NL, E, F, FL, T100, GigE, G, and R.</td>
</tr>
</tbody>
</table>
Event Management

Table 27  Performance event property set (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port WWN</td>
<td>Enter the world wide name (WWN) of the port that encountered an event.</td>
</tr>
<tr>
<td>Source</td>
<td>Enter a string for the target source's cause of the event (for example, user ID or device label).</td>
</tr>
<tr>
<td>Threshold Type</td>
<td>Select the performance threshold type. The options are high critical, high warning, low warning, and low critical.</td>
</tr>
</tbody>
</table>

Product audit event property set

Product audit events occur to notify you of product audits.

Table 28  Product audit event property set

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit ID</td>
<td>Enter the user ID and user's IP address for the audit entry.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the product audit event you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product's IP address.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the product's world wide name (WWN).</td>
</tr>
<tr>
<td>Source</td>
<td>Enter the user ID of the user who performed the action.</td>
</tr>
</tbody>
</table>
### Event types

**Product event property set**

Product events occur to notify you of changes to the product status or information.

**Table 29**  
**Product event property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the product events you want to target.</td>
</tr>
<tr>
<td>Event</td>
<td>Enter a description of the event.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>FRU Position</td>
<td>Enter the position of the FRU that encountered an event.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the product that encountered an event.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the product’s world wide name (WWN).</td>
</tr>
</tbody>
</table>

**Product hardware event property set**

Product hardware events occur to notify you of errors with product hardware.

**Table 30**  
**Product hardware event property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the product hardware events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select a severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>FRU Position</td>
<td>Enter the position of the FRU that encountered an event.</td>
</tr>
<tr>
<td>FRU Type</td>
<td>Enter the type of FRU that encountered the event.</td>
</tr>
<tr>
<td>Hardware Action Type</td>
<td>Specifies when a FRU is inserted or removed.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product’s IP address.</td>
</tr>
</tbody>
</table>
Event Management

Table 30  
**Product hardware event property set (continued)**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node Name</td>
<td>Enter the product's world wide name (WWN).</td>
</tr>
<tr>
<td>Part Number</td>
<td>Enter the part number of the product that encountered the event.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Enter the serial number of the product that encountered the event.</td>
</tr>
</tbody>
</table>

Product link incident event property set

Product link incident events occur to notify you of link incidents.

Table 31  
**Product link incident event property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the product link incident events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product’s IP address.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the product’s world wide name (WWN).</td>
</tr>
<tr>
<td>Port Number</td>
<td>Enter the number that corresponds to the port on which the incident occurred.</td>
</tr>
</tbody>
</table>

Product state event property set

Product state events occur when a device or connection goes Up or Down.

Table 32  
**Product state event property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the product state events you want to target.</td>
</tr>
<tr>
<td>Discovery Type</td>
<td>Select In-band or out-of-band discovery.</td>
</tr>
<tr>
<td>Element Type</td>
<td>Select the element type. The options are Device or Link.</td>
</tr>
</tbody>
</table>
### Product state event property set (continued)

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Level</td>
<td>Select a severity level. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>Fabric Nickname</td>
<td>Enter the nickname of the selected zone set's fabric.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the product that encountered an event.</td>
</tr>
<tr>
<td>Management Link</td>
<td>Select the management link status (down, up, or discovery failed)</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the world wide name (WWN) of the product that encountered an event.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Select the port type. The options are N, NL, E, F, FL, T100, GigE, G, and R.</td>
</tr>
<tr>
<td>Port WWN</td>
<td>Enter the world wide name (WWN) of the port that encountered an event.</td>
</tr>
<tr>
<td>Source</td>
<td>Enter a string for the target source's cause of the event (for example, user ID or device label).</td>
</tr>
</tbody>
</table>

### Product threshold alert event property set

Product threshold alert events occur to notify you when a threshold alert has been reached.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the product threshold alert events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>Interval</td>
<td>Enter the frequency with which notifications should be sent.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product's IP address.</td>
</tr>
<tr>
<td>Name</td>
<td>Enter the product's name, as specified in the Product Properties dialog box.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the product's world wide name (WWN).</td>
</tr>
</tbody>
</table>
**Event Management**

**Table 33**  
**Product threshold alert event property set (continued)**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Number List</td>
<td>Specify the port on which the incident occurred. The options are RX, TX, and RX and TX.</td>
</tr>
<tr>
<td>Product Threshold Type</td>
<td>Enter the port on which the incident occurred.</td>
</tr>
<tr>
<td>Source</td>
<td>Enter a string for the target source's cause of the event. The options are user ID or device label.</td>
</tr>
<tr>
<td>Utilization</td>
<td>Enter the transmit percent utilization of the port.</td>
</tr>
</tbody>
</table>

**Security event property set**

A Security event occurs when a product reaches a specified event level.

**Table 34**  
**Security event property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the security events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product's IP address.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Type the product's world wide name (WWN).</td>
</tr>
<tr>
<td>Source</td>
<td>Enter the user ID of the user who performed the action.</td>
</tr>
</tbody>
</table>
**Event Management**

**Session event property set**

Session events occur to notify you of session changes.

**Table 35  Session event property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the session events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity level of the event. The options are informational, warning, and fatal.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the product that encountered an event.</td>
</tr>
<tr>
<td>Source</td>
<td>Enter the user ID of the user who performed the action.</td>
</tr>
</tbody>
</table>

**SNMP trap event property set**

SNMP trap events occur when the Connectrix Manager application Server receives an SNMP trap.

**Table 36  SNMP trap event property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the SNMP trap events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Select the severity of the event. Values include informational, warning, and fatal.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter a string for the target product’s IP address.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter a string for the product’s world wide name (WWN).</td>
</tr>
<tr>
<td>Source</td>
<td>Enter a string for the target source’s cause of the event (for example, user ID or device label).</td>
</tr>
</tbody>
</table>
User action event property set

User action events occur when you change a setting in the Server.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter a target string that is contained in the description of the user action events you want to target.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Displays the severity level of the event, which is always informational.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Enter the IP address of the Client from which the action was taken.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Enter the world wide name (WWN) of the product that encountered an event.</td>
</tr>
<tr>
<td>Port WWN</td>
<td>Enter the world wide name (WWN) of the port that encountered an event.</td>
</tr>
<tr>
<td>Source</td>
<td>Enter the User ID of the user who performed the action.</td>
</tr>
</tbody>
</table>

User property set

The properties of a user.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clients For This User</td>
<td>Enter the number of Client sessions open for the specified user.</td>
</tr>
<tr>
<td>ID</td>
<td>Enter the user ID of the user who performed the action.</td>
</tr>
</tbody>
</table>
Writing Event Management macros

You can write macros for the Event Management feature to insert relevant data into the Text fields of some action phrases.

The following actions allow macros. Left-click to place the blinking cursor into one of the Text fields indicated below.

- Export/E-mail – subject field and message field
- Launch – arguments field
- Log – description field
- Message – message field

When you right-click in the text area near the blinking cursor, a menu of the context property sets will display. Select one of the choices to insert a bracketed macro at the cursor.

**Note:** You can insert macros into the middle of text strings that you have typed into the Text fields.

When the trigger fires, the values for the context properties that you selected will be inserted into the text in place of the macro. Write the text in such a way that you will know what the value is, since the property name is not inserted along with the value. For example, “The device labeled ${PROP Nickname} has come back online. Its Node Name is ${PROP WWN}.

**Note:** Actions that are triggered by a schedule trigger will not have access to Device and Event properties, because no device is directly involved in triggering the event.
Use the Event Context Property Set to insert properties of the event into an action’s Text field.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Inserts the description of the event.</td>
</tr>
<tr>
<td>Discovery Type</td>
<td>Inserts the in-band or out-of-band discovery type for this event.</td>
</tr>
<tr>
<td>Element Type</td>
<td>Inserts the element type. The values are Device or Link.</td>
</tr>
<tr>
<td>Event Level</td>
<td>Inserts the severity level of the event. The values are include informational, warning, or fatal.</td>
</tr>
<tr>
<td>Fabric Nickname</td>
<td>Inserts the nickname of the port’s fabric.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Inserts the IP address of the product that generated the event.</td>
</tr>
<tr>
<td>Management Link</td>
<td>Inserts the management link status. The values are Down or Up.</td>
</tr>
<tr>
<td>Measure Type</td>
<td>Inserts a performance measurement unit. The values are Transmit, Receive, CRC errors, Loss of Sync Errors, and Loss of Signal Errors.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Inserts the world wide name of the device that generated the event.</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Inserts the product’s status. The values are operational, degraded, failed, or unknown.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Inserts the port number of the port that encountered an event.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Inserts the port type. The values are N, NL, E, F, FL, T100, GigE, G, and R.</td>
</tr>
<tr>
<td>Port WWN</td>
<td>Inserts the world wide name of the port that encountered an event.</td>
</tr>
<tr>
<td>Source</td>
<td>Inserts the label or user ID of the product, process, or user that generated the event.</td>
</tr>
<tr>
<td>Threshold Type</td>
<td>Inserts the performance threshold type. The values are high critical, high warning, low warning, and low critical.</td>
</tr>
</tbody>
</table>
Use a Product Context macro to insert properties of the source product into an action’s Text field.

**Table 40  Product context property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class</td>
<td>Inserts the FICON class to which the node belongs.</td>
</tr>
<tr>
<td>Comments</td>
<td>Inserts the contents from the Comments field of the product’s Product Properties dialog box.</td>
</tr>
<tr>
<td>Contact</td>
<td>Inserts the contents from the Contact field of the product’s Properties dialog box.</td>
</tr>
<tr>
<td>Description</td>
<td>Inserts the contents from the Description field of the product’s Properties dialog box.</td>
</tr>
<tr>
<td>Device Type</td>
<td>Inserts the type of device. The values are HBA, Storage, Switch, Bridge, Hub, NAS, Tape, and Manager.</td>
</tr>
<tr>
<td>Domain ID</td>
<td>Inserts the device’s domain ID.</td>
</tr>
<tr>
<td>Enclosure Name</td>
<td>Inserts the name that has been given to an enclosure for a particular set of devices.</td>
</tr>
<tr>
<td>Firmware</td>
<td>Inserts the device’s firmware level.</td>
</tr>
<tr>
<td>Firmware (in-band)</td>
<td>Inserts the product’s firmware as discovered using in-band discovery methods.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Inserts the device’s IP address.</td>
</tr>
<tr>
<td>Location</td>
<td>Inserts the contents from the Location field of the product’s Properties dialog box.</td>
</tr>
<tr>
<td>Managed By</td>
<td>Inserts the server name of the Connectrix Manager Application Server that has full management of the switch product.</td>
</tr>
<tr>
<td>Management Link</td>
<td>Inserts the status of the management link between the local Connectrix Manager application of this product. The values are Up or Down.</td>
</tr>
<tr>
<td>Model Number</td>
<td>Inserts the product’s model number.</td>
</tr>
<tr>
<td>Model Number (in-band)</td>
<td>Inserts the product’s model number as discovered using in-band discovery methods.</td>
</tr>
</tbody>
</table>
Event Management

Table 40  **Product context property set (continued)**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Inserts the device’s name, as specified in the Product Properties dialog box.</td>
</tr>
<tr>
<td>Name (in-band)</td>
<td>Inserts the product’s name as discovered using in-band discovery methods.</td>
</tr>
<tr>
<td>Nickname</td>
<td>Inserts the user-specified nickname of the product.</td>
</tr>
<tr>
<td>Node WWN</td>
<td>Inserts the product's world wide name (WWN).</td>
</tr>
<tr>
<td>Operational Status</td>
<td>Inserts the product's status. The options are operational, degraded, failed, or unknown.</td>
</tr>
<tr>
<td>Port Count</td>
<td>Inserts the number of ports on the product.</td>
</tr>
<tr>
<td>Port Count (in-band)</td>
<td>Inserts the product’s port count as discovered using in-band discovery methods.</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Inserts the product's serial number.</td>
</tr>
<tr>
<td>Serial Number (in-band)</td>
<td>Inserts the product’s serial number as discovered using in-band discovery methods.</td>
</tr>
<tr>
<td>Tag Number</td>
<td>Inserts the FICON tag number of the product.</td>
</tr>
<tr>
<td>Vendor</td>
<td>Inserts the product’s vendor.</td>
</tr>
<tr>
<td>Vendor (in-band)</td>
<td>Inserts the product’s vendor as discovered using in-band discovery methods.</td>
</tr>
<tr>
<td>Vendor ID</td>
<td>Inserts the vendor’s identification information.</td>
</tr>
</tbody>
</table>

Port context property set

Use a Port Context macro to insert properties of the source port into an action’s Text field.

Table 41  **Port context property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active FC4 Types</td>
<td>Inserts the port’s active Fibre Channel 4 types.</td>
</tr>
<tr>
<td>Blocked Configuration</td>
<td>Inserts the blocked configuration of the port.</td>
</tr>
<tr>
<td>Blocked Reason</td>
<td>Inserts the reason why the port is blocked.</td>
</tr>
<tr>
<td>Property</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Class of Service</td>
<td>Inserts the port’s class of service.</td>
</tr>
<tr>
<td>Fabric Nickname</td>
<td>Inserts the fabric nickname of the fabric to which the port is connected.</td>
</tr>
<tr>
<td>FC Address</td>
<td>Inserts the port’s Fibre Channel address.</td>
</tr>
<tr>
<td>Max. Frame Size (bytes)</td>
<td>Inserts the port’s maximum frame size, in bytes.</td>
</tr>
<tr>
<td>Name</td>
<td>Inserts the name of the port that was specified through the Switch Element Manager.</td>
</tr>
<tr>
<td>Name (in-band)</td>
<td>Inserts the port’s name, as discovered using in-band discovery methods.</td>
</tr>
<tr>
<td>Operational State</td>
<td>Inserts the operational state of the port.</td>
</tr>
<tr>
<td>Port Address</td>
<td>Inserts the address of the port.</td>
</tr>
<tr>
<td>Port Nickname</td>
<td>Inserts a user-specified nickname for the port.</td>
</tr>
<tr>
<td>Port Number</td>
<td>Inserts the number of the port.</td>
</tr>
<tr>
<td>Port Type</td>
<td>Inserts the port type. The values are N, NL, E, F, FL, T100, GigE, G, and R.</td>
</tr>
<tr>
<td>Port WWN</td>
<td>Inserts the world wide name of the port.</td>
</tr>
<tr>
<td>Receive % Utilization</td>
<td>Inserts the receive percent utilization of the port.</td>
</tr>
<tr>
<td>Speed Configured (Gbps)</td>
<td>Inserts the current speed of the port.</td>
</tr>
<tr>
<td>Speed Supported (Gbps)</td>
<td>Inserts the maximum speed of the port.</td>
</tr>
<tr>
<td>State</td>
<td>Inserts the port state. The values are Down or Up.</td>
</tr>
<tr>
<td>Supported FC4 Types</td>
<td>Inserts the Fibre Channel 4 types that the port supports.</td>
</tr>
<tr>
<td>Transmit % Utilization</td>
<td>Inserts the transmit percent utilization of the port.</td>
</tr>
<tr>
<td>VF ID</td>
<td>Inserts the virtual fabric ID for the switch, if applicable.</td>
</tr>
</tbody>
</table>
TIME context property set

Use the TIME Context macro to insert properties of the time and date of the event or schedule into an action’s Text field.

There are an infinite number of time and date formats. The Connectrix Manager application provides three default formats as well as an option for users to define any format they choose given standard Java rules listed below.

- MM/dd/yyyy k:mm—Displays month/day/year hour:minutes (using the 24-hour format)
  Example: 08/12/2004 15:37
- hh:mm:ss – Displays hours:minutes:seconds
  Example 08:32:11
- Raw – Displays a single integer count of “The difference, measured in milliseconds, between the current time and midnight, January 1, 1970 UTC”.
- <User Defined> - Allows the user to follow the Java rules to create any Time and Date format. For information about Java rules, refer to http://java.sun.com/j2se/1.4.2/docs/api/java/text/SimpleDateFormat.html.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM/dd/yyyy k:mm:ss</td>
<td>Inserts the specified date and time by month, day, year, hour, minute, and second.</td>
</tr>
<tr>
<td>hh:mm:ss</td>
<td>Inserts the specified time by hour, minute, and second.</td>
</tr>
<tr>
<td>raw</td>
<td>Inserts the time, in milliseconds, since Jan 1, 1970 UTC. For example, 1027966562386</td>
</tr>
<tr>
<td>&lt;User-defined&gt;</td>
<td>This format comes from the Java SimpleDateFormat class. Refer to for additional information.</td>
</tr>
</tbody>
</table>
Use the System Context macro to insert properties of this Connectrix Manager application’s server into an action’s Text field.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client Count</td>
<td>Inserts the number of application clients logged into this Connectrix Manager application’s server.</td>
</tr>
<tr>
<td>Discovery Off</td>
<td>Inserts a true or false value to indicate whether discovery is turned on or off.</td>
</tr>
<tr>
<td>Event Notification Off</td>
<td>Inserts a true or false value to indicate whether event notification is turned on or off.</td>
</tr>
<tr>
<td>Free Memory</td>
<td>Inserts how much physical memory is available.</td>
</tr>
<tr>
<td>IP Address</td>
<td>Inserts the server’s IP address.</td>
</tr>
<tr>
<td>OS Architecture</td>
<td>Inserts the architecture of the operating system.</td>
</tr>
<tr>
<td>OS Name</td>
<td>Inserts the operating system name. The values are Sun, Linux, HP-UX, AIX, and Windows 98, NT, 2000, 2003, and XP.</td>
</tr>
<tr>
<td>OS Version</td>
<td>Inserts the version of the operating system.</td>
</tr>
<tr>
<td>Region</td>
<td>Inserts the region of the world where the server is located.</td>
</tr>
<tr>
<td>Server Name</td>
<td>Inserts the name of the Connectrix Manager application’s server.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>Inserts the Connectrix Manager application server’s subnet mask.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Inserts the server’s time zone.</td>
</tr>
<tr>
<td>Total Memory</td>
<td>Inserts the amount of total physical memory.</td>
</tr>
<tr>
<td>Trap Forwarding Off</td>
<td>Inserts true or false to indicate whether SNMP trap forwarding is enabled.</td>
</tr>
<tr>
<td>User Count</td>
<td>Inserts the number of users.</td>
</tr>
<tr>
<td>VM Name</td>
<td>Inserts the name of the Java Virtual Machine.</td>
</tr>
<tr>
<td>VM Vendor</td>
<td>Inserts the vendor of the Java Virtual Machine.</td>
</tr>
<tr>
<td>VM Version</td>
<td>Inserts the version of the Java Virtual Machine.</td>
</tr>
</tbody>
</table>
**Event Management**

---

**User context property set**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>The ID of the user who performed the action.</td>
</tr>
<tr>
<td>Clients For This User</td>
<td>The number of Client sessions open for the specified user.</td>
</tr>
</tbody>
</table>

---

**FILE Macro**

The File Macro inserts the contents of the file whose path and file name you specify in the macro. When you select this macro from the macro menu, it inserts the following into the Text field: `${FILE [filename]}`, leaving a single space after FILE [filename], with the file system path and file name of the file whose data you want inserted in the Text field.

---

**EXEC context property set**

The EXEC Context Property Set executes the command that is contained in the macro, then replaces it with the output of that command. When you select this macro from the macro menu, it inserts the following into the Text field: `${EXEC}`. The commands that are run through the EXEC macro are operating system-specific and require the following format.

**Note:** The commands listed in this section are examples and by no means represent a complete list. For a complete list of operating system-specific commands, refer to the documentation for your operating system.

---

**Windows 98**

Some of the supported commands to run through the EXEC macro for Windows 98 operating systems are as follows:

**Note:** A double back slash is required in the file path.

- `${(EXEC command.com /c copy c:\test1.txt c:\test2.txt)},`  
- `${(EXEC command.com /c del c:\test1.txt)},`  
- `${(EXEC command.com /d ping wheaties.mcdata.com)},`
Writing Event Management macros

Windows NT/ W2K/ XP/ 2000 Advanced Server

Some of the supported commands to run through the EXEC macro for Windows NT/ W2K/ XP operating systems are as follows:

$\{(EXEC \texttt{command.com /c type} c:\\test1.txt),

$\{(EXEC \texttt{cmd.exe /c copy} c:\\src c:\\test),

$\{(EXEC \texttt{cmd.exe /c del} c:\\test.txt),

$\{(EXEC \texttt{cmd.exe /d ping} wheaties.mcdata.com),

$\{(EXEC \texttt{cmd.exe /c type} c:\\test1.txt),

Linux

Some of the supported commands to run through the EXEC macro for Linux operating systems are as follows:

$\{(EXEC /bin/cat /usr/home/user1/test.txt),

$\{(EXEC /bin/ping wheaties.mcdata.com),

UNIX

Some of the supported commands to run through the EXEC macro for UNIX operating systems are as follows:

$\{(EXEC /usr/bin/cat /usr/home/user1/test.txt),

$\{(EXEC /usr/sbin/ping wheaties.mcdata.com),

Specifying arguments to the Internet Launcher scripts

This section explains how to specify input arguments to the Internet browser scripts to prevent errors from occurring.

1. Click the Event Management tab on the main window.
2. Click New.
   The Add Rule dialog box displays.
3. From the Type list, select User Action Event.
4. In the Value text box, type Informational.
5. Click Add.
6. From the Action list, Select Launch from the Actions list at the bottom left of the Add Rule dialog box.
7. Select Example_launchIE.bat from the script list.
8. Depending on the operating system and Internet browser you are using, enter a filename into the Arguments textbox using the examples Click OK.
The text file that you specified launches.

**Windows systems running Internet Explorer**

For Windows systems running Internet Explorer, you must do the following:

- Surround a path name that contains white space with double quotes

Insert a double back slash in the file path.

**Linux and UNIX systems running Netscape**

For Linux and UNIX systems running Netscape, type
Advanced event filtering

Advanced event filtering enables you to perform additional filtering on selected events. If you do not want to display certain events in the Event Management dialog box Master Log, you can perform the following steps.

1. Click the Event Management tab on the main window.
   The Event Management dialog box displays.

2. Note the events and descriptions that need to be removed and click the Filter link that is to the right of the Master Log on the bottom of the Event Management dialog box.
   The Define Filter dialog box displays.

3. Select the Include extended events checkbox to display all events that previously displayed for SANavigator.
   Leave this checkbox unchecked to display all events that previously displayed for Connectrix Manager.

4. Select or remove an event type from the Selected Events table.
   - Using the right arrow button, move the event type from the Available Events column to the Selected Events column.
   - Using the left arrow button, remove the event type from the Selected Events column to the Available Events column.

5. Click Advanced Filtering.
   The Advanced Event Filtering dialog box displays.

6. From the Event Type drop-down list, select an event type that you removed from the Event Management dialog box Master Log in the previous steps. Events are listed in alphabetical order.

7. Enter up to 40 characters into the Description Contains text box.
   This text should be the same text that displayed in the Description field for the events that displayed on the Event Management dialog box Master Log.

8. Using the right arrow button, move the event type to the Additional Filters column.

9. Click OK.
   The Define Filter dialog box displays.
10. Click **OK** to save the advanced filter selections.

The Event Management dialog box displays with the revised Master Log information.
This chapter contains instructions and procedure descriptions for using SAN Routing.

- What is SAN routing? ................................................................. 420
- SAN routing definitions .......................................................... 420
- SAN routing groups ............................................................... 423
- Discovering a SAN router ....................................................... 426
- Router port configuration ....................................................... 427
- Zoning scopes ......................................................................... 434
- SAN router configuration ...................................................... 437
- Configuration archive ............................................................. 444
- Applying properties for router consistency ............................. 447
- Creating a log file ................................................................. 448
- Saving changes to Flash memory ............................................ 448
SAN Routing

What is SAN routing?

A SAN router is a Fibre Channel (FC) switch that contains IP routing capabilities.

In SAN routing, connection between ports is terminated at each SAN island. This ensures that transactions can be carried out without the danger that problems at any single SAN island will spread to others. The probability of a major network disruption is thereby minimized, and problems can be isolated and resolved quickly. SAN routing also eliminates confusion if addresses overlap between SAN islands in the context of a larger network.

SAN routing is scalable, making it possible to build a large, evolving, and geographically diverse SAN while ensuring stability and interoperability. The technology is ideally suited for remote storage in enterprises having numerous sites in widely-separated locations.

Note: When the SAN management’s ethernet environment is implemented with a public and private network where the Connectrix Manager clients are on the public and the switches are on the private, it is necessary to add the Router products to the public network in order for the Connectrix Manager clients to launch the Router’s Element Manager.

SAN routing definitions

The following terms are associated with SAN routing. For a glossary of general terms, refer to the online help.

iFCP (Internet Fibre Channel Protocol)

iFCP is a gateway-to-gateway protocol for the implementation of an FC fabric in which TCP/IP switching and routing elements replace FC components. The protocol enables the attachment of existing FC storage products to an IP network by supporting the fabric services required by such devices.

iSCSI Storage Cluster

An iSCSI storage cluster is a storage device with FC and Internet Protocol (IP) on the same machine.

A cluster is a group of products that are interconnected by a high-speed network (typically dedicated). When a server in a cluster...
SAN Routing definitions

fails, one of the other servers in the cluster assumes the responsibility of the failed server, thereby ensuring server, application, and data availability.

**mFCP (Metro Fibre Channel Protocol)**

An mFCP is a protocol in which two SAN Routers in a Metropolitan SAN (mSAN) are connected by a Node to Node connection line, which displays as a single, black line. If the mFCP connection goes down, the connection line disappears.

Storage devices, HBAs, servers, and hosts can be routed “out” from one fabric to another. To be routed “out” means that the device can communicate, using mFCP, with devices in a foreign fabric, and the device can participate in the foreign fabric’s zoning.

**mSAN (Metropolitan SAN)**

An mSAN is a configuration where two or more SANs in a campus setting or metropolitan area are interconnected by SAN routers, using FC connections and protocol.

**R_Port**

An R_Port is any port on a SAN Router that connects to the E_Port of a FC switch to create an interswitch link (ISL).

**R_Port Domain IDs**

In a routed SAN, each R_Port is assigned its own Domain ID. This makes it possible to interconnect fabrics in an mSAN or Internetworked SAN (iSAN) without merging the fabrics.

**Router Fabric**

Router fabrics use SAN routers rather than FC switches. Router fabrics contain a SAN router, or a collection of SAN routers, joined together with mFCP, direct attached storage, hosts, HBAs, and directly-associated iSCSI devices.

A router fabric has similar properties to an FC fabric; however, while an FC fabric contains FC switches and the devices that are attached to them, a router fabric contains SAN routers and the devices that are attached to them. A router fabric is created when one or more SAN routers are discovered.
**Simple and Blended Fabrics**

mSANs or iSANs can be made up of simple (pure) FC fabrics or Blended Fabrics or both.

- **Simple (Pure) Fabrics**: Hosts and storage devices use only the FC protocol.
- **Blended Fabrics**: Hosts and storage devices use both FC and the native IP protocols. The IP protocols could be iSCSI, mFCP or iFCP.
The following sections discuss SAN routing groups-related facts.

**FC fabric groups**

To support SAN routing, the FC fabric group contains routed products, virtual connection lines, cross-fabric connection lines, and multiple connection lines from a unique port.

A FC Fabric Group consists of the following groups and containers:

<table>
<thead>
<tr>
<th>FC fabric group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC Switch</td>
<td>FC switches, iSCSI gateways, and FCIP gateways are all contained within a single FC switch group.</td>
</tr>
<tr>
<td>Storage</td>
<td>Attached storage devices are all contained within a storage group.</td>
</tr>
<tr>
<td>Host</td>
<td>Attached hosts and HBAs are all contained within a host group. A server group can be contained within the host group.</td>
</tr>
<tr>
<td>Routed Products</td>
<td>Devices that have been routed into the fabric are all contained within a routed products group.</td>
</tr>
</tbody>
</table>

**iSCSI groups**

The iSCSI Group consists of iSCSI storage clusters and directly-attached initiators.

<table>
<thead>
<tr>
<th>iSCSI group</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>A storage device that is discovered connected to an iSCSI initiator using IP (is not FC-connected) is contained within a storage group. &lt;br&gt;• iSCSI storage devices contained within the parented container are placed into the storage group.</td>
</tr>
<tr>
<td>Host</td>
<td>An iSCSI Initiator that is discovered by way of an iSCSI storage cluster (and is not FC-connected), is contained within a host group. &lt;br&gt;• iSCSI hosts, servers, and NPIV groups contained within the parented container are placed into the host group. &lt;br&gt;• iSCSI hosts and HBAs are contained within the host group.</td>
</tr>
</tbody>
</table>
**Isolated device group**

FC devices and Fabric Managers for which discovery cannot associate fabric participation are contained within the isolated device group.

**Loop group**

Devices that discovery has detected have loop connectivity are placed into a loop group, which is located inside a storage group.

**mSAN group**

FC Fabrics and Router Fabrics that are connected by an interswitch link (the R_Port router to the E_port router on a switch).

**NPIV group**

The NPIV group is comprised of a loop object and attached HBAs.

**Router fabric groups**

A router fabric group consists of the following group containers:

<table>
<thead>
<tr>
<th>Group container</th>
<th>Description</th>
</tr>
</thead>
</table>
| Host            | • Direct-attached hosts and HBAs are all contained within a host group.  
• All host devices that are members of a targeted Router Fabric or FC Fabric are contained within a host group. |
| Routed Products | • Devices that have been routed into the fabric are all contained within a routed products group, and are grouped by their point of origin.  
• In the FC Fabric, a virtual group is also included within the routed products group. |
## SAN router groups

<table>
<thead>
<tr>
<th>Group container</th>
<th>Description</th>
</tr>
</thead>
</table>
| SAN router groups | ▪ Server groups within the host group can contain both HBAs and iSCSI initiators (direct-attached only).  
  NOTE: Routed representations of HBA or iSCSI devices may not be included in a server group.  
  ▪ Server groups are contained within a host group. |

### Server

- Direct-attached storage devices are contained within a storage group.
- All storage devices that are members of a Router Fabric or FC Fabric, including tape drives, are contained within a storage group.
- Loops, bridges, and NPIV loop storage devices discovered within the Fabric are contained within a storage group.
- All iSCSI storage products that are directly registered with one or more of the SAN routers in the router fabric are contained within a storage group.
- All iSCSI Initiators and HBAs that are directly registered with one or more of the SAN routers in the router fabric are all contained within the hosts group.

### Storage

**Switch group**

FC switches are placed into a switch group with all other switches in a specific fabric.

**Virtual group**

Artifacts (router proxies) created in the FC fabric by the connection between the SAN router and the FC switch are contained within a virtual group.

**Note:** Artifacts include proxy domain 7E and 7F and virtual domain (E_Port to R_Port connectivity).
Discovering a SAN router

Before you can configure the SAN Routers, you must first discover them using the Connectrix Manager application. Discovery is the process by which the application contacts the devices in your SAN. When you log in to a Server, the local network is automatically discovered and displayed on the Physical Map.

For detailed instructions about how to discover specific IP addresses, refer to the *EMC Connectrix Manager* available at http://Powerlink.emc.com.
Router port configuration

The **Router Port Configuration** dialog box enables you to view the R_Ports on a SAN router.

You can open the **Router Port Configuration** dialog box in the following ways:

1. Select **SAN router** from the Connectivity Map or Product List.
2. Select **Configure > SAN Routing > Router Port Configuration** or right-click the **SAN Router** icon and select **Router Port Configuration**.

The **Router Port Configuration** dialog box displays.

3. Select the fabric using the **Router Fabric** list in the upper left corner of the dialog box.
**Assigning a fabric to an R_port**

Use the following procedure to assign a fabric to an R_port:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Router Port Configuration, or right-click the SAN Router icon and select Router Port Configuration.
4. Select the appropriate fabric from the Router Fabric list.
   
   The Available Configuration and Router Fabric tables display configuration and router/port information for the selected fabric.
5. Select an R_port in the Router Fabric table.
   
   If a router is selected in the Router Fabric table rather than an R_port, all ports on that router are assigned to the fabric.
6. Click the right arrow button.
   
   The selected fabric is assigned to the selected R port.
7. Click Apply to save the change.
   
   The Router Change Confirmation and Status dialog box displays.
8. Click OK.
   
   Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the Status area.
9. Click Close to exit the Router Change Confirmation and Status dialog box.

**Setting an insistent domain ID for an R_port**

Setting an insistent domain ID ensures that the preferred domain ID of the switch becomes its assigned domain ID. Insistent domain IDs ensure that duplicate domain IDs are not used within a fabric.

Use the following procedure to flag an R_port domain ID as an insistent domain ID:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Router Port Configuration, or right-click the SAN Router icon and select Router Port Configuration.

3. Find the R port in the Router Fabric table.

4. Select the appropriate fabric from the Router Fabric list.

   The Available Configuration and Router Fabric tables display configuration and router/port information for the selected fabric.

5. Scroll right to find the Insistent Domain ID check box.

6. Click the check box to enable the insistent domain ID.

7. Click Apply to save the change.

   The Router Change Confirmation and Status dialog box displays.

8. Review the Insistent Domain ID field, and click OK.

   Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the Status area.

9. Click Close to exit the Router Change Confirmation and Status dialog box.

---

Establishing or changing a preferred domain ID for an R port

Setting an insistent domain ID ensures that the preferred domain ID of the switch becomes its assigned domain ID.

Use the following procedure to establish or change a preferred domain ID for an R port:

1. Select the SAN router from the Connectivity Map or Product List.

2. Select Configure > SAN Routing > Router Port Configuration, or right-click the SAN Router icon and select Router Port Configuration.

3. Find the R port in the Router Fabric table.

4. Select the appropriate fabric from the Router Fabric list.

   The Available Configuration and Router Fabric tables display configuration and router/port information for the selected fabric.

5. Scroll right to find the Preferred Domain ID field.
6. Click the field to make it editable, and enter the preferred domain ID.

7. Click Apply to save the change.
   - The Router Change Confirmation and Status dialog box displays.

8. Review the Preferred Domain ID field, and click OK.
   - Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the Status area.

9. Click Close to exit the Router Change Confirmation and Status dialog box.

---

### Setting port binding for an R_port

Port binding defines a port membership list with the world wide port name (WWPN) of a switch. The connection cannot be moved from one port to another on the switch without changes to the port membership list.

Use the following procedure to set the port binding for an R_port:

1. Select the SAN router from the Connectivity Map or Product List.

2. Select Configure > SAN Routing > Router Port Configuration, or right-click the SAN Router icon and select Router Port Configuration.

3. Select the appropriate fabric from the Router Fabric list.
   - The Available Configuration and Router Fabric tables display configuration and router/port information for the selected fabric.


5. Scroll right to find the Port Binding check box.

6. Click the check box to enable Port Binding.

7. Click Apply to save the change.
   - The Router Change Confirmation and Status dialog box displays.

8. Review the port binding setting, and click OK.
   - Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the Status area.
9. Click Close to exit the Router Change Confirmation and Status dialog box.

Displaying the status of an R_port

Use the following procedure to display the status of an R_port:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Router Port Configuration, or right-click the SAN Router icon and select Router Port Configuration.
3. Select the appropriate fabric from the Router Fabric list.

The Available Configuration and Router Fabric tables display configuration and router/port information for the selected fabric.
4. Select R_port in the Router Fabric table by looking through the table (explained in Finding an R_port in a router fabric configuration), or by selecting a router fabric configuration from the Available Configurations table and clicking Find.

The selected R_port’s status displays in the Port Status area.

Editing the port binding for an R_port

Use the following procedure to establish or change an R_port bound address:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Router Port Configuration, or right-click the SAN Router icon and select Router Port Configuration.
3. Select the appropriate fabric from the Router Fabric list.

The Available Configuration and Router Fabric tables display configuration and router/port information for the selected fabric.
5. Scroll right to find the Bound Address field.
6. Click the field to make it editable, and edit the existing port binding address.
7. Review the port binding setting, and click the Apply button.
Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the Status area.

8. Click Close to exit the Router Change Confirmation and Status dialog box.

Displaying all fabric switches assigned to an R_port

Use the following procedure to display all fabric switches assigned to an R_port:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Router Port Configuration, or right-click the SAN Router icon and select Router Port Configuration.
3. Select the appropriate fabric from the Router Fabric list.
   The Available Configuration and Router Fabric tables display configuration and router/port information for the selected fabric.
4. Select an R_port in the Router Fabric table.
5. Click the Display All button.
   A dialog box is displayed that lists the WWN, the IP address, and the domain ID of each fabric switch that is attached to the selected SAN Router R-port.

Note: If there is no physical connection on the SAN Router R-port, the Display All button is grayed out.

6. Click OK to close the dialog box.

Finding an R_port in a router fabric configuration

To find a specific R_port in a router fabric configuration from the Router Port Configuration dialog box, either search through the Router Fabric table, or do the following:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Router Port Configuration, or right-click the SAN Router icon and select Router Port Configuration.
3. Select the configuration in the Available Configuration table.
4. Select the appropriate fabric from the **Router Fabric** list.

   The **Available Configuration** and **Router Fabric** tables display configuration and router/port information for the selected fabric.

5. Click the **Find** button.

   The R_port is highlighted in the **Router Fabric** table.
**Zoning scopes**

The Connectrix Manager application supports the following three zoning scopes:

- FC Fabric – zones are managed in the Fibre Channel (FC) fabric.
- Router Fabric – zones are managed in the Router fabric.
- mSAN Fabric – zones are managed in both FC and Router fabrics, depending on how the zone policy is set.

To configure the three zoning scopes, select **Configure > Zoning**.

To edit router fabric zoning configuration properties, follow the procedures in the following sections.

**Router fabric zone configuration properties**

Use the following procedure to display the **Configuration Properties** dialog box.

1. Select the SAN router from the Connectivity Map or Product List.
2. Select **Configure > SAN Routing > Router Port Configuration**, or right-click the **SAN Router** icon and select **Router Port Configuration**.
3. Select the appropriate fabric from the **Router Fabric** list.
   - The **Available Configuration** tables display configuration information for the selected fabric.
4. Click the **Edit** button.

The **Configuration Properties** dialog box is displayed. This dialog box enables you to perform the following tasks:

- Edit the router fabric name.
- Change the interop mode.
- Change the zone policy.
- Enable or disable fabric binding.
- View proxy node WWNs and domain IDs.
**Editing the router fabric name**

Use the following procedure to edit the router fabric zone name:

1. In the Configuration Properties dialog box, highlight and delete the existing router fabric name.
2. Key in the new name for the router fabric. Note the following:
   - Recommended character limit: 60 characters.
   - No duplicate names are allowed.
3. Click OK to save your changes and close the Configuration Properties dialog box.

**Changing the interop mode**

When a router fabric is in interop mode, it is configured so that the SAN can contain heterogeneous router fabrics (router fabrics belonging to different vendors).

Use the following procedure to change the interop mode:

1. In the Configuration Properties dialog box, select a mode from the Interop Mode list:
   - McDATA - McDATA-only router fabrics.
   - Open Fabric 1.0 – merges McDATA and Brocade router fabrics into interop mode.
   - Brocade – Brocade-only router fabrics.
2. Click OK to save your changes and close the Configuration Properties dialog box.

**Changing the zone policy**

The SAN Router automatically updates the fabric with any storage over IP (SoIP) information using the Append Router Zones policy. If a fabric has an SoIP zone with different members than the SAN Router, the SAN Router pushes the latest zones (which are prefixed by “SoIP”) to the fabrics.

**Note:** The Append Router Zones zone policy is the default.

Use the following procedure to change the zone policy:
1. In the **Configuration Properties** dialog box, click the Zone Policy list.

2. Select **No Zone Synch**.

   When the zone policy is set to **No Zone Synch**, the Connectrix Manager application analyzes the zone membership and creates the zones in the affected fabrics. This zone policy provides more flexibility, but renders the zone unscaleable.

3. Click **OK** to save your changes and close the **Configuration Properties** dialog box.

---

**Enabling or disabling fabric binding**

Fabric Binding authorizes the joining of switches based on both WWN and Domain ID, ensuring consistent, unified behavior across all potential fabric access points. When you enable fabric binding, you prevent non-authorized switches access into the fabric.

**Note:** Fabric Binding is only supported on Connectrix M switches and fabrics.

Use the following procedure to enable fabric binding:

1. In the **Configuration Properties** dialog box, perform one of the following actions based on the task you want to complete:
   
   - To enable fabric binding, click **Enable**, and then click **OK**.
   - To disable fabric binding, leave the Fabric Binding check box unchecked. Disable Fabric Binding is the default.

   The **Configuration Properties** dialog box closes.

---

**Viewing proxy node WWNs and Domain IDs**

The Proxy Node table displays the world wide name (WWN) and Domain ID pairs that form a fabric. You cannot edit the WWN or Domain ID.
The **SAN Router Configuration** dialog box allows you to configure any of the following for an individual SAN router or a group of SAN routers:

- Cluster ID
- SNTP
- Date and Time
- SNMP Traps
- iFCP ID

The **SAN Router Configuration** dialog box can be opened in either of the following ways:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select **Configure > SAN Routing > SAN Router Configuration**, or right-click the **SAN Router** icon and select **SAN Router Configuration**.

The **SAN Router Configuration** dialog box displays.

![SAN Router Configuration dialog box](image)
Assigning a cluster ID

The cluster ID is the first level in hierarchy for Metropolitan SAN (mSAN) definition. The allowed range is 1-63, and the default is 1. It is recommended that all SAN routers in an mSAN have the same cluster ID value.

Use the following procedure to assign a cluster ID:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > SAN Router Configuration, or right-click the SAN Router icon and select SAN Router Configuration.
3. Select the mSAN, router fabric, or router to which you want to assign a cluster ID in the hierarchy (or mSAN/Router Fabric/Router table) on the right side of the dialog box.
4. Click the Cluster ID tab.
5. Enter a cluster ID number in the Cluster ID field or click Auto Generate for the system to automatically assign a cluster identifier.
6. Click the Save to Flash check box to save the cluster ID to flash memory.
7. Click OK in the SAN Router Configuration dialog box.
   The Router Change Confirmation and Status dialog box displays.
8. Highlight the change in the Detailed Changes table, and click OK.
   Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the Status area.
9. Click Close in the Router Change Confirmation and Status dialog box.
Enabling SNTP

**Note:** You can only change the computer’s clock through the **Date & Time** tab when Simple Network Time Protocol (SNTP) is disabled.

Use the following procedure to enable SNTP:

1. Select the mSAN, router fabric, or router to which you want to enable SNTP from the Connectivity Map or Product List.
2. Select **Configure > SAN Routing > SAN Router Configuration**, or right-click the **SAN Router** icon and select **SAN Router Configuration**.
3. Click the **Date & Time** tab.
4. Click the **Enable SNTP** check box.
5. Select either the **SNTP server** or **SNTP client** button.
6. If you select the SNTP client, enter the server’s IP address in the **Server Address** field.
7. Select the time zone from the **Time Zone** list.
   You can select the **Daylight Savings** check box only if the time zone you selected from the **Time Zone** list has daylight savings time.
8. Click the **Save to Flash** check box to save this configuration to flash memory.
9. Click **OK** in the **SAN Router Configuration** dialog box.
   The **Router Change Confirmation and Status** dialog box displays.
10. Highlight the change in the Detailed Changes table, and click **OK**.
   Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the **Status** area.
11. Click **Close** in the **Router Change Confirmation and Status** dialog box.
Setting the date and time

Use the following procedure to set the computer’s clock:

1. Select the mSAN, router fabric, or router for which you want to set or edit the date and time from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > SAN Router Configuration, or right-click the SAN Router icon and select SAN Router Configuration.
3. Click the Date & Time tab.
4. Clear the Enable SNTP check box. You can set the date and time only when SNTP is disabled.
5. Select one of the following three buttons:
   - Local – Click to synchronize the clock to the local time zone.
   - GMT – Click to synchronize time to the SNTP network; the GMT time is accurate to within one second of the world time.
   - Manually configured – Click to manually select both the date and the time from the list.
6. Click the Save to Flash check box to save this configuration to flash memory.
7. Click OK in the SAN Router Configuration dialog box.
   The Router Change Confirmation and Status dialog box displays.
8. Highlight the change in the Detailed Changes table, and click OK.
   Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the Status area.
9. Click Close in the Router Change Confirmation and Status dialog box.
Assigning SNMP traps

An SNMP (Simple Network Management Protocol) trap is an event notification originating from an SNMP-managed device and directed to an SNMP network management station.

Use the following procedure to assign an SNMP trap:

1. Select the mSAN, router fabric, or router to which you want to assign an SNMP trap from the Connectivity Map or Product List.

2. Select Configure > SAN Routing > SAN Router Configuration, or right-click the SAN Router icon and select SAN Router Configuration.

3. Click the Traps tab.

4. Select New to add a new SNMP trap.

   Alternatively, you can select a trap from the Available Trap Recipients table.

5. Type in the IP address of the trap destination.

6. Click the Save to Flash check box to save this configuration to flash memory.

7. Click OK in the SAN Router Configuration dialog box.

   The Router Change Confirmation and Status dialog box displays.

8. Highlight the change in the Detailed Changes table, and click OK.

   Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the Status area.

9. Click Close in the Router Change Confirmation and Status dialog box.
Removing an SNMP trap

To remove a trap list from a SAN router, select the device from the list of Available Trap Recipients, and click **Delete**.

Assigning an iFCP ID

Internet Fibre Channel Protocol (iFCP) is a gateway-to-gateway protocol for the implementation of an FC fabric in which TCP/IP switching and routing elements replace FC components.

The allowed iFCP ID range is 0 to 4294967295. It is recommended that all SAN Routers in an mSAN have the same iFCP ID value, and, for easier management, that each mSAN has a different iFCP SAN ID.

**Note:** After you have assigned an iFCP ID, you must reboot for the change to take effect.

Use the following procedure to assign an iFCP ID:

1. Select the mSAN, router fabric, or router to which you want to assign an iFCP ID from the Connectivity Map or Product List.
2. Select **Configure > SAN Routing > SAN Router Configuration**, or right-click the **SAN Router** icon and select **SAN Router Configuration**.
3. Click the **iFCP ID** tab.
4. Enter an iFCP ID number in the **iFCP ID** field or select **Auto Generate**.
5. Click the **Save to Flash** check box to save the iFCP ID to flash memory.
6. Click **OK** in the **SAN Router Configuration** dialog box.
   The **Router Change Confirmation and Status** dialog box displays.
7. Highlight the change in the Detailed Changes table, and click **OK**.
   Notifications that the changes are being applied, and a successful or unsuccessful completion are displayed in the **Status** area.
8. Click **Close** in the **Router Change Confirmation and Status** dialog box.
Reviewing and confirming SAN router configuration changes

Use the following procedure to review and confirm SAN router configuration changes:

1. Select the SAN router from the Connectivity Map or Product List.

2. Select Configure > SAN Routing > SAN Router Configuration, or right-click the SAN Router icon and select SAN Router Configuration.

3. Make a change in the SAN Router Configuration or Router Port Configuration dialog box, and click OK.

   The Router Change Confirmation and Status dialog box displays.

4. Review the changes listed in the Detailed Changes table.

5. Click OK to accept the changes.
Configuration archive

The Configuration Archive dialog box allows you to archive files and reports, which help customer service troubleshoot problems. The Configuration Archive dialog box also enables you to configure TFTP root path properties.

The Configuration Archive dialog box can be opened in either of the following ways:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Configuration Archive, or right-click the SAN Router icon and select Configuration Archive.

The Configuration Archive dialog box is displayed.

Archiving files and reports

Use the following procedure to archive configuration files and reports:

1. From the Configuration Archive dialog box, click the check box to select the file or report you want to archive.

You can archive one or both of the following files:

- Configuration backUp
- System Log
You can archive one or more of the following reports:

<table>
<thead>
<tr>
<th>Report name</th>
<th>Report description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Report</td>
<td>Contains the following configuration information:</td>
</tr>
<tr>
<td></td>
<td>• System properties</td>
</tr>
<tr>
<td></td>
<td>• Address configuration</td>
</tr>
<tr>
<td></td>
<td>• Boot configuration</td>
</tr>
<tr>
<td></td>
<td>• Trap configuration</td>
</tr>
<tr>
<td>R_Port</td>
<td>Contains configuration information for the SAN Router R_ports.</td>
</tr>
<tr>
<td>Consistency Report</td>
<td>Compares the configuration of the SAN Routers in a group and highlights the inconsistencies.</td>
</tr>
<tr>
<td>LUN Mapping</td>
<td>Displays LUN information for a selected SAN.</td>
</tr>
<tr>
<td>Name server</td>
<td>Launches an Internet browser and contacts the SAN Router to populate fields.</td>
</tr>
<tr>
<td>Active zone set</td>
<td>Contains the active zoning configuration in the selected fabric.</td>
</tr>
</tbody>
</table>

2. Enter the location and name for the archive in the **Archive file** field or click **Browse** to select the location and name.

   Make sure you include the full path.

3. Click **OK**.
TFTP root path

Trivial File Transfer Protocol (TFTP) is a simple form of FTP that provides no security features. The TFTP root directory is the base directory to which the TFTP server is allowed access.

Note: You cannot configure the TFTP root path from a remote client.

Configuring the TFTP root path

Use the following procedure to configure the TFTP root path:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Configuration Archive, or right-click the SAN Router icon and select Configuration Archive.
3. Click TFTP Properties.
4. Enter the location and name for the path in the TFTP Root Path field or click Browse to select the location and name. Make sure to include the full path.

   The system verifies that the path you selected or entered is valid, that the TFTP Server is running, and that you have access to the TFTP Server. If any of these conditions do not exist, an error message displays.

5. Click OK to save your changes and close the dialog box.
Applying properties for router consistency

When there is only one router in the fabric, the Router Consistency dialog box displays that router’s properties. If you have two or more SAN routers in your fabric, the Router Consistency dialog box shows a set of properties for each router and enables you to apply one set of properties to all routers across the fabric.

Use the following procedure to apply router properties:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Router Consistency, or right-click the SAN Router icon and select Router Consistency.
   The Router Consistency Properties dialog box is displayed.
3. Examine the displayed router properties, and determine which set you want to apply to all routers in the fabric.
4. Select the router with the desired properties from the Router list.
5. Click OK to apply the selected router’s properties and to close the Router Consistency Properties dialog box.
Creating a log file

Use the following procedure to create a log file from the Log View dialog box:

1. Select the SAN router from the Connectivity Map or Product List.
2. Select Configure > SAN Routing > Log Viewer or right-click the SAN Router icon and select Log Viewer.
3. Enter the full path to the log file in the Log File field, or click Browse to browse to the file.
4. Select one of the following log types:
   - If you selected Interpreted log, select the Include Time range button and select the start and end times for the log in the From and To fields.
   - If you selected Raw log, select the Include Complete log button.
5. Click OK to save your changes and close the dialog box.

Saving changes to Flash memory

There are three ways to save changes made on the Router Port Configuration or SAN Router Configuration dialog boxes to flash memory:

1. Select the Save to flash check box on the dialog box and click OK.
2. Right-click the SAN router icon on the Connectivity Map and click Save to Flash.
3. Left-click the SAN router icon on the Connectivity Map, click Configure on the menu bar, click SANRouting, and click Save to Flash.
This chapter contains the following information.

- Topology overview ................................................................. 450
- Customizing the layout of devices on the topology ............... 452
- Customizing the layout of connections on the topology .......... 453
- Changing a group’s background color ................................... 453
- Changing the product label .................................................... 455
- Changing the port label ......................................................... 456
- Changing the port display ....................................................... 456
- Viewing ports and port properties ........................................ 457
- Viewing port types ............................................................... 458
- Showing connected ports ...................................................... 459
- Determining inactive iSCSI devices ....................................... 459
- Determining port status ........................................................ 459
**Customizing the Topology Layout**

**Topology overview**

You can customize various parts of the topology, including the layout of devices and connections as well as groups’ background colors, to easily and quickly view and monitor devices in your SAN.

The following menu options are available on the View menu. Use these options to customize the topology layout.

**Map Display Layout.** Select to specify a new layout for the desktop icons.

- **Default For <Group_Type>.** Displays the devices in the default format. Group types include Group, Fabric, Isolated Devices Group, NPIV Group, Routed Products Group, Loop Group, Router Group, and mSAN.

  **Note:** When the Default For <Group_Type> map display layout is selected, the Show Ports menu command is unavailable (grayed-out).

- **Custom Grid.** Enables you to drag and drop product or group icons into a variable grid to reorganize the topology. The grid prevents icons from obscuring other icons. If enabled on a group, devices can only be moved within the group. If enabled on a fabric, groups can only be moved within the fabric. In other words, a device cannot be moved outside of its group.

- **Square.** Displays the device icons in a square configuration.

- **Vertical.** Displays the device icons vertically.

- **Horizontal.** Displays the device icons horizontally.

- **Most Connected at Center.** Displays the node that has the most connections at the center of the topology.

- **Directional.** Displays the internal nodes in a position where they mirror the external groups to which they are connected.

- **Background Color.** Select to specify a new background color for the selected group.

  - **Default.** Select to revert to the default background color.

  - **Custom.** Select to define a custom color for the topology background.
Line Types.

Straight. Displays connections using straight lines.

Orthogonal. Displays connections in orthogonal gridlines.

None. Hides the connections between devices.

Product Label.

Note: Changes apply to the selected fabric or the fabric to which the selected item belongs.

Name (Product). Displays the product name as the product label.

Nickname. Displays the nickname as the product label.

Node WWN. Displays the node name as the product label.

IP Address. Displays the IP Address as the product label.

Domain ID. Displays the domain ID as the product label.

Port Label

Note: Changes apply to the selected fabric or the fabric to which the selected item belongs.

Name. Displays the name as the port label.

Nickname. Displays the nickname as the port label.

Port Number. Displays the port number as the port label.

Port Address. Displays the port address as the port label.

Port Name. Displays the port name as the port label.

Mapping and unmapping hubs

Mapping a hub

Mapping to a hub creates a more accurate topology by allowing you to place each hub in the appropriate location of the topology. A loop icon displays in each location that a hub might appear on the Physical Map.

Note: The hubs that are not currently on the Physical Map are displayed in the Unmapped Hubs group in the Isolated Devices area at the bottom of the map.
4. Right-click on a loop icon on the Physical Map and select **Map to Hub**. The **Map to Hub** dialog box displays all discovered hubs. Select the appropriate hub and click **OK**.

5. The selected hub will replace the loop product on the Physical Map.

**Unmapping a hub**

Right-click on the hub and select **Revert to Loop**. A loop will replace the hub on the Physical Map. The hub will display in the Unmapped Hubs group in the Isolated Devices at the bottom of the Physical Map.

---

**Customizing the layout of devices on the topology**

You can customize a group’s layout to make it easier to view the SAN and manage its devices.

1. Right-click a group and select **Map Display Layout**, then select one of the following options:

   **Default For <Group_Type>**: Displays the devices in the default format. Group types include Group, Fabric, Isolated Devices Group, NPIV Group, Routed Products Group, Loop Group, Router Group, and mSAN.

   **Note**: When the Default For <Group_Type> map display layout is selected, the Show Ports menu command is unavailable (grayed-out).

   **Custom Grid**: Enables you to drag and drop device or group icons. Devices can only be moved within a group and groups can only be moved within a fabric. After selecting **Custom Grid**, click device or a group and drag it to the desired location.

   **Square**: Displays the device icons in a square configuration.

   **Vertical**: Displays the device icons vertically.

   **Horizontal**: Displays the device icons horizontally.

   **Most Connected at Center**: Displays the node that has the most connections at the center of the topology.

   **Directional**: Displays the internal nodes in a position where they mirror the external groups to which they are connected.
Customizing the layout of connections on the topology

You can change the way inter-device connections display on the topology.

- Right-click a group and select Line Types, then select one of the following options:
  - **Straight**. Displays connections using straight lines.
  - **Orthogonal**. Displays connections in orthogonal gridlines.
  - **None**. Hides the connections between devices.

Changing a group’s background color

You can customize the topology by changing a group’s background color.

1. Right-click a group and select **Background Color**, then **Custom**.

   The **Choose a Background Color** dialog box displays

   ![Choose a Background Color dialog box](image)

   **Figure 47** Choose a background color dialog box

   - To pick a color from a swatch, click the **Swatches** tab.
   - To specify a color based on hue, saturation, and brightness, click the **HSB** tab. Specify the hue (0 to 359 degrees), saturation (0 to 100%) and brightness (0 to 100%).
Customizing the Topology Layout

- To specify a color based on values of red, green, and blue, click the RGB tab. Specify the values for red, green, and blue (0 to 255).

2. Select or specify a color and preview it in the Preview pane.

3. Click OK to change the background color, or click Reset to return all settings to the color currently being displayed on the topology.

**Note:** To revert the background color to the default blue, right-click the group and select Background Color, then <default>.
Changing the product label

1. Select a product in the Physical Map or Product List.
2. Select View > Product Label, then select one of the following options:
   - Name. Displays the product name as the product label.
   - Nickname. Displays the nickname as the product label.
   - Node WWW. Displays the node name as the product label.
   - IP Address. Displays the IP Address as the product label.
   - Domain ID. Displays the domain ID as the product label.

All product labels within the fabric to which the selected item belongs change to the selected product label type.
Customizing the Topology Layout

Changing the port label

1. Select a port in the Physical Map or Product List.
2. Select View > Port Label, then select one of the following options:
   - **Nickname**. Displays the nickname as the port label.
   - **Name**. Displays the name as the port label.
   - **Port Number**. Displays the port number as the port label.
   - **Port Address**. Displays the port address as the port label.
   - **Port Name**. Displays the port name as the port label.

All port labels within the fabric to which the selected item belongs change to the selected port label type.

Changing the port display

You have the option of viewing connected (or occupied) product ports, unoccupied product ports, or attached ports.

**Note**: Occupied/connected ports are those that originate from a device, such as a switch. Attached ports are ports of the target devices that are connected to the originating device.

1. Select a port in the Physical Map or Product List.
2. Select View > Port Display, then select one or more of the following options:
   - **Occupied Product Ports**. Displays the ports of the devices in the fabrics (present in the physical map) that are connected to other devices.
   - **Unoccupied Product Ports**. Displays the ports of the devices (shown in the physical map) that are not connected to any other device.
   - **Attached Ports**. Displays the attached ports of the target devices.

All port labels within the fabric to which the selected item belongs change to the selected port label type.
**Viewing ports and port properties**

To view ports on the Physical Map, right-click a product icon and select *Show Ports.*

**Note:** Show Ports is unavailable (grayed-out) when the map display layout is set to Default For `<Group_Type>`.

**Note:** This feature is only available for connected products. On bridges and CNT products, only utilized Fibre Channel ports display; IP ports do not display.

To view a port’s properties, right-click on a port and select *Properties,* or double-click on the port.

![Figure 48](image-url) The port *Properties* dialog box displays. *Port Properties dialog box*

**Note:** iSCSI ports that have an FC Address of all zeros are inactive. All others are active.
Customizing the Topology Layout

**Viewing port types**

On the Physical Map, right-click a switch icon and select Show Ports. The port types display showing which ports are connected to which products.

*Note:* Show Ports is unavailable (grayed-out) when the map display layout is set to Default For <Group_Type>.

*Note:* This feature is only available for connected products. On bridges and CNT products, only utilized Fibre Channel ports display. IP ports do not display.

<table>
<thead>
<tr>
<th>Table 46</th>
<th>Port types</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port type</td>
<td>Description</td>
</tr>
<tr>
<td>E</td>
<td>An expansion port connecting two fabrics’ switches.</td>
</tr>
<tr>
<td>F</td>
<td>On a Fibre Channel switch, a port that supports an N_Port.</td>
</tr>
<tr>
<td>SL</td>
<td>SL_Ports allow you to divide a Fibre Channel Private Loop into multiple segments. Each segment can pass frames around as an independent loop and can connect through the fabric to other segments of the same loop.</td>
</tr>
<tr>
<td>TL</td>
<td>Each TL_Port connects to a private loop and allows connectivity between the private loop products and “off loop” products (products not connected to that particular TL_Port).</td>
</tr>
<tr>
<td>FL</td>
<td>An N-Port or F-Port that supports arbitrated loop functions associated with arbitrated loop topology.</td>
</tr>
<tr>
<td>H</td>
<td>Indicates an attached product</td>
</tr>
</tbody>
</table>
Showing connected ports

You can jump from a port to its connected port.

1. Right-click the product whose port connection you want to determine and select Ports.
   The product’s ports display.
2. Right-click a port and select Connected Port.
   The focus jumps to the connected port and the connection is highlighted.

Determining inactive iSCSI devices

For router-discovered iSCSI devices, you can view all of the inactive iSCSI devices in one list. To do this, use the Ports Only view and then sort the devices by FC Address. The devices that have an FC address of all zeros are inactive.

1. From the main window, select View All, Levels, and then Ports Only.
2. In the Ports Only list, use the scroll bar to view the columns to the right and locate the FC Address column.
3. If needed, click the column label to sort the column in ascending order. iSCSI ports that have an FC Address of all zeros are inactive. All others are active.

Determining port status

You can determine whether a port is online or offline by looking at the Physical Map or the Product List. On the Physical Map, right-click on the product whose ports you want to view and select Ports. Offline ports are shown in grey.

To determine a port’s status via the Product List, scroll down the Product List to the product whose ports you want to see and click the + icon. Offline ports are shown in gray.
This appendix describes the procedures for installing the Connectrix Manager client onto a remote workstation.

**Note:** To run the client on a remote workstation, you must first download and install the Connectrix Manager client application from the Connectrix service processor.

- System requirements ................................................................. 462
- Installing the Connectrix Manager ........................................... 462
- Uninstalling the Connectrix Manager................................. 466
Configuring Remote Workstations

System requirements

Downloading and installing the Connectrix Manager client application requires the following:

Note: A maximum of 8 clients are allowed per Connectrix service processor.

Refer to “Client system requirements” on page 42.

Installing the Connectrix Manager

The procedures described here are based on Internet Explorer 5.00 and Netscape 6.

To download and install the Connectrix Manager onto a remote workstation:

1. Obtain the address of the Connectrix service processor from your network administrator.

2. To avoid errors, make sure the Connectrix Manager application is not running on the workstation.

3. In a web browser, type the address into the Location (or Address) field, and press Enter.

The Connectrix Management page (Figure 49 on page 463) displays.
EMC Connectrix Management

- Install Connectrix Manager remote client application.
- Download SNMP MIB files.

<table>
<thead>
<tr>
<th>Install Connectrix Manager Remote Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please follow the instructions for your particular platform to install the application.</td>
</tr>
<tr>
<td>Microsoft Windows 95/98/NT/2000/XP</td>
</tr>
<tr>
<td>Begin Windows Installation</td>
</tr>
<tr>
<td>Sun Solaris/SPARC</td>
</tr>
<tr>
<td>Begin Solaris Installation</td>
</tr>
</tbody>
</table>

**Figure 49** Connectrix Manager web page

4. Read the information related to your operating system.
   If necessary, download and install any necessary patches.
5. Click **Download**.

   If a security warning window appears, click **Yes** on the Internet Explorer window (Figure 50) or the Netscape window (Figure 51).

   **Figure 50**  **Internet Explorer security warning**

   **Figure 51**  **Netscape security warning**
6. After downloading, follow the appropriate instructions:

- Windows — Double-click `emcClientInstall.exe`, and follow the instructions.

  Note: The download includes a Java virtual machine.

- Solaris and Linux:
  a. Open a shell and CD to the directory where you downloaded the installer.
  b. At the prompt, type `sh ./emcClientInstall.bin` and press Enter.

  Note: The download includes a Java virtual machine, which will run automatically when you run the shell script.
Uninstalling the Connectrix Manager

If you need to uninstall the application from your system, follow the instructions in this section.

Windows systems

From the Windows Start menu, select Programs, Connectrix Manager 9.1, Uninstall Connectrix Manager.

The InstallShield wizard takes you through the uninstallation process.

Solaris and Linux systems

Follow these steps:

1. If you created links when you installed the application, go to the directory where the links were created.
   - If you did not create links during installation, go to this directory: <Install_Home>/UninstallerData/

2. Execute the uninstall script:
   - ./Uninstall_Connectrix Manager

3. Follow the instructions.
This appendix provides instructions and considerations when upgrading to Connectrix Manager 9.1 on a rackmount service processor. Information on configuration tasks that you should perform after upgrading is also included. Three possible scenarios exist:

- Upgrade/migration from Connectrix Manager 7.1 on a laptop.
- Upgrade from Connectrix Manager 7.2 on a 1U rackmount service processor.
- Upgrade from Connectrix Manager 8.x or 9.0 on a 1U rackmount service processor. Note Connectrix Manager 8.x includes versions 8.1, 8.6.1, 8.7.1 and 8.9.1.

**Note:** Any reference in text and/or screen shots in this manual regarding Connectrix Manager version 9.1 or 9.1.0 can be used interchangeably; they are all one in the same.

- Prerequisites .......................................................................................... 468
- Upgrade considerations ........................................................................ 469
- Getting started .................................................................................... 470
- Upgrade/migration from a laptop running v7.1 ................................. 471
- Upgrading a 1U server from v7.2 to v9.1 ....................................... 489
- Upgrading a 1U server from v8.x or v9.0 to v9.1 ............................ 504
- Data migrated ...................................................................................... 522
- Data not migrated ................................................................................ 525
- Post-upgrade configuration tasks ..................................................... 526
- Connectrix EC-1500 cabinet installation ........................................... 527
Before upgrading to Connectrix Manager 9.1:

- Obtain the serial number (from the Connectrix Manager documentation kit) and your license key (from EMC Powerlink) for your installation. Refer to “Product licensing overview” on page 43 and “Getting a license key” on page 49 for general information on license and feature keys.

- You must have System Administrator user rights for Connectrix Manager 7.x. Obtain a login ID and password before proceeding. Make sure that a user with username of Administrator and a password of password exists on the Connectrix Manager 7.x server.

- The Connectrix Manager installed on your current notebook Connectrix service processor must be at version 7.1 to migrate to the rackmount service processor running 9.1. If the notebook service processor is running a level lower than 7.1, upgrade it to Connectrix Manager 7.1.

Refer to the upgrade instructions in the Connectrix Manager release notes for the version to which you are upgrading.

If you need to upgrade to version 7.1, note that all switches and directors to be managed must be running Enterprise Operating System (E/OS) version 5.01 or higher. For upgrade procedures, refer to “Managing Firmware Versions” in the Installation and Service Manual for your switch/director.

- All switches and directors to be managed by Connectrix Manager 9.1 must be running E/OS version 6.x or higher. However, although it is supported it is not recommended, you should upgrade to the latest version.

- All switches and directors to be managed by Connectrix Manager 9.1 MUST have their SNMP Agent setting Enabled with a Community Name of public (the Community Name is case-sensitive). Failure to configure these settings will result in Connectrix Manager’s inability to discover the switch/director.
Upgrade considerations

CAUTION

Note the following cautions before upgrading to version 9.1.

- After installing Connectrix Manager 9.1 onto the rackmount Connectrix service processor, all remote clients running down-level versions of Connectrix Manager must install the 9.1 client application.
- Once the rackmount Connectrix service processor is running Connectrix Manager 9.1, 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.
- When migrating data from a notebook service processor to a rackmount service processor running Connectrix Manager 9.1, you can migrate data from the notebook service processor as a mapped (shared) drive. Both service processors must be on the same physical network.
- 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.
- On failure of communication.
  Make sure that all switches are available, so that data and settings are completely migrated. Data for any switch that is unavailable will not be completely migrated. You may have to run the configuration wizard again to migrate the data.
- An environment using 10.x.x.x network addresses for both public and private access can cause the migration to fail if the public adapter (Local Area Connection) is not at the top of the Adapters and Bindings Connection list.
Getting started

If you are upgrading from...

- Connectrix Manager 7.1 on a laptop, proceed to “Upgrade/migration from a laptop running v7.1”.
- Connectrix Manager 7.2 on a 1U rackmount server, proceed to “Upgrading a 1U server from v7.2 to v9.1” on page 489.
- Connectrix Manager 8.x or 9.0 on a 1U rackmount server, proceed to “Upgrading a 1U server from v8.x or v9.0 to v9.1” on page 504.
Upgrade/migration from a laptop running v7.1

This procedure will help you migrate from the laptop service processor running Connectrix Manager 7.1 to the new rackmount service processor running Connectrix Manager 9.1.

Replacing the Connectrix Service processor

Use the following procedure to replace a notebook service processor running Connectrix Manager 7.1 with a rackmount service processor running Connectrix Manager 9.1.

For instructions on the physical mounting of the 1U rackmount service processor and KVM, see the Connectrix EC-1500 Cabinet Installation and Setup Manual, P/N 300-001-737, Rev A01.

Prerequisites

Note the following:

◆ You should have received an upgrade kit containing a 1U rackmount Connectrix service processor with Connectrix Manager 9.1 software installed. Do not initialize the software by entering your license key and serial number until instructed to do so.

◆ The notebook service processor must be at Connectrix Manager version 7.1 to migrate data to the rackmount service processor running Connectrix Manager 9.1.

Note: IP addresses of unavailable switches will not be fully migrated.

◆ Both service processors must be on the same physical network. This may require additional hardware (such as a hub or switch) if no unused Ethernet port is available.

◆ The Connectrix data directory and Connectrix Manager application directory must be on the same drive on the notebook service processor. Typically, these directories are c:\EFDATA and c:\Program Files\EFCM.

◆ You must share the root drive (typically c:\) of the notebook service processor and map this drive on the rackmount service processor. This drive can be shared as read-only. You can then
migrate data from the notebook service processor using the Copy Data and Settings screen in the configuration wizard by browsing to the mapped drive.

- The 1U server must be installed and be powered on.
- The 1U server must have two unique IP addresses (one for the private 10.x.x.x network and one for the public network interface).
- The 1U server must be connected to the internal Ethernet hub and you should be able to successfully ping the IP addresses of all of the switches to be migrated as well as the IP address of the donor laptop.
- The 1U server must be given a unique computer name.

---

**Migrating from a laptop running Connectrix Manager 7.1 (Donor) to a new 1U server running Connectrix Manager 9.1 (Recipient)**

This procedure will assist the user with migrating from a laptop running Connectrix Manager 7.1 (Donor) to a new 1U server running Connectrix Manager 9.1 (recipient).

**Important:** The laptop must be running Connectrix Manager Version 7.1 and a user with username of Administrator and a password of password must exist before you can begin the migration to version 9.1.

1. Backup the configuration of each director and switch managed by the laptop.
   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 (Figure 52 on page 473).

![Backup and Restore Configuration dialog box](image)

**Figure 52** Backup and Restore Configuration dialog box

- **Backup** saves the current DS-24M2 configuration to the server.
- **Restore** copies the backed up configuration to the DS-24M2, overwriting the current configuration.

- Click **Backup**. An **Information** dialog box is displayed, indicating the backup operation was initiated (Figure 53 on page 473).

![Information dialog box](image)

**Figure 53** Information dialog box

- Click **OK** to complete the backup operation, close the dialog box, and return to the **Hardware View**.
- Close the **Hardware View** and return to the **Products View** by clicking close (X) at the upper right corner of the window.
- Repeat step 1a through step 1e for each product (director and switch) managed by the 1U server.

2. Verify Connectrix Manager 7.x remote management sessions have not been restricted.
Upgrading to Connectrix Manager 9.1

a. From the Connectrix Manager 7.x top main menu, click **Configure** and select **Sessions** from the drop-down list to display the *Connectrix: Configure Sessions* dialog, as shown in Figure 54 on page 474.

![Connectrix: Configure Sessions dialog box](image)

**Figure 54**  
*Connectrix: Configure Sessions* dialog box

b. Verify that the displayed window appears as above and that there are not any entries under **Restrict access to the following network addresses**.

c. If there are any entries, remove them by enabling/clicking the radio button for **Restrict access to the following network addresses**.

d. Highlight the entry(s) to be deleted, and click **Remove**.

e. Make sure to re-enable **Allow any network address to connect** option, and then click **OK**. If there are entries in this table that are not IP address, then the migration process will fail even if the restrict option is not enabled.

3. Close the Connectrix Manager application:

a. Close the Connectrix Manager application by selecting **Exit** from the **Product** menu, but DO NOT stop the Connectrix Services.
The Connectrix Manager Login window can remain open.

b. Close any open Connectrix Manager remote Clients.

4. Backup data on the donor laptop. Copy the C:\EfcData and C:\Program Files\EFCM directories to a desktop or to another directory of your choosing.

5. Record the Call Home setup information.
   a. Double-click the Call Home Setup icon on the Windows desktop. The DialEMC Configuration Dialog box displays (Figure 55 on page 475).

![DialEMC Configuration Dialog Box]

b. Record the above information. It will be needed later when configuring ConnectEMC.
6. Before mapping the donor Laptop C:\ drive, ensure that the network properties of the NIC card are configured properly on the new 1U server.

   a. Select the appropriate NIC card:

      – If mapping the drive over the Private NIC card, from the 1U server, select Start, Settings, Network and Dial-up Connections, Local Area Connection 2. The Local Area Connection 2 Status dialog appears. Proceed to step b.

      – If mapping the drive over the Public NIC card, from the 1U server, select Start, Settings, Network and Dial-up Connections, Local Area Connection. The Local Area Connection Status dialog appears. Proceed to step b.

   b. Click the Properties tab. Depending on which NIC was selected, either the Local Area Connection Properties or Local Area Connection 2 Properties window will be displayed.

   c. Ensure that both the Client for Microsoft Networks and File and Printer Sharing for Microsoft Networks settings are enabled, in addition to the Internet Protocol (TCP/IP) setting (Figure 56 on page 476).

   ![Figure 56 Local Area Connection 2 Properties dialog box](image)
d. After selecting the options noted in the previous step, click OK to close the Properties window.

e. Click Close to close the Status window.

7. Map the Donor Laptop C:\ drive to the new 1U server. Disable the Reconnect at logon option.

   a. From the 1U server, open a command prompt (Start Menu, Programs, Accessories, Command Prompt) and ping the IP address or hostname of the Donor Laptop. If the IP address or hostname can be pinged, proceed to the next step; otherwise determine cause of network problem.

   b. From the 1U server, right-click the My Computer icon on the desktop, select Map Network Drive. The Map Network Drive dialog box displays (Figure 57).

   c. Take note of the drive letter in the Drive: pull-down menu for later use.

   d. Enter the IP address or hostname of the Donor Laptop into the Folder text field in the format of `\<ipaddress or hostname\>\C$`.

   Map Network Drive dialog box

   Windows can help you connect to a shared network folder and assign a drive letter to the connection so that you can access the folder using My Computer.

   Specify the drive letter for the connection and the folder that you want to connect to:

   Drive: E:

   Folder: `\172.23.185.198\C$` Browse...

   Example: `\server\share`

   Reconnect at logon

   Connect using a different user name.

   Create a shortcut to a Web folder or FTP site.

   Figure 57 Map Network Drive dialog box
e. Click **Finish**. In our example above, we are mapping the c:\Share on 172.23.185.198 to the E:\ drive on the local 1U server.

   If prompted for a network password, specify the Windows Username and Password for the Donor Laptop (default Username = Administrator, default password = password) and click **OK**.

   A window displaying the contents of the c:\ drive on the donor laptop should open in approximately 10 seconds.

8. Install Connectrix Manager 9.1 on the 1U server. (If the 1U server shipped with Connectrix Manager 9.1 pre-installed, skip to step 9.)

   a. Insert the Software distribution CD provided with your upgrade kit into the CD-ROM drive. If autorun is enabled, the installer begins automatically. If it is not enabled double-click the setup.exe file on the CD. The **InstallAnywhere** wizard will take you through the installation process.

   b. The **Connectrix Manager 9.1** splash screen is briefly displayed followed by the **Introduction** screen. Click **Next**.

   c. The **Choose Install Set** screen is displayed. Select **Server and Client** and click **Next**.

   d. The **Select Install Folder** screen is displayed. Click **Next** to accept the default **Destination Folder C:\Program Files\Connectrix Manager 9.1**.

   e. On the **Pre-Installation Summary** screen, review your installation settings and click **Install**.

   f. On the **Installation Complete** screen, make sure the **Launch Configuration Wizard** checkbox is selected (default), and click **Done**.
9. Perform the migration.
   
a. The **Welcome** dialog should appear. If not, on the 1U server, go to **Start, Programs, Connectrix Manager 9.1**, and select **Connectrix Manager 9.1**. The migration **Welcome** dialog displays (Figure 58 on page 479).

![Welcome dialog](image)

**Figure 58** Connectrix Manager 9.1 Configuration, Welcome dialog

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 (Figure 59 on page 480).
Upgrading to Connectrix Manager 9.1

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?

- Yes - Specify the install path to the previous version
  - Installation Directory
  - Browse
- No

Note: The drive typically is C: \. However, since the drive was mapped on the 1U server as the E: \ drive, we had to specify the E: \ drive. Your drive letter may vary depending on how you performed step 7.

Figure 59  Connectrix Manager 9.1 Configuration, copy data and settings with defaults

d. Accept the default setting of Yes but change the Installation Directory to E:\Program Files\EFCM. Using the Browse button, specify the path to the Connectrix Manager 7.1 EFCM directory on the donor laptop, as shown in Figure 60 on page 481.
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?

- Yes - Specify the install path to the previous version

  Installation Directory: E:\Program Files\EFOM

- No

Figure 60  Copy Data and Settings showing the Installation Directory

e. Click Next to display the Copy Data and Settings (continued) dialog (Figure 61 on page 482).
Upgrading to Connectrix Manager 9.1

Copy Data and Settings (continued)

You have selected to copy data and settings from a 7.x installation.

Please make sure the following requirements are met before you click the "Next" button:
- Connectrix Manager 7.x server must be running.
- Connectrix Manager 7.x local client must be closed.

<table>
<thead>
<tr>
<th>EFCM 7.x Data Directory</th>
<th>E:\EfcData</th>
<th>Browse</th>
</tr>
</thead>
<tbody>
<tr>
<td>P Address or Hostname</td>
<td>10.1.1.1</td>
<td></td>
</tr>
<tr>
<td>System Administrator User ID</td>
<td>Administrator</td>
<td></td>
</tr>
<tr>
<td>Password</td>
<td>********</td>
<td></td>
</tr>
</tbody>
</table>

![Connectrix Manager 9.1 Configuration](image)

Figure 61  Copy and Data Settings (continued) showing the Data Directory

f. Change the EFCM 7.x Data Directory to E:\EfcData.

Using the Browse button, specify the path to the Connectrix Manager 7.1 EfcData directory on the donor laptop as displayed in Figure 61 on page 482.

**Note:** The drive typically is C:\. However, since the drive was mapped on the 1U server as the E:\ drive, we had to specify E:\. Your drive letter may vary depending on how you performed step 7.

g. Enter the IP address of the donor laptop and type the Connectrix Manager application (Version 7.1) user identification and password in the User ID and Password
fields. This is needed to allow the migration utility to properly import data. Default User ID for Connectrix Manager is **Administrator**, the default password is **password**.

**Important:** The laptop must be running Connectrix Manager Version 7.1 and a user with username of **Administrator** and a password of **password** must exist before you can begin the migration to version 9.1.

h. Click **Next** to display the **Connectrix Manager 9.1 Server License** dialog (Figure 62 on page 483).

![Connectrix Manager 9.1 Server License dialog box](image)

**Figure 62 Connectrix Manager Server License dialog box**
Upgrading to Connectrix Manager 9.1

i. 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 49.

j. Click Next to display the Connectrix Manage 9.1 Server License Summary dialog (Figure 63 on page 484).

k. Verify configuration and license information and click Finish.
l. 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.

m. When the Connectrix Manager 9.1 Log In dialog box displays (Figure 64 on page 485), select Exit.

10. After the migration completes, stop Connectrix Manager Service for version 7.1 on the Laptop.
   a. From the Start menu, select Programs, then EMC Connectrix Management, then Stop Services.
   b. A DOS window appears, press any key to continue when prompted to do so.

11. Reboot the 1U server, and log in to Connectrix Manager.
   a. On the 1U 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 application user identification and password in the User ID and Password fields. Default User ID
Upgrading to Connectrix Manager 9.1

for Connectrix Manager is **Administrator**, the default password is **password**. Network address should be left as **localhost**.

c. Click **Login**. The application opens and the Connectrix Manager main window displays (Figure 65 on page 486).

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
- Ethernet Notification Settings

f. All email addresses entered in the Connectrix Manager 7.1 Configured email dialog box will migrate to the email Event Notification Setup User List under one user profile. You must modify the User list in Connectrix Manager 9.1 to assign addresses to individual users.

g. Verify that all director and switch products that were previously managed by the laptop are now managed by the 1U server.

h. Insert a blank pre-formatted CD-RW disk into the CD-RW drive on the 1U service processor. The Connectrix Manager data contained in the C:\Program Files\Connectrix Manager 9.1 directory is automatically backed up to the CD-RW drive as long as a formatted CD-RW disk remains in the drive.

Note: Three options for backing up with the management server are available: Writable CD, Hard drive, and Network drive. In addition, Connectrix Manager 9.1 has a "Backup Now" feature which will perform an immediate backup to any one of these three options.

Important:
Do not format a blank CD-RW disk while the Connectrix Manager application is running. Ensure the Connectrix Manager Services have been stopped before proceeding. For more information, refer to EMC Knowledgebase solution emc96761.

12. Perform one of the following two steps to connect the modem to the COM1 port on the 1U server:

a. Using the existing modem cable, move the DB9 end of the cable from the Donor Laptop to the COM1 port on the 1U server. This will require the removal of the Laptop tray in order to free-up the cable.

or
Upgrading to Connectrix Manager 9.1

b. Using the new modem cable supplied with the 1U server, connect the DB9 end to the COM1 port on the 1U server and the DB25 end to the modem port.

13. Reboot the 1U server. Log in to Connectrix Manager.

a. On the 1U server, go to Start, Programs, Connectrix Manager 9.1 and select Connectrix Manager 9.1.

b. At the Connectrix Manager 9.1 Log In dialog box, type the Connectrix Manager application user identification and password in the User ID and Password fields. Default User ID for Connectrix Manager is Administrator, the default password is password. Network address should be left a localhost.

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

14. Install ConnectEMC, and then configure and test the Call Home feature. For more information, refer to Appendix G, “Call Home Setup Procedure.”

**Note:** If after migrating, some switches are not present, refer to EMC Knowledgebase Solution emc78818.

15. It is no longer necessary to edit the config.properties file in order to support remote client access if the service processor is configured to use dual network cards with a public and private address of 10.x.x.x.

16. If required, load the FibreZoneBridge/Connectrix Bridge to support EMC ControlCenter. The FibreZoneBridge/Connectrix Bridge and the installation notes are available for download from the Powerlink Web site at <http://Powerlink.emc.com>.

17. It is the customer’s responsibility to load any Microsoft patches and anti-virus protection software.
Upgrading a 1U server from v7.2 to v9.1

**Important:** The Connectrix Manager 7.2 Services on the 1U server MUST be running and a user with username of Administrator and a password of password must exist before you can begin the migration to version 9.1.

This procedure will assist users when upgrading from Connectrix Manager 7.02 to Connectrix Manager 9.1 on a 1U server. Connectrix Manager version 7.02 on the 1U server is not removed during the Connectrix Manager 9.1 upgrade process.

**Note:** Connectrix Manager Audit, Event, Session, Product Status, and Fabric log files are not migrated. As a safeguard, you should export and archive these logs in before migrating to Connectrix Manager 9.1.

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 via the Connectrix Manager 7.02 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 for the product displays (Figure 66 on page 489).

![Backup and Restore Configuration dialog box](image)

   - **Backup** saves the current DS-24M2 configuration to the server.
   - **Restore** copies the backed up configuration to the DS-24M2, overwriting the current configuration.

   **Figure 66** Backup and Restore Configuration dialog box
c. Click **Backup**. An **Information** dialog box is displayed, indicating the backup operation was initiated (Figure 67 on page 490).

![Figure 67 Information dialog box](image)

**Figure 67** Information dialog box

d. Click **OK** to complete the backup operation, close the dialog box, and return to the **Hardware View**.

e. Close the **Hardware View** and return to the **Products View** by clicking close (X) at the upper right corner of the window.

f. Repeat **step 1a** through **step 1e** for each product (director and switch) managed by the 1U server.

2. Verify Connectrix Manager 7.x remote management sessions have not been restricted.
Upgrading to Connectrix Manager 9.1

a. From the Connectrix Manager 7.x top main menu, click Configure and select Sessions from the drop-down list. The dialog box in Figure 68 on page 491 shows:

<table>
<thead>
<tr>
<th>Connectrix Configure Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow remote management sessions</td>
</tr>
<tr>
<td>Maximum number of remote management sessions: 8</td>
</tr>
</tbody>
</table>

- Network Address Restrictions
  - Allow any network address to connect
  - Restrict access to the following network addresses:

![Connectrix Configure Sessions dialog box](image)

b. Verify that the displayed window appears as above and that there are not any entries under Restrict access to the following network addresses.

c. If there are any entries, remove them by enabling/clicking the radio button for Restrict access to the following network addresses.

d. Highlight the entry(s) to be deleted and click Remove.

e. Make sure to re-enable Allow any network address to connect option and then click OK. If there are entries in this table that are not IP address then the migration process will fail even if the restrict option is not enabled.

3. Close the Connectrix Manager application.

a. Close the Connectrix Manager application by selecting Exit from the Product menu, but DO NOT stop the Connectrix Services.

b. The Connectrix Manager Log In dialog box can remain open.
Upgrading to Connectrix Manager 9.1

c. Close any open Connectrix Manager remote Clients.

4. Backup data on the 1U server, coping the C:\EfcData and C:\Program Files\EFCM directories to the internal CD-RW (D:) drive.

   a. Insert a pre-formatted CD-RW disk into the internal CD-RW drive.

   Important: Do not format a blank CD-RW disk while the Connectrix Manager application is running. Ensure the Connectrix Manager Services are stopped before proceeding. After the format has completed, restart the services.

   b. At the Windows desktop, double-click the My Computer icon. The My Computer window displays.

   c. At the My Computer window, double-click (C:) icon. The (C:) windows displays.

   d. At the (C:) window, click (select) the C:\EfcData folder. Using the Copy and Paste utilities from the Edit menu, copy the C:\EfcData folder to the CD-RW (D:) drive.

   e. At the (C:) window, click (select) the C:\Program Files\EFCM folder. Using the Copy and Paste utilities from the Edit menu, copy the C:\Program Files\EFCM folder to the CD-RW (D:) drive.

   f. Remove the CD from the CD-RW drive for safe keeping.

5. Record the Call Home Setup configuration.
a. Double-click the Call Home Setup icon on the Windows desktop. The DialEMC Configuration Dialog box displays (Figure 69 on page 493).

b. Record the above information. It will be needed later when configuring ConnectEMC.

6. Install Connectrix Manager 9.1 on the 1U server.

Note: Virus protection software can interfere with installation. Make sure you disable any virus protection software such as Norton or McAfee before installation of server and/or clients.

a. Insert the Software distribution CD provided with your upgrade kit into the CD-ROM drive. If autorun is enabled, the installer begins automatically. If it is not enabled double-click the setup.exe file on the CD. The InstallAnywhere wizard will take you through the installation process.

b. The Connectrix Manager 9.1 splash screen is briefly displayed followed by the Introduction screen, click Next.

c. The Choose Install Set screen is displayed. Select Server and Client, click Next.
d. The Select Install Folder screen is displayed. Click Next to accept the default Destination Folder C:\Program Files\Connectrix Manager 9.1.

e. On the Pre-Installation Summary screen, review the your installation settings and click Install.

f. On the Installation Complete screen, make sure the Launch Configuration Wizard checkbox is selected (default), and click Done.

7. Perform the migration.

a. The Welcome page should appear. If not, on the 1U server, go to Start, Programs, Connectrix Manager 9.1, and select Connectrix Manager 9.1. The migration Welcome page should appear (Figure 70 on page 494).
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 (Figure 71).

d. Accept the default setting of Yes but change the Installation Directory to C:\Program Files\EFCM. Using the Browse button, specify the path to the Connectrix Manager 7.2 EFCM directory as displayed in Figure 72 on page 496.
e. Click Next to display the Copy Data and Settings (continued) dialog (Figure 73 on page 497).
Upgrading a 1U server from v7.2 to v9.1

Figure 73 Copy Data and Settings (continued) with Data Directory shown

- Change the EFCM 7.x Data Directory to `C:\EfcData`. Using the Browse button, specify the path to the Connectrix Manager 7.2 EfcData directory on the 1U server as displayed in Figure 73 on page 497.

- Enter the IP address of the 1U server, and type the Connectrix Manager application (Version 7.2) user identification and password in the User ID and Password fields. This is needed to allow the migration utility to properly import data. Default User ID for Connectrix Manager is Administrator, the default password is password.
Upgrading to Connectrix Manager 9.1

Important: The 1U server must be running Connectrix Manager Version 7.2 the 7.2 services MUST be running, and a user with username of Administrator and a password of password must exist before you can begin the migration to version 9.1.

h. Click Next to display the Connectrix Manager 9.1 Server License dialog (Figure 74 on page 498).

![Connectrix Manager 9.1 Server License dialog box](image)

Please enter the Serial Number and License Key below.

Serial Number: [Field]

License Key: [Field]

Figure 74 Connectrix Manager 9.1 Server License dialog box

i. 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 49.
j. Click Next. The second Connectrix Manager 9.1 License panel displays (Figure 75 on page 499).

![Figure 75 Connectrix Manager 9.1 Server License Summary dialog box]

- User ID: Administrator
- Connectrix Manager 9.1 Server Name: CONNECTRIXSVT
- Win32® Service: Automatic/Start Now
- Copy Data and Settings: Yes
- Version: Connectrix Manager 9.1
- Build: 40
- Expiration: None
- Clients: 25
- Licensed Ports: 4096

k. Verify configuration and license information, and click Finish.

l. 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.

m. When the Connectrix Manager 9.1 Log In dialog box displays (Figure 76 on page 500), click Exit.
8. Reboot the 1U server, and log in to Connectrix Manager.
   a. On the 1U server, go to Start > Programs > Connectrix Manager 9.1 and select Connectrix Manager 9.1.
   b. At the Connectrix Manager 9.1 Log In dialog box, type the Connectrix Manager application user identification and password in the User ID and Password fields. Default User ID for Connectrix Manager is Administrator, the default password is password. Network address should be left a localhost.
   c. Click Login. The application opens and the Connectrix Manager main window appears (Figure 77 on page 501).

Note: After the migration completes, the Connectrix Manager Services for version 7.2 are stopped and disabled. However, this will not prevent the Connectrix Manager 7.2 Log In dialog box from appearing after a reboot. Though it is not necessary for the Connectrix Manager 7.2 application to be uninstalled immediately it will prevent this from occurring.
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
   - Ethernet Notification Settings

Figure 77  Main window (Connectrix Manager)
Upgrading to Connectrix Manager 9.1

f. All email addresses entered in the Connectrix Manager 7.2 Configured email dialog box will migrate to the email Event Notification Setup User List under one user profile. You must modify the User list in Connectrix Manager 9.1 to assign addresses to individual users.

g. Verify that all director and switch products that were previously available are now managed by Connectrix Manager 9.1.

h. Insert a blank pre-formatted CD-RW disk into the CD-RW drive on the 1U service processor. The Connectrix Manager data contained in the C:\Program Files\Connectrix Manager 9.1 directory is automatically backed up to the CD-RW drive as long as a formatted CD-RW disk remains in the drive.

Note: Three options for backing up with the management server are available: Writable CD, Hard drive, and Network drive. In addition, Connectrix Manager 9.1 has a “Backup Now” feature which will perform an immediate backup to any one of these three options.

Important: Do not format a blank CD-RW disk while the Connectrix Manager application is running. Ensure the Connectrix Manager Services have been stopped before proceeding. For more information, refer to EMC Knowledgebase solution emc96761.

9. Install ConnectEMC, and then configure and test the Call-home feature. For more information, refer to Appendix G, “Call Home Setup Procedure”.

10. After completing the installation of ConnectEMC, the previous version's Call Home icon, entitled Call Home Setup, is now obsolete. To remove it from the desktop, right-click the icon and select Delete from the pull-down list.

11. It is no longer necessary to edit the config.properties file in order to support remote client access if the service processor is configured to use dual network cards with a public and private address of 10.x.x.x.

12. If required, load the FibreZoneBridge/Connectrix Bridge to support EMC ControlCenter. The FibreZoneBridge/Connectrix Bridge and the installation notes are available for download from the Powerlink website at <http://Powerlink.EMC.com>.
13. It is the customer’s responsibility to load any Microsoft patches and anti-virus protection software.
Upgrading to Connectrix Manager 9.1

Upgrading a 1U server from v8.x or v9.0 to v9.1

This procedure will assist users when upgrading from Connectrix Manager 8.1, 8.6.1, 8.7.1, 8.9.1, or 9.0 to Connectrix Manager 9.1 on a 1U server.

**Important:** A user with username of **Administrator** and a password of **password** must exist before you can begin the migration to version 9.1.

**Note:** 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.

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 upper-right corner of the window.

   f. Repeat step 1a through step 1e for each product (director and switch) managed by the 1U server.

2. When the final product configuration file is backed up, close the Connectrix Manager application and stop the Connectrix Services on the 1U server.
Important: Connectrix Manager Services for version 8.x or 9.0 on the 1U server MUST be stopped in order for the upgrade to complete successfully.

a. Close any open Connectrix Manager Remote Clients.

b. Close the Connectrix Manager application on the 1U server by selecting Exit from the SAN menu.
   - If upgrading from Connectrix Manager 8.1, proceed to step c.
   - If upgrading from Connectrix Manager 8.6.1, skip step c and proceed to step d.
   - If upgrading from Connectrix Manager 8.7.1, skip steps c and d and proceed to step e.
   - If upgrading from Connectrix Manager 8.9.1, skip steps c, d and e and proceed to step f.
   - If upgrading from Connectrix Manager 9.0, skip steps c, d, e and f and proceed to step g.

c. Stop the Connectrix Services. From the Start menu, select Programs, then Connectrix Manager 8.1, then Stop Services. Proceed to step 3.

d. Stop the Connectrix Services. From the Start menu, select Programs, then Connectrix Manager 8.6.1, then Stop Services. Proceed to step 3.

e. Stop the Connectrix Services. From the Start menu, select Programs, then Connectrix Manager 8.7.1, then Stop Services. Proceed to step 3.

f. Stop the Connectrix Services. From the Start menu, select Programs, then Connectrix Manager 8.9.1, then Stop Services. Proceed to step 3.

g. Stop the Connectrix Services. From the Start menu, select Programs, then Connectrix Manager 9.0, then Stop Services. Proceed to step 3.

3. Remove the CD from the CD-RW drive for safe keeping.

Note: Virus protection software can interfere with installation. Make sure you disable any virus protection software such as Norton or McAfee before installation of server and/or clients. Instructions should be located in the manual for your particular.
4. Install Connectrix Manager 9.1 on the 1U server.
   a. Insert the Software distribution CD provided with your upgrade kit into the CD-ROM drive. If autorun is enabled, the installer begins automatically. If it is not enabled double-click the setup.exe file on the CD. The InstallAnywhere wizard will take you through the installation process.
   b. The Connectrix Manager 9.1 splash screen is briefly displayed followed by the Introduction screen. Click Next.
   c. The Choose Install Set screen is displayed. Select Server and Client, and click Next.
   d. The Select Install Folder screen is displayed. Click Next to accept the default Destination Folder C:\Program Files\Connectrix Manager 9.1.
   e. On the Pre-Installation Summary screen, review your installation settings and click Install.
   f. On the Installation Complete screen, make sure the Launch Configuration Wizard checkbox is selected (default), and click Done.

5. Perform the migration.
   a. The Welcome page should appear (Figure 78 on page 507). If not, on the 1U server, go to Start, Programs, Connectrix Manager 9.1 and select Connectrix Manager 9.1.
Upgrading a 1U server from v8.x or v9.0 to v9.1

- Figure 78 Connectrix Manager 9.1 Configuration, Welcome dialog box

b. Click Next. The License Agreement panel displays.

c. Select Yes, and click Next. The Copy Data and Settings dialog box displays (Figure 79 on page 508).
Upgrading to Connectrix Manager 9.1

Copy Data and Settings

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?

- Yes - Specify the install path to the previous version
- No

Figure 79 Connectrix Manager 9.1 Configuration, Copy Data and Settings dialog box

- If upgrading from Connectrix Manager 8.1, proceed to step d.
- If upgrading from Connectrix Manager 8.6.1, skip step d and proceed to step e.
- If upgrading from Connectrix Manager 8.7.1, skip steps d and e and proceed to step f.
- If upgrading from Connectrix Manager 8.9.1, skip steps d, e, and f and proceed to step g.
- If upgrading from Connectrix Manager 9.0, skip steps d, e, f, and g and proceed to step h.
d. Accept the default setting of Yes, but change the **Installation Directory** to `C:\Program Files\Connectrix Manager 8.1`. Using the **Browse** button, specify the path to the **Connectrix Manager 8.1** directory as displayed in Figure 80 on page 509. Proceed to step i.

![Connectrix Manager 9.1 Configuration](image)

**Copy Data and Settings**

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?

- **Yes** - Specify the install path to the previous version

  **Installation Directory** `C:\Program Files\Connectrix Manager 8.1`  
  **Browse**

- **No**

**Figure 80**  
**Copy Data and Settings for Connectrix Manager 8.1**
e. Accept the default setting of Yes, but change the **Installation Directory** to `C:\Program Files\Connectrix Manager 8.6.1`. Using the **Browse** button, specify the path to the **Connectrix Manager 8.6.1** directory as displayed in **Figure 81** on page 510. Proceed to step i.

![Figure 81 Copy Data and Settings for Connectrix Manager 8.6.1](image1)

f. Accept the default setting of Yes, but change the **Installation Directory** to `C:\Program Files\Connectrix Manager 8.7.1`. Using the **Browse** button, specify the path to the **Connectrix Manager 8.7.1** directory as displayed in **Figure 82** on page 511. Proceed to step i.
Upgrading a 1U server from v8.x or v9.0 to v9.1

Figure 82  Copy Data and Settings for Connectrix Manager 8.7.1

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?

- Yes - Specify the install path to the previous version
  - Installation Directory: C:\Program Files\Connectrix Manager 8.7.1
- No
g. Accept the default setting of Yes, but change the **Installation Directory** to C:\Program Files\Connectrix Manager 8.9.1. Using the **Browse** button, specify the path to the Connectrix Manager 8.9.1 directory as displayed in **Figure 83** on page 512. Proceed to step i.

![Connectrix Manager 9.1 Configuration](image)

**Copy Data and Settings**

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?

- Yes - Specify the install path to the previous version
  
  **Installation Directory** C:\Program Files\Connectrix Manager 8.9.1 [Browse]

- No

![Figure 83 Copy Data and Settings for Connectrix Manager 8.9.1](image)

h. Accept the default setting of Yes, but change the **Installation Directory** to C:\Program Files\Connectrix Manager 9.0. Using the **Browse** button, specify the path to the Connectrix Manager 9.0 directory as displayed in **Figure 84** on page 513. Proceed to step i.
Upgrading a 1U server from v8.x or v9.0 to v9.1

Upgrading to Connectrix Manager 9.1

Figure 84 Copy Data and Settings for Connectrix Manager 9.1

i. Click Next. A Connectrix Manager Message window displays (Figure 85 on page 513).

Figure 85 Nickname message
j. Click OK. The Connectrix Manager 9.1 Server License panel displays (Figure 86 on page 514). The serial number and license fields will contain the values from the Connectrix Manager 9.0 installation; however, the fields will NOT contain the values from the Connectrix Manager 8.1, 8.6.1, 8.7.1, or 8.9.1 installation. 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 “Obtaining a license key” on page 45.

![Connectrix Manager 9.1 Server License dialog box](image)
k. Click Next. The Connectrix Manager 9.1 Server License Summary dialog displays (Figure 87 on page 515).

![Connectrix Manager 9.1 Server License Summary dialog box]

Please verify the contents of your configuration and license.

<table>
<thead>
<tr>
<th>User ID</th>
<th>Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectrix Manager 9.1 Server Name</td>
<td>CONNECTRIXSVT</td>
</tr>
<tr>
<td>Win32® Service</td>
<td>Automatic/Start Now</td>
</tr>
<tr>
<td>Copy Data and Settings</td>
<td>Yes</td>
</tr>
<tr>
<td>Version</td>
<td>Connectrix Manager 9.1</td>
</tr>
<tr>
<td>Build</td>
<td>40</td>
</tr>
<tr>
<td>Expiration</td>
<td>None</td>
</tr>
<tr>
<td>Clients</td>
<td>25</td>
</tr>
<tr>
<td>Licensed Ports</td>
<td>4096</td>
</tr>
</tbody>
</table>

**Modules**

Group Configuration Manager | Enabled

Figure 87  Connectrix Manager 9.1 Server License Summary dialog box

l. Verify configuration and license information, and click Finish.

m. 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.
n. When the Connectrix Manager 9.1 Log In dialog displays (Figure 88 on page 516), click Exit.

![Figure 88 Connectrix Manager 9.1 Log In dialog box](image)

6. Reboot the 1U server. Log in to Connectrix Manager.
   a. On the 1U server, go to Start, Programs> Connectrix Manager 9.1 and select Connectrix Manager 9.1.
   b. At the Connectrix Manager 9.1 Log In dialog, type the Connectrix Manager application user identification and password in the User ID and Password fields. Default User ID for Connectrix Manager is Administrator, the default password is password. Network address should be left a localhost.
c. Click **Login**. The application opens and the Connectrix Manager main window appears (Figure 89 on page 517).

d. At the Connectrix Manager 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
Upgrading to Connectrix Manager 9.1

- Trap Forwarding Information
- Ethernet Notification Settings
- Call Home Information (Desktop Icon)

f. Verify that all director and switch products that were previously available are now managed by Connectrix Manager 9.1.

g. Reinsert the CD into the CD-RW drive that was removed in Step 3. The Connectrix Manager data contained in the C:\Program Files\Connectrix Manager 9.1 directory is automatically backed up to the CD-RW drive as long as a formatted CD-RW disk remains in the drive.

Note: Three options for backing up with the management server are available: Writable CD, Hard drive, and Network drive. In addition, Connectrix Manager 9.1 has a "Backup Now" feature which will perform an immediate backup to any one of these three options.

Important:
Do not format a blank CD-RW disk while the Connectrix Manager application is running. Ensure the Connectrix Manager Services have been stopped before proceeding. For more information, refer to EMC Knowledgebase solution emc96761.

7. Test the Call-home feature. For more information, refer to Appendix G, “Call Home Setup Procedure”.

8. It is no longer necessary to edit the config.properties file in order to support remote client access if the service processor is configured to use dual network cards with a public and private address of 10.x.x.x.

9. Upon completion of the upgrade the Connectrix Manager 8.1, 8.6.1, 8.7.1, 8.9.1, or 9.0 services are no longer available, but the directory structure and desktop icons associated with version 8.1, 8.6.1, 8.7.1, 8.9.1, or 9.0 remain. Therefore, once you have confirmed that the upgrade was successful you may want to proceed with the 8.1, 8.6.1, 8.7.1, 8.9.1, or 9.0 uninstall process to remove these items.

a. From the Start menu, select Programs> Connectrix Manager 8.1, 8.6.1, 8.7.1, 8.9.1, or 9.0, 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**.

10. If the **EMC FibreZoneBridge/Connectrix Bridge** was installed prior to upgrading, it will no longer be operational upon completion of the upgrade. Therefore, you must uninstall the bridge software, reboot the service processor, re-installed the bridge and then reboot the service processor one more time in order to restore communication between ControlCenter and Connectrix Manager 9.1. The **FibreZoneBridge/Connectrix Bridge** and the installation notes are available for download from the Powerlink website at <http://Powerlink.EMC.com>.

11. However, additional steps (such as configuring the Network Drive Credentials) are necessary if you wish to continue backing up to a network drive. For more details, refer to “**Configuring backup to a network drive**” on page 2-22.

12. It is the customer’s responsibility to load any Microsoft patches and anti-virus protection software.

---

**Upgrade procedure for remote clients**

To log into the Connectrix service processor as a client and use Connectrix Manager 9.1, you must download the client application to your system:

1. Make sure that Connectrix Manager is not running on the remote machine.

2. Open a Web browser.

3. Type the IP address of the Connectrix service processor in the **Location** (or **Address**) box on the browser, and press **Enter**.

4. When the remote client installation screen appears, select the appropriate download for your operating system.

5. Follow instructions in the configuration wizard to install the client to your system.
6. To start the application:
   • On Windows systems, select **Start, Programs, Connectrix Manager 9.1, Connectrix Manager** or **Connectrix Manager Client**. (**Connectrix Manager** launches both the service processor and client. **Connectrix Manager Client** launches only the client application.)
   • On UNIX systems, type `./ConnectrixClient` and press **Enter**.

---

**Migrating data after initializing Connectrix Manager 9.1**

If you did not migrate the Connectrix Manager 8.1, 8.6.1, 8.7.1, 8.9.1, or 9.0 data and settings when you initialized Connectrix Manager 9.1 on the rackmount service processor (in other words, you did not select **Yes** from the **Copy Data and Settings** screen), you can migrate data using the appropriate procedure.

**Do not uninstall Connectrix Manager 9.1 before performing this procedure.**

---

**Upgrading to Connectrix Manager 9.1**

To upgrade:

1. Refer to “Upgrading a 1U server from v8.x or v9.0 to v9.1” on page 504.
2. Perform all steps under “Editing ConnectrixManager_co.bat file” on this page.

**Editing set_commonEnv_post.bat file**

*Note:* Perform these steps on your rackmount service processor.

1. Shut down Connectrix Manager 9.1. From the **Start** menu, select **Connectrix Manager 9.1> Stop Services**.
2. Go to the **bin** directory located under C:\Program Files\Connectrix Manager 9.1, right click on the **set_commonEnv_post.bat** file and select edit to open the file.
3. At the very end of the line that starts with the following string, add a space, then the word **doit**.

   ```
   set WIZARD_END_ARGS=Wizard doit
   ```

4. Save and close the **set_commonEnv_post.bat** file.
5. Perform the migration as instructed in “Upgrading a 1U server from v8.x or v9.0 to v9.1” on page 504.

   Upon completion, shut down the Connectrix Manager 9.1 services and return to this page to complete step 6.

   From the Start menu, select Connectrix Manager 9.1, Stop Services.

6. Repeat step 2 through step 4, removing the space and the word doit.
Upgrading to Connectrix Manager 9.1

**Data migrated**

Specific data is migrated when you select the Yes option from the Copy Data and Settings dialog box when you upgrade the Connectrix Manager software on the Connectrix service processor. This section explains the data that is migrated and not migrated.

Data stored in the c:\EfcData directory is migrated to the comparable data directories on the new service processor running Connectrix Manager 9.1.

**User information**

Migrated user information includes:

- User ID
- Password (encrypted in MD5 format)
- User name
- User rights:
  - System Administrator — Transfers to Connectrix Manager 9.1 as the System Administrator user group.
  - Product Administrator — Transfers to Connectrix Manager 9.1 as the Product Administrator user group.
  - Operator — Transfers to Connectrix Manager 9.1 as the Operator user group.
  - Maintenance — Transfers to Connectrix Manager 9.1 as the Maintenance user group.

**Zoning**

Zones and zone sets are migrated to the default Zoning Library.

**Email event configuration**

All email addresses entered in the Connectrix Manager 7.x Configure Email dialog box will migrate to the Email Event Notification Setup User List under one user. You must modify the User List in Connectrix Manager 9.1 to assign addresses to individual users.
**Switch identification**

All switches and directors identified in the Connectrix Manager 7 Products view are migrated into Connectrix Manager discovery and are placed in the **Selected Individual Addresses** table of the **Discover Setup** dialog box. These switches will be managed by Connectrix Manager 9.1.

Note that if data did not migrate completely, you can enter the IP address of the switch in that dialog box.

**FAF libraries**

File access facility (FAF) library data is migrated. This includes all information from the **Configure Address - “Active”** dialog box (FICON management style only) in Connectrix Manager 7 Product Manager.

**Sessions configuration**

Information from the **Configure Sessions** dialog box is migrated:

- Network addresses of computers allowed or prohibited from remote sessions.
- Maximum number of remote sessions allowed.

**SNMP configuration**

All data from the SNMP configuration is migrated. This includes the enable/disable flag and 12 rows of trap information that is configured in the Connectrix Manager **Configure SNMP** dialog box.

**Firmware library**

The Firmware Library is migrated in the upgrade process; however, release rules are not. Since release rules are required, an error will result when you attempt to send a firmware version in the library to a switch. To avoid this problem, add the latest firmware file to the firmware library. This will also add the new release rules and resolve the problem.
Upgrading to Connectrix Manager 9.1

Logs

Product/Element Manager Audit, Event, Hardware, Link Incident, and Threshold Alert logs are migrated.

Nicknames

Nicknames configured through the Configure Nicknames dialog box in the Connectrix Manager are migrated.

Threshold alert configurations

Data input through the Configure Threshold Alert wizard in the Product Manager.
This data is not migrated:

- Configurations for optional Connectrix Manager features, such as Open Trunking, SANtegrity Binding, Enterprise Management Mode, and FlexPort. A Connectrix Manager 9.1 license key that contains these features must be installed.
- Except the firmware library, FAF files, and Product Manager logs, other Product Manager data is not migrated, since it is stored in switch memory for access by the Element Manager.
- 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.
- Files created using the **Backup and Restore Configuration** option in the Product Managers (NVRAM backup) are not migrated.
- Performance data from the Performance view in the Product Manager.
Post-upgrade configuration tasks

After upgrading to Connectrix Manager 9.1, you should perform the following tasks.

User configuration

Although user data from earlier Connectrix Manager versions is migrated, there are additional tasks that you must perform, such as configuring email addresses and filtering event notifications. Refer to Chapter 7, “Configuring User Groups,” for additional information.

Call Home

To set up the call home feature, you first specify the support center information through the call home configuration (call home icon in the Connectrix Manager desktop). You must also enable call home notification through the Event Notification option under the Monitor menu. For details refer to “Configure Call Home notification” on page 678.

Event notification

This includes configuring email and call home event notification. Refer to “Using event notification features” on page 251.

Note that all email addresses entered in the Connectrix Manager 6 or 7 Configure Email dialog box will migrate to the Connectrix Manager 9.1 Email Event Notification Setup User List under one user. You must modify the User List in Connectrix Manager 9.1 to assign addresses to individual users.

Configuring SAN devices

Perform the applicable procedures in Chapter 9, "Configuring SAN Products and Fabrics”. This includes steps for configuring Enterprise Fabric Mode (an optional feature), fabric binding (an optional feature), and trap forwarding.

Ethernet event notification

Ethernet Event notification is disabled.
Connectrix EC-1500 cabinet installation

For procedures on the physical installation of the Connectrix 1U rackmount service processor and keyboard, video and mouse (KVM) unit into the Connectrix cabinet refer to the Connectrix EC-1500 Cabinet Installation and Setup Manual, P/N 300-001-737, Rev A01.
This appendix describes the SNMP agent component in the Connectrix service processor. The Connectrix Manager SNMP agent implements the objects defined in the Fibre Channel Management (fcmgmt) MIB Version 3.1 and a small number of objects defined in MIB II. Through implementation of these MIB objects, the agent acts as a translator of information stored on the Connectrix service processor and attached directors into a form usable by SNMP management stations such as HP OpenView.

◆ Downloading MIB information ............................................. 530
◆ Fibre Channel Management MIB support............................ 533
◆ MIB-II support ................................................................. 605
**Downloading MIB information**

To access SNMP variables, download the necessary MIBs (listed in Figure 91 on page 532) to SNMP management stations from the Connectrix service processor’s web page using any standard Web browser. The URL for the web page depends on the Connectrix service processor’s host name on your network.

1. Obtain the address of the Connectrix service processor from your network administrator.

2. In a web browser, type the address into the Location (or Address) field, and press Enter.

   This displays the Connectrix Management page (Figure 90 on page 531).
EMC Connectrix Management

- Install Connectrix Manager remote client application
- Download SNMP MIB files

<table>
<thead>
<tr>
<th>Install Connectrix Manager Remote Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please follow the instructions for your</td>
</tr>
<tr>
<td>particular platform to install the</td>
</tr>
<tr>
<td>application.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Microsoft Windows 95/98/NT/2000/XP</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Microsoft Windows NT requires Service</td>
</tr>
<tr>
<td>Pack 5 to support the Java 2 platform</td>
</tr>
<tr>
<td>used by the installer program and the</td>
</tr>
<tr>
<td>Connectrix Manager application. If the</td>
</tr>
<tr>
<td>patches have been applied, click the</td>
</tr>
<tr>
<td>following button to begin the</td>
</tr>
<tr>
<td>installation process. You will receive</td>
</tr>
<tr>
<td>a Java Security warning requesting</td>
</tr>
<tr>
<td>permission to download and start the</td>
</tr>
<tr>
<td>installer program, and to read and</td>
</tr>
<tr>
<td>write files on your system. You must</td>
</tr>
<tr>
<td>grant these permissions to allow</td>
</tr>
<tr>
<td>installation of the Connectrix Manager</td>
</tr>
<tr>
<td>application.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Begin Windows Installation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Sun Solaris/SPARC</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Sun Solaris requires specific patches</td>
</tr>
<tr>
<td>to support the Java 2 platform used by</td>
</tr>
<tr>
<td>the installer program and the</td>
</tr>
<tr>
<td>Connectrix Manager application. Please</td>
</tr>
<tr>
<td>read the Solaris patch requirements</td>
</tr>
<tr>
<td>prior to installing the Connectrix</td>
</tr>
<tr>
<td>Manager application. If the patches</td>
</tr>
<tr>
<td>have been applied, click the following</td>
</tr>
<tr>
<td>button to begin the installation</td>
</tr>
<tr>
<td>process. You will receive a Java Security</td>
</tr>
<tr>
<td>warning requesting permission to</td>
</tr>
<tr>
<td>download and start the installer</td>
</tr>
<tr>
<td>program, and to read and write files</td>
</tr>
<tr>
<td>on your system. You must grant these</td>
</tr>
<tr>
<td>permissions to allow installation of</td>
</tr>
<tr>
<td>the Connectrix Manager application.</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Begin Solaris Installation</td>
</tr>
</tbody>
</table>

Figure 90  Connectrix Management web page

3. Click the Download SNMP MIB files link.
   This displays the MIB download area (Figure 91 on page 532).
### Download SNMP MIB Files

These MIB files are provided in standard ASN.1 syntax and may be installed into the MIB database of any SNMPv1 compliant Network Management Station.

<table>
<thead>
<tr>
<th>MIB Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FibreAlliance MIB v3.1</td>
<td>This MIB is implemented by the SNMP agent that runs on the Service Processor PC and a family of EMC Fibre Channel switch products including the ED-140M and ED-64M Directors and the DS-32M, DS-32M, DS-24M, DS-16M2 and DS-16M switches. Use the Configure option in the Connectrix Manager application or in the corresponding Connectrix Product Manager to configure access to this MIB from authorized SNMP Network Management Stations.</td>
</tr>
<tr>
<td>fcmgmt_v31.mib</td>
<td></td>
</tr>
<tr>
<td>FibreAlliance MIB v3.0</td>
<td>This MIB is implemented by the SNMP agent that runs on the Service Processor PC and a family of EMC Fibre Channel switch products including the ED-140M and ED-64M Directors and the DS-32M, DS-32M, DS-24M, DS-16M2 and DS-16M switches. Use the Configure option in the Connectrix Manager application or in the corresponding Connectrix Product Manager to configure access to this MIB from authorized SNMP Network Management Stations.</td>
</tr>
<tr>
<td>fcmgmt_v30.mib</td>
<td></td>
</tr>
<tr>
<td>SNMP Framework MIB</td>
<td>This MIB is needed to successfully compile and install the FibreAlliance MIB on the Network Management Station.</td>
</tr>
<tr>
<td>snmp-framework.mib</td>
<td></td>
</tr>
<tr>
<td>Fibre Channel Fabric Element MIB</td>
<td>These two MIB's are implemented by the SNMP agent that runs on the switch. Use the Configure option in the corresponding Connectrix Product Manager to configure access to these MIB's.</td>
</tr>
<tr>
<td>fcfbe.mib</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 91**  **SNMP MIB files download area**

4. Click a MIB to display it.

   To download a MIB, click **File, Save As** from the browser’s menu bar, and save the file to a local directory.
Fibre Channel Management MIB support

Notes on current support

Fibre Channel Management MIB (fcmgmt.mib) revision 200105080000Z is implemented in the Connectrix Manager and is embedded in the Connectrix M-series microcode. (Support for this MIB is not embedded in the ED-1032 microcode.)

The MIB conforms to SMIv2 rules, and defines nine groups of objects:

- Connectivity Unit Group
- Firmware Revisions
- Sensor Table
- Port Table
- Event Table
- Link Table
- Trap Registration Table
- Port Statistics
- SNS (nameserver) table

A single scalar object, revisionNumber, is defined under the Fibre Channel Management MIB base.

Connectrix Service Processor SNMP Agent

Connectrix service processor agent MIB objects

The following sections define the Fibre Channel Management MIB objects and how they are implemented in the Connectrix service processor SNMP agent. Unless otherwise noted, all MIB objects are read-only.

Connectivity Unit Group objects

The Connectivity Unit Group contains information about the directors and switches that are configured in the Connectrix service
The group contains five simple objects and four tables: Connectivity Unit, Firmware, Port, Sensor, and Event.

**Table 47 Connectrix Service Processor Connectivity Group table**

<table>
<thead>
<tr>
<th>Object type name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitNumber</td>
<td>INTEGER</td>
<td>The number of managed EMC units defined to the Connectrix service processor.</td>
<td>R</td>
<td>The number of connectivity units present on this system. May be a count of the boards in a chassis or the number of full boxes in a rack.</td>
</tr>
<tr>
<td>fcConnURL</td>
<td>DisplayString</td>
<td>http://[Connectrix Manager addr]/launch/start where [Connectrix Manager addr] is the network address of the Connectrix service processor.</td>
<td>R</td>
<td>The top-level URL of the system. If it does not exist the value is an empty string. The URL format is implementation dependent and can have keywords embedded that are preceded by a percent sign (e.g., %USER); The following are the defined keywords that will be recognized and replaced with data during a launch: USER — Replace with username PASSWORD — Replace with password GLOBALID — Replace with global ID SERIALNO — Replace with serial number A management application will read this object from the MIB, provide values for any of the keywords listed above that are present in the string, and then use the URL to invoke or launch the program referenced.</td>
</tr>
</tbody>
</table>
**Connectivity Unit table**

The connectivity unit table contains general information on the connectivity units. Each row in the table contains information for a particular switch/director.

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitId</td>
<td>OCTET STRING</td>
<td>WWN of switch/director</td>
<td>R</td>
<td>The unique identification for this connectivity unit among those within this proxy domain. The value must be unique within the proxy domain because it is the index variable for fcConnUnitTable. The value assigned to a given connectivity unit should be persistent across agent and unit resets. It should be the same as fcConnUnitGlobalId if fcConnUnitGlobalId is known and stable.</td>
</tr>
<tr>
<td>fcConnUnitGlobalId</td>
<td>FcGlobalId</td>
<td>WWN of switch/director</td>
<td>R</td>
<td>An optional global-scope identifier for this connectivity unit. It must be a WWN for this connectivity unit or 16 octets of value zero. WWN formats requiring fewer than 16 octets must be extended to 16 octets with trailing zero octets. If a WWN is used for fcConnUnitId, the same WWN must be used for fcConnUnitGlobalId. When a non-zero value is provided, it should be persistent across agent and unit resets. It should be globally unique. It should be one of these FC-PH/PH3 formats: IEEE (NAA=1) IEEE Extended (NAA=2) IEEE Registered (NAA=5) IEEE Registered extended (NAA=6)</td>
</tr>
</tbody>
</table>

(continued on next page)
Table 48  Connectrix Service Processor ConnUnit table  (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FcConnUnitGlobalId (continued)</td>
<td></td>
<td></td>
<td></td>
<td>Use of the IEEE formats allows any IEEE-registered vendor to assure global uniqueness independently. The following are some references on IEEE WWN formats:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://standards.ieee.org/regauth/oui/t">http://standards.ieee.org/regauth/oui/t</a> utorials/fibrecomp_id.html</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If one or more WWNs are associated with the connectivity unit via other management methods, one of them should be used for FcConnUnitGlobalId. If there is not a WWN assigned specifically to the connectivity unit, there is some merit, though not a requirement, to using a WWN assigned to (one of) its permanently attached FC/LAN interface(s). This cannot risk uniqueness, though. As a counterexample, if your agent runs in a host and the host has an HBA, it is quite possible that agent, host, and HBA will all be distinct connectivity units, so the host and agent cannot use the WWN of the HBA. Another example: If your hub has a built-in Ethernet port, it might be reasonable for the hub to use its LAN address (prefixed with the appropriate NAA) as its FcConnUnitId. But if the Ethernet were a replaceable PCCard, the hub should have an independent ID.</td>
</tr>
<tr>
<td>fcConnUnitType</td>
<td>FcUnitType</td>
<td>switch(4)</td>
<td>R</td>
<td>The type of this connectivity unit.</td>
</tr>
<tr>
<td>fcConnUnitNumPorts</td>
<td>Unsigned32</td>
<td>Number of ports from PROD_CNFG.</td>
<td>R</td>
<td>Number of physical ports in the connectivity unit (internal/embedded, external).</td>
</tr>
</tbody>
</table>
Fibre Channel Management MIB support

Connectrix Service Processor SNMP Agent

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitState</td>
<td>INTEGER</td>
<td>online and coming-online will indicate online state (2), and offline and going-offline will indicate offline state (3).</td>
<td>R</td>
<td>This object reports the overall state of the connectivity unit. The meaning of all values is essentially self-explanatory. Any of these values may occur with any of the fcConnUnitStatus values. The values are defined as follow: unknown (1), online (2), offline (3).</td>
</tr>
<tr>
<td>fcConnUnitStatus</td>
<td>INTEGER</td>
<td>This value will be mapped from current status of switch in such a way that operational status indicates ok (3), degraded status indicates warning (4), failed status indicate failed (5).</td>
<td>R</td>
<td>This object reports the overall status of the connectivity unit. The warning (4) value means that the connectivity unit needs attention; all other values are essentially self-explanatory. Any of these values may occur with any of the fcConnUnitState values. The values are defined as follow: unknown (1), unused (2), ok (3), warning(4), failed (5).</td>
</tr>
<tr>
<td>fcConnUnitProduct</td>
<td>SnmpAdminString</td>
<td>OEM product name.</td>
<td>R</td>
<td>The connectivity unit vendor's product model name.</td>
</tr>
<tr>
<td>fcConnUnitSerialNo</td>
<td>SnmpAdminString</td>
<td>OEM serial number.</td>
<td>R</td>
<td>The serial number identification for this connectivity unit.</td>
</tr>
<tr>
<td>fcConnUnitUpTime</td>
<td>TimeTicks</td>
<td></td>
<td>R</td>
<td>The number of centiseconds since the last unit initialization.</td>
</tr>
<tr>
<td>fcConnUnitUrl</td>
<td>DisplayString</td>
<td>Same as fcConnURL.</td>
<td>R</td>
<td>URL to launch a management application, if applicable. Otherwise empty string. In a standalone unit, this would be the same as the top-level URL. This has the same definition as systemURL for keywords.</td>
</tr>
<tr>
<td>fcConnUnitDomainId</td>
<td>OCTET STRING(3)</td>
<td>FFCCXX XX is the active domainId of the switch.</td>
<td>R</td>
<td>24-bit Fibre Channel address ID of this connectivity unit. Following the Fibre Channel standard, the right-most bit of the right-most octet is for the least significant bit of the address value; the left-most bit of the left-most octet, if needed, is for the most significant bit of the address value. If this value is not applicable, all bits set to 1.</td>
</tr>
</tbody>
</table>
### Connectix Service Processor ConnUnit table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitProxyMaster</td>
<td>INTEGER</td>
<td>yes (3)</td>
<td>R</td>
<td>A value of 'yes' means this is the proxy master unit for a set of managed units. For example, this could be the only unit with a management card in it for a set of units. A standalone unit should return 'yes' for this object. The values are defined as follow: unknown (1), no (2), yes (3).</td>
</tr>
<tr>
<td>fcConnUnitPrincipal</td>
<td>INTEGER</td>
<td></td>
<td>R</td>
<td>Whether this connectivity unit is the principal unit within the group of fabric elements. If this value is not applicable, return unknown. The values are defined as follow: unknown (1), no (2), yes (3).</td>
</tr>
<tr>
<td>fcConnUnitNumSensors</td>
<td></td>
<td></td>
<td>R</td>
<td>The number of sensors.</td>
</tr>
<tr>
<td>fcConnUnitNumRevs</td>
<td></td>
<td>1</td>
<td>R</td>
<td>The number of revisions in the fcConnUnitRevsTable.</td>
</tr>
<tr>
<td>fcConnUnitModuleId</td>
<td>OCTET STRING(16)</td>
<td>return 16 zeros (currently not supported).</td>
<td>R</td>
<td>This is a unique ID, persistent between boots, that can be used to group a set of connectivity units together into a module. The intended use would be to create a connectivity unit with a fcConnUnitType of 'module' to represent a physical or logical group of connectivity units. Then the members of the group would set the value of fcConnUnitId for this 'container' connectivity unit. FcConnUnitModuleId should be zeros if this connectivity unit is not part of a module.</td>
</tr>
<tr>
<td>fcConnUnitName</td>
<td>A textual string (up to 24 characters) of the name of the switch.</td>
<td></td>
<td>R/W</td>
<td>A name for this connectivity unit. This object value should be persistent between boots.</td>
</tr>
<tr>
<td>fcConnUnitInfo</td>
<td>SnmpAdminString</td>
<td></td>
<td>R/W</td>
<td>Information about this connectivity unit. This object value should be persistent between boots.</td>
</tr>
<tr>
<td>FA MIB object name</td>
<td>Type</td>
<td>Product mapping</td>
<td>Access</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------</td>
<td>--------</td>
<td>--------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fcConnUnitControl</td>
<td>INTEGER</td>
<td>Always return unknown (1) on read operation.</td>
<td>R/W</td>
<td>This object is used to control the addressed connectivity unit.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ResetConnUnitWarmStart (4), offlineConnUnit (5), and onlineConnUnit (6) will be</td>
<td></td>
<td>Note: 'ColdStart' and 'WarmStart' are as defined in mib-2 and are not meant to be a factory reset.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>supported by PCP.</td>
<td></td>
<td>ResetConnUnitColdStart: The addressed unit performs a 'ColdStart' reset.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ResetConnUnitWarmStart (4) indicates IPL on the switch is performed.</td>
<td></td>
<td>ResetConnUnitWarmStart: The addressed unit performs a 'WarmStart' reset.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OfflineConnUnit: The addressed unit puts itself into an implementation dependant</td>
<td></td>
<td>OfflineConnUnit: The addressed unit puts itself into an implementation dependant 'offline' state. In</td>
</tr>
<tr>
<td></td>
<td></td>
<td>'offline' state. In general, if a unit is in an offline state, it cannot be</td>
<td></td>
<td>general, if a unit is in an offline state, it cannot be used to perform meaningful Fibre Channel work.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OnlineConnUnit: The addressed unit puts itself into an implementation dependant</td>
<td></td>
<td>OnlineConnUnit: The addressed unit puts itself into an implementation dependant 'online' state. In</td>
</tr>
<tr>
<td></td>
<td></td>
<td>'online' state. In general, if a unit is in an online state, it is capable of</td>
<td></td>
<td>general, if a unit is in an online state, it is capable of performing meaningful Fibre Channel work.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>performing meaningful Fibre Channel work.</td>
<td></td>
<td>Note: Each implementation may chose not to support SNMP Set operations for any or all of these values.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>For Sets specifying varbinds for instances of this object and values not</td>
<td></td>
<td>For Sets specifying varbinds for instances of this object and values not supported by a given</td>
</tr>
<tr>
<td></td>
<td></td>
<td>supported by a given implementation, the agent will return the SNMP WrongValue</td>
<td></td>
<td>implementation, the agent will return the SNMP WrongValue PDU error code.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDU error code.</td>
<td></td>
<td>The values are defined as follow:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>unknown (1), invalid (2), resetConnUnitColdStart (3), resetConnUnitWarmStart (4), offlineConnUnit (5),</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>onlineConnUnit (6).</td>
</tr>
</tbody>
</table>

Table 48 Connectrix Service Processor ConnUnit table (continued)
### Table 48  Connectrix Service Processor ConnUnit table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitContact</td>
<td>SnmpAdminString</td>
<td>Contact information for this connectivity unit. Writable and persistent across IPL.</td>
<td>R/W</td>
<td>Contact information for this connectivity unit. The contact information is intended to facilitate contacting someone in case of problems, questions, etc. (e.g., the help desk internal to a company).</td>
</tr>
<tr>
<td>fcConnUnitLocation</td>
<td>SnmpAdminString</td>
<td>The physical location of the switch. Writable and persistent across IPL.</td>
<td>R/W</td>
<td>Location information for this connectivity unit.</td>
</tr>
<tr>
<td>fcConnUnitEventFilter</td>
<td>FcEventSeverity</td>
<td>Writable and it is set to the Default value of info(8) after IPL.</td>
<td>R/W</td>
<td>This value defines the event severity that will be logged by this connectivity unit. All events of severity less than or equal to fcConnUnitEventFilter are logged in the fcConnUnitEventTable.</td>
</tr>
<tr>
<td>fcConnUnitNumEvents</td>
<td></td>
<td>Number of events in the fcConnUnitEventTable. It is always &lt;= 200, the maximum size of the event table.</td>
<td>R</td>
<td>Number of events currently in the fcConnUnitEventTable.</td>
</tr>
<tr>
<td>fcConnUnitMaxEvents</td>
<td>Gauge(32bits)</td>
<td>200</td>
<td>R</td>
<td>Max number of events that can be recorded at any one time in the fcConnUnitEventTable.</td>
</tr>
<tr>
<td>fcConnUnitEventCurrID</td>
<td>Gauge(32bits)</td>
<td>The current event index is used as the last used event ID.</td>
<td>R</td>
<td>The last used event ID (fcConnUnitEventIndex) recorded in the fcConnUnitEventTable. When no events are presently recorded in the fcConnUnitEventTable, the value of this object must be zero.</td>
</tr>
</tbody>
</table>
Fibre Channel Management MIB support

**Firmware table**  
The firmware table contains information on the firmware revisions supported by a particular connectivity unit.

### Table 49  
**Connectrix Service Processor Firmware table**

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitRevsIndex</td>
<td>Gauge(32 bits)</td>
<td>Not accessible</td>
<td>Not accessible</td>
<td>A unique value among all fcConnUnitRevsEntries with the same value of fcConnUnitId, in the range between 1 and fcConnUnitNumRevs[fcConnUnitId].</td>
</tr>
<tr>
<td>fcConnUnitRevsRevision</td>
<td>SnmpAdminString</td>
<td>XX.XX.XX (The revision of the switch).</td>
<td>R</td>
<td>A vendor-specific value identifying a revision of a component of the connectivity unit.</td>
</tr>
<tr>
<td>fcConnUnitRevsDescription</td>
<td>SnmpAdminString</td>
<td>&quot;Switch Firmware Level&quot;</td>
<td>R</td>
<td>Description of a component in the fcConnUnit to which the revision corresponds.</td>
</tr>
</tbody>
</table>

**Sensor table**  
The sensor table contains information on the status of the fan and power supply components on a given director.

### Table 50  
**Connectrix Service Processor Sensor table**

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*fcConnUnitSensorIndex</td>
<td>Gauge(32 bits)</td>
<td>Not accessible</td>
<td>Not accessible</td>
<td>A unique value among all fcConnUnitSensorEntries with the same value of fcConnUnitId, in the range between 1 and fcConnUnitNumSensorEntries[fcConnUnitId].</td>
</tr>
<tr>
<td>FcConnUnitSensorName</td>
<td>SnmpAdminString</td>
<td>The module name of the FRU, such as FAN, PWR, or THM</td>
<td>R</td>
<td>A textual identification of the sensor intended primarily for operator use.</td>
</tr>
</tbody>
</table>

Fibre Channel Management MIB support
<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitSensorStatus</td>
<td>INTEGER</td>
<td>This value is evaluated from FRU status. The active, backup and update-busy states are mapped to ok (3). And the failed state is mapped to failed (5).</td>
<td>R</td>
<td>The status indicated by the sensor. The values are defined as follow: unknown (1) – the unit cannot determine the status, other (2) – the status does not fit any of the remaining values, ok (3) – indicates good status, warning (4) – indicates the unit needs attention, failed (5) B indicates the unit is non-functional.</td>
</tr>
<tr>
<td>fcConnUnitSensorInfo</td>
<td>SnmpAdminString</td>
<td>The serial number of the FRUs. It is not supported if the module is failed.</td>
<td>R</td>
<td>Miscellaneous static information about the sensor such as its serial number.</td>
</tr>
<tr>
<td>cConnUnitSensorMessage</td>
<td>SnmpAdminString</td>
<td>The textual description of the FRU status, such as “active” or “failed”.</td>
<td>R</td>
<td>This describes the status of the sensor as a message. It may also provide more resolution on the sensor indication, for example ‘Cover temperature 1503K, above nominal operating range’.</td>
</tr>
</tbody>
</table>
Table 50  Connectrix Service Processor Sensor table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitSensorType</td>
<td>INTEGER</td>
<td>fan (4) or power-supply (5)</td>
<td>R</td>
<td>The type of component being monitored by this sensor. The unknown (1) and other (2) values meanings analogous to those for the fcConnUnitSensorStatus object; all other values are essentially self-explanatory. The values are defined as follow: unknown (1), other (2), battery (3), fan (4), powerSupply (5), transmitter (6), enclosure (7), board (8), and receiver (9).</td>
</tr>
<tr>
<td>fcConnUnitSensorcharacteristic</td>
<td>INTEGER</td>
<td>Not supported. Always other (2)</td>
<td>R</td>
<td>The characteristics being monitored by this sensor. The unknown (1) and other (2) values meanings analogous to those for the fcConnUnitSensorStatus object; emf (5) refers to electromagnetic field; all other values are essentially self-explanatory. The values are defined as follow: unknown (1), other (2), temperature (3), pressure (4), emf (5), currentValue (6), airflow (7), frequency (8), and power (9).</td>
</tr>
</tbody>
</table>
The port table contains information on the physical ports on a given director.

### Table 51: Connectrix Service Processor Port table

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>fcConnUnitPortIndex</code></td>
<td>Unsigned32</td>
<td>The port index.</td>
<td>R</td>
<td>A unique value among all <code>fcConnUnitPortEntries</code> on this connectivity unit, between 1 and <code>fcConnUnitNumPorts</code>.</td>
</tr>
<tr>
<td><code>fcConnUnitPortType</code></td>
<td>INTEGER</td>
<td>If the port is Not installed notPresent(3)</td>
<td>R</td>
<td>The port type refers to the protocol active on the port and can take one of the following values: unknown (1) – cannot be determined, other (2) – none of the following, notPresent (3) – no port, hubPort (4) – hub port, nPort (5) – end port for fabric, iPort (6) – end port for loop, fIPort (7) – public loop, fPort (8) – fabric port, ePort (9) – fabric expansion port, gPort (10) – generic fabric port, domainController (11) – domain controller, hubController (12) – hub controller, scsi (13) – parallel SCSI port, escon (14) – escon port, lan (15) – LAN port, wan (16) – WAN port.</td>
</tr>
</tbody>
</table>
**Table 51  Connectrix Service Processor Port table (continued)**

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
</table>
| fcConnUnitPortFCClassCap      | FcPortFCClass | If the port is not installed, `fcConnUnitPortFCClassCap = 0`  
else if  
  H_Port 0x18 = class2(0x10) + class3(0x08)  
  B_Port 0x58 = classF(0x40) + class2(0x10) + class3(0x08)  
else it depends on the  
configured Port Type:  
  Gx_Port 0x58 = classF(0x40) + class2(0x10) + class3(0x08)  
  G_Port 0x58 = classF(0x40) + class2(0x10) + class3(0x08)  
  Fx_Port 0x18 = class2(0x10) + class3(0x08)  
  Fx_Port 0x18 = class2(0x10) + class3(0x08)  
  E_Port 0x58 = classF(0x40) + class2(0x10) + class3(0x08) | R      | Bit mask that specifies the classes of service capability of this port. If this object is not applicable, the agent MUST return all bits set to zero.                                                    |

| fcConnUnitPortFCClassOp       | FcPortFCClass | If the port is Not installed  
fcConnUnitPortFCClassOp = 0  
else if the Port State is offline  
fcConnUnitPortFCClassOp = 0  
else it depends on the  
operating Port Type:  
  Fx_Port Use Class of Service specified in Fabric Login  
  FL_Port Use Class of Service specified in one or more Fabric Login's (OR'd together)  
  E_Port 0x58 = classF(0x40) + class2(0x10) + class3(0x08) | R      | Bit mask that specifies the classes of service that are currently operational at this port. If this object is not applicable, the agent MUST return all bits set to zero. |
<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortState</td>
<td>INTEGER</td>
<td></td>
<td>R</td>
<td>The current state of the port hardware. The bypassed value (4) means that the port is online but is currently being isolated from the loop or fabric for some reason; the other values are essentially self-explanatory. Any value for this object may co-exist with any value for the fcConnUnitPortStatus object. The values are defined as follow: unknown (1), online (2), offline (3), bypassed (4).</td>
</tr>
</tbody>
</table>

*If port has InvalidAttachment, the port state is online.*
*If the port not installed, the port state is unknown.*
*If the port has a link failure, the port state is offline.*
*If the port is available, the port state is online.*
*If the port state is blocked, the port state is offline.*
*If the port is unavailable, the port state is online.*
*If the port is running internal diagnostics, the port state is diagnostics.*
*If the port is running external loops, the port state is diagnostics.*
*If the port experiences link reset, the port state is online.*
*If the port experiences link failure, the port state is online.*
*If the port shows service required, the port state is online.*
*If the port experiences port failure, the port state is online.*
*If the port is inactive, the port state is offline.*
*In any other cases, the port state is online (should not happen).*
*When link is down: return unknown (1).*
Fibre Channel Management MIB support

Connectrix Service Processor SNMP Agent

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatus</td>
<td>INTEGER</td>
<td>• If port has InvalidAttachment, the port state is online.</td>
<td>R</td>
<td>The current overall protocol status for the port. The warning value (4) means that the port needs attention; the notParticipating value (6) means that protocol is not being processed; the initializing value (7) means that the port has been manually or automatically isolated from the loop or fabric; the other values are essentially self-explanatory. Any value for this object may co-exist with any value for the fcConnUnitPortState object. The values are defined as follow: unknown (1), unused (2), ok (3), warning (4), failure (5), notParticipating (6), initializing (7), bypassed (8).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port not installed, the port state is unknown.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port has a link failure, the port state is offline.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is available, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port state is blocked, the port state is offline.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is unavailable, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is running internal diagnostics, the port state is diagnostics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is running external loops, the port state is diagnostics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port experiences link reset, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port experiences link failure, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port shows service required, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port experiences port failure, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is inactive, the port state is offline.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In any other cases, the port state is online (should not happen).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When link is down: return unknown (1).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Connectrix Service Processor SNMP Agent

**Table 51** Connectrix Service Processor Port table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortTransmitterType</td>
<td>INTEGER</td>
<td>This is mapped from the port technology as follow: not present and serial indicate unknown (1), optical sw1g and optical sw2g indicate shortwave (4). Optical lw1g and optical lw2g indicate longwave (5), copper db9 and copper amp indicate copper (6). (Get the value from port technology owned by FPM).</td>
<td>R</td>
<td>The technology of the port transceiver. The values are defined as follow: unknown (1), other (2), unused (3), shortwave (4) longwave (5), copper (6), and scsi (7), longwaveNoOFC (8), shortwaveNoOFC (9), longwaveLED (10).</td>
</tr>
<tr>
<td>fcConnUnitPortModuleType</td>
<td>INTEGER</td>
<td>If the port is not installed, return gbicNotInstalled (8). Otherwise return smallFormFactor (9).</td>
<td>R</td>
<td>The module type of the port connector. This object refers to the hardware implementation of the port. The embedded value (4) means ‘fixed’ (e.g., oneXnine). The values are defined as follow: unknown (1), other (2), gbic (3), embedded (4), glm (5), gbicSerialId (6), gbicNoSerialId (7), gbicNotInstalled (8), smallFormFactor (9).</td>
</tr>
<tr>
<td>fcConnUnitPortWwn</td>
<td>FcNameId</td>
<td>World Wide Name of the port.</td>
<td>R</td>
<td>The World Wide Name of the port. If applicable, otherwise empty string.</td>
</tr>
<tr>
<td>fcConnUnitPortFCId</td>
<td>OCTET STRING</td>
<td>If it is F-port, return fabric address of the node in form of [domain, area, node]. (Supported by Login Server) If it is E-port, return left-adjusted domain ID of the switch.</td>
<td>R</td>
<td>This is the assigned Fibre Channel ID of this port. This value is expected to be a Big Endian value of 24 bits. If this is loop, then it is the ALPA that is connected. If this is an Eport, then it will only contain the domain ID left justified, zero filled. If this port does not have a Fibre Channel address, return all bits set to 1.</td>
</tr>
<tr>
<td>fcConnUnitPortSerialNoSn</td>
<td>SnmpAdminString</td>
<td>Not applicable</td>
<td>R</td>
<td>The serial number identification of the unit (e.g., for a GBIC). If this is not applicable, return a zero-length string.</td>
</tr>
</tbody>
</table>

---

EMC Connectrix Manager User Guide
### Table 51: Connectrix Service Processor Port table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortRevision</td>
<td>SnmpAdminString</td>
<td>Not applicable</td>
<td>R</td>
<td>The port revision (e.g., for a GBIC).</td>
</tr>
<tr>
<td>fcConnUnitPortVendor</td>
<td>SnmpAdminString</td>
<td>Not applicable</td>
<td>R</td>
<td>The port vendor (e.g., for a GBIC).</td>
</tr>
<tr>
<td>fcConnUnitPortSpeed</td>
<td>Gauge (32 bits)</td>
<td>Return 100000 kilobytes for 1 Gb/s switches and 200000 kilobytes for 2 Gb/s switches.</td>
<td>R</td>
<td>The speed of the port in kilobytes per second.</td>
</tr>
<tr>
<td>fcConnUnitPortControl</td>
<td>INTEGER</td>
<td>ResetConnUnitPort(3), offlineConnUnitPort(6), onlineConnUnitPort(7), and portFailure(42501) are the only set-operations supported. Always return unknown (1) on read.</td>
<td>R/W</td>
<td>This object is used to control the addressed fcConnUnit's port. Valid commands are: Unknown (1) and invalid (2) are only used as values that are read. ResetConnUnitPort (3): If the addressed connectivity unit allows this operation to be performed on this port, the addressed port performs a vendor-specific 'reset' operation. Examples of these operations are: the Link Reset protocol, the Loop Initialization protocol, or a resynchronization occurring between the transceiver in the addressed port to the transceiver that the port is connected to. BypassConnUnitPort (4): If the addressed connectivity unit allows this operation to be performed to this port, the addressed port performs a vendor-specific 'bypass' operation. Examples of these operations are: transitioning from online to offline, a request (NON-PARTICIPATING) command to the Loop Port state machine, or removal of the port from an arbitrated loop by a hub. (continued on next page)</td>
</tr>
</tbody>
</table>
### Connectrix Service Processor Port Table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortControl</td>
<td></td>
<td></td>
<td></td>
<td>UnbypassConnUnitPort (5): If the addressed connectivity unit allows this operation to be performed to this port, the addressed port performs a vendor-specific 'unbypass' operation. Examples of these operations are: the Link Failure protocol, a request (PARTICIPATING) command to the Loop Port state machine, or addition of the OfflineConnUnitPort (6): If the addressed connectivity unit allows this operation to be performed to this port, the addressed port performs a vendor-specific 'offline' operation. Examples of these operations are: disabling a port’s transceiver, the Link Failure protocol, request (NON-PARTICIPATING) command to the Loop Port state machine, or removal of the port from an arbitrated loop by a hub. OnlineConnUnitPort (7): If the addressed connectivity unit allows this operation to be performed to this port, the addressed port performs a vendor-specific 'online' operation. Examples of these operations are: enabling a port’s transceiver, the Link Failure protocol, request (PARTICIPATING) command to the Loop Port state machine, or addition of the port from an arbitrated loop by a hub.</td>
</tr>
<tr>
<td>(continued)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 51  Connectrix Service Processor Port table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortControl (continued)</td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> Each implementation may chose not to support SNMP Set operations for any or all of these values. For Sets specifying varbinds for instances of this object and values not supported by a given implementation, the agent will return the SNMP WrongValue PDU error code.</td>
</tr>
<tr>
<td>fcConnUnitPortName</td>
<td>SnmpAdminString</td>
<td>Port name.</td>
<td>R/W</td>
<td>A string describing the addressed port.</td>
</tr>
<tr>
<td>fcConnUnitPortPhysicalNumber</td>
<td>Gauge (32 bits)</td>
<td>Physical port number from 0 to Maximum port number – 1</td>
<td>R</td>
<td>This is the internal port number this port is known by. In many implementations, this should be the same as fcConnUnitPortIndex. Some implementations may have an internal port representation not compatible with the rules for table indexes. In that case, provide the internal representation of this port in this object. This value may also be used in the fcConnUnitLinkPortNumberX or fcConnUnitLinkPortNumberY objects of the fcConnUnitLinkTable.</td>
</tr>
</tbody>
</table>
Table 51  Connectrix Service Processor Port table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortProtocolCap</td>
<td>OCTET STRING (2)</td>
<td>If the port is not installed fcConnUnitPortProtocolCap = 0</td>
<td>R</td>
<td>Bit mask that specifies the driver level protocol capability of this port. If this is not applicable, return all bits set to zero. The bits have the following definition: unknown – 0, Loop – 1, Fabric – 2, SCSI – 4, TCP/IP - 8, VI – 16, FICON – 32.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>else if Redcloud H_Port 1 = Loop(1) B_Port 2 = Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>else it depends on the configured Port Type: Gx_Port 3 = Loop(1) + Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>G_Port 2 = Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fx_Port 3 = Loop(1) + Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>F_Port 2 = Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E_Port 2 = Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortProtocolOp</td>
<td>OCTET STRING (2)</td>
<td>If the port is Not installed fcConnUnitPortProtocolOp = 0</td>
<td>R</td>
<td>Bit mask that specifies the driver level protocol(s) that are currently operational. If this is not applicable, return all bits set to zero. This object has the same definition as fcConnUnitPortProtocolCap.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>else if the Port State is offline fcConnUnitPortProtocolOp = 0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>else it depends on the operating Port Type: F_Port 2 = Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>FL_Port 1 = Loop(1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E_Port 2 = Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>H_Port 1 = Loop(1)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>B_Port 2 = Fabric(2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortNodeWwn</td>
<td>FcNameId</td>
<td>Switch/director WWN.</td>
<td>R</td>
<td>The Node World Wide Name of the port if applicable, otherwise all zeros. This should have the same value for a group of related ports. The container is defined as the largest physical entity. For example, all ports on HBAs on a host will have the same Node WWN. All ports on the same storage subsystem will have the same Node WWN.</td>
</tr>
</tbody>
</table>
**Table 51  Connectrix Service Processor Port Table (continued)**

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortHWState (added from Mib3.0)</td>
<td>INTEGER</td>
<td>• If port has InvalidAttachment, the port state is online.</td>
<td>R</td>
<td>The hardware detected state of the port. The values are defined as follow: unknown (1), failed (2) – port failed diagnostics,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port not installed, the port state is unknown.</td>
<td></td>
<td>bypassed (3) – FCAL bypass, loop only, active (4) – connected to a device, loopback (5) – Port in ext loopback, txfault (6) – Transmitter fault, noMedia (7) – media not installed, linkDown (8) – waiting for activity (rx sync).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port has a link failure, the port state is offline.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is available, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port state is blocked, the port state is offline.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is unavailable, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is running internal diagnostics, the port state is diagnostics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is running external loops, the port state is diagnostics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port experiences link reset, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port experiences link failure, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port shows service required, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port experiences port failure, the port state is online.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• If the port is inactive, the port state is offline.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• In any other cases, the port state is online (should not happen).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• When link is down: return unknown (1).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Event table**  
The table of connectivity unit events. Errors, warnings, and information should be reported in this table.

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitEventIndex</td>
<td>Gauge (32 bits)</td>
<td>Return the event index defined by MIB provider which follows the definition described in the connUnitEventIndex description.</td>
<td>R</td>
<td>Each connectivity unit has its own event buffer. As it wraps, it may write over previous events. This object is an index into the buffer. It is recommended that this table be read using 'getNext's to retrieve the initial table. The management application should read the event table at periodic intervals and then determine if any new entries were added by comparing the last known index value with the current highest index value. The management application should then update its copy of the event table. If the read interval is too long, it is possible that there may be events that may not be contained in the agent's internal event buffer. For example, an agent may read events 50-75. At the next read interval, fcConnUnitEventCurrID is 189. If the management app tries to read event index 76, and the agent's internal buffer is 100 entries max, event index 76 will no longer be available. The index value is an incrementing integer starting from one every time there is a table reset. On table reset, all contents are emptied and all indices are set to zero. When an event is added to the table, the event is assigned the next higher integer value than the last item entered into the table. If the index value reaches its maximum value, the next item entered will cause the index value to roll over and start at one again.</td>
</tr>
<tr>
<td>FA MIB object name</td>
<td>Type</td>
<td>Product mapping</td>
<td>Access</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fcConnUnitREventTime</td>
<td>DisplayString (0..15)</td>
<td>Return the time when the event occurred. When link is down: return NULL</td>
<td>R</td>
<td>This is the real time when the event occurred. It has the following format:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DDMYYYY HHMMSS</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DD = day number, MM = month number, YYYY = year number, HH = hour number, MM = minute number, SS = seconds number</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>If not applicable, return either a NULL string.</td>
</tr>
<tr>
<td>fcConnUnitSEventTime</td>
<td>TimeTicks</td>
<td>Can be translated from connUnitREventTime. When link is down: return NULL</td>
<td>R</td>
<td>This is the sysuptime timestamp when the event occurred.</td>
</tr>
<tr>
<td>fcConnUnitEventSeverity</td>
<td>FcEventSeverity</td>
<td>The mapping from switch event severity level to FcEventSeverity:</td>
<td>R</td>
<td>The event severity level:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SWITCH MIB</td>
<td></td>
<td>unknown (1)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>informational info (8)</td>
<td></td>
<td>emergency (2)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>minor error (5)</td>
<td></td>
<td>alert (3)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>major critical (4)</td>
<td></td>
<td>critical (4)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>severe emergency (2)</td>
<td></td>
<td>error (5)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>warning (6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>notify (7)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>info (8)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>debug (9)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>mark (10)</td>
</tr>
<tr>
<td>fcConnUnitEventType</td>
<td>INTEGER</td>
<td>Always return status (3). When link is down: return NULL</td>
<td>R</td>
<td>The type of this event. The values are defined as follow: unknown (1), other (2), status (3), configuration (4), topology (5).</td>
</tr>
<tr>
<td>fcConnUnitEventObject</td>
<td>OBJECT IDENTIFIER</td>
<td>Only the OID of a conUnit is returned. Other information is not supported.</td>
<td>R</td>
<td>This is used with the fcConnUnitEventType to identify which object the event refers to. It can be the OID of a connectivity unit or of another object like fcConnUnitPortStatus[...].</td>
</tr>
<tr>
<td>fcConnUnitEventDescr</td>
<td>SnmpAdminString</td>
<td>Return the event reason code description. When link is down: return NULL</td>
<td>R</td>
<td>The description of the event.</td>
</tr>
</tbody>
</table>
**Link table**

The link table contains information on the Fibre Channel links that exist between a particular director and a Fibre Channel device or another switch.

**Table 53 Connectrix Service Processor Link table**

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitLinkIndex</td>
<td>Gauge(32 bits)</td>
<td>Agent maintains this counter for all switches.</td>
<td>R</td>
<td>This index is used to create a unique value for each entry in the link table with the same connUnitLinkUnitId. The value can only be reused if it is not currently in use and the value is the next candidate to be used. This value wraps at the highest value represented by the size of the INTEGER. This value is reset to zero when the system is Reset and the first value to be used is one.</td>
</tr>
<tr>
<td>fcConnUnitLinkNodeIdX</td>
<td>OCTET STRING (16)</td>
<td>The WWN of this switch or device X.</td>
<td>R</td>
<td>The node WWN of the unit at one end of the link. If the node WWN is unknown and the node is a connUnit in the responding agent then the value of this object MUST BE equal to its connUnitID.</td>
</tr>
<tr>
<td>fcConnUnitLinkPortNumberX</td>
<td>Integer32</td>
<td>The port number of device X.</td>
<td>R</td>
<td>The port number on the unit specified by connUnitLinkNodeIdX if known, otherwise -1. If the value is nonnegative then it will be equal to connUnitPortPhysicalNumber.</td>
</tr>
<tr>
<td>fcConnUnitLinkPortWwnX</td>
<td>OCTET STRING</td>
<td>The port WWN of device X. Available when the attached device to this port is in LOGIN state. Otherwise all zeros.</td>
<td>R</td>
<td>The port WWN of the unit specified by connUnitLinkNodeIdX if known, otherwise 16 octets of binary 0.</td>
</tr>
<tr>
<td>fcConnUnitLinkNodeIdY</td>
<td>OCTET STRING (16)</td>
<td>The node WWN of device Y. Available when the attached device is in LOGIN state. Otherwise all zeros.</td>
<td>R</td>
<td>The node WWN of the unit at the other end of the link. If the node WWN is unknown and the node is a connUnit in the responding SNMP agency then the value of this object MUST BE equal to its connUnitID.</td>
</tr>
<tr>
<td>FA MIB object name</td>
<td>Type</td>
<td>Product mapping</td>
<td>Access</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------</td>
<td>-----------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fcConnUnitLinkPortNumberY</td>
<td>Integer32</td>
<td>The port number of device Y. Available for E/B ports. Unavailable for F/H ports (-1 is returned).</td>
<td>R</td>
<td>The port number on the unit specified by connUnitLinkNodeIdY if known, otherwise -1. If the value is nonnegative then it will be equal to connUnitPortPhysicalNumber.</td>
</tr>
<tr>
<td>fcConnUnitLinkPortWwnY</td>
<td>OCTET STRING</td>
<td>The port WWN of device Y when Y is an EMC M-series switch. RC- not supported (all zeros.)</td>
<td>R</td>
<td>The port WWN on the unit specified by connUnitLinkNodeIdY if known, otherwise 16 octets of binary 0.</td>
</tr>
<tr>
<td>fcConnUnitLinkAgentAddressY</td>
<td>OCTET STRING</td>
<td>(16)</td>
<td>R</td>
<td>The address of an FCMGMT MIB agent for the node identified by connUnitLinkNodeIdY, if known; otherwise 16 octets of binary 0.</td>
</tr>
<tr>
<td>fcConnUnitLinkAgentAddressTypeY</td>
<td>Unsigned32</td>
<td></td>
<td>R</td>
<td>If connUnitLinkAgentAddressY is nonzero, it is a protocol address. ConnUnitLinkAgentAddressType Y is the 'address family number' assigned by IANA to identify the address format. (e.g., 1 is Ipv4, 2 is Ipv6). If connUnitLinkAgentAddressY is all zeros, then this value is ignored.</td>
</tr>
<tr>
<td>fcConnUnitLinkAgentPortY</td>
<td>Unsigned32</td>
<td></td>
<td>R</td>
<td>The IP port number for the agent. This is provided in case the agent is at a non-standard SNMP port.</td>
</tr>
</tbody>
</table>
Port statistics

There is one and only one statistics table for each individual port. For all objects in statistics table, if the object is not supported by the conn unit then the high order bit is set to 1 with all other bits set to zero. The high order bit is reserved to indicate if the object is supported or not. All objects start at a value of zero at hardware initialization and continue incrementing till end of 63 bits and then wrap to zero.

The Port Statistics table contains Fibre Channel port statistics for a given director.

Table 53  Connectrix Service Processor Link table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitLinkUnitTypeY</td>
<td>FcUnitType</td>
<td>Switch(4) for E or B port. Otherwise return unknown(1).</td>
<td>R</td>
<td>Type of the FC connectivity unit as defined in connUnitType.</td>
</tr>
<tr>
<td>fcConnUnitLinkConnIdY</td>
<td>OCTET STRING</td>
<td>F-port: [domainId][areaCode][portNumber]</td>
<td>R</td>
<td>This is the Fibre Channel ID of this port. If the connectivity unit is a switch, this is expected to be a Big Endian value of 24 bits. If this is a loop, then it is the ALPA that is connected. If this is an E-port, then it will only contain the domain ID. If not any of those, unknown or cascaded loop, return all bits set to 1.</td>
</tr>
</tbody>
</table>

Table 54  Connectrix Service Processor Port Statistics table

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*fcConnUnitPortStatIndex</td>
<td>Unsigned32</td>
<td>A port number, starting from 1 to maximum number of ports.</td>
<td>R</td>
<td>A unique value among all entries in this table, between 0 and fcConnUnitNumPort[fcConnUnitPortUnitId]</td>
</tr>
</tbody>
</table>
### Table 54  Connectrix Service Processor Port Statistics table  (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountError</td>
<td>Counter64</td>
<td>This MIB object counts address ID errors, CRC errors, delimiter errors, frames too short, invalid transmission words, link failures, primitive sequence errors, signal losses, synchronization losses. (Only supports low 32 bits of counter, high 32 bits are set to zero.)</td>
<td>R</td>
<td>A count of the errors that have occurred on this port.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxObjects</td>
<td>Counter64</td>
<td>stTxFrames (64 bit counter)</td>
<td>R</td>
<td>The number of frames/packets/los/etc that have been transmitted by this port. Note: A Fibre Channel frame starts with SOF and ends with EOF. FC loop devices should not count frames passed through. This value represents the sum total for all other Tx objects.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountRxObjects</td>
<td>Counter64</td>
<td>stRxFrames (64 bit counter)</td>
<td>R</td>
<td>The number of frames/packets/los/etc that have been received by this port. Note: A Fibre Channel frame starts with SOF and ends with EOF. FC loop devices should not count frames passed through. This value represents the sum total for all other Rx objects.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxElements</td>
<td>Counter64</td>
<td>stTxOctets (64 bit counter)</td>
<td>R</td>
<td>The number of octets or bytes that have been transmitted by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput. Note, for Fibre Channel, ordered sets are not included in the count.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountRxElements</td>
<td>Counter64</td>
<td>stRxOctets (64 bit counter)</td>
<td>R</td>
<td>The number of octets or bytes that have been received by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput. Note, for Fibre Channel, ordered sets are not included in the count.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountBBCreditZero</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of transitions in/out of Bbcredit zero state. The other side is not providing any credit. Note, this is a Fibre Channel stat only.</td>
</tr>
<tr>
<td>FA MIB object name</td>
<td>Type</td>
<td>Mapping</td>
<td>Access</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------------</td>
<td>---------------</td>
<td>-------------</td>
<td>--------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fcConnUnitPortStatInputBuffersFull</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of occurrences when all input buffers of a port were full and outbound buffer-to-buffer credit transitioned to zero. There is no credit to provide to other side.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel stat only.</td>
</tr>
<tr>
<td>fcConnUnitPortStatFBSYFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of times that FBSY was returned to this port as a result of a frame that could not be delivered to the other end of the link. This occurs if either the Fabric or the destination port is temporarily busy. Port can only occur on SOFc1 frames (the frames that establish a connection).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat. This is the sum of all classes. If you cannot keep the by class counters, then keep the sum counters.</td>
</tr>
<tr>
<td>fcConnUnitPortStatPBSYFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of times that PBSY was returned to this port as a result of a frame that could not be delivered to the other end of the link. This occurs if the destination port is temporarily busy. PBSY can only occur on SOFc1 frames (the frames that establish a connection).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat. This is the sum of all classes. If you cannot keep the class counters, then keep the sum counters.</td>
</tr>
<tr>
<td>fcConnUnitPortStatFRJTFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of times that FRJT was returned to this port as a result of a Frame that was rejected by the fabric.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is the total for all classes and is a Fibre Channel only stat.</td>
</tr>
</tbody>
</table>
### Table 54  Connectrix Service Processor Port Statistics table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountPRJTFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of times that FRJT was returned to this port as a result of a Frame that was rejected at the destination N_Port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is the total for all classes and is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1RxFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of Class 1 Frames received at this port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1TxFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of Class 1 Frames transmitted out this port. Note, this is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1FBSYFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of times that FBSY was returned to this port as a result of a Class 1 Frame that could not be delivered to the other end of the link. This occurs if either the Fabric or the destination port is temporarily busy. FBSY can only occur on SOFc1 frames (the frames that establish a connection).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1PBSYFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of times that PBSY was returned to this port as a result of a Class 1 Frame that could not be delivered to the other end of the link. This occurs if the destination N. Port is temporarily busy. PBSY can only occur on SOFc1 frames (the frames that establish a connection).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
</tbody>
</table>
### Table 54  Connectrix Service Processor Port Statistics table  (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountClass1FRJTFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>Count of times that FRJT was returned to this port as a result of a Class 1 Frame that was rejected by the fabric.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1PRJTFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>Count of times that FRJT was returned to this port as a result of a Class 1 Frame that was rejected at the destination N_Port. Note, this is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2RxFrames</td>
<td>Counter64</td>
<td>stC2FramesIn (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td>Count of Class 2 Frames received at this port.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2TxFrames</td>
<td>Counter64</td>
<td>stC2FramesOut (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td>Count of Class 2 Frames transmitted out this port.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2FBSYFrames</td>
<td>Counter64</td>
<td>stC2FabricBusy (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td>Count of times that FBSY was returned to this port as a result of a Class 2 Frame that could not be delivered to the other end of the link. This occurs if either the Fabric or the destination port is temporarily busy. FBSY can only occur on SOFc1 frames (the frames that establish a connection).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FA MIB object name</td>
<td>Type</td>
<td>Mapping</td>
<td>Access</td>
</tr>
<tr>
<td>------------------------------------</td>
<td>----------</td>
<td>--------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2PBSYFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2FRJTFrames</td>
<td>Counter64</td>
<td>stC2FabricReject (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2PRJTFrames</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass3RxFrames</td>
<td>Counter64</td>
<td>stC3FramesIn (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass3TxFrames</td>
<td>Counter64</td>
<td>stC3FramesOut (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Connectrix Service Processor Port Statistics table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
</table>
| fcConnUnitPortStatCountClass3Discards | Counter64 | stC3Discards (64 bit counter)   | R      | Count of Class 3 Frames that were discarded upon reception at this port. There is no FBSY or FRJT generated for Class 3 Frames. They are simply discarded if they cannot be delivered.  
**Note:** This is a Fibre Channel only stat. |
| fcConnUnitPortStatCountRxMulticastObjects | Counter64 | Not supported                     | R      | Count of Multicast Frames or Packets received at this port.                                                                                                                                               |
| fcConnUnitPortStatCountTxMulticastObjects | Counter64 | Not supported                     | R      | Count of Multicast Frames or Packets transmitted out this port.                                                                                                                                            |
| fcConnUnitPortStatCountRxBroadcastObjects | Counter64 | Not supported                     | R      | Count of Broadcast Frames or Packets received at this port.                                                                                                                                              |
| fcConnUnitPortStatCountTxBroadcastObjects | Counter64 | Not supported                     | R      | Count of Broadcast Frames or Packets transmitted out this port. On a Fibre Channel loop, count only OPNr frames generated.                                             |
| fcConnUnitPortStatCountRxLinkResets     | Counter64 | stLinkResetsIn (Only supports low 32 bits of counter, high 32 bits are set to zero) | R      | Count of Link resets. This is the number of LRns received.  
**Note:** This is a Fibre Channel only stat. |
| fcConnUnitPortStatCountTxLinkResets     | Counter64 | stLinkResetsOut (Only supports low 32 bits of counter, high 32 bits are set to zero) | R      | Count of Link resets. This is the number LRns transmitted.  
**Note:** This is a Fibre Channel only stat. |
### Table 54  Connectrix Service Processor Port Statistics table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountNumberLinkResets</td>
<td>Counter64</td>
<td>StLinkResetsIn + StLinkResetsOut (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of Link resets and LIPs detected at this port. The number times the reset link protocol is initiated. These are the count of the logical resets, a count of the number of primitives.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountRxOfflineSequences</td>
<td>Counter64</td>
<td>StOlssIn (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of Offline Primitive OLS received at this port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxOfflineSequences</td>
<td>Counter64</td>
<td>StOlssOut (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of Offline Primitive OLS transmitted by this port. Adamseeters are the number times the reset link protocol is initiated. These are the count of the logical resets, a count of the number of primitives.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountNumberOfflineSequences</td>
<td>Counter64</td>
<td>StOlssIn + StOlssOut (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of Offline Primitive sequence received at this port. Doxing are the number times the reset link protocol is initiated. These are the count of the logical resets, a count of the number of primitives.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountLinkFailures</td>
<td>Counter64</td>
<td>StLinkFailures (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of link failures. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
</tbody>
</table>
### Table 54 Connectrix Service Processor Port Statistics (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountInvalidCRC</td>
<td>Counter64</td>
<td>stInvalidCrcs (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of frames received with invalid CRC. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Loop ports should not count CRC errors passing through when monitoring. Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountInvalidTxWords</td>
<td>Counter64</td>
<td>stInvalidTxWords (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of invalid transmission words received at this port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountPrimitiveSequenceProtocolErrors</td>
<td>Counter64</td>
<td>stPrimSeqProtoErrors (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of primitive sequence protocol errors detected at this port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountLossOfSignal</td>
<td>Counter64</td>
<td>stSigLosses (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of instances of signal loss detected at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>FA MIB object name</td>
<td>Type</td>
<td>Mapping</td>
<td>Access</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-----------</td>
<td>--------------------------------------</td>
<td>--------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountLossOfSynchronization</td>
<td>Counter64</td>
<td>stSyncLosses (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of instances of synchronization loss detected at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountInvalidOrderedSets</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of invalid ordered sets received at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountFramesTooLong</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of frames received at this port where the frame length was greater than what was agreed to in FLOGI/PLOGI. This could be caused by losing the end of frame delimiter. Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountFramesTruncated</td>
<td>Counter64</td>
<td>stFramesTooShort (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of frames received at this port where the frame length was less than the minimum indicated by the frame header – normally 24 bytes, but it could be more if the DFCTL field indicates an optional header should have been present. Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountAddressErrors</td>
<td>Counter64</td>
<td>stAddrIDErrors (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of frames received with unknown addressing. E.g. unknown SID or DID. The SID or DID is not known to the routing algorithm. Note: This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>FA MIB object name</td>
<td>Type</td>
<td>Mapping</td>
<td>Access</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------</td>
<td>----------------------------------------</td>
<td>--------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountDelimiterErrors</td>
<td>Counter64</td>
<td>stDelimiterErrors (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
<td>Count of invalid frame delimiters received at this port. An example is a frame with a class 2 start and a class 3 at the end.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountEncodingDisparityErrors</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
<td>Count of disparity errors received at this port.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
</tbody>
</table>
**Name Server table**

This table is accessed either directly if the management software has an index value or via GetNexts. The value of the indexes is not required to be contiguous. Each entry created in this table will be assigned an index. This relationship is kept persistent until the entry is removed from the table or the system is reset. The total number of entries is defined by the size of the table.

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitSnsPortIndex</td>
<td>UNSIGNED32 (Same as Gauge)</td>
<td>A port number, starting from 1 to maximum number of ports.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsPortIdentifier</td>
<td>FcAddressId</td>
<td>3 bytes FcAddress in the least significant bytes.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsPortName</td>
<td>FcNameId</td>
<td>Port WWN Name</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsNodeName</td>
<td>FcNameId</td>
<td>Node Name</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsClassOfSvc</td>
<td>OCTET STRING (SIZE (1))</td>
<td>Class of Service that matches the FC class service convention used in name server.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsNodeIPAddress</td>
<td>OCTET STRING (SIZE (16))</td>
<td>Node IP address</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsProcAssoc</td>
<td>OCTET STRING (SIZE (8))</td>
<td>Process Associator</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsFC4Type</td>
<td>OCTET STRING (SIZE (32))</td>
<td>FC4 type</td>
<td>R</td>
</tr>
</tbody>
</table>

*fcConnUnitSnsPortIndex*:
- Description: The physical port number of this SNS table entry. Each physical port has an SNS table with 1-n entries indexed by fcConnUnitSnsPortIdentifier (port address).

*fcConnUnitSnsPortIdentifier*:
- Description: The Port Identifier for this entry in the SNS table.

*fcConnUnitSnsPortName*:
- Description: The Port WWN Name for this entry in the SNS table.

*fcConnUnitSnsNodeName*:
- Description: The Node Name for this entry in the SNS table.

*fcConnUnitSnsClassOfSvc*:
- Description: The classes of service offered by this entry in the SNS table.

*fcConnUnitSnsNodeIPAddress*:
- Description: The Ipv6 formatted address of the Node for this entry in the SNS table. In order for this data to be present, IP address must have been registered with the switch.

*fcConnUnitSnsProcAssoc*:
- Description: The Process Associator for this entry in the SNS table. See FC-PH sec. 19.4.

*fcConnUnitSnsFC4Type*:
- Description: The FC-4 Types supported by this entry in the SNS table. Bitmap of FC-4 types supported.
### Table 55 Name Server table (continued)

<table>
<thead>
<tr>
<th>FA MIB object name</th>
<th>Type</th>
<th>Mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>fcConnUnitSnsPortType</strong></td>
<td>OCTET STRING</td>
<td>Port type</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>(SIZE (1))</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Port Type of this entry in the SNS table.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>fcConnUnitSnsPortIPAddress</strong></td>
<td>OCTET STRING</td>
<td>Port IP Address</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>(SIZE(16))</td>
<td></td>
<td></td>
</tr>
<tr>
<td>In order for this data to be present, IP address must have been registered with the switch.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>fcConnUnitSnsFabricPortName</strong></td>
<td>FcNameld</td>
<td>Fabric Port Name</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Fabric Port name of this entry in the SNS table.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>fcConnUnitSnsHardAddress</strong></td>
<td>FcGlobalId</td>
<td>Bytes address from name server in the least significant bytes.</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Hard ALPA of this entry in the SNS table. This address is device selected, not dynamically assigned.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>fcConnUnitSnsSymbolicPortName</strong></td>
<td>DisplayString</td>
<td>Symbolic port name</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>(SIZE (0..79))</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Symbolic Port Name of this entry in the SNS table.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>fcConnUnitSnsSymbolicNodeName</strong></td>
<td>DisplayString</td>
<td>Symbolic node name</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>(SIZE (0..79))</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The Symbolic Node Name of this entry in the SNS table.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The trap registration group allows for the control of trap generation on the Connectrix service processor SNMP agent. The group consists of two scalar objects and a trap registration table.

### Table 56 SNMP Trap Registration Group table

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcTrapMaxClients</td>
<td>Unsigned32</td>
<td>The maximum number of SNMP trap recipients can be supported in the system.</td>
<td>R</td>
<td>The maximum number of SNMP trap recipients supported by the connectivity unit.</td>
</tr>
<tr>
<td>fcTrapClientCount</td>
<td>Unsigned32</td>
<td>The current number of trap recipients.</td>
<td>R</td>
<td>The current number of rows in the trap table.</td>
</tr>
</tbody>
</table>

The Trap Registration table contains a row for each trap recipient. When the SNMP agent generates a trap a copy is sent to each of the recipients in the table depending upon the severity of the trap and the setting of the trapRegFilter object.

### Table 57 Trap Registration table

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcTrapRegIpAddress</td>
<td>IpAddress</td>
<td>Trap recipient’s IP address.</td>
<td>R/C</td>
<td>The IP address of a client registered for traps.</td>
</tr>
<tr>
<td>fcTrapRegPort</td>
<td>Unsigned32</td>
<td>UDP port.</td>
<td>R/C</td>
<td>The UDP port to send traps to for this host. Normally this would be the standard trap port (162).</td>
</tr>
<tr>
<td>fcTrapRegFilter</td>
<td>FcEventSeverity</td>
<td>The severity filter.</td>
<td>R/C</td>
<td>This value defines the trap severity filter for this trap host. The fcConnUnit will send to the designated target entity traps that have a severity level less than or equal to this value.</td>
</tr>
</tbody>
</table>
**fcTrapRegRowState**

**Type:** RowStatus

**Product mapping:** RowStatus

**Access:** R/C

**Description:** Specifies the operational status of the row. A RowStatus object may take any of six defined values:
- **active:** traps may be sent as specified in this row; a management application may change the value of any objects in the row when the status is active.
- **notInService:** traps will not be sent using this row.
- **notReady:** the conceptual row exists in the agent, but is missing information necessary to send traps (i.e., if any of the other objects in the row are not present or contain invalid values); this value may not be supplied by a management application.
- **createAndGo:** supplied by a management application wishing to create a new instance of a conceptual row, supplying valid values for all the other objects in the row, and have its status automatically set to active, making it available for use in sending traps.
- **createAndWait:** supplied by a management application wishing to create a new instance of a conceptual row but not make it available for use in sending traps at that time; and,
- **destroy:** supplied by a management application wishing to delete an existing conceptual row.

**Table 57 Trap Registration table (continued)**

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
</table>
| fcTrapRegRowState   | RowStatus | RowStatus       | R/C    | Specifies the operational status of the row. A RowStatus object may take any of six defined values:  
- active: traps may be sent as specified in this row; a management application may change the value of any objects in the row when the status is active.  
- notInService: traps will not be sent using this row.  
- notReady: the conceptual row exists in the agent, but is missing information necessary to send traps (i.e., if any of the other objects in the row are not present or contain invalid values); this value may not be supplied by a management application.  
- createAndGo: supplied by a management application wishing to create a new instance of a conceptual row, supplying valid values for all the other objects in the row, and have its status automatically set to active, making it available for use in sending traps.  
- createAndWait: supplied by a management application wishing to create a new instance of a conceptual row but not make it available for use in sending traps at that time; and,  
- destroy: supplied by a management application wishing to delete an existing conceptual row. |
The following FCMGMT MIB traps are generated from the Connectrix service processor when the SNMP agent is active and when one or more trap recipients have been configured in the Connectrix Manager.

### Table 58 Trap type table

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Type No.</th>
<th>Product mapping</th>
<th>OID and value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitStatusChange</td>
<td>1</td>
<td>Generated when the switch’s online status or operational status changes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitDeletedTrap</td>
<td>2</td>
<td>Not supported on the connUnit.</td>
<td>N/A</td>
<td>An fcConnUnit has been deleted from this agent. Recommended severity level (for filtering): warning</td>
</tr>
<tr>
<td>fcConnUnitEventTrap</td>
<td>3</td>
<td>Generated when a new event is generated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitSensorStatusChange</td>
<td>4</td>
<td>Generated when one of fans/powers status is changed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatusChange</td>
<td>5</td>
<td>Generated when a port state/status is changed.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The overall status of the connectivity unit has changed. Recommended severity level (for filtering): alert
The following sections define the director/switch MIB objects and how they are implemented in the product SNMP agent.

### Table 59  Director/ Switch type definition table

<table>
<thead>
<tr>
<th>Type</th>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FcNameId</td>
<td>OCTET STRING (SIZE(8))</td>
<td>Represents the World Wide Name (WWN; IEEE 60-bit variety; standard part of T11 definitions for fibre channel) associated with a Fibre Channel (FC) entity.</td>
</tr>
<tr>
<td>FcGlobalId</td>
<td>OCTET STRING (SIZE(16))</td>
<td>Represents the Worldwide Name (WWN; IEEE 124-bit variety) associated with a Fibre Channel (FC) entity.</td>
</tr>
<tr>
<td>FcEventSeverity</td>
<td>INTEGER</td>
<td>The set of values which define the event severity that will be logged by this connectivity unit. Values unknown (1) through debug (9) are essentially self-explanatory; mark (10) means that all messages are logged. The values are defined as follow: unknown (1), emergency (2), alert (3), critical (4), error (5), warning (6), notify (7), info (8), debug (9), mark (10).</td>
</tr>
<tr>
<td>FcUnitType</td>
<td>INTEGER</td>
<td>The values are defined as follow: unknown (1) – cannot be determined, other (2) -- none of the following, hub (3) -- passive connectivity unit supporting loop protocol, switch (4) -- active connectivity unit supporting multiple protocols, gateway (5) -- unit that converts not only the interface but also the frame into another protocol. The assumption is that there is always two gateways connected together. For example, FC &lt;-&gt; ATM, converter (6) -- unit that converts from one interface to another, For example, FC &lt;-&gt; SCSI, hba(7) -- host bus adapter, proxyAgent (8) -- software proxy-agent, storageDevice (9) -- disk, cd, tape, etc, host (10) -- host computer, storageSubsystem (11) -- raid, library, etc, module (12) -- subcomponent of a system, swDriver (13) -- software driver, storageAccessDevice (14) -- Provides storage management and access for heterogeneous hosts and heterogeneous devices.</td>
</tr>
<tr>
<td>FcPortFCClass</td>
<td>BITS</td>
<td>Represents the class(es) of service represented on a given port, in a given operational context. The values are defined as follow: unknown (0), classF (1), class1(2), class2 (3), class3 (4), class4 (5), class5 (6), class6 (7).</td>
</tr>
</tbody>
</table>
Connectivity Unit Group objects

The Connectivity Unit Group contains information about the director switches that are configured in the Connectrix service processor. The group contains five simple objects and four tables: Connectivity Unit, Firmware, Port, Sensor, and Event.

Table 60 Connectivity Unit Group table

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitNumber</td>
<td>INTEGER</td>
<td>1</td>
<td>R</td>
<td>The number of connectivity units present on this system. May be a count of the boards in a chassis or the number of full boxes in a rack.</td>
</tr>
<tr>
<td>fcConnURL</td>
<td>DisplayString</td>
<td><a href="http://switch's">http://switch's</a> IP-addr (The switch's IP address is Supported by PCP)</td>
<td>R</td>
<td>The top-level URL of the system. If it does not exist the value is an empty string. The URL format is implementation-dependent and can have keywords embedded that are preceded by a percent sign (e.g., %USER). The following are the defined keywords that will be recognized and replaced with data during a launch: USER – Replace with username. PASSWORD – Replace with password. GLOBALID – Replace with global ID. SERIALNO – Replace with serial number. A management application will read this object from the MIB, provide values for any of the keywords listed above that are present in the string, and then use the URL to invoke or launch the program referenced.</td>
</tr>
<tr>
<td>fcConnUnitSnsMaxRows</td>
<td>Counter32</td>
<td>The number of the entries of the Name Server Table.</td>
<td>R</td>
<td>The maximum number of rows in the fcConnUnitSnsTable table.</td>
</tr>
</tbody>
</table>

Fibre Channel Management MIB support
Connectivity Group table

The fcConnUnitTable contains general information on the system’s connectivity units.

**Table 61 fcConnUnit table**

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Product Mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitId</td>
<td>The unique identification for this connectivity unit among those within this proxy domain. The value must be unique within the proxy domain because it is the index variable for fcConnUnitTable. The value assigned to a given connectivity unit should be persistent across agent and unit resets. It should be the same as fcConnUnitGlobalId if fcConnUnitGlobalId is known and stable.</td>
<td>OCTET STRING</td>
<td>Switch WWN.</td>
</tr>
<tr>
<td>fcConnUnitGlobalId</td>
<td>An optional global-scope identifier for this connectivity unit. It must be a WWN for this connectivity unit or 16 octets of value zero. WWN formats requiring fewer than 16 octets must be extended to 16 octets with trailing zero octets. If a WWN is used for fcConnUnitId, the same WWN must be used for fcConnUnitGlobalId. When a non-zero value is provided, it should be persistent across agent and unit resets. It should be globally unique. It should be one of these FC-PH/PH3 formats: IEEE (NAA=1) IEEE Extended (NAA=2) IEEE Registered (NAA=5). IEEE Registered extended (NAA=6). Use of the IEEE formats allows any IEEE-registered vendor to assure global uniqueness independently. The following are some references on IEEE WWN formats: <a href="http://standards.ieee.org/regauth/oui/tutorials/fibreformat.html">http://standards.ieee.org/regauth/oui/tutorials/fibreformat.html</a> <a href="http://standards.ieee.org/regauth/oui/tutorials/fibrecomp_id.html">http://standards.ieee.org/regauth/oui/tutorials/fibrecomp_id.html</a>. If one or more WWNs are associated with the connectivity unit via other management methods, one of them should be used for fcConnUnitGlobalId. If there is not a WWN assigned specifically to the connectivity unit, there is some merit, though not a requirement, to using a WWN assigned to (one of) its permanently attached FC/LAN interface(s). This cannot risk uniqueness, though. As a counter example, if your agent runs in a host and the host has an HBA, it is quite possible that agent, host, and HBA will all be distinct connectivity units, so the host and agent cannot use the WWN of the HBA. Another example: if your hub has a built-in Ethernet port, it might be reasonable for the hub to use its LAN address (prefixed with the appropriate NAA) as its fcConnUnitId. But if the Ethernet were a replaceable PCCard, the hub should have an independent ID.</td>
<td>FcGlobalId</td>
<td>Switch WWN. (Supported by PCP)</td>
</tr>
<tr>
<td>fcConnUnitType</td>
<td>The type of this connectivity unit.</td>
<td>FcUnitType</td>
<td>switch(4)</td>
</tr>
<tr>
<td>fcConnUnitNumports</td>
<td>Number of physical ports in the connectivity unit (internal/embedded, external).</td>
<td>Unsigned32</td>
<td>Number of ports from PROD_CNFG.</td>
</tr>
</tbody>
</table>
### fcConnUnit table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product Mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitState</td>
<td>This object reports the overall state of the connectivity unit. The meaning of all values is essentially self-explanatory. Any of these values may occur with any of the fcConnUnitStatus values. The values are defined as follow: unknown (1), online (2), offline (3).</td>
<td>INTEGER</td>
<td>online and coming-online will indicate online state (2), and offline and going-offline will indicate offline state (3).</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitStatus</td>
<td>This object reports the overall status of the connectivity unit. The warning (4) value means that the connectivity unit needs attention; all other values are essentially self-explanatory. Any of these values may occur with any of the fcConnUnitState values. The values are defined as follow: unknown (1), unused (2), ok (3), warning (4), failed (5).</td>
<td>INTEGER</td>
<td>This value will be mapped from current status of switch in such a way that operational status indicates ok (3), degraded status indicates warning (4), failed status indicate failed (5). (Supported by PCP)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitProduct</td>
<td>The connectivity unit vendor’s product model name.</td>
<td>SnmpAdminString</td>
<td>The OEM product name. (This information is stored in VPD, supported by STATUSMGR)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSerialNo</td>
<td>The serial number identification for this connectivity unit.</td>
<td>SnmpAdminString</td>
<td>OEM serial number. (This information is stored in VPD, supported by STATUSMGR)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitUpTime</td>
<td>The number of centiseconds since the last unit initialization.</td>
<td>TimeTicks</td>
<td>Supported by MCK.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitUrl</td>
<td>URL to launch a management application, if applicable. Otherwise empty string. In a standalone unit, this would be the same as the top-level URL. This has the same definition as systemURL for keywords.</td>
<td>DisplayString</td>
<td>Same as fcConnURL.</td>
<td>R/W</td>
</tr>
<tr>
<td>fcConnUnitDomainId</td>
<td>24 bit Fibre Channel address ID of this connectivity unit. Following the Fibre Channel standard, the right-most bit of the right-most octet is for the least significant bit of the address value; the left-most bit of the left-most octet, if needed, is for the most significant bit of the address value. If this value is not applicable, all bits set to 1.</td>
<td>OCTET STRING (SIZE (3))</td>
<td>FFCCXX, where XX is the active domain id of the switch.</td>
<td>R</td>
</tr>
</tbody>
</table>
Table 61 fcConnUnit table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product Mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitProxyMaster</td>
<td>A value of 'yes' means this is the proxy master unit for a set of managed units. For example, this could be the only unit with a management card in it for a set of units. A standalone unit should return 'yes' for this object. The values are defined as follow: unknown (1), no (2), yes (3).</td>
<td>INTEGER</td>
<td>yes(3)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPrincipal</td>
<td>Whether this connectivity unit is the principal unit within the group of fabric elements. If this value is not applicable, return unknown. The values are defined as follow: unknown (1), no (2), yes (3).</td>
<td>INTEGER</td>
<td>Supported by Fab_contr1 subsystem</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitNumSensors</td>
<td>Number of sensors in the fcConnUnitSensorTable.</td>
<td>Unsigned32</td>
<td>The number of sensors</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitNumRevs</td>
<td>The number of revisions in the fcConnUnitRevsTable.</td>
<td>Unsigned32</td>
<td>1</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitModuleId</td>
<td>This is a unique ID persistent between boots, that can be used to group a set of connectivity units together into a module. The intended use would be to create a connectivity unit with a fcConnUnitType of 'module' to represent a physical or logical group of connectivity units. Then the members of the group would set the value of fcConnUnitId for this 'container' connectivity unit. fcConnUnitModuleId should be zeros if this connectivity unit is not part of a module.</td>
<td>OCTET STRING(SIZE(16))</td>
<td>return 16 zeros.(currently not supported)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitName</td>
<td>A name for this connectivity unit. This object value should be persistent between boots.</td>
<td>SnmpAdminString</td>
<td>switch’s configured name. (Supported by PCP)</td>
<td>R/W</td>
</tr>
<tr>
<td>fcConnUnitInfo</td>
<td>Information about this connectivity unit. This object value should be persistent between boots.</td>
<td>SnmpAdminString</td>
<td>A textual description of the product. (Supported by PCP)</td>
<td>R/W</td>
</tr>
</tbody>
</table>
### Table 61  \textit{fcConnUnit} table  (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **fcConnUnitControl** | This object is used to control the addressed connectivity unit.  

\textbf{NOTE:} 'ColdStart' and 'WarmStart' are as defined in mib-2 and are not meant to be a factory reset.  

- \texttt{resetConnUnitColdStart}: the addressed unit performs a 'ColdStart' reset.  
- \texttt{resetConnUnitWarmStart}: the addressed unit performs a 'WarmStart' reset.  
- \texttt{offlineConnUnit}: the addressed unit puts itself into an implementation dependant 'offline' state. In general, if a unit is in an offline state, it cannot be used to perform meaningful Fibre Channel work.  
- \texttt{onlineConnUnit}: the addressed unit puts itself into an implementation dependant 'online' state. In general, if a unit is in an online state, it is capable of performing meaningful Fibre Channel work.  

\textbf{Note:} Each implementation may chose not to support SNMP Set operations for any or all of these values. For Sets specifying varbinds for instances of this object and values not supported by a given implementation, the agent will return the SNMP WrongValue PDU error code.  

The values are defined as follow: unknown (1), invalid (2), \texttt{resetConnUnitColdStart} (3), \texttt{resetConnUnitWarmStart} (4), \texttt{offlineConnUnit} (5), \texttt{onlineConnUnit} (6).  

**INTEGER** Always return unknown (1) on read operation. \texttt{resetConnUnitWarmStart} (4), \texttt{offlineConnUnit} (5), and \texttt{onlineConnUnit} (6) will be supported by PCP. \texttt{resetConnUnitWarmStart} (4) indicates IPL on the switch is performed. \texttt{resetConnUnitColdStart} (3) is not supported.  

| **fcConnUnitContact** | Contact information for this connectivity unit. The contact information is intended to facilitate contacting someone in case of problems, questions, etc. (e.g., the help desk internal to a company).  

**SnmpAdminString** Contact information for this connectivity unit. (supported by PCP) Writable and persistent across IPL.  

| **fcConnUnitLocation** | Location information for this connectivity unit.  

**SnmpAdminString** The physical location of the switch. (Supported by PCP) Writable and persistent across IPL.  

| **fcConnUnitEventFilter** | This value defines the event severity that will be logged by this connectivity unit. All events of severity less than or equal to \texttt{fcConnUnitEventFilter} are logged in the \texttt{fcConnUnitEventTable}.  

**FcEventSeverity** Writable and it is set to the Default value of info(8) after IPL.  

| **fcConnUnitNumEvents** | Number of events currently in the \texttt{fcConnUnitEventTable}.  

**Unsigned32** Number of events in the \texttt{fcConnUnitEventTable}. it is always <= 200, the maximum size of the event table.  

The following values are supported by PCP.  

| **resetConnUnitWarmStart** | Indicates IPL on the switch is performed.  

\texttt{resetConnUnitColdStart} is not supported.  

| **offlineConnUnit** | The addressed unit puts itself into an implementation dependant 'offline' state.  

In general, if a unit is in an offline state, it cannot be used to perform meaningful Fibre Channel work.  

| **onlineConnUnit** | The addressed unit puts itself into an implementation dependant 'online' state. In general, if a unit is in an online state, it is capable of performing meaningful Fibre Channel work...  

Each implementation may chose not to support SNMP Set operations for any or all of these values. For Sets specifying varbinds for instances of this object and values not supported by a given implementation, the agent will return the SNMP WrongValue PDU error code.  

The values are defined as follow: unknown (1), invalid (2), \texttt{resetConnUnitColdStart} (3), \texttt{resetConnUnitWarmStart} (4), \texttt{offlineConnUnit} (5), \texttt{onlineConnUnit} (6).  

**INTEGER** Always return unknown (1) on read operation. \texttt{resetConnUnitWarmStart} (4), \texttt{offlineConnUnit} (5), and \texttt{onlineConnUnit} (6) will be supported by PCP. \texttt{resetConnUnitWarmStart} (4) indicates IPL on the switch is performed. \texttt{resetConnUnitColdStart} (3) is not supported.  

**R/W**
The firmware table lists the revisions supported by the associated connectivity units.

### Table 62  Firmware table

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product Mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;fcConnUnitRevsIndex&quot;</td>
<td>A unique value among all fcConnUnitRevsEntries with the same value of fcConnUnitId, in the range between 1 and fcConnUnitNumRevs[fcConnUnitId].</td>
<td>Unsigned32</td>
<td>Not accessible</td>
<td>R</td>
</tr>
<tr>
<td>&quot;fcConnUnitRevsRevision&quot;</td>
<td>A vendor-specific value identifying a revision of a component of the connectivity unit.</td>
<td>SnmpAdminString</td>
<td>XX.XX.XX (The reversion of the switch).</td>
<td>R</td>
</tr>
<tr>
<td>&quot;fcConnUnitRevsDescription&quot;</td>
<td>Description of a component in the fcConnUnit to which the revision corresponds.</td>
<td>SnmpAdminString</td>
<td>“Switch Firmware Level”</td>
<td>R</td>
</tr>
</tbody>
</table>
### Sensor table

The sensor table list the sensors supported by each connectivity unit.

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EMCCConnUnitSensorEntryIndex</td>
<td>A unique value among all fcConnUnitSensorEntries with the same value of fcConnUnitId, in the range between 1 and fcConnUnitNumSensors[fcConnUnitId].</td>
</tr>
<tr>
<td>EMCCConnUnitSensorName</td>
<td>A textual identification of the sensor intended primarily for operator use.</td>
</tr>
<tr>
<td>EMCCConnUnitSensorStatus</td>
<td>The status indicated by the sensor. The values are defined as follow: unknown (1) -- the unit cannot determine the status, other (2) -- the status does not fit any of the remaining values, ok (3) -- indicates good status, warning (4) -- indicates the unit needs attention, failed (5) -- indicates the unit is non-functional.</td>
</tr>
<tr>
<td>EMCCConnUnitSensorInfo</td>
<td>Miscellaneous static information about the sensor such as its serial number.</td>
</tr>
<tr>
<td>EMCCConnUnitSensorMessage</td>
<td>This describes the status of the sensor as a message. It may also provide more resolution on the sensor indication, for example 'Cover temperature 1503K, above nominal operating range'.</td>
</tr>
<tr>
<td>EMCCConnUnitSensorType</td>
<td>The type of component being monitored by this sensor. The unknown (1) and other (2) values meanings analogous to those for the fcConnUnitSensorStatus object; all other values are essentially self-explanatory. The values are defined as follow: unknown (1), other (2), battery (3), fan (4), powerSupply (5), transmitter (6), enclosure (7), board (8), and receiver (9).</td>
</tr>
<tr>
<td>EMCCConnUnitSensorCharacteristic</td>
<td>The characteristics being monitored by this sensor. The unknown (1) and other (2) values meanings analogous to those for the fcConnUnitSensorStatus object; emf (5) refers to electromagnetic field; all other values are essentially self-explanatory. The values are defined as follow: unknown (1), other (2), temperature (3), pressure (4), emf (5), currentValue (6), airflow (7), frequency (8), and power (9).</td>
</tr>
</tbody>
</table>
## Port Table

The port table provides generic information on ports for a specific fcConnUnit.

### Table 64 Port table

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Product mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortIndex</td>
<td>A unique value among all fcConnUnitPortEntries on this connectivity unit, between 1 and fcConnUnitNumPorts.</td>
<td>INTEGER</td>
<td>Not accessible.</td>
</tr>
<tr>
<td>fcConnUnitPortType</td>
<td>The port type refers to the protocol active on the port and can take one of the following values: unknown (1) -- cannot be determined, other (2) -- none of the following, notPresent (3) -- no port, hubPort (4) -- hub port, nPort (5) -- end port for fabric, iPort (6) -- end port for loop, fIPort (7) -- public loop, fPort (8) -- fabric port, ePort (9) -- fabric expansion port, gPort (10) -- generic fabric port, domainController (11) -- domain controller, hubController (12) -- hub controller, scsi (13) -- parallel SCSI port, escon (14) -- escon port, lan (15) -- LAN port, wan (16) -- WAN port.</td>
<td>INTEGER</td>
<td>It is f_port(8) if a device is connected to the port (Specified by login Server) or e_port(9) if a switch is connected to the port (Specified by Fabric Controller) otherwise it is g_port(10), if nothing is connected to the port.</td>
</tr>
<tr>
<td>fcConnUnitPortFCClassCap</td>
<td>Bit mask that specifies the classes of service capability of this port. If this object is not applicable, the agent MUST return all bits set to zero.</td>
<td>FcPortFCClass</td>
<td>For E, G port, return (26) = class_two(8) + class_three(16) + class_f(2). For F port, return (24) = class_two(8) + class_three(16).</td>
</tr>
<tr>
<td>fcConnUnitPortFCClassOp</td>
<td>Bit mask that specifies the classes of service that are currently operational at this port. If this object is not applicable, the agent MUST return all bits set to zero.</td>
<td>FcPortFCClass</td>
<td>For E port, return (26) = class_two(8) + class_three(16) + class_f(2). For G port, return unknown(0), For F port, return class_two(8) or class_three(16) or both. (The class of the services is decided through Login Server database)</td>
</tr>
<tr>
<td>fcConnUnitPortState</td>
<td>The current state of the port hardware. The bypassed value (4) means that the port is online but is currently being isolated from the loop or fabric for some reason; the other values are essentially self-explanatory. Any value for this object may co-exist with any value for the fcConnUnitPortStatus object. The values are defined as follow: unknown (1), online (2), offline (3), bypassed (4).</td>
<td>INTEGER</td>
<td>See PortStateMapping document: PortStateFuj2.0.doc.</td>
</tr>
</tbody>
</table>
### Table 64 Port table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatus</td>
<td>The current overall protocol status for the port. The warning value (4) means that the port needs attention; the notParticipating value (6) means that protocol is not being processed; the initializing value (7) means that the port is in the process of coming into service; the bypassed value (8) means that the port has been manually or automatically isolated from the loop or fabric; the other values are essentially self-explanatory. Any value for this object may co-exist with any value for the fcConnUnitPortStatus object. The values are defined as follow: unknown (1), unused (2), ok (3), warning (4), failure (5), notParticipating (6), initializing (7), bypassed (8).</td>
<td>INTEGER</td>
<td>See PortStateMapping document: PortStateFuji2.0.doc.</td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortTransmitterType</td>
<td>The technology of the port transceiver. The values are defined as follow: unknown (1), other (2), unused (3), shortwave (4), longwave (5), copper (6), and scsi (7), longwaveNoOFC (8), shortwaveNoOFC (9), longwaveLED (10).</td>
<td>INTEGER</td>
<td>This is mapped from the port technology as follow: not present and serial indicate unknown(1), optical sw1g and optical sw2g indicate shortwave(4), optical lw1g and optical lw2g indicate longwave(5), copper db9 and copper amp indicate copper(6). (Get the value from port technology owned by FPM).</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortModuleType</td>
<td>The module type of the port connector. This object refers to the hardware implementation of the port. The embedded value (4) means 'fixed' (e.g., oneXnine). The values are defined as follow: unknown (1), other (2), gbic (3), embedded (4), glm(5), gbicSerialId (6), gbicNoSerialId (7), gbicNotInstalled (8), smallFormFactor (9).</td>
<td>INTEGER</td>
<td>If the port is not installed, return gbicNotInstalled(8). Otherwise return smallFormFactor(9).</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortWwn</td>
<td>The World Wide Name of the port. If applicable, otherwise empty string.</td>
<td>FcNameId</td>
<td>World Wide Name of the port. (Supported by PCP)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortFCId</td>
<td>This is the assigned Fibre Channel ID of this port. This value is expected to be a Big Endian value of 24 bits. If this is loop, then it is the ALPA that is connected. If this is an eport, then it will only contain the domain ID left justified, zero filled. If this port does not have a Fibre Channel address, return all bits set to 1.</td>
<td>OCTET STRING</td>
<td>If it is F-port, return fabric address of the node in form of [domain, area, node]. (Supported by Login Server) If it is E-port, return left-adjusted domain ID of the switch.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortSerialNoSn</td>
<td>The serial number identification of the unit (e.g., for a GBIC). If this is not applicable, return a zero-length string.</td>
<td>SnmpAdminString</td>
<td>Not applicable.</td>
<td>R</td>
</tr>
</tbody>
</table>
### Table 64 Port table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortRevision</td>
<td>The port revision (e.g., for a GBIC).</td>
</tr>
<tr>
<td>fcConnUnitPortVendor</td>
<td>The port vendor (e.g., for a GBIC).</td>
</tr>
<tr>
<td>fcConnUnitPortSpeed</td>
<td>The speed of the port in kilobytes per second.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>SnmpAdminString</td>
<td>Not applicable.</td>
<td>R</td>
</tr>
<tr>
<td>SnmpAdminString</td>
<td>Not applicable.</td>
<td>R</td>
</tr>
<tr>
<td>Gauge32</td>
<td>Return 100000 kilobytes for 1 Gig switches and 200000 kilobytes for 2 Gig switches.</td>
<td>R</td>
</tr>
</tbody>
</table>
Table 64  Port table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortControl</td>
<td>This object is used to control the addressed fcConnUnit's port. Valid commands are:</td>
</tr>
<tr>
<td></td>
<td>Unknown (1) and invalid (2) are only used as values that are read.</td>
</tr>
<tr>
<td></td>
<td>ResetConnUnitPort (3): If the addressed connectivity unit allows this operation to be performed</td>
</tr>
<tr>
<td></td>
<td>on this port, the addressed port performs a vendor-specific 'reset' operation. Examples of</td>
</tr>
<tr>
<td></td>
<td>these operations are: the Link Reset protocol, the Loop Initialization protocol, or a</td>
</tr>
<tr>
<td></td>
<td>resynchronization occurring between the transceiver in the addressed port to the transceiver</td>
</tr>
<tr>
<td></td>
<td>to which the port is connected.</td>
</tr>
<tr>
<td></td>
<td>bypassConnUnitPort (4): If the addressed connectivity unit allows this operation to be</td>
</tr>
<tr>
<td></td>
<td>performed to this port, the addressed port performs a vendor-specific 'bypass' operation.</td>
</tr>
<tr>
<td></td>
<td>Examples of these operations are: transitioning from online to offline, a request (NON-</td>
</tr>
<tr>
<td></td>
<td>PARTICIPATING) command to the Loop Port state machine, or removal of the port from an</td>
</tr>
<tr>
<td></td>
<td>arbitrated loop by a hub.</td>
</tr>
<tr>
<td></td>
<td>unbypassConnUnitPort (5): If the addressed connectivity unit allows this operation to be</td>
</tr>
<tr>
<td></td>
<td>performed to this port, the addressed port performs a vendor-specific 'unbypass' operation.</td>
</tr>
<tr>
<td></td>
<td>Examples of these operations are: the Link Failure protocol, a request (PARTICIPATING)</td>
</tr>
<tr>
<td></td>
<td>command to the Loop Port state machine, or addition of the port to an arbitrated loop by a</td>
</tr>
<tr>
<td></td>
<td>hub.</td>
</tr>
<tr>
<td></td>
<td>offlineConnUnitPort (6): If the addressed connectivity unit allows this operation to be</td>
</tr>
<tr>
<td></td>
<td>performed to this port, the addressed port performs a vendor-specific 'offline' operation.</td>
</tr>
<tr>
<td></td>
<td>Examples of these operations are: disabling a port's transceiver, the Link Failure protocol,</td>
</tr>
<tr>
<td></td>
<td>request (NON-PARTICIPATING) command to the Loop Port state machine, or removal of the port</td>
</tr>
<tr>
<td></td>
<td>from an arbitrated loop by a hub.</td>
</tr>
<tr>
<td></td>
<td>onlineConnUnitPort (7): If the addressed connectivity unit allows this operation to be</td>
</tr>
<tr>
<td></td>
<td>performed to this port, the addressed port performs a vendor-specific 'online' operation.</td>
</tr>
<tr>
<td></td>
<td>Examples of these operations are: enabling a port's transceiver, the Link Failure protocol,</td>
</tr>
<tr>
<td></td>
<td>request (PARTICIPATING) command to the Loop Port state machine, or addition of the port from</td>
</tr>
<tr>
<td></td>
<td>an arbitrated loop by a hub.</td>
</tr>
<tr>
<td></td>
<td>Note: Each implementation may chose not to support SNMP Set operations for any or all of</td>
</tr>
<tr>
<td></td>
<td>these values. For Sets specifying varbinds for instances of this object and values not</td>
</tr>
<tr>
<td></td>
<td>supported by a given implementation, the agent will return the SNMP WrongValue PDU error code.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Type</th>
<th>Product mapping</th>
</tr>
</thead>
<tbody>
<tr>
<td>INTEGER</td>
<td>ResetConnUnitPort(3), offlineConnUnitPort(6), onlineConnUnitPort(7), and</td>
</tr>
<tr>
<td></td>
<td>portFailure(42501) are the only set-operations are supported. Always return</td>
</tr>
<tr>
<td></td>
<td>unknown(1) on read. (supported by PCP)</td>
</tr>
<tr>
<td>fcConnUnitPortName</td>
<td>A string describing the addressed port.</td>
</tr>
<tr>
<td>SnmpAdminString</td>
<td>Port Name</td>
</tr>
<tr>
<td></td>
<td>R/W</td>
</tr>
</tbody>
</table>

Fibre Channel Management MIB support
<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortPhysicalNumber</td>
<td>This is the internal port number this port is known by. In many implementations, this should be the same as fcConnUnitPortIndex. Some implementations may have an internal port representation not compatible with the rules for table indexes. In that case, provide the internal representation of this port in this object. This value may also be used in the fcConnUnitLinkPortNumberX or fcConnUnitLinkPortNumberY objects of the fcConnUnitLinkTable.</td>
<td>Unsigned32</td>
<td>Physical port number from 0 to Maximum port number - 1</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortProtocolCap (added from Mib3.0)</td>
<td>Bit mask that specifies the driver level protocol capability of this port. If this is not applicable, return all bits set to zero. The bits have the following definition: unknown - 0, Loop - 1, Fabric - 2, SCSI - 4, TCP/IP - 8, VI - 16, FICON - 32.</td>
<td>OCTET STRING</td>
<td>Fabric(2)</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortProtocolOp (added from Mib3.0)</td>
<td>Bit mask that specifies the driver level protocol(s) that are currently operational. If this is not applicable, return all bits set to zero. This object has the same definition as fcConnUnitPortProtocolCap.</td>
<td>OCTET STRING</td>
<td>Same as above</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortNodeWwn (added from Mib3.0)</td>
<td>The Node World Wide Name of the port if applicable, otherwise all zeros. This should have the same value for a group of related ports. The container is defined as the largest physical entity. For example, all ports on HBAs on a host will have the same Node WWN. All ports on the same storage subsystem will have the same Node WWN.</td>
<td>FcNameId</td>
<td>switch WWN</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortHWState (added from Mib3.0)</td>
<td>The hardware detected state of the port. The values are defined as follow: unknown (1), failed (2) -- port failed diagnostics, bypassed (3) -- FCAL bypass, loop only, active (4) -- connected to a device, loopback (5) -- Port in ext loopback, txfault (6) -- Transmitter fault, noMedia (7) -- media not installed, linkDown (8) -- waiting for activity (rx sync).</td>
<td>INTEGER</td>
<td>See PortStateMapping document: PortStateFuji2.0.doc.</td>
<td>R</td>
<td></td>
</tr>
</tbody>
</table>
Event table

The table of connectivity unit events. Errors, warnings, and information should be reported in this table.

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*fcConnUnitEventIndex</td>
<td>Each connectivity unit has its own event buffer. As it wraps, it may write over previous events. This object is an index into the buffer. It is recommended that this table be read using 'getNext's to retrieve the initial table. The management application should read the event table at periodic intervals and then determine if any new entries were added by comparing the last known index value with the current highest index value. The management application should then update its copy of the event table. If the read interval is too long, it is possible that there may be events that may not be contained in the agent's internal event buffer. For example, an agent may read events 50-75. At the next read interval, fcConnUnitEventCurrID is 189. If the management app tries to read event index 76, and the agent's internal buffer is 100 entries max, event index 76 will no longer be available. The index value is an incrementing integer starting from one every time there is a table reset. On table reset, all contents are emptied and all indices are set to zero. When an event is added to the table, the event is assigned the next higher integer value than the last item entered into the table. If the index value reaches its maximum value, the next item entered will cause the index value to roll over and start at one again.</td>
</tr>
<tr>
<td>fcConnUnitREventTime</td>
<td>This is the real time when the event occurred. It has the format: DDMMYYYY HHMMSS, where DD = day number, MM = month number, YYYY = year number, HH = hour number, MM = minute number, SS = seconds number. If not applicable, return a NULL string.</td>
</tr>
<tr>
<td>fcConnUnitSEventTime</td>
<td>This is the sysuptime timestamp when the event occurred.</td>
</tr>
<tr>
<td>fcConnUnitEventSeverity</td>
<td>The event severity level. The mapping from switch event severity level to FcEventSeverity:</td>
</tr>
<tr>
<td>FcEventSeverity</td>
<td>SWITCH informational info(8) minor error(5) major critical(4) severe emergency(2)</td>
</tr>
</tbody>
</table>


**Link table**

The link table is intended to organize and communicate any information the agent which would assist a management application to discover the CONNECTIVITY UNITS in the framework and the TOPOLOGY of their interconnect. That is, the goal is to assist the management application not only to LIST the elements of the framework, but to MAP them.

With this goal, the agent should include as much as it possesses about any links from its own connectivity units to others, including links among its own units.

An agent should include partial information about links if it is not able to fully define them. For an entry to be considered to be valid, both the X (local) and the Y (remote) need to have one valid value.

If the agent is able to discover links which do not directly attach to members of its agency and its discovery algorithm gives some assurance the links are recently valid, it MAY include these links.

Link information entered by administrative action MAY be included even if not validated directly if the link has at least one endpoint in this agency, but should not be included otherwise.

A connectivity unit can fill the table in as best it can. One of the methods to fill this in would be to use the RNID ELS (ANSI document 99-422v0). This allows one to query a port for the information needed for the link table.

---

**Table 65  Event table (continued)**

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitEventType</td>
<td>The type of this event. The values are defined as follow: unknown (1), other (2), status (3), configuration (4), topology (5).</td>
</tr>
<tr>
<td>fcConnUnitEventObject</td>
<td>This is used with the fcConnUnitEventType to identify which object the event refers to. It can be the OID of a connectivity unit or of another object like fcConnUnitPortStatus[...]</td>
</tr>
<tr>
<td>fcConnUnitEventDescr</td>
<td>The description of the event.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitEventType</td>
<td>INTEGER</td>
<td>Always status(3).</td>
<td></td>
</tr>
<tr>
<td>fcConnUnitEventObject</td>
<td>OBJECT IDENTIFIER</td>
<td>Only the OID of the fcConnUnit is returned. Other information is not supported.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitEventDescr</td>
<td>SnmpAdminString</td>
<td>&quot;Reason code XX&quot;, XX is the event reason code.</td>
<td>R</td>
</tr>
</tbody>
</table>
This table is accessed either directly if the management software has an index value or via GetNexts. The value of the indexes are not required to be contiguous. Each entry created in this table will be assigned an index. This relationship is kept persistent until the entry is removed from the table or the system is reset. The total number of entries are defined by the size of the table.

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitLinkIndex</td>
<td>This value is used to create a unique value for each entry in the link table with the same fcConnUnitId. The value can only be reused if it is not currently in use and the value is the next candidate to be used. This value is allowed to wrap at the highest value represented by the number of bits. This value is reset to zero when the system is reset and the first value to be used is 1.</td>
</tr>
<tr>
<td>fcConnUnitLinkIdX</td>
<td>The node WWN of the unit at one end of the link. If the node WWN is unknown and the node is a fcConnUnit in the responding agent then the value of this object MUST BE equal to its fcConnUnitId.</td>
</tr>
<tr>
<td>fcConnUnitLinkPortNumberX</td>
<td>The port number on the unit specified by fcConnUnitLinkIdX if known, otherwise -1. If the value is non-negative then it will be equal to fcConnUnitPortPhysicalNumber.</td>
</tr>
<tr>
<td>fcConnUnitLinkPortWwnX</td>
<td>The port WWN of the unit specified by fcConnUnitLinkIdX if known, otherwise 16 octets of binary 0.</td>
</tr>
<tr>
<td>fcConnUnitLinkIdY</td>
<td>The node WWN of the unit at the other end of the link. If the node WWN is unknown and the node is a fcConnUnit in the responding SNMP agent then the value of this object MUST BE equal to its fcConnUnitId.</td>
</tr>
</tbody>
</table>

### Table 66 Link table

<table>
<thead>
<tr>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>fcConnUnitLinkIndex</em></td>
<td>A link index.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkIdX</td>
<td>The WWN of the local fcConnUnit is returned. This information is available for both E and F ports</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkPortNumberX</td>
<td>The fcConnUnit’s local port number is returned. This information is available for both E and F ports.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkPortWwnX</td>
<td>The local side port WWN on the link. This information is available for both E and F ports.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkIdY</td>
<td>The attached node WWN on the link. This information is available for E ports and F ports. E port NodeIdY can be retrieved from RNID. F port NodeIdY is supported by FLOGI.</td>
<td>R</td>
</tr>
</tbody>
</table>
## Table 66  Link Table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitLinkPortNumberY</td>
<td>The port number on the unit specified by fcConnUnitLinkNodeIdY if known, otherwise -1. If the value is non-negative then it will be equal to fcConnUnitPortPhysicalNumber.</td>
<td>Integer32</td>
<td>The attached port number on the link. This information is available only for E ports from ISR. For F port, -1 is returned.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkPortWwnY</td>
<td>The port WWN on the unit specified by fcConnUnitLinkNodeIdY if known, otherwise 16 octets of binary 0.</td>
<td>OCTET STRING</td>
<td>The attached port WWN on the link. This information is available for F ports only. For E port, return 16 octets of binary 0.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkAgentAddressY</td>
<td>The address of an FCMGMT MIB agent for the node identified by fcConnUnitLinkNodeIdY, if known; otherwise 16 octets of binary 0.</td>
<td>OCTET STRING</td>
<td>Get the value from RNID, owned by Login Server.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkAgentAddressTypeY</td>
<td>If fcConnUnitLinkAgentAddressY is non-zero, then it is a protocol address. fcConnUnitLinkAgentAddressTypeY is the ‘address family number’ assigned by IANA to identify the address format. (e.g., 1 is Ipv4, 2 is Ipv6).</td>
<td>Unsigned32</td>
<td>Get the value from RNID, owned by Login Server.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkAgentPortY</td>
<td>The IP port number for the agent. This is provided in case the agent is at a non-standard SNMP port.</td>
<td>Unsigned32</td>
<td>Get the value from RNID, owned by Login Server.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkUnitTypeY</td>
<td>Type of the FC connectivity unit as defined in fcConnUnitType.</td>
<td>FcUnitType</td>
<td>If it is E port, return switch (4). Otherwise return RNID type Y.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitLinkConnIdY</td>
<td>This is the Fibre Channel ID of this port. If the connectivity unit is a switch, this is expected to be a 24-bit Big Endian value. If this is loop, then it is the ALPA that is connected. If this is an e-port, then it will only contain the domain ID. If not any of those, unknown or cascaded loop, return all bits set to 1.</td>
<td>OCTET STRING</td>
<td>For F ports, return Fibre Channel Address. For E ports, return left adjusted domainId of the switch.</td>
<td>R</td>
</tr>
</tbody>
</table>
**Port Statistics Table**

There is one and only one statistics table for each individual port. For all objects in statistics table, if the object is not supported by the conn unit then the high order bit is set to 1 with all other bits set to zero. The high order bit is reserved to indicate if the object if supported or not. All objects start at a value of zero at hardware initialization and continue incrementing till end of 63 bits and then wrap to zero.

### Table 67 Port Statistics Table

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product mapping from PSCC to switch</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatIndex</td>
<td>A unique value among all entries in this table, between 0 and fcConnUnitNumPort[fcConnUnitPortUnitId]</td>
<td>Gauge (32 bits)</td>
<td>A port number, starting from 1 to maximum number of ports.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountError</td>
<td>A count of the errors that have occurred on this port.</td>
<td>Counter64</td>
<td>This object counts:</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>- address ID errors</td>
<td></td>
<td>• address ID errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- CRC errors</td>
<td></td>
<td>• CRC errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- delimiter errors</td>
<td></td>
<td>• delimiter errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- frames too short</td>
<td></td>
<td>• frames too short</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- invalid transmission words</td>
<td></td>
<td>• invalid transmission words</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- link failures</td>
<td></td>
<td>• link failures</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- primitive sequence errors</td>
<td></td>
<td>• primitive sequence errors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- signal losses</td>
<td></td>
<td>• signal losses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- synchronization losses</td>
<td></td>
<td>• synchronization losses</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Supports only the low 32 bits of counter; high 32 bits are set to zero).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxObjects</td>
<td>The number of frames/packets/IOs/etc that have been transmitted by this port.</td>
<td>Counter64</td>
<td>stTxFrames (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td>Note: A Fibre Channel frame starts with SOF and ends with EOF. FC loop devices should not count frames passed through. This value represents the sum total for all other Tx objects.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 67 Port Statistics table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product mapping from PSCC to switch</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountRxObjects</td>
<td>The number of frames/packets/IOs/etc that have been received by this port.</td>
<td>Counter64</td>
<td>stRxFrames (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> A Fibre Channel frame starts with SOF and ends with EOF. FC loop devices should not count frames passed through. This value represents the sum total for all other Rx objects.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxElements</td>
<td>The number of octets or bytes that have been transmitted by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput.  [Note:** For Fibre Channel, ordered sets are not included in the count.</td>
<td>Counter64</td>
<td>stTxOctets (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountRxElements</td>
<td>The number of octets or bytes that have been received by this port. One second periodic polling of the port. This value is saved and compared with the next polled value to compute net throughput.  [Note:** For Fibre Channel, ordered sets are not included in the count.</td>
<td>Counter64</td>
<td>stRxOctets (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountBBCreditZero</td>
<td>Count of transitions in/out of BB_Credit zero state. The other side is not providing any credit.  [Note:** This is a Fibre Channel stat only.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountInputBuffersFull</td>
<td>Count of occurrences when all input buffers of a port were full and outbound buffer-to-buffer credit transitioned to zero. There is no credit to provide to other side. Note, this is a Fibre Channel stat only.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
</tbody>
</table>
Table 67  Port Statistics Table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product mapping from PSCC to switch</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountFBSYFrames</td>
<td>Count of times that FBSY was returned to this port as a result of a frame that could not be delivered to the other end of the link. This occurs if either the Fabric or the destination port is temporarily busy. Port can only occur on SOFc1 frames (the frames that establish a connection). Note: This is a Fibre Channel only stat. This is the sum of all classes. If you cannot keep the by class counters, then keep the sum counters.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountPBSYFrames</td>
<td>Count of times that PBSY was returned to this port as a result of a frame that could not be delivered to the other end of the link. This occurs if the destination port is temporarily busy. PBSY can only occur on SOFc1 frames (the frames that establish a connection). Note: This is a Fibre Channel only stat. This is the sum of all classes. If you cannot keep the by class counters, then keep the sum counters.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountFRJTFrames</td>
<td>Count of times that FRJT was returned to this port as a result of a Frame that was rejected by the fabric. Note: This is the total for all classes and is a Fibre Channel only stat.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountPRJTFrames</td>
<td>Count of times that FRJT was returned to this port as a result of a Frame that was rejected at the destination NxPort. Note: This is the total for all classes and is a Fibre Channel only stat.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1RxFrames</td>
<td>Count of Class 1 Frames received at this port. Note: This is a Fibre Channel only stat.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
</tbody>
</table>
### Port Statistics table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountClass1TxFrames</td>
<td>Count of Class 1 Frames transmitted out this port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td></td>
<td>Counter64</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1FBSYFrames</td>
<td>Count of times that FBSY was returned to this port as a result of a Class 1 Frame that could not be delivered to the other end of the link. This occurs if either the Fabric or the destination port is temporarily busy. FBSY can only occur on SOFc1 frames (the frames that establish a connection).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td></td>
<td>Counter64</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1PBSYFrames</td>
<td>Count of times that PBSY was returned to this port as a result of a Class 1 Frame that could not be delivered to the other end of the link. This occurs if the destination NxPort is temporarily busy. PBSY can only occur on SOFc1 frames (the frames that establish a connection).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td></td>
<td>Counter64</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1FRJTFrames</td>
<td>Count of times that FRJT was returned to this port as a result of a Class 1 Frame that was rejected by the fabric.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td></td>
<td>Counter64</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass1PRJTFrames</td>
<td>Count of times that FRJT was returned to this port as a result of a Class 1 Frame that was rejected at the destination NxPort.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td></td>
<td>Counter64</td>
</tr>
</tbody>
</table>
### Table 67 Port Statistics table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountClass2RxFrames</td>
<td>Count of Class 2 Frames received at this port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>Type</td>
<td>Product mapping from PSCC to switch</td>
</tr>
<tr>
<td>Counter64</td>
<td>stC2FramesIn (64 bit counter)</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2TxFrames</td>
<td>Count of Class 2 Frames transmitted out this port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>Type</td>
<td>Product mapping from PSCC to switch</td>
</tr>
<tr>
<td>Counter64</td>
<td>stC2FramesOut (64 bit counter)</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2FBSYFrames</td>
<td>Count of times that FBSY was returned to this port as a result of a Class 2 Frame that could not be delivered to the other end of the link. This occurs if either the Fabric or the destination port is temporarily busy. FBSY can only occur on SOFc1 frames (the frames that establish a connection).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>Type</td>
<td>Product mapping from PSCC to switch</td>
</tr>
<tr>
<td>Counter64</td>
<td>stC2FabricBusy (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2PBSYFrames</td>
<td>Count of times that PBSY was returned to this port as a result of a Class 2 Frame that could not be delivered to the other end of the link. This occurs if the destination N_Port is temporarily busy. PBSY can only occur on SOFc1 frames (the frames that establish a connection).</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>Type</td>
<td>Product mapping from PSCC to switch</td>
</tr>
<tr>
<td>Counter64</td>
<td>Not supported</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass2FRJTFrames</td>
<td>Count of times that FRJT was returned to this port as a result of a Class 2 Frame that was rejected by the fabric.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td>Type</td>
<td>Product mapping from PSCC to switch</td>
</tr>
<tr>
<td>Counter64</td>
<td>stC2FabricReject (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
</tr>
</tbody>
</table>
Table 67 Port Statistics table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product mapping from PSCC to switch</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitPortStatCountClass2PRJTFrames</td>
<td>Count of times that FRJT was returned to this port as a result of a Class 2 Frame that was rejected at the destination N_Port.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass3RxFrames</td>
<td>Count of Class 3 Frames received at this port.</td>
<td>Counter64</td>
<td>stC3FramesIn (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass3TxFrames</td>
<td>Count of Class 3 Frames transmitted out this port.</td>
<td>Counter64</td>
<td>stC3FramesOut (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountClass3Discards</td>
<td>Count of Class 3 Frames that were discarded upon reception at this port. There is no FBSY or FRJT generated for Class 3 Frames. They are simply discarded if they cannot be delivered.</td>
<td>Counter64</td>
<td>stC3Discards (64 bit counter)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountRxMulticastObjects</td>
<td>Count of Multicast Frames or Packets received at this port.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxMulticastObjects</td>
<td>Count of Multicast Frames or Packets transmitted out this port.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountRxBroadcastObjects</td>
<td>Count of Broadcast Frames or Packets received at this port.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxBroadcastObjects</td>
<td>Count of Broadcast Frames or Packets transmitted out this port. On a Fibre Channel loop, count only OPN frames generated.</td>
<td>Counter64</td>
<td>Not supported</td>
<td>R</td>
</tr>
<tr>
<td>EMC MIB object name</td>
<td>Description</td>
<td>Type</td>
<td>Product mapping from PSCC to switch</td>
<td>Access</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------</td>
<td>-------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountRxLinkResets</td>
<td>Count of Link resets. This is the number of LRs received.</td>
<td>Counter64</td>
<td>StLinkResetsIn (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxLinkResets</td>
<td>Count of Link resets. This is the number LRs transmitted.</td>
<td>Counter64</td>
<td>StLinkResetsOut (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountNumberLinkResets</td>
<td>Count of Link resets and LIPs detected at this port. The number times the reset link protocol is initiated. These are the count of the logical resets, a count of the number of primitives.</td>
<td>Counter64</td>
<td>StLinkResetsIn + StLinkResetsOut (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountRxOfflineSequences</td>
<td>Count of Offline Primitive OLS received at this port.</td>
<td>Counter64</td>
<td>StoIssIn (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountTxOfflineSequences</td>
<td>Count of Offline Primitive OLS transmitted by this port. Note, this is a Fibre Channel only stat.</td>
<td>Counter64</td>
<td>StoIssOut (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td>EMC MIB object name</td>
<td>Description</td>
<td>Type</td>
<td>Product mapping from PSCC to switch</td>
<td>Access</td>
</tr>
<tr>
<td>--------------------</td>
<td>-------------</td>
<td>------------</td>
<td>------------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>fcConnUnitPortStatCountNumberOfflineSequences</td>
<td>Count of Offline Primitive sequence received at this port.</td>
<td>Counter64</td>
<td>stOlssIn + stOlssOut (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountLinkFailures</td>
<td>Count of link failures. This count is part of the Link Error Status Block (LESB), (FC-PH 29.8).</td>
<td>Counter64</td>
<td>stLinkFailures (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountInvalidCRC</td>
<td>Count of frames received with invalid CRC. This count is part of the Link Error Status Block (LESB), (FC-PH 29.8). Loop ports should not count CRC errors passing through when monitoring.</td>
<td>Counter64</td>
<td>stInvalidCrcs (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountInvalidTxWords</td>
<td>Count of invalid transmission words received at this port. This count is part of the Link Error Status Block (LESB), (FC-PH 29.8).</td>
<td>Counter64</td>
<td>stInvalidTxWords (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountPrimitiveSequenceProtocolErrors</td>
<td>Count of primitive sequence protocol errors detected at this port. This count is part of the Link Error Status Block (LESB), (FC-PH 29.8).</td>
<td>Counter64</td>
<td>stPrimSeqProtoErrors (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td>R</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>EMC MIB object name</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountLossOfSignal</td>
<td>Count of instances of signal loss detected at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counter64 stSigLosses (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountLossOfSynchronization</td>
<td>Count of instances of synchronization loss detected at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counter64 stSyncLosses (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountInvalidOrderedSets</td>
<td>Count of invalid ordered sets received at port. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counter64 Not supported</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountFramesTooLong</td>
<td>Count of frames received at this port where the frame length was greater than what was agreed to in FLOGI/PLOGI. This could be caused by losing the end of frame delimiter.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counter64 Not supported</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>fcConnUnitPortStatCountFramesTruncated</td>
<td>Count of frames received at this port where the frame length was less than the minimum indicated by the frame header - normally 24 bytes, but it could be more if the DFCTL field indicates an optional header should have been present.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Counter64 stFramesTooShort (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Connectrix Service Processor SNMP Agent

**Table 67 Port Statistics table (continued)**

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fCConnUnitPortStatCountAddressErrors</td>
<td>Count of frames received with unknown addressing, e.g. unknown SID or DID. The SID or DID is not known to the routing algorithm.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td></td>
<td>Type: Counter64                                                                                        Access: R</td>
</tr>
<tr>
<td></td>
<td>stAddrIDErrors (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
</tr>
<tr>
<td>fCConnUnitPortStatCountDelimiterErrors</td>
<td>Count of invalid frame delimiters received at this port. An example is a frame with a class 2 start and a class 3 at the end.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td></td>
<td>Type: Counter64                                                                                        Access: R</td>
</tr>
<tr>
<td></td>
<td>stDelimiterErrors (Only supports low 32 bits of counter, high 32 bits are set to zero)</td>
</tr>
<tr>
<td>fCConnUnitPortStatCountEncodingDisparityErrors</td>
<td>Count of disparity errors received at this port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This is a Fibre Channel only stat.</td>
</tr>
<tr>
<td></td>
<td>Type: Counter64                                                                                        Access: R</td>
</tr>
<tr>
<td></td>
<td>Not supported</td>
</tr>
</tbody>
</table>

**Name Server table** This table is accessed either directly if the management software has an index value or via GetNexts. The value of the indexes is not required to be contiguous. Each entry created in this table will be assigned an index. This relationship is kept persistent until the entry is removed from the table or the system is reset. The total number of entries is defined by the size of the table.

**Table 68 Name Server table**

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*fCConnUnitSnsPortIndex</td>
<td>The physical port number of this SNS table entry. Each physical port has an SNS table with 1-n entries indexed by fCConnUnitSnsPortIdentifier (port address)</td>
</tr>
<tr>
<td></td>
<td>Type: Counter64                                                                                        Access: R</td>
</tr>
<tr>
<td></td>
<td>INTEGER</td>
</tr>
<tr>
<td></td>
<td>A port number, starting from 1 to maximum number of ports.</td>
</tr>
</tbody>
</table>
### Table 68 Name Server table (continued)

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Description</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitSnsPortIdentifier</td>
<td>The Port Identifier for this entry in the SNS table.</td>
<td>FcAddressId</td>
<td>3 bytes FcAddress in the least significant bytes.</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsPortName</td>
<td>The Port WWN Name for this entry in the SNS table.</td>
<td>FcNameId</td>
<td>Port WWN Name</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsNodeName</td>
<td>The Node Name for this entry in the SNS table.</td>
<td>FcNameId</td>
<td>Node Name</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsClassOfSvc</td>
<td>The Classes of Service offered by this entry in the SNS table.</td>
<td>OCTET STRING (SIZE (1))</td>
<td>Class of Service that matches the FC class service convention used in name server</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsNodeIPAddress</td>
<td>The IPv6 formatted address of the Node for this entry in the SNS table.</td>
<td>OCTET STRING (SIZE(16))</td>
<td>Node IP address</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsProcAssoc</td>
<td>The Process Associator for this entry in the SNS table.</td>
<td>OCTET STRING (SIZE (8))</td>
<td>Process Associator</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsFC4Type</td>
<td>The FC-4 Types supported by this entry in the SNS table.</td>
<td>OCTET STRING (SIZE (32))</td>
<td>FC4 type</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsPortType</td>
<td>The Port Type of this entry in the SNS table.</td>
<td>OCTET STRING (SIZE (1))</td>
<td>Port type</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsPortIPAddress</td>
<td>The IPv6 formatted address of this entry in the SNS table.</td>
<td>OCTET STRING (SIZE(16))</td>
<td>Port IP Address</td>
<td>R</td>
</tr>
<tr>
<td>fcConnUnitSnsFabricPortName</td>
<td>The Fabric Port name of this entry in the SNS table.</td>
<td>FcNameId</td>
<td>Fabric Port Name</td>
<td>R</td>
</tr>
</tbody>
</table>
Connectrix Service Processor SNMP Agent

The trap registration group allows for the control of trap generation on the SNMP agent. The group consists of two scalar objects and a trap registration table.

**Table 69 Trap Registration Group table**

<table>
<thead>
<tr>
<th>EMC MIB object name</th>
<th>Type</th>
<th>Product mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcTrapMaxClients</td>
<td>Unsigned32</td>
<td>The maximum number of SNMP trap recipients can be supported in the system.</td>
<td>R</td>
<td>The maximum number of SNMP trap recipients supported by the connectivity unit.</td>
</tr>
<tr>
<td>fcTrapClientCount</td>
<td>Unsigned32</td>
<td>The current number of trap recipients</td>
<td>R</td>
<td>The current number of rows in the trap table.</td>
</tr>
</tbody>
</table>

**Table 70 SNMP Trap Registration table**

<table>
<thead>
<tr>
<th>EMC MIB Object Name</th>
<th>Type</th>
<th>Product Mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*fcTrapRegIpAddress</td>
<td>IpAddress</td>
<td>Trap recipient's IP address.</td>
<td>R/C</td>
<td>The IP address of a client registered for traps.</td>
</tr>
</tbody>
</table>
Table 70  SNMP Trap Registration table  (continued)

<table>
<thead>
<tr>
<th>EMC MIB Object Name</th>
<th>Type</th>
<th>Product Mapping</th>
<th>Access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcTrapRegPort</td>
<td>Unsigned32</td>
<td>UDP port.</td>
<td>R/C</td>
<td>The UDP port to send traps to for this host. Normally this would be the standard trap port (UDP/162).</td>
</tr>
<tr>
<td>fcTrapRegFilter</td>
<td>FcEventSeverity</td>
<td>(This information not exposed in SNMP configuration dialog)</td>
<td>R/C</td>
<td>This value defines the trap severity filter for this trap host. The fcConnUnit will send to the designated target entity traps that have a severity level less than or equal to this value.</td>
</tr>
<tr>
<td>fcTrapRegRowState</td>
<td>RowStatus</td>
<td>Row status.</td>
<td>R/C</td>
<td>Operational status of the row. A RowStatus object may take any of six defined values:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• active (1): traps may be sent as specified in this row. A management application may change the value of any objects in the row when the status is active.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• notInService (2): traps will not be sent using this row.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• notReady (3): The conceptual row exists in the agent, but is missing information necessary to send traps (i.e., if any of the other objects in the row are not present or contain invalid values); this value may not be supplied by a management application.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• createAndGo (4): supplied by a management application wishing to create a new instance of a conceptual row, supplying valid values for the all other objects in the row, and have its status automatically set to active, making it available for use in sending traps.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• createAndWait (5): supplied by a management application wishing to create a new instance of a conceptual row but not make it available for use in sending traps at that time; and,</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>• destroy (6): supplied by a management application wishing to delete an existing conceptual row.</td>
</tr>
</tbody>
</table>
**Trap type table**

This table shows trap types.

<table>
<thead>
<tr>
<th>Trap name</th>
<th>Type No.</th>
<th>Product mapping</th>
<th>OID and value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fcConnUnitStatusChange</td>
<td>1</td>
<td>Generated when the switch=s online status or operational status changes</td>
<td>&quot;.1.3.6.1.2.1.8888.1.1.3.1.6&quot; + unitld fcConnUnitStatus,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;1.3.6.1.2.1.8888.1.1.3.1.5&quot; + unitld fcConnUnitState</td>
<td></td>
</tr>
<tr>
<td>fcConnUnitDeletedTrap</td>
<td>2</td>
<td>Not supported on the connUnit.</td>
<td>N/A</td>
<td>An fcConnUnit has been deleted from this agent. Recommended severity level (for filtering): warning</td>
</tr>
<tr>
<td>fcConnUnitEventTrap</td>
<td>3</td>
<td>Generated when a new event is generated.</td>
<td>&quot;.1.3.6.1.2.1.8888.1.1.7.1.1&quot; + unitld fcConnUnitEventIndex,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;1.3.6.1.2.1.8888.1.1.7.1.5&quot; + unitld fcConnUnitEventType,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;1.3.6.1.2.1.8888.1.1.7.1.6&quot; + unitld fcConnUnitEventObject,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;1.3.6.1.2.1.8888.1.1.7.1.7&quot; + unitld fcConnUnitEventDescr</td>
<td>An event has been generated by the connectivity unit. Recommended severity level (for filtering): info</td>
</tr>
<tr>
<td>fcConnUnitSensorStatusChange</td>
<td>4</td>
<td>Generated when one of fans/powers status is changed.</td>
<td>&quot;.1.3.6.1.2.1.8888.1.1.5.1.3&quot; + unitld + sensor_nbr fcConnUnitSensorState</td>
<td>The overall status of the connectivity unit has changed. Recommended severity level (for filtering): alert</td>
</tr>
<tr>
<td>fcConnUnitPortStatusChange</td>
<td>5</td>
<td>Generated when a port state/status is changed.</td>
<td>&quot;.1.3.6.1.2.1.8888.1.1.6.1.6&quot; + unitld + port_nbr fcConnUnitPortStatus,</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>&quot;1.3.6.1.2.1.8888.1.1.6.1.5&quot; + unitld + port_nbr fcConnUnitPortState</td>
<td>The overall status of the connectivity unit has changed. Recommended severity level (for filtering): alert</td>
</tr>
</tbody>
</table>
MIB-II support

The Connectrix service processor SNMP agent supports 2 objects from MIB-II:

Table 72  Supported MIB-II Objects

<table>
<thead>
<tr>
<th>Object</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sysObject ID</td>
<td>Returns 1.3.6.1.4.1.289.</td>
</tr>
<tr>
<td>sysUpTime</td>
<td>Returns the total length of time that the Connectrix Manager SNMP agent has been running.</td>
</tr>
</tbody>
</table>

Generic traps

The following generic traps are generated by the Connectrix service processor SNMP agent:

- **warmStart** — Reports that the Connectrix Manager SNMP agent is reinitializing.
- **linkUp** — Signals that one of the agent’s communications links has come up.
- **authenticationFailure** — An indication that the agent has received an improperly authenticated protocol message. This trap is disabled by default but may be enabled using the Connectrix Manager.
This appendix provides instructions for updating the configuration properties file.

- Specifying a host IP address in multi-NIC networks .................. 608
- Editing master log settings .................................................. 609
Specifying a host IP address in multi-NIC networks

When you have multiple network card server/hosts (two cards in the same machine), you must configure the trap event distributor to know which network card it should listen to for receiving traps.

To change the IP address, you need to edit the `smp.server.edipaddress` variable to instruct the trap event distributor to use a specific IP address.

To specify an IP address for the trap event distributor, complete the following steps.

1. Open the `<Install_Home>\resources\Server\config.properties` file using a text editor (for example, Notepad).
2. Add the following line:
   ```
   smp.server.edipaddress=x.x.x.x
   ```
   (where `x.x.x.x` is the desired IP Address)
3. Save the file and restart the server.
**Editing master log settings**

The application keeps a log of events that occur in the SAN. By default, the event history is kept for 45 days, until 100 MB of disk space is taken up, or when the number of entries reaches 2000.

You can manually change the retention period and the disk space usage assigned to entries in the Master Log. For a list of the editable parameters, refer to Table 73.

To edit the master log settings, complete the following steps.

1. Open the `<Install_Home>/resources/Server/config.properties` file using a text editor (for example, Notepad).

2. Add the following lines:

   ```
   # Maximum space reserved for the log (where XX is a value between 1MB and 1024MB, inclusive)
   smp.log.maxLogDiskSpace=XX
   # Maximum number of days to retain the log (where XX is the number of days between 1 and 365 to retain the log)
   smp.log.maxLogRetentionDays=XX
   ```

3. Save the file and restart the server.

Table 73  
Master log parameters

<table>
<thead>
<tr>
<th>Type</th>
<th>Default</th>
<th>Minimum</th>
<th>Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Retention Days</td>
<td>45 days</td>
<td>1 day</td>
<td>365 days</td>
</tr>
<tr>
<td>Log Disk Space</td>
<td>1000 MB</td>
<td>1 MB</td>
<td>4096 MB</td>
</tr>
</tbody>
</table>
This appendix provides instructions for using the SANtegrity Security Center.

- SANtegrity Security Center features .................................................. 612
- Accessing the Security Center ............................................................. 614
- Security window components ............................................................ 615
- Managing updates to security data ..................................................... 617
- About the security tabs ...................................................................... 618
- Using the Security tabs ...................................................................... 619
- Working with virtual fabrics ............................................................... 621
- Setting authentication methods ........................................................... 622
- CHAP secrets ...................................................................................... 623
- Accessing the Users tab ...................................................................... 624
- Security Authentication Users tab ....................................................... 625
- Accessing the Software tab ................................................................. 631
- Security Authentication Software tab ................................................ 632
- Accessing the Devices tab ................................................................. 640
- Security Authentication Devices tab .................................................. 641
- Accessing the IP Access Control tab .................................................... 650
- Security Authentication IP Access Control tab ................................... 651
- Accessing Radius Servers tab ............................................................. 655
- Security Authentication Radius Servers tab ....................................... 656
- Accessing the Security Log ................................................................. 661
- Viewing the Security Log ................................................................. 662
SANtegrity Security Center features

The SANtegrity Security Center (Security Center) is a tool for viewing and configuring your installation’s Fibre Channel authentication parameters. The Security Center provides a single central User Interface for managing the authentication settings of all SANtegrity-capable switches and directors in the installation. The Security Center features are accessed from the Security tab. These features include:

- Security policy management.
- Application of fabric-wide settings to storage network devices.
- Support of a mediated secret management system and security-centric reporting and logging.
- Reports of the storage network configuration, security events and ports or settings that are out of policy to serve as warnings against potential misuse.
- Summaries of the security configuration for each security-capable device in each fabric.
- User-friendly interface with configuration tabs for updating each switch’s SANtegrity authentication values. Each tab relates to a specific authentication task. For example, there is a tab to define which users are allowed to sign on to the switch to perform management tasks, and which management interfaces are enabled. Another tab allows you to define the IP addresses from which management requests may originate, and whether the switch or director will limit management requests based on originating IP address.
- The ability to easily apply changes to all switches or directors in a fabric. This key feature allows you to define the authentication parameters for one switch, and, by a few simple additional clicks, propagate the changes to one or more additional switches in the fabric. Thus, the Security Administrator can view and manage security settings for entire fabrics at once.
- A Security Log containing a record of all security-related configuration updates, as well as security-related events such as illegal login requests.
The Security Center is designed to be a single point of control for the Security Administrator. Although the Element Manager has the ability to configure the SANtegrity parameters for a single switch, only the Security Center provides installation-wide Fibre Channel security configuration and monitoring.
### Accessing the Security Center

The SANtegrity Security Center feature requires a license key, and is not available unless the Security license key is installed on the server. The SANtegrity Security Center is accessed from the Security tab on the main window and displays Fabric information, Authentication information, Master Log, and Security Log.

Access the SANtegrity Security Center by clicking the Security tab or F8 on the main window. In order to use the Security Center, you must have Security Administrator privilege.

**Note:** If discovery is not complete when the Security tab is first accessed, a message may temporarily display advising you that the device cannot be configured because it is not currently managed by the server.

To change the default display, place the cursor on the divider until a double arrow displays. Click and drag the adjoining divider to resize the window. You can also show or hide an area by clicking the left or right arrow on the divider.

**Note:** On the tool bar the **Display By** option and the **Search Box** option are disabled.
Security window components

The Security window contains five regions or components for viewing and configuring security features — the Fabrics List, the Authentication table, the Security tabs, the Master Log, and the Security Log.

Fabrics list

The upper left part of the Security window shows the Fabrics list. The Fabrics list displays all discovered fabrics listed by their WWNs with their operational status on the left side if the status is available. When a fabric is selected from the left side, all Switches and Directors within the fabric are displayed in the top table. This includes devices not managed by this Server and offline devices.

Although all devices display, only products managed by the Server can be configured. These products display with their corresponding product icon. This product icon is the same one that displays on the topology map.

If a product is not managed by this SAN application Server, the product displays a generic icon.

If discovery is not complete when the Security tab is first accessed, a message may temporarily display informing you that the device cannot be configured because it is not currently managed by the server.

Authentication table

The upper right part of the Security window displays the main working area, which includes the Authentication Product Configuration table. The table contains a summary of security-related values for each switch or director in a fabric. This table automatically refreshes to reflect the latest changes to the products listed. Some information is not available for switches and directors that are not managed or that are not at the correct firmware level.

Note: 256-Port Directors do not work with a web server interface. Therefore, if you view the product configuration information for a 256-Port Director, the columns related to web server information show N/A.
**SANtegrity Security Center**

---

**Security tabs**

The lower part of the main work area is a tabbed pane containing a set of five tabs for completing security configuration tasks.

---

**Master Log**

The lower left part of the Security window displays the server Master Log.

---

**Security Log**

The lower right part of the window displays the Security Log.
Managing updates to security data

We recommend that a single Security Administrator make updates to the security configuration. However, if security data is changed from another interface, such as your Web Server interface or Telnet while the Security Center is in view, the security administrator is notified so that the administrator can decide whether to accept the changes.

Data changes from other sources

If the security settings for a switch or director are changed from another management interface, then the following occurs:

- If the switch or director that has been changed from another interface is not currently being configured by your Connectrix Manager application user, and the top table reflects the changes.
- If the changes made from another interface affect the switch or director whose security data is currently being modified by a security administrator, a message displays indicating the security settings have been changed from an external source. The message allows you to choose whether to load the new settings from the switch or director or keep your changes.
- Click Load New Settings, and the information in the display on the top table and configuration on the bottom tab update. All working data is overridden by the new data in the switch or director.
- Click Keep Changes, and the updates are not reflected in the tab. You can continue entering changes in the tab. When all changes are entered, click the Apply or Apply To button to send them to the switch or director and override the externally entered changes.

Verifying changes in the Change Confirmation and Status dialog box

After you enter any changes in the Security Authentication tabs, your click Apply or Apply to (if you are populating a group of products). The final dialog box you are presented before your changes are applies is the Change Confirmation and Status dialog box.

This dialog box allows you to carefully review the changes before proceeding with the updates.
About the security tabs

There are five tabs in the Authentication section:

- The Users tab allows the security administrator to configure the user management interfaces to the switch or director. With the Users tab, the Security Administrator specifies whether the Telnet interface and the Web server interface interfaces are enabled, what method the switch or director uses to authenticate users and which users are authorized to use these interfaces.

- The Software tab allows the security administrator to set up software applications that can communicate with the switch or director through APIs. The most common use of this tab is to define the security settings for this Server, so the switch or director can authenticate Server requests to manage the switch or director. This tab is also used to configure security setting for OSMS (in-band) management.

- The Devices tab allows the security administrator to configure how the switch or director authenticates connection requests from other devices. The Devices tab is PFE key enabled. If a proper PFE key is not provided, the Devices tab is not accessible.

- The IP Access Control tab allows the security administrator to define the IP addresses from which management requests can originate, and whether the switch or director limits management requests based on originating IP address.

- The Radius Servers tab allows the security administrator to define which RADIUS Servers the switch or director are to use to obtain authentication data.
Using the Security tabs

The Security tabs share some common buttons and functionality. Review this list for some general instructions on working on the tabs.

- Use the Reset button to discard any changes you have entered on the tab and reload the settings from the switch or director.

- Use the Apply button to apply changes made on this tab to the switch or director. If there is only one product to which changes need to be applied, then only that product is listed. The product ID is identified by its Node name. By default, this product is highlighted and selected.

- Use the Apply To Other Products dialog box to select the switches or directors to which you want to send the changes.

Use the Security Change Confirmation and Status dialog box to verify the changes about to be made to each switch or director and to observe the progress of these changes.

The Security Change Confirmation and Status dialog box includes the user ID who initiated the changes, the time that the changes were planned, the Server ID from which the changes are populated, and all of the affected switches and directors. Server ID is identified by its Server name plus IP address.

If there are no security settings being changed, the Security Change Confirmation and Status displays with the Detailed Changes table displaying a message that no changes were found. Clicking the Start button, displays a Status window message that the security settings are identical and that there are no changes to apply.

- Use the Apply To button to apply changes made on this tab to this switch or director, as well as to other switches or directors in this fabric. When you click the Apply To button, the Apply To Other Products dialog box displays, so you can select the other switches and directors to which to apply the changes.

If you applied the same user settings to multiple products, the product list displays multiple product names that were selected from the Apply To dialog box. By default, the product that was selected from the top table for configuration is highlighted. The content of Detailed Changes table changes as you click through different products from the product list.
The **Detailed Changes** table includes all of the individual configurations that security administrator has made on the **User** tab. The columns of this table vary depending on from which tab the security administrator is accessing the confirmation information.

**Note:** The **Apply To** button is not available on the Element Manager SANtegrity Authentication tabs. The **Apply To** button is available on the Connectrix Manager application SANtegrity Security Center tabs, except for the **Devices** tab.

The differences between the to-be-populated setting and current settings on each individual product are displayed, because the **Apply To** dialog box takes changes made on user settings for one product, and generalizes them to multiple products whose user settings can be totally different. The new settings replace the existing settings on other products.

To thoroughly check the new changes, click the different products on the product list and view the detailed changes.

**Note:** Applying user-related settings to multiple products causes the new settings to override the existing settings completely.

When you click **Start**, the Connectrix Manager application Server populates the changes to the switch or director specified in the products list.

The bottom **Status** window displays the status of each product. If all changes are successfully populated to a product, the status displays the product name and a successful message.
Working with virtual fabrics

Note: This information only applies if virtual switches are configured on Directors discovered through your Connectrix Manager application.

The Fabrics panel displays fabrics and core switches. Select a fabric in this panel to display all fabric switches in the Product Configuration table. Virtual switches, highlighted with a “V” icon, and core switches that do not contain virtual switches both display in the table.

Selecting the Core Switch Group entry in the Fabrics panel to display available core switches discovered by the Connectrix Manager application. Core switches are the “physical” Director or partition where the virtual switches are configured. Be aware that actions performed on a core switch may affect multiple virtual switches.

If you select a virtual switch in the Product Configuration table, only those Security tabs are available that contain configuration parameters allowed for virtual switches. Options and display on available tabs are modified for virtual switches.

- On the Devices tab, ports that display in the Port Authentication List table are those assigned to the virtual switch. A VF ID column displays the virtual fabric identifier for the virtual fabric where the port is assigned. If you select a core switch in the Product Configuration panel, options are not available on the Devices tab, such as Edit Secret, Enable E_Port Authentication, and Enable N_Port Authentication.
- On the Software tab, OSMS options are only available if a virtual switch is selected. The remaining options (Enable Authentication, Method, Include Current Server, and Permitted Software, are only available if a core switch is selected.)
Setting authentication methods

Several tabs require you to specify the method the switch or director is to use to authenticate the user’s credentials — **Local Only**, **RADIUS Only**, or **RADIUS then Local**.

If you want to specify RADIUS authentication, you must first define at least one RADIUS server. If no RADIUS servers have been configured, then the only option presented is **Local only**.

---

**Note:** In this context, a user can be a user, a software ID, or another device.

- **Local Only** causes each switch or director to use its local user database for authentication.

  Some RADIUS servers store passwords unencrypted in plain text files. If **Local Only** is used, there is no unencrypted central repository of the password information as your Connectrix Manager application encrypts this information.

- **RADIUS Only** causes the switch or director to use the RADIUS server to authenticate users.

  If the RADIUS server is not available, then users cannot connect. RADIUS is acknowledged as being an industry standard and is convenient to use because all passwords can be managed from a central location. However, if a **RADIUS Only** method is used, the ability to authenticate is directly related to the quality of the IP network being used to communicate with the RADIUS server. If you are authenticating E_Ports, the stability of the fabric is dependent on the stability of the IP network. The risk is smaller, if you use **RADIUS then Local** or **Local Only**.

- **RADIUS then Local** causes the switch or director to first attempt to use the RADIUS server, if available, to authenticate users. If the RADIUS server is not available, then the local database is used.
SANtegrity Security Center supports the Challenge Handshake Authentication Protocol (CHAP). The switch uses CHAP to authenticate all users except Telnet and Web Server interface users.

The service (switch or director) sends the client requestor a random challenge value. The client must reply with a response that generated using a cryptographic hash calculation including a shared secret. This means that both the authenticator (switch or director), and the client must know the same client secret. Bi-directional or single-direction authentication is supported, and unique secrets exist for each entity.

When you add or edit a device from the Devices tab, you enter or generate the CHAP secret.

Use these guidelines when entering or generating CHAP secrets:

- Each CHAP secret must consists of a 32-digit hexadecimal value or 16 ASCII characters. To specify ASCII characters, precede the value with a $, such as, $abcdefghijklmnop.

- Some RADIUS servers require secrets to be entered in ASCII. If you are using a RADIUS server, you can either type in the hexadecimal equivalent of the ASCII value or precede the ASCII value with a $. For example, you can either type in 61616161616161616161616161616161 or #$aaaaaaaaaaaaaaaa.

- The Generate button generates a random 32-digit hexadecimal value. You may not be able to specify this value to RADIUS.
**Accessing the Users tab**

The Users tab lets the security administrator set up role-based user access to the selected switch or director through the Web Server or Telnet management interfaces.

To access the Users tab, click the Users tab in the Security feature.
Security Authentication Users tab

Opening the User tab

Click the Users tab on the Security > Authentication Product Configuration main window. The window displays user information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Displays Add/Edit User dialog box, so a user can be added to the Permitted Users table.</td>
</tr>
<tr>
<td>Apply</td>
<td>Click Apply to populate the changes to the Switch and Director.</td>
</tr>
<tr>
<td>Apply To</td>
<td>If same security settings need to be populated to more than one Switch or Director, clicking Apply To applies the changes to multiple Switches and Directors. A dialog box displays listing the qualified Switches and Directors. To be listed in this dialog the Switch and Director must be manageable and using EO/S 7.0 or later.</td>
</tr>
<tr>
<td>Edit</td>
<td>Displays Add/Edit User dialog box, so the selected entry in the Permitted Users table can be edited.</td>
</tr>
<tr>
<td>Enable Telnet</td>
<td>Enables the Telnet CLI interface. If not enabled, the Switch or Director cannot be managed using the Telnet interface.</td>
</tr>
<tr>
<td>Enable Web Server</td>
<td>Enables the Web Server interface. If not enabled, the Switch or Director cannot be managed using the Web Server interface.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays the Help content related to the current tab.</td>
</tr>
<tr>
<td>Method - Telnet</td>
<td>Select the method that the Switch or Director uses to authenticate Telnet users. Select Local Only, Radius Only, or Radius then Local. If you have not defined any Radius Servers, only the Local Only option is available. To define Radius Servers, access the Radius tab.</td>
</tr>
</tbody>
</table>
Overview of tasks to be completed

1. Decide if you want users to manage the Switch or Director using the Web Server interface. If the Web Server interface is enabled, the Switch or Director authenticates Web Server interface users.

   a. If yes, add the users that you want to allow to use the Web Server interface to the Permitted Users table. For more information, refer to Make sure that the Web Server interface checkbox is checked in the table for this user.

   - Set the method you have decided to use for Web Server authentication. For more information, refer to . If you are using RADIUS authentication, be sure to define your RADIUS Servers in the Radius Servers tab first.

| Field                        | Description                                                                 |
– Make sure that the Web Server is enabled. For more information, refer to “Enabling and disabling the Web server and Telnet interfaces” on page 628.

b. If no, make sure that the Web Server interface is disabled. For more information, refer to “Enabling and disabling the Web server and Telnet interfaces” on page 628. If the Web Server interface is disabled, no user can manage the Switch or Director using the Web server interface, and the Permitted Users table is ignored.

2. Decide if you want users to manage the Switch or Director using Telnet. If Telnet is enabled, the Switch or Director always authenticates Telnet users.

   a. If yes, add the users that you want to allow to use Telnet to the Permitted Users table. Make sure that the Telnet checkbox is checked in the table for this user.

   – Set the authentication method that you have decided to use for Telnet authentication. If you are using RADIUS authentication, be sure to define your RADIUS servers in the Radius Servers tab first.

   – Make sure that the Switch or Director Telnet interface is enabled. For more information, refer to “Enabling and disabling the Web server and Telnet interfaces” on page 628.

   – Decide if you want Telnet transmissions to be encrypted using the Secure Shell (SSH) protocol, and make sure the SSH checkbox is checked if yes, refer to “Enabling and disabling SSH” on page 628.

b. If no, make sure that the Switch or Director Telnet interface is disabled. For more information, refer to “Enabling and disabling the Web server and Telnet interfaces” on page 628. If the Telnet interface is disabled, no user can manage the Switch or Director using Telnet, and the Permitted Users table is ignored.

3. Click Apply or Apply To and the confirmation dialog box displays. If all displayed changes are satisfactory, click Start to send the changes to the Switches and Directors. For more information, refer to “The Apply to Other Products dialog box displays listing the qualified Switches and Directors. Using the Security Change Confirmation and Status dialog box” on page 630.
You can also use this tab to change the user authentication configuration. Refer to sections mentioned above.

**Configuring Web server and Telnet security**

**Enabling and disabling the Web server and Telnet interfaces**
To enable or disable the Web Server or Telnet interfaces, check or uncheck the appropriate checkbox. If the checkbox for the Web Server or Telnet is not checked, then no user can log in to the Switch or Director through this interface.

**Enabling and disabling SSH**
If the SSH checkbox is checked, then all management data between the workstation and the Switch or Director through telnet is encrypted using the SSH protocol.

**Specifying the Authentication Method for the Web server and Telnet interfaces**
When the interfaces are enabled, the Web Server and Telnet can be set to authenticate to a local database on the Switch or Director, a RADIUS Server, or a RADIUS Server then a local database. To specify the authentication method used by the Web Server or Telnet, select the appropriate choice from the corresponding Method dropdown box.

The Connectrix Manager application cannot automatically populate the RADIUS Server with information from the Web Server or Telnet. Therefore, a message advises you that you have set the Web Server or Telnet Authentication Method to **Radius Only**, and that you must properly define the software on the RADIUS Server to ensure that authentication succeeds and that connectivity between software and product is established.

**Assigning users to a switch or director**
1. To add permitted users, press the **Add** button.

   The **Add/Edit User** dialog box displays.

   a. In the **Add/Edit Users** dialog box, type values for the **User ID** and **Password** fields. The **User ID** field can be 1-23 ASCII characters, with no double or single quotes and no white space. The **Password** fields must be 1-24 ASCII characters.

   b. Click **OK**.
c. The new user is added to the **Permitted Users** table. The role defaults to **Administrator**. You can change the role by clicking in the **Role** field.

d. You must check Web Server and/or Telnet checkboxes. All users must be authorized for at least one of the interfaces.

2. To edit permitted users passwords, select a single user and click **Edit**.

The **Add/Edit Users** dialog box displays. You can modify the **Password** fields. The **Password** fields must be 1-24 ASCII characters.

3. To remove permitted users, select one or multiple users and click **Remove**.

   **Note:** There must be at least one user in the **Permitted Users** table with Administrator role and Web server authority, and one user with Administrator role and Telnet authority, even if these interfaces are not enabled. This can be a single user.

4. Click **Apply** and verify the changes in the **Detailed Changes** list. Click Start at the bottom of the dialog box to accept the changes.

   **Note:** When the Switch or Director is first installed, there is a default user setup in the Switch or Director user base. The ID of the user is **Administrator** and the password is **password**. This user has both Web server and Telnet authority. This user displays in the table.

---

**Using the Apply To button**

The security administrator can add the same set of users on multiple Switches and Directors by clicking **Apply To**.

**Note:** This feature is not available from the Element Managers.

To add the same set of users to multiple Switches and Directors, do the following:

1. Click the **Apply To** button.
The **Apply to Other Products** dialog box displays listing the qualified Switches and Directors. **Using the Security Change Confirmation and Status dialog box**

Clicking **OK** on the **Apply To** dialog box or clicking **Apply** from the **User** tab, displays a **Security Change Confirmation and Status** dialog box.
Accessing the Software tab

The Software tab allows the Security Administrator to define software access to the switch or director through API and OSMS interfaces. Unlike the Web server and Telnet interfaces, the API and OSMS authentication require a CHAP secret as password. OSMS interface is for software to manage the switch or director in-band over Fibre Channel. The only information needed for OSMS interface is the OSMS secret.

API users are identified by their designated software ID. Typically, the API user is the current Connectrix Manager server, and its name is the server name defined at installation. Whenever the current server is present in the Permitted Software list, the Software tab displays with an asterisk next to the current server ID.

To access the Software tab, click the Software tab in the Security feature.
**Security Authentication Software tab**

**Opening the Software tab**

Click the **Software** tab on the **Security, Authentication Product Configuration** main window. The window displays software information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply</td>
<td>Click <strong>Apply</strong> to populate the changes to the Switch or Director.</td>
</tr>
<tr>
<td>Apply To</td>
<td>If same security settings need to be populated to more than one Switch or Director, clicking <strong>Apply To</strong> applies the changes to multiple</td>
</tr>
<tr>
<td></td>
<td>Switches and Directors. A dialog box displays listing the qualified Switches and Directors. To be listed in this dialog the Switch and</td>
</tr>
<tr>
<td></td>
<td>Director must be a manageable and using EO/S 7.0 or later.</td>
</tr>
<tr>
<td>Enable Authentication - API</td>
<td>Enable or disable authentication of attempts by software program, such as this Server, to manage the Switch or Director using an Application</td>
</tr>
<tr>
<td>Enable Authentication - OSMS</td>
<td>Interface (API). Authentication cannot be enabled unless the current Server is included in the <strong>Permitted Software</strong> list.</td>
</tr>
<tr>
<td>Generate</td>
<td>Generates an OSMS Secret. The Server generates a random 32-digit hexadecimal value.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays the Help content related to the current tab.</td>
</tr>
<tr>
<td>Include current server</td>
<td>Choose whether to include the current Server in the <strong>Permitted Software</strong> list.</td>
</tr>
<tr>
<td>Include current server - Properties</td>
<td>Display <strong>Server Properties</strong> dialog box, so the settings for the current Server can be ed or changed.</td>
</tr>
</tbody>
</table>
Overview of tasks to be completed

1. Decide if you want the API authentication to be enabled on the Switch or Director. If this option is enabled, only the defined software IDs can manage the Switch or Director.

   a. If API authentication is to be enabled:
      
      - The current Server’s ID must be added to the list. Refer to “Defining the Server’s CHAP secret” on page 635.
      - Decide if other software IDs should be authorized to originate management requests, and add them to the Permitted Software List. Refer to “Adding an additional software ID” on page 637.

---

**Field** | **Description**
--- | ---
Method - API | This field is the method that the Switch or Director uses to authenticate software programs. Select Local Only, RADIUS Only, or RADIUS then Local. If you have not defined any RADIUS servers, only the Local Only option is available. To define RADIUS servers, access the Radius Servers tab.
OSMS Key | Type the OSMS secret. This must be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits. For example, $abcdefghijklmnopqrstuvwxyz.
Permitted Software - Add | Add a software ID to the permitted software list.
Permitted Software - Edit | Edit the selected entry in the permitted software list.
Permitted Software - Remove | Delete selected entries from the permitted software list.
Reset | Clicking the Reset button repopulates the original security settings from the Switch or Director. As a result, all user modified data is cleared.
Retype Key | Retype the same value that was typed in OSMS Secret.
SANtegrity Security Center

– Set the authentication method that you have decided to use. Refer to “Specifying the Authentication Method for API users” on page 638. Be sure to define your RADIUS servers in the Radius Servers tab first if you want to use RADIUS authentication.

– Enable API authentication. If API authentication is not to be enabled:
  – Make sure the API Enable Authentication checkbox is unchecked. The Permitted Software List is ignored if API authentication is disabled.

2. Decide if you want OSMS authentication to be enabled.
   a. If OSMS authentication is to be enabled:
      – Make sure the OSMS CHAP Secret is defined. Refer to “Defining OSMS CHAP secret” on page 639.
      – Enable OSMS authentication. Refer to “Enabling OSMS authentication” on page 638.
   b. If OSMS authentication is not to be enabled:
      – Make sure the OSMS Enable Authentication checkbox is unchecked. Refer to “Enabling OSMS authentication” on page 638.

3. Click Apply or Apply To and review the information in the confirmation dialog box. If all displayed changes are satisfactory, click Start to send the changes to the Switches and Directors. Refer to.

You can also use this tab to change the API or OSMS authentication configuration. Refer to

---

**Configuring software authentication**

**Enabling API authentication**

To enable or disable API authentication, check or uncheck the Enable Authentication checkbox for API. If API authentication is enabled, the following guidelines must be followed:

* There must be a minimum of one entry in the Permitted Software field. If not, a warning message displays when Apply is clicked. It is required that the current server is included. If the current server is not included, the current server would lose manageability and you would be forced to use an alternate management interface to disable API authentication. If you click Apply or Apply To
without including the current server in the permitted list, a message displays that says you must include the current Server in the Permitted Software list before enabling API authentication.

- The current server’s CHAP secret must be defined.
- The current server cannot be deleted. If the user removes the current server with API authentication turned on, and Apply or Apply To is clicked, a message displays that says the current Server ID cannot be removed when API authentication is enabled.

Adding the current server to the permitted software list: The Include Current Server checkbox

1. The Permitted Software list displays software IDs that are allowed to access the Switch or Director through an API.

2. To allow the Server to manage the Switch or Director, add the current Server to the permitted list by selecting the checkbox Include Current Server. The current Server must be in the permitted list, if API authentication is to be enabled.

3. If the current Server does not have a CHAP Secret defined, a message displays that says you have not defined a CHAP secret for this Server.

   You must define the CHAP secret. If a CHAP Secret is defined, click OK to add the current Server to the Permitted Software list.

   The Server name must be unique. The Switch or Director does not allow duplicate user names. In addition, the Server name should be unique across the installation. If in your installation multiple Connectrix Manager Servers can manage the same Switch or Director at different times, make sure that each Server has a unique ID. Otherwise, if the Servers have different secrets one of the Servers cannot manage the Switch or Director.

4. After the current Server ID is stored in the Switch or Director and the changes are applied, the Include Current Server checkbox is disabled, but still selected. The checkbox is enabled if the current Server is removed from the Permitted Software list.

Defining the Server's CHAP secret

The Server cannot be added unless the CHAP secret is defined.
To define the Server’s CHAP secret, click the Properties button and complete the Server Properties dialog box. In that dialog box, the Server secret must be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcdefghijlmnop.

Note: Some RADIUS servers accept ASCII values only, so if your installation is using a RADIUS server, then you should use the ASCII form.

The Server name is prepopulated on the Server Properties dialog box, and is the name that was specified during your Connectrix Manager application’s installation.

Whenever you change either the Server name or the CHAP secret in the Server Properties dialog box, make sure to apply the change to all Switches or Directors that this Server manages. Otherwise, some of the Switches or Directors can become unmanageable. Never change the Server name or secret using the Telnet or Web server interfaces without making the corresponding change in your Connectrix Manager Server. Otherwise, the Server cannot manage the Switch or Director.

Removing the current server
To remove the current Server, you can do one of the following:

- Before the Server ID has been added to the Switch or Director, the current Server can be removed by unchecking the Include Current Server checkbox.
- After the Server ID has been added to the Switch or Director, the Include Current Server checkbox is disabled. To remove the current Server, highlight its entry in the Permitted Software list and click Remove. If the current Server is not included in the Permitted Software list the Include Current Server checkbox is enabled.
- You cannot remove the current Server if API authentication is enabled. If you try, Apply fails with a message stating that you cannot remove the current Server while API authentication is enabled.

Editing the CHAP secret for the current server
To edit the CHAP secret of the current Server:

1. Select the current Server and click Edit.
A message displays that says to use the **Server Properties** dialog box to edit the current Server’s properties.

2. Click **OK** to display the **Server Properties** dialog box.

3. Edit the Server ID or **CHAP secret**.

   If the Server ID or CHAP secret is changed, a message displays that when you change the Server ID, you must also update the authenticating Switches and Directors, or this Server becomes out-of-sync and the Switches or Directors cannot be managed.

4. Click **OK** to return to the **Software** tab.

**Note:** When you change this Server’s secret, each time you display the **Software** tab for a Switch or Director that has the old secret, a message displays stating that the current Server secret is different from the one stored on the device. Be sure to apply the new secret before leaving the **Software** tab for that Switch or Director.

### Adding an additional software ID

1. To add another Server or other API user to **Permitted Software** list, click **Add**.

   The **Add or Edit Software ID and CHAP Secret** dialog box displays.

2. Type a unique **Software ID**. The software ID cannot have double or single quotes or white space.

3. Type or **Generate** the **CHAP Secret** fields. The CHAP Secret can be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcdefgijkmnop. Alternatively, you can click the **Generate** button to have the Connectrix Manager application generate a random 32-digit hexadecimal value. Some RADIUS servers accept ASCII values only, so if your installation is using a RADIUS server you should always use the ASCII form.

4. Click **OK**.

   The new software is added to the **Permitted Software** list.
Editing the CHAP secret for another API user

1. To edit entries for another API user in the Permitted Software list, select a single entry and click Edit.

2. The Add or Edit Software ID and CHAP Secret dialog box displays. You can modify the CHAP Secret fields. The CHAP Secret must be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcdefghijklmnopqrstuvwxyz.

3. Click OK to return to the Software tab.

Removing another Server

To remove software IDs, select one or multiple users and click Remove. Although you can remove software IDs from the Permitted Software list, you cannot remove the last entry in the list while the API authentication is enabled.

Specifying the Authentication Method for API users

For the API Authentication Method, the following applies:

Use the Method dropdown menu to select Local Only, Radius Only, or Radius then Local. The default is Local Only.

If a RADIUS server has not been defined on the Radius Servers tab, the Radius Only and Radius then Local options are not available from the dropdown menu.

The Connectrix Manager application cannot automatically populate API information to the RADIUS server so a message displays that says, you have set API Authentication Method to Radius Only and that if you have not properly defined the software on the RADIUS server, API authentication fails and the connectivity between software and product is broken.

Enabling OSMS authentication

OSMS is a PFE key dependent feature up to E/OS 6.2. If the license key is not installed, then OSMS authentication is not available.

OSMS is not PFE key dependent after E/OS 6.2; however, it is still required to enable authorization.
To enable or disable OSMS authentication, check or uncheck the **Enable Authentication** checkbox for OSMS. The **OSMS CHAP secret** must also be defined, if OSMS authentication is enabled.

**Note:** OSMS authentication can only be enabled if OSMS support has been enabled in the Element Manager.

---

### Defining OSMS CHAP secret

To define the OSMS CHAP Secret, you can click the **Generate** button. The Server creates a 32-digit hexadecimal random value. If you want to use a specific CHAP secret, enter the CHAP secret in **OSMS Key** and **Retype OSMS Key** fields. The CHAP secret must be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcedfghijklmnop.

Click **OK** on the confirmation dialog box that displays.

---

### Applying changes and confirmation

To apply the change:

1. From the **Software** tab, click **OK** on the **Apply** or **Apply To** dialog box.

   The **Security Change Confirmation and Status** dialog box displays. This dialog box is similar to the dialog box that displays from the **User** tab. The only difference is the **Detailed Change** table. This table displays the difference between the current settings of **Software** tab and to-be-populated new settings. The behavior of this dialog box is the same as the one for **User** tab.

2. Click **Start**.

3. If there are no security settings being changed, the **Security Change Confirmation and Status** displays with the **Detailed Changes** table displaying a message stating that no changes were found. Clicking the **Start** button displays a **Status** window message stating that the security settings are identical and that there are no changes to apply.
Accessing the Devices tab

The Devices tab defines whether the switch or director authenticates requests by other devices to connect to the this switch or director. Device authentication is configured on a port-by-port basis. You can specify default authentication settings for the switch or director; and you can also configure individual switch and director ports to always authenticate or to never authenticate.

**Note:** Port authentication settings override switch authentication settings.

You can also use the Devices tab to define the devices that are allowed to connect to authenticating ports. The features in the Devices tab can only be configured if the switch has the proper PFE key installed. If not, the Devices tab is disabled.

To access the Devices tab, click the Devices tab in the Security feature.
Security Authentication Devices tab

Opening the Devices tab

You need to have a SANtegrity Authentication Feature key to access the Devices tab. Click the Devices tab on the Security, Authentication Product Configuration main window. The window displays device information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add</td>
<td>Use to add detached devices or add managed Switches and Directors in this fabric that are not already connected to this Switch or Director. In the element manager, you can only add detached devices.</td>
</tr>
<tr>
<td>Apply</td>
<td>Click Apply to accept new additions or changes to device information.</td>
</tr>
<tr>
<td>Authenticated Devices</td>
<td>This table lists the devices for which the Switch or Director knows the CHAP secret and therefore can authenticate. An entry in this list does not mean that the Switch or Director is currently authenticating this device. Whether the Switch or Director is authenticating this device depends on the Authentication State setting for the connected port in the Port Authentication list.</td>
</tr>
<tr>
<td>Authenticated Devices - NodeName - Add, Edit, Remove</td>
<td>Add, edit or remove an entry from the Authenticated Devices list.</td>
</tr>
<tr>
<td>Authenticated Devices - Nickname</td>
<td>Displays the nickname for the device in the Authenticated Devices list.</td>
</tr>
<tr>
<td>Authenticated Devices - E_Port</td>
<td>The device connects using E_Port and the Switch or Director uses E_Port authentication on this device.</td>
</tr>
<tr>
<td>Authenticated Devices - N_Port</td>
<td>The device connects using N_Port and the Switch or Director uses N_Port authentication on this device.</td>
</tr>
<tr>
<td>Edit Secret</td>
<td>Edit the Switch or Director’s CHAP secret.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>Enable Authentication - E_Port</td>
<td>Enable or disable E_Port authentication by default. If this option is enabled, the Switch or Director authenticates any E_Port connection requests to a Switch or Director port with Authentication State set to Switch Default.</td>
</tr>
<tr>
<td>Enable Authentication - N_Port</td>
<td>Enable or disable N_Port authentication by default. If this option is enabled, the Switch or Director authenticates any N_Port connection requests to a Switch or Director port with Authentication State set to Switch Default.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays the Help content related to the current tab.</td>
</tr>
<tr>
<td>Method - E_Port</td>
<td>Displays the method that the Switch or Director uses for E_Port authentication. Select Local Only, Radius Only, or Radius then Local. If you have not defined any Radius Servers, only the Local Only option is available. To define Radius Servers, access the Radius tab.</td>
</tr>
<tr>
<td>Method - N_Port</td>
<td>Displays the method that the Switch or Director uses for N_Port authentication. Select Local Only, Radius Only, or Radius then Local. If you have not defined any Radius Servers, only the Local Only option is available. To define Radius Servers, access the Radius tab.</td>
</tr>
<tr>
<td>Node Name</td>
<td>Displays the Switch or Director's node name.</td>
</tr>
<tr>
<td>Port Authentication List - Authentication State</td>
<td>Displays the authentication state for the Switch or Director port. Display with a drop down list when selected. Three options are Switch Default, Forced Enabled, and Force Disabled. If the authentication is enabled for the port, either by default or because the string setting is Force Enabled, this does mean that the Switch or Director knows how to authenticate the connected device. There must be an entry for the connected device in the Authenticated Devices table.</td>
</tr>
<tr>
<td>Port Authentication List - Nickname (Attached)</td>
<td>Displays the nickname of the attached device.</td>
</tr>
<tr>
<td>Port Authentication List - NodeName (Attached)</td>
<td>Displays the WWN of the attached device. If attached port is an E_Port, this displays the WWNN of the attached device. If the attached port is an N_Port, this displays the WWPN of the attached device port.</td>
</tr>
</tbody>
</table>
Components of the Devices tab

The Devices tab includes the following elements.

- The Node Name area (upper left) displays the World Wide Node Name (WWNN) for this Switch or Director, and allows you to define or change this device’s CHAP secret.

- The Authentication area (upper right) is used to manage the default device authentication states and the methods the Switch or Director uses for authentication.

- The Port Authentication List (lower left) displays all of the Switches, Directors, and end nodes connected to this Switch or Director. This list tracks the security settings for each Switch or Director port and for the devices connected to the ports. Connected devices can include:
  - Managed, SANtegrity II capable Switches and Directors
  - Non-SANtegrity II compatible Switches and Directors
  - Non-manageable Switches and Directors
  - Non-McDATA or non-EMC Directors
  - JBOD
  - HBA

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port Authentication List - Port #</td>
<td>Displays the port number of each individual Switch or Director port.</td>
</tr>
<tr>
<td>Port Authentication List - Port Name</td>
<td>Displays the WWN of each individual port on this Switch or Director.</td>
</tr>
<tr>
<td>Port Authentication List - Type</td>
<td>Displays the port type of connected device.</td>
</tr>
<tr>
<td>Port Authentication List - Secret</td>
<td>Displays whether a secret is defined for the device. This value can be Set, Needed or blank. This is Set if the attached device is in the Authenticated Devices table. If the attached device is not in that table and authentication is effectively enabled for the port this is Needed.</td>
</tr>
<tr>
<td>Reset</td>
<td>Clicking the Reset button repopulates the original security settings from the Switch or Director. As a result, all user modified data is cleared.</td>
</tr>
</tbody>
</table>
Other storage devices

If a connected device is SANtegrity capable, your Connectrix Manager application can discover its current security settings and display them on the table. If not, your Connectrix Manager application only displays limited information about that device. Each column can be sorted and the column position can be adjusted. By default, the ports with attached devices are displayed at the top of the list, in attached node order.

The Authenticated Devices list (lower right) displays the list of devices that are currently in the Director’s local database. There can be both connected and detached devices in this database. Devices in this table must have a CHAP secret defined.

**Overview of tasks to be completed**

- Make sure this Switch or Director has a CHAP secret. Refer to
- Decide whether this Switch or Director authenticates connection attempts.
- If this device authenticates:
  - Decide which devices you want to authenticate, and add them to the Authenticated Devices list.
  - Set the authentication methods you have decided to use. Refer to “Setting authentication methods” on page 645. If you want to use Radius authentication, define your Radius Servers in the Radius tab first.
  - Set the default authentication values for E_Port and N_Port. Refer to “Setting default authentication values” on page 645.
  - Decide if you want any port settings to override the defaults. If
  - If the device is not going to authenticate, make sure that the default authentication values for E_Port and N_Port are disabled, and that all ports are set to Switch Default.

*Note:* You can also select to authenticate only N_Port connections or only E_Port connections.
• Click **Apply** and read the confirmation dialog box. If all displayed changes are satisfactory, click **Start** to send the changes to the Switch or Director. Refer to “Applying changes and confirmation” on page 653.

• Also use the **Devices** tab to change the device authentication configuration. Refer to “Removing a device from the Authenticated Devices table” on page 648.

---

**Configuring device authentication**

**Defining this device’s CHAP secret**

1. To define, change or check the value of this device’s CHAP secret, click the **Edit Secret** button.

2. The Change Secret dialog box displays. Enter and retype the CHAP Secret. The secret must be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcdefghijklmnopqrstuvwxyz. You can also click the **Generate** button to have the Server create a 32-digit hexadecimal secret. When changing the existing CHAP secret of a device, all other devices that authenticate this device need to have their local database refreshed, or the connectivity will be broken.

**Setting default authentication values**

◆ To set the default value for E_Port authentication, check or uncheck the **Enable E_Port Authentication** checkbox. The authentication state for the individual ports can override the default.

◆ To set the default value for N_Port authentication, check or uncheck the **Enable N_Port Authentication** checkbox. The authentication state for the individual ports can override the default.

**Setting authentication methods**

◆ To specify the authentication method used for E_Port authentication, select the appropriate method from the corresponding dropdown box. The application checks whether any Radius Servers have been defined on the **Radius** tab. If not, the **Radius Only** and **Radius then Local** options do not display in the dropdown list.

◆ **Local Only** causes the Switch or Director to check its local database only to verify if the Switch or Director on the other end is allowed to communicate.
The Connectrix Manager application cannot automatically populate E_Port authentication information to the Radius Server so a message displays that says, you have set E_Port Authentication Method to **Radius Only** and that if you have not properly defined the software on the Radius Server, E_Port authentication fails and the connectivity between software and product is broken.

**Setting port Authentication States**
- To change the authentication state for a Switch or Director port, click the **Authentication State** value for that port. A dropdown box displays.
- The values are **Switch Default**, **Force Disabled**, and **Force Enabled**.
- If a port is configured to be **Force Enabled**, the port always authenticates the other end of the link regardless of the default authentication state set at the Switch level.
- If a port is configured to be **Force Disabled**, that port does not authenticate connection attempts at any time.
- If a port is specified as **Switch Default**, this port abides by all authentication settings configured for this Switch or Director. All ports are set to this state at product initialization time.
- If **Force Enabled** is selected, or **Switch Default** is selected and the default is enabled, but the Switch or Director does not have the secret for the attached device in this database, the port secret value changes to **Needed**. You should add the connected device to the **Authenticated Devices** table.

**Adding a connected device to the Authenticated Devices table**
- To add a connected device to the **Authenticated Devices** table, either double-click on the appropriate row in the Port Authentication list or select the appropriate row and click the right arrow.
- If the device is connected using E_Port and this is a managed device, one of two things can happen.
  - **E_Port Device has CHAP Secret**: If the connected device already has a secret, the Server automatically adds the secret to this Switch or Director’s database.
• **E_Port Device has no CHAP Secret**: If the connected device does not have a secret, the Change Secret dialog box displays with the WWN of the connected device.

  If you click the Generate button, the Server creates a 32-digit hexadecimal random value. If you want to use a specific CHAP secret, type a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcdefgijklmnop. The new secret is propagated to the connected managed device as its own CHAP secret.

  Click **OK** and the device is now added to the Authenticated Devices table.

• **All Other Connected Devices**: If the device is connected using an N_Port or is not a managed Switch or Director, a warning message displays that you must manually enter and validate the device’s secret. The Add Device dialog box displays. Complete the CHAP Secret fields. If you click the Generate button, the Server creates a 32-digit hexadecimal random value. If you want to use a specific CHAP secret, type the value in the CHAP Secret and Retype CHAP Secret fields. The CHAP secret must be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcdefgijklmnop. The new secret is propagated to the connected managed device as its own CHAP secret.

  Note: Your Connectrix Manager application cannot populate secrets to non-managed devices. You must use whatever interface is provided by a non-managed device to manually enter its new secret.

  Click **OK** and the device is now added to the Authenticated Devices table.

**Changing the CHAP secret for a device**

• To edit an entry in the Authenticated Devices table, select the entry and click **Edit**.

  • **Managed Device**: A message displays stating that you must edit the target device’s secret from its own Device configuration tab.

  • **Other Devices**: The Change Secret dialog box displays with the WWN of the connected device. Complete the CHAP Secret fields. If you click the Generate button, the Server creates a 32-digit hexadecimal random value. If you want to use a specific CHAP secret, type the value in the CHAP Secret...
and Retype CHAP Secret fields. The CHAP secret must be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcdefghijklmnop.

Note: Your Connectrix Manager application cannot populate secrets to non-managed devices. You must use whatever interface is provided by a non-managed device to manually enter its new secret.

Click OK to return to the Devices tab.

Removing a device from the Authenticated Devices table
To remove an entry from the Authenticated Devices table, select the entry and click Remove. If the device is connected to a port that has authentication enabled, a message displays stating that the device you have selected to remove is set to be authenticated, and removing the device causes the authenticated link to fail. Click OK if you still want the device removed; otherwise, click Cancel.

Adding a detached device:
1. To add a detached device, select the Add button to display the Add Device dialog box.
2. Select either E_Port or N_Port to specify the desired authentication type for the device.
3. Type in the Node Name (WWN) of attached device.

Note: If Node Name is already in the Authenticated Devices list or it is not valid, the new entry is rejected.

4. Complete the CHAP Secret fields. If you click the Generate button, the Server creates a 32-digit hexadecimal random value. If you want to use a specific CHAP secret, type the value in the CHAP Secret and Retype CHAP Secret fields. The CHAP secret must be entered as a 32-digit hexadecimal value, or as a $ followed by 16 ASCII digits, such as, $abcdefghijklmnop. The new secret is propagated to the connected managed device as its own CHAP secret.
5. Click OK and the device is added to the Authenticated Devices table.
6. Click OK on the confirmation dialog box that displays when you click Apply from the Devices tab. This dialog box lets you confirm changes.
Applying changes and confirmation

1. Click **Apply** from the **Devices** tab.

   If there are any ports in the **Port Authentication** list with secret, **Needed**, a message displays that says the devices have not been put into the **Authenticated Devices** list and as a result the connectivity between the devices and the Switch or Director is broken.

2. Select **Yes** and the authentication is enabled between the current Switch or Director and the connected devices with Switch or Director ports set to **Enabled**.

   Select **No** and return to the **Devices** tab where you can add the devices to the **Authenticated Devices** list.

3. The **Security Change Confirmation and Status** dialog box displays.

   This dialog box is similar in behavior to the **Security Change Confirmation and Status** that displays from the **User** tab. The only difference is in the **Detailed Changes** table. On the **Devices** tab there is no **Apply To** available, so there is always be one product in the product list. This table displays the difference between the current settings of **Devices** tab and to-be-populated new settings.

4. You can click **Apply** even if there are no security settings being changed.

   If there are no security settings being changed, the **Security Change Confirmation and Status** dialog box displays with the **Detailed Changes** table showing that **No Changes were Found** on the first row.

5. Click **Start** and the status window displays a message the says the security settings are identical and there are no changes to apply.
SANtegrity Security Center

Accessing the IP Access Control tab

The switch IP Access Control tab lets you restrict the IP addresses that are allowed to manage the switch. If the IP Access Control (IP ACL) feature is enabled, IP addresses that are not on this list cannot manage the switch or director.
## Security Authentication IP Access Control tab

### Opening the IP Access Control tab

Click the **IP Access Control** tab on the **Security, Authentication Product Configuration** main window. The window displays IP Access Control information.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply</td>
<td>Click <em>Apply</em> to populate the changes to the Switch or Director.</td>
</tr>
<tr>
<td>Apply To</td>
<td>If same security settings need to be populated to more than one Switch or Director, clicking <em>Apply To</em> applies the changes to multiple Switches and Directors. A dialog box displays listing the qualified Switches and Directors. To be listed in this dialog the Switch and Director must be a manageable and using EO/S 7.0 or later.</td>
</tr>
<tr>
<td>Enable IP Access Control</td>
<td>Enable or disable <strong>IP Access Control</strong>. If <strong>IP Access Control</strong> enabled, the current Server's IP address is automatically added. If this option is enabled, the Switch or Director only accepts management requests originating from an IP address in the list.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays the Help content related to the current tab.</td>
</tr>
<tr>
<td>Permitted IP Addresses - Add, Edit, or Remove</td>
<td>Add, edit, or remove a permitted IP address range or single IP address to the <strong>Permitted IP Access Control List</strong>.</td>
</tr>
<tr>
<td>Permitted IP Addresses - End</td>
<td>The ending IP address of an entry listed in the <strong>Permitted IP Access Control List</strong>.</td>
</tr>
<tr>
<td>Permitted IP Addresses - Start</td>
<td>The starting IP address of an entry listed in the <strong>Permitted IP Access Control List</strong>.</td>
</tr>
<tr>
<td>Reset</td>
<td>Click the <strong>Reset</strong> button to repopulate the original security settings from the Switch or Director. As a result, all user modified data is cleared.</td>
</tr>
</tbody>
</table>
Overview of tasks to be completed

- Decide if you want the IP ACL feature to be enabled on the Switch or Director.
- If IP ACL is to be enabled, decide what IP addresses are authorized to originate management requests, and add them to the Permitted Access Control List. Refer to “Adding entries to the Permitted Access Control List” on page 652.
- Enable the IP ACL feature. Refer to “enabling and disabling IP ACL” on page 652 section.
- If IP ACL is not to be enabled, disable the IP ACL feature. Refer to “enabling and disabling IP ACL” on page 652.
- Click Apply or Apply To and read the confirmation dialog. If all displayed changes are satisfactory, click Start to send the changes to the Switches or Directors. Refer to “Applying changes and confirmation” on page 659.
- Also use this tab to change the IP ACL configuration.

Configuring the IP Access Control feature

enabling and disabling IP ACL
To enable IP Access Control, select the Enable IP Access Control checkbox. If this option is enabled, the Switch or Director only accepts management requests originating from an IP address in the list. The Server automatically adds its own IP address to the list when IP Access Control is enabled. If the Enable IP Access Control List checkbox is checked, restricted access to the IP addresses in the Permitted Access Control List is enforced. If not checked, management interfaces can access the Switch or Director from any IP address. The checkbox is only enabled if there is at least one IP address in the list.

Adding entries to the Permitted Access Control List

Note: The maximum number of entries in the Permitted Access Control list is 32.

To add a permitted IP address or an IP address range, click the Add button. The Add/Edit IP Address or Range dialog box displays. Select the appropriate button, IP address or IP Address Range, then complete the appropriate value. The IP range is defined by a starting
IP address and ending IP address. For ranges, the ending address must be greater than the starting address. Exact duplicate ranges are not allowed, but ranges can overlap or be included in other ranges in the list. **Editing entries to the permitted access control list**

To edit a permitted IP address or IP address range, select the entry and click the **Edit** button. The **Add/Edit IP Address or Range** dialog box displays. Select the appropriate button, **IP address** or **IP Address Range**, then complete the appropriate value. For ranges, the ending address must be greater than the starting address. Exact duplicate ranges are not allowed, but ranges can overlap or be included in other ranges in the list.

**Note:** If multiple IP address or ranges are selected, **Edit** is disabled.

**Removing entries from the permitted access control list**

You can remove multiple IP addresses at a time.

To delete entries from the **Permitted IP Access Control List**, select the entries, then click the **Remove** button. You cannot remove this Server’s IP address from the **Permitted IP Access Control List** while the **Enable IP ACL** checkbox is checked. To remove the Server IP from the list, disable IP ACL.

Click **OK** on the confirmation dialog box that displays when you click **Apply To** or **Apply** button from the **IP Access** tab. This dialog box lets you confirm the changes.

**Applying changes and confirmation**

To apply the change:

1. From the **IP ACL** tab, Click **Apply** or **Apply To**.
   
   The **Security Change Confirmation and Status** dialog box displays.
   
   This dialog box is similar in behavior to the **Security Change Confirmation and Status** that displays from the **User** tab. The only difference is in the **Detailed Changes** table. This table displays the difference between the current settings of **IP ACL** tab and to-be-populated new settings.

2. Click **Start**.
   
   If there are no security settings being changed and you click **Apply** or **Apply To**, the **Security Change Confirmation and Status** dialog box displays with a message that says no changes
were found. Click **Start** and a message displays in the **Status** window that says the security settings are identical and that there are no changes to apply.

3. Click **Start** and the status window displays a message that says the security settings are identical and there are no changes to apply.
Accessing Radius Servers tab

Use this tab to specify the RADIUS servers from which switch or director obtains authentication information. Use of the tab is optional. It is only necessary if the switch or director is using RADIUS authentication.
Security Authentication Radius Servers tab

To access the Radius Servers tab, click the Radius Servers tab in the Security feature.

Opening the Radius Servers tab

Click the Radius Servers tab on the Security, Authentication Product Configuration main window. The window displays the RADIUS servers that have been defined on this Switch or Director. Up to three RADIUS servers can be defined.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apply</td>
<td>Click <strong>Apply</strong> to populate the changes to the Switch or Director.</td>
</tr>
<tr>
<td>Apply To</td>
<td>If same security settings need to be populated to more than one Switch or Director, clicking <strong>Apply To</strong> applies the changes to multiple Switches. A dialog box displays listing the qualified Switches and Directors. To be listed in this dialog the Switch and Director must be manageable and using EO/S 7.0 or later.</td>
</tr>
<tr>
<td>Dead Time</td>
<td>Displays the dead time for a RADIUS server. The value applies to all available RADIUS servers. If a RADIUS server does not respond to an authentication request, it can be marked as dead for a specified time interval. Dead Time can be from 0 to 1440 minutes. The default is 0.</td>
</tr>
<tr>
<td>Help</td>
<td>Displays the Help content related to the current tab.</td>
</tr>
<tr>
<td>RADIUS Servers and Sequence - Clear</td>
<td>Use this to clear the selected RADIUS servers entry.</td>
</tr>
<tr>
<td>RADIUS Servers and Sequence - Edit</td>
<td>Edit the selected RADIUS servers entry.</td>
</tr>
<tr>
<td>RADIUS Servers and Sequence - IP Address</td>
<td>Displays the host name for RADIUS server. This must be a valid IP address. the Switch or Director cannot resolve host names using DNS.</td>
</tr>
<tr>
<td>RADIUS Servers and Sequence - Move Down</td>
<td>Use this to move selected server down in the list.</td>
</tr>
<tr>
<td>Permitted IP Access Control List - Move Up</td>
<td>Use this to move selected server up in the list.</td>
</tr>
</tbody>
</table>
Overview of tasks to be completed

- Decide if you want to use RADIUS authentication for one or more user types:
  - Telnet or Web server users
  - Software users
  - Devices

- If yes, ensure there is at least one entry in the Radius Servers table.
  - If there is more than one RADIUS server defined, decide how long a RADIUS server that has been unreachable will be bypassed. Refer to “Changing the Dead Time” on page 659.
  - After the changes to this tab have been applied, set the Authentication Method to RADIUS Only, RADIUS then Local in the User, Software, or Devices tab, as needed.

- If no, then no changes to this tab are necessary, even if there are already RADIUS servers defined. Defining RADIUS servers has no effect unless at least one tab has RADIUS Only or RADIUS then Local set. This is true irrespective of whether authentication is enabled on that tab.
• Click Apply or Apply To and review the confirmation dialog box. If all displayed changes are satisfactory, click Start to send the changes to the Switch or Director. Refer to “Applying changes and confirmation” on page 659.

• Also, use this tab to change the Radius configuration. Refer to sections mentioned above.

---

**Configuring RADIUS servers**

The RADIUS Servers table has up to three entries. The order of the entries determine the order the Switch or Director uses to request authentication information from the RADIUS server. If the first device does not respond after a certain amount of time due to connection or other configuration problems, then the next RADIUS server is used, and so on.

The RADIUS Servers and Sequence table includes information about the following:

• The Host Name can be an IP Address.
• The UDP Port displays the number that the device uses to contact the Radius Server. The port number is 1812 by default.
• The Timeout(sec) displays the amount of time to wait for a response from the Radius Server before retransmitting the packet. It can be one to 1000, and the default is four seconds.
• The Retries column specifies the number of times a packet is sent to a RADIUS server if a response is not received before the timeout. After the retransmit limit is reached, the Switch or Director changes to the next server. The value may be 1 to 100. The default is three attempts.

**Adding a RADIUS server to the table**

To add a RADIUS server, select a blank line in the RADIUS Servers table and click Edit. The Add/Edit RADIUS Server dialog box displays.

The dialog is prepopulated with the default values for Retries, Timeout seconds, and UDP Port. You can use these values or change the values. You must enter the IP address of the RADIUS server and the key. This is the ‘s or Director’s password that was specified when adding the Switch or Director as a client to the RADIUS server configuration. Click OK to return to the Radius Servers tab.
**Editing an entry in the table**
To edit a RADIUS server entry, select the entry in the RADIUS Servers table and click Edit. The Add/Edit Radius Server dialog box displays.

You can change any of the values displayed, but all fields must be populated. The IP Address field must contain the IP address of the RADIUS server. The Switch or Director cannot use DNS to resolve host names. The RADIUS server key is the Switch’s or Director’s password that was specified when adding the Switch or Director as a client to the RADIUS server configuration. Click OK.

**Removing a RADIUS server**
To remove a RADIUS server entry, select the entry and click Clear. If you try to remove the last entry and at least one tab specifies RADIUS authentication, an error message displays stating that you are attempting to remove all RADIUS servers, but at least one authentication method uses RADIUS. You must set all authentication methods to Local Only, before removing the last RADIUS server.

**Changing the RADIUS server sequence**
To change the order of precedence of RADIUS servers, select the appropriate entry and click the Move Up or Move down button as necessary, until the desired order is achieved.

**Changing the Dead Time**
The Dead Time setting located below the RADIUS Servers and Sequence table applies to all available RADIUS Servers. If a RADIUS Server does not respond to an authentication request, it can be marked as dead for a specified time interval. This can speed up authentication by eliminating timeouts and retransmissions. If no alternate RADIUS servers are available, which means that only one server is configured or that all servers are marked as dead, then the dead time is ignored. The dead time can be 0 to 1440 minutes and the default is 0. To change the Dead Time, type the new value in the Dead Time field.

**Applying changes and confirmation**
1. Click Apply from the Radius Servers tab.
2. The Security Change Confirmation and Status dialog box displays.
This dialog box is similar in behavior to the Security Change Confirmation and Status that displays from the User tab. The only difference is in the Detailed Changes table. This table displays the difference between the current settings of Radius Servers tab and to-be-populated new settings.

3. You can click Apply or Apply To even if there are no security settings being changed.

   If there are no security settings being changed, the Security Change Confirmation and Status Servers dialog box displays with the Detailed Changes table showing that No Changes were Found on the first row.

4. Click Start and the status window displays a message the says the security settings are identical and there are no changes to apply.
Accessing the Security Log

You must have security administrator privileges to use the Security log. By default, the security administrator is in the System Administrator user group and the Security Administrator user group.

- From the Connectrix Manager application, select Monitor, then Logs, and then Security to open Security Log window. The Security log is also visible in the bottom section of the main Security window.
- From the main Element Manager window, select Logs > Security Log to display the Security Log window.
Viewing the Security Log

This security log displays the following security information:

- **Severity.** The severity level of the event (informational, change, error).
- **User.** The user associated with the event.
- **Reason.** The reason code for the event or conditions that caused the failure.
- **Description.** The security event category. The information also includes the description and details of the event and the IP address of the product.
- **Date/Time.** The date and time that the event occurred. The format is `yyyy/mm/dd hh:mm:ss tt`. The last two characters (hundredth of seconds) are needed due to possible higher frequency rate of some of the advanced logs.
- **Count.** The number of times that the same event occurs.
- **Category.** The security category, such as successful connections, disconnections, and configuration changes, and authentication changes.
- **IP.** The IP address from where the event occurred.
- **Role.** The role of the user.
- **Interface.** The interface from where the event occurred, such as embedded web server (EWS) or Command Line Interface (CLI).

### Table 74 Security Log handling

<table>
<thead>
<tr>
<th>Security Log Reason Code</th>
<th>Security Log Category (event type)</th>
<th>Description</th>
<th>Trigger Level (severity level)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Successful Connections (10000 - 10099)</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10000</td>
<td>Successful Connections</td>
<td>EWS User Connected</td>
<td>Informational</td>
</tr>
<tr>
<td>10001</td>
<td>Successful Connections</td>
<td>CLI User Connected</td>
<td>Informational</td>
</tr>
<tr>
<td>10002</td>
<td>Successful Connections</td>
<td>Management Server Logged In</td>
<td>Informational</td>
</tr>
<tr>
<td>10003</td>
<td>Successful Connections</td>
<td>API Management Client Connected</td>
<td>Informational</td>
</tr>
<tr>
<td>10004</td>
<td>Successful Connections</td>
<td>Maintenance Port Logged In</td>
<td>Informational</td>
</tr>
</tbody>
</table>
### Security Log handling (continued)

<table>
<thead>
<tr>
<th>Security Log Reason Code</th>
<th>Security Log Category (event type)</th>
<th>Description</th>
<th>Trigger Level (severity level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disconnections (10100 - 10199)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10100</td>
<td>Disconnections</td>
<td>CLI User Disconnected</td>
<td>Informational</td>
</tr>
<tr>
<td>10101</td>
<td>Disconnections</td>
<td>Management Server User Disconnected</td>
<td>Informational</td>
</tr>
<tr>
<td>10102</td>
<td>Disconnections</td>
<td>API Management Client Disconnected</td>
<td>Informational</td>
</tr>
<tr>
<td>10103</td>
<td>Disconnections</td>
<td>SSH Client Protocol Error</td>
<td>Informational</td>
</tr>
<tr>
<td>10104</td>
<td>Disconnections</td>
<td>Maintenance Port User Logged Out</td>
<td>Informational</td>
</tr>
<tr>
<td>Security Systems Configuration Changes (10200 - 10299)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10200</td>
<td>Configuration Changes</td>
<td>Time of Day Changed</td>
<td>Change</td>
</tr>
<tr>
<td>10201</td>
<td>Configuration Changes</td>
<td>EWS and CLI Passwords have been Reset</td>
<td>Change</td>
</tr>
<tr>
<td>10202</td>
<td>Configuration Changes</td>
<td>SSH Keys have been Reset</td>
<td>Change</td>
</tr>
<tr>
<td>10203</td>
<td>Configuration Changes</td>
<td>Default Password Not Changed</td>
<td>Change</td>
</tr>
<tr>
<td>Authorization Errors (10300 - 10399)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10300</td>
<td>Authorization Failures</td>
<td>Fabric Binding Mismatch</td>
<td>Error</td>
</tr>
<tr>
<td>10301</td>
<td>Authorization Failures</td>
<td>Unauthorized Switch Binding WWN</td>
<td>Error</td>
</tr>
<tr>
<td>10302</td>
<td>Authorization Failures</td>
<td>Unauthorized Port Binding WWN</td>
<td>Error</td>
</tr>
<tr>
<td>10303</td>
<td>Authorization Failures</td>
<td>Authorization Failure: E_Prot ILS Reject</td>
<td>Error</td>
</tr>
<tr>
<td>10304</td>
<td>Authorization Failures</td>
<td>Incompatible E_Prot Security Attributes</td>
<td>Error</td>
</tr>
<tr>
<td>10305</td>
<td>Authorization Failures</td>
<td>IP Access Control List Violation</td>
<td>Error</td>
</tr>
<tr>
<td>10306</td>
<td>Authorization Failures</td>
<td>Management Server Access Control List Violation</td>
<td>Error</td>
</tr>
<tr>
<td>Authentication Errors (10400 - 10499)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10400</td>
<td>Authentication Failures</td>
<td>EWS Wrong User Name</td>
<td>Error</td>
</tr>
<tr>
<td>10401</td>
<td>Authentication Failures</td>
<td>CLI Wrong User Name</td>
<td>Error</td>
</tr>
</tbody>
</table>
### Table 74 Security Log handling (continued)

<table>
<thead>
<tr>
<th>Security Log Reason Code</th>
<th>Security Log Category (event type)</th>
<th>Description</th>
<th>Trigger Level (severity level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10402</td>
<td>Authentication Failures</td>
<td>Maintenance Port Wrong User Password</td>
<td>Error</td>
</tr>
<tr>
<td>10403</td>
<td>Authentication Failures</td>
<td>SNMP Wrong Community</td>
<td>Error</td>
</tr>
<tr>
<td>10404</td>
<td>Authentication Failures</td>
<td>Authentication Error: API Management Client</td>
<td>Error</td>
</tr>
<tr>
<td>10405</td>
<td>Authentication Failures</td>
<td>Authentication Error: FC N_Port</td>
<td>Error</td>
</tr>
<tr>
<td>10406</td>
<td>Authentication Failures</td>
<td>Authentication Error: FC E_Port</td>
<td>Error</td>
</tr>
<tr>
<td>10407</td>
<td>Authentication Failures</td>
<td>Authentication Error: OS Management Server</td>
<td>Error</td>
</tr>
<tr>
<td>10408</td>
<td>Authentication Failures</td>
<td>OS Management Server Authentication Not Provided</td>
<td>Error</td>
</tr>
</tbody>
</table>

#### Security Log Miscellaneous (10500 - 10599)

<table>
<thead>
<tr>
<th>Security Log Reason Code</th>
<th>Security Log Category (event type)</th>
<th>Description</th>
<th>Trigger Level (severity level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10500</td>
<td>System</td>
<td>Security Log Reset</td>
<td>Informational</td>
</tr>
<tr>
<td>10501</td>
<td>System</td>
<td>Security Log has Wrapped</td>
<td>Informational</td>
</tr>
<tr>
<td>10502</td>
<td>System</td>
<td>Audit Log Reset</td>
<td>Informational</td>
</tr>
<tr>
<td>10540</td>
<td>System</td>
<td>PLOGI/FLOGI WWPN Mismatch</td>
<td>Informational</td>
</tr>
<tr>
<td>10541</td>
<td>System</td>
<td>PLOGI/FLOGI WWNN Mismatch</td>
<td>Informational</td>
</tr>
<tr>
<td>10550</td>
<td>System</td>
<td>Nameserver: Device Deregistration</td>
<td>Change</td>
</tr>
<tr>
<td>10551</td>
<td>System</td>
<td>Nameserver: WWPN Registration</td>
<td>Change</td>
</tr>
<tr>
<td>10552</td>
<td>System</td>
<td>Nameserver: WWNN Registration</td>
<td>Change</td>
</tr>
<tr>
<td>10553</td>
<td>System</td>
<td>Nameserver: WWPN Registration for another Device -- Invalid Operation attempted</td>
<td>Error</td>
</tr>
<tr>
<td>10553</td>
<td>System</td>
<td>Nameserver: WWNN Registration for another Device -- Invalid Operation attempted</td>
<td>Error</td>
</tr>
</tbody>
</table>
This appendix contains information for troubleshooting:

- Problems with addresses .............................................................. 666
- Problems with discovery ............................................................ 667
- Problems with fabric binding ...................................................... 670
- Problems with LUNs ................................................................. 671
- Problems with products ............................................................ 672
- Miscellaneous problems ........................................................... 673
## Troubleshooting

### Problems with addresses

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| **No subnets or addresses selected.**        | 1. Select **Setup** from the **Discover** menu.  
2. Select the **Out-of-Band** tab.  
3. Click on the subnet or individual address you would like to discover in the **Available Addresses** pane.  
4. Click the < button to move your choice to the **Selected Subnets** pane, or to the **Selected Individual Addresses** pane.  
5. Click **OK**.                                                                                                           |
| **Wrong IP addresses selected.**             | 1. Select **Setup** from the **Discover** menu.  
2. Select the **Out-of-Band** tab.  
3. Verify that the IP addresses in the **Selected Subnets** and **Selected Individual Addresses** panes are the correct current addresses for the SAN.  
4. Click **OK**.                                                                                                           |
| **Wrong community strings are selected.**    | 1. Select **Setup** from the **Discover** menu.  
2. Select the **Out-of-Band** tab.  
3. Select an IP address.  
4. Click **Change**.  
5. Select the desired community strings.  
6. Click **OK**.                                                                                                           |
Problems with discovery

Determining the discovery state

Note: The Product List panel may be hidden by default. To view all panels, select All Panels from the View menu, or press F12.

You can determine the discovery status of products by looking at the Status column in the Product List. Additionally, the operational status called Unknown is equivalent to the discovery state named Offline. The operational statuses, Operational, Degraded, and Failed are equivalent to a discovery state of Online.

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Discovery is turned off.</td>
<td>Select On from the Discover menu.</td>
</tr>
<tr>
<td>Devices are not being discovered.</td>
<td>Ensure that your SNMP communication parameters are set correctly in order to discover EMC switches.</td>
</tr>
</tbody>
</table>
| Discovered devices are not being displayed. | To correctly discover all SAN devices, specify each device in the Out-of-Band dialog box, either by the individual IP address or by subnet.  
   1. Select Setup from the Discover menu.  
   2. Select the General tab.  
   3. Select the Out-of-Band Discovery check box.  
   4. Select the Out-of-Band tab to specify the IP addresses you want to discover through out-of-band discovery.  
   5. Add, change, and remove IP addresses, as necessary. Refer to “Configuring address properties” on page 161 for instructions.  
   6. Select IP addresses from the Available Addresses table and add them to the Selected Subnets or Selected Individual Addresses tables by clicking the buttons.  
   7. Click OK. |
|                                              | Ensure that you’ve selected to view the fabric that includes the discovered devices. |
|                                              | Ensure that only one copy of the application is being used to monitor and manage the same devices in a subnet. |
## Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| Broadcast request blocked by routers.        | Resolution 1: If you know the IP addresses and the addresses are not in the Available Addresses pane:  
   1. Select Setup from the Discover menu.  
   2. Select the Out-of-Band tab.  
   3. Click Add.  
   4. Enter data in the dialog box.  
   5. Click OK.  
   6. Repeat steps 1 through 5 until all your addresses are available.  
   7. Select the IP addresses you would like to discover in the Available Addresses pane.  
   8. Click the button to move your choices to the Selected Individual Addresses pane.  
   9. Click OK.  

Resolution 2: If you know the IP addresses and the addresses are listed in the Available Addresses pane:  
1. Select Setup from the Discover menu.  
2. Select the Out-of-Band tab.  
3. Select the IP addresses you would like to discover in the Available Addresses pane.  
4. Click the button to move your choices to the Selected Individual Addresses pane.  
5. Click OK. |

| Discovery time is excessive.                 | 1. Select SAN > Options.  
2. Select the SNMP Discovery (under Software Configuration).  
3. Decrease the value in the SMTP Timeout field.  
4. Select the Apply settings to all currently defined IP addresses check box.  
5. Click Apply or OK. |

| The EMC Library (emc_jsymapi) could not be loaded. | Verify that the library is in the correct path or that the SymAPI server is installed. |

| The symapi.jar file is not in the class path.   | Verify that the symapi.jar file has been copied into Connectrix Manager’s Connectrix Manager’s directory. |

| Can’t open an Element Manager for a device.     | Ensure that only one copy of the application is being used to monitor and manage the device. Only one copy of the application should be used to monitor and manage the same devices in a subnet. |

| Cannot see HBA in Discovery Setup dialog box.   | Connectrix ManagerConnectrix Manager levels. Verify the driver levels with EMC. Verify HBA driver levels. |
## Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| Discovery is not enabled.                                               | 1. Select **Setup** from the **Discover** menu.  
2. Select the **General** tab.  
3. Select either the **Out-of-Band Discovery** check box or the **In-Band Discovery** check box, or both.  
4. Click **OK**.                                                              |
| Devices cycle between online and offline.                              | 1. Select **SAN > Options**.  
2. Select the **SNMP Discovery** (under **Software Configuration**).  
3. Increase the value in the **SMTP Timeout** field.  
4. Select the **Apply settings to all currently defined IP addresses** check box.  
5. Click **Apply** or **OK**.                                                                 |
| Discovery of a Cisco 5428 device failed.                               | This product may not respond to broadcast discovery. Add the specific IP Address of the device to the **Selected Individual Addresses** table of the **Discover Setup** dialog box to discover the device. Refer to the related Help or user manual for more information. |
| Attempting to discover an ED-1000M Director ED-100000M displays "Too many sessions" and "No response" statuses. | Verify that no other Connectrix Manager Connectrix Manager application is currently discovering the ED-10000M Director ED-100000M. Remove the ED-10000M Director ED-100000M IP Address from all other Connectrix Manager Connectrix Manager application Discover Setup dialogs. The ED-10000M Director ED-100000M will not display in the current topology if any other Connectrix Manager Connectrix Manager application is discovering the Director. |
**Problems with fabric binding**

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot disable Fabric Binding while Enterprise Fabric Mode is active.</td>
<td>You may have attempted to disable Fabric Binding through the Fabric Binding dialog box while Enterprise Fabric Mode was enabled. Disable the Enterprise Fabric Mode through the Enterprise Fabric Mode dialog box before disabling Fabric Binding.</td>
</tr>
</tbody>
</table>
| Fabric Binding failed because data cannot be populated to the switch. | The following list provides the possible causes of Fabric Binding failure:  
  - Fabric is busy or is rebuilding.  
  - Switch is busy.  
  - Insistent Domain ID is not checked for all switches in the fabric.  
  - Firmware doesn't support Fabric Binding (SAN Routers with firmware below version 4.7, non-Connectrix M switches)  
  - Network failure.  
  - Switch is undergoing firmware upgrade/downgrade or NDCLA (Non disruptive Code Load Activation).  
  - Switch is offline.  
  - Binding feature not licensed. |
## Problems with LUNs

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
</table>
| The application cannot currently manage LUNs on this device.          | - Verify the following conditions have been met:  
  - Check the discovery setup.  
  - Verify that discovery is not still in progress.  
  - Verify that the management application is installed in the appropriate path.  
  - Verify that the device you’ve selected is a supported device configuration.  
  - Verify that the device is on-line.  
  - Verify that the management server is running. |
| Communication with the storage management application failed.         | - Verify the following conditions have been met:  
  - Verify that the device is on-line.  
  - Verify that the management server is running. |
| LUN Management actions failed.                                        | - Verify the following conditions have been met:  
  - Verify that the device is on-line.  
  - Verify that the management server is running.  
  - Verify that the Client is communicating with the Server.  
  - Verify that a green Server connection indicator displays on the status bar.  
  - Verify that the LUN data configuration was not changed while the dialog box was open. |
## Troubleshooting

### Problems with products

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>HBAs not connected to SAN.</td>
<td>Check your physical cables and connectors.</td>
</tr>
<tr>
<td>Switches not connected to Ethernet.</td>
<td>Check your physical cables and connectors.</td>
</tr>
<tr>
<td>Switches not connected to SAN.</td>
<td>Check your physical cables and connectors.</td>
</tr>
<tr>
<td>Cannot disable Fabric Binding while Enterprise Fabric Mode is active.</td>
<td>You may have attempted to disable Fabric Binding through the <strong>Fabric Binding</strong> dialog box while Enterprise Fabric Mode was enabled. Disable the Enterprise Fabric Mode through the <strong>Enterprise Fabric Mode</strong> dialog box before disabling Fabric Binding.</td>
</tr>
</tbody>
</table>
## Miscellaneous problems

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cannot delete text in Telnet session window in Linux system</td>
<td>On Linux systems, you must use <strong>CTRL + BACKSPACE</strong> to delete text in the Telnet session window.</td>
</tr>
<tr>
<td>“Code Execution Error: Array Index Out-Of-Bounds” displays.</td>
<td>Retry the command or action. If the problem persists, contact Customer Support.</td>
</tr>
<tr>
<td>“Code Execution Error: Internal Exception” displays.</td>
<td>Retry the command or action. If the problem persists, contact Customer Support.</td>
</tr>
<tr>
<td>“Code Execution Error: Missing Property File” displays.</td>
<td>Retry the command or action. If the problem persists, contact Customer Support.</td>
</tr>
<tr>
<td>“Code Execution Error: Invalid Product Type” displays.</td>
<td>Retry the command or action. If the problem persists, contact Customer Support.</td>
</tr>
<tr>
<td>The Server doesn’t seem to be starting.</td>
<td>Examine the Server log (&lt;Install_Home&gt;/Server/Universe_Home/TestUniversel_Working/EventStorageProvider/event.log) for diagnostic information.</td>
</tr>
<tr>
<td>Server to Client communication is inhibited.</td>
<td>In some cases, a network may utilize virtual private network (VPN) or firewall technology, which can prohibit communication between Servers and Clients. In other words, a Client can find a Server, appear to log in, but will immediately be logged out because the Server cannot reach the Client. To resolve this issue, the application will automatically detect the network configuration and run the Client in “polling mode” when necessary. When the Client is not running in polling mode, the Server calls the client whenever it has new data.</td>
</tr>
<tr>
<td>Data and settings not imported during installation.</td>
<td>Open an MS-DOS window and enter the following script at the command line: Install_Service &lt;startstatus&gt; &lt;runnow&gt; where startstatus parameter is manual or auto and runnow parameter is true or false</td>
</tr>
</tbody>
</table>
## Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows service does not display correctly in the Computer Management (Windows 2000) or Service Control Manager (Windows NT) window.</td>
<td>If you installed or uninstalled the Win32 service while the Computer Management or Service Control Manager window was open, the service will not display. Close the window and re-open it to see the changes.</td>
</tr>
<tr>
<td>The product will not install on a Windows system.</td>
<td>Verify that the system has 100 MB available on the C drive. The program requires 100 MB for installation, but only 50 MB to run.</td>
</tr>
<tr>
<td>Mapping a loop to a hub causes the loop group and the outermost portion of the topology's background group color or layout format to revert to the default.</td>
<td>Make the background and/or layout changes after mapping the loop to the hub.</td>
</tr>
<tr>
<td>Using Fabric Manager or Device Manager to manage Cisco MDS9xx switches.</td>
<td>Install JRE 1.4 or greater, which includes Java Web Start.</td>
</tr>
<tr>
<td>The system reboots or is unable to gather SNMP information.</td>
<td>Multiple SNMP calls are being sent to a device that can't handle the constant requests for information. To resolve this issue, verify that the devices you are discovering are not being discovered by another Server. Discovering devices using multiple Servers may result in errors.</td>
</tr>
<tr>
<td>Receiving error “Compatibility between &lt;TARGET VERSION&gt; and &lt;CURRENT VERSION&gt; is unknown. Do you want to continue?”</td>
<td>Firmware files are included in the upgrade process, but release rules are not. Since release rules are required when sending another firmware version to a switch, this error will result. To fix this problem, add the latest firmware file to the firmware library. This will also add the new release rules and resolve the problem.</td>
</tr>
<tr>
<td>Error occurs when trying to delete a nickname.</td>
<td>Once assigned, a nickname cannot be deleted and left blank.</td>
</tr>
<tr>
<td>An indirectly connected device does not display.</td>
<td>Make sure you have the SANtegrity Authentication PFE key enabled.</td>
</tr>
<tr>
<td>Problem</td>
<td>Resolution</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Need more information about features.</td>
<td>Many of the features described in this document are explained in more detail in other manuals or Help modules. Search the online Help or refer to the related user manual for more information. To find all the help topics that contain a particular word or phrase: 1. On the Help window, click the tab with the magnifying glass icon. 2. In the Find field, enter the word or phrase for which you want to search. 3. Press Enter.</td>
</tr>
<tr>
<td>System response time sluggish when backup occurs.</td>
<td>If system response time becomes extremely sluggish, check the event log directory (&lt;Install_Home&gt;/Server/Universe_Home/TestUniverse/W оking/EventStorageProvider). If it contains large log files (more than 50,000 KB), delete or move all except the current day’s log files.</td>
</tr>
<tr>
<td>The zoning method is not supported.</td>
<td>You are trying to set zoning methods that produce invalid zones. For example, the application does not permit you to set a domain/port or fabric address zone in an interoperable EMC fabric because it would create an invalid zone.</td>
</tr>
</tbody>
</table>
This appendix provides instructions for the Call Home setup procedure.

- Configure Call Home notification ................................................. 678
- Enable and test Call Home notification ........................................ 692
- Test remote access ............................................................................ 695
**Configure Call Home notification**

The Call Home feature allows the Connectrix service processor to automatically dial out or email to the EMC support center to report system problems. The support center server accepts calls from the Connectrix service processor, logs reported events, and can notify one or more support center representatives.

**Get information from the DialEMC Configuration dialog box**

The DialEMC Configuration dialog box shown in Figure 92 shows the Connectrix Manager 7.2 1U server DialEMC modem init strings.

![DialEMC Configuration dialog box](image)

If this is an upgrade, record the above information, which will be needed later when configuring ConnectEMC.
Availability of the DialEMC Configuration dialog box is an indication that the migration or upgrade from Connectrix Manager 7.2 to 9.1 has not yet been implemented. Therefore, after you record the DialEMC Configuration information, return to Appendix G, "Upgrading Connectrix Manager," to complete the upgrade process.

Upon completion of the upgrade, you will be instructed to return here to configure and test the call home feature.

Set Call Home Configuration

When you installed the Connectrix Manager application, a Call Home Configuration icon was added to your desktop.

5. Double-click the Call Home Configuration icon on the desktop.
6. Populate fields with correct data for installation location and click OK.

![Call Home Configuration dialog box with example data]

- The Modem Number is the phone number to which the modem is connected and also is registered in Clarify to associate this phone number with this customer location. Do not enter the phone number that will be dialed to connect to EMC. This phone number is entered from the ConnectEMC Console, see step a on page G-685.

- The Cabinet Serial Number is the cabinet serial number configured in Clarify for this installation.

- Site Name is the Customer’s Site Name in Clarify.

**Note:** Misconfiguration of the above data will result in an unknown dial home.
Install ConnectEMC

CAUTION
Before installing ConnectEMC verify that DialEMC is no longer installed. If it is installed and you have not recorded the phone numbers configured in DialEMC record the phonenumbers now.

To verify that DialEMC is no longer installed, click the Start button, Settings, Control Panel, Add/Remove Programs, and verify that DialEMC is not installed. If DialEMC is installed, uninstall it by selecting Remove in Add/Remove Programs.

1. If ConnectEMC is already installed, skip to step 9.
   To verify, go to Start menu, Programs and ensure EMC Applications / ConnectEMC / ConnectEMC Configuration options are available. If not, proceed to step 4.

   Note: EMC personnel can obtain the ConnectEMC Installer from the Global Services Internal website (http://www.cs.isus.EMC.com), under Application Download Area, ESN Product Information, ConnectEMC or the Connectrix Manager software CD shipped with the customer’s order.

2. Copy the ConnectEMC Installer to the 1U service processor in a temporary directory, double-click connectemc.EXE to launch installer. After the ConnectEMC Installation dialog box displays, click Yes.

   Figure 95   ConnectEMC Installation dialog box
Call Home Setup Procedure

3. Do not click **Cancel**, this dialog will remain running during install for 2 to 4 minutes.

![Installing dialog box](image)

**Figure 96** Installing dialog box

4. When installation is complete this screen will appear, click **OK**.

![Installation complete dialog box](image)

**Figure 97** Installation complete dialog box

5. If you have Connectrix Manager up and running and are logged into it, go to the **SAN** menu, and select **Exit**.
6. Then, go to the Start menu, and select Shutdown > Restart to reboot the service processor.
Call Home Setup Procedure

Configure ConnectEMC

ConnectEMC can be configured to call home using either a Dialup Connection or by sending an email. In either case, a Modem Number and a Cabinet Serial Number are required when configuring Call Home Configuration using the icon on the Connectrix service processor’s desktop. (In other words, even if you have chosen email as the call-home mechanism, a modem number must be associated with the install.)

Note: A functioning modem phone line is still required for remote support even though you may have selected email home for call-home event notification.

1. From the Start menu go to Programs > EMC Applications > ConnectEMC, and select ConnectEMC Configuration. The ConnectEMC Console dialog box appears.

Choose a call-home method:

- If configuring call home for a Dialup Connection, proceed to step 10.
- If configuring call home for email, proceed to Step 11.

![ConnectEMC Console dialog box](Image)
2. Configure the Dialup Connection.
   a. From the Connection Menu, go to Add Item, and select Dialup Connection.

   ![New Dialup Connection dialog box]

   b. The Phone Number entered in the Phone Number field is similar to the phone numbers entered in the DialEMC Configuration dialog box.
   - For UUNET lookup, enter the appropriate phone number for the UUNET Protocol selected for your geographical area.
   - For DirectDial, enter the correct EMC phone number for the locality from which you are dialing.
   c. Use the UUNET website to get the UUNET local access information.
Call Home Setup Procedure

Note: UUNET ACCESS

UUNET local access numbers can be found at the following website:

http://www.wcom.net/customer_support/access_numbers/index.shtml

d. Configure the first Call Home number. A description, similar to the one displayed in Figure 101 on page 686, is required.

![New Dialup Connection - First Call Home number](image)

e. Click OK.

f. Configure the second Call Home number.
From the **Connection** menu, goto **Add Item**, and select **Dialup Connection**. Enter the phone number for the 2nd dial-up number. Enter appropriate for your location as done previously for the 1st number, except select an alternate phone number.

Make sure to select **Use this connection on failure (Failover)** in the **Alert Type** pulldown in the **General Settings** box, and add a description, similar to the one displayed in Figure 102 on page 687.

![New Dialup Connection](image)

**Figure 102** New Dialup Connection - Second Call Home number

- Click **OK**.
- Repeat steps f and g to enter up to four (4) alternate phone numbers as done in the past with DialEMC.
- Click **OK** to return to the **ConnectEMC Console** dialog box.
Call Home Setup Procedure

Figure 103 Completed setup

The ConnectEMC Console shows the completed setup.

**Note:** The Test Current Configuration option, available using the ConnectEMC Console, is not supported at this time.

j. Proceed to “Enable and test Call Home notification” on page 692 to verify call home is successful.
3. Configure the **Email Connection**.

   a. From the **Connection** Menu, go to **Add Item**, and select **Email Connection**. The **New Email Connection** dialog box appears.

   ![New Email Connection dialog box](image)

   b. In the **Email Address** field, enter the destination email address `emailalert@emc.com`.

   c. In the **Mail Server** field, enter the IP address or the name of the SMTP mail server that the 1U Server can use to send the email.

   d. Configure the **Description** field. A description, similar to the one displayed in **Figure 105 on page 690**, is required.
Call Home Setup Procedure

Figure 105  New Email Connection dialog box (completed)

e. Click **OK** to return to the **ConnectEMC Console** dialog box (Figure 106 on page 691).
f. The ConnectEMC Console shows the completed setup. In addition to the Email Connection, a Dialup Connection can be configured as a Failover option if a modem is available. For more details, refer to steps 10f and 10g.

Note: The Test Current Configuration option, available via the ConnectEMC Console, is not supported at this time.

g. Proceed to “Enable and test Call Home notification” on page 692, to verify call home is successful.
Enable and test Call Home notification

1. From the View ALL - Connectrix Manager window, go to the Monitor menu, and select Event Notification, Call Home.

2. On the Call Home Event Notification Setup dialog box, mark the checkbox for Enable Call Home Event Notification.
3. Click **Send Test** to test.

Log into Clarify to verify call home. Successful call home should appear in Clarify as a **SymptomCode 0**. (See Example 1, next.)

**Example 1: Clarify Call Home results (Successful)**

```
Connect Home
ConnectNum: <customer's modem # will be display here>

dh1
DeviceType: Connectrix
Model : Connectrix Manager 9.1
SymptomCode: 0
Category: Status
Severity: Warning
Component : EFC Server
ComponentID: <customer's cabinet serial # will be displayed here>
SubComponent: 0
SubComponentID: 0
CallHome: Yes
FirstTime: 2004-05-17T14:33:12
LastTime: 2004-05-17T14:33:12
Count : 1
<![CDATA[
]]>
[End of CDATA]
<![CDATA[Event Code Description: N/A
Firmware Version: 4.0.2 8.1 <Do not confuse this with Connectrix firmware>
]]>
[End of CDATA]
```

4. Click **OK** to close the **Call Home Event Notification Setup** dialog box.

5. If call home is unsuccessful, view the C:\Program Files\EMC\ConnectEMC\logs\ConnectEMCDial.log file for an explanation of the failure. If you are unable to determine the cause of the problem, contact the EMC Customer Support Center for technical assistance. When contacting the EMC Customer Support Center, be prepared to provide all the files contained within these directories:

   C:\Program Files\EMC\ConnectEMC\archive
   C:\Program Files\EMC\ConnectEMC\failed
   C:\Program Files\EMC\ConnectEMC\logs
Example 2 is the results of a successful call home as recorded by ConnectEMCDial.log.

**Example 2: ConnectEMCDial.log**

**** OPEN DEBUG FILE - DIAL LOG BEGIN ****

05/17/04 14:33:27 ConnectEMCWinDial started.
05/17/04 14:33:27 Modem setting:
  Comm Port "TAPI"
  Port Sharing 0
  Modem Type ""
  Modem Init String ""
05/17/04 14:33:27 Start looking for a TAPI modem.
05/17/04 14:33:27 1 TAPI device - MultiModem MT2834BA.
05/17/04 14:33:27 Dial setting:
  PhoneNumber "9,18006262452"
  Dial Protocol "Direct Dial"
  ZModem Timeout 50
05/17/04 14:33:27 Dial to 9,18006262452
05/17/04 14:33:57 Modem MultiModem MT2834BA CONNECT to 9,18006262452.
05/17/04 14:33:57 Dial protocol is Direct Dial.
05/17/04 14:33:58 Sent:
  05/17/04 14:34:00 Received: Username:
  05/17/04 14:34:00 Sent: ONALERT
  05/17/04 14:34:00 Received: Password:
  05/17/04 14:34:01 Sent: DIALEMC
  05/17/04 14:34:01 Received: FIELDWATCH
  05/17/04 14:34:01 Received: Choice:
  05/17/04 14:34:04 Sent: GOXFER~
  05/17/04 14:34:04 Received: ENTER PHONE
  05/17/04 14:34:05 Sent: 000000
  05/17/04 14:34:05 Got FEP connection.
05/17/04 14:34:05 List of files:
  File Count 1
  1 File Name "C:\Program Files\EMC\ConnectEMC\poll\RSC_TEST2_051704_143326187.xml"
    1 Status 1
05/17/04 14:34:05 Add to the list 1-th file
  "C:\Program Files\EMC\ConnectEMC\poll\RSC_TEST2_051704_143326187.xml".
05/17/04 14:34:06 Starting ZModem Transfer of 1 files.
05/17/04 14:34:10 SUCCESSFUL transfer of "C:\Program Files\EMC\ConnectEMC\poll\RSC_TEST2_051704_143326187.xml".
05/17/04 14:34:10 ZModem transfer done.
05/17/04 14:34:10 File transfer result:
  1 File Name "C:\Program Files\EMC\ConnectEMC\poll\RSC_TEST2_051704_143326187.xml"
    2 Status 0
05/17/04 14:34:13 The modem MultiModem MT2834BA on port 130 hanged up.
05/17/04 14:34:14 TAPI closed.
05/17/04 14:34:14 ConnectEMCWinDial finished SUCCESSFULLY.
Test remote access

Once you have successfully tested call home, ensure EMCMRemote Host is installed and functioning properly. EMCMRemote Host v5.02 is required when running Windows 2003.

EMC personnel can obtain the latest EMCMRemote Host application and documentation from the Global Services Internal website (http://www.cs.isus.EMC.com), under Application Download Area, ESN Product Information, EMCMRemote.

Important: For displaying devices on Windows 2003 the following reset operation must be performed on an EMCMRemote Host (Connectrix server) after the reboot step of the initial installation, and whenever the primary display device settings are changed.

To initialize the EMCMRemote Host computer’s video device:

1. Open a command window (Start > Run; in the field Open, enter cmd).
2. Change directory to the \SymmRemote folder (C:\Program Files\EMC\SymmRemote)
3. Run rddu -r
4. Close the command window.
5. Reboot the host.

Note: Resetting the EMCMRemote Host display device synchronizes its settings with those of the primary display.
This provides optional procedures for configuring your Connectrix Manager Client and Server applications to function across remote networks through a firewall.

- Introduction ................................................................. 698
- Secure Socket Layer (SSL) ............................................. 698
- Default Server Ports .................................................... 699
- Configuring the application to use dual network cards .... 700
- Polling client function ................................................... 702
- Configuring TCP port numbers to allow firewall access .... 704
Introduction

With the introduction of SANtegrity in Connectrix Manager 8.9.1 and higher, there are new methods for configuring Firewall Access. This document describes the client/server connectivity settings and firewall solutions for Connectrix Manager 9.1 and future versions.

Connectrix Manager, out of the box, is configured to use only two ports to connect the client and server thus eliminating the need to configure Connectrix Manager for use through a firewall for all but very special cases. Only the firewall needs to be configured to allow duplex traffic on ports 51510 and 51511 for Connectrix Manager to work through a firewall. If these ports are not acceptable they are configurable as shown in “Forcing server and client export port number” on page 706.

Document nomenclature

- **Server**: Server with a capital first letter indicates the Connectrix Manager Server
- **Client**: Client with a capital first letter indicates the Connectrix Manager Client application.
- **Edit**: When the document calls to Edit, use a text editor (such as Notepad)
- **<installDir>**: The directory in which Connectrix Manager was installed (usually c:\Program Files\Connectrix Manager 9.1)

Secure Socket Layer (SSL)

SANtegrity 2 introduced ‘privacy’ using SSL for the Connectrix Manager Client /Connectrix Manager Server connection. In order to maintain compatibility with SSL enabled and standard servers, Connectrix Manager requires two ports be used. One port (default=51511) is used for the initial connection and lookup of the Version Compatibility object whereas the second port (51510) is encrypted and used for all application traffic.

**Note**: SSL is enabled by default. It is recommended that the default not be changed.
Disabling SSL

The best practice is to keep SSL enabled as the overhead of encrypting the TCP connection is negligible. In the case where privacy of Connectrix Manager data is not necessary, SSL can be disabled from the SAN > Options Menu, and then unchecking "Enable SSL" under the Server Connection settings.

Default Server Ports

Connectrix Manager 8.6.1 introduced the concept of Default Server Ports. In Connectrix Manager 8.1 the ports would automatically ‘float’ both increasing the lookup time for the clients and creating extra steps for using Connectrix Manager through a firewall. Connectrix Manager 8.9.1 or higher is pre-configured to lock the application traffic to ports 51510 and 51511 to simplify configuration of remote clients through a firewall. With Default Server Ports the server will fail to initialize if ANY of the ports it needs are unavailable. If any of the ports are unavailable, simply change the port number to an unused port. (See “Forcing server and client export port number” on page 706.)

Default port numbers

- 51510 SSL encrypted / all traffic between client and server
- 51511 unencrypted / Connectrix Manager version and directory (registry)
- 51512 CLI Proxy
- 51513 ECCAPI

Note: the Server Connection and Export ports can be configured from the Connectrix Manager SAN > Options, Server Connection settings dialog as outlined "Forcing Server and Client Export Port Number on page H-15" or whatever the new page # becomes once you delete the crossed out content below.

To change the CLI or ECCAPI port values use the procedure below.
Modifying the default Connectrix Manager Server Ports

Modifying any of the default server ports can be accomplished by editing:

c:\Program Files\Connectrix Manager 9.1.0\resources\Server\config.properties

This file is self-documented.

Server/config.properties ports section

# Most Secure setup for use through a firewall.  
# Two Ports must be opened, one for the RMI registry lookup and one for the SSL data connections.  
smp.registry.port=51511  
smp.server.export.port=51510

# Secure setup for use through a firewall with only one port open.  Note that SSL connections and RMI registry
# connections cannot coexist on a single port thus SSL must be disabled.  
#smp.ssl=false
#smp.registry.port=51511
#smp.server.export.port=51511

# The port number the CliProxy listens on.  The usual telnet default is 23.  
Connectrix Manager default is 51512.  
smp.server.cliProxyListeningPort=51512

# The ECC API's remote object will be exported on this port.  Default = 51513  
# smp.server.ecc.api.export.port=51513

Note: If you change the default Server registry port (smp.registry.port) make sure to modify c:\Program Files\Connectrix Manager 9.1.0\resources\Client\config.properties to include a setting of
smp.registry.port=XXXX where XXXX matches the port used in the Server/config.properties.

Configuring the application to use dual network cards

Issues with Client-to-Server connectivity can be due to different causes.  Some examples are:

- The Connectrix Service processor is configured to use both NICs and the IP addresses are very similar.
- The Connectrix Service processor is behind a firewall that performs network address translation.

In order to ensure that Clients can connect to the Server, edit the config.properties file to manually specify the IP address that the Server should communicate to its Clients.
1. Edit the Program Files\Connectrix Manager 8.9.1\resources\Server\config.properties file using a text editor (for example, WordPad).

2. On a line of its own, add `java.rmi.server.hostname=x.x.x.x`
   
   where x.x.x.x is the Connectrix 1U service processor’s IP address bound to the desired network card or firewall NAT address.

3. Save and Close the file.

4. Exit out of the Connectrix Manager Application.

5. Stop the Connectrix Manager services. From the Start menu, select Programs, then Connectrix Manager 8.9, then Stop Services.

6. Start the Connectrix Manager services. From the Start menu, select Programs, then Connectrix Manager 8.9, then Start Services.

7. Log in from the remote client.

For Connectrix service processors with the above mentioned network configurations, the SNMP trap forwarding service may need to be configured with the exact IP address of the NIC that should be "listened" to for traps from managed switches, typically the private NIC used for connection to the network in the Connectrix cabinet with the managed directors/switches. To specify which IP will be returned, edit the `smp.server.edipaddress` variable to instruct the Trap Event Distributor to use a specific IP address.

1. Edit `c:\Program Files\Connectrix Manager 8.9.1\resources\Server\config.properties`

2. Add `smp.server.edipaddress=x.x.x.x`
**Polling client function**

In some cases, a network may use virtual private network (VPN) or firewall technology, which can prohibit communication between a Server and the Client. In other words, a Client can find a Server, appear to log in, but is immediately logged out because the Server cannot reach the Client’s remote object. To resolve this issue, the Connectrix Manager application automatically detects the network configuration and runs the Client in “polling mode” when necessary.

When the Client is not running in polling mode, the Server calls the Client’s remote object whenever it has new data. When the Client is running in polling mode, the Server queues up the data and the Client’s remote object periodically (approximately every 5 or 10 seconds) checks in and gets the data. Thus, the original two-way communication is transformed into one-way communication, allowing passage through firewalls.

**Configuring for faster logins**

When a Client attempts to log into a Server, the Server normally calls back to verify communication. In a firewall situation, this call fails and the Server automatically treats the Client as a “polling” Client. It may take up to 45 seconds for this call-back to fail (worst case). You can configure a polling parameter in configure properties files to let the Server know ahead of time that the Client is a “polling” Client. This skips the call-back from the Server and decreases the login time.

**Forcing a client to be polling**

To force a specific Client to be a polling Client, edit the Client config.properties file located in the `<Install_Home>\resources\Client\` directory. Edit the `smp.callback.passive` parameter as in the following example.

This parameter only affects this Client; all other Clients can be regular Clients.

1. Open the `<Install_Home>\resources\Client\config.properties` file using a text editor (for example, Notepad).
2. Go to the following lines:

```# Forces this Client to be a polling Client.
# Enable by un-commenting this parameter.
# smp.callback.passive```
3. Remove the pound sign (#) in front of the smp.callback.passive parameter.

   # Forces this Client to be a polling Client.
   # Enable by un-commenting this parameter.
   smp.callback.passive

4. Save the file and restart the server.

**Forcing all clients to be polling**

To force all Clients communicating with a Server to be treated as polling Clients (regardless of the parameters the Clients launch with), edit the Server config.properties file located in the `<Install_Home>\resources\Server\` directory.

Edit the smp.callback.passive parameter as in the following example.

1. Open the `<Install_Home>\resources\Server\config.properties` file using a text editor (for example, Notepad).

2. Go to the following lines:

   # Force all Clients communicating with a Server to be treated as
   # polling Clients (regardless of their startup parameters).
   # Enable by un-commenting this parameter.
   # smp.callback.passive

3. Remove the pound sign (#) in front of the smp.callback.passive line.

   # Force all Clients communicating with a Server to be treated as
   # polling Clients (regardless of their startup parameters).
   # Enable by un-commenting this parameter.
   smp.callback.passive

4. Save the file and restart the server.
Configuring TCP port numbers to allow firewall access

This section provides details about configuring TCP port numbers for RMI Servers and Registries to allow Connectrix Manager Client and Server application to function across firewalls.

Connectrix Manager with RMI at TCP port level

The RMI protocol lies between the Connectrix Manager application and the TCP/IP layer, as shown in Table 75.

<table>
<thead>
<tr>
<th>Table 75: RMI protocol level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectrix Manager Server</td>
</tr>
<tr>
<td>RMI</td>
</tr>
<tr>
<td>TCP/IP</td>
</tr>
</tbody>
</table>

The Connectrix Manager Server and Clients communicate with each other through the RMI Server. This is a full-duplex function. However, before the RMI Server on the Connectrix Manager Client can communicate with the RMI Server on the Connectrix Manager Server, it must know the TCP port number of the RMI Server. The function of the RMI registry is to communicate this TCP port number to the Connectrix Manager Client. Once this is done successfully, communication can take place between the RMI Server on the Connectrix Manager Server and the Connectrix Manager Client. (The Connectrix Manager Server obtains the TCP port number of the RMI Server on the Client during initial communications.)
The TCP port numbers of the RMI server are randomly and automatically selected on both the Connectrix Manager Server and Client as a full-duplex function. This poses a major problem for firewalls because the Client must be able to address the Server’s RMI registry and the Server’s remote objects. Also, the Server must be able to address the Client’s remote objects. Firewalls are configured to block all unknown incoming connections with no mapping of outgoing connections based on a socket part of TCP and IP.

To work around this problem for Connectrix Manager, firewall administrators must set which ports are used by the Client and Server by editing parameters in Connectrix Manager M batch files. Use of the following procedures depend on how the firewall is set up. If the firewall prevents the Client from connecting to arbitrary ports on the Server, then you must fix both the Server’s registry and export port. If the firewall prevents the Server from connecting to arbitrary ports on the Client, then you must fix the Client’s export port.

- If the firewall prevents the Client from connecting to arbitrary ports on the Server, then perform both of these procedures:
  “Forcing port in RMI registry” on page 706.
  “Forcing server and client export port number” on page 706.

**Note:** Configure the Server’s export port only.
If the firewall prevents the Server from connecting to arbitrary ports on the Client, then configure the Client’s export port using the following procedure:

“Forcing server and client export port number” on page 706.

---

**Forcing port in RMI registry**

To force the RMI registry to use a particular TCP port for an RMI server, you must configure the Server Connection Port.

1. From the SAN menu, select **Options**.
   - The **Options** dialog box displays.
2. In the **Category** list, select **Server Connection**.
   - The Server Connection fields display to the right of the Category list.
3. In the Server Connection Port # field, enter the TCP port number (between 0 - 65535).
4. Click **Apply** or **OK** to save your work.
5. Restart the application for your changes to take effect.

---

**Forcing server and client export port number**

To force the Server and Client to export a specific TCP port number for an RMI server, you must configure the client and the server export ports.

Note that the server and the client export ports are different ports. Although the server export number could match the client export port, it is not necessary.

1. Select **SAN > Options**.
   - The **Options** dialog box displays.
2. In the **Category** list, select **Client Export Port**.
   - The **Client Export Port** fields display to the right of the **Category** list.
3. In the Client Export Port # field, enter the TCP port number (number between 0 - 65535).
4. Click **Apply** to save your work.
5. In the **Category** list, select **Server Connection**.

   The **Server Connection** fields display to the right of the **Category** list.

6. In the Server Export (SSL) Port # field, enter the TCP port number.

7. Click **Apply** or **OK** to save your work.

   **Note:** If the firewall prevents the Server from connecting to arbitrary ports on the Client, then you must force the export port of the Client. If the firewall prevents the Client from connecting to the Server, then just force the export port of the Server.

8. Restart the application for your changes to take effect.
This appendix presents the requirements for the customer-supplied service processor.

- Platform requirements ................................................................. 710
- Automatic backup device .............................................................. 711
- EMC Call Home and remote support ........................................... 712
- Recommended operating system modifications ....................... 713
- Third-party software ................................................................. 721
Customer-Supplied Service Processor Requirements

Platform requirements

Hardware platform must meet the following minimum requirements:

- **CPU**: One Intel Pentium P4 3.0 Ghz – multi CPU’s o.k.
- **RAM**: 1 gig (2 gig strongly recommended)
- **Graphics Card**: 8 MB minimum, 32 MB recommended
- **HD**: 40 gig
- **COM Ports**: One 9-pin serial port for connection of EMC modem.
- **CD-RW Drive**: One 24/8x CD-RW/DVD Combo, Data only (see Automatic Backup section below)
- **Ethernet**: Two 10/100 Mbps ethernet ports, one for private LAN that switches are on and one for public net for remote Connectrix Manager clients if so desired.
- **OS**: Microsoft Windows 2000 Professional w/SP4 or later service packs and hotfixes.
  
  Microsoft Windows 2003 w/SP1 and later service packs and hotfixes.

*Note*: Windows XP and/or UNIX is not supported for a customer-supplied service processor platform.

Each Connectrix Manager customer-supplied service processor can have a maximum of 25 client sessions.

Connectrix Manager cpu and memory usage is directly proportional to the number of products being managed. It is strongly recommended that you do not exceed the limits published in the release notes with a customer-supplied service processor.

Server should be connected to video, keyboard, mouse display device, either dedicated peripherals or shared video switching device for local access to server. Compatibility with EMC applications and Windows Terminal services cannot be guaranteed.
Operating System services – OS services such as SNMP, http, and ftp will cause conflicts with the embedded functions within Connectrix Manager. These operating system or other third-party services must be disabled. Note sometimes Windows Automatic Update will install updates for these services and in turn re-enable the service. Therefore, if you plan to run Windows Automatic Update it is recommended that the Microsoft operating services for the above not be installed.

**Automatic backup device**

Connectrix Manager has an automatic backup service that runs in the background. This service will backup critical Connectrix Manager information to a drive/directory location. This service can be configured so that the backups occur to the drive directory location of choice.

If the platform being used can contain multiple hard drives then selecting a secondary hard drive destination would probably be the most convenient and reliable choice. Also if the customer system contains two hard drives that are mirrored and then divided into two partitions (logical drives) then this will lessen the chances of data loss.

**Note:** A single hard-drive system could be partitioned into two logical drives, with the secondary partition (D:\ drive) being smaller in size; 1~ 5 gig and the automatic backup could occur to the D:\ drive, however there is no data protection in the event the hard drive were to fail.

External storage devices can also be used for a backup destination, such as a CD-RW drive, USB attached storage device, i.e., USB Zip Drive 250 MB or a mapped network drive.

If a CD-RW drive is chosen then the CD drive should be a CD-RW drive and blank CD-RW UDF formatted media will need to remain in the CD-RW drive so that the automatic backup of Connectrix Manager data can occur to the CD-RW disk. Note drivers and software for the CD-RW drive must present CD-RW to the OS as an accessible storage device for the writing of files without the need to launch special CD-RW disk burning software. The automatic backup application just writes to the D:\ drive, it does not interface with special CD burning software.
Customer-Supplied Service Processor Requirements

A suitable software tool would be Nero InCD by Ahead Software. Note a regular CD-R or DVD burner is not a suitable alternative because the backup function needs to write to the CD-RW disk repeatedly. Note media will have to be monitored and replaced when it becomes full and/or if it becomes defective, with a mapped network drive and/or second hard drive replacing media is not an issue.

Whichever external drive type is chosen it will need to be mounted/mapped to the platform such that the OS can utilize the device as a standard drive letter. Devices that require manual intervention before being written to, such as a CD-R drive will not work.

Note: The network drive backup is an option for both Windows 2000 and Windows 2003 platforms.

For configuring an alternate backup destination follow the procedures in Chapter 2 of the Connectrix Manager User Guide. Note there are specific settings for the Backup Service that must be configured properly for backing up to a network drive detailed in Chapter 2, “Getting Started”.

EMC Call Home and remote support

You will need to purchase the EMC Multitech Multitech MT2834xx or MT5634ZBA modem, contact your EMC sales representative to order the correct modem for your country/location. No other brand/type modem can be used. You also will need to provide a DB9 Female to DB25 Male, 9-Conductor Standard AT Modem Cable, similar to BlackBox part# BC00302 for connection of the modem to the COM1 port on your server platform.

EMC will need to install it’s remote support applications ConnectEMC v1.05.00 and EMCRemote Host v5.0 on the customer supplied service processor. The EMC Multitech MT2834xx modem will need to be connected to a COM port on the server for these applications. Note DialEMC and SymmRemote are used for Connectrix Manager 7.2 and ConnectEMC replaces DialEMC for Connectrix Manager 8.x, see Appendix G, “Call Home Setup Procedure,” for further information on ConnectEMC and Call Home Setup Procedures. Note the EMC modem will need to be connected to
Recommended operating system modifications

Windows active desktop

Windows Active desktop should be disabled as well as the following settings made.

1. From the Windows Start menu, select Settings, Control Panel.
2. Double-click Display.
3. Select the Web tab, and clear the Show Web content on my Active Desktop option.

If you do not have a Web tab, skip this step 3 and continue with the remaining steps in this procedure.

4. Select the Effects tab, and clear the following options:
   - Use transition effects for menus and tooltips
   - Smooth edges of screen fonts
   - Show icons using all possible colors
   - Show window contents while dragging
5. Click **OK** to save the display changes, and return to the control panel.

6. Double-click **Mouse**.

7. Select the **Pointers** tab, and clear the **Enable pointer shadow** option.

8. Click **OK**.

---

**UDP communications**

If the platform and managed products are configured to reside on a public network and that public network is very busy and/or susceptible to large amounts of dropped frames, then to improve UDP communications over the Ethernet ports you may have to add the following registry entries:

- Three settings were added in the Windows registry in the following location:

  ```
  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AFD\Parameters
  ```

- The three parameters added:

  - **DefaultReceiveWindow**
    - New value - 65536
    - Default – 8192
    - Description: The number of receive bytes that AFD buffers on a connection before imposing flow control.

  - **DefaultSendWindow**
    - New value - 65536
    - Default – 8192

  - **FastSendDatagramThreshold**
    - New value - 2048
    - Default – 1024

The resulting key looks as follows:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Service\AFD\Parameters]
"DefaultReceiveWindow"=dword:00010000
"DefaultSendWindow"=dword:00010000
"FastSendDatagramThreshold"=dword:00000800
```
NIC binding order modifications

The network interface that is used for the public LAN IP address should be set in the binding order to be the first in the list of network adapters.

1. Right click My Network Places, and select Properties. The Network and Dial-up Connections dialog is displayed.
2. Select the Local Area Connection entry by single clicking it.
3. From the Advanced pull-down menu, choose the Advanced Settings menu item. The Advanced Settings dialog is displayed.
4. Verify that the Local Area Connection 2 entry is listed first in the Connections: area of the Adapters and Bindings tab.
5. With Local Area Connection 2 still selected, click the down arrow key to move it below the Local Area Connection entry.
6. When done, it should appear as follows:

Verify network properties

Verify the network properties of the server are set properly for multiple network connections. If this Registry entry already exists, then there is no need to recreate it with these procedures. This change will prevent the local Connectrix Manager client (running on the service processor) from being unable to communicate with the Connectrix Manager Server service (also running on the service processor) if the public Ethernet interface on the server were ever to lose the link to the Public Network.
1. Edit the Registry by going to the **Start Menu**, click **Run**, and then type **regedit** (Figure 108).

![Figure 108 Run>regedit](image)

2. The following **Registry Editor** window will appear and the dialog below will be displayed (Figure 109).

![Figure 109 Registry Editor>My Computer, HKEY_LOCAL_MACHINE](image)

3. Double-click **HKEY_LOCAL_MACHINE**, and then **SYSTEM**, **CurrentControlSet**, **Services**, **Tcpip**, **Parameters** (Figure 110 on page 718).
4. Ensure Parameters is highlighted; select Edit> New> DWORD Value (Figure 111 on page 718).

5. Enter the name DisableDHCPMediaSense and press Enter. With DisableDHCPMediaSense highlighted, right-click and select Modify option (Figure 112 on page 719).
6. Enter a value of 1 in the **Value data** field and click **OK** (Figure 113 on page 719).

7. Verify the new entry appears as follows (Figure 114 on page 720).
Customer-Supplied Service Processor Requirements

Figure 114 Registry Editor> DisableDHCMPMediaSense Modified

Network - other

Note: It is highly recommended that the network configuration model designed for an EMC-supplied Connectrix service processor also be adhered to for a customer supplied service processor.

The Directors and/or switches should be configured to reside on a private LAN isolated from other public network traffic and one LAN interface on the service processor be connected to this network for communication to the directors/switches, that is, 10.x.x.x network.

If so desired the second LAN interface in the service processor should be connected to a management LAN used by the SAN administrators to use remote Connectrix Manager client installations. The customers’ network security guidelines may dictate what type of LAN this is but it is recommended that it NOT be a generally available wide open public LAN, but rather one restricted for use by the SAN administrators.

Field experience with large data center networks that introduce new or unusual Ethernet technologies, including aggressive monitoring systems, may be disruptive to the management services provided by the Connectrix service processor. Careful thought and planning should go into connecting LAN interfaces on the same network shared by the customer-supplied service processor.
Customer-Supplied Service Processor Requirements

For details regarding configuring the service processor for Connectrix Manager client use through a firewall see Appendix H, “Configuring Connectrix Manager for Firewall Access”.

Third-party software

Generally speaking anti-virus software is the most common third-party application requested for installation, that is, Norton and McAfee. There are no known issues that prevent the use of these anti-virus applications. However EMC cannot guarantee any level of performance and/or reliability with third-party applications. If a customer deems a certain piece of software necessary to install on their server then they can do so with the condition that it may need to be uninstalled in the event it causes conflicts with the EMC applications. Remote control applications such as PCAnywhere cannot be installed because they will directly conflict with EMCRremote. Other remote control applications, such as Terminal Services and VNC, may work but it is recommended that they NOT be installed.

This workstation must be dedicated for Connectrix Manager and EMC’s remote support applications designed for Connectrix service processors. This platform cannot also be used for other services such as file and print, email, database, web server, etc.

Customer assumes responsibility for support of hardware platform and software compatibility for any other applications they choose to load onto platform.
This provides information about user privileges and access levels.

- **Overview** ................................................................. 724
- **About user privileges** .................................................. 725
- **About user groups and access levels** ........................... 742
Overview

Connectrix Manager provides the User Administrator with a high level of control over what functions your users can see and/or use. This section describes the effect that each user privilege has on the application when placed in one of the three available configurations: no privilege, read-only, and read/write.

User privilege is Connectrix Manager’s method of providing role-based access control (RBAC) to the software’s user administrator.
About user privileges

In Connectrix Manager groups are assigned privileges and views. Privileges are not directly assigned to users; users get privileges because they belong to groups. If a user is assigned to two or more groups they receive the highest level (no privilege, read-only, read/write) for the privilege assigned to any of the groups to which they belong. The following table defines all the privileges in Connectrix Manager and the behavior of the application if the privilege is not given, read only, or read/write.

### Table 76 Privileges

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Session Management</td>
<td>Allows you to view and disconnect client sessions.</td>
<td>Disables the Active Sessions command on the SAN menu.</td>
<td>Enables the Active Sessions command on the SAN menu.</td>
<td>Enables the Active Sessions command on the SAN menu.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Allows you to open the Active Sessions dialog box; however, disables the Disconnect User and OK buttons.</td>
<td>Enables all functions in the Active Sessions dialog box.</td>
</tr>
<tr>
<td>Add/Delete Properties</td>
<td>Allows you to define new properties as well as remove them.</td>
<td>Disables the Add, Edit and Delete buttons on the Create View dialog box Columns tab. Disables the Add Column, Edit Column, and Delete Column commands on the right-click menu of the Product List column headers. Disables the Add, Edit, and Delete commands on the property headers in property sheets.</td>
<td>Same as No Privilege</td>
<td>Enables the Add, Edit, and Delete properties commands and buttons in the Create View and Edit View dialog boxes, the Product List column header right-click menu, and the Property Sheet property header right-click menu.</td>
</tr>
<tr>
<td>Backup</td>
<td>Allows you to control the function that copies (backs up) the application data files to another disk.</td>
<td>Disables the Backup Now and Configure command on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the Options dialog box.</td>
<td>Enables the Configure command on the Backup icon right-click menu on the application status bar. Disables all controls on the Backup page of the Options dialog box.</td>
<td>Enables the Backup Now and Configure commands on the Backup icon right-click menu on the application status bar. Enables all functions in the Backup page of the Options dialog box.</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
<td>No Privilege</td>
<td>Read-Only</td>
<td>Read/Write</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call Home Event Notification Setup</td>
<td>Allows you to enable and disable call home notification. Enables privilege control access to the Call Home Configuration command in the application &lt;Install_Home&gt; directory. Allows you to enter the call center phone number and the local telephone number.</td>
<td>Disables the Call Home command on the main menu.</td>
<td>Enables the Call Home command in the application &lt;Install_Home&gt; directory. Enables the Enable Call Home Event Notification check box. Enables the Test and OK buttons.</td>
<td>Enables the Call Home command on the main menu. Enables all functions in the dialog box.</td>
</tr>
<tr>
<td>Discover On/Off</td>
<td>Allows you to turn product discovery on and off.</td>
<td>Disables the On and Off commands in the Discover menu.</td>
<td>Same as No Privilege</td>
<td>Enables the On and Off commands in the Discover menu.</td>
</tr>
<tr>
<td>E-mail Event Notification Setup</td>
<td>Allows you to define the e-mail server used to send e-mail.</td>
<td>Disables Event Notification E-mail command on the Monitor menu and the E-mail Event Notification Setup button in the Users dialog box. Currently asks, “Are you sure you want to assign Event Management privileges to this group that does not otherwise have read/write for: E-mail Event Notification Setup?”.</td>
<td>Enables the Event Notification E-mail command on the Monitor menu and the E-mail Event Notification Setup button in the Users dialog box. Allows you to open the E-Mail Event Notification Setup dialog box; however, disables the OK button.</td>
<td>Enables Event Notification E-mail command on the Monitor menu and the E-mail Event Notification Setup button in the Users dialog box. Enables all functions in the E-Mail Event Notification Setup dialog box.</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
<td>No Privilege</td>
<td>Read-Only</td>
<td>Read/Write</td>
</tr>
<tr>
<td>------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Enterprise Fabric Mode</td>
<td>Allows you to activate Fabric Binding, Switch Binding, Insistent Domain ID, Rerouting Delay, and Domain RSCN's.</td>
<td>Disables the Enterprise Fabric Mode command from Configure menu.</td>
<td>Allows you to open the Enterprise Fabric Mode dialog box; however, disables the OK button.</td>
<td>Enables Enterprise Fabric Mode command from Configure menu. Enables all functions in the Enterprise Fabric Mode dialog box.</td>
</tr>
<tr>
<td>Event Management</td>
<td>Allows you to define rules with event triggers and actions.</td>
<td>Disables the Event Management tab.</td>
<td>Enables access to the Event Management tab and allows existing rules to be selected and viewed. Disables all action buttons on the tab.</td>
<td>Enables access to the Event Management tab and enables all functions on the tab.</td>
</tr>
<tr>
<td>Export</td>
<td>Allows you to export SAN files, Performance data, Master logs, Connectivity map, Connectivity XML, Product list, Reports, Nicknames, Status, and Zone set activation history.</td>
<td>Disables the Export command on the SAN menu.</td>
<td>Enables the Export command on the SAN menu. Allows you to open the Export dialog box; however, disables the dialog box buttons.</td>
<td>Enables the Export command on the SAN menu. Enables all functions in the Export dialog box.</td>
</tr>
<tr>
<td>Fabric Binding</td>
<td>Allows you to define the switches allowed to join a fabric. Allows you to control access to the Fabric Binding dialog box from the Configure menu.</td>
<td>Disables the Fabric Binding command on the Configure menu.</td>
<td>Enables the Fabric Binding command on the Configure menu; however, disables the OK button.</td>
<td>Enables the Fabric Binding command on the Configure menu. Enables all functions in the dialog box.</td>
</tr>
</tbody>
</table>
### Table 76 Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frame Sniffer</td>
<td>Allows you to count frames passed by a switch port that meet specific criteria. Allows you to control access to the Frame Sniffer dialog box from the Monitor menu.</td>
<td>Disables the Frame Sniffer command on the Monitor menu.</td>
<td>Enables the Frame Sniffer command on the Monitor menu; however, disables the OK button.</td>
<td>Enables the Frame Sniffer command on the Monitor menu. Enables all functions in the dialog box.</td>
</tr>
<tr>
<td>Group Manager – Create Event Log</td>
<td>Allows you to create a log that lists all events that are associated with any of the products in the specified group. Allows you to control access to the Create Event Log function.</td>
<td>Enables the Group Manager command on the Configure menu; however, disables the Create Event Log option. Enables Log &gt; Group on the Monitor menu.</td>
<td>Enables the Group Manager command on the Configure menu; however, disables the Create Event Log option. Enables Group Log on the Monitor menu.</td>
<td>Enables the Group Manager command on the Configure menu and enables the Create Event Log option. Enables Group Log on the Monitor menu.</td>
</tr>
<tr>
<td>Group Manager – Firmware Install</td>
<td>Allows you to install firmware on a group of products (either switches or directors). Allows you to control access to the Firmware Install function.</td>
<td>Enables the Group Manager command on the Configure menu; however, disables the Firmware Install option.</td>
<td>Same as no privilege.</td>
<td>Enables the Group Manager command on the Configure menu and enables the Firmware Install option.</td>
</tr>
<tr>
<td>Group Manager – Run Data Collection</td>
<td>Allows you to collect maintenance data about a group of switches or directors. Allows you to control access to the Run Data Collection function.</td>
<td>Enables the Group Manager command on the Configure menu; however, disables the Run Data Collection option.</td>
<td>Same as no privilege.</td>
<td>Enables the Group Manager command on the Configure menu and enables Run Data Collection option.</td>
</tr>
</tbody>
</table>
Table 76  Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>Allows you to import SAN files (zip), SANvergence Manager Data (mSAN list), Nicknames, Properties (csv) of products and ports, Server HBA Mappings (csv), Storage Port Mappings (csv), and the Zone set activation history (zip). Allows you to control access to the Import dialog box from SAN menu.</td>
<td>Disables the Import command on the SAN menu.</td>
<td>Same as no privilege.</td>
<td>Enables the Import command on the SAN menu and enables the functions in the dialog box.</td>
</tr>
<tr>
<td>License Update</td>
<td>Allows you to update your license. Allows you to control access to the License dialog box from the Help menu.</td>
<td>Disables the License command on the Help menu.</td>
<td>Enables the License command on the Help menu; however, disables the Update and OK buttons.</td>
<td>Enables the License command on the Help menu and enables you to change the license key.</td>
</tr>
</tbody>
</table>
### User Privileges

#### Table 76 Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
</table>
| Log Management             | Allows you to control access to the Export, Clear, Show and Hide commands in the Master Log and individual logs (audit, event, fabric, group, product status, session, and security). | Disables the Export, Clear, Show and Hide commands in the Master Log and individual logs. Enables Show All and Export commands. Disables the Clear and Export buttons on the individual logs. Note that the Export command on the master log right-click menu is controlled by the Export privilege (launches the Export dialog box). If this privilege is removed and the Event Management privilege is assigned then this message appears:  

```html
<title: <Product> <Message>
<Warning>Removing the Log Management privilege does not remove users' ability for Log Management in Event Management. You might also want to consider removing the Event Management privilege as well.

```<<OK>>

| Map Editing                | Recommend Remove                                                                                   | Same as No Privilege                                                                 | Enables the Export, Clear, Show, and Hide commands for the master log and individual logs. Enables the commands on the master log right-click menu (except possibly the Export command). Note that the Export command on the master log is dependent on both this privilege and the Export privilege because this command opens the Export dialog box. Enables all functions in the individual logs. |
|----------------------------|--------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|---------------------------------------------------------------------------|---------------------------------------------------------------------------|
| Map Loop to Hub           | Allows you to identify the discovered hub that is replacing or can replace a loop icon in the Connectivity Map. | Disables the Map to Hub command in the Discover menu and on loop icons.       | Same as No Privilege                                                                 | Enables all Map to Hub functions.                                         |
### Table 76  Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Map Port to Storage</td>
<td>Allows you to construct multi-port storage systems out of individual storage ports.</td>
<td>Disables the Storage Port Mapping command from Discover menu and right-click menus for Storage products and ports in the tree and map.</td>
<td>Enables the Storage Port Mapping command from Discover menu right-click menus for Storage products and ports in the tree and map. Allows you to open the Storage Port Mapping dialog box; however, disables the Create, Delete, right and left arrow, and OK buttons.</td>
<td>Enables the Storage Port Mapping command from Discover menu and right-click menus for Storage products and ports in the tree and map. Enables all functions on the Storage Port Mapping dialog box.</td>
</tr>
<tr>
<td>Monitor Ethernet Event</td>
<td>Allows you to enable events for loss of Ethernet connection.</td>
<td>Disables Ethernet Event on the Monitor menu.</td>
<td>Enables Ethernet Event on the Monitor menu. Allows you to open the Configure Ethernet Event dialog box; however, disables the Enable Ethernet check box, the Ethernet Timeout text box, and the OK button.</td>
<td>Enables Ethernet Event on the Monitor menu. Enables all functions on the Configure Ethernet Event dialog box.</td>
</tr>
<tr>
<td>Nicknames</td>
<td>Allows you to configure Nicknames for the Product.</td>
<td>Disables the Nicknames command in the Configure menu. Disables editing in the Nickname and Port Nickname columns in the product list. Disables Nickname editing in properties sheets.</td>
<td>Enables the Nickname command in the Configure menu. Allows you to open the Configure Nicknames dialog box; however, disables the Add, Remove, Import, and OK buttons. Disables editing in the Nickname and Port Nickname columns in the product list. Disables Nickname editing in properties sheets.</td>
<td>Enables the Nickname command in the Configure menu and enables all functional buttons. Enables editing in the Nickname and Port Nickname columns in the product list. Enables Nickname editing in properties sheets.</td>
</tr>
</tbody>
</table>
## User Privileges

### Table 76 Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Performance</strong></td>
<td>Allows you to configure the performance subsystem, the display of performance graphs, and threshold settings.</td>
<td>Disables entire performance submenu off the Monitor menu as well as the right-click Performance Graph(s) command on ports and switch products.</td>
<td>Enables entire performance submenu off the Monitor menu as well as the right-click Performance Graph(s) command on ports and switch products. Allows you to open the Performance Setup dialog box; however, disables the OK button. No changes can be made. Allows you to open the Performance Graphs dialog box and enables all controls; however, disables the check boxes under the Set Thresholds label on the individual port dialog box (double-click a graph).</td>
<td>Enables entire performance submenu off the Monitor menu and the right-click Performance Graph(s) command on ports and switch products. Enables changes to the Performance Setup dialog box. Allows you to open the Performance Graphs dialog box and enables all controls. Enables all functions on the individual port dialog box (double-click a graph).</td>
</tr>
<tr>
<td><strong>Persist Fabric</strong></td>
<td>Allows you to define the current devices and connections present in a fabric as a baseline and to highlight any changes to that baseline</td>
<td>Disables the Persist Fabric, Unpersist Fabric, and Unpersist Product commands on the Monitor menu and right-click menus of Fabrics and Products. Allows you to see the persistence displays.</td>
<td>Same as no privilege.</td>
<td>Enables the Persist Fabric, Unpersist Fabric, and Unpersist Product commands on the Monitor menu and right-click menus of Fabrics and Products.</td>
</tr>
<tr>
<td><strong>Planning</strong></td>
<td>Allows you to display and edit a planning desktop.</td>
<td>Disables the Planned SAN button on the main toolbar, the New, Open, Save, and Save As Plan commands in the SAN menu and the Planned SAN command on the View menu.</td>
<td>Enables the Open Plan command in the SAN menu which allows you to display a SAN Plan.</td>
<td>Enables the Planned SAN button on the main toolbar and the New, Open, Save, and Save As Plan commands in the SAN menu and the Planned SAN command on the View menu.</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
<td>No Privilege</td>
<td>Read-Only</td>
<td>Read/Write</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port Fencing</td>
<td>Allows you to configure the function that logs ports out of fabrics automatically if they are misbehaving.</td>
<td>Disables the Port Fencing command from the Configure menu.</td>
<td>Enables the Port Fencing command from the Configure menu. Disables the Thresholds Add, Edit, and Delete buttons, the right- and left-arrow threshold assignment buttons, and the Port Unblock and Properties buttons, and the OK button on the Port Fencing dialog box.</td>
<td>Enables the Port Fencing command from the Configure menu. Enables all functions on the Port Fencing dialog box.</td>
</tr>
<tr>
<td>Product Administration</td>
<td>NOTE: This privilege affects EOSc and EOSn switch product Element Managers.</td>
<td>An Element Manager privilege that enables most functionally.</td>
<td>Same as No Privilege</td>
<td>Enables the functions described in the Element Manager User Manual.</td>
</tr>
<tr>
<td>Product Maintenance</td>
<td>NOTE: This privilege affects EOSc and EOSn switch product Element Managers.</td>
<td>An Element Manager privilege that enables maintenance functions.</td>
<td>Same as No Privilege</td>
<td>Enables the functions described in the Element Manager User Manual.</td>
</tr>
<tr>
<td>Product Operation</td>
<td>NOTE: This privilege affects EOSc and EOSn switch product Element Managers.</td>
<td>An Element Manager privilege that enables operator functions.</td>
<td>Same as No Privilege</td>
<td>Enables the functions described in the Element Manager User Manual.</td>
</tr>
</tbody>
</table>
### User Privileges

#### Table 76 Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties Edit</td>
<td>Allows you to edit many director and switch properties.</td>
<td>Enables the Properties command on Edit menu and right-click menus. Disables edit function (removes green triangles) from editable property fields except Nickname columns in Product List. Editing Nicknames is controlled by the Nickname privilege.</td>
<td>Same as No Privilege</td>
<td>Enables Properties command on Edit menu and right-click menus. Enables editable properties (marked by a green triangle) in the Product List and the Properties Sheets.</td>
</tr>
<tr>
<td>Report</td>
<td>Allows you to generate and view the following reports:</td>
<td>Disables the Reports &gt; View command and the Reports &gt; Generate command on the Monitor menu. If this privilege is removed and the Event Management privilege is assigned then this message appears: &lt;title: &lt;Product&gt; Message&gt; &lt;Warning&gt;Removing the Report privilege does not remove users’ ability to generate reports in Event Management. You might also want to consider removing the Event Management privilege as well. &lt;&lt;OK&gt;&gt;</td>
<td>Enables the Reports &gt; View command on the Monitor menu. Enables the Reports &gt; Generate command on the Monitor menu.</td>
<td>Enables the Reports &gt; View command and the Reports &gt; Generate command on the Monitor menu.</td>
</tr>
</tbody>
</table>

- **No Privilege**
  - Enables the Properties command on Edit menu and right-click menus.
  - Enables the Remote Access command on the SAN menu.
  - Enables the Reports > View command and the Reports > Generate command on the Monitor menu.

- **Read-Only**
  - Enables the Remote Access command on the SAN menu.

- **Read/Write**
  - Enables the Remote Access command on the SAN menu.
  - Enables the Reports > View command and the Reports > Generate command on the Monitor menu.
Table 76  Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAN Router Configuration</td>
<td>Allows you to view and configure SAN routing products.</td>
<td>Disables the Router Port Configuration, SAN Router Configuration, Configuration Archive, Router Consistency, Log Viewer, Save to Flash, and Enable LUN Mapping commands on the Configure &gt; SAN Routing menu and right-click menus. Disables the Reports submenu commands in the Monitor menu. Disables the Reports command on the right-click menu.</td>
<td>Enables the Router Port Configuration, SAN Router Configuration, Configuration Archive, Router Consistency, and Log Viewer commands on the Configure &gt; SAN Routing menu and right-click menus; however, disables configuration controls. Disables the Save to Flash and Enable LUN Mapping commands on the Configure &gt; SAN Routing menu and right-click menus. Enables the following Monitor &gt; Reports commands Consistency, iFCP Connections and Zones, LUN Mapping, Name Server, R Port, and Router Configuration. Enables the Reports command on the right-click menu and all its submenu items.</td>
<td>Enables the Router Port Configuration, SAN Router Configuration, Configuration Archive, Router Consistency, Log Viewer, Save to Flash, Enable LUN Mapping, and Reports commands on the Configure &gt; SAN Routing menu and right-click menus. Enables all functions on the associated dialog boxes.</td>
</tr>
</tbody>
</table>

About user privileges
<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Servers</td>
<td>Allows you to identify all the HBAs that are in the same server.</td>
<td>Disables the Servers command from the Discover menu. Disable the Server right-click command on HBAs.</td>
<td>Enables Servers command from the Discover menu and right-click menu; however, disables the Create, Delete, and OK buttons.</td>
<td>Enables Servers command from the Discover menu and right-click menu. Enables all functions in the Servers dialog box.</td>
</tr>
</tbody>
</table>
### Table 76  Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup Tools</td>
<td>Allows you to define and place commands on product icons and in the Tools menu.</td>
<td>Disables the Setup Tools command on the Tools menu. Any existing Tools and/or right-click commands already defined or defined by others are available for use; however, you cannot configure new items. If this privilege is removed and the Event Management privilege is assigned then this message appears: <code>&lt;title: &lt;Product&gt; Message&gt; &lt;Warning&gt;Removing the Log Management privilege does not remove users’ ability for Setup Tools in Event Management. You might also want to consider removing the Event Management privilege as well. &lt;&lt;OK&gt;&gt;</code></td>
<td>Enables the Setup Tools command on the Tools menu; however, disables the OK button.</td>
<td>Enables the Setup Tools command on the Tools menu. Enables all functions in the Setup Tools dialog box.</td>
</tr>
<tr>
<td>Show Route</td>
<td>Allows you to highlight the route through the fabric that two-end nodes use to communicate.</td>
<td>Disables the Show Route commands on the Monitor menu and right-click menus on ports. Disables the Hide Route command on the Monitor menu.</td>
<td>Same as no privilege.</td>
<td>Enables the Show Route commands on the Monitor menu and right-click menus on ports.</td>
</tr>
<tr>
<td>Shutdown</td>
<td>Allows you to exit and close the server and optionally the client.</td>
<td>Disables the Shutdown command on the SAN menu.</td>
<td>Same as no privilege.</td>
<td>Enables the Shutdown command on the SAN menu.</td>
</tr>
</tbody>
</table>
### Table 76 Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMP Agent Configuration</td>
<td>Allows you to configure community strings and trap recipients for the SNMP Agent.</td>
<td>Disables the SNMP Agent &gt; On, Off, and Setup commands on the Monitor menu. If this privilege is removed and the Event Management privilege is assigned then this message appears: &lt;title: &lt;Product&gt; Message&gt; &lt;Warning&gt; Removing the SNMP privilege does not remove users’ ability for SNMP configuration in Event Management. You might also want to consider removing the Event Management privilege as well. &lt;&lt;&lt;OK&gt;&gt;</td>
<td>Disables the SNMP Agent &gt; On, and Off commands on the Monitor menu. Enables the SNMP Agent &gt; Setup command on the Monitor menu; however, disables all functions in the SNMP Setup dialog box.</td>
<td>Enables the SNMP Agent &gt; On, Off, and Setup commands on the Monitor menu. Enables all functions in the SNMP Setup dialog box.</td>
</tr>
<tr>
<td>Software Configuration Parameters</td>
<td>Allows you to configure some of the properties of the client and server of the management application.</td>
<td>Disables the Software Configuration Parameters folder and sub pages in the Options dialog box. The configuration cannot be viewed.</td>
<td>Enables the Software Configuration Parameters folder and sub pages in the Options dialog box; however, disables the OK and Apply button when any of the sub pages are selected.</td>
<td>Enables the Software Configuration Parameters folder and sub pages in the Options dialog box. Enables all functions when any of those sub pages are selected.</td>
</tr>
<tr>
<td>Trap Forwarding</td>
<td>Allows you to specify where to forward the traps it receives from other systems.</td>
<td>Disables the Trap Forwarding command from the Monitor menu.</td>
<td>Enables the Trap Forwarding command from the Monitor menu however, disables the Add, Remove, and OK buttons.</td>
<td>Enables the Trap Forwarding command from the Monitor menu. Enables all functions in the Configure Trap Forwarding dialog box.</td>
</tr>
</tbody>
</table>
### Table 76 Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Management</td>
<td>Allows you to create and the define users, groups, as well as assign privileges and views to groups.</td>
<td>Disables the Users command on the main SAN and the Users button on the main tool bar. Disables the User List button in the Event Notification Setup dialog box.</td>
<td>Enables the Users command on the SAN menu and the Users button on the main tool bar; however, disables the Add, Edit, and Remove Users, the Add and Remove Groups, and the OK buttons on the Users dialog box. Enables the Edit Groups button to display the Group dialog box (with OK button disabled).</td>
<td>Enables the Users command on the SAN menu and the Users button on the main tool bar. Enables all functions on the Users dialog box and the secondary Group dialog box.</td>
</tr>
<tr>
<td>View Management</td>
<td>Allows you to create, edit, and delete views. Selecting from views should always be allowed unless restricted by the assignment of Views in the Group definition in the Users dialog box.</td>
<td>Disables the Create View, Copy View, Edit View, Delete View, and Connectivity View commands in the View &gt; Manage View menu and the first tab header on the main desktop. Allows you to select an assigned views but not create or change.</td>
<td>Enables the Create View and Edit View commands in the View &gt; Manage View menu and the first tab header on the main desktop; however, disables the OK button in the Create View or Edit View dialog boxes. Enables the Copy View, Delete View, and Connectivity View &gt; Create and Refresh commands. Allows you to select an assigned views but not create or change.</td>
<td>Activates all view commands in the View &gt; Manage View menu and the first tab header on the main desktop. Enables all functions in the dialog boxes.</td>
</tr>
<tr>
<td>Virtual Fabric</td>
<td>Allows you to configure virtual switches and fabrics.</td>
<td>Disables the Virtual Switches command from the Configure menu. However, this does not restrict the Virtual Switches command in the Element Managers.</td>
<td>Enables the Virtual Switches command in the Configure menu; however, disables the Edit and OK buttons in the Virtual Switches dialog box.</td>
<td>Enables the Virtual Switches command in the Configure menu. Enables all functions in the Virtual Switches dialog box.</td>
</tr>
<tr>
<td>Privilege</td>
<td>Description</td>
<td>No Privilege</td>
<td>Read-Only</td>
<td>Read/Write</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Zoning Activation</strong></td>
<td>Allows you to activate a zone set selected in the zoning dialog box</td>
<td>Disables the Activate, Deactivate, and Zoning Policies buttons in the Zoning dialog box.</td>
<td>Same as no privilege.</td>
<td>Enables the Activate, Deactivate, and Zoning Policies buttons in the Zoning dialog box.</td>
</tr>
<tr>
<td><strong>Zoning Fabric Libraries</strong></td>
<td>Allows you to edit data in the Fabric Zone Libraries.</td>
<td>Removes the fabric library from the Zoning Library drop down list in the Zoning dialog box. Disables all the fabric libraries in the list of targets in the Copy Into right-click commands.</td>
<td>Includes the fabric library in the Zoning Library drop down list in the Zoning dialog box. Disables the Save To on the Zoning dialog box - Active Zone Set tab. Disables the right-arrow (for adding), left arrow (for removing), New Zone, New Member, New Set, Import, OK, and Apply buttons on the Zoning dialog box - Zone Library tab. Enables Cancel and Help buttons in the Zoning dialog box. Enables Find and Export buttons in the Zoning dialog box - Zone Library tab. Enables Compare and Report buttons in the Zoning dialog box - Active Zone Set tab.</td>
<td>Includes the fabric library in the Zoning Library drop down list in the Zoning dialog box. Enables all functions on the dialog boxes.</td>
</tr>
</tbody>
</table>
### Table 76 Privileges (continued)

<table>
<thead>
<tr>
<th>Privilege</th>
<th>Description</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoning Global Library (no mSAN and Router Fabric)</td>
<td>Allows you to add data in the Global Zone Library. Does not effect on Router Fabric or mSAN libraries.</td>
<td>Removes Global Library from the Zoning Library drop down list in the Zoning dialog box. Disables the Global command in the list of targets in the Copy Into right-click commands.</td>
<td>Includes the fabric library in the Zoning Library drop down list in the Zoning dialog box. Disables the Save To on the Zoning dialog box - Active Zone Set tab. Disables the right-arrow (for adding), left arrow (for removing), New Zone, New Member, New Set, Import, OK, and Apply buttons on the Zoning dialog box - Zone Library tab. Enables Cancel and Help buttons in the Zoning dialog box. Enables Find and Export buttons in the Zoning dialog box - Zone Library tab. Enables Compare and Report buttons in the Zoning dialog box - Active Zone Set tab. Enables all commands for the Potential Member right-click menu. Enables Port label, Search, and Properties commands for the Zones right-click menu. Enables Properties command for the Zone Sets right-click menu. Enables Properties command for the Zones in Zone Sets right-click menu.</td>
<td>Includes the Global Library in the Zoning Library drop down list in the Zoning dialog box. Enables all functions on the dialog boxes.</td>
</tr>
</tbody>
</table>
User Privileges

About user groups and access levels

A user with administrative privileges can assign users to user groups. Five pre-configured user groups (see below) are available with the application; however, System Administrators can also create user groups manually.

Table 77 User groups

<table>
<thead>
<tr>
<th>Feature</th>
<th>User Groups with Read/Write Access</th>
<th>User Groups with Read-Only Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Session Management</td>
<td>System Administrator, Security Administrator</td>
<td>Operator, Maintenance, Product Administrator</td>
</tr>
<tr>
<td>Add/Delete Properties</td>
<td>System Administrator</td>
<td>Operator, Maintenance, Product Administrator</td>
</tr>
<tr>
<td>Backup</td>
<td>System Administrator, Maintenance, Product Administrator</td>
<td>Operator</td>
</tr>
<tr>
<td>Call Home Event Notification Setup</td>
<td>System Administrator, Maintenance</td>
<td>Operator, Product Administrator</td>
</tr>
<tr>
<td>Device Administration</td>
<td>System Administrator, Product Administrator</td>
<td></td>
</tr>
<tr>
<td>Device Maintenance</td>
<td>System Administrator, Maintenance</td>
<td></td>
</tr>
<tr>
<td>Device Operation</td>
<td>System Administrator, Operator</td>
<td></td>
</tr>
<tr>
<td>Discover On/Off</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Discovery Setup</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Email Event Notification Setup</td>
<td>System Administrator, Maintenance</td>
<td>Operator, Product Administrator</td>
</tr>
<tr>
<td>Enterprise Fabric Mode</td>
<td>System Administrator, Security Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Event Management</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Export</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>FabricBinding</td>
<td>System Administrator, Security Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Frame Sniffer</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
</tbody>
</table>
### Table 77  User groups (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>User Groups with Read/Write Access</th>
<th>User Groups with Read-Only Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Manager – Create Event Log</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Group Manager – Firmware Install</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Group Manager – Run Data Collection</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Import</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>License Update</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Log Management</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>LUN Management</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Map Editing</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Map HBA to Server</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Map Loop to Hub</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Map Port to Storage</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Monitor Ethernet Event</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Performance</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Persist Fabric</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Planning</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>PortFencing</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
</tbody>
</table>
### User Privileges

#### Table 77 User groups (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>User Groups with Read/Write Access</th>
<th>User Groups with Read-Only Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties Edit</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Remote Access</td>
<td>System Administrator, Security Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Report</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Setup Tools</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Show Route</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Shutdown</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>SNMP Agent Configuration</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Software Configuration Properties</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Trap Forwarding</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>User Management</td>
<td>System Administrator, Security Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>View Management</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>VirtualFabric</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Zone Activating and Editing</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Zone Editing Only</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
</tbody>
</table>
### User groups (continued)

<table>
<thead>
<tr>
<th>Feature</th>
<th>User Groups with Read/Write Access</th>
<th>User Groups with Read-Only Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoning Activation</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Zoning Fabric Libraries</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
<tr>
<td>Zoning Global Library</td>
<td>System Administrator</td>
<td>Maintenance, Operator, Product Administrator</td>
</tr>
</tbody>
</table>
Table 78 lists the user groups and assigned privileges for fresh install.

<table>
<thead>
<tr>
<th>Group</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Administrator</td>
<td></td>
<td></td>
<td>Active Session Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Add / Delete Properties</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Backup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Call Home Event Notification</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Setup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Discover On/Off</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Discovery Setup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>E-mail Event Notification Setup</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Enterprise Fabric Mode</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Event Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Export</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Fabric Binding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Frame Sniffer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Group Manager – Create Event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Log</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Group Manager – Firmware Install</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Group Manager – Run Data Collection</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Import</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>License Update</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Log Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Map Editing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Map Loop to Hub</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Map Port to Storage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Monitor Ethernet Event</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Nicknames</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Performance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Persist Fabric</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Planning</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Port Fencing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Product Administration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Product Maintenance</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Product Operation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Properties Edit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Remote Access</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ReporSAN Router Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Security Admin</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Servers</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Setup Tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Show Route</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Shutdown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>SNMP Agent Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Software Configuration Parameters</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Trap Forwarding</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>View Management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Virtual Fabric</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Zoning Activation</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Zoning Fabric Libraries</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Zoning Global Library</td>
</tr>
</tbody>
</table>
### User groups and assigned privileges for fresh install (continued)

<table>
<thead>
<tr>
<th>Group</th>
<th>No Privilege</th>
<th>Read-Only</th>
<th>Read/Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>No Privilege</td>
<td>Read-Only</td>
<td>Read/Write</td>
</tr>
<tr>
<td>---------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Maintenance</td>
<td>Product Administration</td>
<td>Active Session Management&lt;br&gt;Add/Delete Properties&lt;br&gt;Discover On/Off&lt;br&gt;Discovery Setup&lt;br&gt;Enterprise Fabric Mode&lt;br&gt;Event Management&lt;br&gt;Export&lt;br&gt;Fabric Binding&lt;br&gt;Frame Sniffer&lt;br&gt;Group Manager – Create Event Log&lt;br&gt;Group Manager – Firmware Install&lt;br&gt;Group Manager – Run Data Collection&lt;br&gt;Import&lt;br&gt;License Update&lt;br&gt;Log Management&lt;br&gt;Map Editing&lt;br&gt;Map Loop to Hub&lt;br&gt;Map Port to Storage&lt;br&gt;Monitor Ethernet Event&lt;br&gt;Nicknames&lt;br&gt;Performance&lt;br&gt;Persist Fabric&lt;br&gt;Planning&lt;br&gt;Port Fencing&lt;br&gt;Properties Edit&lt;br&gt;Remote Access&lt;br&gt;Report&lt;br&gt;San Router Configuration&lt;br&gt;Security Admin&lt;br&gt;Servers&lt;br&gt;Setup Tools&lt;br&gt;Show Route&lt;br&gt;Shutdown&lt;br&gt;SNMP Agent Configuration&lt;br&gt;Software Configuration&lt;br&gt;Parameters&lt;br&gt;Trap Forwarding&lt;br&gt;User Management&lt;br&gt;View Management&lt;br&gt;Virtual Fabric&lt;br&gt;Zoning Activation&lt;br&gt;Zoning Fabric Libraries&lt;br&gt;Zoning Global Library</td>
<td>Backup&lt;br&gt;Call Home Event Notification&lt;br&gt;Setup&lt;br&gt;Product Maintenance&lt;br&gt;E-mail Event Notification Setup</td>
</tr>
<tr>
<td>Group</td>
<td>No Privilege</td>
<td>Read-Only</td>
<td>Read/Write</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Group</td>
<td>No Privilege</td>
<td>Read-Only</td>
<td>Read/Write</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-------------------------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Product Administrator</td>
<td>Product Maintenance</td>
<td>Active Session Management</td>
<td>Backup</td>
</tr>
<tr>
<td></td>
<td>Product Operation</td>
<td>Add / Delete Properties</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Call Home Event Notification</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Setup</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Discover On/Off</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Discovery Setup</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>E-mail Event Notification Setup</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enterprise Fabric Mode</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Event Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Export</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fabric Binding</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Frame Sniffer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group Manager – Create Event Log</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group Manager – Firmware Install</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Group Manager – Run Data Collection</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Import</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>License Update</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Log Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Editing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Loop to Hub</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Map Port to Storage</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Monitor Ethernet Event</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Nicknames</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Performance</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Persist Fabric</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Planning</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Port Fencing</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Properties Edit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Remote Access</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Report</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SAN Router Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Security Admin</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Servers</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Setup Tools</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Show Route</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Shutdown</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SNMP Agent Configuration</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Software Configuration Parameters</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Trap Forwarding</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>User Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>View Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Virtual Fabric</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zoning Activation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zoning Fabric Libraries</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Zoning Global Library</td>
<td></td>
</tr>
</tbody>
</table>

Table 78  User groups and assigned privileges for fresh install (continued)
Table 79 lists the Element Manager privileges and access control for managed products other than an ED-10000M.

**Table 79 Element Manager privileges and access control (For managed products other than an ED-10000M)**

<table>
<thead>
<tr>
<th>User Functions</th>
<th>Product Administrator</th>
<th>Product Operation</th>
<th>Product Maintenance</th>
<th>Security Admin</th>
<th>PFE Required</th>
<th>Data Disrupting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow/Prohibit Matrix, Active (FICON style only)</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Allow/Prohibit Matrix, Stored (FICON style only)</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternate Control Prohibit, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>API Password (i10K only)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Backup/Restore Configuration</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Call Home Notification, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card (FRU) Beaconing, Enable</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Channel Wrap, Enable on port (FICON style only)</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>CNT WAN, Enable</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Collection</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Date/Time Synchronization, Enable</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date/Time, Configure</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail Notification, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Export Configuration</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fabric Parameters, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Feature Key, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware Library, Manage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firmware Library, View</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>User Functions</td>
<td>Product Administrator</td>
<td>Product Operation</td>
<td>Product Maintenance</td>
<td>Security Admin</td>
<td>PFE Required</td>
<td>Data Disrupting</td>
</tr>
<tr>
<td>----------------------------------------</td>
<td>-----------------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>----------------</td>
<td>--------------</td>
<td>----------------</td>
</tr>
<tr>
<td>FICON CUP Zoning</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>?</td>
</tr>
<tr>
<td>FMS, Configure</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>FMS, Enable</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Identification/Nickname, Configure</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPL</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Link Incident (LIN) Alert, Clear</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Audit, Clear</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Embedded Port, Clear</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Embedded Port, Modify</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Event, Clear</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Hardware, Clear</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Link Incident (LIN), Clear</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Open Trunking, View (Note: This log cannot be cleared)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Log, Port Threshold Alert, Clear</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Security*</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Log, Switch Fabric, Clear</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Log, Switch Performance Threshold Alert, Clear</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management Style, Select</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online State, Set switch</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>
### Table 79  Element Manager privileges and access control (For managed products other than an ED-10000M) (continued)

<table>
<thead>
<tr>
<th>User Functions</th>
<th>Product Administrator</th>
<th>Product Operation</th>
<th>Product Maintenance</th>
<th>Security Admin</th>
<th>PFE Required</th>
<th>Data Disrupting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Trunking, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
<td>✗</td>
</tr>
<tr>
<td>OSMS, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>OSMS, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td>✗</td>
</tr>
<tr>
<td>Partitioning, Configure (i10K only)</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Port Beaconing, Enable</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Port Diagnostics</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ports, Configure</td>
<td>• Name</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Blocked</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td></td>
<td>• RX BB Credit</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LIN Alerts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Speed</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Port Binding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Preferred Path, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>Reset Port</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>✗</td>
</tr>
<tr>
<td>SANtegrity Authentication* (in Element Manager and Security Center)</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reset Switch/Partition (NVRAM)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statistics Counters, Clear</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### User Privileges

#### Table 79  Element Manager privileges and access control (For managed products other than an ED-10000M) (continued)

<table>
<thead>
<tr>
<th>User Functions</th>
<th>Product Administrator</th>
<th>Product Operation</th>
<th>Product Maintenance</th>
<th>Security Admin</th>
<th>PFE Required</th>
<th>Data Disrupting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Swap Ports (FICON style only)</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Binding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x⁷</td>
<td></td>
</tr>
<tr>
<td>• Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Connection Policy</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Membership List</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Parameters, Configure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x⁶</td>
<td></td>
</tr>
<tr>
<td>• Domain RSCNs</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Insistent Domain IDs</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Switch/Director Speed</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Zoning RSCNs</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Performance Threshold Alert, Clear Alert (i10K only)</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Performance Threshold Alert, View Data (i10K only)</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switchover (FRU)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>System Error Light, Clear</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet, Enable</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threshold Alerts, Clear</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threshold Alerts, Configure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit Beaconing, Enable</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Server, Enable</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>WWN or Nickname, Configure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 79   Element Manager privileges and access control (For managed products other than an ED-10000M) (continued)

<table>
<thead>
<tr>
<th>User Functions</th>
<th>Product Administrator</th>
<th>Product Operation</th>
<th>Product Maintenance</th>
<th>Security Admin</th>
<th>PFE Required</th>
<th>Data Disrupting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zoning Alerts, Clear</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control Path Processor Access</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Install and Replace Services Modules</td>
<td>√ √</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Operating Parameters</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Services Modules</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ports, Configure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Type</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Virtualization Engines</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Virtualization Engine Statistics</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. Specifically Interop mode, requiring switch offline  
b. Feature(s) may **not** be disruptive to data traffic. However, since purpose of command may affect access control mechanism or design of SAN fabric, probably should be an item limited to users with Admin Domain privileges.  
c. Hot Cat not disruptive, but load of different switch software version is a management function that should be controlled.  
d. Activation has been known to cause problems in large fabrics  
e. For Maintenance-level users, ports can be blocked only from the right-click menu option (not the dialog)  
f. Feature(s) may not be disruptive to data traffic. However, because the purpose of the command may affect the access control mechanism or design of SAN fabric, probably should be an item limited to users with Admin Domain privileges.

Table 80 lists access control for the ED-10000M products.

### Table 80   Access control for ED-10000M products

<table>
<thead>
<tr>
<th>Element Manager Feature</th>
<th>Product Administrator</th>
<th>Operator</th>
<th>Maintenance</th>
<th>Security Administrator</th>
<th>PFE Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow/Prohibit Matrix, Active (FICON style only)</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Allow/Prohibit Matrix, Stored (FICON style only)</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alternate Control Prohibit, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 80   Access control for ED-10000M products (continued)

<table>
<thead>
<tr>
<th>Element Manager Feature</th>
<th>Product Administrator</th>
<th>Operator</th>
<th>Maintenance</th>
<th>Security Administrator</th>
<th>PFE Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>API Password (i10K only)</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Backup/Restore Configuration</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Call Home Notification, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Card (FRU) Beaconing, Enable</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Channel Wrap, Enable on port (FICON style only)</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNT WAN, Enable</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Data Collection</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Date/Time Synchronization, Enable</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Date/Time, Configure</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-mail Notification, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Export Configuration</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fabric Parameters, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√(^a)</td>
</tr>
<tr>
<td>Feature Key, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>(^b)</td>
</tr>
<tr>
<td>Firmware Library, Manage</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td>(^c)</td>
</tr>
<tr>
<td>Firmware Library, View</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>FICON CUP Zoning</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>FMS, Configure</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FMS, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Identification/Nickname, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IPL</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 80  Access control for ED-10000M products (continued)

<table>
<thead>
<tr>
<th>Element Manager Feature</th>
<th>Product Administrator</th>
<th>Operator</th>
<th>Maintenance</th>
<th>Security Administrator</th>
<th>PFE Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Incident (LIN) Alert, Clear</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Audit, Clear</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Embedded Port, Clear</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Embedded Port, Modify</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Event, Clear</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Hardware, Clear</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Link Incident (LIN), Clear</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Open Trunking, View (Note: This log cannot be cleared)</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Log, Port Threshold Alert, Clear</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Switch Fabric, Clear</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Log, Switch Performance Threshold Alert, Clear</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>Management Style, Select</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Online State, Set switch</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Open Trunking, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td>√</td>
</tr>
<tr>
<td>OSMS, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OSMS, Enable</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Partitioning, Configure (j10K only)</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Beaconing, Enable</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Diagnostics</td>
<td>√</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Ports, Configure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### User Privileges

#### Table 80  Access control for ED-10000M products (continued)

<table>
<thead>
<tr>
<th>Element Manager Feature</th>
<th>Product Administrator</th>
<th>Operator</th>
<th>Maintenance Administrator</th>
<th>Security Administrator</th>
<th>PFE Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Name</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Blocked</td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>• RX BB Credit</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• LIN Alerts</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Speed</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Port Binding</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Preferred Path, Configure</td>
<td>√</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Reset Port</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reset Switch/Partition (NVRAM) Configuration</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SNMP, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Statistics Counters, Clear</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Swap Ports (FICON style only)</td>
<td>√</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Binding</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x1</td>
</tr>
<tr>
<td>• Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Connection Policy</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Membership List</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Parameters, Configure</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x1</td>
</tr>
<tr>
<td>• Domain RSCNs</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Insistent Domain IDs</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Switch/Director Speed</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Zoning RSCNs</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**Table 80  Access control for ED-10000M products (continued)**

<table>
<thead>
<tr>
<th>Element Manager Feature</th>
<th>Product Administrator</th>
<th>Operator</th>
<th>Maintenance</th>
<th>Security Administrator</th>
<th>PFE Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch Performance Threshold Alert, Clear Alert (i10K only)</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switch Performance Threshold Alert, View Data (i10K only)</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Switchover (FRU)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>System Error Light, Clear</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telnet, Enable</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threshold Alerts, Clear</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threshold Alerts, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit Beaconing, Enable</td>
<td>√</td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web Server, Enable</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>WWN or Nickname, Configure</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Zoning Enforcement Alerts, Clear</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a. Specifically Interop mode, requiring switch offline
b. Feature(s) may not be disruptive to data traffic. However, since purpose of command may affect access control mechanism or design of SAN fabric, probably should be an item limited to users with Admin Domain privileges.
c. Hot Cat not disruptive, but load of different switch software version is a management function that should be controlled.
d. Activation has been known to cause problems in large fabrics
e. For Maintenance-level users, ports can be blocked only from the right-click menu option (not the dialog)
f. Feature(s) may not be disruptive to data traffic. However, since purpose of command may affect access control mechanism or design of SAN fabric, probably should be an item limited to users with Admin Domain privileges.
This appendix provides useful reference information.

- Icon legend .......................................................... 762
- Keyboard shortcuts .................................................. 764
- GNU Lesser General Public License ......................... 766
Various icons are used to illustrate devices and connections in a SAN. The following tables list icons that display on the Physical Map.

The following table lists the SAN product icons that display on the topology. Some of the icons shown in Table 81 only display when certain features are licensed.

**Table 81 Product icons**

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="SAN Router" /></td>
<td>SAN Router</td>
<td><img src="image" alt="Generic Switch or Director" /></td>
<td>Generic Switch or Director</td>
</tr>
<tr>
<td><img src="image" alt="ASM Switch" /></td>
<td>ASM Switch</td>
<td><img src="image" alt="Blade Switch" /></td>
<td>Blade Switch</td>
</tr>
<tr>
<td><img src="image" alt="Bridge" /></td>
<td>Bridge</td>
<td><img src="image" alt="Director" /></td>
<td>Director</td>
</tr>
<tr>
<td><img src="image" alt="FCIP Bridge or Gateway" /></td>
<td>FCIP Bridge or Gateway</td>
<td><img src="image" alt="Host" /></td>
<td>Host</td>
</tr>
<tr>
<td><img src="image" alt="Host Bus Adapter (HBA)" /></td>
<td>Host Bus Adapter (HBA)</td>
<td><img src="image" alt="Hub" /></td>
<td>Hub</td>
</tr>
<tr>
<td><img src="image" alt="iSCSI Device" /></td>
<td>iSCSI Device</td>
<td><img src="image" alt="iSCSI Bridge or Gateway" /></td>
<td>iSCSI Bridge or Gateway</td>
</tr>
<tr>
<td><img src="image" alt="iSCSI" /></td>
<td>iSCSI</td>
<td><img src="image" alt="JBOD" /></td>
<td>JBOD</td>
</tr>
<tr>
<td><img src="image" alt="JDISK" /></td>
<td>JDISK</td>
<td><img src="image" alt="Network Attached Storage (NAS)" /></td>
<td>Network Attached Storage (NAS)</td>
</tr>
<tr>
<td><img src="image" alt="Loop" /></td>
<td>Loop</td>
<td><img src="image" alt="Storage" /></td>
<td>Storage</td>
</tr>
<tr>
<td><img src="image" alt="Server" /></td>
<td>Server</td>
<td><img src="image" alt="Unknown" /></td>
<td>Unknown</td>
</tr>
<tr>
<td><img src="image" alt="Tape" /></td>
<td>Tape</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Product status icons

Table 82 lists the SAN group icons that display.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon.png" alt="No icon" /></td>
<td>Operational</td>
</tr>
<tr>
<td><img src="icon.png" alt="Attention" /></td>
<td>Attention</td>
</tr>
<tr>
<td><img src="icon.png" alt="Degraded" /></td>
<td>Degraded</td>
</tr>
<tr>
<td><img src="icon.png" alt="Device Added" /></td>
<td>Device Added</td>
</tr>
<tr>
<td><img src="icon.png" alt="Device Removed" /></td>
<td>Device Removed</td>
</tr>
<tr>
<td><img src="icon.png" alt="Failed" /></td>
<td>Failed</td>
</tr>
<tr>
<td><img src="icon.png" alt="Routed In" /></td>
<td>Routed In</td>
</tr>
<tr>
<td><img src="icon.png" alt="Routed Out" /></td>
<td>Routed Out</td>
</tr>
<tr>
<td><img src="icon.png" alt="Unknown/Link Down" /></td>
<td>Unknown/Link Down</td>
</tr>
<tr>
<td><img src="icon.png" alt="Virtual Switch" /></td>
<td>Virtual Switch</td>
</tr>
</tbody>
</table>

### Event icons

Table 83 lists the event icons that display.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="icon.png" alt="Informational" /></td>
<td>Informational</td>
</tr>
<tr>
<td><img src="icon.png" alt="Warning" /></td>
<td>Warning</td>
</tr>
<tr>
<td><img src="icon.png" alt="Fatal" /></td>
<td>Fatal</td>
</tr>
</tbody>
</table>
**Keyboard shortcuts**

You can use the keystrokes shown in Table 84 to perform common functions.

*Note:* To open a menu using keystrokes, press ALT + the underlined letter. To open a submenu, release the ALT key first, then press the key for the underlined letter of the submenu option.

<table>
<thead>
<tr>
<th>Menu item or function</th>
<th>Keyboard shortcut</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Panels</td>
<td>F12</td>
</tr>
<tr>
<td>Collapse</td>
<td>CTRL + L</td>
</tr>
<tr>
<td>Command Tool</td>
<td>SHIFT + F4</td>
</tr>
<tr>
<td>Connectivity Map</td>
<td>F7</td>
</tr>
<tr>
<td>Copy</td>
<td>CTRL + C</td>
</tr>
<tr>
<td>Cut</td>
<td>CTRL + X</td>
</tr>
<tr>
<td>Delete</td>
<td>Delete</td>
</tr>
<tr>
<td>Delete All</td>
<td>CTRL +Delete</td>
</tr>
<tr>
<td>Event Management</td>
<td>F11</td>
</tr>
<tr>
<td>Expand</td>
<td>CTRL + E</td>
</tr>
<tr>
<td>Help</td>
<td>F1</td>
</tr>
<tr>
<td>Insert Devices</td>
<td>CTRL +D</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>SHIFT + F1</td>
</tr>
<tr>
<td>Master Log</td>
<td>F5</td>
</tr>
<tr>
<td>Multiple Devices (Planned SAN only)</td>
<td>CTRL + D</td>
</tr>
<tr>
<td>Netscape</td>
<td>SHIFT + F2</td>
</tr>
<tr>
<td>New Plan</td>
<td>CTRL + N</td>
</tr>
<tr>
<td>Open Plan</td>
<td>CTRL + O</td>
</tr>
<tr>
<td>Open SAN menu</td>
<td>F10</td>
</tr>
<tr>
<td>Menu item or function</td>
<td>Keyboard shortcut</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Paste</td>
<td>CTRL + V</td>
</tr>
<tr>
<td>Product List</td>
<td>F9</td>
</tr>
<tr>
<td>Properties</td>
<td>CTRL + P</td>
</tr>
<tr>
<td>Security Center</td>
<td>F8</td>
</tr>
<tr>
<td>Select All</td>
<td>CTRL + A</td>
</tr>
<tr>
<td>Select Connections</td>
<td>CTRL + T</td>
</tr>
<tr>
<td>Show Ports</td>
<td>F4</td>
</tr>
<tr>
<td>View Utilization</td>
<td>CTRL + U</td>
</tr>
<tr>
<td>Zoom In</td>
<td>CTRL + NumPad+</td>
</tr>
<tr>
<td>Zoom Out</td>
<td>CTRL + NumPad-</td>
</tr>
</tbody>
</table>
GNU Lesser General Public License

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc., 9 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete
object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it
becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

---

**GNU Lesser General Public License terms and conditions for copying, distribution, and modification**

1. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables. The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)
"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

2. You may copy and distribute verbatim copies of the Library’s complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a. The modified work must itself be a software library.

   b. You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

   c. You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

   d. If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.
(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

5. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you
accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

6. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

7. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work
under terms of your choice, provided that the terms permit modification of the work for the customer’s own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a. Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable “work that uses the Library”, as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b. Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user’s computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c. Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d. If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e. Verify that the user has already received a copy of these materials or that you have already sent this user a copy.
For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

8. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

   a. Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

   b. Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

9. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the
Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

11. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients’ exercise of the rights granted herein.

You are not responsible for enforcing compliance by third parties with this License.

12. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
13. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

14. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

15. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

No Warranty

16. Because the library is licensed free of charge, there is no warranty for the library, to the extent permitted by applicable law.

Except when otherwise stated in writing the copyright holders and/or other parties provide the library "as is" without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The entire risk as to the quality and performance of the library is with you. should the library prove defective, you assume the cost of all necessary servicing, repair or correction.
17. In no event unless required by applicable law or agreed to in writing will any copyright holder, or any other party who may modify and/or redistribute the library as permitted above, be liable to you for damages, including any general, special, incidental or consequential damages arising out of the use or inability to use the library (including but not limited to loss of data or data being rendered inaccurate or losses sustained by you or third parties or a failure of the library to operate with any other software), even if such holder or other party has been advised of the possibility of such damages.
This glossary contains terms related to EMC Connectrix. Many of these terms are used in this manual. The glossary includes terms and definitions from:


## Glossary

### A

**Access Control**
List of all devices that can access other devices across the network and the permissions associated with that access. See also persistent binding and zoning.

**Active Domain ID**
The Domain ID actively being used by a switch. It is assigned to a switch by the principal switch.

**Active Zone Set**
A zone set that is currently enabled. (Only one zone set at a time can be active.) Zoning across the fabric is determined by the characteristics of the active zone set.

**Agent**
Software that processes queries on behalf of an application and returns replies.

**Alarm**
An SNMP message notifying an operator of a network problem.

**Any-to-Any Port Connectivity**
For each source port, software configured hardware routing tables that define the destination ports with which the source port is allowed to communicate.

**Application**
(1) The use to which an information processing system is put, for example, a payroll application, an airline reservation application, a network application. (2) A collection of software components used to perform specific types of work on a computer.

**Arbitration**
The process of selecting one respondent from a collection of several candidates that request service concurrently.

**ASIC**
Application-Specific Integrated Circuit, a circuit designed for a specific purpose, such as implementing lower-layer Fibre Channel protocols (FC-0). ASICs contrast with general-purpose devices such as memory chips or microprocessors, which can be used in many different applications.

**ASCII**
American Standard Code for Information Interchange.

**Audit Log**
A log containing summaries of actions taken by a Connectrix Management software user, recording an audit trail of changes. For example: adding, modifying, or deleting user or product administration records the operation, including the date and time, in the audit log.
| **Authentication** | Verification of the identity of a process or person. |
| **B** |  |
| **BB_Credit** | See Buffer-to-Buffer Credit. |
| **Beaconing** | Repeated transmission of a beacon light and message until the error is corrected or bypassed. |
| **BER** | See Bit Error Rate. |
| **Bidirectional** | In Fibre Channel, the capability to simultaneously communicate at maximum speeds (100 Mbps) in both directions over a link. |
| **Bit Error Rate** | Ratio of received bits that contain errors to total of all bits transmitted. |
| **Blocked Port** | Devices communicating with a blocked port are prevented from logging in to a Connectrix switch or communicating with other devices attached to the Connectrix switch. A blocked port continuously transmits the off-line sequence (OLS). |
| **Bridge** | A device that connects and passes packets between two network segments that use the same communications protocol. |
| **Broadcast** | Send a transmission to all N_Ports on a fabric. |
| **Broadcast Frames** | Data packet, also known as a broadcast packet, whose destination address specifies all computers on a network. See also multicast. |
| **Buffer** | Storage area for data in transit. Buffers compensate for differences in processing speeds between devices. |
| **Buffer-to-Buffer Credit** | The maximum number of frames a port can transmit without receiving a receive ready signal from the receiving device. |
C

Call Home
A product feature that allows the Connectrix service processor to automatically dial out to a support center and report system problems. The support center server accepts calls from the Connectrix service processor, logs reported events, and can notify one or more support center representatives. Telephone numbers and other information are configured through the Windows NT dial-up networking application. The Call Home function can be enabled and disabled through the Element Manager.

Channel
Point-to-point link that transports data from one point to the other.

Class 2 Fibre Channel Service
In Class 2 service, the fabric and destination N_Ports provide connectionless service with notification of delivery or nondelivery between the two N_Ports.

Class 3 Fibre Channel Service
Class 3 service provides a connectionless service without notification of delivery between N_Ports. (This is also known as datagram service.) The transmission and routing of Class 3 frames is the same as for Class 2 frames.

Community
A relationship between an SNMP agent and a set of SNMP managers that defines authentication, access control, and proxy characteristics.

Community Name
A name that represents an SNMP community that the agent software recognizes as a valid source for SNMP requests. An SNMP management program that sends an SNMP request to an agent program must identify the request with a community name that the agent recognizes or the agent discards the message as an authentication failure. The agent counts these failures and reports the count to the manager program upon request, or sends an authentication failure trap message to the manager program.

Community Profile
Information that specifies which management objects are available to what management domain or SNMP community name.

Connectionless
Nondedicated link. Typically used to describe a link between nodes that allows the switch to forward Class 2 or Class 3 frames as resources (ports) allow. Contrast with the dedicated bandwidth that is required in a Class 1 Fibre Channel Service point-to-point link.
<table>
<thead>
<tr>
<th><strong>Connectivity Unit</strong></th>
<th>A hardware component that contains hardware (and possibly software) that provides Fibre Channel connectivity across a fabric. Connectrix switches are example of a Connectivity Unit.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Connectrix Management Software</strong></td>
<td>The software application that implements the management user interface for all managed products. The Connectrix Management software can run either locally on the Connectrix service processor or remotely on a user workstation.</td>
</tr>
<tr>
<td><strong>Connectrix Service Processor</strong></td>
<td>A PC shipped with a product for the sole purpose of running the Connectrix Management software.</td>
</tr>
<tr>
<td><strong>Credit</strong></td>
<td>A numeric value that determines the flow control value for a switch handling Class 2 traffic in a fabric.</td>
</tr>
<tr>
<td><strong>CTP</strong></td>
<td>Control Processor, a circuit card or subsystem that contains the microprocessor director. The CTP also initializes hardware components of the system after power-on. A 10/100 Mbps RJ-45 twisted pair connector is located on the CTP to connect to the Ethernet LAN and communicate with the Connectrix service processor or SNMP management station.</td>
</tr>
<tr>
<td><strong>D</strong></td>
<td><strong>DASD</strong> Direct Access Storage Device.</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>Pertaining to an attribute, value, or option that is assumed when none is explicitly specified.</td>
</tr>
<tr>
<td><strong>Default zone</strong></td>
<td>Contains all attached devices that are not members of any active zone.</td>
</tr>
<tr>
<td><strong>Device</strong></td>
<td>(1) A piece of equipment, such as a server or storage device, that is attached to a Connectrix switch or a similar product. A device as defined here is not controlled by the Connectrix Element Manager and its operating parameters. (2) In EMC Symmetrix, a uniquely addressable physical or logical part of the Symmetrix subsystem, such as a disk. (This description is presented here only to clarify a term used in other EMC documents.)</td>
</tr>
<tr>
<td><strong>Dialog Box</strong></td>
<td>A pop-up window containing informational messages or fields to be modified with desired options. This term is often used interchangeably with <em>window</em>.</td>
</tr>
<tr>
<td><strong>Glossary</strong></td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>DID</strong></td>
<td>Destination ID, the address identifier that indicates the targeted destination of the transmitted frame.</td>
</tr>
<tr>
<td><strong>Director</strong></td>
<td>(1) An Enterprise-Class Fibre Channel switch. The Connectrix ED-64M Director is a fully redundant Fibre Channel switch, containing: dual power supplies, fan modules, CTP cards, SBRs, and multiple FPMs, all hot-swappable. (2) A board-level module in the Symmetrix that provides the interface between host channels (via an associated adapter module in the Symmetrix) and Symmetrix disk devices. (This description is presented here only to clarify a term used in other EMC documents.)</td>
</tr>
<tr>
<td><strong>DNS</strong></td>
<td>See Domain Name Service Name.</td>
</tr>
<tr>
<td><strong>Domain ID</strong></td>
<td>A number (1 to 31) that uniquely identifies a switch in a fabric. A distinct Domain ID is allocated to each switch in the fabric by the principal switch.</td>
</tr>
<tr>
<td><strong>Domain Name Service Name</strong></td>
<td>Host or node name for a system that is translated to an IP address through a Name Server. All DNS names have a host name component and, if fully qualified, a domain component, such as <code>host1.abcd.com</code>. In this example, <code>host1</code> is the host name.</td>
</tr>
<tr>
<td><strong>DWDM</strong></td>
<td>Dense Wavelength Division Multiplexing, a process in which different channels of data are carried at different wavelengths over one pair of fiber optic links. This is in contrast with a conventional fiber optic system in which only one channel is carried over a single wavelength traveling through a single fiber.</td>
</tr>
<tr>
<td><strong>E</strong></td>
<td></td>
</tr>
<tr>
<td><strong>E_D_TOV</strong></td>
<td>See Error Detect Time Out Value.</td>
</tr>
<tr>
<td><strong>E_Port</strong></td>
<td>Expansion Port, a physical interface within the Fibre Channel switch that attaches to another E_Port on a Fibre Channel switch through an interswitch link.</td>
</tr>
<tr>
<td><strong>Embedded Web Server</strong></td>
<td>A management interface embedded on the switch’s code that offers features similar to (but not as robust as) the Connectrix Manager and Element Manager.</td>
</tr>
<tr>
<td><strong>Error Detect Time Out Value</strong></td>
<td>Defines the time the switch waits for an expected response before declaring an error condition. The error detect time-out value</td>
</tr>
</tbody>
</table>
(E_D_TOV) can be set within a range of two-tenths of a second to one second using the Connectrix switch Element Manager.

**Error Message**
An indication that an error has been detected. *See also* Information Message and Warning Message.

**ESD**
Electrostatic discharge.

**Ethernet**
A baseband LAN that allows multiple station access to the transmission medium at will without prior coordination and which avoids or resolves contention.

**Event Log**
A record of significant events that have occurred on a Connectrix switch, such as FRU failures, degraded operation, and port problems.

**Expansion Port**
A physical interface that attaches to another E_Port on a Fibre Channel switch through an interswitch link to form a multiswitch fabric.

**Explicit Fabric Login**
F_Ports support a data field size that is agreed upon during fabric login.

**F**

**FA**
Fibre Adapter, another name for a Symmetrix Fibre Channel director.

**Fabric**
One or more switching devices that interconnect Fibre Channel N_Ports, and route Fibre Channel frames based on destination IDs in the frame headers.

**Fabric Element**
Any active switch or director in the fabric.

**Fabric Login**
Process used by N_Ports to establish their operating parameters including the presence or absence of a fabric, paths to other N_Ports, and specific operating characteristics for each port.

**Fabric Port**
Physical interface within the fabric, which attaches to an N_Port through a point-to-point full duplex link connection.

**Fabric Tree**
A hierarchical list in the Connectrix Manager of all fabrics currently known to the Connectrix service processor. The tree includes all members of the fabrics, listed by WWN or nickname.
### Glossary

**Failover**  
The process of detecting a failure on an active Connectrix switch FRU and the automatic transition of functions to a backup FRU.

**Fan-in/Fan-out**  
Terms used to describe the server:storage ratio, where a graphic representation of a 1:n (fan-in) or n:1 (fan-out) logical topology looks like a hand-held fan, with the wide end toward n.

A fan-in or fan-out rate is often referred to as just the n part of the ratio; for example, a 1:6 fan-in is also called a fan-in rate of 6.

<table>
<thead>
<tr>
<th>Server</th>
<th>Switch</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan-In</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Server</th>
<th>Switch</th>
<th>Storage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fan-Out</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**FCP**  
A standard Fibre Channel protocol used to run SCSI over Fibre Channel.

**FC-SW**  
The Fibre Channel Fabric standard.

**Fibre**  
A general term used to cover all physical media types supported by the Fibre Channel specification, such as optical fiber, twisted pair, and coaxial cable.

**Fiber optics**  
The branch of optical technology concerned with the transmission of radiant power through fibers made of transparent materials such as glass, fused silica, and plastic.

Either a single discrete fiber or a nonspatially aligned fiber bundle can be used for each information channel. Such fibers are often called optical fibers to differentiate them from fibers used in non-communication applications.

**Fibre Channel**  
The general name of an integrated set of ANSI standards that define new protocols for flexible information transfer. Logically, Fibre Channel is a high-performance serial data channel.

**Firmware**  
The program code (embedded software) that resides and executes on a connectivity device, such as a Connectrix switch, a Symmetrix Fibre Channel director, or a host bus adapter (HBA).
Flash Memory  A computer chip with a read-only memory that retains its data when the power is turned off, and that can be erased and reprogrammed without being removed from the circuit board.

F_Port  Fabric Port, a physical interface within the fabric. An F_Port attaches to an N_Port through a point-to-point full-duplex link connection.

Frame  The smallest indivisible packet of data that is sent on a link.

Frame Header  Control information placed before data when encapsulating data for network transmission.

FRU  Field-Replaceable Unit, a hardware component that can be replaced as an entire unit. The Connectrix switch Element Manager can display status for the FRUs installed in the unit.

G  Gateway Address  In TCP/IP, a device that connects two systems that use the same or different protocols.

G_Port  A physical interface within the fabric capable of acting either as an F_Port or an E_Port (extension port) depending on the port type at the other end of the link.

GUI  Graphical user interface.

H  Hardware Log  A record of FRU insertions and removals in a Connectrix switch.

HBA  See Host Bus Adapter.

Hexadecimal  Pertaining to a numbering system with base of 16; valid numbers use the digits 0 through 9 and characters A through F (which represent the numbers 10 through 15).

High Availability  A performance feature characterized by hardware component redundancy and hot-swappability (enabling non-disruptive maintenance). High-availability systems maximize system uptime while providing superior reliability, availability, and serviceability.
**Glossary**

**Hop**
Data movement from one node to the next.

**Host Bus Adapter**
A bus card in a host system that allows the host system to connect to a fabric.

**I/O**
See Input/Output.

**IML**
Initial Machine Load, initiated through the IML button on a Connectrix switch. An IML issues a hardware reset for all installed CTP subsystems on the switch, but does not affect other hardware.

**In-Band Management**
Transmission of monitoring/control functions over the Fibre Channel interface.

**Information Message**
A message telling a user that a function is performing normally or has completed normally. User acknowledgement might or might not be required, depending on the message. See also Error Message and Warning Message.

**Input/Output**
(1) Pertaining to a device whose parts can perform an input process and an output process at the same time. (2) Pertaining to a functional unit or channel involved in an input process, output process, or both (concurrently or not), and to the data involved in such a process. (3) Pertaining to input, output, or both.

**Interface**
(1) A shared boundary between two functional units, defined by functional characteristics, signal characteristics, or other characteristics as appropriate. The concept includes the specification of the connection of two devices having different functions. (2) Hardware, software, or both, that links systems, programs, or devices.

**Internet Protocol**
See IP.

**Interoperability**
The ability to communicate, execute programs, or transfer data between various functional units over a network.

**Interswitch Link**
See ISL.
**IP** Internet Protocol, the TCP/IP standard protocol that defines the datagram as the unit of information passed across an internet and provides the basis for connectionless, best-effort packet delivery service. IP includes the ICMP control and error message protocol as an integral part.

**IP Address** A unique string of numbers that identifies a device on a network. The address consists of four groups (quadrants) of numbers delimited by periods. (This is called *dotted-decimal* notation.) All resources on the network must have an IP address. A valid IP address is in the form `nnn.nnn.nnn.nnn`, where each `nnn` is a decimal in the range 0 to 255.

**IPL** Initial Program Load, initiated through a menu option in a Connectrix switch Element Manager. This performs the same function as an IML, but resets the active CTP only. It does not affect the backup CTP subsystem if it is installed.

**ISL** A physical E_Port connection between two switches in a fabric.

**Laser** A device that produces optical radiation using a population inversion to provide light amplification by stimulated emission of radiation and (generally) an optical resonant cavity to provide positive feedback. Laser radiation can be highly coherent temporally, spatially, or both.

**LED** Light-emitting diode.

**Link** The physical connection between two devices on a switched fabric.

**Link Incident** A problem detected on a fiber optic link; for example, loss of light, or invalid sequences.

**Load Balancing** The ability to distribute traffic over all network ports that are the same distance from the destination address by assigning different paths to different messages. Increases effective network bandwidth.

**Loopback Plug** In a fiber optic environment, a type of duplex connector used to wrap the optical output signal of a device directly to the optical input.

**Loopback Test** Test that checks attachment or control unit circuitry, without checking the mechanism itself, by returning the output of the mechanism as input.
Glossary

**LUN**
Logical Unit Number; a number, assigned to a storage device, that (in combination with the storage device node port’s WWN) represents a unique identifier for a logical device on a storage area network.

**M**

**MAC Address**
Media Access Control address, the hardware address of a device connected to a shared network.

**Maintenance Port**
RS-232 connector on a Connectrix switch where a PC running an ASCII terminal emulator can be attached or dial-up connection made for specialized maintenance support.

**Managed Product**
A hardware product that can be managed using the Connectrix Element Manager. For example, a Connectrix switch is a managed product.

**Management Session**
Exists when a user logs on to the Connectrix Management software and successfully connects to the product server. The user must specify the network address of the product server at logon time.

**Media Access Control**
See MAC Address.

**Megabyte (MB)**
A unit of measure for storage size, loosely one million bytes. One megabyte actually equals 1,048,576 bytes.

**MIB**
Management Information Base, a related set of objects (variables) containing information about a managed device and accessed via SNMP from a network management station.

**Multicast**
Multicast is used when multiple copies of data are to be sent to designated, multiple, destinations.

**Multiswitch Fabric**
Fibre Channel fabric created by linking more than one switch or director together to allow communication. See also ISL.

**Multiswitch Linking**
Port-to-port connections between two switches.
N

**Name Server**
The program facility that allows the N_Ports to register and discover Fibre Channel attributes.

**Network Address**
A name or address that identifies a managed product, such as a Connectrix switch, or a Connectrix service processor on a TCP/IP network. The network address can be either an IP address in dotted decimal notation, or a Domain Name Service (DNS) name as administered on a customer network. All DNS names have a host name component and (if fully qualified) a domain component, such as `host1.emc.com`. In this example, `host1` is the host name and `EMC.com` is the domain component.

**Nickname**
A name representing one or more port numbers or World Wide Names.

**Node**
The point at which one or more functional units connect to the network.

**N_Port**
Node Port, a physical interface within an end device (node) which can attach to an F_Port or directly to another N_Port through a point-to-point link connection.

**NVRAM**
Nonvolatile random access memory.

O

**Offline Sequence**
A sequence sent by the transmitting port to indicate that it has detected a problem while attempting to initialize a link.

**OLS**
See Offline Sequence.

**Operating System**
Software that controls the execution of programs and that may provide such services as resource allocation, scheduling, input/output control, and data management. Although operating systems are predominantly software, partial hardware implementations are possible.

**Optical Cable**
A fiber, multiple fibers, or a fiber bundle in a structure built to meet optical, mechanical, and environmental specifications.

**OS**
See Operating System.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out-of-Band Management</td>
<td>Transmission of monitoring/control functions outside of the Fibre Channel interface.</td>
</tr>
<tr>
<td>Panel</td>
<td>A subdivision of a window in a GUI used to group related information within the window. Typically, a heading and/or frame marks the panel as an individual entity of the window. As with a window, data within the panel is usually confined to that panel. Size and shape of the panel and its data is dependent upon the purpose of the panel, and may or may not be modified by user changes to the window size and shape.</td>
</tr>
<tr>
<td>Parameter</td>
<td>(1) A characteristic element whose value is a variable that is given a constant value for a specified application. (2) An item in a menu for which the user specifies a value or for which the system provides a value when the menu is interpreted. (3) Data passed between programs or procedures.</td>
</tr>
<tr>
<td>Password</td>
<td>(1) A value used in authentication or a value used to establish membership in a group having specific privileges. (2) A unique string of characters known to the computer system and to a user who must specify it to gain full or limited access to a system and to the information stored within it.</td>
</tr>
<tr>
<td>Path</td>
<td>In a network, any route between any two nodes.</td>
</tr>
<tr>
<td>Persisted Fabric</td>
<td>A fabric whose topology has been recorded at a particular moment, for the purpose of tracking major changes.</td>
</tr>
<tr>
<td>Persistent Binding</td>
<td>Server-level access control uses configuration information to bind a server device name to a specific Fibre Channel storage volume or logical unit number, through a specific HBA and storage port WWN.</td>
</tr>
<tr>
<td>Port</td>
<td>(1) An access point for data entry or exit. (2) A receptacle on a device to which a cable for another device is attached.</td>
</tr>
<tr>
<td>Port Card</td>
<td>Field replaceable hardware component that provides the connection for fiber cables and performs specific device-dependent logic functions.</td>
</tr>
<tr>
<td>Port Name</td>
<td>A symbolic name that the user defines for a particular port through the Element Manager.</td>
</tr>
<tr>
<td><strong>POST</strong></td>
<td>Power-On Self Test, a series of self-tests executed each time the unit is booted or reset.</td>
</tr>
<tr>
<td><strong>Preferred Domain ID</strong></td>
<td>Domain ID that a switch is assigned by the principal switch in a switched fabric. The preferred domain ID becomes the active domain ID except when configured otherwise by the user.</td>
</tr>
<tr>
<td><strong>Principal Switch</strong></td>
<td>In a multiswitch fabric, the switch that allocates domain IDs to itself and to all other switches in the fabric. There is always one principal switch in a fabric. If a switch is not connected to any other switches, it acts as its own principal switch.</td>
</tr>
<tr>
<td><strong>Product</strong></td>
<td>(1) Connectivity Product, a generic name for a switch, director, or any other Fibre Channel product. (2) Managed Product, a generic hardware product that can be managed by the Element Manager (a Connectrix switch is a managed product). Note distinction from the definition for Device.</td>
</tr>
<tr>
<td><strong>Element Manager</strong></td>
<td>A software component of the Connectrix Management software, such as a Connectrix switch Element Manager, that implements the management user interface for a specific product. When a Product instance is opened from the Connectrix Management software Products view, the corresponding Element Manager is invoked.</td>
</tr>
<tr>
<td><strong>Product Name</strong></td>
<td>A user configurable identifier assigned to a Managed Product. Typically, this name is stored on the product itself. For a Connectrix switch, the Product Name can also be accessed by an SNMP Manager as the System Name. The Product Name should align with the host name component of a Network Address.</td>
</tr>
<tr>
<td><strong>Products view</strong></td>
<td>The top-level display in the Connectrix Management software user interface that displays icons of Managed Products.</td>
</tr>
<tr>
<td><strong>Protocol</strong></td>
<td>(1) A set of semantic and syntactic rules that determines the behavior of functional units in achieving communication. (2) A specification for the format and relative timing of information exchanged between communicating parties.</td>
</tr>
</tbody>
</table>
Glossary

R

**R_A_TOV**  
See Resource Allocation Time Out Value.

**Resource Allocation Time Out Value**  
Is used to time out operations that depend on the maximum possible time that a frame could be delayed in a fabric and still be delivered. The resource allocation time out value of (R_A_TOV) can be set within a range of two-tenths of a second to 120 seconds using the Connectrix switch Element Manager.

**Remote Access Link**  
The ability to communicate with a data processing facility through a remote data link.

**Remote Notification**  
The system can be programmed to notify remote sites of certain classes of events.

**Remote User Workstation**  
A workstation, such as a PC, using Connectrix Management software and Element Manager software that can access the Connectrix service processor over a LAN connection. A user at a remote workstation can perform all of the management and monitoring tasks available to a local user on the Connectrix service processor.

S

**SAN**  
See Storage Area Network.

**Segmented E_Port**  
E_Port that has ceased to function as an E_Port within a multiswitch fabric due to an incompatibility between the fabrics that it joins.

**SEL**  
System error light.

**Service Processor**  
See Connectrix Service Processor.

**Session**  
See Management Session.

**SFP**  
Small form-factor pluggable, a type of shortwave or longwave optic transceiver.

**SMTP**  
Simple Mail Transfer Protocol, a TCP/IP protocol that allows users to create, send, and receive text messages. SMTP protocols specify how messages are passed across a link from one system to another. They do not specify how the mail application accepts, presents or stores the mail.
### SNMP
Simple Network Management Protocol, a TCP/IP protocol that generally uses the User Datagram Protocol (UDP) to exchange messages between a management information base (MIB) and a management client residing on a network.

### Storage Area Network
A network linking servers or workstations to disk arrays, tape backup systems and other devices, typically over Fibre Channel.

### Subnet Mask
Used by a computer to determine whether another computer with which it needs to communicate is located on a local or remote network. The network mask depends upon the class of networks to which the computer is connecting. The mask indicates which digits to look at in a longer network address and allows the router to avoid handling the entire address. Subnet masking allows routers to move the packets more quickly. Typically, a subnet may represent all the machines at one geographic location, in one building, or on the same local area network.

### Switch Priority
Value configured into each switch in a fabric that determines its relative likelihood of becoming the fabric’s principal switch.

### TCP/IP

### Topology
Logical and/or physical arrangement of stations on a network.

### Trap
An asynchronous (unsolicited) notification of an event originating on an SNMP-managed device and directed to a centralized SNMP Network Management Station.

### Toggle
To change the state of a feature/function that has only two states. For example, if a feature/function is enabled, toggling changes the state to disabled.
Glossary

**U**

**ULP**  Upper Layer Protocol, the protocol user of FC-4, including IPI, SCSI, IP, and SBCCS.

**Unblocked Port**  Devices communicating with an unblocked port can log in to a Connectrix switch or a similar product and communicate with devices attached to any other unblocked port if the devices are in the same zone.

**Unicast**  Unicast routing provides one or more optimal path(s) between any of two switches that make up the fabric. (This is used to send a single copy of the data to designated destinations.)

**URL**  Uniform Resource Locater, the addressing system used by the World Wide Web. It describes the location of a file or server anywhere on the Internet.

**W**

**Warning Message**  An indication that a possible error has been detected. See also Error Message and Information Message.

**World Wide Name**  A unique identifier, even on global networks. The WWN is a 64-bit number (XX:XX:XX:XX:XX:XX:XX:XX).

**WWN**  See World Wide Name.

**Z**

**zone**  A set of devices that can access one another. All connected devices may be configured into one or more zones. Devices in the same zone can “see” each other, while different zones cannot.

**Zoning**  Zoning allows an administrator to group several devices by function or by location. All devices connected to a connectivity product, such as a Connectrix switch, may be configured into one or more zones.

**zone set**  A set of zones.
A
access
assigning 4-7
changing 4-9
removing 4-9
access levels
defined 6-2
user groups 6-2
activating
zone sets 12-10
activating discovery 5-4
active sessions, viewing 4-12
adding
IP addresses 5-5
servers 4-4
trap recipients 8-4, 9-46
users 4-7
zone members 12-7
zones 12-9
adding users to groups 7-2
admin access, assigning 4-7, 4-9
administrator access, defined 6-2
alerts, clearing ISL alerts 9-42
assigning users to groups 7-2
attention, products needing 9-4
audit log
copying from 10-5
overview 10-2

B
browse access, assigning 4-7, 4-9

call home notification, configuring 10-8
call home status, determining 3-8
call-home event notification
configuring in Connectrix Manager 8.x G-2
enabling in Connectrix Manager 7.x D-12
changing
fabric properties 9-21
IP addresses 5-6
nicknames of fabrics 9-21
product properties 9-3
product types 9-3
TCP/IP ports 8-6
user accounts 4-9
users 4-9
zone names 11-2
zone set names 11-2, 11-3
clearing ISL alerts 9-42
clients
number of 3-8
Comments xxiv
community strings
configuring 5-7
reverting to default 5-9
comparing zone sets 11-9
compatibility, with applications 8-6
configuring
community strings 5-7
event notification
call home 10-8
e-mail 10-7
trap forwarding 9-45
connections
Index

monitoring utilization 13-2
  on persisted fabrics 9-42
  status, determining 3-7
Connectrix management overview 1-2
Connectrix Manager
  starting 2-7
Connectrix Manager 7.x
  comparing to version 8.x D-2
  exiting D-5
  logging in D-4
  logging out D-5
Connectrix Manager 8.x
  comparing to version 7.x D-2
  downloading from Web A-5
Connectrix Manager application
  starting 2-7
Connectrix Manager views, compared
  Connectrix Manager 7.x D-6
  Connectrix Manager 8.x D-9
Connectrix service processor
  described 1-5
  copying from logs 10-5
  copying, zone sets 11-5
  creating
    zone members 12-6
    zone sets 12-8
    zones 12-5
  creating user groups 6-3
  creating, user accounts 4-7

D
data
  exporting 4-16, 13-4
  importing 4-16
data migrated on upgrade B-52
data not migrated on upgrade B-55
deactivating discovery 5-4
deactivating zone sets 12-12
default community strings 5-9
default zones
  disabling 12-12
  enabling 12-12
degraded icon 2-38
delay, setting for zoning 11-10
deleting
  reports 10-11
  users 4-9
  zone sets 11-6
  zones 11-5
deleting users from groups 7-3
determining users 4-7
devices, finding in persisted fabrics 9-44
disabling default zones 12-12
discovery
  issues F-2
  out-of-band 5-2
  overview 5-2
  turning on and off 5-4, 5-10
disk, exporting to 4-16
duplicating, zone sets 11-5

eediting trap recipients 8-5
eediting user groups 6-6
eediting zone names 11-2
e-mail event notification, configuring
  in Connectrix Manager 7.x D-13
  e-mail notification, configuring 10-7
  e-mail, exporting to 4-16
  enabling default zones 12-12
  enterprise fabric mode
    configuring 9-27
    overview 9-26
Ethernet events, configuring
  in Connectrix Manager 7.x D-14
  ethernet events, enabling 10-9
  event log
    copying from 10-5
    overview 3-4, 10-2
  event notification
    configuring 10-9
    call home 10-8
    email 10-7
    overview 10-7
  events
    copying 10-5
    exporting 10-4
    filtering 4-10, 10-5
    icons 2-39
    monitoring 10-2
    viewing 10-3
  exporting
a zone set 12-14
events 10-4
files 4-16
overview 4-16
performance data 13-4

F
fabric binding
  adding switches 9-29
  overview 9-28
  procedure 9-28
fabrics
  changing nicknames for 9-21
  changing properties 9-21
  determining status 3-8
  determining status of 9-21
  persisted, determining status 9-41
  persisting 9-40
  unpersisting 9-40
  unpersisting product 9-41
  viewing 10-4
fabrics, managing and monitoring
  in Connectrix Manager 7.x D-39
  in Connectrix Manager 8.x. See discovery and zoning
failed icon 2-38
feature keys
  enabling in Connectrix Manager 7.x D-24
features, finding on Connectrix Manager screens D-43
FICON management server
  enabling D-30
  parameters D-30
files
  exporting 4-16
  importing 4-16, 4-19
files, exporting 13-4
filtering events
  in master log 10-5
  per user 4-10
finding
  members in zone 11-7
  products 9-2
  topics in help 2-37
  zones in zone set 11-7
finding users 7-4
flyovers, turning on and off 4-15
frame sniffer
  events in log 9-47
G
generating reports 10-10
ghost icon, in persisted fabrics 9-42, 9-43, 9-44
ghost products, finding corresponding real products 9-44
groups
  assigning users 7-2
  creating for users 6-3
  determining 7-4
  editing for users 6-6
  finding users in 7-4
  removing users 7-3
H
hide routes, overview 9-7
I
icons
  persisted fabric 9-41, 9-42, 9-43, 9-44
  persisted fabrics 9-41
importing 4-16, 4-19
importing a zone set 12-15
information bar 3-7
installing
  license key 2-15
IP addresses
  adding 5-5
  changing 5-6
  removing 5-7
ISLs, clearing alerts 9-42
K
keyboard shortcuts 2-39
L
launching Connectrix Manager application 2-7
layout, changing in persisted fabrics 9-43
license key
  installing 2-15
  retrieving 2-15
Index

license, See license key
listing zone members 11-8
log entries, copying 10-5
log file, location 3-4
logging in 4-2
logging in to Connectrix Manager
in version 7.x D-4
logging out 4-3
logs
  comparing Connectrix 7.X and 8.01 D-25
  exporting 10-4
  overview 3-4, 10-2
  viewing 10-3, 10-4

M
management server configuration, comparing
  Connectrix Manager versions D-29
management server, FICON, enabling D-30
management sessions, remote
  configuring in Connectrix Manager 7.x D-21
managing reports 10-10
master log
  copying from 10-5
  filtering 10-5
  icons 2-39
  illustrated 3-4
  location 3-4
  overview 3-4
members, finding in zones 11-7
merging, persisted fabrics 9-43
MIB information, downloading C-2
minimap
  attaching 3-5
  detaching 3-5
  overview 3-5
  resizing 3-6
minus icon, persisted fabrics 9-42
monitoring
  connection utilization 13-2
  port performance 13-6
  switch performance 13-3
  monitoring events 10-2

N
naming conventions 11-12
new features, ordering 2-16
nickname, switch, configuring
  in Connectrix Manager 7.x D-15
nicknames, importing and exporting
  in Connectrix Manager 7.x D-17
notifications
  configuring call home 10-8
  configuring e-mail 10-7
  overview 10-7

O
offline icon 2-38
online help, searching 2-37
opening
  Connectrix Manager 2-7
operational icon 2-38
ordering upgrades 2-16
out-of-band discovery
  overview 5-2

P
pasting events from logs 10-5
performance data
  storing 13-4
performance thresholds, setting 13-6, 13-7
persisted fabrics
  clearing alerts 9-42
  connection status, determining 9-42
  determining status 9-41
  finding devices in 9-44
  ghost icon 9-42, 9-43, 9-44
  icon 9-41, 9-42, 9-43, 9-44
  icons 9-41
  layout changes 9-43
  merging 9-43
  minus icon 9-42
  plus icon 9-42
  principal switches in 9-43
  splitting 9-43
persisting fabrics 9-40
physical map
  exporting 4-16
  zooming in 4-14
  zooming out 4-14
plus icon, persisted fabrics 9-42
polling client H-2
  configure for faster logins H-2
ports, monitoring performance 13-6
preferred path D-33
principal switches, in persisted fabrics 9-43
product list
  exporting 4-16
  overview 3-3
  viewing 3-3
Product Manager (Connectrix Manager 7.x),
  compared to Element Manager (8.x) D-26
product state log
  copying from 10-5
  overview 10-2
product status icons 2-38
product status, determining 9-4
products
  changing properties 9-3
  changing types 9-3
  determining problems 9-4
  determining status 9-4
  finding 9-2
  finding in persisted fabrics 9-44
  searching for 9-2
  status icons 2-38
  status, determining 3-8
  unpersisting 9-41
properties
  switch, displaying
    in Connectrix Manager 7.x D-37
  viewing for zone sets 11-6
  viewing for zones 11-6
properties, device route 9-7

R
remote client upgrades B-50
removing
  IP addresses 5-7
  members from zone 12-9
  trap recipients 8-5, 9-47
  users 4-9
  zone sets 11-6
  zones 12-10
removing user groups 6-8
removing users from groups 7-3
renaming
  zone sets 11-2, 11-3
  zones 11-2
reports
  deleting 10-11
  generating 10-10
  overview 10-10
  viewing 10-11
requirements, system 2-2
retrieving license key 2-15
routers, blocked broadcast request F-3
routes
  hiding 9-7
  showing 9-5
  viewing 9-7
running, Connectrix Manager 2-7

S
SAN files
  exporting 4-16
  importing 4-19
saving, performance data 13-4
searching
  for members in zone 11-7
  for products 9-2
  for zones in zone sets 11-7
online help 2-37
server name, determining 3-8
servers
  adding 4-4
  determining name 3-8
  determining status 3-7
  logging in 4-2
  logging out 4-3
  sessions 4-12
service processor. See Connectrix service processor
service, requesting 9-4
session log
  copying from 10-5
  overview 10-2
sessions
  viewing 4-12
sessions, remote
  configuring in Connectrix Manager 7.x D-21
  displaying in Connectrix Manager 7x D-22
setting performance thresholds 13-6, 13-7
shortcuts 2-39
Index

show routes
   overview 9-5
   procedure 9-5
   requirements 9-5, 9-30
showing levels of detail, physical map 4-15
sniffer
   events in log 9-47
SNMP agent
   configuring in Connectrix Manager 7.x D-19
   snmp agent
      configuring 8-2
      overview 8-2
      turning off 8-3
      turning on 8-3
SNMP trap events, changing TCP/IP ports 8-6
splitting persisted fabrics 9-43
starting
   Connectrix Manager 2-7
   starting Connectrix Manager 2-7
status bar 3-7
status, determining for fabric 9-21
storing, performance data 13-4
switch, adding to Connectrix Manager views
   in Connectrix Manager 7.x D-11
switch, monitoring performance 13-3
symapi.jar, class path issues F-3
system requirements 2-2

T
TCP/IP ports, changing 8-6
toolbar, description 3-6
toolbox, description 3-7
topology, See physical map
trap forwarding, configuring 9-45
trap recipients
   adding 8-4, 9-46
   configuring 8-2
   editing 8-5
   overview 8-2
   removing 8-5, 9-47
traps, types of C-45
troubleshooting
   .license setup F-6
   address issues F-4
discovery issues F-2
   import issue F-5
   installation issue F-6
   managing Cisco switches F-6
   mapping loop to hub F-6
   product issues F-4
   server startup issue F-5
   server-client communication issue F-5
   serverinit.txt setup F-6
   Windows service issue F-5
turning off discovery 5-10
turning on discovery 5-10

U
uninstalling Connectrix Manager A-8
unknown icon 2-38
unpersisting fabrics 9-40
unpersisting products 9-41
upgrade procedure
   remote clients B-50
upgrading
   Connectrix Manager application 2-16
   upgrading Connectrix Manager
      cautions B-3
      data migrated B-52
      data not migrated B-55
      post upgrade tasks B-56
      prerequisites B-2
user access level, determining 3-8
user group
   access levels 6-2
user groups
   creating 6-3
   editing 6-6
   removing 6-8
user list, viewing 4-7
users
   access levels 6-2
   adding 4-7
   assigning to groups 7-2
   changing 4-9
determining permissions 7-4
filtering events for 4-10
finding in groups 7-4
groups 6-2
removing 4-9
removing from groups 7-3
viewing all 4-7
users, Connectrix Manager
    administering in Connectrix Manager 7.x
    D-35

V
    viewing
        active sessions 4-12
        events 10-3
        fabric events 10-4
        product list 3-3
        reports 10-11
        routes 9-7
        users 4-7
        zooming in 4-14
        zooming out 4-14

W
    workstation, installing Connectrix Manager onto
    A-1

Z
    zone members
        adding to zones 12-7
        creating 12-6
        listing 11-8
        removing from zones 12-9
    zone sets
        activating 12-10
        adding zones 12-9
        comparing 11-9
        creating 12-8
        deactivating 12-12
        deleting 11-6
        duplicating 11-5
        exporting 12-14
        importing 12-15
        naming conventions 11-12
        properties, viewing 11-6
        removing zone 12-10
        renaming 11-2, 11-3
    zones
        adding to zone sets 12-9
        creating 12-5
        deleting 11-5
        finding in zone sets 11-7
        naming conventions 11-12
        properties, viewing 11-6
        removing 12-10
        renaming 11-2
    zoning
        naming conventions 11-12
        steps 12-3
        zoning delay, setting 11-10
        zooming in 4-14
        zooming out 4-14