IBM® System Storage®

Network Advisor SAN User Manual

Supporting IBM Network Advisor version 11.1

READ BEFORE USING

This product contains software that is licensed under written license agreements. Your use of such software is subject to the license agreements under which they are provided.

GA32-0940-00

IBM® Sytem Storage®

Network Advisor SAN User Manual

Supporting IBM Network Advisor version 11.1

GA32-0940-00

The following paragraph does not apply to any country (or region) where such provisions are inconsistent with local law.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states (or regions) do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

GA32-0940-00

Contents

About This Document

Chapter 1 Getting Started

Chapter 5 Application Configuration

Chapter 7 Call Home

Chapter 8 View Management

Chapter 9 Third-party tools

Chapter 10 **Server Management Console**

Chapter 12 **Host Port Mapping**

Chapter 13 **Storage Port Mapping**

Chapter 15 Fibre Channel over Ethernet

Chapter 17 **FC-FC Routing Service Management**

Chapter 18 **Virtual Fabrics**

Chapter 19 **SAN Encryption configuration**

Chapter 21 Fibre Channel over IP

Chapter 22 Fabric Binding

Chapter 23 Port Fencing

Chapter 26 Troubleshooting

Chapter 27 Performance Data

Chapter 28 Frame Monitor

Chapter 29 Policy Monitor

Chapter 30 Fault Management

Appendix A Application menus

Appendix B Call Home Event Tables

Appendix C User Privileges

Appendix D Regular Expressions

Appendix E Database Fields

About This Document

In this chapter

How this document is organized

This document is organized to help you find the information that you want as quickly and easily as possible. This document supports Network Advisor 11.1.0 and later.

The document contains the following components:

- Chapter 1, "Getting Started," provides a high-level overview of the user interface.
- Chapter 2, "Licenses," provides information about the Management application license and upgrading your license.
- Chapter 3, "Patches," provides information about installing patches.
- Chapter 4, "Discovery," describes how to discover SANs.
- Chapter 5, "Application Configuration," provides Management application configuration instructions.
- Chapter 6, "User Account Management," provides information on how to manage users.
- Chapter 7, "Call Home," provides call home configuration instructions.
- Chapter 8, "View Management," provides view and topology configuration instructions.
- Chapter 9, "Third-party tools," provides instructions for adding and launching third-party tools.
- Chapter 10, "Server Management Console," provides information on using the Server Management Console to stop and start the Management application services, backup the Management application database, and capture technical support information.
- Chapter 11, "SAN Device Configuration," provides device configuration instructions.
- Chapter 12, "Host Port Mapping," provides instructions about how to create Hosts and assign the HBAs to them and import an externally created Host port mapping file (.CSV) to the Management application.
- Chapter 13, "Storage Port Mapping," provides instructions about how to create and assign properties to a Storage Device.

- Chapter 14, “Host management,”provides information on how to configure an HBA.
- Chapter 15, “Fibre Channel over Ethernet,”provides information on how to configure an FCoE.
- Chapter 16, “Security Management,” provides security configuration instructions.
- Chapter 17, “FC-FC Routing Service Management,” provides information on how to manage Fibre Channel Routing.
- Chapter 18, “Virtual Fabrics,” provides logical switch configuration instructions.
- Chapter 19, “SAN Encryption configuration,” provides information on encryption.
- Chapter 20, “Zoning,” provides zoning configuration instructions.
- Chapter 21, “Fibre Channel over IP,” provides information on how to configure an FCIP.
- Chapter 22, “Fabric Binding,” provides fabric binding instructions.
- Chapter 23, “Port Fencing,” provides information on how to configure port fencing.
- Chapter 24, “VLAN Management,” provides information on how to manage Virtual Local Area Networks (VLANs).
- Chapter 25, “Deployment Manager,” provides information about how to view, deploy, and manage deployment configurations.
- Chapter 26, “Troubleshooting,” provides troubleshooting details.
- Chapter 27, “Performance Data,” provides information on how to manage performance.
- Chapter 28, “Frame Monitor,”provides information on how to monitor frames.
- Chapter 29, “Policy Monitor,”provides information on how to configure best practice guidelines.
- Chapter 30, “Fault Management,” provides event management instructions.
- Chapter 31, “Technical Support,”provides server, client, and device support save instructions.
- Chapter 32, “Reports,” provides generating report instructions.
- Appendix A, “Application menus,”provides information about the main and shortcut menus.
- Appendix B, “Call Home Event Tables,” provides supplemental information about call home event tables.
- Appendix C, “User Privileges,” provides supplemental information about user privileges and access levels.
- Appendix D, “Regular Expressions,” provides a summary of Unicode regular expression constructs that you can use in the Management application.
- Appendix E, “Database Fields,” provides reference information related to databases.

Supported hardware and software

In those instances in which procedures or parts of procedures documented here apply to some devices but not to others, this guide identifies exactly which devices are supported and which are not.

Although many different software and hardware configurations are tested and supported by Network Advisor 11.1.X, documenting all possible configurations and scenarios is beyond the scope of this document.

Fabric OS software support

The following firmware platforms are supported by this release of Network Advisor 11.1.X:

- Fabric OS 5.0 or later in a pure Fabric OS fabric
- Fabric OS 6.0 or later in a Mixed Fabric

NOTE
For platform specific Fabric OS requirements, refer to the **Firmware level required** column in Table 1.

NOTE
Discovery of a Secure Fabric OS fabric in strict mode is not supported.

- M-EOS and M-EOSn 9.6.X or later in a mixed Fabric OS and M-EOS fabric
- M-EOS and M-EOSn 9.9.2 or later in a pure M-EOS fabric

Fabric OS hardware support

Table 1 provides a list of the hardware platforms supported by this release of Network Advisor 11.1.X as well as any platform specific Fabric OS requirements.

TABLE 1 Supported Hardware

IBM Name	Terminology used in documentation	Firmware level required
SAN16B-2	16-port, 4 Gbps FC Switch	Refer to "Fabric OS software support" on page xxxix.
SAN24B-4	24-port, 8 Gbps FC Switch	Fabric OS v6.1.0 or later
SAN32B-2	32-port, 4 Gbps FC Switch	Refer to "Fabric OS software support" on page xxxix.
SAN64B-2	64-port, 4 Gbps FC Switch	Fabric OS v5.2.0 or later
SAN32B-3	32-port, 4 Gbps FC Interop Switch	Fabric OS v5.2.1 or later
SAN40B-4	40-port, 8 Gbps FC Switch	Fabric OS v6.1.0 or later
SAN80B-4	80-port, 8 Gbps FC Switch	Fabric OS v6.1.0 or later
SAN48B-5	48-port, 16 Gbpsswitch	Fabric OS v7.0.0 or later
SAN18B-R	4 Gbps Router, Extension Switch	Fabric OS v5.1.0 or later
SAN04B–R	4 Gbps Extension Switch	Fabric OS v5.1.0 or later
FR4-18i Extension Blade	4 Gbps Router, Extension Blade	Refer to "Fabric OS software support" on page xxxix.
SAN06B–R	8 Gbps Extension Switch	Fabric OS v6.3.0 or later

TABLE 1 Supported Hardware

IBM Name	Terminology used in documentation	Firmware level required
IBM Converged Switch B32	8 Gbps 8-FC-port, 10 GbE 24-CEE port Switch	Fabric OS v6.1.2_CEE
Brocade 8470 FCoE embedded switch	FCoE Embedded Switch	Fabric OS v6.3.1_CEE
Brocade VA-40FC switch	8 Gbps 40-port Switch	Refer to "Fabric OS software support" on page xxxix.
SAN256B	Director Chassis	Refer to "Fabric OS software support" on page xxxix.
SAN256B with FC4-16, FC4-32, and FC4-48 Blades	Director Chassis with 4 Gbps 16-FC port, 4 Gbps 32-FC port, and 4 Gbps 48-FC port Blades	Fabric OS v5.2.0 or later (FC4-48)
SAN256B with FR4-18i Blade	Director Chassis with 4 Gbps router, Extension Blades	Fabric OS v5.1.0 or later (FR4-18i)
SAN256B with FC4-16IP Blade	Director Chassis with 4 Gbps 8-FC port and 8 GbE iSCSI Blade	Fabric OS v5.2.0 or later (FC$-16IP)
SAN256B with FC10-6 Blade	Director Chassis with 10 Gbps 6-port ISL Blades	Fabric OS v5.3.0 or later (FC10-6)
SAN768B[1]	384-port Backbone Chassis	Fabric OS v6.0.0 or later
SAN768B[1] with FC8-16, FC8-32, and FC8-48 Blades	384-port Backbone Chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port Blades	Fabric OS v6.0.0 or later
SAN768B[1] with FC8-64 Blade	384-port Backbone Chassis with 8 Gbps 64-port Blade	Fabric OS v6.4.0
SAN768B[1] with FR4-18i Blade	384-port Backbone Chassis with 4 Gbps Router, Extension Blades	Fabric OS v6.0.0 or later
SAN768B[1] with FC10-6 Blade	384-port Backbone Chassis with FC 10 - 6 ISL Blade	Fabric OS v6.2.0
SAN768B[1] with FX8-24 Extension Blades	384-port Backbone Chassis with 8 Gbps Extension Blades	Fabric OS v6.3.1_CEE
SAN768B[1] with FCoE10-24 Blades	384-port Backbone Chassis with 8 Gbps 24-port FCoE Blades	Fabric OS v6.3.1_CEE
SAN384B	192-port Backbone Chassis	Fabric OS v6.0.0 or later
SAN384B with FC8-16, FC8-32, and FC8-48 Blades	192-port Backbone Chassis with 8 Gbps 16-FC port, 8 Gbps 32-FC port, and 8 Gbps 48-FC port Blades	Fabric OS v6.2.0
SAN384B with FC8-64 Blade	192-port Backbone Chassis with 8 Gbps 64-port Blade	Fabric OS v6.4.0
SAN384B with FR4-18i Blades	192-port Backbone Chassis with 4 Gbps Router, Extension Blades	Fabric OS v6.2.0
SAN384B with FC10-6 Blades	192-port Backbone Chassis with FC 10 - 6 ISL Blades	Fabric OS v6.2.0
SAN384B with FX8-24 Extension Blades	192-port Backbone Chassis with 8 Gbps 12-FC port, 10 GbE ports, 2-10 GbE ports Extension Blades	Fabric OS v6.3.1_CEE
SAN384B with FCoE10-24 Blades	192-port Backbone Chassis with 8 Gbps 24-port FCoE Blade	Fabric OS v6.3.0 or later

TABLE 1 Supported Hardware

IBM Name	Terminology used in documentation	Firmware level required
SAN384B-2	16 Gbps 192-port Backbone Chassis	Fabric OS v7.0.0 or later
SAN768B-2	16 Gbps 384-port Backbone Chassis	Fabric OS v7.0.0 or later
SAN32B-E4 Encryption Switch	8 Gbps Encryption Switch	Fabric OS v6.1.1_enc or later
FS8-18 Encryption Blade	Encryption Blade	Refer to "Fabric OS software support" on page xxxix.
FC8-16 Blade	FC 8 GB 16-port Blade	Refer to "Fabric OS software support" on page xxxix.
FC8-32 Blade	FC 8 GB 32-port Blade	Refer to "Fabric OS software support" on page xxxix.
FC8-48 Blade	FC 8 GB 48-port Blade	Refer to "Fabric OS software support" on page xxxix.
FC8-64 Blade	FC 8 GB 64-port Blade	Refer to "Fabric OS software support" on page xxxix.
FC10-6 Blade	FC 10 - 6 ISL Blade	Refer to "Fabric OS software support" on page xxxix.
FC16-32 Blade	16 Gbps 32-port blade	Fabric OS v7.0.0 or later
FC16-48 Blade	16 Gbps 48-port blade	Fabric OS v7.0.0 or later
FCoE10-24 Blade	10 Gig FCoE Port Router Blade	Refer to "Fabric OS software support" on page xxxix.
FX8-24 Extension Blade [1]	8 Gbps Extension Blade	Refer to "Fabric OS software support" on page xxxix.
SAN140M Director	140-Port Director	Refer to "Fabric OS software support" on page xxxix.
SAN256M Director	256-Port Director	Refer to "Fabric OS software support" on page xxxix.

[1] Professional Plus Trial and Licensed version can discover, but not manage this device. Use the device's Element Manager, which can be launched from the Connectivity Map, to manage the device. This device cannot be used as a Seed switch.

What's new in this document

This is a new document.

Document conventions

This section describes text formatting conventions and important notice formats used in this document.

Text formatting

The narrative-text formatting conventions that are used are as follows:

bold text	Identifies command names Identifies the names of user-manipulated GUI elements Identifies keywords and operands Identifies text to enter at the GUI or CLI
italic text	Provides emphasis Identifies variables Identifies paths and Internet addresses Identifies document titles
`code text`	Identifies CLI output Identifies command syntax examples

For readability, command names in the narrative portions of this guide are presented in mixed lettercase: for example, switchShow. In actual examples, command lettercase is often all lowercase. Otherwise, this manual specifically notes those cases in which a command is case sensitive.

Notes, cautions, and warnings

The following notices and statements are used in this manual. They are listed below in order of increasing severity of potential hazards.

NOTE
A note provides a tip, guidance or advice, emphasizes important information, or provides a reference to related information.

ATTENTION
An Attention statement indicates potential damage to hardware or data.

Key terms

For definitions of SAN-specific terms, visit the Storage Networking Industry Association online dictionary at:

http://www.snia.org/education/dictionary

Additional information

This section lists additional IBM-specific documentation that you might find helpful.

For more information about IBM SAN products, see the following Web site:
www.ibm.com/servers/storage/san/

For support information for this product and other SAN products, see the following Web site:
www.ibm.com/servers/storage/support/san

Visit *www.ibm.com/contact/* for the contact information for your country or region. You can also contact IBM within the United States at 1-800-IBMSERV (1-800-426-7378). For support outside the United States, you can find the service number at: *www.ibm.com/planetwide/*.

Getting technical help

Contact IBM support for hardware, firmware, and software support, including product repairs and part ordering. To expedite your call, have the following information available:

1. Network Advisor Serial Number
2. General Information
   - Switch model
   - Switch operating system version
   - Error numbers and messages received
   - supportSave command output
   - Detailed description of the problem, including the switch or fabric behavior immediately following the problem, and specific questions
   - Description of any troubleshooting steps already performed and the results
   - Serial console and Telnet session logs
   - syslog message logs
3. Switch Serial Number

   The switch serial number and corresponding bar code are provided on the serial number label, as illustrated below.:

   FT00X0054E9

   FT00X0054E9

   The serial number label is located as follows:

   - SAN16B-2—On the nonport side of the chassis
   - SAN24B-4, SAN32B-2, SAN64B-2, SAN40B-4, SAN80B-4, SAN18B-R, SAN04B–R, SAN06B-R, and IBM Converged Switch B32—On the switch ID pull-out tab located inside the chassis on the port side on the left
   - SAN32B-3—On the switch ID pull-out tab located on the bottom of the port side of the switch

- SAN256B—Inside the chassis next to the power supply bays
- SAN768B—On the bottom right on the port side of the chassis
- SAN384B—On the bottom right on the port side of the chassis, directly above the cable management comb

4. World Wide Name (WWN)

   Use the **wwn** command to display the switch WWN.

   If you cannot use the **wwn** command because the switch is inoperable, you can get the WWN from the same place as the serial number, except for the SAN768B. For the SAN768B, access the numbers on the WWN cards by removing the WWN bezel at the top of the nonport side of the chassis.

How to send your comments

Your feedback is important in helping us provide the most accurate and high-quality information. If you have comments or suggestions for improving this document, send us your comments by e-mail to starpubs@us.ibm.com.

Be sure to include the following:

- Exact publication title (paste into the e-mail subject line)
- Publication form number (for example, GC26-1234-02)
- Page, table, or illustration numbers
- A detailed description of any information that should be changed

Chapter

Getting Started

1

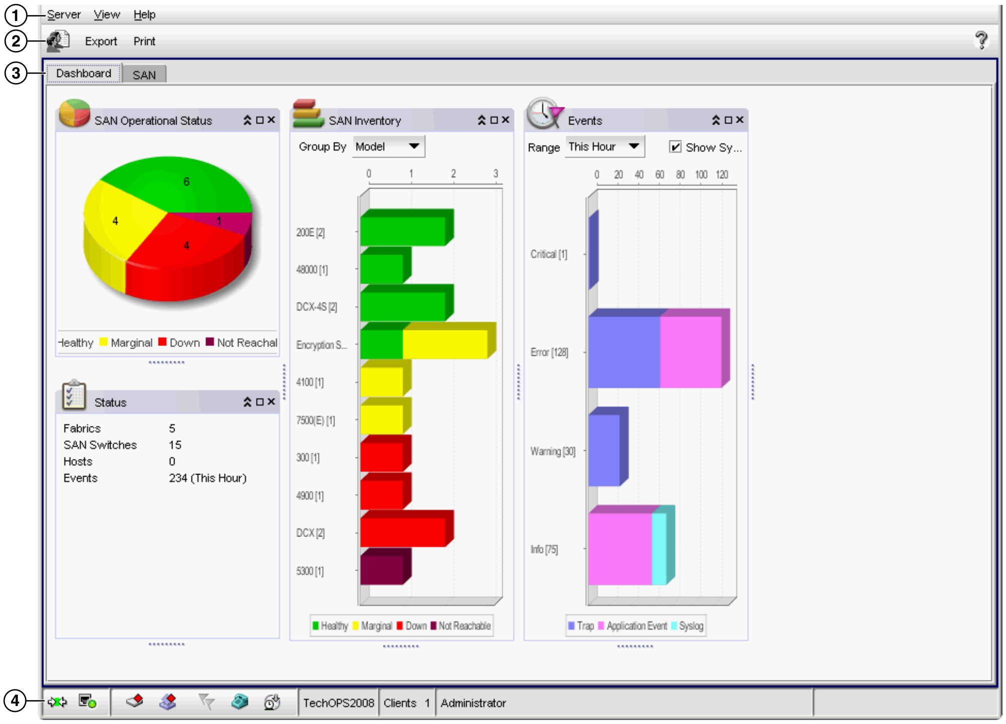
In this chapter

User interface components

The Management application provides easy, centralized management of the network, as well as quick access to all product configuration applications. Using this application, you can configure, manage, and monitor your networks with ease.

The Management application's main window contains a number of areas. The following graphic illustrates the various areas, and descriptions of them are listed below.

NOTE
Some panels may be hidden by default. To view all panels, select View > Show Panels > All Panels, or press F12.



Fabrics	5
SAN Switches	15
Hosts	0
Events	234 (This Hour)

FIGURE 1 Main window

1. Menu bar. Lists commands you can perform on the Management application. The available commands vary depending on which tab (SAN or Dashboard) you select. For a list of available commands, refer to Appendix A, “Application menus”.

2. Toolbar. Provides buttons that enable quick access to dialog boxes and functions. The available buttons vary depending on which tab (SAN or Dashboard) you select. For a list of available commands, refer to “SAN tab” on page 8, , or “Dashboard tab” on page 3.

3. Tabs. Provides quick access to the following views:

   - Dashboard tab. Provides a high-level overview of the network managed by Management application server. For more information, refer to the “Dashboard tab”.
   - SAN tab. Displays the Master Log, Minimap, Connectivity Map (topology), and Product List. For more information, refer to the “SAN tab”.

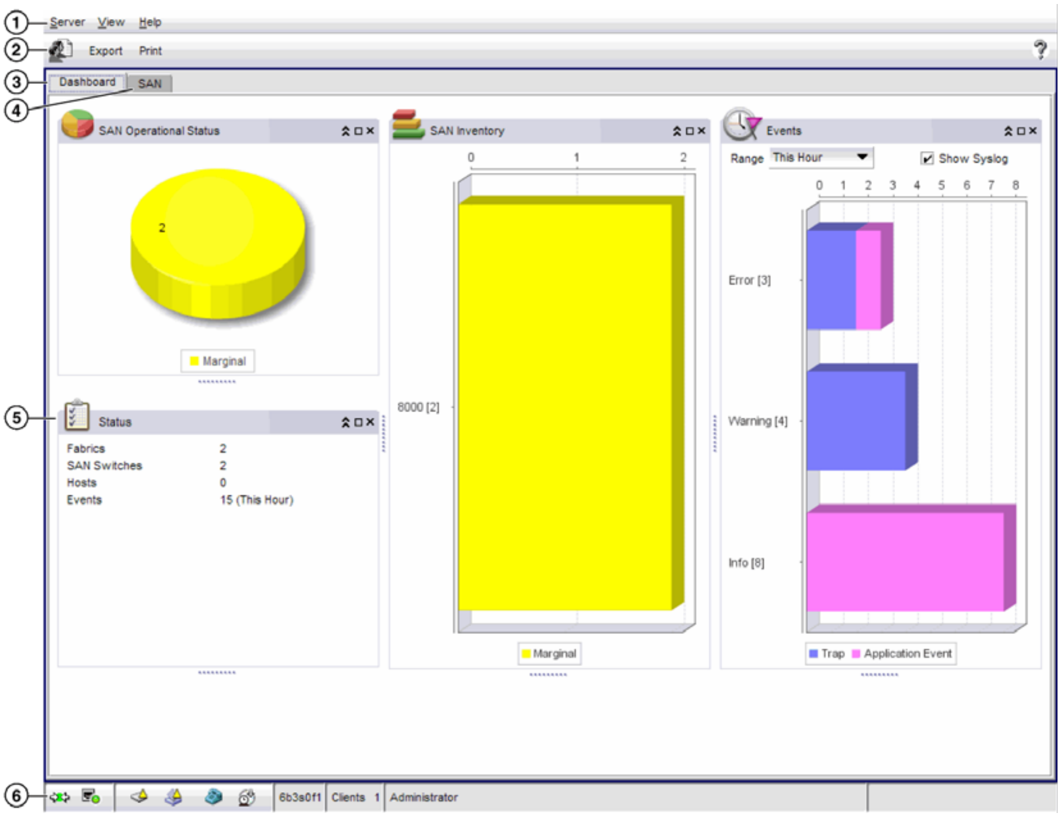
4. Status bar. Displays the connection, port, product, fabric, special event, call home, and backup status, as well as Server and User data.

Dashboard tab

NOTE
Only devices in your area of responsibility (AOR) display in the dashboard.

The **Dashboard** tab provides a high-level overview of the network and the current states of managed devices. This allows you to easily check the status of the devices on the network. The dashboard also provides several features to help you quickly access reports, device configuration, and system logs.

The dashboard updates every 5 seconds regardless of the currently selected tab (SANor Dashboard) or the SAN size. However, data may become momentarily out of sync between the dashboard and other areas of the application. For example, if you remove a product from the network while another user navigates from the dashboard to a more detailed view of the product, the product may not appear in the detailed view.



Fabrics	2
SAN Switches	2
Hosts	0
Events	15 (This Hour)

FIGURE 2 Main Window - Dashboard tab

1. **Menu bar.** Lists commands you can perform on the Dashboard. For a list of **Dashboard** tab menu commands, refer to "Dashboard main menus" on page 909.
2. **Toolbar.** Provides buttons that enable quick access to dialog boxes and functions.
3. **Dashboard tab.** Provides a high-level overview of the network managed by Management application server. For more information, refer to the "Dashboard tab".
4. **SAN tab.** Displays the Master Log, Minimap, Connectivity Map (topology), and Product List. For more information, refer to the "SAN tab".

5. **Widgets.** Displays operational status, inventory status, event summary, and overall network/fabric status.
6. **Status bar.** Displays the connection, port, product, fabric, special event, call home, and backup status, as well as Server and User data.

Menu bar

The menu bar is located at the top of the main window. For a list of the many functions available on each menu, refer to "Dashboard main menus" on page 909.

Toolbar

The toolbar (Figure 3) is located beneath the menu bar and provides icons and buttons to perform various functions.

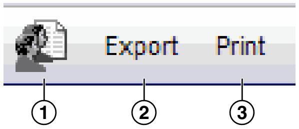


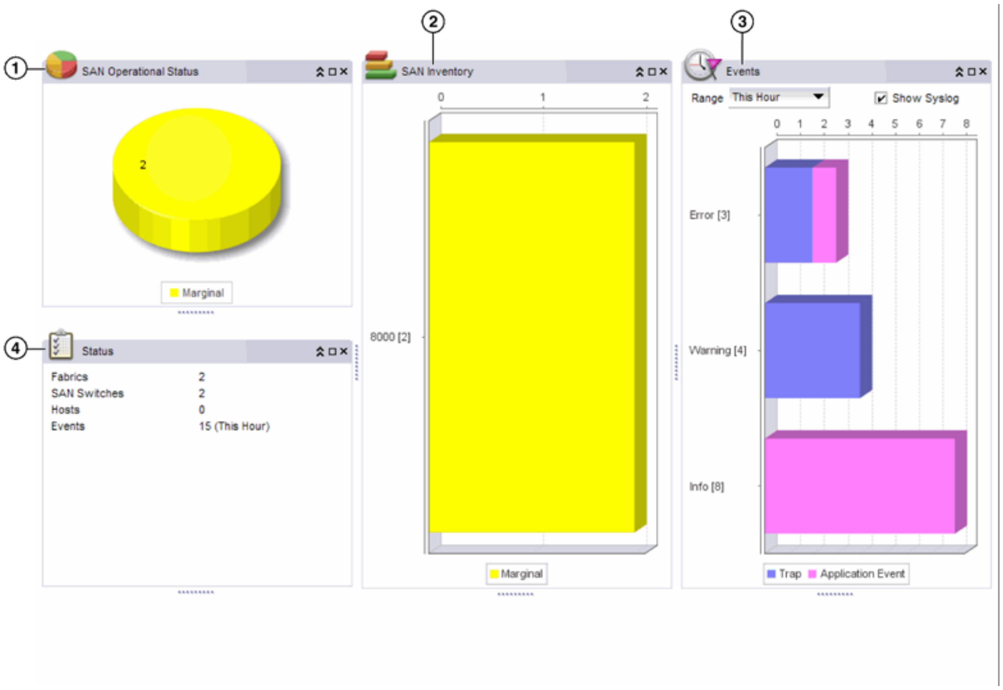
FIGURE 3 Toolbar

The tool bar contains the following buttons:

1. **Users**—Displays the **Users** dialog box. Use to configure users, user groups, and permissions
2. **Export**—Saves the current dashboard display (all widgets) in a .png format
3. **Print**—Prints the dashboard display (all widgets).

Widgets

The Dashboard contains four widgets which can be shown or hidden, resized, collapsed or expanded, as well as maximized or minimized; however you cannot detach a widget. The status and inventory widget colors are defined in “Event type color codes” on page 6.



Range: This Hour
☑ Show Syslog

Fabrics	2
SAN Switches	2
Hosts	0
Events	15 (This Hour)

FIGURE 4 Widgets

The Dashboard includes the following widgets:

1. SAN Operational Status. Displays the device status as a pie chart. Displays the device status as a percentage of the total number of devices. Displays the percentage in various colors on each slice. Displays the color legend below the pie chart. Displays tooltips on mouse-over to show the number of devices in that state. When there is one status category with less than one percent of the total number of devices, the status widget displays the number of devices in each category on each slice.

   The SAN operational and inventory widgets display the status using the following color-code:

   TABLE 2 Status color codes

Color	Type
Green	Healthy
Yellow	Marginal
Red	Down
Maroon	Not Reachable
Gray	Unknown

2. **SAN Inventory**. Displays the SAN products inventory as stacked bar graphs. Displays each group as a separate bar on the graph. Displays the current state of all products discovered for a group in various colors on each bar. Displays the color legend below the y-axis. Displays tooltips on mouse-over to show the number of devices in that state.

   Inventory widget customization

   Group By list—Select to display product inventory for a specific grouping. The group type and number in the group displays to the left of the associated bar. For example, v7.0.0 [3] where v7.0.0 is the firmware number and [3] is the number of devices running that firmware level. To change the grouping, select one of the following from the list.

   - **Firmware**—Displays the product inventory by firmware release.
   - **Model**—Displays the product inventory by model.
   - **Location**—Displays the product inventory by physical location.
   - **Contact**—Displays the product inventory by contact name.

3. **Events**. Displays the number of events by severity level for a specified time range as a stacked bar graph. you can customize this widget to display a specific time range. Options include: This Hour, Last Hour, Last 24 Hours, Last 7 Days, or Last 30 Days.

   The Events widgets displays the Event types using the following color-code:

TABLE 3 **Event type color codes**

Color	Type
Purple	Traps
Pink	Application events
Salmon	Security events
Aqua	Syslog events

For more information about event types, refer to Fault Management.

The Events widget only includes events from products that are in your AOR.

The x-axis represents the number of occurrences of a particular event severity during the selected time period. If you move your mouse over a bar, a tool tip shows the number of events with that severity level during the selected time period. Also, for each severity, the cumulative number of traps, application events, and security events are reported next to the horizontal bar. If Syslog messages are included, then they are included in the count. To conserve space, the number is shown as is or truncated to the nearest 1000("K") or 1,000,000("M").

By default, Syslog events are included in the summary; however, since Syslog events occur at a much higher frequency than other events and therefore could askew the bars for the other events, you can exclude Syslog events. If they're excluded, they will not be displayed in the legend. Users' selections are persisted (per user per server).

Events widget customization

- **Range** list—Select to display event information for a specific duration. To change the duration, select one of the following from the list.
  - **This Hour**—Displays event information for the current hour beginning when the Dashboard is displayed.
  - **Last Hour**—Displays event information for the previous hour to when the Dashboard is displayed.
  - **Yesterday**—Displays event information for the previous day beginning at 12AM of the previous day.
  - **Last 7 Days**—Displays event information for the last 7 days, including the current day.
  - **Last 30 Days**—Displays event information for the last 30 days, including the current day
- **Show Syslog** check box—Select to include Syslog information (default) on the Event Summary pane. To exclude Syslog information, clear the check mark.

4. **Status**. Displays the number products managed and the number of events within the selected event time range. Displays various IP management processes and their current state. Displays the following items for each product license:
   - Fabrics
   - SAN Switches
   - Hosts
   - Events
   - sFlow

Widget functions

- **Title bar buttons**. All widgets have the following three (left to right) title bar buttons: expand/collapse, maximize/minimize, and close.
- **Resizing**. All widgets can be resized by dragging the grab bars. Use the vertical grab bars between widget columns to adjust the width of widgets in the adjacent columns. Use the Horizontal grab bars to adjust the height of adjacent widget rows.
- **Tooltips**. Only widgets with a pie chart or bar graph display tooltips when you mouse over a section or bar.
  - For the pie chart widgets, the tooltip displays the name of the category, number of items in that category, and the percentage.
  - For the bar graph widgets, the tooltip displays the count represented by the selected bar.
- **Navigation**. The Events widget enables you to navigate away from the dashboard. If the ratio between the biggest and smallest section of a pie chart reaches 5000:1, you should maximize the widget prior to navigating away from the widget.
  - Double-click a bar in the Events widget to navigate to a event custom report (HTML) that displays the events corresponding to the event type selected. For information about report details, refer to Fault Management.
- **Zoom**. The Events widget enables you to zoom in to view tooltips. If the ratio between the longest and shortest bar reaches 5000:1, you should maximize the widget prior to using zoom. To zoom in on an area of a widget, drag the mouse (upper left corner to lower right corner) to select one or more bars. To return the widget to its original state, reverse the selection (drag from lower right corner to upper left corner).

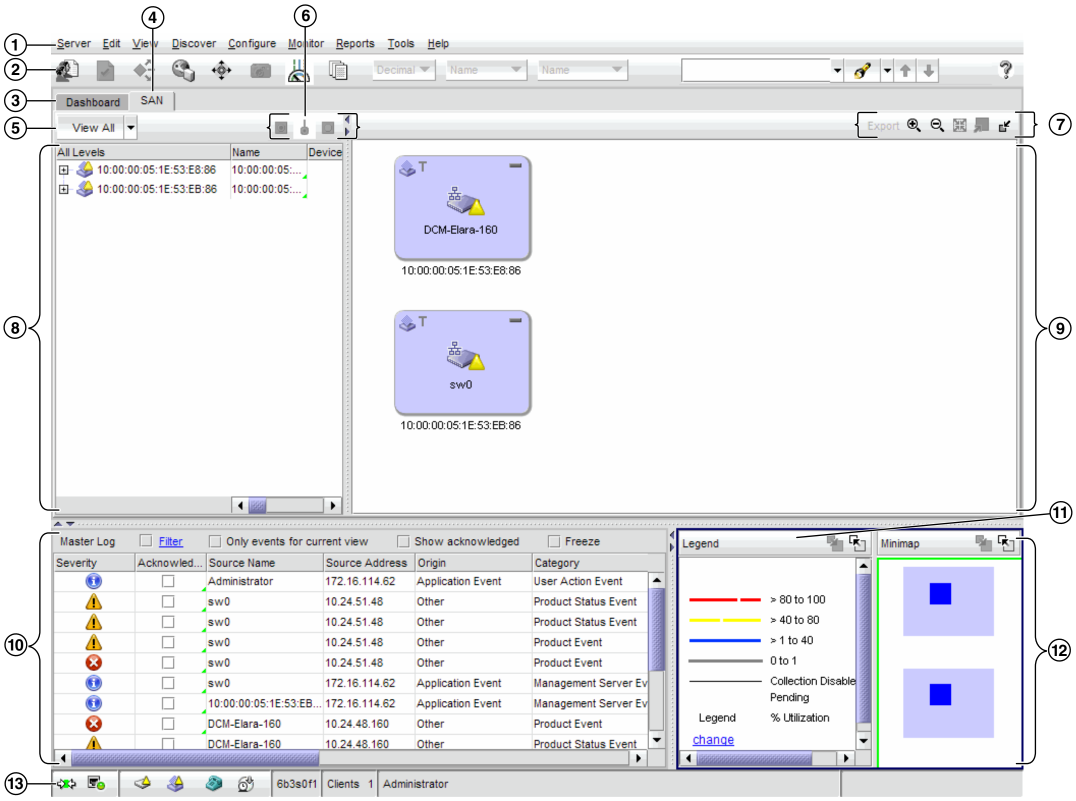
- **Export.** To take a snapshot (.png) of the dashboard, complete the following steps.
  a. Click **Export**.
  b. Browse to the location where you want to save the snapshot.
  c. Enter a name for the snapshot in the **File Name** field.
  d. Click **Save**.
- **Print.** To print the dashboard, complete the following steps.
  a. Click **Print**.
  b. Click **OK**.

SAN tab

The **SAN** tab (Figure 5) displays the Product List, Topology Map, Master Log, Utilization Legend, and Minimap.

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.

NOTE
Some areas may be hidden by default. To view areas of the **SAN** tab, select **View > Show Panels > All Panels**, or press **F12**.



All Levels	Name	Device
⊞ 10:00:00:05:1E:53:E8:86	10:00:00:05:...	
⊞ 10:00:00:05:1E:53:EB:86	10:00:00:05:...	

Master Log □ Filter □ Only events for current view □ Show acknowledged □ Freeze

Severity	Acknowled...	Source Name	Source Address	Origin	Category
ℹ	□	Administrator	172.16.114.62	Application Event	User Action Event
⚠	□	sw0	10.24.51.48	Other	Product Status Event
⚠	□	sw0	10.24.51.48	Other	Product Status Event
⚠	□	sw0	10.24.51.48	Other	Product Event
✖	□	sw0	10.24.51.48	Other	Product Event
ℹ	□	sw0	172.16.114.62	Application Event	Management Server Ev
ℹ	□	10:00:00:05:1E:53:EB...	172.16.114.62	Application Event	Management Server Ev
✖	□	DCM-Elara-160	10.24.48.160	Other	Product Event
⚠	□	DCM-Elara-160	10.24.48.160	Other	Product Status Event

FIGURE 5 Main window - SAN tab

1. **Menu bar.** Lists commands you can perform on the **SAN** tab. For a list of **SAN** tab menu commands, refer to “SAN main menus” on page 910.
2. **Main toolbar.** Provides buttons that enable quick access to dialog boxes and functions. For a list of available commands, refer to “Main toolbar” on page 10.
3. **Dashboard tab.** Provides a high-level overview of the network managed by Management application server. For more information, refer to the “Dashboard tab”.
4. **SAN tab.** Displays the Master Log, Minimap, Connectivity Map (topology), and Product List.
5. **View All list.** Enables you to create, copy, or edit a view, select to how to view the Product list (All Levels, Products and Ports, Products Only, or Ports Only) and to select which view you want to display in the main window.
6. **Port Display buttons.** Provides buttons that enable quick access to configuring how ports display. Not enabled until you discover a fabric or host. For more information, refer to “Port Display buttons” on page 11.
7. **Product List.** Lists the devices discovered in the Management application.
8. **Connectivity Map.** Displays the topology, including discovered and monitored devices and connections.
9. **Connectivity Map toolbar.** Provides tools for viewing the Connectivity Map as well as exporting the Connectivity Map as an image. Does not display until you discover a fabric.
10. **Master Log.** Displays all events that have occurred on the Management application.
11. **Utilization Legend.** (Trial and Licensed version only) Indicates the percentage ranges represented by the colored, dashed lines on the Connectivity Map. Only displays when you select **Monitor > Performance > View Utilization** or click the **Utilization** icon on the toolbar.
12. **Minimap.** Displays a “bird’s-eye” view of the entire topology. Does not display until you discover a fabric.
13. **Status bar.** Displays the connection, port, product, fabric, special event, call home, and backup status, as well as Server and User data.

Menu bar

The menu bar is located at the top of the main window. Some menu items display as disabled unless you select the correct object from the product list or topology map. For a list of the many functions available on each menu, refer to “SAN main menus” on page 910.

Main toolbar

The toolbar is located beneath the Menu bar and provides icons to perform various functions.

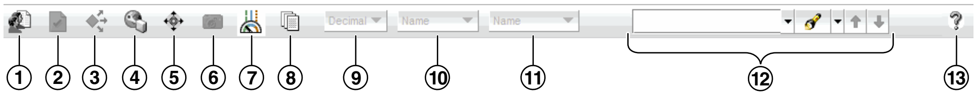


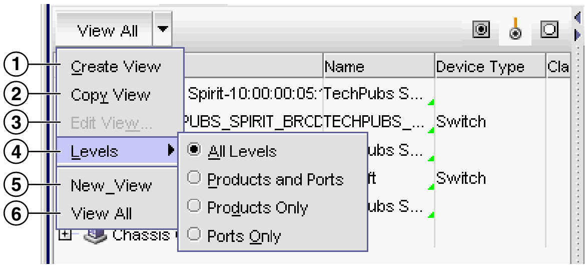
FIGURE 6 SAN main toolbar

The icons on your toolbar vary based on the licensed features on your system.

1. **Users.** Displays the **Users** dialog box. Use to configure users, user groups, and permissions.
2. **Properties.** Displays the **Properties** dialog box of the selected device or fabric. Use to view or edit device or fabric properties.
3. **Launch Element Manager.** Launches the Element Manager of the selected device. Use to configure a device through its Element Manager.
4. **Discover Setup.** Displays the **Discover Setup** dialog box. Use to configure discovery.
5. **Zoning.** Displays the **Zoning** dialog box. Use to configure zoning.
6. **Track Fabric Changes.** Select to turn track fabric changes on or off for the selected device or group.
7. **View Utilization.** Displays or hides the utilization legend.
8. **View Report.** Displays the **View Reports** dialog box. Use to view available reports.
9. **Domain ID/Port #.** Use to set the domain ID or port number to display as decimal or hex in the Connectivity Map.
10. **Product Label.** Use to set the product label for the devices in the Connectivity Map.
11. **Port Label.** Use to set the port label for the devices in the Connectivity Map.
12. **Product List Search.** Use to search for a device in the product list. For detailed instructions, refer to “Search” on page 196
13. **Help.** Displays the Online Help.

View All list

The **View All** list is located at the top left side of the window and enables you to create, copy, or edit a view, select to how to view the Product list (All Levels, Products and Ports, Products Only, or Ports Only) and to select which view you want to display in the main window. Does not display until you discover a fabric. To discover a fabric, refer to "Discovering fabrics" on page 53.



1. **Create View.** Select to create a new view.
2. **Copy View.** Select to copy an existing view.
3. **Edit View.** Select to edit an existing view.
4. **Levels.** Select the level at which you want to view the Product list, Options include: All Levels, Products and Ports, Products Only, or Ports Only.
5. *View_Name.* Any additional views that you create. Select which view you want to display in the main window.
6. **View All.** Select to display the default view of the main window.

Port Display buttons

The **Port Display** buttons are located at the top right of the Product List and enable you to configure how ports display. You have the option of viewing connected (or occupied) product ports, unoccupied product ports, or attached ports. Not enabled until you discover a fabric or host.

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.

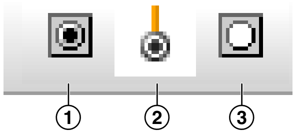


FIGURE 7 **Port Display buttons**

1. **Show/Hide Occupied Port.** Displays or hides the ports of the devices in the fabrics (present in the connectivity map) that are connected to other devices.
2. **Show/Hide Attached Port.** Displays or hides the attached ports of the target devices.
3. **Show/Hide Unoccupied Port.** Displays or hides the ports of the devices (shown in the connectivity map) that are not connected to any other device.

Connectivity Map toolbar

The Connectivity Map toolbar is located at the top right side of the **View** window and provides tools to export the topology, to zoom in and out of the Connectivity Map, collapse and expand groups, and fit the topology to the window. Not enabled until you discover a fabric.

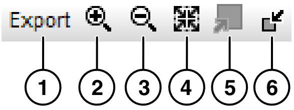


FIGURE 8 The Connectivity Map toolbar

1. **Export.** Use to export the topology to a PNG file.
2. **Zoom In.** Use to zoom in on the Connectivity Map.
3. **Zoom Out.** Use to zoom out on the Connectivity Map.
4. **Fit in View.** Use to scale the map to fit within the Connectivity Map area.
5. **Expand.** Use to expand the map to show all ports in use on a device.
6. **Collapse.** Use to collapse the map to show only devices (hides ports).

Product List

The Product List, located on the **SAN** 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 **View** > **Show Panels** > **Product List** or press **F9**.

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 (presented here in alphabetical order) are included in the Product List.

- **Additional Port Info.** Displays additional port information.
- **All Levels.** Displays all discovered fabrics, groups, devices, and ports as both text and icons. Also, displays the status of the fabrics, groups, devices, and ports. For a list of icons that display in the **All Levels** column, refer to the following tables:
  - “SAN product icons” on page 18
  - “SAN group icons” on page 19
  - “SAN port icons” on page 20
- **Additional Port Info.** Displays additional information about the port.
- **Attached Port #.** Displays the number of the attached port.
- **BB Credit.** Displays the BB Credit of the port.
- **Class.** Displays the class value of the FICON device port.
- **Contact.** Displays the name of the person or group you should contact about the product. This field is editable at the fabric level.
- **Description.** Displays the description of the product. This field is editable at the fabric level.
- **Product Type.** Displays the type of product.

- Domain ID. Displays the Domain ID for the product in the format xx(yy), where xx is the normalized value and yy is the actual value on the wire.
- FC Address. Displays the Fibre Channel address of the port.
- Firmware. Displays the firmware version of the product.
- IP Address. Displays the IP address (IPv4 or IPv6 format) of the product.
- Location. Displays the physical location of the product. This field is editable at the fabric level.
- Model. Displays the model number of the product.
- Name. Displays the name of the product or port. This field is editable at the fabric, device, and port level.
- Port #. Displays the number of the port.
- Port Count. Displays the number of ports on the product.
- Port Type. Displays the type of port (for example, expansion port, node port, or NL_port).
- Protocol. Displays the protocol for the port.
- Serial #. Displays the serial number of the product.
- Speed Configured (Gbps). Displays the actual speed of the port in Gigabits per second.
- State. Displays the state for the product and the port.
- Status. Displays the status for the product and the port.
- Symbolic Name. Displays the symbolic name for the port.
- TAG. Displays the tag number of the product.
- Vendor. Displays the name of the product's vendor.
- WWN. Displays the world wide name of the product or port.
- Zone Alias. Displays the zone alias of the product or port.

Connectivity Map

The Connectivity Map, which displays in the upper right area of the main widow, is a grouped map that shows physical and logical connectivity of SAN components, including discovered and monitored devices and connections. These components display as icons in the Connectivity Map. For a list of icons that display in the Connectivity Map, refer to the following tables:

- "SAN product icons" on page 18
- "SAN group icons" on page 19
- "Event icons" on page 22

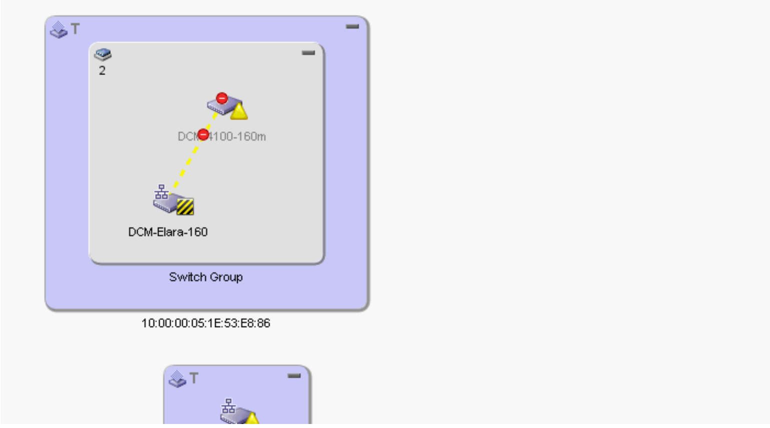


FIGURE 9 Connectivity Map

The Management application displays all discovered fabrics in the Connectivity Map by default. To display a discovered Host in the Connectivity Map, you must select the Host in the Product List. You can only view one Host and physical and logical connections at a time.

Master Log

The Master Log, which displays in the lower left area of the main window, lists the events and alerts that have occurred on the SAN. If you do not see the Master Log, select **View > Show Panels > All Panels** or press **F5**.

You can sort the Master Log by clicking a column heading. By default, the Master Log is sorted by the **Last Event Server Time** column. To filter information in the Master Log, refer to "Filtering events in the Master Log" on page 888.

- The following fields and columns are included in the Master Log:**Severity.** The severity of the event. When the same event (Warning or Error) occurs repeatedly, the Management application automatically eliminates the additional occurrences. For more information about events, refer to "Fault Management" on page 823. For a list of the event icons, refer to "Event icons" on page 22.
- **Acknowledged.** Whether the event is acknowledged or not. Select the check box to acknowledge the event.
- **Source Name.** The product on which the event occurred.
- **Source Address.** The IP address (IPv4 or IPv6 format) of the product on which the event occurred.
- **Origin.** The event source type (for example trap, pseudo event, application, or syslog).

- **Category.** The type of event that occurred (for example, client/server communication events).
- **Description.** A description of the event.
- **Last Event Server Time.** The time and date the event last occurred on the server.
- **Count.** The number of times the event occurred.
- **Module Name.** The name of the module on which the event occurred.
- **Message ID.** The message ID of the event.
- **Product Address.** The IP address of the product on which the event originated.
- **Contributor.** The name of the contributor on which the event occurred.
- **Node WWN.** The world wide name of the node on which the event occurred.
- **Fabric Name.** The name of the fabric on which the event occurred.
- **Operational Status.** The operational status (such as, unknown, healthy, marginal, or down) of the product on which the event occurred.
- **First Event Product Time.** The time and date the event first occurred on the product.
- **Last Event Product Time.** The time and date the event last occurred on the product.
- **First Event Server Time.** The time and date the event first occurred on the server.
- **Audit.** The audit of the event.
- **Virtual Fabric ID.** The VFID of the product on which the event occurred.
- **Zone Alias.** Displays the zone alias of the product or port.

Utilization Legend

The Utilization Legend, which displays in the lower right corner of the main window, indicates the percentage ranges represented by the colored, dashed lines on the Connectivity Map. It only displays when you select **Monitor > Performance > View Utilization** or click the **Utilization** icon on the toolbar.

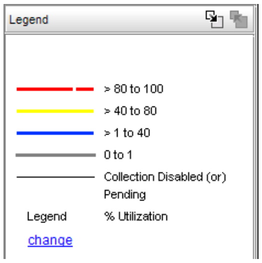


FIGURE 10 Utilization Legend

The colors and their meanings are outlined in the following table.

Line Color	Utilization Defaults
Red line	80% to 100% utilization
Yellow line	40% to 80% utilization
Blue line	1% to 40% utilization
Gray line	0% to 1% utilization
Black line	Utilization disabled

For more information about the utilization legend, refer to “SAN Connection utilization” on page 791.

Minimap

The **Minimap**, which displays in the lower right 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 Connectivity Map. To jump to a specific location on the Connectivity Map, click that area on the Minimap. A close-up view of the selected location displays on the Connectivity 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. Does not display until you discover a fabric.

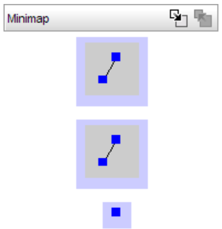


FIGURE 11 Minimap

Anchoring or floating the Minimap

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

- To float the Minimap and view it in a separate window, click the **Detach** icon ( ) in the upper right corner of the Minimap.
- To anchor the Minimap and return the Minimap to its original location on the main window, do one of the following steps:
  - Click the **Attach** icon ( ) in the upper right corner of the Minimap.
  - Click the **Close** icon (☒) in the upper right corner of the Minimap.
  - Double-click the logo in the upper left corner of the Minimap.
  - Click the logo in the upper left 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.

Status bar

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 the current status of products, fabrics, and backup.

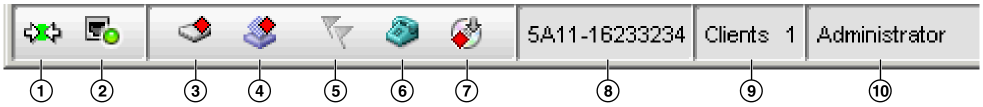


FIGURE 12 Status Bar

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

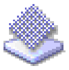
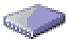
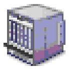
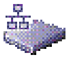
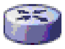
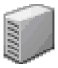
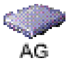
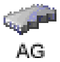
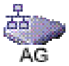
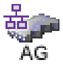
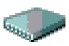
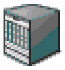
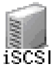
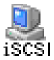
1. **Connection Status.** Displays the Server-Client connection status.
2. **Port Status.** Displays port status for the following ports: SNMP, Syslog, FTP, and Web Server. Click to launch the **Port Status** dialog box. For more information about port status, refer to "Viewing port status" on page 33.
3. **Product Status.** 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 displays as degraded. Click this icon to open the **Product Status Log**.
4. **Fabric Status.** 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 Connectivity Map or Product List and click this icon to open the related **Fabric Log** (only available for persisted fabrics).
5. **Special Events.** Displays whether or not a special event has been triggered. Click to launch the **Spcial Events** dialog box. For more information about special events, refer to "Creating an event action definition" on page 847
6. **Call-Home Status.** (Trial and Licensed version only) Displays a call home status icon when one or more product are discovered, which allows you to determine the current call home status. Click to launch the **Call Home Notification** dialog box. For more information about Call Home status and icons, refer to "Viewing Call Home status" on page 173.
7. **Backup Status.** Displays a backup status icon, which allows you to determine the current backup status. Right-click and select **Backup now** to begin back up immediatly. Right-click and select **Configure backup** to launch the **Options** dialog box - **Server Backup** pane and configure backup. 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.
8. **Server Name.** Displays the name of the Server to which you are connected.
9. **Total Users.** Displays the number of clients logged into the server.
10. **User's ID.** Displays the user ID of the logged in user.
11. **Trial license** (Not shown). Displays the trial expiration information to the right of the User's ID.

Icon legend

Various icons are used to illustrate devices and connections in a network. The following tables list icons that display on the Connectivity Map and Product List.

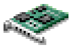
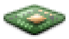
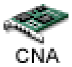
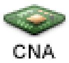
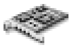
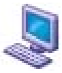
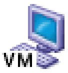
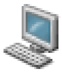
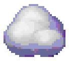
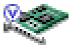
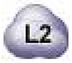
SAN product icons

The following table lists the manageable SAN product icons that display on the topology. Fabric OS manageable devices display with blue icons and M-EOS manageable devices display with green icons. Unmanageable devices display with gray icons. Some of the icons shown only display when certain features are licensed.

Icon	Description	Icon	Description
	Fabric		Fabric OS Switch and Blade Switch
	Fabric OS Director		Fabric OS CEE Switch
	Fabric OS Router		Storage
	Fabric OS FC Switch in Access Gateway mode (single-fabric connected)		Fabric OS FC Switch in Access Gateway mode (multiple-fabric connected)
	Fabric OS CEE Switch in Access Gateway mode (single-fabric connected)		Fabric OS CEE Switch in Access Gateway mode (multiple-fabric connected)
	M-EOS Switch		M-EOS Director
	iSCSI Target		iSCSI Initiator

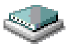
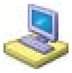
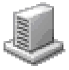
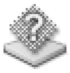
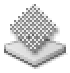
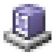
Host product icons

The following table lists the manageable Host product icons that display on the topology. Fabric OS manageable devices display with blue icons and M-EOS manageable devices display with green icons. Unmanageable devices display with gray icons. Some of the icons shown only display when certain features are licensed.

Icon	Description	Icon	Description
	HBA		HBA Mezzanine Card
	CNA		CNA Mezzanine Card
	Unmanaged HBA		Host
	VM Host		Unmanaged Host
	Ethernet Cloud		Virtual HBA
	Layer 2 Clouds		

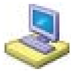
SAN group icons

The following table lists the manageable SAN product group icons that display on the topology.

Icon	Description	Icon	Description
	Switch Group		Host Group
	Storage Group		Unknown Fabric Group
	Unmanaged Fabric Group		Chassis Group

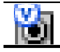
Host group icons

The following table lists the manageable Host product group icons that display on the topology.

Icon	Description	Icon	Description
	Host Group		

SAN port icons

The following table lists the port icons that display in the Product List.

Icon	Description
	Occupied FC Port
	Unoccupied FC Port
	Attached FC Port
	Trunk (port group)
	IP and 10 GE Port
	Attached IP and 10 GE Port
	Attached-to-Cloud 10 GE Port
	Virtual Port
	Virtual FCoE Port
	Attached FCoE Port
	Pre-boot Virtual Port
	Virtual Attached Port

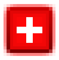
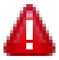
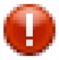
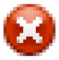
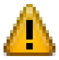
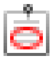
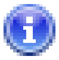
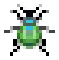
SAN product status icons

The following table lists the product status icons that display on the topology.

Icon	Status
No icon	Healthy/Operational
⚠	Attention
◆	Bottleneck
△	Degraded/Marginal
⊕	Device Added
⊖	Device Removed/Missing
◆	Down/Failed
↘	Routed In
↩	Routed Out
▢	Unknown/Link Down
▨	Unreachable

Event icons

The following table lists the event icons that display on the topology and Master Log. For more information about events, refer to "Fault Management" on page 823.

Event Icon	Description
	Emergency
	Alert
	Critical
	Error
	Warning
	Notice
	Informational
	Debug

Management server and client

The Management application has two parts: the Server and the Client. The Server is installed on one machine and stores device-related information; it does not have a user interface. To view information through a user interface, you must log in to the Server through a Client. The Server and Clients 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 Switches and the Servers or Clients. In other words, a Server or Client can find a Switch, appear to log in, but is immediately logged out because the Switch cannot reach the Server or Client. To resolve this issue, check to determine if the ports in the table below need to be opened up in the firewall.

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 is immediately logged out because the Server cannot reach the Client. To resolve this issue, check to determine if the ports in the table below need to be opened up in the firewall.

TABLE 4 Trial and Licensed version ports

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
20[1]	FTP Port (Control)	TCP	FTP Control port for internal FTP server	Client–Server Switch–Server	Yes Yes
21[1, 2]	FTP Port (Data)	TCP	FTP Data port for internal FTP server	Client–Server Switch–Server	Yes Yes
22[1]	SSH or Secure Telnet	TCP	Sectelnet port from server to switch/client to switch	Server–Switch Client–Switch	Yes
23[1]	Telnet	TCP	Telnet port from server/client to switch	Server–Switch Client–Switch	Yes
25	SMTP Server port	TCP	SMTP Server port for E-mail communication	Server–SMTP Server	Yes
49	TACACS+ Authentication port	TCP	TACACS+ server port for authentication if TACACS+ is chosen as an external authentication	Server–TACACS+ Server	Yes
80	jboss.web.http.port	TCP	Non-SSL HTTP/1.1 connector port	Client–Server	Yes
80[3, 4]	Switch http	TCP	Switch non-SSL http port for http and CAL communication	Server–Switch Client–Switch	Yes
161[1]	SNMP Port	UDP	Default SNMP port	Server–Switch	Yes
162[3]	snmp.trap.port	UDP	Default SNMP trap port	Switch–Server	Yes
389	LDAP Authentication Server Port	TCP	LDAP server port for authentication if LDAP is chosen as an external authentication	Server–LDAP Server	Yes
443[3, 4, 5]	Switch https	TCP	Switch SSL http port for https and CAL communication	Server–Switch Client–Switch	Yes
514[6]	Syslog Port	UDP	Default Syslog Port	Switch–Server	Yes

TABLE 4 Trial and Licensed version ports (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
636	LDAP Authentication SSL port	TCP	LDAP server port for authentication if LDAP is chosen as an external authentication and SSL is enabled	Server–LDAP Server	Yes
1024[1, 7]	MPI	TCP	MPI trap recipient port	Switch–Server	Yes
1812	RADIUS Authentication Server Port	TCP	RADIUS server port for authentication if RADIUS is chosen as an external authentication	Server–RADIUS Server	Yes
2048[1, 9]	MPI	TCP	MPI discovery NMRU port	Server–Switch	Yes
2049[1,5,7,9]	MPI	TCP	MPI discovery NMRU port for SSL	Server–Switch	Yes
2638[8]	Database port (Enforced during install)	TCP	Port used by database	Server–Database Remote ODBC–Database	Yes
4430[1, 5, 7]	MPI	TCP	XML-RCP port for SSL	Server–Switch	Yes
5988	SMI Agent port	TCP	SMI Agent port	Server–SMI Agent	Yes
5989	SMI Agent port with SSL enabled	TCP	SMI Agent port with SSL enabled	Server–SMI Agent	Yes
8080[1, 7]	MPI	TCP	XML-RCP port/HTTP port	Server–Switch	Yes
24600[10]	jboss.naming.jnp.port - port 0	TCP	Bootstrap JNP service port	Client–Server	Yes
24601	jboss.connector.ejb3.port - port 1	TCP	EJB3 connector port	Client–Server	Yes
24602	jboss.connector.bisocket.port - port 2	TCP	Bisocket connector port	Client–Server	Yes
24603	jboss.connector.bisocket.secondary.port - port 3	TCP	Bisocket connector secondary port	Client–Server	Yes
24604[5]	jboss.connector.sslbisocket.port - port 4	TCP	SSL Bisocket connector port	Client–Server	Yes
24605[5]	jboss.connector.sslbisocket.secondary.port - port 5	TCP	SSL Bisocket connector secondary port	Client–Server	Yes
24606	smp.registry.port - port 6	TCP	RMI registry port	Client–Server	Yes
24607	smp.server.export.port - port 7	TCP	RMI export port	Client–Server	Yes
24608	smp.server.cliProxyListening port - port 8	TCP	CLI proxy telnet port	Client–Server	Yes
24609	jboss.naming.rmi.port - port 9	TCP	RMI naming service port	Client–Server	Yes
24610	jboss.jrmp.invoker.port - port 10	TCP	RMI/JRMP invoker port	Client–Server	Yes
24611	jboss.pooled.invoker.port - port 11	TCP	Pooled invoker port	Client–Server	Yes
24612	jboss.connector.socket.port - port 12	TCP	Socket invoker port	Server	No
24613	jboss.web.ajp.port - port 13	TCP	AJP 1.3 connector port	Server	No
24614	jboss.web.service.port – port 14	TCP	Web service port	Server	No
24615	connector.bind.port – port 15	TCP	Port to listen for requests on	Server	No

TABLE 4 Trial and Licensed version ports (Continued)

Port Number	Ports	Transport	Description	Communication Path	Open in Firewall
55555[10]	Client Export Port	TCP	Client port to which server pushes the M-EOS device Element Manager updates	Server–Client	Yes
55556	Launch in Context (LIC) client hand shaking port	TCP	Client port used to check if a Management application client opened using LIC is running on the same host **NOTE:** If this port is in use, the application uses the next available port.	Client	No

1 Port is not configurable (either in the switch or the Management server).

2 Every FTP session requires an additional port which is randomly picked. If the firewall is enabled then FTP operation (used for firmware download, technical support, firmware import (from client-server) and so on.) will fail.

3 Ports configurable in the switch and the Management server. Port must be the same for all switches managed by the Management server.

4 Ports used to launch the Web Tools application for Fabric OS switches from the Management client. This is applicable only when the Fabric OS version is earlier than 6.1.1.

5 Port used for SSL communication. If SSL is enabled, you must open 443*, 24604, and 24605 in the firewall. If SSL is not enabled, port 80* must be open in the firewall and 443*, 24604, and 24605 can be closed. An asterisk (*) denotes the default web server port number. If you set the web server port number to a port other than the default, you must open that port in the firewall.

6 The Syslog listening port is configurable in the Management server. The switch always sends syslog messages to port 514. If you have any other syslog daemon on the Management server machine already listening to 514, then the Management Server can be configured to listen to a different port. You must manually configure relay in existing syslogd to forward the syslog messages to the Management Server listening on the configured port.

7 Ports used for communicating with M-EOSn (M-i10K) directors. M-i10K always uses NMRU over SSL (2049). M-i10K always uses 8080 for http requests (firmware download, configuration backup/ restore, data collection). If M-EOSn firmware version is less than 9.1 the Management application uses 8080 for XML-RPC requests (discovery and asset collection). If the M-EOSn firmware version is more than 9.1 then it always uses SSL port (4430) for XML-RPC.

8 Port must be opened in firewall for the server when the remote ODBC client needs to talk to the Management database server (Only for EE). The same port is used by the Management server to database server (local). This is not used by the Management client.

9 Ports used for communicating with M-EOS (excluding M-i10K) switches (only required when the Management server manages M-EOS switches).

10 Port should be opened in firewall in the Management client to allow communication between server and client (only applicable for M-EOS switches). If this port is not opened in the firewall, then the M-EOS element manager does not receive updates. Also if multiple clients are opened, it will try to use the next available port (55556). So if there are n clients opened in the same machine then you must open 55555 (configurable) to 55555 + n ports in the firewall.

11 The Management server tries to find a contiguous block of 16 ports from the starting port configured (for example, 24600); if any port in this range is not available for the Management application, then you must provide a new starting port. Note that Port 1 to Port 15 in “Ports” column of the table above are not separately configurable and those ports vary based on the starting port number configuration (specified as Port 0 in the above table). The port numbers mentioned in the table above are the default ports (for example, when 24600 is selected as the starting port number).

Logging into a server

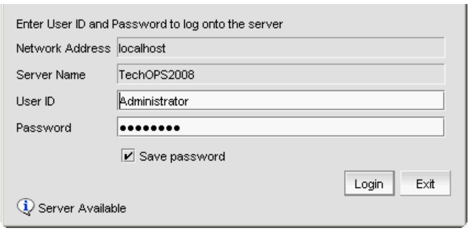
You must log into a server to monitor your network.

NOTE
You must have an established user account on the server to log in.

To log into a server, complete the following steps.

1. Double-click the desktop icon or open the application from the **Start** menu.

   The **Log In** dialog box displays (Figure 13).



Enter User ID and Password to log onto the server

Network Address localhost

Server Name TechOPS2008

User ID Administrator

Password ••••••••

☑ Save password

FIGURE 13 Log In dialog box

2. Enter your user name and password.
3. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

   To change your password, refer to "Changing your password" on page 150.
4. Click **Login**.
5. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Launching a remote client

To launch a remote client, complete the following steps.

1. Open a web browser and enter the IP address of the Management application server in the **Address** bar.

   If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address*:*Port_Number*.

   The Management application web start screen displays.
2. Click the Management application web start link.

   The **Log In** dialog box displays.
3. Enter your user name and password.

   The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change.
4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

5. Click **Login**.
6. Click **OK** on the **Login Banner** dialog box.

   The Management application displays.

Clearing previous versions of the remote client

The remote client link in the **Start** menu does not automatically upgrade when you upgrade the Management application. You must clear the previous version from the Java cache.

To clear the Java cache, complete the following steps.

1. Select **Start** > **Settings** > **Control Panel** > **Java**.

   The **Java Control Panel** dialog box displays.
2. Click **View** on the **General** tab.

   The **Java Cache Viewer** dialog box displays.
3. Right-click the application and select **Delete**.
4. Click **Close** on the **Java Cache Viewer** dialog box.
5. Click **OK** on the **Java Control Panel** dialog box.

   To create a remote client link in the **Start** menu, refer to "Launching a remote client" on page 26.

Launching the Configuration Wizard

You can re-launch the Configuration wizard to change the following configurations:

- FTP server
- Server IP
- Server Ports
- SMI Agent

NOTE
Changes to these configurations require a server restart.

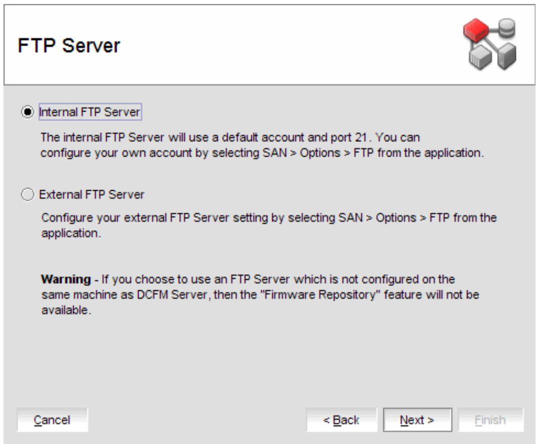
NOTE
You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **11.X.X** > **Server Management Console**).

1. Choose one of the following options:
   - On Windows systems, select **Start** > **Programs** > *Management_Application_Name* **11.X.X** > *Management_Application_Name* **Configuration**.
   - On UNIX systems, execute `sh` *`Install_Home`*`/bin/configwizard` on the terminal.
2. Click **Next** on the **Welcome** screen.
3. Click **Yes** on the confirmation message.

4. Select **Internal FTP Server** or **External FTP Server** on the **FTP Server** screen and click **Next**.

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

NOTE
If you use an FTP Server which is not configured on the same machine as the Management application, the Firmware Repository feature will not be available.



FTP Server

● Internal FTP Server

The internal FTP Server will use a default account and port 21. You can configure your own account by selecting SAN > Options > FTP from the application.

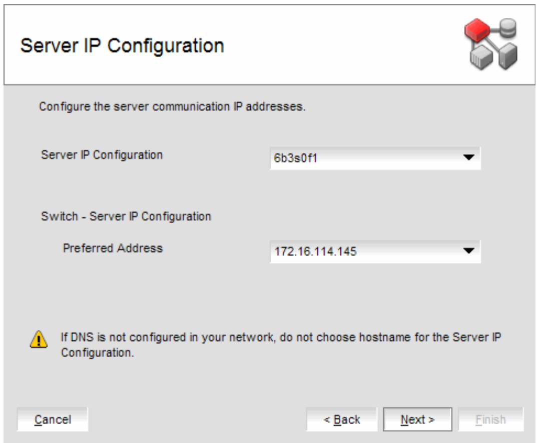
○ External FTP Server

Configure your external FTP Server setting by selecting SAN > Options > FTP from the application.

Warning - If you choose to use an FTP Server which is not configured on the same machine as DCFM Server, then the "Firmware Repository" feature will not be available.

FIGURE 14 FTP Server screen

5. Complete the following steps on the **Server IP Configuration** screen.



Server IP Configuration

Configure the server communication IP addresses.

Server IP Configuration: 6b3s0f1

Switch - Server IP Configuration

Preferred Address: 172.16.114.145

If DNS is not configured in your network, do not choose hostname for the Server IP Configuration.

FIGURE 15 Server IP Configuration screen

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

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

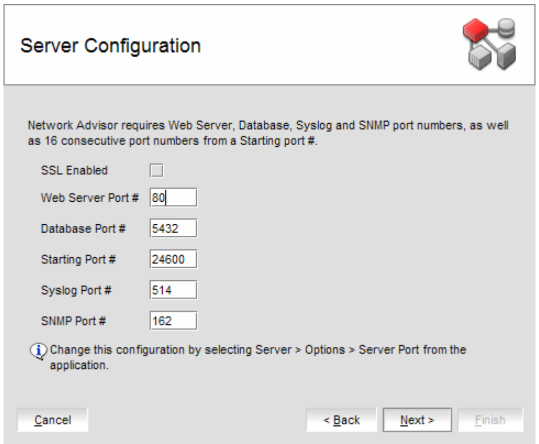
If DNS is not configured for your network, do not select the ‘hostname’ option from either the **Server IP Configuration** or **Switch - Server IP Configuration Preferred Address** list. Selecting the ‘hostname’ option prevents clients and devices from communicating with the Server.

If you select a specific IP address from the **Server IP Configuration** screen and the selected IP address changes, you will not be able to connect to the server. To change the IP address, refer to “Configuring an explicit server IP address” on page 120.

c. Click **Next**.

6. Complete the following steps on the **Server Configuration** screen.

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


Server Configuration

Network Advisor requires Web Server, Database, Syslog and SNMP port numbers, as well as 16 consecutive port numbers from a Starting port #.

SSL Enabled ☐
Web Server Port # 80
Database Port # 5432
Starting Port # 24600
Syslog Port # 514
SNMP Port # 162

Change this configuration by selecting Server > Options > Server Port from the application.

FIGURE 16 Server Configuration screen

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

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

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

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

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

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

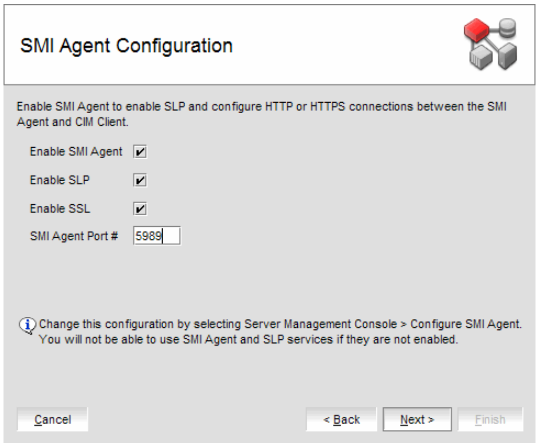
NOTE
The server requires 16 consecutive free ports beginning with the starting port number.

f. Click **Next**.

If you enter a syslog port number already in use, a message displays. Click **No** on the message to remain on the **Server Configuration** screen and edit the syslog port number (return to step 6a). Click **Yes** to close the message and continue with step 7.

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

7. Complete the following steps on the **SMI Agent Configuration** screen.



SMI Agent Configuration

Enable SMI Agent to enable SLP and configure HTTP or HTTPS connections between the SMI Agent and CIM Client.

Enable SMI Agent ☑

Enable SLP ☑

Enable SSL ☑

SMI Agent Port # 5989

Change this configuration by selecting Server Management Console > Configure SMI Agent. You will not be able to use SMI Agent and SLP services if they are not enabled.

FIGURE 17 SMI Agent Configuration screen

a. Enable the SMI Agent by selecting the **Enable SMI Agent** check box.

b. Enable the SLP by selecting the **Enable SLP** check box.

c. Enable the SSL by selecting the **Enable SSL** check box.

d. Enter the SMI Agent port number in the **SMI Agent Port #** field (default is 5989 if SSL is enabled; otherwise, default is 5988).

e. Click **Next**.

8. Verify your configuration information on the **Server Configuration Summary** screen and click **Next**.

9. Complete the following steps on the **Start Server** screen:

a. Select the **Start SMI Agent** check box, if necessary.

b. Select the **Start SLP** check box, if necessary.

c. Select the **Start Client** check box, if necessary.

d. Click **Finish**.

After all of the services (Server, SLP, SMI Agent and Client) are started, the **Log In** dialog box displays.

10. Click **Yes** on the restart server confirmation message.

11. Enter your user name and password.

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

12. Click **Login**.
13. Click **OK** on the Login Banner.

Changing the database user password

To change the read/write or read only database password, complete the following steps in the Install_Home/bin directory.

1. Open a command window.
2. Type **dbpassword** *`User_Name Password New_Password Confirm_Password`* and press **Enter**.

   Where *`User_Name`* is your user name, *`Password`* is your current password, and *`New_Password`* and *`Confirm_Password`* are your new password. The read/write user name and password defaults are dcmadmin and passw0rd (zero), respectively. The read only user name and password defaults are dcmuser and password (all lowercase), respectively.

   If the password changed successfully, the following message displays:
   Password changed successfully.

   If an error occurs and the password did not change, the following message displays:
   Error while updating password. Please try again.
   Press any key to continue.

   If the current password and new password are the same, the following message displays:
   Old and New passwords cannot be same. Use different password and try again.
   Press any key to continue.

   If the new password and confirm password do not match, the following message displays:
   New password and confirm password do not match. Please try again.
   Press any key to continue.
3. Launch the Server Management Console.
4. Click the **Services** tab.
5. Click **Stop** to stop all services.
6. Click **Close** to close the Server Management Console.
7. Launch the Server Management Console.
8. Click **Start** to start all services.

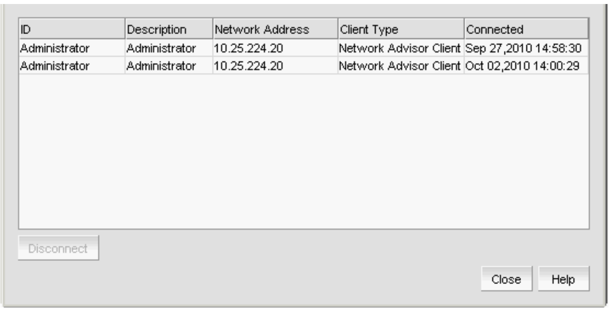
   NOTE
   If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.
9. Click **Close** to close the Server Management Console.

Viewing active sessions

To view the Management application active sessions, complete the following steps.

1. Select **Server > Active Sessions.**

   The **Active Sessions** dialog box displays (Figure 19).



ID	Description	Network Address	Client Type	Connected
Administrator	Administrator	10.25.224.20	Network Advisor Client	Sep 27,2010 14:58:30
Administrator	Administrator	10.25.224.20	Network Advisor Client	Oct 02,2010 14:00:29

FIGURE 18 Active Sessions dialog box

2. Review the active session information.

   The following information displays:

   - **ID**—Displays the name of the user (for example, Administrator).
   - **Description**—Displays the description of the user (for example, Operator).
   - **Network Address**—Displays the network address of the user.
   - **Client Type**—Displays the type of Management application client.
   - **Connected**—Displays the date and time the user connected to the server.

3. Click **Close.**

Disconnecting users

To disconnect a user, complete the following steps.

1. Select **Server > Active Sessions.**

   The **Active Sessions** dialog box displays.

2. Select the user you want to disconnect and click **Disconnect.**

3. Click **Yes** on the confirmation message.

4. The user you disconnected receives the following message:

   The Client has been disconnected by *User_Name* from *IP_Address* at *Disconnected_Date_and_Time*.

5. Click **Close.**

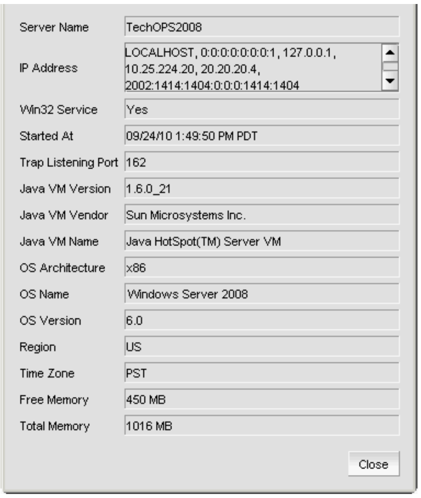
   When you disconnect a client from using the Active Sessions dialog box, the following event displays in the Master Log: Disconnect Client *User_Name* @ *IP_Address*.

Viewing server properties

To view the Management application server properties, complete the following steps.

1. Select **Server > Server Properties**.

   The **Server Properties** dialog box displays.



Server Name	TechOPS2008
IP Address	LOCALHOST, 0:0:0:0:0:0:0:1, 127.0.0.1, 10.25.224.20, 20.20.20.4, 2002:1414:1404:0:0:0:1414:1404
Win32 Service	Yes
Started At	09/24/10 1:49:50 PM PDT
Trap Listening Port	162
Java VM Version	1.6.0_21
Java VM Vendor	Sun Microsystems Inc.
Java VM Name	Java HotSpot(TM) Server VM
OS Architecture	x86
OS Name	Windows Server 2008
OS Version	6.0
Region	US
Time Zone	PST
Free Memory	450 MB
Total Memory	1016 MB

FIGURE 19 Server Properties dialog box

2. Click **Close**.

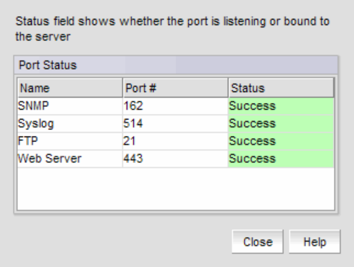
Viewing port status

You can view the port status for the following ports: FTP, SNMP, Syslog, and Web Server.

To view the port status, complete the following steps.

1. Click the port status icon ( ).

   The **Port Status** dialog box displays.



Status field shows whether the port is listening or bound to the server

Port Status

Name	Port #	Status
SNMP	162	Success
Syslog	514	Success
FTP	21	Success
Web Server	443	Success

FIGURE 20 Port Status dialog box

   The status options are as follows:

   - Success—The port is listening or bound to the server.
   - Failed—The port fails to listen or bind to the server.
   - Disabled (FTP port only)—only displays when the FTP server is external. This is considered a normal status.

2. Click **Close**.

Supported open source software products

Table 5 lists the open source software third-party software products used in this release.

TABLE 5 Supported Open Source Software Third-party Software Products

Open Source Software	License Type
7-ZipLZMASDK 4.65	public domain
Abator 1.1	Apache License v2.0
ApacheAnt 1.7.1	Apache License v2.0
ApacheCommonsBeanUtils 1.8.1	Apache License v2.0
ApacheCommonsCodec 1.4	Apache License v2.0
ApacheCommonsCollections 3.2.1	Apache License v2.0
ApacheCommonsCompress 1.0	Apache License v2.0
ApacheCommonsConfiguration 1.6	Apache License v2.0
ApacheCommonsDBCP 1.2.2	Apache License v2.0
ApacheCommonsDigester 2.0	Apache License v2.0
ApacheCommonsDiscovery 0.4	Apache License v2.0
ApacheCommonsFileUpload 1.2.1	Apache License v2.0
ApacheCommonsHTTPClient 3.1	Apache License v2.0
ApacheCommonsIO 1.4	Apache License v2.0
ApacheCommonsJXPath 1.3	Apache License v2.0
ApacheCommonsLang 2.4	Apache License v2.0
ApacheCommonsLogging 0.4	Apache License v2.0
ApacheCommonsMath 2.0	Apache License v2.0
ApacheCommonsNet 2.0	Apache License v2.0
ApacheCommonsPool 1.5.4	Apache License v2.0
ApacheCommonsValidator 1.3.1	Apache License v2.0
Apache Extras Companion for Apache log4j 1.1	Apache License v2.0
ApacheFTPServer 1.0.3	Apache License v2.0
Apache Log4j 1.2.16	Apache License v2.0
ASM 3.2	Custom License
Axis 1.4	Apache License v2.0
AXL Radius Client API 3.29	AXL Radius Client License
BeanScriptingFramework 2.4.0	Apache License v2.0
BeanShell 2.0b4	Sun Public License / Gnu Lesser Public License
BouncyCastleCryptoProvider 1.45	Bouncy Castle License
CastorBindingFramework 0.9.9.1	Apache License v2.0
DNSJava 2.0.7	BeanShell Software License

TABLE 5 Supported Open Source Software Third-party Software Products (Continued)

Open Source Software	License Type
dom4j 1.6.1	dom4j License
EnterpriseDTFTP 1.5.6	LGPL
GlazedLists 1.8.0	LGPL or MPL
GoogleGuice 1.0	Apache
HPInsightSoftwareVCEMWebClientSDK 6.2	HP SOFTWARE DEVELOPMENT KIT LICENSE AGREEMENT
HornetQ 2.0.0	Apache License v2.0
iBATISDAOFramework 2.2.0	Apache
iBatisforJava 2.3.4	Apache License v2.0
Infinispan 4.0.0 FINAL	LGPL v2.1
InstallAnywhere 2008	Commercial
Ireasoning SNMP API 4.0	IREASONING
iTextJavaPDFLibrary 2.1.7	Affero General Public License
JasperReports 3.6.1	GNU Lesser General Public License version 3
JavaCIFSClientLibrary 1.3.12	LGPL v2.1
JavaServiceWrapper 3.3.9	Custom License
JavaTar2.5andTarTool1.4	public domain
JaxenXpathLibrary 1.1.1	Jaxen License
JbcParser 3.7	Math Parser License
JBossApplicationServer 5.1.0 GA	LGPL
JBossWeb 2.1.9	GNU Lesser General Public License version 3
JCalendar 1.3.3	LGPL v2.1
JCommon 1.0.16	LGPL v2.1
JDOM 1.1.1	Apache Style
JFreeChart 1.0.13	LGPL v2.1
JGoodiesForms 1.2.1	BSD
JGoodiesLooks 2.2.2	BSD
JGraph 5.13.0.1	BSD Style
JIDE 2.10.1	JIDE Software License
Jmesa 2.4.5	Apache
JSON-RPCJava 1.0.1	Apache License v2.0
KajabityTools 0.1	Apache License v2.0
L2Fprod.comCommonComponents 7.3	Apache License v2.0
MaverickJavaSSHAPI 1.4.25	SSH Tools License
MimeTypeDetectionUtility 2.1.2	Apache License v2.0
MyBatisPersistenceFrameworkandSchhemaMigrationsforJava 3.0.2 GA	Apache License v2.0

TABLE 5 Supported Open Source Software Third-party Software Products (Continued)

Open Source Software	License Type
OpenSAML 2.3.0	Apache License v2.0
OpenSSLforLinux 1.0.0a	OpenSSL License
PostgreSQL 8.4.3	PostgreSQL License
QualityFirstLibrary 0.99.0	Mozilla License V1.1 and qflib License
Quartz Enterprise Job Scheduler 1.66	Apache License v2.0
RockSawRawSocketLibrary 1.0.0	Apache License v2.0
SafeNet Sentinel Caffe 1.6.1	SafeNet License
SafeNet Sentinel RMS SDK 8.2.2	SafeNet License
SimpleLoggingFacadeforJava 1.5.8	SLF4J License
SunJavaRuntimeEnvironment 1.6.0_21	Commercial
TableLayout 2009-06-10	Custom License
VIJavaAPI 2.1	BSD License
WBEM Solutions J WBEM Server 3.4.4	Commercial
WebNMSSNMPAPI 4.0.6	WebNMS License
XML RPC 1.2-B1	Open Source
YourKitJavaProfiler 9.5.1	YourKit License

SAN feature-to-firmware requirements

Use the following table to determine whether the Management application SAN features are only available with a specific version of the Fabric OS firmware, M-EOS firmware, or both, as well as if there are specific licensing requirements.

Feature	Fabric OS	M-EOS
Access Gateway (AG)	AG connected to Fabric OS devices requires firmware 5.2 or later.	AG connected to M-EOS devices requires firmware 9.6 or later.
Call Home (Trial and Licensed version Only)	Requires Fabric OS 5.2 or later for supportSave. Requires Fabric Watch license for SNMP traps.	Requires M-EOS and M-EOSn 9.6.X or later.
Configuration Management	Requires Fabric OS 5.3 or later	
Discovery	Requires Fabric OS 5.0 or later for the seed switch in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later for the seed switch in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS 9.9.2 or later for the seed switch in a pure M-EOS fabric. Requires M-EOS and M-EOSn 9.6.X or later for discovery.
Encryption (Trial and Licensed version Only)	Requires Fabric OS 6.1.1_enc or 6.2 or later.	Not available.
Enhanced Group Management (Trial and Licensed version Only)	Requires Enhanced Group Management license.	Not available.
Fault Management	Requires Fabric OS 4.4 or later for SNMP traps	Requires M-EOS and M-EOSn 9.6.X or later.
Fabric Binding (Trial and Licensed version Only)	Requires Fabric OS 5.2 or later in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS and M-EOSn 9.6.X or later.
FCIP Management	Requires Fabric OS 5.1 or later to modify. Requires Fabric OS 5.3 or later for FCIP tunnels. Requires FCIP license. Requires Fabric OS 6.0 or later to enable the FICON Emulation tab on the FCIP Tunnel Advanced Settings dialog box.	Not available.
FCoE Management	Requires FCoE license on the device. Requires Fabric OS version v6.1.2_CEE or later.	Not available.
FICON (Trial and Licensed version Only)	Requires Fabric OS 5.2 or later for cascaded FICON. Requires Fabric OS 6.0 or later for advanced FICON. Requires Fabric OS 6.1.1 or later to configure multiple Allow/Prohibit matrices. Requires FICON CUP license to allow CUP management features.	Only supports cascaded FICON configuration for mixed fabrics.
Firmware Management	Requires Fabric OS 5.0 or later. Requires Fabric OS 6.1.1 or later on 8G devices. Requires Enhanced Group Management license to perform group actions.	Firmware download is only available through the Element Manager.
High Integrity Fabric	Requires Fabric OS 5.2 or later in a pure Fabric OS fabric. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric.	Requires M-EOS and M-EOSn 9.6.X or later.

Feature	Fabric OS	M-EOS
Meta SAN	Requires Fabric OS 5.2 or later for FC router and router domain ID configuration. Requires Fabric OS 6.0 or later in a mixed Fabric OS and M-EOS fabric. Requires Integrated Routing license.	Not available.
Performance	Requires Fabric OS 5.0 or later for FC_ports, end-to-end monitors, and marching ants. Requires Fabric OS 5.3 or later for GE_ports and FCIP tunnels. Requires Fabric OS 6.2 or later for Top Talkers. Requires Advanced Performance Monitoring (APM) license for end-to-end monitoring and Top Talkers. Requires Enhanced Group Management license for HIstorical graphs and tables. Requires Fabric Watch license for Performance thresholds.	Requires M-EOS and M-EOSn 9.6.X or later for FC_ports and marching ants.
Port Fencing (Trial and Licensed version Only)	Requires Fabric OS 6.2 or later. Requires Fabric OS 6.3 or later for State Change and C3 Discard Frames violation types.	Requires M-EOS and M-EOSn 9.6.X or later.
Security Management	Requires Fabric OS 5.2 and later for SCC Policy. Requires Fabric OS 5.2 and later for DCC Policy. Requires Fabric OS 5.3 and later for IP Filter Policy. Requires Fabric OS 6.0 and later for AD/LDAP Server Configuration. Requires Fabric OS 5.0 and later for RADIUS Server Configuration.	Not available.
Technical Support Data Collection	Requires Fabric OS 5.2 or later.	Data collection support is only available through the Element Manager.
Troubleshooting and Diagnostics	Requires Fabric OS 5.2 or later.	Not available.
Virtual Fabrics (Trial and Licensed version Only)	Requires at least one Virtual Fabrics-enabled physical chassis running Fabric OS 6.2 or later.	Virtual Fabric configuration is only available through the Element Manager.
Zoning	Requires Fabric OS 5.0 or later for pure Fabric OS fabrics. Requires Fabric OS 6.0 or later for McDATA Fabric Mode. Requires Adaptive Networking license for Quality of Service zones.	Requires M-EOS and M-EOSn 9.6.X or later for a pure M-EOS fabric and Mixed Fabrics in Interopmode 3.

Accessibility features for the Management application

Accessibility features help users who have a disability, such as restricted mobility or limited vision, to use information technology products successfully.

The following list includes the major accessibility features in the Management application:

- Keyboard shortcuts
- Look and Feel

Keyboard shortcuts

You can use the keystrokes shown in the table below to perform common functions.

NOTE
To open a menu using keystrokes, press ALT plus the underlined letter. To open a submenu, open the menu, then press the key for the underlined letter (SHIFT plus letter for capitals) of the submenu option.

Menu Item or Function	Keyboard Shortcut
All Panels	F12
Collapse	CTRL + L
Command Tool	SHIFT + F4
Connectivity Map	F7
Copy	CTRL + C
Cut	CTRL + X
Delete	Delete
Delete All	CTRL +Delete
Help	F1
Internet Explorer	SHIFT + F2
Master Log	F5
FireFox	SHIFT + F1
Paste	CTRL + V
Product List	F9
Properties	Alt-Enter
Select All	CTRL + A
Show Ports	F4
SSH	Shift-F5
View Utilization	CTRL + U
Zoom In	CTRL + NumPad+
Zoom Out	CTRL + NumPad-

Look and Feel

You can configure the Management application to mimic your system settings as well as define the size of the font.

'Look' refers to the appearance of graphical user interface widgets and 'feel' refers to the way the widgets behave.

The Management application currently uses the '*Management_Application* Default Look and Feel' for some of the components (for example, Layout, Minimap, and so on) and the "Java Metal Look and Feel" for others.

Setting the look and feel

NOTE
Setting the look and feel is only supported on Windows systems.

The following table details the Management application components that change when you set the look and feel as well as those components that do not change.

Components Affected	Components Not Affected
All Java native components with Metal Look And Feel are affected.	The Connectivity map does not change when devices are present. You must change the theme using the map display settings (View > Map Display).
The Menu bar, Tool bar, Status bar, as well as all tables and dialog boxes are affected.	All icons and images are not affected.
Layout is affected only when it is empty.	The Minimap is not affected.

1. Select Server > Options.

   The Options dialog box displays.

2. Select Look and Feel in the Category list.
3. Choose from one of the following options:
   - Select Default to configure the look and feel back to the Management application defaults.
   - Select System to configure the Management application to have the look and feel of your system.

     This changes the look and feel for the components that use 'Java Metal Look and Feel'. For example, if you have your system display color scheme set to 'High Contrast #1', then the Management application will be set to 'High Contrast #1'. Font size of the components is not affected by theme changes.
4. Click Apply or OK to save your work.
5. Click OK on the message.

   NOTE
   Changes do not take affect until after you restart the client.

Changing the font size

The **Options** dialog box enables you to change the font size for all components including the Connectivity map of the Management application interface.

Font size changes proportionately in relation to the system resolution. For example, if the system resolution is 1024 x 768, the default font size would be 8 and large font size would be 10.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Look and Feel** in the **Category** list.
3. Select one of the following options from the **Font Size** list:
   - Select **Default** to return to the default font size.
   - Select **Small** to change the font to a smaller font size.
   - Select **Large** to change the font to a larger font size.

   NOTE
   Changing the font size to **Large** may cause the interface components (for example, text and button labels) to display incorrectly.

4. Click **Apply** or **OK** to save your work.
5. Click **OK** on the message.

   NOTE
   Changes do not take affect until after you restart the client.

Chapter

Licenses 2

In this chapter

Overview

NOTE
If your installation does not require a license key, the **License** dialog box does not display.

License keys are unique strings of alphanumeric characters that verify ownership of the Management application software as well as determine the maximum port count allowed or any additional features that you receive as part of the license.

NOTE
SAN Professional Plus Trial and Licensed version can manage up to 2560 ports and 4 Fabrics.

NOTE
SAN Enterprise Trial and Licensed version can manage up to 9000 ports and 24 Fabrics.

Managed count

The Management application audits and verifies the managed count against the maximum limit for your license under the following conditions:

- Every 3 hours from server start time. Note that you may be able to manage more products or ports than the maximum licensed limit briefly (maximum of three hours) between these periodic checks.
- When a new client logs in to the server.
- When you access the License dialog box (Help > License).

Managed SAN port count calculation

The managed port count is calculated using the following rules:

NOTE
If you exceed the maximum port count for your version, software functionality is impacted and you must reduce the port count using the Discover Fabrics dialog box or contact your vendor to purchase an additional license for your version.

1. Only counts switches discovered from the SAN tab.
2. The switch port must be licensed.
3. The ports must belong to a currently monitored fabric.
4. ICL ports are not counted.
5. The port must be a physical port (for example, VE Ports are not counted the 4 Gbps Router, Extension Switch; however, the Gbit ports are counted).
6. Access Gateway ports are counted.
7. The ports from discovered Virtual Fabrics are counted.
8. The ports from managed Fabric OS and M-EOS switches are counted.
9. The ports from unmanaged, unreachable, and missing switches are not counted.

Entering the license key

A license key is required to run the application. The key specifies the expiration date of a trial license, as well as the number of ports allowed.

NOTE
You are not required to enter a license key for a trial license. If you selected 75 Days Trial during installation, you can use the application, including all of its features, for a trial period of 75 days. At the termination of the trial period, a “license expired’ confirmation message displays. You must enter a license key to continue using the application.

Before you enter the license key you must install the application. For step-by-step instructions, refer to “Installing the Application” in the *Installation Guide*.

1. Select **Help > License.**

   The **License** dialog box displays

2. Choose from one of the following options:

   - Enter the license key in the **License Key** field.

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

   - Browse to the license file.

3. Click **Update** to extract the new license information.

   Review the new information in the **License** dialog box fields.

4. Click **OK** to set the new license on the Server.

   A message displays. Click **OK** to close the message and log off the client. To see the changes to the client, open the application and log in.

Upgrading the application

The quickest and simplest method of moving from one version to another is to enter the new license information on the **License** dialog box. The following table lists the available upgrade paths:

TABLE 6 SAN upgrade paths

Current Software Release	To Software Release
Professional Plus trial	Enterprise Trial or Licensed version
Professional Plus Licensed version	Enterprise Licensed version
Enterprise trial	Enterprise Licensed version

1. Select **Help > License.**

   The **License** dialog box displays.

2. Enter the license key (on the Key Certificate) in the **License Key** field and click **Update.**
3. Click **OK** on the message.

   The Client closes after updating the license successfully. Restart the Server through the Server Management Console for the changes to take effect.

4. Open the application (double-click the desktop icon or open from the **Start** menu).

   The **Log In** dialog box displays.

5. Enter your user name and password.

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

6. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.
7. Click **Login.**
8. Click **OK** on the **Login Banner.**

Chapter

Patches 3

In this chapter

Installing a patch

The patch installer enables you to update the Management application between releases. Each patch installer includes the previous patches within a specific release. For example, patch F (11.X.Xf) includes the upgrades in the patch installers for A (11.X.Xa) through E (11.X.Xe).

To install a patch, complete the following steps.

1. Stop all services by completing the following steps.

   a. Launch the Server Console.

   b. Click the **Services** tab.

   c. Click **Stop** to stop all services.

   NOTE
   If you perform patch upgrade while services are running, an error message displays.

2. Go to the `*Install_Home*/bin` directory.

3. Execute the patch file for your operating system:

   `patch.bat` (Windows)

   `patch.sh` (UNIX)

   The **Upgrade** dialog box displays.

4. Browse to the patch file.

   The patch zip file uses the following naming convention: dcm_<*Major_Version*><*Minor_Version*><*Revision_Number*><*Patch_Version*><*Company_Name*>.zip (for example dcm_1110a_*Company_Name*.zip).

5. Click **Upgrade**.

   If the patch process is interrupted (for example, loss of power), you must restart the patch process.

   The patch installer performs the following functions:

   - Extracts patch files to the *Install_Home* folder.
   - Creates a back up (zip) of the original files to be updated and copies the zip file to the *Install_Home*\patch-backup directory. For example, *Install_Home*\patch-backup\dcm_1110a_*Company_Name*.zip.
   - Generates a patch log.
   - Updates the conf file (*Install_Home*\conf\patch.conf) to include the patch version applied and patch created date.
   - Updates the patch version in the **About** dialog box (Select **Help** > **About** in the main window).

6. Start all services by completing the following steps.

   a. Launch the Server Console.

   b. Click the **Services** tab.

   c. Click **Start** to start all services.

Uninstalling a patch

Note that only one set of back up files are retained which enables you revert back to the previous version. You can only revert back one version. For example:

- If you upgrade from patch A to patch B, you can revert back to patch A.
- If you upgrade from patch A to patch B to patch C then to patch F, you can only revert back to patch C.

To uninstall a patch, complete the following steps.

1. Stop all services by completing the following steps.

   a. Launch the Server Console.

   b. Click the **Services** tab.

   c. Click **Stop** to stop all services.

2. Go to the *Install_Home*/patch-backup directory.

3. Extract the patch zip file (for example, dcm_1110a_*Company_Name*.zip).

4. Open the restore.xml file from the extracted files.

   The artifacts (jar files, war files, and so on) you need to replace display as separate file tags in the restore.xml file. The location of each artifact in the extracted folder is detailed in the src value under each file tag.

5. Go to the location of the first artifact (as shown in the src value under the file tag).

6. Copy the artifact from the extracted folder to the source folder in the *Install_Home*/patch-backup directory.

7. Repeat step 5 and 6 for all artifacts listed in the restore.xml folder.
8. Go to the *Install_Home*/conf directory.
9. Open the version.properties file in a text editor.
10. Change the patch version (patch.version) value to the reverted patch (for example, if you are reverting from patch F to patch C then `patch.version = c`).

    If the previous version is the initial version (no patches), change the patch version value to none (for example, `patch.version = None`).
11. Go to the *Install_Home*/patch-backup/conf directory.
12. Copy the patch.conf file in this directory to the *Install_Home*/conf directory.

    If the previous version is the initial version (no patches), delete the patch.conf file in the *Install_Home*/conf directory.
13. Start all services by completing the following steps.
    a. Launch the Server Console.
    b. Click the **Services** tab.
    c. Click **Start** to start all services.

Chapter

Discovery 4

In this chapter

SAN discovery overview

Discovery is the process by which the Management application contacts the devices in your SAN. When you configure discovery, the application discovers devices connected to the SAN. The application illustrates each device and its connections on the Connectivity Map (topology).

When you discover a fabric, the Management application checks to confirm that the seed switch is running a supported Fabric OS or M-EOS version in the fabric, and if it is not, the Management application prompts you to select a new seed switch.

NOTE
Discovery of a Secure Fabric OS fabric in strict mode is not supported.

For a Fabric OS fabric, the seed switch must be the primary Fabric Configuration Server (FCS). If you use a non-primary FCS to discover the fabric, the Management application displays an error and will not allow the discovery to proceed. If the Management application has already discovered the fabric, but afterward you create the FCS policy and the seed switch is not a primary FCS, an event is generated during the next poll.

The Management application cannot discover a fabric that is in the process of actively configuring to form a fabric. Wait until the fabric is formed and stable, then re-attempt the fabric discovery.

After fabric discovery successfully completes, all clients are updated to display the newly discovered fabric.

During fabric discovery, if you have defined IPv6 IP addresses for the switch, the Management application remembers the IP address only.

NOTE
Professional Plus edition can discover up to 4 fabrics.

NOTE
Professional Plus edition can discover, but not manage the Backbone chassis.Use the device's Element Manager, which can be launched from the Connectivity Map, to manage the device. This device cannot be used as a Seed switch.

FCS policy and seed switches

The Management application requires that the seed switch is the primary Fabric Configuration Server (FCS) switch at the time of discovery.

Setting time on the fabric will set the time on the primary FCS switch, which will then distribute the changes to other switches.

When FCS Policy is defined, ConfigDownload is allowed only from the primary FCS switch, but Management application does not check at the time of download that the switch is the primary FCS Switch.

NOTE
Switches running in Access Gateway mode cannot be used as the seed switch.

NOTE
The Backbone Chassis cannot be used as seed switch to discover and manage edge fabrics. You must discover a seed switch from each edge fabric to discover and manage the edge fabric.

NOTE
The Backbone Chassis can only discover and manage the backbone fabric.

Discovering fabrics

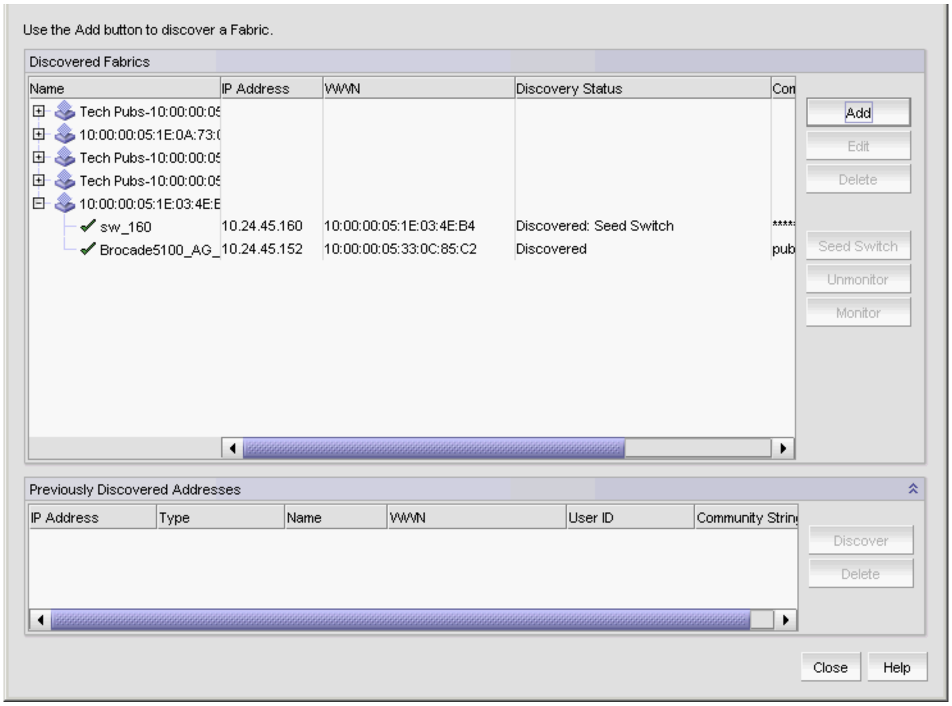
NOTE
Fabric OS devices must be running Fabric OS 5.0 or later. M-EOS devices must be running M-EOS 9.6 or later.

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

To discover specific IP addresses or subnets, complete the following steps.

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.



Use the Add button to discover a Fabric.

Discovered Fabrics

Name	IP Address	WWN	Discovery Status	Con
⊞ Tech Pubs-10:00:00:0!				
⊞ 10:00:00:05:1E:0A:73:(				
⊞ Tech Pubs-10:00:00:0!				
⊞ Tech Pubs-10:00:00:0!				
⊟ 10:00:00:05:1E:03:4E:E				
✓ sw_160	10.24.45.160	10:00:00:05:1E:03:4E:B4	Discovered: Seed Switch	*****
✓ Brocade5100_AG_	10.24.45.152	10:00:00:05:33:0C:85:C2	Discovered	pub

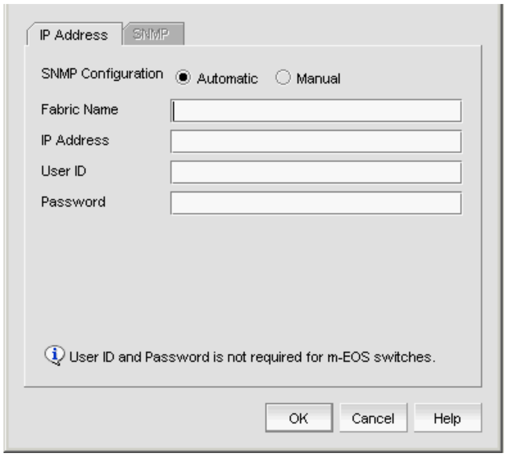
Previously Discovered Addresses

IP Address	Type	Name	WWN	User ID	Community Strin

FIGURE 21 Discover Fabrics dialog box

2. Click **Add** to specify the IP addresses of the devices you want to discover.

   The **Add Fabric Discovery** dialog box displays.



SNMP Configuration ● Automatic ○ Manual

Fabric Name

IP Address

User ID

Password

ⓘ User ID and Password is not required for m-EOS switches.

FIGURE 22 Add Fabric Discovery dialog box (IP Address tab)

3. Enter a name for the fabric in the **Fabric Name** field.
4. Enter an IP address for a device in the **IP Address** field.

   For seed switch requirements, refer to "Seed switch requirements" on page 67.

NOTE
The Backbone Chassis cannot be used as seed switch to discover and manage edge fabrics. You must discover a seed switch from each edge fabric to discover and manage the edge fabric.

NOTE
The Backbone Chassis can only discover and manage the backbone fabric.

NOTE
Professional Plus editions cannot manage the Backbone Chassis.

NOTE
Professional Plus edition can discover up to 4 fabrics.

For M-EOS devices, the Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the Operating System has IPv4 mode only or dual stack mode. The IPv6 format is valid when the Operating System has IPv6 mode only or dual stack mode.

If the firmware version is between M-EOS 9.6.X and 9.9.2, only the domain ID, WWN, and topology are obtained for fabric members. To manage other fabric members, you must enter specific IP addresses in the **Add Fabric Discovery** dialog box.

For Admin Domain (AD) discovery, Fabric OS switch must have Physical AD visibility.

For Virtual Fabric discovery device requirements, refer to "Virtual Fabrics requirements" on page 421.

To discover a Virtual Fabric device, you must have the following permissions:

- Switch user account with Chassis Admin role permission on the physical chassis.
- Switch and SNMPv3 user account with access rights to all logical switches (all Fabric IDs (1 - 128).

  For information about configuring permissions on a Fabric OS device, refer to the *Fabric OS Administrator's Guide*.:

5. (Fabric OS devices only) Enter the user ID and password for the switch in the **User ID** and **Password** fields.
6. Choose one of the following options:

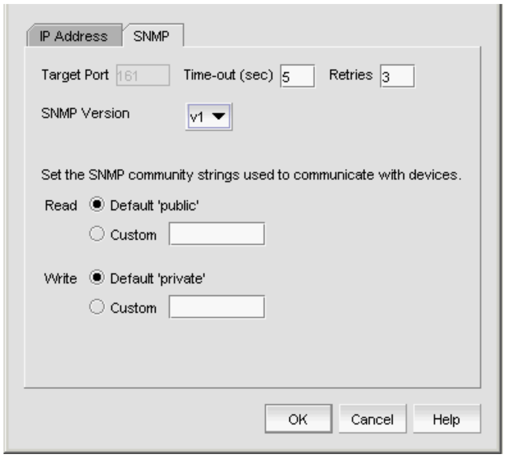
- Select the **Automatic** option to use the default SNMPv3 profile.

  The default SNMPv3 profile uses the following attributes:

Attribute	Value
Timeout	5 seconds
Retries	3
User name	snmpadmin1
Context name	None
Auth Protocol	None
Priv Protocol	None

- Select the **Manual** option to configure SNMP and complete the following steps.

  a. Click the **SNMP** tab.



Target Port 161 Time-out (sec) 5 Retries 3

SNMP Version v1

Set the SNMP community strings used to communicate with devices.

Read ● Default 'public'
○ Custom

Write ● Default 'private'
○ Custom

FIGURE 23 Add Fabric Discovery dialog box (SNMP - v1 tab)

  b. Enter the duration (in seconds) after which the application times out in the **Time-out (sec)** field.

  c. Enter the number of times to retry the process in the **Retries** field.

d. Select the SNMP version from the **SNMP Version** list.

- If you selected v1, continue with step e.
- If you select v3, the SNMP tab displays the v3 required parameters. Go to step i.

  To discover a Fabric OS device (not virtual fabric-capable), you must provide the existing SNMPv3 username present in the switch.

  To discover a Virtual Fabric device, you must configure SNMPv3 and your SNMP v3 user account must be defined as a Fabric OS switch user.

  When you discovers Virtual Fabric-enabled switch with the SNMPv3 username “admin”, which is the same as the Fabric OS switch user, the Management application automatically creates an SNMP username “admin” in the switch by replacing the sixth username.

e. Specify the **Read** option by selecting **Default ‘public’** or **Custom**.

f. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

g. Specify the **Write** option by selecting **Default ‘private’** or **Custom**.

h. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

Go to step 7.

i. If you are configuring a 256-port director, select the **Configure for** *256-Port_Director_Name* check box.

- If you selected **Configure for** *256-Port_Director_Name*, go to step m.
- If you did not select **Configure for** *256-Port_Director_Name*, continue with step j.

j. Enter a user name in the **User Name** field.

k. Enter a context name In the **Context Name** field.

l. Select the authorization protocol in the **Auth Protocol** field.

m. Enter the authorization password in the **Auth Password** field.

- If you selected **Configure for** *256-Port_Director_Name*, go to step 7.
- If you did not select **Configure for** *256-Port_Director_Name*, continue with step n.

n. Select the privacy protocol in the **Priv Protocol** field.

o. Enter the privacy password in the **Priv Password** field.

7. Click **OK** on the **Add Fabric Discovery** dialog box.

   If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays.

   a. Select the **Select** check box for each undiscovered seed switch to discover their fabrics.

   b. Click **OK** on the **Undiscovered Seed Switches** dialog box.

8. Repeat step 2 through step 7 for each fabric you want to discover.

9. Click **Close** on the **Discover Fabrics** dialog box.

Editing the password for multiple devices

You can only edit password for Fabric OS devices in the same fabric.

To edit the password for multiple devices within the same fabric, complete the following steps.

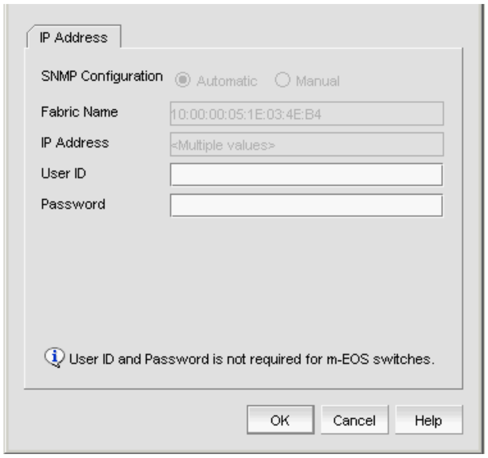
1. Select **Discover** > **Fabrics.**

   The **Discover Fabrics** dialog box displays.

2. Select multiple devices within the same fabric from the **Discovered Fabrics** table.

3. Click **Edit**.

   The *Fabric_Name* **Edit Switches** dialog box displays.



SNMP Configuration ● Automatic ○ Manual

Fabric Name 10:00:00:05:1E:03:4E:B4

IP Address <Multiple values>

User ID

Password

User ID and Password is not required for m-EOS switches.

FIGURE 24 Edit Switches dialog box

4. Enter the user ID for the switch in the **User ID** field.

5. Enter the password for the switch in the **Password** field.

6. Click **OK.** on the *Fabric_Name* **Edit Switches** dialog box.

   The **Credential Update Status** dialog box displays. This dialog box displays the status of the change on the selected devices. If you selected a logical switch, the updated credentials will be applied to the other logical switches in the same chassis.

   - **IP Address**—The IP address of the device.
   - **WWN**—The world wide name of the device.
   - **Name**—The name of the device.
   - **FID**—The fabric ID of the logical switch.
   - **Fabric Name**—The name of the fabric where device is located.
   - **Status**—The status of the update (such as Sucess, Failed, or Not Applicable).
   - **Reason**—The reason for the status for Failed or Not Applicable.
     - Failed—Not Reachable
     - Not Applicable—Credentials will not be applied for M-EOS switches

7. Click **Close.** on the **Credential Update Status** dialog box.

Configuring SNMP credentials

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.

2. Select an IP address from the **Discovered Fabrics** table.
3. Click **Edit.**

   The **Add Fabric Discovery** dialog box displays.

4. To revert to the default SNMPv3 settings, click the **Automiatic** option. Go to step 19.
5. To manually configure SNMP, select the **Manual** option. Go to step 6.
6. Click the **SNMP** tab.
7. Select the SNMP version from the **SNMP Version** list.
   - If you selected v1, continue with step 8.
   - If you select v3, the **SNMP** tab displays the v3 required parameters. Go to step 12.

     To discover a Virtual Fabric device, you must configure SNMPv3 and your SNMP v3 user account must be defined as a Fabric OS switch user.

8. Specify the **Read** option by selecting **Default 'public'** or **Custom.**
9. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.
10. Specify the **Write** option by selecting **Default 'private'** or **Custom**.

11. If you selected **Custom**, enter the community string in the **Custom** and **Confirm Custom** fields.

    Go to step 7.

12. If you are configuring a 256-Port director, select the **Configure for** *256-Port_Director_Name* check box.

    - If you selected **Configure for** *256-Port_Director_Name*, go to step 16.
    - If you did not select **Configure for** *256-Port_Director_Name*, continue with step 13.

13. Enter a user name in the **User Name** field.

14. Enter a context name In the **Context Name** field.

15. Select the authorization protocol in the **Auth Protocol** field.

16. Enter the authorization password in the **Auth Password** field.

    - If you selected **Configure for** *256-Port_Director_Name*, go to step 19.
    - If you did not select **Configure for** *256-Port_Director_Name*, continue with step 17.

17. Select the privacy protocol in the **Priv Protocol** field.

18. Enter the privacy password in the **Priv Password** field.

19. Click **OK** on the **Add Fabric Discovery** dialog box.

    If the seed switch is not partitioned, continue with step 20.

    If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays.

    a. Select the **Select** check box for each undiscovered seed switch to discover their fabrics.

    b. Click **OK** on the **Undiscovered Seed Switches** dialog box.

20. Click **Close** on the **Discover Fabrics** dialog box.

Reverting to a default SNMP community string

To revert to the default SNMP parameters, complete the following steps.

1. Select **Discover > Fabrics.**

   The **Discover Fabrics** dialog box displays.

2. Select an IP address from the **Discovered Fabrics** table.

3. Click **Edit.**

   The **Add Fabric Discovery** dialog box displays.

4. Select the **Automatic** option.

5. Click **OK** on the **Add Fabric Discovery** dialog box.

6. Click **Close** on the **Discover Fabrics** dialog box.

Removing a fabric from active discovery

If you decide you no longer want the Management application to discover and monitor a specific fabric, you can delete it from active discovery. Deleting a fabric also deletes the fabric data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a fabric from active discovery, complete the following steps.

1. Select **Discover > Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select the fabric you want to delete from active discovery in the **Discovered Fabrics** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.

   The deleted fabric displays in the **Previously Discovered Addresses** table.

5. Click **Close** on the **Discover Fabrics** dialog box.

Rediscovering a previously discovered fabric

To return a fabric to active discovery, complete the following steps.

1. Select **Discover > Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select the fabric you want to return to active discovery in the **Previously Discovered Addresses** table.
3. Click **Discover**.
4. Click **OK** on the confirmation message.

   The rediscovered fabric displays in the **Discovered Fabrics** table.

5. Click **Close** on the **Discover Fabrics** dialog box.

Deleting a fabric

To delete a fabric permanently from discovery, complete the following steps.

1. Select **Discover > Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select one or more switches that you want to delete permanently from discovery in the **Previously Discovered Addresses** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Click **Close** on the **Discover Fabrics** dialog box.

Viewing the fabric discovery state

The Management application enables you to view device status through the **Discover Setup** dialog box.

To view the discovery status of a device, complete the following steps.

1. Select **Discover** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Right-click a fabric and select **Expand All** to show all devices in the fabric.

   The **Name** field displays the discovery status icons in front of the device name. The following table illustrates and describes the icons that indicate the current status of the discovered devices.

TABLE 7 Discovery Status Icons

Icon	Description
✓	Displays when the fabric or host is managed and the management status is okay.
⚠	Displays when the switch is managed and the switch management status is not okay.
✖	Displays when the fabric or host is not managed.

The **Discovery Status** field details the actual status message text, which varies depending on the situation. The following are samples of actual status messages:

- Discovered: Seed Switch: Not registered for SNMP Traps
- Discovered: Seed Switch: Not Manageable: Not registered for SNMP Traps
- Discovered: Current seed switch is not recommended. Change Seed Switch. : Seed Switch: Not registered for SNMP Traps
- New Discovery Pending

Troubleshooting fabric discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

1. Verify IP connectivity by issuing a ping command to the switch.

   a. Open the command prompt.

   b. From the Server, type `ping` *`Switch_IP_Address`*.

2. Enter the IP address of the device in a browser to verify the http reachablity.

   For example, *http://10.1.1.11*.

M-EOSn discovery troubleshooting

The following section states a possible issue and the recommended solution for M-EOSn discovery errors.

Problem	Resolution
M-EOS seed switch discovery is not supported using SNMPv3 on the following devices: • 32-Port, 2 Gbps Switch • 16-Port, 4 Gbps Fabric Switch • 24-Port Fabric Switch • 32-Port, 4 Gbps Switch • 140-Port Director	Discover the device using SNMPv1. To configure SNMPv3 and manage the device, complete the following steps. 1 Select **Discover** > **Fabrics**. The **Discover Fabrics** dialog box displays. 2 Select an IP address from the **Discovered Fabrics** table. 3 Click **Edit**. The **Add Fabric Discovery** dialog box displays. 4 Select the **Manual** option. 5 Click the **SNMP** tab. 6 Select the v3 from the **SNMP Version** list. 7 If you are configuring a 256-Port director, select the **Configure for** *256-Port_Director_Name* check box. • If you selected **Configure for** *256-Port_Director_Name*, go to step 11. • If you did not select **Configure for** *256-Port_Director_Name*, continue with step 8. 8 Enter a user name in the **User Name** field. 9 Enter a context name In the **Context Name** field. 10 Select the authorization protocol in the **Auth Protocol** field. 11 Enter the authorization password in the **Auth Password** field. • If you selected **Configure for** *256-Port_Director_Name*, go to step 14. • If you did not select **Configure for** *256-Port_Director_Name*, continue with step 12. 12 Select the privacy protocol in the **Priv Protocol** field. 13 Enter the privacy password in the **Priv Password** field. 14 Click **OK** on the **Add Fabric Discovery** dialog box. If the seed switch is not partitioned, continue with step 15. If the seed switch is partitioned, the **Undiscovered Seed Switches** dialog box displays. a. Select the **Select** check box for each undiscovered seed switch to discover their fabrics. b. Click **OK** on the **Undiscovered Seed Switches** dialog box. 15 Click **Close** on the **Discover Fabrics** dialog box.
If a fabric is formed with a M-EOSn 256-Port Director in dual IP address mode and then dual mode is disabled, the Management application cannot discover the 256-Port Director.	Rediscover the fabric.

Virtual Fabric discovery troubleshooting

The following section state possible issues and the recommended solutions for Virtual Fabric discovery errors.

Problem	Resolution
At the time of discovery, the seed switch is Virtual Fabric-enabled; however, the user does not have Chassis Admin role for the seed switch. At the time of discovery, the user does not have the Chassis Admin role for all other switches in the fabric. After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, the user does not have Chassis Admin role.	Make sure the user account has Chassis Admin role on the Fabric OS device.
At the time of discovery, the seed switch is Virtual Fabric-enabled; however, the user does not have access to all possible logical switches (access to all possible Fabric IDs 1 - 128). At the time of discovery, the user does not have access to all possible logical switches for all other devices in the fabric. After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, the user does not have access to all possible logical switches.	Make sure the user account has access rights to all logical switches (access to all possible Fabric IDs 1 - 128) on the Fabric OS device.
At the time of discovery, SNMP v3 is not configured. At the time of discovery, SNMP v3 is not configured for all other switches in the fabric. After discovery, a device is upgraded to Fabric OS 6.2 or later and is Virtual Fabric-enabled; however, SNMP v3 is not configured	Configure the SNMP v3 information for the Virtual Fabric-enabled device.
At the time of discovery or fabric refresh, the SNMP v3 user account does not have the Chassis Admin role.	Make sure the SNMP v3 user account has the Chassis Admin role on the Fabric OS device.
At the time of discovery or refresh, the SNMP v3 user account does not have access to all possible logical switches (access to all possible Fabric IDs 1 - 128). This access is required to obtain performance statistics from all logical switches.	Make sure the SNMP v3 user account has access rights to all logical switches (access to all possible Fabric IDs 1 - 128) on the Fabric OS device.
At the time of discovery or fabric refresh, the SNMP v3 user account does not have a matching Fabric OS switch user account. This is required to obtain performance statistics from all logical switches.	Make sure the SNMP v3 user account is also defined as a Fabric OS switch user.
At the time of fabric refresh, the physical chassis is reachable; however, a previously discovered logical switch is not reachable.	The logical switch has been deleted or the Fabric ID was changed. To find a logical switch, right-click the physical chassis within the **Chassis Group** in the **Product List** and select **Logical Switches**. All logical switches on the selected physical chassis display in a list.

SAN Fabric monitoring

NOTE
Monitoring is not supported on Hosts. The upper limit to the number of HBA and CNA ports that can be monitored at the same time is 32. The same upper limit applies if switch ports and HBA ports are combined. You can select switch ports and adapter ports from a maximum of ten devices.

Fabric monitoring enables discovery of and data collection for the specified fabric and all associated devices. The Management application enables you to view fabric monitoring status through the **Discover Fabrics** dialog box. The following table illustrates and describes the icons that indicate the current status of the discovered switches.

TABLE 8 Monitor Icons

Icon	Description
✓	Displays when the switch is managed and the switch management status is okay.
⚠	Displays when the switch is managed and the switch management status is not okay.
✖	Displays when the fabric is not managed.

For Professional Plus, the default monitoring interval is 120 seconds (minimum interval is 120 seconds).

Table 6 details the default and minimum monitoring intervals used to query the monitored switches:

TABLE 9 Monitor Intervals

SAN Size	Default	Minimum
Small	120 seconds (2 minutes)	60 seconds (1 minute)
Medium	900 seconds (15 minutes)	120 seconds (2 minutes)
Large	1800 seconds (30 minutes)	180 seconds (3 minutes)

To change the monitoring interval, refer to “Configuring asset polling” on page 125.

Monitoring discovered fabrics

NOTE
Monitoring is not supported on Hosts.

To monitor a fabric and all associated devices, complete the following steps.

1. Select **Discovery** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select the fabric you want to monitor from the **Discovered Fabrics** table.
3. Click **Monitor**.

   The monitor function fails if the fabric has user-defined Admin Domains created or if the fabric is merged with another fabric already in the monitored state.

4. Click **Close** on the **Discover Fabrics** dialog box.

Stop monitoring of a discovered fabric

NOTE
Monitoring is not supported on Hosts.

When you stop monitoring of a fabric, you stop discovery of and data collection for the specified fabric and all associated devices.

To stop monitoring a fabric and all associated devices, complete the following steps.

1. Select **Discovery** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.

2. Select the fabric you want to stop monitoring from the **Discovered Fabrics** table.
3. Click **Unmonitor**.
4. Click **Close** on the **Discover Fabrics** dialog box.

SAN Seed switch

The seed switch must be running a supported Fabric OS or M-EOS version and must be HTTP-reachable.

Sometimes, the seed switch is auto-selected, such as when a fabric segments or when two fabrics merge. Other times, you are prompted (an event is triggered) to change the seed switch, such as in the following cases:

- If, during fabric discovery, the Management application detects that the seed switch is not running a supported version, you are prompted to change the seed switch.
- When one or more switches join the fabric or if the switch firmware is changed on any of the switches in the fabric, the Management application checks to make sure that the seed switch is still running a supported version. If it is not, then you are prompted to either upgrade the firmware on the seed switch or to change the seed switch to a switch running a supported firmware.

If a fabric of switches running only Fabric OS 5.X or later is created due to segmentation, the Management application continues to monitor that fabric, but if any switch with a later Fabric OS version joins the fabric, an event is triggered informing you that the seed switch is not running the latest firmware and you should change to the seed switch running the highest firmware.

ATTENTION
If a seed switch is segmented or merged, historical data such as offline zone DB, profile and reports, and Firmware Download Profile can be lost. Segmentation of a seed switch does not result in formation of a new fabric. If a merge occurs, the historical data is lost only from the second fabric.

You can change the seed switch as long as the following conditions are met:

- The new seed switch is HTTP-reachable from the Management application.
- The new seed switch is a primary FCS.
- The new seed switch is running the latest Fabric OS or M-EOS version in the fabric.

This operation preserves historical and configuration data, such as performance monitoring and user-customized data for the selected fabric.

ATTENTION
If the seed switch firmware is downgraded from Fabric OS 5.2.X to an earlier version, then all RBAC-related data is discarded from the Management application.

If, during the seed switch change, the fabric is deleted, but the rediscovery operation fails (for example, if the new seed switch becomes unreachable using HTTP), then you must rediscover the fabric again. If you rediscover the fabric using a switch that was present in the fabric before the change seed switch operation was performed, then all of the historical and configuration data is restored to the rediscovered fabric. If you rediscover the fabric using a switch that was added to the fabric after the fabric was deleted, then the historical and configuration data is lost.

If multiple users try to change the seed switch of the same fabric simultaneously, only the first change seed switch request is executed; subsequent requests that are initiated before the first request completes will fail.

If another user changes the seed switch of a fabric you are monitoring, and if you have provided login credentials for only that seed switch in the fabric, then you lose connection to the seed switch.

Seed switch requirements

Depending on your environment, you must meet the following hardware and firmware version requirements for seed switches.

Fabric OS devices:

- For Fabric OS only fabrics, the seed switch must be running Fabric OS 5.0 or later.
- For mixed fabrics (Fabric OS and M-EOS), the seed switch must be running Fabric OS 6.0 or later.

  For a complete list of all supported Fabric OS hardware, refer to "Supported hardware and software" on page xxxvii l.

M-EOS devices:

- For pure M-EOS fabrics, the seed switch must be running M-EOS 9.6.X or later.

  If the firmware version is between M-EOS 9.6.X and 9.9.2, only the domain ID, WWN, and topology are obtained for fabric members. To manage other fabric members, you must enter specific IP addresses in the **Discover Fabrics** dialog box.

  If the firmware version is M-EOS 9.9.2 or later, discovery obtains all fabric member information for all fabric members. Fabric member information includes Domain ID, WWN, IP address (IPv4 and IPv6), Firmware Version, Model, and Vendor Name. The following M-EOS devices are both seed switch-capable and allow fabric member information collection:

  - 32-Port, 4 Gbps Switch
  - 16-Port, 4 Gbps Switch
  - 140-Port Director
  - 256-Port Director

  The following M-EOS devices are seed switch-capable; however, they do not obtain fabric member information:

  - 16-Port, 1 Gbps and 2 Gbps Switch
  - 32-Port, 1 Gbps and 2 Gbps Switch
  - 24-Port, 2 Gbps Switch
  - 64-Port Director

Seed switch failover

The Management application collects fabric-wide data (such as, fabric membership, connectivity, name server information, zoning, and so on) using the seed switch. Therefore when a seed switch becomes unreachable or there is no valid seed switch, the fabric becomes unmanageable.

When the seed switch cannot be reached for three consecutive fabric refresh cycles, the Management application looks for another valid seed switch in the fabric, verifies that it can be reached, and has valid credentials. If the seed switch meets this criteria, the Management application automatically fails over to the recommended seed switch.

Note that it is possible that auto-failover may occur to a seed switch not running the latest firmware version. In this instance, any functionality which has a direct dependency on the firmware version of the seed switch is affected and restricted by the failover seed switch capabilities.

Seed switch failover to a M-EOS switch is supported in a Mixed fabric with following restrictions:

- In Interop Mode 2 Fabrics, Defined Zone information is lost and the Management application cannot push the defined zone configuration to the switch because the M-EOS device is a seed switch.
- Dynamic updates do not occur when an end device is connected or removed from Fabric OS switch. Updates only occur during the asset polling cycle. The asset polling cycle defaults are baed on SAN size (Small – 2 minutes, Medium – 15 minutes, Large – 30 minutes).
- If the firmware version is M-EOS 9.9.2 or later, discovery obtains all fabric member information for all fabric members. Fabric member information includes Domain ID, WWN, IP address (IPv4 and IPv6), Firmware Version, Model, and Vendor Name. The following M-EOS devices are both seed switch-capable and allow fabric member information collection:
  - 32-Port, 4 Gbps Switch
  - 16-Port, 4 Gbps Switch
  - 140-Port Director
  - 256-Port Director

  The following M-EOS devices are seed switch-capable; however, they do not obtain fabric member information:

  - 16-Port, 1 Gbps and 2 Gbps Switch
  - 32-Port, 1 Gbps and 2 Gbps Switch
  - 24-Port, 2 Gbps Switch
  - 64-Port Director
- Updates to Fabric OS switches (such as, Virtual Fabrics, FCR, Admin Domain, Switch Name and so on) do not occur.
- If the M-EOS switch is not seed switch capable and a switch joins the fabric, the IP address displays as ‘0.0.0.0’. You must manually edit the IP Address from the **Discover Fabrics** dialog box to manage the switch.
- Updates to firmware version and IP address of existing members do not occur.
- After failover to M-EOS switch occurs, if the Fabric OS switch becomes reachable again the Management application does not failover automatically to the Fabric OS switch. The seed switch status updates to “Current Seed switch is not recommended” in **Discover Fabrics** dialog box. You must manually change the seed switch to the Fabric OS switch using the **Change Seed Switch** dialog box. For more information, refer to “Changing the seed switch” on page 69.

Changing the seed switch

When you change the seed switch for a fabric, the Management application performs the following checks in the order they are listed:

- Identifies all switches and removes those running unsupported firmware version.
- Identifies which of the remaining switches are running the latest firmware versions.
- Filters out those switches that are not reachable.
- Identifies which switches are Virtual Fabric-enabled switches (Fabric OS only).

  If there are Virtual Fabric-enabled switches, the Management application only uses these switches as recommended seed switches. If there are no Virtual Fabric-enabled switches, continue with the next check.
- Identifies which switches are Virtual Fabric-capable devices (Fabric OS only).

  If there are Virtual Fabric-capable switches, the Management application only uses these switches as recommended seed switches. If there are no Virtual Fabric-capable switches, the Management application uses the list from the second check.

To change the seed switch, complete the following steps.

1. Select **Discovery** > **Fabrics**.

   The **Discover Fabrics** dialog box displays.
2. Select the fabric for which you want to change the seed switch from the **Discovered Fabrics** table.

   If a device joins or merges with a fabric and fabric tracking is active, you must accept changes to the fabric before the new devices display in the **Seed Switch** dialog box. For more information about fabric tracking, refer to “Fabric tracking” on page 134.
3. Click **Seed Switch.**

   If the fabric contains other switches that are running the latest version and are also HTTP-reachable from the Management application, the **Seed Switch** dialog box appears. Otherwise, a message displays that you cannot change the seed switch.
4. Select a switch to be the new seed switch from the **Seed Switch** dialog box.

   You can select only one switch. Only switches that are running the latest Fabric OS version in the fabric are displayed. The current seed switch is not displayed in this list.
5. Click **OK** on the **Seed Switch** dialog box.

   If you are not already logged in to the seed switch, the **Fabric Login** dialog box displays.

   If you are successfully authenticated, the fabric is deleted from the Management application without purging historical data, and the same fabric is rediscovered with the new seed switch.
6. Click **Close** on the **Discover Fabrics** dialog box.

Host discovery

The Management application enables you to discover individual hosts, import a group of Host from a comma separated values (CSV) file, or import all hosts from discovered fabrics or VM managers.

NOTE
Host discovery requires HCM Agent 2.0 or later.

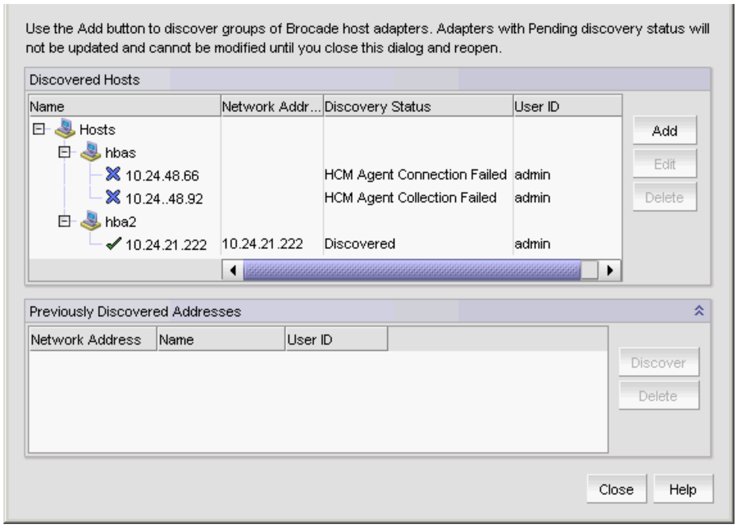
NOTE
SMI and WMI discovery are not supported.

Discovering Hosts by Network address or host name

To discover a Host by Network address or host name, complete the following steps.

1. Select **Discover** > **Host Adapters**.

   The **Discover Host Adapters** dialog box displays.



Use the Add button to discover groups of Brocade host adapters. Adapters with Pending discovery status will not be updated and cannot be modified until you close this dialog and reopen.

Discovered Hosts

Name	Network Addr...	Discovery Status	User ID
⊟ Hosts			
⊟ hbas			
✗ 10.24.48.66		HCM Agent Connection Failed	admin
✗ 10.24..48.92		HCM Agent Collection Failed	admin
⊟ hba2			
✓ 10.24.21.222	10.24.21.222	Discovered	admin

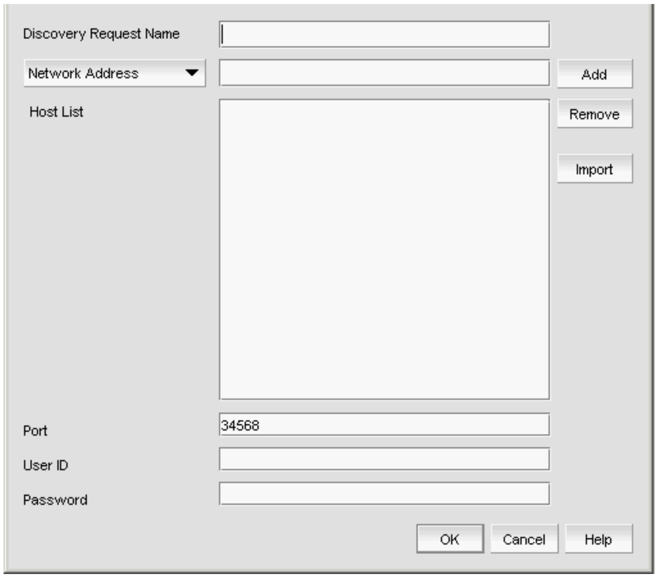
Previously Discovered Addresses

Network Address	Name	User ID

FIGURE 25 Add Host Adapters dialog box

2. Click **Add**.

   The **Add Host Adapters** dialog box displays.



34568

FIGURE 26 Add Host Adapters dialog box

3. (Optional) Enter a discovery request name (such as, Manual 06/12/2009) in the **Discovery Request Name** field.
4. Select **Network Address** from the list.
5. Enter the IP address (IPv4 or IPv6 formats) or host name in the **Network Address** field.
6. Click **Add**.

   The IP address or host name of the Host displays in the **Host List**.
7. Configure Host credentials, if necessary.
   a. Enter the HCM Agent port number in the **Port** field.
   b. Enter your username in the **User ID** field.
   c. Enter your password **Password** field.
8. Repeat step 5 through step 7 for each Host you want to discover.
9. Click **OK** on the **Add Host Adapters** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.
10. Click **Close** on the **Discover Host Adapters** dialog box.

Importing Hosts from a CSV file

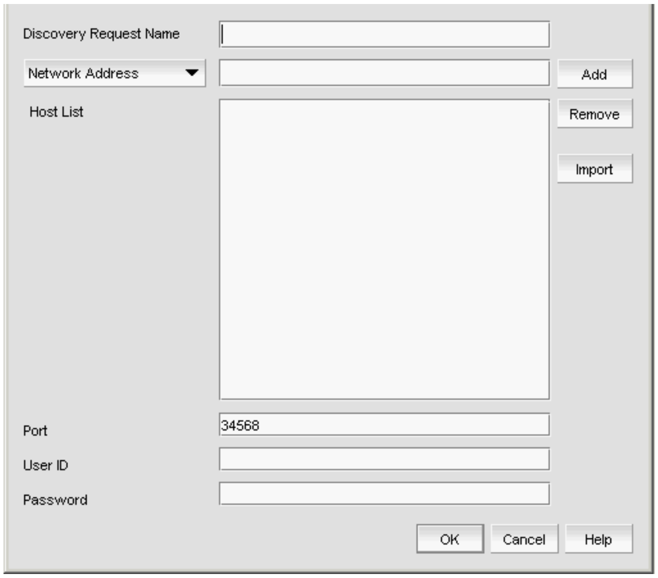
To discover Hosts by importing a CSV file, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Click **Add**.

   The **Add Host Adapters** dialog box displays.



Discovery Request Name

Port: 34568

User ID

Password

FIGURE 27 Add Host Adapters dialog box

3. Click **Import**.

   The **Open** dialog box displays.

4. Browse to the CSV file location.

   The CSV file must meet the following requirements:

   - Comma separated IP address or host names
   - No commas within the values
   - No escaping supported

     For example, XX.XX.XXX.XXX, XX.XX.X.XXX, computername.company.com

5. Click **Open**.

   The CSV file is imported to the **Add Host Adapters** dialog box. During import, duplicate values are automatically dropped. When import is complete, the imported values display in the **Host List**. If the file cannot be imported, an error displays.

6. Verify the imported values in the **Host List** .

7. Configure Host credentials, if necessary.
   a. Enter the HCM Agent port number in the Port field.
   b. Enter your username in the User ID field.
   c. Enter your password Password field.
8. Click OK on the Add Host Adapters dialog box.

   If an error occurs, a message displays. Click OK to close the error message and fix the problem.

   A Host Group displays in Discovered Hosts table with pending status. To update the status from pending you must close and reopen the Discover Host Adapters dialog box.
9. Click Close on the Discover Host Adapters dialog box.

Importing Hosts from a Fabric

To discover a Host from a discovered fabric, complete the following steps.

1. Select Discover > Host Adapters.

   The Discover Host Adapters dialog box displays.
2. Click Add.

   The Add Host Adapters dialog box displays.

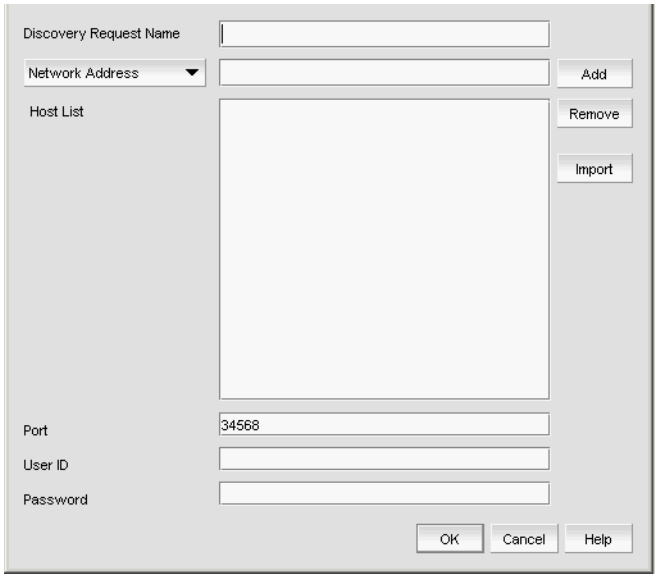

Port: 34568

FIGURE 28 Add Host Adapters dialog box

3. Enter a discovery request name (such as, MyFabric) in the Discovery Request Name field.
4. Select Hosts in Fabrics from the list.
5. Select All fabrics or an individual fabric from the list.

6. Click **Add**.

   All hosts which are part of a managed fabric and have a registered host name display in the list. If no host with a registered host name exists, an error message displays. Click **OK** to close the error message.

7. Configure Host credentials, if necessary.

   a. Enter the HCM Agent port number in the **Port** field.

   b. Enter your username in the **User ID** field.

   c. Enter your password **Password** field.

8. Click **OK** on the **Add Host Adapters** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.

9. Click **Close** on the **Discover Host Adapters** dialog box.

Importing Hosts from a VM manager

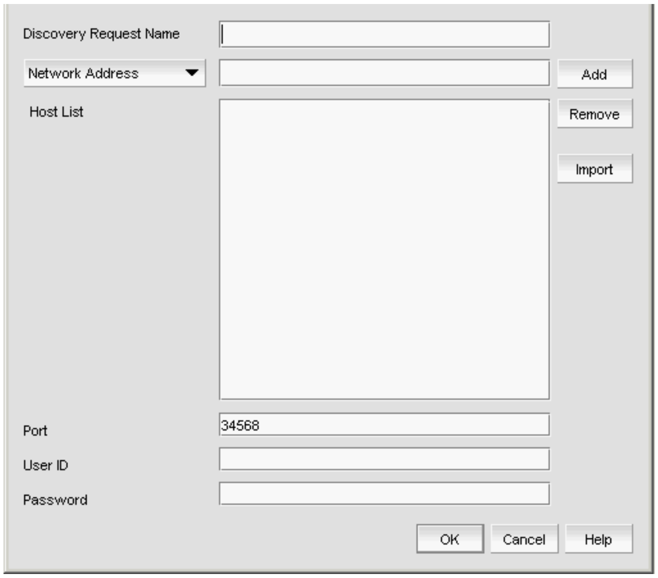
To discover Hosts from a discovered VM manager, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Click **Add**.

   The **Add Host Adapters** dialog box displays.



Port: 34568
User ID
Password

FIGURE 29 Add Host Adapters dialog box

3. Enter a discovery request name (such as, MyVMManager) in the **Discovery Request Name** field.

4. Select **Hosts from VM Manager** from the import by list.

5. Select **All VM** or an individual VM from the list.
6. Click **Add**.

   All hosts which are part of a discovered VM manager and have a registered host name display in the list. If no host with a registered host name exists, an error message displays. Click **OK** to close the error message.
7. Configure Host credentials, if necessary.
   a. Enter the HCM Agent port number in the **Port** field.
   b. Enter your username in the **User ID** field.
   c. Enter your password **Password** field.
8. Click **OK** on the **Add Host Adapters** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A Host Group displays in **Discovered Hosts** table with pending status. To update the status from pending you must close and reopen the **Discover Host Adapters** dialog box.
9. Click **Close** on the **Discover Host Adapters** dialog box.

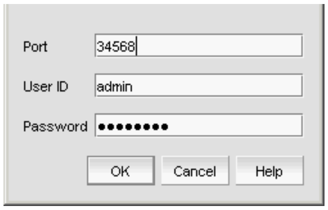
Editing Host adapter credentials

To edit Host credentials, complete the following steps.

1. Select **Discover > Host Adapters**.

   The **Discover Host Adapters** dialog box displays.
2. Select the Host in the **Discovered Hosts** list and click **Edit**.

   The **Edit Host Adapters** dialog box displays.



Port 34568

User ID admin

Password ••••••••

FIGURE 30 Edit Host Discovery dialog box

3. Enter the HCM Agent port number in the **Port** field if necessary.
4. Enter your username in the **User ID** field.
5. Enter your password **Password** field.
6. Click **OK** on the **Edit Host Adapters** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.
7. Click **Close** on the **Discover Host Adapters** dialog box.

Removing a host from active discovery

If you decide you no longer want the Management application to discover and monitor a specific host, you can delete it from active discovery. Deleting a host also deletes the host data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a host from active discovery, complete the following steps.

1. Select **Discover** > **Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to delete from active discovery in the **Discovered Hosts** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.

   The deleted host displays in the **Previously Discovered Addresses** table.

5. Click **Close** on the **Discover Host Adapters** dialog box.

Rediscovering a previously discovered fabric

To return a host to active discovery, complete the following steps.

1. Select **Discover** > **Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to return to active discovery in the **Previously Discovered Addresses** table.
3. Click **Discover**.
4. Click **OK** on the confirmation message.

   The rediscovered host displays in the **Discovered Hosts** table.

5. Click **Close** on the **Discover Host Adapters** dialog box.

Deleting a host adapter from discovery

To delete a host permanently from discovery, complete the following steps.

1. Select **Discover** > **Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Select the host you want to delete permanently from discovery in the **Previously Discovered Addresses** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Click **Close** on the **Discover Host Adapters** dialog box.

Viewing the host discovery state

The Management application enables you to view device discovery status through the **Discover Host Adapters** dialog box.

To view the discovery status of a device, complete the following steps.

1. Select **Discover** > **Host Adapters**.

   The **Discover Host Adapters** dialog box displays.

2. Right-click the Hosts node select **Expand All** to show all devices.

   The **Name** field displays the discovery status icons in front of the device name. The following table illustrates and describes the icons that indicate the current status of the discovered devices.

   TABLE 10 Discovery Status Icons

Icon	Description
✓	Displays when the fabric or host is managed and the management status is okay.
⚠	Displays when the switch is managed and the switch management status is not okay.
✖	Displays when the fabric or host is not managed.

   The **Discovery Status** field details the actual status message text, which varies depending on the situation. The following are samples of actual status messages:

   - Discovered
   - New Discovery Pending
   - Created host structure differs from discovered host; Discovery ignored
   - Brocade HBA Discovery Failed: HCM Agent connection failed
   - HCM Agent collection failed

Troubleshooting host discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

1. Verify IP connectivity by issuing a ping command to the switch.

   a. Open the command prompt.

   b. From the Server, type `ping` *`Device_IP_Address`*.

2. Enter the IP address of the device in a browser to verify the SNMP settings.

   For example, *http://10.1.1.11*.

VM Manager Discovery

The Management application enables you to discover VM managers.

NOTE
VM Manager discovery requires vCenter Server 4.0 or later.

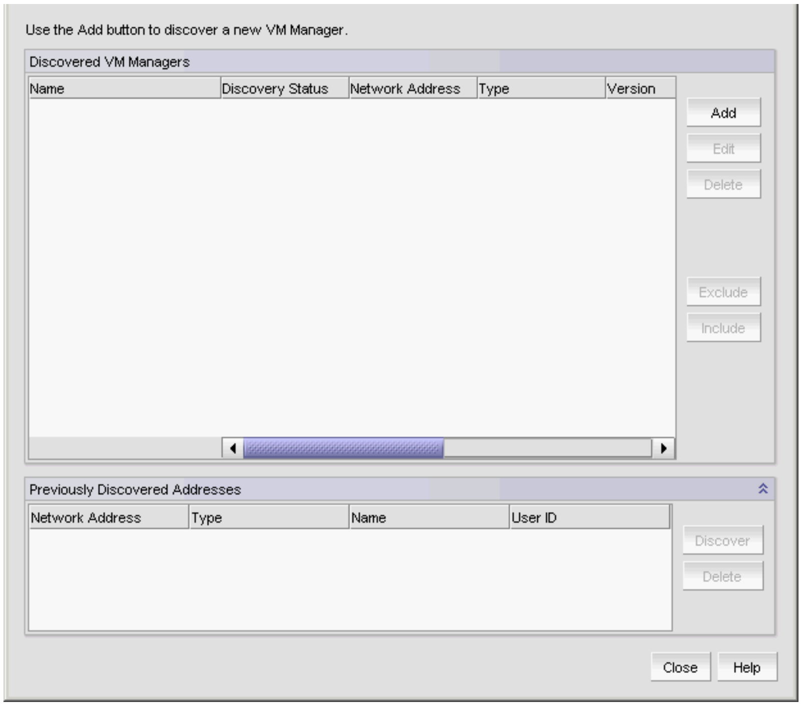
NOTE
You can discover up to 10 VM Managers.

Discovering a VM manager

To discover a VM manager, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.



Use the Add button to discover a new VM Manager.

Discovered VM Managers

Name	Discovery Status	Network Address	Type	Version

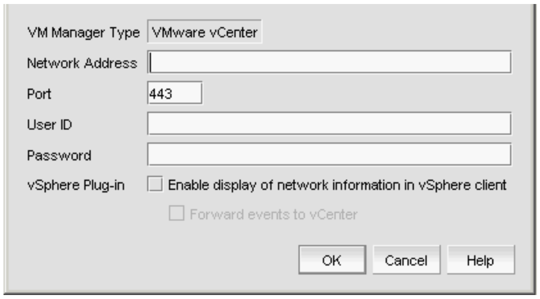
Previously Discovered Addresses

Network Address	Type	Name	User ID

FIGURE 31 Discover VM Managers dialog box

2. Click **Add**.

   The **Add VM Manager** dialog box displays.



VM Manager Type: VMware vCenter

Network Address:

Port: 443

User ID:

Password:

vSphere Plug-in: □ Enable display of network information in vSphere client

□ Forward events to vCenter

FIGURE 32 Add VM Manager dialog box

3. Enter the IP address or host name in the **Network Address** field.
4. Enter the VM manager port number in the **Port** field.
5. Enter the VM manager username in the **User ID** field.
6. Enter the VM manager password **Password** field.
7. Select the **Enable display of network information in vSphere client** check box to enable vSphere client plug-in registration.

   Clear to disable vSphere client plug-in registration.
8. Select the **Forward event to vCenter** check box to enable event forwarding from the Management application to vCenter.

   Clear to disable event forwarding.
9. Click **OK** on the **Add VM Manager** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

   A VM manager displays in **Discovered VM Managers** table with pending status. To update the status from pending you must close and reopen the **Discover VM Managers** dialog box.
10. Click **Close** on the **Discover VM Managers** dialog box.

Editing a VM manager

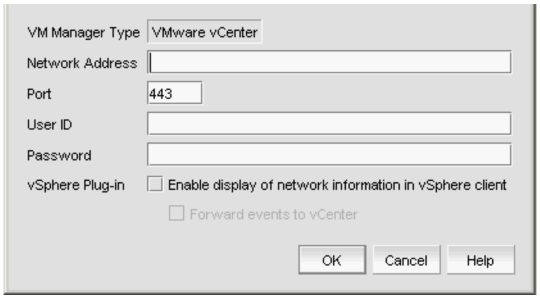
To edit VM manager discovery, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the Host in the **Discovered VM Managers** list and click **Edit**.

   The **Edit VM Manager** dialog box displays.



VM Manager Type: VMware vCenter

Network Address:

Port: 443

User ID:

Password:

vSphere Plug-in: □ Enable display of network information in vSphere client

□ Forward events to vCenter

FIGURE 33 Edit VM Manager dialog box

3. Change the VM manager port number in the **Port** field.
4. Enter the VM manager username in the **User ID** field.
5. Enter the VM manager user password **Password** field.
6. Select the **Enable display of network information in vSphere client** check box to enable vSphere client plug-in registration.

   Clear to disable vSphere client plug-in registration.

7. Select the **Forward event to vCenter** check box to enable event forwarding from the Management application to vCenter.

   Clear to disable event forwarding.

8. Click **OK** on the **Edit VM Manager** dialog box.

   If an error occurs, a message displays. Click **OK** to close the error message and fix the problem.

9. Click **Close** on the **Discover VM Managers** dialog box.

Excluding a host from VM manager discovery

To exclude host from VM manager discovery complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the Host you want to exclude in the **Discovered VM Managers** list and click **Exclude.**.
3. Click **Close** on the **Discover VM Managers** dialog box.

Including a host in VM manager discovery

To include host in VM manager discovery complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select a Host you want to include in the **Discovered VM Managers** list and click **Include.**.
3. Click **Close** on the **Discover VM Managers** dialog box.

Removing a VM manager from active discovery

If you decide you no longer want the Management application to discover and monitor a specific VM manager, you can delete it from active discovery. Deleting a VM manager also deletes the data on the server (both system collected and user-defined data) except for user-assigned names for the device port, device node, and device enclosure information.

To delete a VM manager from active discovery, complete the following steps.

1. Select **Discover > VM Managers.**

   The **Discover VM Managers** dialog box displays.

2. Select the VM manager you want to delete from active discovery in the **Discovered VM Managers** table.
3. Click **Delete.**
4. Click **OK** on the confirmation message.

   The deleted VM manager displays in the **Previously Discovered Addresses** table.

5. Click **Close** on the **Discover VM Managers** dialog box.

Rediscovering a previously discovered VM manager

To return a VM manager to active discovery, complete the following steps.

1. Select **Discover > VM Managers.**

   The **Discover VM Managers** dialog box displays.

2. Select the VM manager you want to return to active discovery in the **Previously Discovered Addresses** table.
3. Click **Discover.**
4. Click **OK** on the confirmation message.

   The rediscovered VM manager displays in the **Discovered VM Managers** table.

5. Click **Close** on the **Discover VM Managers** dialog box.

Deleting a VM manager from discovery

To delete a host permanently from discovery, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Select the VM manager you want to delete permanently from discovery in the **Previously Discovered Addresses** table.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Click **Close** on the **Discover VM Managers** dialog box.

Viewing the VM manager discovery state

The Management application enables you to view device discovery status through the **Discover VM Managers** dialog box.

To view the discovery status of a device, complete the following steps.

1. Select **Discover > VM Managers**.

   The **Discover VM Managers** dialog box displays.

2. Right-click the Hosts node select **Expand All** to show all devices.

   The **Discovery Status** field details the actual status message text, which varies depending on the situation.

   The following are samples of actual VMM status messages:

   - Active
   - Failed – Not reachable
   - Failed – Authentication failure

   The following are samples of actual ESX host status messages:

   - Active
   - Discovery pending,
   - Excluded,
   - Conflict – Existing Host <hostname>

Troubleshooting VM manager discovery

If you encounter discovery problems, complete the following checklist to ensure that discovery was set up correctly.

1. Verify IP connectivity by issuing a ping command to the switch.
   a. Open the command prompt.
   b. From the Server, type `ping` *`Device_IP_Address`*.
2. Enter the IP address of the device in a browser to verify the SNMP settings.

   For example, *http://10.1.1.11*.

Chapter

Application Configuration

5

In this chapter

Server Data backup

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

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 Management 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 data is backed up to the following directories:

- Backup\databases — contains database and log files.
- Backup\data — contains M-EOS switches Element Manager data files (including Dump files, Data collection progress files, Director/Switch firmware files FAF files, Switch technical supportSave, and Switch backup files) and Fabric OS miscellaneous files.
- Backup\conf – contains the Management application configuration files.
- Backup\cimom – contains the SMIA configuration files.

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 Management Server is backed up toD:\Backup (Windows systems) by default. If there is not second hard disk, this is a rewritable (CD-RW) compact disk. Make sure you have a CD-RW disk in the CD recorder drive to ensure that backup can occur. Critical information from the Management application is automatically backed up to the CD-RW when the data directory contents change or when you restart the Management 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

The Management server backs 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\Backup and D:\Backup\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 because it may be incomplete.

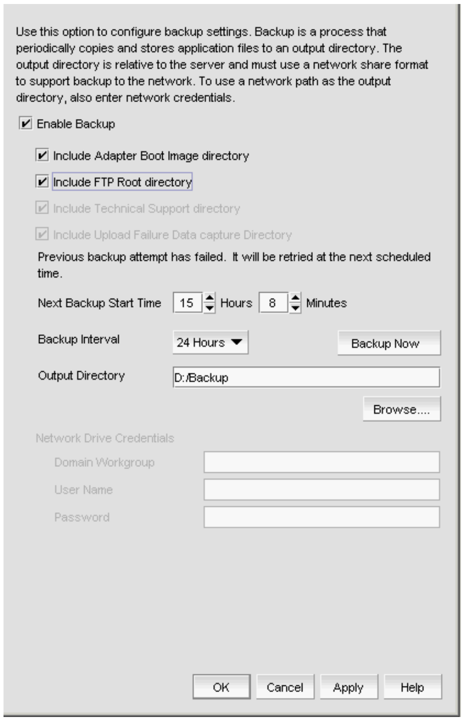
Configuring backup to a writable CD

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 Management application can no longer back up to the disc.

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

1. Select **Server** > **Options.**

   The **Options** dialog box displays (Figure 34).



Use this option to configure backup settings. Backup is a process that periodically copies and stores application files to an output directory. The output directory is relative to the server and must use a network share format to support backup to the network. To use a network path as the output directory, also enter network credentials.

☑ Enable Backup

☑ Include Adapter Boot Image directory

☑ Include FTP Root directory

☑ Include Technical Support directory

☑ Include Upload Failure Data capture Directory

Previous backup attempt has failed. It will be retried at the next scheduled time.

Next Backup Start Time 15 Hours 8 Minutes

Backup Interval 24 Hours

Output Directory D:/Backup

Network Drive Credentials

Domain Workgroup

User Name

Password

FIGURE 34 Options dialog box (Server Backup option)

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

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

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

4. Choose one or more of the following options:
   - Select the Include Adapter Boot Image directory check box.
   - Select the Include FTP Root directory check box.

     If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.
   - Select the Include Technical Support directory check box, if necessary.
   - Select the Include Upload Failure Data Capture directory check box, if necessary.
5. Enter the time (using a 24-hour clock) you want the backup process to begin in the Next Backup Start Time Hours and Minutes fields.
6. Select an interval from the Backup Interval drop-down list to set how often backup occurs.
7. 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.
8. 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.
9. 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 the Management application is installed.

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

1. Select Server > Options.

   The Options dialog box displays.
2. Select Server Backup in the Category list.

   The currently defined directory displays in the Backup Output Directory field.
3. Select the Enable Backup check box, if necessary.

4. Choose one or more of the following options:
   - Select the **Include Adapter Boot Image directory** check box.
   - Select the **Include FTP Root directory** check box.

     If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.
   - Select the **Include Technical Support directory** check box, if necessary.
   - Select the **Include Upload Failure Data Capture directory** check box, if necessary.
5. Enter the time (using a 24-hour clock) you want the backup process to begin in the **Next Backup Start Time Hours** and **Minutes** fields.
6. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
7. Browse to the hard drive and directory to which you want to back up your data.
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 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

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.

NOTE
The Management application should not directly access local or network resources through mapped drive letters. When the Management application must access a remote resource (or any process that is running in a different security context), you should use the Universal Naming Convention (UNC) name to access the resource. For more information about services and redirected drives, refer to http://support.microsoft.com/kb/180362/en-us.

NOTE
Configuring backup to a network drive is not supported on UNIX systems.

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.

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

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **Server Backup** in the **Category** list.

   The currently defined directory displays in the **Backup Output Directory** field.
3. Select the **Enable Backup** check box, if necessary.

4. Choose one or more of the following options:
   - Select the Include Adapter Boot Image directory check box.
   - Select the Include FTP Root directory check box.

     If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump, are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.
   - Select the Include Technical Support directory check box, if necessary.
   - Select the Include Upload Failure Data Capture directory check box, if necessary.
5. Enter the time (using a 24-hour clock) you want the backup process to begin in the Next Backup Start Time Hours and Minutes fields.
6. Select an interval from the Backup Interval drop-down list to set how often backup occurs.
7. Click Browse to choose the network share and directory to which you want to back up your data, or enter the network share and directory path.

   NOTE
   You must specify the directory in a network share format (for example, \\network-name\share-name\directory). Do not use the drive letter format (C:\directory).
8. If you want to configure backup to a network drive on a Windows system, complete the following steps.
   a. Enter the name of the Windows domain or workgroup in which you are defined in the Domain Workgroup field.

      NOTE
      You must be authorized to write to the network device.

   b. Enter your Windows login name in the User Name field.

   c. Enter your Windows password in the Password field.
9. 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

Backup is enabled by default. However, if it has been disabled, complete the following steps to enable the function.

1. Select **Server** > **Options**.

   The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.
3. Select the **Enable Backup** check box.
4. Click **Apply** or **OK**.

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 **Server** > **Options**.

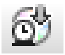
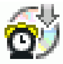
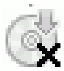
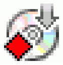
   The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.
3. Clear the **Enable Backup** check box.
4. Click **Apply** or **OK**.

Viewing the backup status

The Management application enables you to view the backup status at a glance by providing a backup status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the backup function.

TABLE 11

Icon	Description
	Backup in Progress—displays the following tooltip: “Backup started at hh:mm:ss, in progress... *XX* directories are backed up.”
	Countdown to Next Scheduled Backup—displays the following tooltip: “Next backup scheduled at hh:mm:ss.”
	Backup Disabled—displays the following tooltip: “Backup is disabled.”
	Backup Failed—displays the following tooltip: “Backup failed at hh:mm:ss mm/dd/yyyy.”

Changing the backup interval

When the backup feature is enabled, your SAN is protected by automatic backups. The backups occur every 24 hours by default. However, you can change the interval at which backup occurs.

ATTENTION
Do NOT modify the backup.properties file.

To change the backup interval, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.
3. Select an interval from the **Backup Interval** drop-down list to set how often backup occurs.
4. Click **Apply** or **OK**.

   The minimum value is 6 hours 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, right-click the **Backup** icon and select **Backup Now**.

OR

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Server Backup** in the **Category** list.
3. Click **Backup Now**.

   The backup process begins immediately. There is no confirmation message.

4. Click **Apply** or **OK**.

Reviewing backup events

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

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

The following backup events appear in the Master Log:

- Backup started
- Backup error
- Backup Enabled
- Backup Disabled
- Backup Now
- Backup destination change
- Backup interval change
- Backup start time change
- Domain workgroup change
- User name change
- User password change
- Number of files backed up on completion
- Network share access problem when backup starts or during backup (not when the backup configuration is changed)

Server Data restore

NOTE
You cannot restore data from a previous version of the Management application.

NOTE
You cannot restore data from a higher or lower configuration (Trial or Licensed version) of the Management application.

NOTE
You cannot restore data from a different package of the Management application.

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

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

- Backup\databases — contains database and log files.
- Backup\data — contains M-EOS switches Element Manager data files (including Dump files, Data collection progress files, Director/Switch firmware files FAF files, Switch technical supportSave, and Switch backup files) and Fabric OS miscellaneous files.

- Backup\conf – contains the Management application configuration files.
- Backup\cimom – contains the SMIA configuration files.

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.

Restoring data

1. (Windows) Open the **Server Management Console** from the **Start** menu on the Management application server.

   OR

   (UNIX) Open *Install_Home/bin* from the Management application server and type `./smc.sh` at the command line.

2. Click the **Services** tab.

   The tab lists the Management application services.

3. Click **Stop Services** to stop all of the services.
4. Click the **Restore** tab.
5. Browse to the backup location.

   Browse to the location specified in the **Output Directory** field on the **Options** dialog box - Backup pane.

6. Click **Restore**.

   Upon completion, a message displays the status of the restore operation. Click **OK** to close the message and the Server Management Console. For the restored data to take effect, re-launch the Configuration Wizard using the instructions in "Launching the Configuration Wizard" on page 27.

Restoring data to a new server

If your Management application server fails and you must recover information to a new server, restore the data (Refer to "Restoring data" on page 94 for complete instructions).

SAN Display

You can configure the display for FICON and reset the display to the default settings.

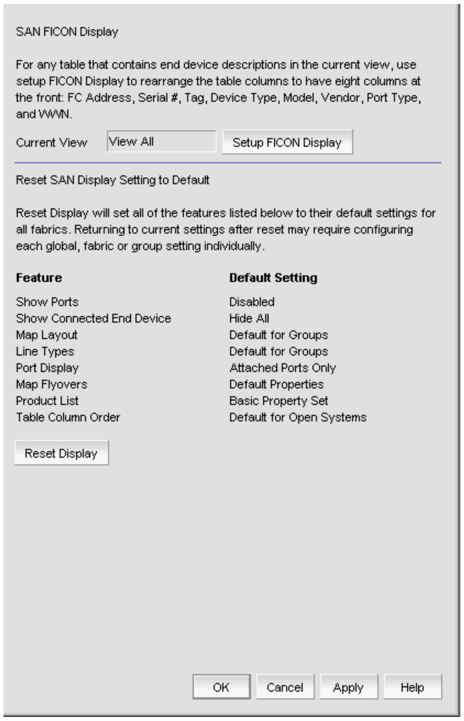
Setting your FICON display

FICON display setup rearranges the columns of any table that contains end device descriptions to move the following eight columns to be the first columns: FC Address, Serial #, Tag, Device Type, Model, Vendor, Port Type, and WWN.

To set the FICON display, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays (Figure 35).



SAN FICON Display

For any table that contains end device descriptions in the current view, use setup FICON Display to rearrange the table columns to have eight columns at the front: FC Address, Serial #, Tag, Device Type, Model, Vendor, Port Type, and WWN.

Current View: View All

Reset SAN Display Setting to Default

Reset Display will set all of the features listed below to their default settings for all fabrics. Returning to current settings after reset may require configuring each global, fabric or group setting individually.

Feature	Default Setting
Show Ports	Disabled
Show Connected End Device	Hide All
Map Layout	Default for Groups
Line Types	Default for Groups
Port Display	Attached Ports Only
Map Flyovers	Default Properties
Product List	Basic Property Set
Table Column Order	Default for Open Systems

FIGURE 35 Options dialog box (SAN Display option)

2. Select **SAN Display** in the **Category** list.
3. Click **Set Up FICON Display.**

   All tables that contain end device descriptions display the following columns as the first eight columns: FC Address, Serial #, Tag, Device Type, Model, Vendor, Port Type, and WWN.
4. Click **Apply** or **OK** to save your work.

Resetting your display

You can reset your system to display the default display settings. Note that returning to current settings after a reset may require configuring each global fabric or group setting individually. The following table (Table 12) details the settings that change with reset and the associated default state.

TABLE 12 Default Display Settings

Settings	Default State
Show port	Disabled.
Show connected end device	Set to Hide All.
Map Layout	Set to default for Groups.
Line Types	Set to default for Groups.
Port Display	Set to Attached Ports only.
Map Flyovers	Set to include the following properties: • Product Display—Name, Device Type, WWN, IP Address, and Domain ID. • Connection Display—Name (port), Address, Node WWN, Port WWN, and Port #.
Product List	Set to only display basic property list.
Table Column Order	Set to default for open system.

To reset the Management application to the default display and view settings, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays.

2. Select **SAN Display** in the **Category** list.
3. Click **Reset Display.**
4. Click **Yes** on the reset confirmation message.

   The display and view settings are immediately reset to the default display settings (as detailed in the Default display Settings table (Table 12)).

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

SAN End node display

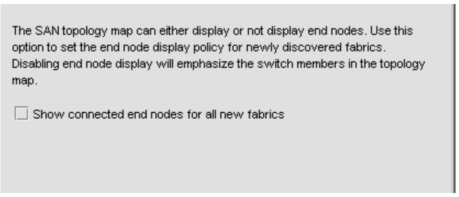
The connectivity map can be configured to display or not display end nodes. This option enables you to set the end node display for all newly discovered fabrics. Note that disabling end node display limits the connectivity map to emphasize switch members only.

Displaying end nodes

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

1. Select **Server > Options**.

   The **Options** dialog box displays (Figure 36).



The SAN topology map can either display or not display end nodes. Use this option to set the end node display policy for newly discovered fabrics. Disabling end node display will emphasize the switch members in the topology map.

□ Show connected end nodes for all new fabrics

FIGURE 36 **Options dialog box (SAN End Node Display option)**

2. Select **SAN End Node Display** in the **Category** list.
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.

SAN Ethernet loss events

An Ethernet event occurs when the Ethernet link between the Management Server and the managed SAN device is lost. You can configure the application to enable events when the Ethernet connection is lost.

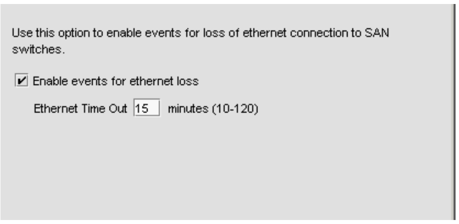
Enabling SAN Ethernet loss events

The **Options** dialog box enables you to configure the Management application to generate an Ethernet event after a device is offline for a specific period of time.

To enable Ethernet loss events, complete the following steps.

1. Select **Server > Options.**

   The **Options** dialog box displays.



Use this option to enable events for loss of ethernet connection to SAN switches.

☑ Enable events for ethernet loss

Ethernet Time Out 15 minutes (10-120)

FIGURE 37 Options dialog box (SAN Ethernet Loss Event option)

2. Select **SAN Ethernet Loss Events** in the **Category** list.
3. Select the **Enable events for ethernet loss** check box.
4. Enter the Ethernet time out value (10 to 120 minutes).
5. Click **Apply** or **OK** to save your work.

Disabling SAN Ethernet loss events

To disable Ethernet loss events, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **SAN Ethernet Loss Events** in the **Category** list.
3. Clear the **Enable events for ethernet loss** check box.
4. Click **Apply** or **OK** to save your work.

Event storage

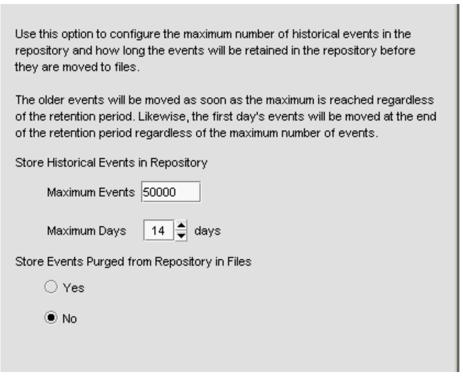
You can configure the number of historical events in the repository as well as how long the events will be retained.

Configuring event storage

To configure event storage, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays (Figure 38).



Use this option to configure the maximum number of historical events in the repository and how long the events will be retained in the repository before they are moved to files.

The older events will be moved as soon as the maximum is reached regardless of the retention period. Likewise, the first day's events will be moved at the end of the retention period regardless of the maximum number of events.

Store Historical Events in Repository

Maximum Events 50000

Maximum Days 14 days

Store Events Purged from Repository in Files

○ Yes

● No

FIGURE 38 **Options dialog box (Event Storage option)**

2. Select **Event Storage** in the **Category** list.
3. Enter the maximum number of events you want to be retained in the repository in the **Maximum Events** field.

   Depending on your installation, the maximum number of events stored are as follows:

   - Professional Plus—1 through 1,000,000
   - Enterprise—1 through 10,000,000

   Older events are purged at midnight on the date the maximum event limit is reached regardless of the retention days.
4. Enter then number of days (1 through 30) you want to store events in the **Maximum Days** field.

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

Storing historical events purged from repository

To store historical events purged from the repository, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **Event Storage** in the **Category** list.
3. Select the **Yes** option.
4. Click **OK**.

   NOTE
   Purged events from the master log table are stored in the *Install_Home*\data\archive\events directory. These files are retained for a maximum of 7 days.

Flyovers

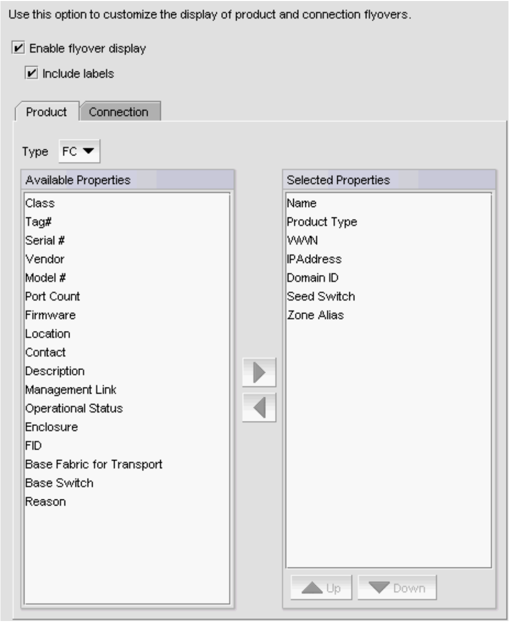
You can configure your system to display information for products and connections in a pop-up window on the Connectivity Map.

Configuring flyovers

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

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **Flyovers** in the **Category** list.
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. Select the **Product** tab (Figure 39).
6. Select the protocol type (FC or IP) and complete the following steps to select the product properties you want to display on flyover.



Use this option to customize the display of product and connection flyovers.

☑ Enable flyover display

☑ Include labels

Type FC

Available Properties

Class
Tag#
Serial #
Vendor
Model #
Port Count
Firmware
Location
Contact
Description
Management Link
Operational Status
Enclosure
FID
Base Fabric for Transport
Base Switch
Reason

Selected Properties

Name
Product Type
WWN
IPAddress
Domain ID
Seed Switch
Zone Alias

FIGURE 39 Options dialog box (Flyovers option, Product tab)

a. Select each property you want to display in the product flyover from the **Available Properties** table.

Depending on which protocol you select, some of the following properties may not be available for all protocols:

Fibre Channel (default)

- Name
- Device Type
- WWN
- IP Address
- Domain ID
- Class
- Tag#
- Serial #
- Vendor
- Model #
- Port Count
- Seed Switch
- Firmware
- Location
- Contact
- Description
- Management Link
- Operational Status
- Enclosure
- Reason
- FID
- Base Fabric for Transport
- Base Switch
- Zone Alias

IP

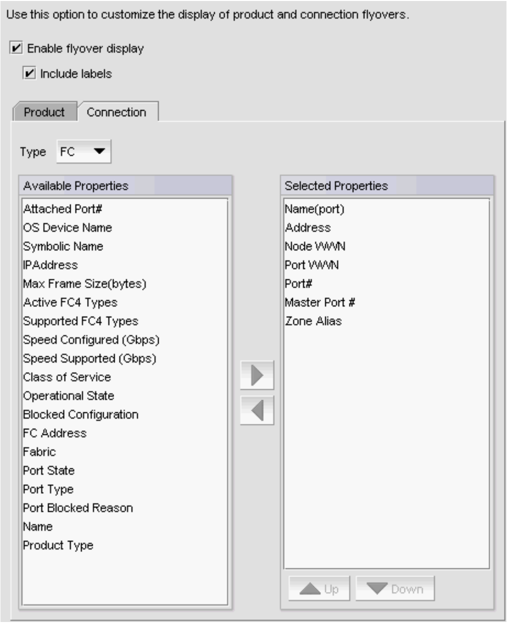
- Display Name
- IP Address

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

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

The properties displayed in the **Selected Properties** table appear in the flyover display.

7. Select the **Connection** tab (Figure 40) and complete the following steps to select the information you want to display on flyover.



Use this option to customize the display of product and connection flyovers.

☑ Enable flyover display

☑ Include labels

Type FC

Available Properties

Attached Port#
OS Device Name
Symbolic Name
IPAddress
Max Frame Size(bytes)
Active FC4 Types
Supported FC4 Types
Speed Configured (Gbps)
Speed Supported (Gbps)
Class of Service
Operational State
Blocked Configuration
FC Address
Fabric
Port State
Port Type
Port Blocked Reason
Name
Product Type

Selected Properties

Name(port)
Address
Node WWN
Port WWN
Port#
Master Port #
Zone Alias

FIGURE 40 Options dialog box (Flyovers option, Connection tab)

a. Select the protocol from the **Protocol** list.

The default protocol is Fibre Channel. Depending on which protocol you select, some properties may not be available for all protocols.

b. Select each property you want to display in the connection flyover from the **Available Properties** table.

Depending on which protocol you select, some of the following properties may not be available for all protocols:

Fibre Channel (default)

- Active FC4 Types
- Address
- Attached Port#
- Blocked Configuration
- Class of Service
- Device Type
- Fabric
- FC Address
- IP Address
- Master Port #
- Max Frame Size (bytes)
- Name
- Name (port)
- Node WWN
- Operational State
- OS Device Name
- Port #
- Port Blocked Reason
- Port State
- Port Type
- Port WWN
- Speed Configured (Gbps)
- Speed Supported (Gbps)
- Symbolic Name
- Supported FC4 Types
- Zone Alias

FCoE

- Name
- Node WWN
- MAC
- Port#
- Port Type
- FCoE Index #

IP

- *IP_Address:Port-IP_Address:Port*

c. Click the right arrow to move the selected properties to the **Selected Properties** table.

d. Use the **Move Up** and **Move Down** buttons to reorder the properties in the **Selected Properties** table.

The properties displayed in the **Selected Properties** table appear in the flyover display.

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

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

The pop-up window containing the product, port, or connection information displays.

For the product icon, the pop-up window displays the display name and IP address of the device.

For the connection, the pop-up window displays the IP address and port number for each device at either end of the connection. If one of the connections is a cloud, the port number does not display.

SAN Names

You can use Names as a method of providing familiar simple names to products and ports in your SAN. Using your Management application you can:

- Set names to be unique or non-unique.
- Fix duplicate names.
- Associate a name with a product, port WWN,or Fabric Assigned WWN currently being discovered.
- Add a WWN and an associated name for a product or port that is not yet being discovered.
- Remove or disassociate a name from a WWN.

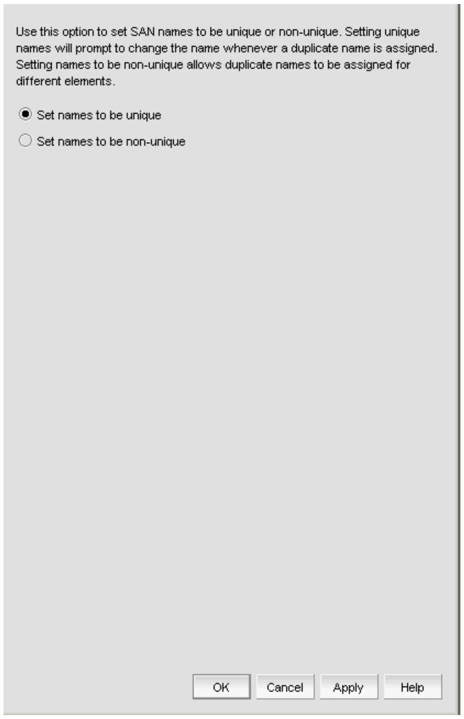
Setting names to be unique

You can edit duplicate names so that each device has a unique name. Note that the **Duplicated Names** dialog box only displays when you set names to be unique and there are duplicate names in the system.

To edit duplicate names, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays (Figure 41).



Use this option to set SAN names to be unique or non-unique. Setting unique names will prompt to change the name whenever a duplicate name is assigned. Setting names to be non-unique allows duplicate names to be assigned for different elements.

● Set names to be unique

○ Set names to be non-unique

FIGURE 41 Options dialog box (SAN Names option)

2. Select **SAN Names** in the **Category** list.
3. Select **Set names to be unique** to require that names be unique on your system.
4. Click **OK** on the **Options** dialog box.

5. Click **OK** on the “duplicate names may exist” message.
   To fix duplicated names, refer to “Fixing duplicate names” on page 105.

Setting names to be non-unique

You can choose to allow duplicate names in your fabric.

To set names to be non-unique, complete the following steps.

1. Select **Server > Options.**

   The **Options** dialog box displays.

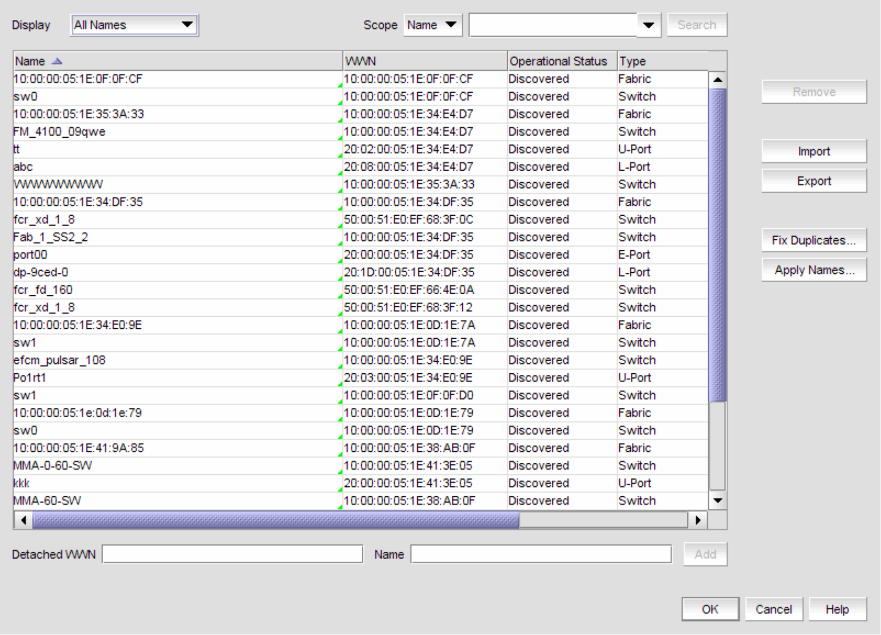
2. Select **SAN Names** in the **Category** list.
3. Select **Set names to be non-unique** to allow duplicate names on your system.
4. Click **OK** on the **Options** dialog box.

Fixing duplicate names

To fix duplicated names, complete the following steps.

1. Select **Configure > Names.**

   The **Configure Names** dialog box displays (Figure 42).



Name	WWN	Operational Status	Type
10:00:00:05:1E:0F:0F:CF	10:00:00:05:1E:0F:0F:CF	Discovered	Fabric
sw0	10:00:00:05:1E:0F:0F:CF	Discovered	Switch
10:00:00:05:1E:35:3A:33	10:00:00:05:1E:34:E4:D7	Discovered	Fabric
FM_4100_09qwe	10:00:00:05:1E:34:E4:D7	Discovered	Switch
tt	20:02:00:05:1E:34:E4:D7	Discovered	U-Port
abc	20:08:00:05:1E:34:E4:D7	Discovered	L-Port
WWWWWWWW	10:00:00:05:1E:35:3A:33	Discovered	Switch
10:00:00:05:1E:34:DF:35	10:00:00:05:1E:34:DF:35	Discovered	Fabric
fcr_xd_1_8	50:00:51:E0:EF:68:3F:0C	Discovered	Switch
Fab_1_SS2_2	10:00:00:05:1E:34:DF:35	Discovered	Switch
port00	20:00:00:05:1E:34:DF:35	Discovered	E-Port
dp-9ced-0	20:1D:00:05:1E:34:DF:35	Discovered	L-Port
fcr_fd_160	50:00:51:E0:EF:66:4E:0A	Discovered	Switch
fcr_xd_1_8	50:00:51:E0:EF:68:3F:12	Discovered	Switch
10:00:00:05:1E:34:E0:9E	10:00:00:05:1E:0D:1E:7A	Discovered	Fabric
sw1	10:00:00:05:1E:0D:1E:7A	Discovered	Switch
efcm_pulsar_108	10:00:00:05:1E:34:E0:9E	Discovered	Switch
Po1rt1	20:03:00:05:1E:34:E0:9E	Discovered	U-Port
sw1	10:00:00:05:1E:0F:0F:D0	Discovered	Switch
10:00:00:05:1e:0d:1e:79	10:00:00:05:1E:0D:1E:79	Discovered	Fabric
sw0	10:00:00:05:1E:0D:1E:79	Discovered	Switch
10:00:00:05:1E:41:9A:85	10:00:00:05:1E:38:AB:0F	Discovered	Fabric
MMA-0-60-SW	10:00:00:05:1E:41:3E:05	Discovered	Switch
kkk	20:00:00:05:1E:41:3E:05	Discovered	U-Port
MMA-60-SW	10:00:00:05:1E:38:AB:0F	Discovered	Switch

FIGURE 42 Configure Names dialog box

2. Click **Fix Duplicates.**

   The **Duplicated Names** dialog box displays.

3. Select one of the following options.
   - If you select **Append Incremental numbers for all repetitive names**, the names are edited automatically using incremental numbering.
   - If you select **I will fix them myself**, edit the name in the **Name** field.
4. Click **OK** on the **Duplicated Names** dialog box.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Viewing names

To view names associated with devices by name, complete the following steps.

1. Select **Configure** > **Names**.

   The **Configure Names** dialog box displays.
2. Select **All Names** from the **Display** list.

   Only devices with a name display. The table displays the Name, WWN, Operational Status, Type, and a Description of the device.
3. Click **OK** to close the **Configure Names** dialog box.

Adding a name to an existing device

To add a name to an existing device, complete the following steps.

1. Select **Configure** > **Names**.

   The **Configure Names** dialog box displays.
2. Select how you want to display devices from the **Display** list.

   You can display devices by **All Names**, **All WWNs**, **Fabric Assigned WWNs**, **Only Fabrics**, **Only Products**, **Only Ports**, or **Switch and N Ports**.

   All discovered devices display.
3. Select the device to which you want to assign a name in the **Display** table.
4. Double-click in the **Name** column for the selected device or port and enter a name for the device or port.

   If you set names to be unique on the **Options** dialog box and the name you entered already exists, the entry is not accepted. To search for the device already using the name, refer to "Searching for a device by name" on page 109 or "Searching for a device by WWN" on page 110 in the **Configure Names** dialog box or "Searching for a device" on page 197 in the connectivity map.

   NOTE
   If you segment a fabric, the Fabric's name follows the assigned principal switch.
5. Click **OK** on the confirmation message.
6. Click **OK** to close the **Configure Names** dialog box.

Adding a name to a new device

To add a new device and name it, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Enter the WWN of the device in the **Detached WWN** field.
3. Enter a name for the device in the **Name** field.
4. Click **Add**.

   The new device displays in the table.

   If you set names to be unique on the **Options** dialog box and the name you entered already exists, a message indicating the name already in use displays. Click **OK** to close the message and change the name.

5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Applying a name to a detached WWN

To apply a name to a detached wwn, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Click **Apply Names**.

   If there are any detached WWNs in a discovered state, the **Apply Names** dialog box displays.

3. Select or clear the check box for the associated switch or switch port.

   Select a check box to apply the detached name as the switch or switch port name and remove the duplicated WWN entry (detached) in the **Configure Names** dialog box.

   Clear a check box to remove the duplicated WWN entry (detached) in the **Configure Names** dialog box.

4. Click **OK** on the **Apply Names** dialog box.
5. Click **OK** on the **Configure Names** dialog box.

Removing a name from a device

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. In the **Display** table, select the name you want to remove.
3. Click **Remove**.

   An application message displays asking if you are sure you want clear the selected name.

4. Click **Yes**.

5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Editing names

To edit the name associated with a device, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.
2. Select **All Names** from the **Display** list.

   Only devices with a name display. The table displays the Name, WWN, Operational Status, Type, and a Description of the device.
3. Click the name you want to edit in the **Name** column.
4. Edit the name and press **Enter**.
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Exporting names

To export the names associated with devices, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.
2. Click **Export.**

   The **Export Files** dialog displays.
3. Browse to the location where you want to save the export file.

   Depending on your operating system, the default export location are as follows:

   - Desktop\My documents (Windows)
   - \root (Linux)
4. Enter a name for the file and click **Save.**
5. Click **OK** to close the **Configure Names** dialog box.

Importing Names

If the name length exceeds the limitations detailed in the following table, you must edit the name (in the CSV file) before import. Names that exceed these limits will not be imported. If you migrated from a previous version, the .properties file is located in the *Install_Home*\migration\data folder.

TABLE 13

Device	Character limit
Fabric OS switch 6.2 or later	30 (24 character limit when in FICON mode)
Fabric OS switch 6.1.X or earlier	15
Fabric OS switch port 7.0 or later	128 (24 character limit when in FICON mode)
Fabric OS switch port 6.4.X or earlier	32 (24 character limit when in FICON mode)
M-EOS switch	24
M-EOS switch port	24
HBA	256
HBA port	256
Others names	128

To import names, complete the following steps.

1. Select **Configure** > **Names**.

   The **Configure Names** dialog box displays.

2. Click **Import.**

   The **Import Files** dialog displays.

3. Browse to the import (.csv) file location.
4. Select the file and click **Import.**
5. Click **OK** to close the **Configure Names** dialog box.
6. Click **OK** on the confirmation message.

Searching for a device by name

You can search for objects (switch, fabric, product, ports, or N Ports) by name. To search for a name in the Connectivity Map, refer to “Searching for a device” on page 197.

To search by name, complete the following steps.

1. Select **Configure** > **Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.
3. Select **Name** from the **Scope** list.

4. Enter the name you want to search for in the **Search** field.

   You can search on partial names.

   NOTE
   To search for a device, the device must be discovered and display in the topology.

5. Click **Search**.

   All devices with the specified name (or partial name) are highlighted in the **Display** table. You may need to scroll to see all highlighted names.

   If the search finds no devices, a ‘no item found’ message displays.

6. Click **OK** to close the **Configure Names** dialog box.

Searching for a device by WWN

You can search for objects (switch, fabric, product, ports, or N Ports) by WWN (world wide name). To search for a WWN in the Connectivity Map, refer to “Searching for a device” on page 197.

To search by WWN, complete the following steps.

1. Select **Configure > Names**.

   The **Configure Names** dialog box displays.

2. Select **All Names** from the **Display** list.
3. Select **WWN** from the **Scope** list.
4. Enter the WWN you want to search for in the **Search** field.

   You can search on partial WWNs.

   NOTE
   To search for a device, the device must be discovered and display in the topology.

5. Click **Search**.

   All devices with the specified WWN (or partial WWN) are highlighted in the **Display** table. You may need to scroll to see all highlighted WWNs.

   If the search finds no devices, a ‘no item found’ message displays.

6. Click **OK** to close the **Configure Names** dialog box.

Security

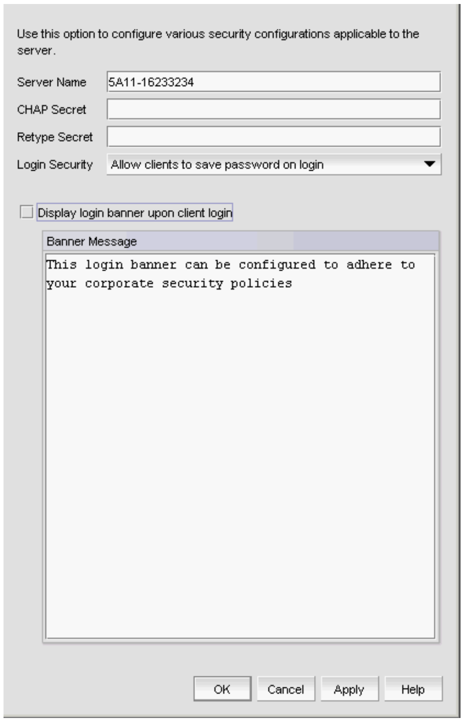
You can configure the Server Name, CHAP secret value, and login banner, and modify whether or not to allow clients to save passwords. When the login banner is enabled, each time a client connects to the server, the login banner displays with a legal notice provided by you. The client's users must acknowledge the login banner to proceed, otherwise they are logged out.

Configuring the server name

To set the CHAP secret, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays (Figure 43).



Use this option to configure various security configurations applicable to the server.

Server Name 5A11-16233234

CHAP Secret

Retype Secret

Login Security Allow clients to save password on login

□ Display login banner upon client login

Banner Message

```
This login banner can be configured to adhere to
your corporate security policies
```

FIGURE 43 Options dialog box (Security Misc option)

2. Select **Security Misc** in the **Category** list.
3. Enter the server name in the **Server Name** field.

   The **Server Name** field cannot be empty.
4. Enter a password in the **CHAP Secret** field.

   The secret must be entered as a 32-digit hexadecimal value, or as a 16-digit ASCII value preceded by a dollar sign ($), for example, $abcdefghijklmnop.

5. Re-enter the password in the **Retype Secret** field.

   If the secret does not meet the application requirements or the **CHAP Secret** and **Retype Secret** entries do not match, an error message displays. Click **OK** to re-enter the **CHAP Secret** and **Retype Secret** values.

   You are about to modify the ID/Secret of this server. Check all products that this server is managing and make sure the corresponding Software ID/Secret is updated appropriately. If you fail to do so, your server may not be able to manage the products any more.

6. Click **OK** on the confirmation message.
7. Click **Apply** or **OK** to save your work.

Setting the CHAP secret

To set the CHAP secret, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Enter a password in the **CHAP Secret** field.

   The secret must be entered as a 32-digit hexadecimal value, or as a 16-digit ASCII value preceded by a dollar sign ($), for example, $abcdefghijklmnop.

4. Re-enter the password in the **Retype Secret** field.

   If the secret does not meet the application requirements or the **CHAP Secret** and **Retype Secret** entries do not match, an error message displays. Click **OK** to re-enter the **CHAP Secret** and **Retype Secret** values.

   You are about to modify the ID/Secret of this server. Check all products that this server is managing and make sure the corresponding Software ID/Secret is updated appropriately. If you fail to do so, your server may not be able to manage the products any more.

5. Click **OK** on the confirmation message.
6. Click **Apply** or **OK** to save your work.

Configuring login security

To configure login security, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Choose one of the following options:
   - To allow users to save their password in the **Login Security** list, select **Allow clients to save password on login**.
   - To not allow users to save their password in the **Login Security** list, select **Do NOT allow clients to save password on login**.
4. Click **Apply** or **OK** to save your work.

Configuring the login banner display

To configure the login banner display, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Select the **Display login banner upon client login** check box.
4. Enter the message you want to display every time a user logs into this server in the **Banner Message** field.

   This field contains a maximum of 1024 characters.

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

Disabling the login banner

To disable the login banner display, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Security Misc** in the **Category** list.
3. Clear the **Display login banner upon client login** check box.

   NOTE
   Users logging into the client will not see the banner when logging in to this Server.

4. Click **Yes** on the confirmation message.
5. Click **Apply** or **OK** to save your work.

Syslog Registration

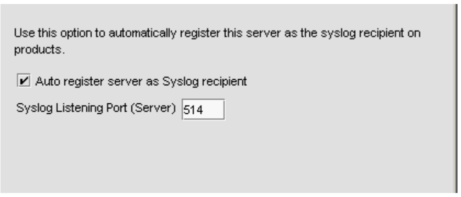
You can automatically register the server as the syslog recipient on products.

Registering a server as a Syslog recipient automatically

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Syslog Registration** in the Category pane.



Use this option to automatically register this server as the syslog recipient on products.

☑ Auto register server as Syslog recipient

Syslog Listening Port (Server) 514

FIGURE 44 Options dialog box (Trap Registration option)

3. Select the **Auto register server as Syslog recipient** check box, if necessary.

   This check box is selected by default.

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

Configuring the Syslog listing port number

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Syslog Registration** in the Category pane.
3. Enter the Syslog listening port number of the Server in the **Syslog Listening Port (Server)** field, if necessary.

   The default Syslog listening port number is 514 and is automatically populated.

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

SNMP Trap Registration

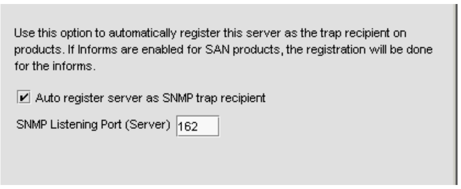
You can automatically register the server as the trap recipient on products. If SAN products have Informs enabled, the registration is for the Informs.

Registering a server as a SNMP trap recipient automatically

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Trap Registration** in the Category pane.



Use this option to automatically register this server as the trap recipient on products. If Informs are enabled for SAN products, the registration will be done for the informs.

☑ Auto register server as SNMP trap recipient

SNMP Listening Port (Server) 162

FIGURE 45 Options dialog box (Trap Registration option)

3. Select the **Auto register server as SNMP trap or informs recipient** check box, if necessary.

   This check box is selected by default.

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

Configuring the SNMP trap listing port number

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Trap Registration** in the Category pane.
3. Enter the SNMP listening port number of the Server in the **SNMP Listening Port (Server)** field, if necessary.

   The default SNMP listening port number is 162 and is automatically populated.

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

SNMP Trap Forwarding Credentials

You can configure SNMP credentials for the traps forwarded by the server.

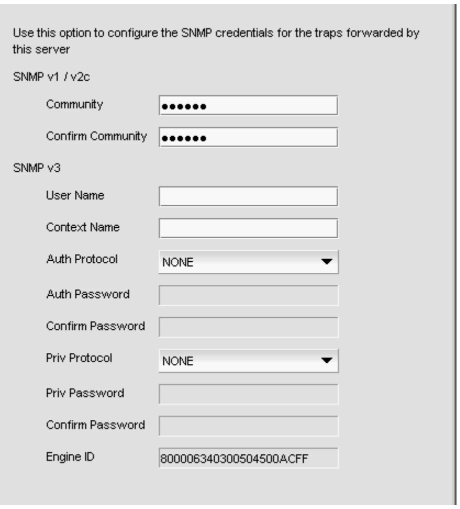
Configuring SNMP v1 and v2c credentials

To configure a SNMP v1 or v2c credentials, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Trap Forwarding Credentials** in the Category pane.



Use this option to configure the SNMP credentials for the traps forwarded by this server

SNMP v1 / v2c

Community •••••••

Confirm Community •••••••

SNMP v3

User Name

Context Name

Auth Protocol NONE

Auth Password

Confirm Password

Priv Protocol NONE

Priv Password

Confirm Password

Engine ID 800006340300504500ACFF

FIGURE 46 Options dialog box (Trap Forwarding Credentials option)

3. Enter the unique community string (case sensitive, 1 to 16 characters). in the **Community** and **Confirm Community** fields.

   Displays as asterisks. Allows all printable ASCII characters.

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

Configuring SNMP v3 credentials

To configure a SNMP v1 or v2c credentials, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Trap Forwarding Credentials** in the Category pane.

3. Enter a unique label (case sensitive, 1 to 16 characters) to identify the credentials in the **User Name** field.

   Allows all printable ASCII characters.

4. Select on of the following authentication types from the **Authentication Type** options.
   - HMAC_MD5
   - HMAC_SHA
5. Enter the SNMP v3 user name (case sensitive, 1 to 16 characters) in the **Auth Password** and **Confirm Password** fields.

   Allows all printable ASCII characters.
6. Select one of the following privacy protocol types from the **Privacy Protocol** options.
   - CBC-DES
   - CFB_AES-128
7. Enter the privacy password (case sensitive, 8 to 16 characters) in the **Priv Password** and **Confirm Password** fields.

   Displays as asterisks. Allows all printable ASCII characters.
8. Click **Apply** or **OK** to save your work.

Software Configuration

The Management application allows you to configure the following software settings:

- Client export port—A port for communication between the client and server.
- Client/Server IP—IP configuration settings.
- Memory allocation—Memory allocation for the client and server.
- Product communication—Connections between the server and SAN switches or IP products.
- FTP/SCP—Internal or external FTP server settings.
- Server port—Server port settings.
- Support mode—Support settings to allow enhanced diagnostics.

Client export port

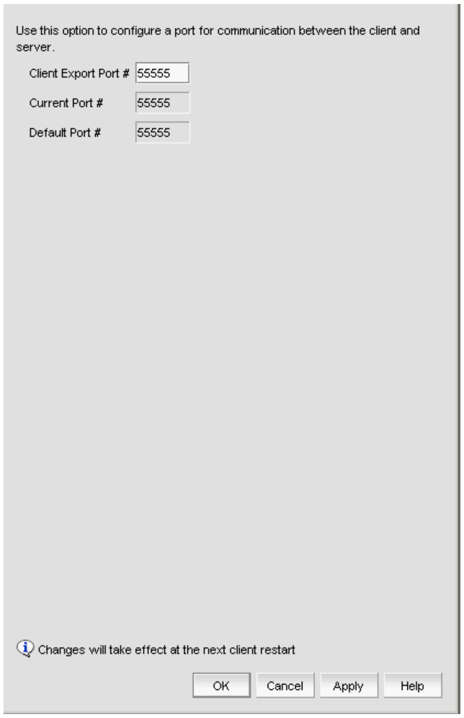
You can configure a port for communication between the client and server.

Configuring the client export port

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

1. Select **Server > Options**.

   The **Options** dialog box displays.
2. Select **Client Export Port** to assign a communications port between the client and server in the **Category** list.



Use this option to configure a port for communication between the client and server.

Client Export Port # 55555

Current Port # 55555

Default Port # 55555

Changes will take effect at the next client restart

FIGURE 47 Options dialog box (Client Export Port option)

3. Enter the client export port number to set a fixed port number for the client in the **Client Export Port** field.
4. Click **Apply** or **OK** to save your work.

NOTE
Changes to this option take effect after a client restart.

5. Click **OK** on the "changes take effect after client restart" message.

Client/Server IP

You can configure connections between the client or switches and the Management application server.

Configuring the server IP address

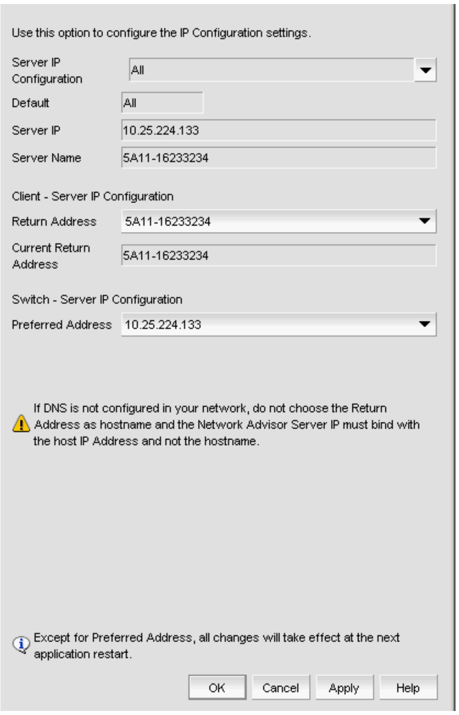
NOTE
The server binds using IPv6 address by default if your Operating System is IPv6-enabled (dual mode or IPv6 only). The server binds using IPv4 address by default if your Operating System is IPv4-enabled. Servers running in dual mode allow the client to communicate from both IPv6 and IPv4 addresses.

To configure the IP address used by the server for client-server communications, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Client/Server IP** in the **Category** list to set the IP address.



Use this option to configure the IP Configuration settings.

Server IP Configuration: All

Default: All

Server IP: 10.25.224.133

Server Name: 5A11-16233234

Client - Server IP Configuration

Return Address: 5A11-16233234

Current Return Address: 5A11-16233234

Switch - Server IP Configuration

Preferred Address: 10.25.224.133

If DNS is not configured in your network, do not choose the Return Address as hostname and the Network Advisor Server IP must bind with the host IP Address and not the hostname.

Except for Preferred Address, all changes will take effect at the next application restart.

FIGURE 48 Options dialog box (Client/Server IP option)

3. Choose one of the following options in the **Server IP Configuration** list.
   - Select **All**. Go to step 4.
   - Select a specific IP address. Continue with step 5.
   - Select **localhost**. Continue with step 5.

   When **Server IP Configuration** is set to **All**, you can select any available IP address as the **Return Address.** If you select a specific IP address, the **Return Address** list shows the same IP address and you cannot change it.
4. Select the return IP address in the **Client - Server IP Configuration Return Address** list.
5. Select the preferred IP address in the **Switch - Server IP Configuration Preferred Address** list.

   If DNS is not configured for your network, do not select the 'hostname' option from either the **Return Address** or **Preferred Address** list. Selecting the 'hostname' option prevents clients and devices from communicating with the Server.
6. Click **Apply** or **OK** to save your work.

   NOTE
   Changes to this option take effect after an application restart.

   NOTE
   You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **11.X.X** > **Server Management Console**).
7. Click **OK** on the "changes take effect after application restart" message.

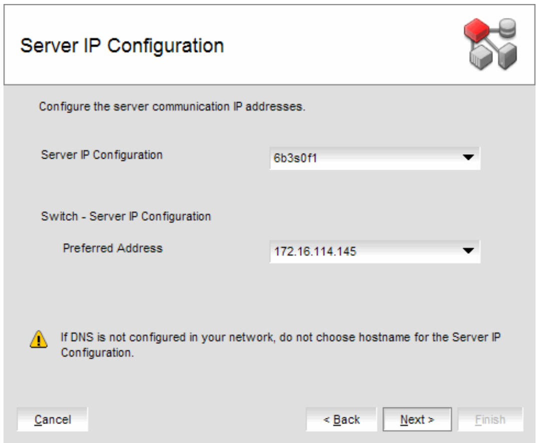
Configuring an explicit server IP address

If you selected a specific IP address from the **Server IP Configuration** screen during installation and the selected IP address changes, you will not be able to connect to the server. To connect to the new IP address, you must manually update the IP address information.

To change the IP address, complete the following steps.

1. Choose one of the following options:
   - On Windows systems, select **Start** > **Programs** > *Management_Application* **11.X.X** > *Management_Application* **Configuration**.
   - On UNIX systems, execute sh Install_Home/bin/configwizard in terminal.
2. Click **Next** on the **Welcome** screen.
3. Click **Yes** on the confirmation message.
4. Click **Next** on the **FTP Server** screen.

5. Complete the following steps on the **Server IP Configuration** screen (Figure 49).



Server IP Configuration

Configure the server communication IP addresses.

Server IP Configuration: 6b3s0f1

Switch - Server IP Configuration

Preferred Address: 172.16.114.145

If DNS is not configured in your network, do not choose hostname for the Server IP Configuration.

FIGURE 49 Server IP Configuration screen

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

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

      If DNS is not configured for your network, do not select the “hostname” option from either the **Server IP Configuration** or **Switch - Server IP Configuration Preferred Address** list. Selecting the “hostname” option prevents clients and devices from communicating with the server.

   c. Click **Next**.

6. Click **Next** on the **Server Configuration** screen.

7. Click **Next** on the **SMI Agent Configuration** screen.

8. Verify your configuration information on the **Server Configuration Summary** screen and click **Next**.

9. Click **Finish** on the **Start Server** screen.

10. Click **Yes** on the restart server confirmation message.

11. Enter your user name and password.

    The defaults are **Administrator** and **password**, respectively.

12. Click **Login**.

13. Click **OK** on the Login Banner.

Configuring the application to use dual network cards

Issues with Client-to-Server connectivity can be due to different reasons. 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.

NOTE
The server binds using IPv6 address by default if your Operating System is IPv6-enabled (dual mode or IPv6 only). The server binds using IPv4 address by default if your Operating System is IPv4-enabled. Servers running in dual mode allow the client to communicate from both IPv6 and IPv4 addresses.

To configure the IP address 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 **Server** > **Options**.

   The **Options** dialog box displays.

2. Select **Client/Server IP** in the **Category** list to set the IP address.

3. Choose one of the following options in the **Server IP Configuration** list.

   - Select **All**. Go to step 4.
   - Select a specific IP address. Continue with step 5.
   - Select **localhost**. Continue with step 5.

   When **Server IP Configuration** is set to **All**, you can select any available IP address as the **Return Address**. If you select a specific IP address, the **Return Address** field shows the same IP address and you cannot change it.

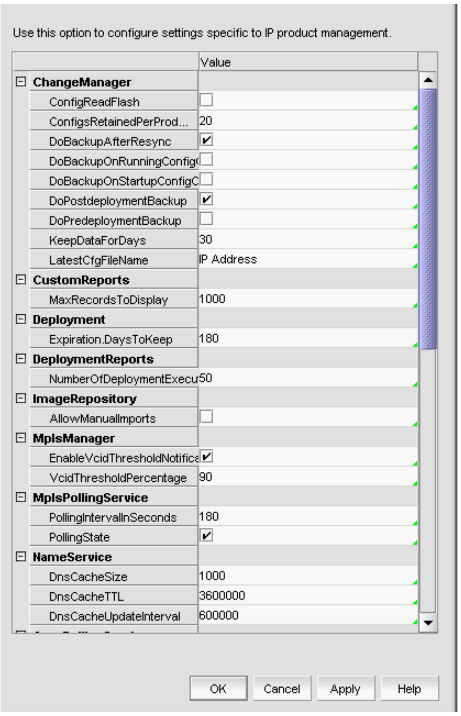
4. Select the return IP address in the **Client - Server IP Configuration Return Address** list.

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

   NOTE
   Changes take effect after you restart the Management Server.

   NOTE
   You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **11.X.X** > **Server Management Console**).

6. Click **OK** on the “changes take effect after “application restart” message.



Use this option to configure settings specific to IP product management.

	Value
⊟ **ChangeManager**	
ConfigReadFlash	☐
ConfigsRetainedPerProd...	20
DoBackupAfterResync	☑
DoBackupOnRunningConfig(	☐
DoBackupOnStartupConfigC	☐
DoPostdeploymentBackup	☑
DoPredeploymentBackup	☐
KeepDataForDays	30
LatestCfgFileName	IP Address
⊟ **CustomReports**	
MaxRecordsToDisplay	1000
⊟ **Deployment**	
Expiration.DaysToKeep	180
⊟ **DeploymentReports**	
NumberOfDeploymentExecu	50
⊟ **ImageRepository**	
AllowManualImports	☐
⊟ **MplsManager**	
EnableVcidThresholdNotifica	☑
VcidThresholdPercentage	90
⊟ **MplsPollingService**	
PollingIntervalInSeconds	180
PollingState	☑
⊟ **NameService**	
DnsCacheSize	1000
DnsCacheTTL	3600000
DnsCacheUpdateInterval	600000

FIGURE 50 Options dialog box (IP Preferences option)

Memory allocation

You can configure memory allocation for the client and server to improve performance. You can trigger switch polling when a state changes or you can poll at intervals when no state change occurs.

NOTE
SAN size is a consideration in selection of polling periods.

Configuring memory allocation settings

To configure memory allocation settings, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays.

2. Select **Memory Allocation** in the **Category** list to set the memory allocation for the server and client.

3. (Enterprise only) In the **SAN Network Size is** list, complete the following steps:

   a. Select the size of the SAN (small, medium, or large) you want to configure.

      Memory and asset polling values change to the new default values when you change the SAN Network size. You may increase these values.

      Default values for SAN only Server

      Server Heap Size

For a 32-bit Windows/Linux Server

- Small : 768 MB
- Medium : 1024 MB
- Large : 1024 MB

For a 64-bit Windows Server

- Small : 20481024 MB
- Medium : 1500 MB
- Large : 10242048 MB

Client Heap Size (for both 32 and 64-bit servers)

- Small : 512 MB
- Medium : 512 MB
- Large : 768 MB

b. Click **OK** on the confirmation message.

4. Enter the memory allocation (MB) for the client in the **Client Memory Allocation** field.

   If you enter an invalid value, an error message displays with the minimum value allowed. Click **OK** and edit the value again.

   Minimum values for SAN only are as follows:

   - Professional Plus: 512 MB
   - Enterprise Small: 512 MB
   - Enterprise Medium: 512 MB
   - Enterprise Large: 768 MB

   NOTE
   There is no restriction on the Client Heap Size value. The correct Client Heap Size value should be given according to the RAM present in the server where it is launched.

5. Enter the memory allocation (MB) for the server in the **Server Memory Allocation** field.

   If you enter an invalid value, an error message displays with the minimum value allowed. Click **OK** and edit the value again.

   Minimum values are as follows:

   For a 32-bit Windows/Linux Server

   - Professional Plus: 1024 MB
   - Enterprise Small : 768 MB
   - Enterprise Medium : 1024 MB
   - Enterprise Large : 1024 MB

   For a 64-bit Windows Server

   - Professional Plus: MB
   - Enterprise Small : 1024 MB
   - Enterprise Medium : 1500 MB
   - Enterprise Large : 2048 MB

NOTE
There is no restriction on the maximum value for Server Heap Size in a 64-Bit Server. The correct server heap size value must be given according to the RAM present in the server.

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

NOTE
Changes to this option take effect after an application restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **11.X.X > Server Management Console**).

7. Click **OK** on the “changes take effect after application restart” message.

Configuring asset polling

Asset polling allows you set the length of time between state change polling. To maximize the efficiency of the polling feature (balance the amount of possible information with any possible performance impact), base your settings on the size of the SAN.

To configure asset polling, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **Memory Allocation** in the **Category** list to set the memory allocation for the server and client.

3. Enter how often you want to check for state changes in the **Check for state change every** field.

   You cannot enter a value lower than the default minimum value.

   Default minimum values are as follows:

   - Small: 60 seconds
   - Medium: 120 seconds
   - Large: 180 seconds

4. Enter how often (default is 120 seconds) you want to check for state changes in the **If no state change, Poll switch every** field.

   Default values are as follows:

   - Small: 120 seconds
   - Medium: 900 seconds
   - Large: 1800 seconds

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

NOTE
Changes to this option take effect after an application restart.

NOTE
You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **11.X.X** > **Server Management Console**).

6. Click **OK** on the "changes take effect after application restart" message.

Product communication

You can configure connections between the switch and the Management application server.

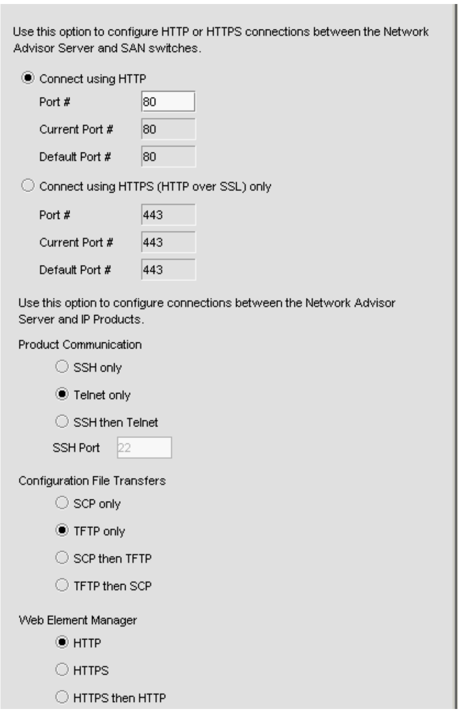
Configuring SAN communication

To configure SAN communication, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays.

2. Select **Product Communication** from the **Software Configurations list** in the **Category** pane.



Use this option to configure HTTP or HTTPS connections between the Network Advisor Server and SAN switches.

● Connect using HTTP

Port # 80

Current Port # 80

Default Port # 80

○ Connect using HTTPS (HTTP over SSL) only

Port # 443

Current Port # 443

Default Port # 443

Use this option to configure connections between the Network Advisor Server and IP Products.

Product Communication

○ SSH only

● Telnet only

○ SSH then Telnet

SSH Port 22

Configuration File Transfers

○ SCP only

● TFTP only

○ SCP then TFTP

○ TFTP then SCP

Web Element Manager

● HTTP

○ HTTPS

○ HTTPS then HTTP

FIGURE 51 Options dialog box (Product Communication option)

3. Choose one of the following options:
   - If you want to connect using HTTP, complete the following steps.
     a. Select the **Connect using HTTP** option.
     b. Enter the connection port number in the **Port #** field. Continue with step 4.
   - If you want to connect using HTTPS (HTTP over SSL), complete the following steps.
     a. Select the **Connect using HTTPS (HTTP over SSL) only** option.
     b. Enter the connection port number in the **Port #** field. Continue with step 4.
4. Click **Apply** or **OK** to save your work.

   Changes to this option take effect after an application restart.
5. Click **OK** on the “changes take effect after application restart” message.

FTP/SCP

File Transfer Protocol (FTP) is a network protocol used to transfer data from one computer to another over a TCP computer network. During installation, a built-in FTP server and its services are installed. Other FTP servers on your system are recognized by the application as external FTP servers.

For Windows systems, the built-in FTP server is the default configuration and installation starts the FTP service if port 21 is not used by any other FTP server. For UNIX systems, built-in FTP is the default for UNIX systems during installation; the external FTP server is the default only if port 21 is busy.

Note that when uninstalling the application the built-in FTP server is removed with all other services even if the FTP service is used by firmware upgrade or supportSave features.

Secure Copy (SCP) is a means of securely transferring computer files between a local and a remote host or between two remote hosts, using the Secure Shell (SSH) protocol. You must configure SCP on your machine to support Technical Support and firmware download.

Accessing the FTP server folder

Choose from one of the following options to access the FTP server folder:

- To access the internal FTP folder, select **Monitor > Techsupport > View Repository.**
- To access the external FTP folder, type the following in a browser window:
  ftp://*Username@External_FTP_Server_IP_Address*
  (for example, ftp://admin@10.1.1.1) and press **Enter**. Type your password in the pop-up window and press **Enter**. The external FTP folder displays.

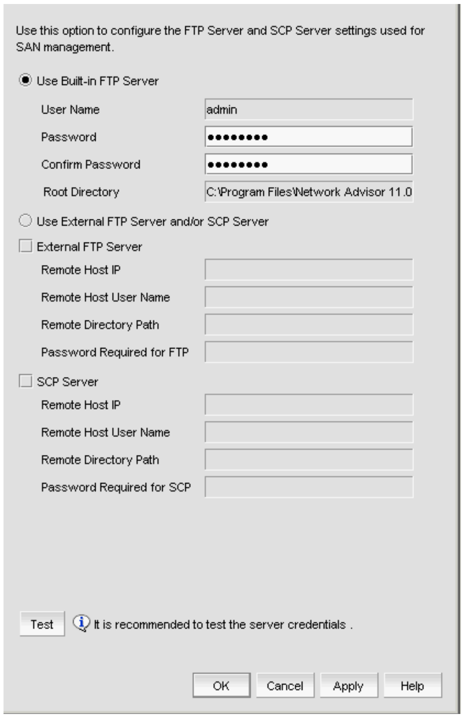
Configuring an internal FTP server

To configure the internal FTP server settings, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays (Figure 52).

2. Select **FTP/SCP** in the **Category** list.



Use this option to configure the FTP Server and SCP Server settings used for SAN management.

● Use Built-in FTP Server

User Name	admin
Password	••••••••
Confirm Password	••••••••
Root Directory	C:\Program Files\Network Advisor 11.0

○ Use External FTP Server and/or SCP Server

□ External FTP Server

Remote Host IP	
Remote Host User Name	
Remote Directory Path	
Password Required for FTP	

□ SCP Server

Remote Host IP	
Remote Host User Name	
Remote Directory Path	
Password Required for SCP	

Test — It is recommended to test the server credentials .

FIGURE 52 Options dialog box (SAN FTP/SCP option)

3. Select the **Use built-in FTP Server** option to use the default built-in FTP server.

   All active fields are mandatory.

4. Change your password by entering a new password in the **Password** and **Confirm Password** fields.

5. Click **Test** to test the FTP server.

   An "FTP Server running successfully" or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

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

Configuring an external FTP server

To configure the external FTP server settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP** in the **Category** list.
3. Select the **Use External FTP Server and/or SCP Server** option.
4. Select the **External FTP Server** check box to configure the external FTP server.

   All fields are mandatory.

5. Enter the IP address for the remote host in the **Remote Host IP** field.
6. Enter a user name in the **Remote User Name** field
7. Enter the path to the remote host in the **Remote Directory Path** field.

   Use a slash (/) or a period (.) to denote the relative root directory of the FTP server. Do not give an absolute path.

8. Enter the password in the **Password Required for FTP** field.
9. Click **Test** to test the FTP server.

   An "FTP Server running successfully" or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

10. Click **OK** on the message.
11. Click **Apply** or **OK** to save your work.

Configuring a FTP or SCP server

To configure the SCP server settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP** in the **Category** list.
3. Select the **Use External FTP Server and/or SCP Server** option.
4. Select the **FTP Server** check box to configure the external FTP server.

   All fields are mandatory.

5. Enter the IP address for the remote host in the **Remote Host IP** field.
6. Enter a user name in the **Remote User Name** field.
7. Enter the path to the remote host in the **Remote Directory Path** field.

   Use a slash (/) or period (.) to denote the root directory. Do not give an absolute path.

8. Enter the password in the **Password Required for FTP** field.

9. Click **Test** to test the FTP server.

   A “Server running successfully” or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

10. Click **OK** on the message.
11. Click **Apply** or **OK** to save your work.

Testing the FTP and SCP server

To test the FTP and SCP server, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays.

2. Select **FTP/SCP** in the **Category** list.
3. Choose one or more of the following options:
   - If you are using the internal FTP server, select the **Use built-in FTP Server** option.

     For step-by-step instructions about configuring the built-in server, refer to “Configuring an internal FTP server” on page 128.

   - If you are using the external FTP server, select the **Use External FTP Server** option.

     For step-by-step instructions about configuring the built-in server, refer to “Configuring an external FTP server” on page 129.

4. Click **Test**.

   An “FTP or SCP Server running successfully” or an error message displays.

   If you receive an error message, make sure your credentials are correct, the server is running, the remote directory path exists, and you have the correct access permission; then try again.

5. Click **OK** on the message.
6. Click **OK** to close the **Options** dialog.

Server port

You can configure the server port settings so that you can assign a web server port number and set the server port to be SSL-enabled.

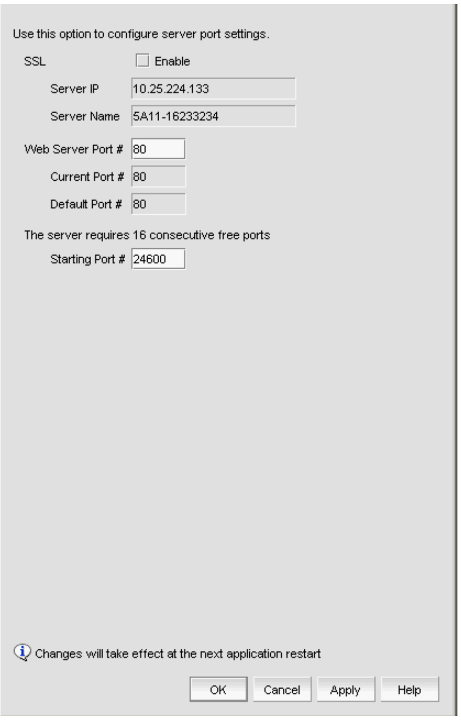
Configuring the server port

To configure server settings, complete the following steps.

1. Select **Server > Options**.

   The **Options** dialog box displays (Figure 53).

2. Select **Server Port** in the **Category** list.



Use this option to configure server port settings.

SSL □ Enable

Server IP 10.25.224.133

Server Name 5A11-16233234

Web Server Port # 80

Current Port # 80

Default Port # 80

The server requires 16 consecutive free ports

Starting Port # 24600

Changes will take effect at the next application restart

FIGURE 53 Options dialog box (Server Port option)

3. Select the **Enable SSL** check box to enable this function for the server port.

4. Enter a port number in the **Web Server Port #** field.

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

5. Enter a port number in the **Starting Port #** field.

   For Trial and Licensed version, the server requires 16 consecutive free ports beginning with the starting port number.

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

NOTE
Changes to this option take effect after application restart.

7. Click **OK** on the "changes take effect after application restart" message.

Support mode

You can configure support settings to allow enhanced diagnostics.

Configuring support mode settings

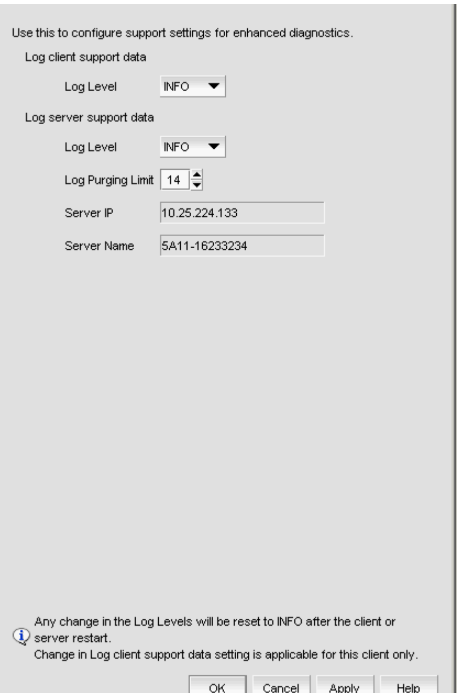
To configure support mode settings, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays (Figure 54).

2. Select **Support Mode** in the **Category** list to enable or disable support modes.

NOTE
Only use this option when directed to by customer support.



Use this to configure support settings for enhanced diagnostics.

Log client support data

Log Level INFO

Log server support data

Log Level INFO

Log Purging Limit 14

Server IP 10.25.224.133

Server Name 5A11-16233234

Any change in the Log Levels will be reset to INFO after the client or server restart.
Change in Log client support data setting is applicable for this client only.

FIGURE 54 Options dialog box (Support Mode option)

3. Select the **Log client support data - Log Level** list, and select the type of log data you want to configure.

   Log level options include: **All**, **Fatal**, **Error**, **Warn**, **Info**, **Debug**, **Trace**, and **Off**. Default is **Info**.

   The log level options return to the default value (Info) when the client or server is restarted.

4. Select the **Log server support data - Log Level** list, and select the type of log data you want to configure.

   Log level options include: **All**, **Fatal**, **Error**, **Warn**, **Info**, **Debug**, **Trace**, and **Off**. Default is **Info**.

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

NOTE
Changes to the **Log client support data** or **Log server support data** log levels reset to the default (INFO) after a client or server restart.

NOTE
Changes to the **Log client support data** log level is applicable for this client only.

client. log file properties

- Each log file is limited to 5 MB. When a file reaches the maximum size, and there are less than 5 log files for the Client, a new file is created.
- For local clients, log files (client.log.1 through client.log.5) are created in the *User_Home/Product_Name/localhost* directory.
- For web start clients, log files (client.log.1 through client.log.5) are created in the *User_Home/Product_Name/Server_IP_Address* directory.

server. log file properties

- There is only one server.log file each day with no log size limit.
- The server.log file rolls over at 12:00 midnight everyday.
- When the log file rolls over, it is compressed and renamed using the following file name format:

  server.yyyy-mm-dd.log.zip
  for example, server.2010-04-14.log.zip, server.2010-04-15.log.zip, and so on
- For servers, log files are created in the *Install_Home*/logs/server directory.

Configuring the server log file purge limit

To configure server log file purging, complete the following steps.

1. Select **Server** > **Options**.

   The **Options** dialog box displays.

2. Select **Support Mode** in the **Category** list to enable or disable support modes.

NOTE
Only use this option when directed to by customer support.

3. Select the maximum number of days to retain the server log file in the **Log Purging Limit** field.
4. Click **Apply** or **OK** to save your work.

Fabric tracking

When you discover a new fabric and initial discovery is complete, fabric tracking is automatically enabled. Subsequently, if a switch or end-device is added to or removed from the fabric, a plus (+) or minus (-) icon displays (see table below) next to the product icon. Connections are also tracked. A new connection displays a solid gray line with a added icon and missing connections display a yellow dashed line with a removed icon.

TABLE 14

⊕	Device Added
⊖	Device Removed

When you enable fabric tracking and a switch is missing from the fabric, a warning level call home event (Switch Switch_WWN is missing from the fabric Fabric_Name) is generated in the Master Log and a call home alert is sent to the corresponding call center for this event.

To avoid call home events for missing switches, create a call home event filter and clear the 'Switch is missing from the Fabric' check box in the Available Call Home Event Types table. Once you create the call home event filter, assign it to the appropriate call center. To create a call home event filter, refer to "Defining an event filter" on page 175.

Enabling fabric tracking

1. Enable fabric tracking by choosing one of the following options:

   - Select a fabric on the Product List or Connectivity Map and select **Monitor > Track Fabric Changes**.
   - Right-click a fabric on the Product List or Connectivity Map and select **Track Fabric Changes**.

   The **Accept Changes Summary** dialog box displays. This dialog box includes the following information:

   - **Do not show me this again** check box--Select if you do not want to see this dialog box again when you enable or disable fabric tracking or accept changes for a switch or fabric.
   - **Fabric Name**—Displays the name of the selected fabric.
   - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), name, IP address, WWN, and domain ID.
   - **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), device type, port, port WWN, node WWN, and attached port number.
   - **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (⊕) or removed (⊖) from the fabric) and connection type as well as the WWN, domain ID, IP address, and port number of the connected switches.

2. Click **Yes** to accept changes.

Disabling fabric tracking

1. Disable fabric tracking by choosing one of the following options:

   - Select the fabric on which you want to disable fabric tracking on the Product List or Connectivity Map and select **Monitor > Track Fabric Changes.**
   - Right-click the fabric on which you want to disable fabric tracking on the Product List or Connectivity Map and select **Track Fabric Changes.**

   The **Accept Changes Summary** dialog box displays. This dialog box includes the following information:

   - **Do not show me this again** check box--Select if you do not want to see this dialog box again when you enable or disable fabric tracking or accept changes for a switch or fabric.
   - **Fabric Name**—Displays the name of the selected fabric.
   - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), name, IP address, WWN, and domain ID.
   - **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), device type, port, port WWN, node WWN, and attached port number.
   - **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (⊕) or removed (⊖) from the fabric) and connection type as well as the WWN, domain ID, IP address, and port number of the connected switches.

2. Click **Yes.**

Accepting changes for a fabric

1. Accept the changes to a fabric by choosing one of the following options:

   - Select a fabric on the Product List or Connectivity Map and select **Monitor > Accept Changes.**
   - Right-click a fabric on the Product List or Connectivity Map and select **Accept Changes.**

   The **Accept Changes Summary** dialog box displays. This dialog box includes the following information:

   - **Do not show me this again** check box--Select if you do not want to see this dialog box again when you enable or disable fabric tracking or accept changes for a switch or fabric.
   - **Fabric Name**—Displays the name of the selected fabric.
   - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), name, IP address, WWN, and domain ID.

- **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), device type, port, port WWN, node WWN, and attached port number.
- **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (⊕) or removed (⊖) from the fabric) and connection type as well as the WWN, domain ID, IP address, and port number of the connected switches.

2. Click **Yes** to accept changes.

Accepting changes for all fabrics

1. Accept the changes to all fabrics by choosing one of the following options:

   - Click in the white space on the Connectivity Map and select **Monitor > Accept All Changes**.
   - Right-click in the white space on the Connectivity Map and select **Accept All Changes**.

   A message displays listing the following information:

   - **Do not show me this again** check box--Select if you do not want to see this dialog box again when you enable or disable fabric tracking or accept changes for a switch or fabric.
   - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), name, fabric name, IP address, WWN, and domain ID.
   - **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), device type, port, fabric name, port WWN, node WWN, and attached port number.
   - **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (⊕) or removed (⊖) from the fabric) and connection type as well as the fabric name, WWN, domain ID, IP address, and port number of the connected switches.

2. Click **Yes** to accept changes.

Accepting changes for a switch, access gateway, or phantom domain

1. Accept the changes to a switch, access gateway, or phantom domain by choosing one of the following options:

   - Select the switch, access gateway, or phantom domain on the Product List or Connectivity Map and select **Monitor > Accept Changes**.
   - Right-click the switch, access gateway, or phantom domain on the Product List or Connectivity Map and select **Accept Change**.

   The **Accept Changes Summary** dialog box displays. This dialog box includes the following information:

   - **Do not show me this again** check box--Select if you do not want to see this dialog box again when you enable or disable fabric tracking or accept changes for a switch or fabric.
   - **Fabric Name**—Displays the name of the selected fabric.
   - **Switches**—This table shows a brief summary of the switches including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), name, IP address, WWN, and domain ID.

- **Device Ports**—This table shows a brief summary of the device ports including status (whether the device port will be added (⊕) or removed (⊖) from the fabric), device type, port, port WWN, node WWN, and attached port number.
- **Connections**—This table shows a brief summary of the switch connections including the status (whether the device port will be added (⊕) or removed (⊖) from the fabric) and connection type as well as the WWN, domain ID, IP address, and port number of the connected switches.

2. Click **Yes** to accept changes.

Chapter

User Account Management 6

In this chapter

Users overview

The Management application allows you to manage accounts of users who manage devices on the network. When a user logs in to the Management application, the user name and password can be authenticated and authorized by the local server or by a supported external server.

User accounts are assigned privileges, which you define within roles. Each privilege provides access to a specific feature of the Management application. This enables you to maintain privileges common to a group of administrators within a role, instead of in individual accounts.

You can group devices, access points, and their groups in areas of responsibilities (AORs), then assign one or more AORs to a user's privilege. When you assign a user an AOR, that user will be able to manage only the devices in that AOR. Devices in a user's AOR are the only devices that user sees in device trees and on the **Dashboard** tab. You can place selected devices, device groups, port groups, access points, access point groups, and access point port groups in an AOR.

Users who create a device group are the only users who can manage the devices in that group. Other users may view the groups, but do not have the ability to add, delete, or modify the groups.

Configuration requirements

To administer accounts on the Management application server, you must have an administrative login on the platform on which the Management application is running. Use the "Administrator" login to create other logins with administrative permissions.

User accounts

NOTE
You must have User Management Read and Write privileges to add new accounts, set passwords for accounts, and apply roles to the accounts. For a list of privileges, refer to "User Privileges" on page 939.

Management application user accounts contain the identification of the Management application user, as well as privileges, roles, and AORs assigned to the user. Privileges provide access to the features in Management application. A role is a group of selected privileges. A role can be assigned to one or more Management application users who need access to the same menu options.

An AOR contains selected fabrics and devices that an Management application user is allowed to manage.

Creating a new user account

To create a new user account, complete the following steps.

1. Select **Server** > **Users**.

   The **Users** dialog box displays.

2. Click **Add** under the **Users** table.

   The **Add User** dialog box displays.

3. Enter a unique name to identify the user in the **User ID** field.
4. Enter a password for the user in the **Password** and **Confirm Password** fields.

   Passwords displays as dots (.). For password policy details, refer to "Viewing your password policy" on page 150.

5. Select the **Account Status** - **Enable** check box to enable the account of the user.

   Account Status is enabled by default.

6. (Optional) Enter the full name of the user in the **Full Name** field.
7. (Optional) Enter a description for the user in the **Description** field.
8. (Optional) Enter the phone number of the user in the **Phone Number** field.
9. Select the **E-mail Notification** - **Enable** check box to enable e-mail notification for the user.

   E-mail Notification is disabled by default.

10. Click **Filter** to set up basic event filters for the user.

    For step-by-step instructions about setting up basic event filters, refer to "Setting up basic event filtering" on page 825.

11. Enter the e-mail address of the user in the **E-mail Address** field.

    Enter more than one e-mail address, separating each with a semi-colon.

12. Assign roles and AORs by selecting the role or AOR in the **Available Roles / AOR** table and click the right arrow button to move the role or AOR to the **Selected Roles / AOR** table.

    Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

13. Remove roles and AORs by selecting the role or AOR in the **Selected Roles / AOR** table and click the left arrow button to move the role or AOR to the **Available Roles / AOR** table.

    Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

14. Click **OK** to save the new user and close the **Add User** dialog box.

    The new user account displays in the **Users** table of the **Users** dialog box. You must assign at least one role to a user account. Users without an assigned role cannot log into the client.

15. Click **Close** to close the **Users** dialog box.

Copying a user account

You can create a user account by copying an existing one. When you copy an account, you copy the selected roles and AORs of that account. You can then enter a new user name, ID, e-mail address, and telephone number.

To create a new user account from an existing account, complete the following steps.

1. Select **Server** > **Users**.

   The **Users** dialog box displays.

2. Select the user account you want to copy and click **Duplicate** under the **Users** table.

   The **Duplicate User** dialog box displays.

3. Enter a unique name to identify the user in the **User ID** field.

4. Enter a password for the user in the **Password** and **Confirm Password** fields.

   Passwords displays as dots (.). For password policy details, refer to “Viewing your password policy” on page 150.

5. Select the **Account Status** - **Enable** check box to enable the account of the user.

   Account Status is enabled by default.

6. (Optional) Enter the full name of the user in the **Full Name** field.

7. (Optional) Enter a description for the user in the **Description** field.

8. (Optional) Enter the phone number of the user in the **Phone Number** field.

9. Select the **E-mail Notification** - **Enable** check box to enable e-mail notification for the user.

   E-mail Notification is disabled by default.

10. Click **Filter** to set up basic event filters for the user.

    For step-by-step instructions about setting up basic event filters, refer to “Setting up basic event filtering” on page 825.

11. Enter the e-mail address of the user in the **E-mail Address** field.

    Enter more than one e-mail address, separating each with a semi-colon.

12. Assign roles and AORs by selecting the role or AOR in the **Available Roles / AOR** table and click the right arrow button to move the role or AOR to the **Selected Roles / AOR** table.

    Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

13. Remove roles and AORs by selecting the role or AOR in the **Selected Roles / AOR** table and click the left arrow button to move the role or AOR to the **Available Roles / AOR** table.

    Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

14. Click **OK** to save the new user and close the **Duplicate User** dialog box.

    The new user account displays in the **Users** table of the **Users** dialog box.

15. Click **Close** to close the **Users** dialog box.

Editing a user account

To make changes to an existing user account, complete the following steps.

1. Select **Server** > **Users.**

   The **Users** dialog box displays.

2. Select the user account you want to edit and click **Edit** under the **Users** table.

   The **Edit User** dialog box displays.

3. (Optional) Change the full name of the user in the **Full Name** field.

4. Change a password for the user in the **Password** and **Confirm Password** fields.

   Passwords displays as dots (.). For password policy details, refer to “Viewing your password policy” on page 150.

5. Select the **Account Status** - **Enable** check box to enable the account of the user.

   Clear the **Account Status** - **Enable** check box to disable the account of the user.

   Account Status is enabled by default.

6. (Optional) Change the full name of the user in the **Full Name** field.

7. (Optional) Change a description for the user in the **Description** field.

8. (Optional) Change the phone number of the user in the **Phone Number** field.

9. Select the **E-mail Notification** - **Enable** check box to enable e-mail notification for the user.

   Clear the **E-mail Notification** - **Enable** check box to disable e-mail notification for the user.

   E-mail Notification is disabled by default.

10. Click **Filter** to set up basic event filters for the user.

    For step-by-step instructions about setting up basic event filters, refer to “Setting up basic event filtering” on page 825.

11. Enter the e-mail address of the user in the **E-mail Address** field.

    Enter more than one e-mail address, separating each with a semi-colon.

12. Assign roles and AORs by selecting the role or AOR in the **Available Roles / AOR** table and click the right arrow button to move the role or AOR to the **Selected Roles / AOR** table.

    Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

13. Remove roles and AORs by selecting the role or AOR in the **Selected Roles / AOR** table and click the left arrow button to move the role or AOR to the **Available Roles / AOR** table.

    Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

14. Click **OK** to save the user account and close the **Edit User** dialog box.

    If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **OK** on the confirmation message, the user is logged out and must log back in to see the changes.

15. Click **Close** to close the **Users** dialog box.

Assigning roles and areas of responsibility to a user account

To assign roles and AORs to an existing user account, complete the following steps.

1. Select **Server** > **Users**.

   The **Users** dialog box displays.

2. Select the user account you want to edit and click **Edit** under the **User**s table.

   The **Edit User** dialog box displays.

3. Assign roles and AORs by selecting the role or AOR in the **Available Roles / AOR** table and click the right arrow button to move the role or AOR to the **Selected Roles / AOR** table.

   Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

4. Click **OK** to save the user account and close the **Edit User** dialog box.

   If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **OK** on the confirmation message, the user is logged out and must log back in to see the changes.

5. Click **Close** to close the **Users** dialog box.

Removing roles and areas of responsibility to a user account

To remove roles and AORs to an existing user account, complete the following steps.

1. Select **Server** > **Users**.

   The **Users** dialog box displays.

2. Select the user account you want to edit and click **Edit** under the **User**s table.

   The **Edit User** dialog box displays.

3. Remove roles and AORs by selecting the role or AOR in the **Selected Roles / AOR** table and click the left arrow button to move the role or AOR to the **Available Roles / AOR** table.

   Select multiple roles or AORs by holding down the CTRL key and clicking more than one role or AOR.

4. Click **OK** to save the user account and close the **Edit User** dialog box.

   If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **OK** on the confirmation message, the user is logged out and must log back in to see the changes.

5. Click **Close** to close the **Users** dialog box.

Disabling a user account

To make the user account inactive, but keep it in the database, you can disable the user account.

NOTE
You cannot disable the default "Administrator" account.

To disable a user account, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the enabled user account you want to disable in the **Users** table and click **Disable**.
3. Click **Yes** on the confirmation message.

   If currently accessing the server, the user will be logged out once the user account is disabled. The user cannot log back in until you re-enable the user account.

4. Click **Close** to close the **Users** dialog box.

Enabling a user account

To re-activate a user account, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Select the disabled user account you want to enable in the **Users** table and click **Enable**.
3. Click **Yes** on the confirmation message.
4. Click **Close** to close the **Users** dialog box.

Deleting a user account

NOTE
You cannot delete the default "Administrator" user account.

To permanently delete a user account from the server, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Select the user you want to delete in the **Users** table and click **Delete.**
3. Click **Yes** on the confirmation message.

   If currently accessing the server, the user will be logged out once the user account is deleted.

4. Click **Close** to close the **Users** dialog box.

Unlocking a user account

NOTE
You must have User Management Read and Write privileges to unlock a user account.

You can unlock a user account when a user is locked out of the system because of too many invalid login attempts.

To unlock a user account, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Select the locked user account you want to unlock in the **Users** table and click **Unlock.**
3. Click **Yes** on the confirmation message.
4. Click **Close** to close the **Users** dialog box.

Password policies

NOTE
You must have User Management Read and Write privileges to configure password policy.

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. The purpose of the password policy is to establish a standard for the creation of strong passwords, the protection of those passwords, and the frequency of change.

Configuring a password policy

To configure password policies for all user accounts, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click the **Policy** tab.
3. Configure the password expiration by completing the following steps.
   1. Enter the maximum number of days that can elapse before a password must be changed by the user in the **Password Age** field.

      Valid values are 0 through 999. The default is 0, which means the policy is disabled.

   2. Enter the number of days to warn the user prior to password expiration in the **Warning Period** field.

      Only enabled when the **Password Age** value is greater than zero. Valid values are 0 through 998. The default is 0. The **Warning Period** value must be less than the **Password Age** value.

4. Enter the number of unique passwords you must use before you can reuse a password in the **History Count** field.

   Valid values are 1 through 24. The default is 1. When you update the **History Count** value, the current password history is not cleared.

5. Configure the password format by completing the following steps.
   1. Select the **Empty Password - Allow** check box to allow user accounts to be created or edited with empty passwords or to allow passwords with any format.

      Empty Password is enabled by default.

   2. Enter the minimum password length in the **Minimum Length** field.

      Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 4 through 127. The default is 8.

   3. Enter the minimum number of uppercase characters required in the **Upper Case Characters** field.

      Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 0.

d. Enter the minimum number of lowercase characters required in the **Lower Case Characters** field.

Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 0.

e. Enter the minimum number of digits required in the **Number of Digits** field.

Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 0.

f. Enter the minimum number of punctuation characters required in the **Punctuation Required** field.

Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 0.

g. Enter the maximum number that the same character can repeat without a different intervening character in the **Maximum Repeat** field.

Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 2.

h. Enter the maximum number of sequence characters from the ASCII collating series or keyboard sequences in the **Maximum Sequence** field.

For example, 'ab' is a sequence of 2 and '456' is a sequence of 3.

Only enabled when the **Empty Password - Allow** check box is clear. Valid values are 0 through 127. The default is 1.

6. Configure the password lockout support by completing the following steps.

a. Enter the number of failed login attempts allowed before the user account is locked out in the **Lockout Threshold** field.

Valid values are 0 through 999. The default is 0 (disabled).

b. Enter the time frame after which the account automatically unlocks and resumes normal operation in the **Lockout Duration** field.

Only enabled when the **Lockout Threshold** is greater than zero. If you specify zero, the user account is locked out indefinitely until an administrator manually unlocks it. Valid values are 0 through 99999. The default is 30.

7. Configure the password login policy by completing the following steps.

a. Select **Concurrent Login** or **Single Login** from the **Login Mode** list.

Single Login allows only one user to login at a time. If you selected **Single Login**, continue with step b.

Concurrent Login allows multiple users to login at the same time. If you selected **Concurrent Login**, go to step 8.

b. Select **Reject New Sessions** or **Logout Existing Sessions** from the **Action** list.

8. Click **View Policy Violators** to view the user accounts affected by any policy violations caused by your changes to the **Policy** tab before you save your work.

If none of the user accounts violate the updated password policy, an empty **View Policy Violators** dialog box displays.

9. Click **Apply.**

10. Click **Yes** on the confirmation message.
11. Click **Close** to close the **Users** dialog box.

Viewing password policy violators

To view password policy violators, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.
2. Click the **Policy** tab.
3. Click **View Policy Violators.**

   The **View Policy Violators** dialog box displays.
4. Review the password policy violator details.

   The **View Policy Violators** dialog box includes the following details:

   - **User ID**—Displays the identifier of the user who violated the password policy.
   - **Full Name**—Displays the full name of the user who violated the password policy.
   - **Reason**—Displays the reason the user violated the password policy.
5. Click **Close** on the **View Policy Violators** dialog box.
6. Click **Close** on the **Users** dialog box.

User profiles

User profiles contain the standard identification information of the user account, such as name, password, phone number, and e-mail address. The Management application enables you to make the following changes to your user profile:

- Change your name
- Change your password
- Change your user account description
- Change your phone number
- Change your e-mail address
- View your account state
- View your password policy
- Reset Management application messages
- Enable e-mail notification
- Configure e-mail notification

Viewing your user profile

To view your user profile, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays the following information:

   - **User ID**—Displays your user identifier.
   - **Full Name**—Displays the name if entered while adding a user; otherwise, this field is blank.
   - **Password**—Displays your password as dots (.). If the password policy is configured for an empty password, this field is blank.
   - **Confirm Password**—Displays your password as dots (.). If the password policy is configured for an empty password, this field is blank.
   - **Description**—Displays your description if entered while adding a user; otherwise, this field is blank.
   - **Phone Number**—Displays your phone number if entered while adding a user; otherwise, this field is blank.
   - **Account State**—Displays the current state of the account. Valid states include:
     - Active
     - Locked out by user manager
     - Locked out threshold reached
     - Password expired
     - Password format policy violated
     - Password history policy violated
   - **E-mail Notification Enable** check box—Select to enable e-mail notification.
   - **Filter**—Click to configure e-mail notification.
   - **E-mail Address**—Displays your e-mail addresses if entered while adding a user; otherwise, this field is blank.
   - **Password Age**—Displays the age of the password in days. Default is zero.
   - **Password Policy View** button—Click to display the current password policy.
   - **Optional Messages Reset** button—Click to reset all optional messages to the default behavior.

2. Click **OK** on the **User Profile** dialog box.

Editing your user profile

To edit your user profile, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.

2. Change your name in the **Full Name** field.
3. Change your password in the **Password** and **Confirm Password** fields.

   Passwords display as dots (.).

4. Change your user profile description in the **Description** field.

5. Change your phone number in the **Phone Number** field.
6. Select the **E-mail Notification Enable** check box to enable e-mail notification.

   Clear the **E-mail Notification Enable** check box to disable e-mail notification.
7. Click **Filter** to set up basic event filters.

   For step-by-step instructions about setting up basic event filters, refer to "Setting up basic event filtering" on page 825.
8. Change your e-mail address in the **E-mail Address** field.

   Enter more than one e-mail address, separating each with a semi-colon.
9. Click **OK** on the **User Profile** dialog box to save your changes.

Changing your password

To change your password from your user profile, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.
2. Change your password in the **Password** and **Confirm Password** fields.

   Passwords display as dots (.).
3. Click **OK** on the **User Profile** dialog box to save your changes.

If your password expires or your current password violates the password policy, you will be prompted to change your password from the **Change Password** dialog box. To view your password policy, click **Password Policy - View**.

To change your password from the **Change Password** dialog box, complete the following steps.

1. Enter your current password in the **Existing Password** field.
2. Enter your new password in the **New Password** and **Confirm Password** fields.

   Passwords display as dots (.).
3. Click **OK** to save your new password.

Viewing your password policy

To view your password policy, complete the following steps.

1. Select **Server > User Profile**.

   The **User Profile** dialog box displays.
2. Click **Password Policy - View** to display your password policy.

   The **Password Policy** dialog box displays.
3. Click **OK** on the **Password Policy** dialog box.
4. Click **OK** on the **User Profile** dialog box.

Resetting optional messages

To reset all Management application optional messages to their default behaviors, complete the following steps.

1. Select **Server > User Profile.**

   The **User Profile** dialog box displays.

2. Click **Optional Messages Reset**.

   The **Password Policy** dialog box displays.

3. Click **Yes** on the confirmation message.

   A successful reset message displays.

4. Click **OK** on the **User Profile** dialog box.

Configuring e-mail notification

To configure and enable e-mail notification, complete the following steps.

1. Select **Server > User Profile.**

   The **User Profile** dialog box displays.

2. Select the **E-mail Notification - Enable** check box to enable e-mail notification.

3. Click **Filter** to set up basic event filter.

   For step-by-step instructions about setting up basic event filters, refer to "Setting up basic event filtering" on page 825.

4. Enter your e-mail address in the **E-mail Address** field.

   Enter more than one e-mail address, separating each with a semi-colon.

5. Click **OK** on the **User Profile** dialog box.

Roles

NOTE
You must have User Management Read and Write privileges to view, add, modify, or delete roles.

A role is a group of Management application tasks or privileges that can be assigned to several users who have similar functions.

When you create a role, it immediately becomes available in the **Users** dialog box.

Creating a new role

To create a new role, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Click **Add** under the **Roles** table.

   The **Add Role** dialog box displays.

3. Enter a name of the role in the **Name** field.
4. (Optional) Enter a short description for the role in the **Description** field.
5. Add or remove privileges as needed.

   For step-by-step instructions, refer to "Adding privileges to a role" on page 152 or "Removing privileges from a role" on page 153.

6. Click **OK** to save the new role and close the **Add Role** dialog box.

   The new role displays in the **Roles** list of the **Users** dialog box. To add users to this role, follow the instructions in "Assigning roles and areas of responsibility to a user account" on page 143.

7. Click **Close** to close the **Users** dialog box.

Adding privileges to a role

Each option under the Management application main menu corresponds to a privilege. By adding a privilege to a role and assigning that role to a user, you give the user access to a feature of the Management application. When a user logs in to the Management application, the user sees only the options that correspond to the privileges listed in the **Add Roles**, **Edit Roles**, or **Duplicate Roles** dialog box.

To add privileges to a role, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Click **Add**, **Edit**, or **Duplicate** under the **Roles** table.

   The **Add Roles**, **Edit Roles**, or **Duplicate Roles** dialog box displays.

3. Add read and write access by selecting the features to which you want to allow read and write access in the **Available Privileges** list and click the right arrow button to move the features to the **Read & Write Privileges** list.

   Select multiple features by holding down the CTRL key and clicking more than one privilege. The features are moved to the **Read & Write Privileges** list.

4. Add read-only access by selecting the features to which you want to allow read-only access in the **Available Privileges** list and click the right arrow button to move the features to the **Read Only Privileges** list.

   Select multiple features by holding down the CTRL key and clicking more than one privilege. The features are moved to the **Read Only Privileges** list.

5. Click **OK** to save your work.

6. Click **Close** to close the **Users** dialog box.

Removing privileges from a role

You remove privileges from the **Edit** or **Duplicate Users** dialog boxes.

To remove privileges from role, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the role you want to edit in the **Roles** table and click **Edit** or **Duplicate** under the **Roles** table.

   The **Edit Roles** or **Duplicate Roles** dialog box displays.

3. Remove read and write access by selecting the features to which you want to remove read and write access in the **Read & Write Privileges** list and click the left arrow button to move the features to the **Available Privileges** list.

   Select multiple features by holding down the CTRL key and clicking more than one privilege. The features are moved to the **Available Privileges** list.

4. Remove read-only access by selecting the features to which you want to remove read-only access in the **Read Only Privileges** list and click the right arrow button to move the features to the **Available Privileges** list.

   Select multiple features by holding down the CTRL key and clicking more than one privilege. The features are moved to the **Available Privileges** list.

5. Click **OK** to save your work.

6. Click **Close** to close the **Users** dialog box.

Copying a role

You can create a new role by copying an existing one. When you copy a role, you copy the selected privileges in that role.

To copy an existing role, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Select the role you want to copy in the **Roles** table and click **Duplicate.**

   The **Duplicate Role** dialog box displays.

3. Enter a name of the role in the **Name** field.

4. (Optional) Enter a short description for the role in the **Description** field.

5. Add or remove privileges as needed.

   For step-by-step instructions, refer to "Adding privileges to a role" on page 152 or "Removing privileges from a role" on page 153.

6. Click **OK** to save the role and close the **Duplicate Role** dialog box.

   The new role displays in the **Roles** list of the **Users** dialog box. To add users to this role, follow the instructions in "Assigning roles and areas of responsibility to a user account" on page 143.

7. Click **Close** to close the **Users** dialog box.

Editing a role

To make changes to an existing role, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Select the role you want to edit in the **Roles** table and click **Edit.**

   The **Edit Role** dialog box displays.

3. (Optional) Change the short description for the role in the **Description** field.

4. Add or remove privileges as needed.

   For step-by-step instructions, refer to "Adding privileges to a role" on page 152 or "Removing privileges from a role" on page 153.

5. Click **OK** to save the role and close the **Edit Role** dialog box.

   If you make changes to the user's role or AOR while the user is logged in, a confirmation message displays. When you click **OK** on the confirmation message, the user is logged out and must log back in to see the changes.

6. Click **Close** to close the **Users** dialog box.

Deleting a role

To delete a role, complete the following steps.

1. Select **Server** > **Users**.

   The **Users** dialog box displays.

2. Select the role you want to delete in the **Roles** table and click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **Close** to close the **Users** dialog box.

Areas of responsibility

NOTE
You must have User Management Read and Write privileges to view, add, modify, or delete operational areas of responsibility.

An area of responsibility (AOR) allows you to place Fabricsand Hosts into management groups that can be assigned to an Management application user. Users can manage only the Fabricsand Hosts in the AOR assigned to them, because only devices their AOR display in the Product List and Topology Map.

For example, devices 10.10.10.1, 10.10.10.2, and 10.10.14.3 may be placed in AOR Group 1. This AOR group can then be assigned to UserA. When using the Management application, UserA will be able to create configurations, generate reports, and perform backups only to entries in AOR Group 1 (which consists of devices 10.10.10.1, 10.10.10.2, and 10.10.14.3).

Creating an AOR

When creating an AOR, you assign devices or groups to that AOR. After you save the AOR, it can be assigned to one or more user account. Users of those accounts can then view the devices or groups in their assigned AOR. Users can deploy configurations and payloads only to devices in assigned AORs.

When you create an AOR, it immediately becomes available in the **Users** dialog box.

To create an AOR, complete the following steps.

1. Select **Server** > **Users**.

   The **Users** dialog box displays.

2. Click **Add** under the **AOR** table.

   The **Add AOR** dialog box displays.

3. Enter a name of the AOR in the **Name** field.
4. (Optional) Enter a short description for the AOR in the **Description** field.
5. Assign or remove products as needed.

   For step-by-step instructions, refer to “Assigning products to an AOR” on page 156 or “Removing products from an AOR” on page 156.

6. Click **OK** to save the new AOR and close the **Add AOR** dialog box.

   The new AOR displays in the **AOR** list of the **Users** dialog box.

7. Click **Close** to close the **Users** dialog box.

Assigning products to an AOR

You can assign fabricsand hosts to an AOR from the **Add**, **Edit**, or **Duplicate AOR** dialog box.

To assign fabricsand hosts to an AOR, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Click **Add**, **Edit**, or **Duplicate** under the **AOR** table.

   The **Add AOR**, **Edit AOR**, or **Duplicate AOR** dialog box displays.

3. Click the **Fabrics** tab.

4. Select the fabrics you want to assign to the AOR in the **Available Fabrics** table and click the right arrow button to move the products to the **Selected Products** table.

   Select multiple fabrics by holding down the CTRL key and clicking more than one fabric.

5. Click the **Hosts** tab.

6. Select the hosts you want to assign to the AOR in the **Available Hosts** table and click the right arrow button to move the products to the **Selected Products** table.

   Select multiple hosts by holding down the CTRL key and clicking more than one host.

7. Click **OK** to save your work

8. Click **Close** to close the **Users** dialog box.

Removing products from an AOR

You can remove fabricsand hosts from and AOR from the **Edit AOR** or **Duplicate AOR** dialog box.

To remove fabricsand hosts from the AOR, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Click **Edit** or **Duplicate** under the **AOR** table.

   The **Edit AOR** or **Duplicate AOR** dialog box displays.

3. In the **Selected Products** table, select the products or groups you want to remove and click the left arrow button.

   Select multiple products or groups by holding down the CTRL key and clicking more than one item.

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

5. Click **Close** to close the **Users** dialog box.

Copying an AOR

To create a new AOR by copying an existing one, complete the following steps.

1. Select **Server** > **Users**.

   The **Users** dialog box displays.

2. Select the AOR you want to copy in the **AOR** table and click **Duplicate**.

   The **Duplicate AOR** dialog box displays.

3. Change the name of the AOR in the **Name** field.
4. (Optional) Change the short description for the AOR in the **Description** field.
5. Assign or remove products as needed.

   For step-by-step instructions, refer to “Assigning products to an AOR” on page 156 or “Removing products from an AOR” on page 156.

6. Click **OK** to save the new AOR and close the **Duplicate AOR** dialog box.

   The new AOR displays in the **AOR** table of the **Users** dialog box. To add this AOR to a user, follow the instructions in “Assigning roles and areas of responsibility to a user account” on page 143.

7. Click **Close** to close the **Users** dialog box.

Editing an AOR

To make changes to an existing AOR, complete the following steps.

1. Select **Server** > **Users**.

   The **Users** dialog box displays.

2. Select the AOR you want to edit in the **AOR** table and click **Edit**.

   The **Edit AOR** dialog box displays.

3. (Optional) Change the short description for the AOR in the **Description** field.
4. Assign or remove products as needed.

   For step-by-step instructions, refer to “Assigning products to an AOR” on page 156 or “Removing products from an AOR” on page 156.

5. Click **OK** to save the AOR and close the **Edit AOR** dialog box.

   If you make changes to the user’s role or AOR while the user is logged in, a confirmation message displays. When you click **Yes** on the confirmation message, the user is logged out and must log back in to see the changes.

6. Click **Close** to close the **Users** dialog box.

Deleting an AOR

To delete an AOR, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Select the AOR you want to delete in the **AOR** table and click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **Close** to close the **Users** dialog box.

LDAP authorization

NOTE
You must have User Management Read and Write privileges to map roles and AORs to Active Directory groups.

Lightweight Directory Access Protocol (LDAP) authorization enables you to configure user access rights to Active Directory groups (including users, contacts, computers, and other Active Directory groups).

Loading an Active Directory group

To load an Active Directory group, complete the following steps.

1. Select **Server > Users**.

   The **Users** dialog box displays.

2. Click the **LDAP Authorization** tab.
3. Click **Fetch**.

   The **Fetch AD Group** dialog box displays.

4. Select the LDAP server network address from the **Network Address** list.
5. Enter the TCP port number in the **TCP Port** field.

   The default is 389.

6. Select the authentication protocol **MD5** from the **Authentication** list.
7. Enter your LDAP server user login name in the **User Name** field.
8. Enter your LDAP server user login password in the **Password** field.
9. Select the **Security Enable** check box to enable the security channel between the Management application server and the LDAP server.

   When you select the **Security Enable** check box, the TCP port number automatically changes to port 636 and you must enable certificate services on the LDAP server.

10. Click **OK**.

    The **Active Directory Groups** table displays with all first level Active Directory groups available in the specified LDAP server, as well as any Active Directory groups already mapped in the Management server (Local database).

    To assign or remove roles and AORs, refer to "Assigning roles and AORs to an Active Directory group" on page 159 or "Removing roles and AORs from an Active Directory group" on page 159.

11. Click **Close** to close the **Users** dialog box.

Assigning roles and AORs to an Active Directory group

When you assign roles and AOR's to an Active Directory group and save the configurations, when you reopen the **Users** dialog box and select the **LDAP Authorization** tab, only the configured Active Directory group is available.

To assign roles and AORs to an Active Directory group, complete the following steps.

1. Select the roles and AORs you want to assign to the Active Directory group in the **Available Roles / AORs** table.

   Select multiple roles and AORs by holding down the CTRL key and clicking more than one role and AOR.

2. Select the Active Directory group to which you want to assign the selected roles and AORs in the **Active Directory Groups** table.
3. Click the right arrow button.

   The selected roles and AORs are moved to the **Active Directory Groups** table.

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

Removing roles and AORs from an Active Directory group

To remove roles and AORs from an Active Directory group, complete the following steps.

1. Select the roles and AORs you want to remove in the **Active Directory Groups** table.

   Select multiple roles and AORs by holding down the CTRL key and clicking more than one role and AOR.

2. Click the left arrow button.

   The selected roles and AORs are moved to the **Available Roles / AORs** table.

3. Click **OK** to save your work.

Deleting an Active Directory group

To delete an Active Directory group, complete the following steps.

1. Select one or more Active Directory groups that you want to delete from the **Active Directory Groups** table.
2. Click **Delete**.
3. Click **Yes** on the confirmation message.
4. Click **OK** on the deletion successful message.
5. Click **OK** to save your work.

Chapter

7

Call Home

In this chapter

About call home

NOTE
Call Home is supported on Windows systems for all modem and E-mail call home centers and is supported on Unix for the E-mail call home centers.

Call Home notification allows you to configure the Management application Server to automatically send an e-mail or dial-in to a support center to report system problems on specified devices (Fabric OSand M-EOS switches, routers, and directors). If you are upgrading from a previous release, all of your Call Home settings are preserved.

Call Home supports multiple call home centers which allows you to configure different devices to contact different call home centers. When you make any call home configuration changes or a call home event trigger occurs, the Management application generates an entry to the Master Log.

You can configure Call Home for the following call home centers:

- Brocade E-mail (Windows and Unix)
- Brocade International (Windows only)
- Brocade North America (Windows only)
- EMC (Windows only)
- HP LAN (Windows only)
- IBM (Windows only)
- IBM E-mail (Windows and Unix)
- Oracle E-mail (Windows and Unix)

When configuring modem and LAN Call Home centers, you must enter the customer contact information in the device's Element Manager. You may also need to configure the Management application server IP address manually as a SNMP trap recipient for Fabric OSand Internetwork OS devices.

Call Home allows you to automate tasks that occur when the call home event trigger is fired. When a call home event trigger occurs, the Management application generates the following actions:

- Sends an e-mail to a specified recipient or dials-in to a support center.
- Triggers supportSave on the switch (if supportSave is enabled on the switch) prior to sending an alert. The supportSave location is included in the alert.

  NOTE
  The HP LAN Call Home alert displays the directory separation characters with a double backslash (\\) instead of a single backslash (\).

- Adds an entry to the Master Log file and screen display.
- Generates a XML report (only available with EMC call centers) with the product details which is sent with the E-mail.
- Generates an HTML report for E-mail-based Call Home centers.

For more information about Call Home events, refer to "Call Home Event Tables" on page 935. For more information about Event Management, refer to "Fault Management" on page 823.

Call Home allows you to perform the following tasks:

- Assign devices to and remove devices from the call home centers.
- Define filters from the list of events generated by Fabric OSand M-EOS devices.
- Edit and remove filters available in the Call Home Event Filters table.
- Apply filters to and remove filters from the devices individually or in groups.
- Edit individual call home center parameters to dial a specified phone number or E-mail a specific recipient.
- Enable and disable individual devices from contacting the assigned call home centers.
- Show or hide call home centers on the display.
- Enable and disable call home centers.

System requirements

Call Home (except for E-Mail and HP LAN) requires the following hardware equipment:

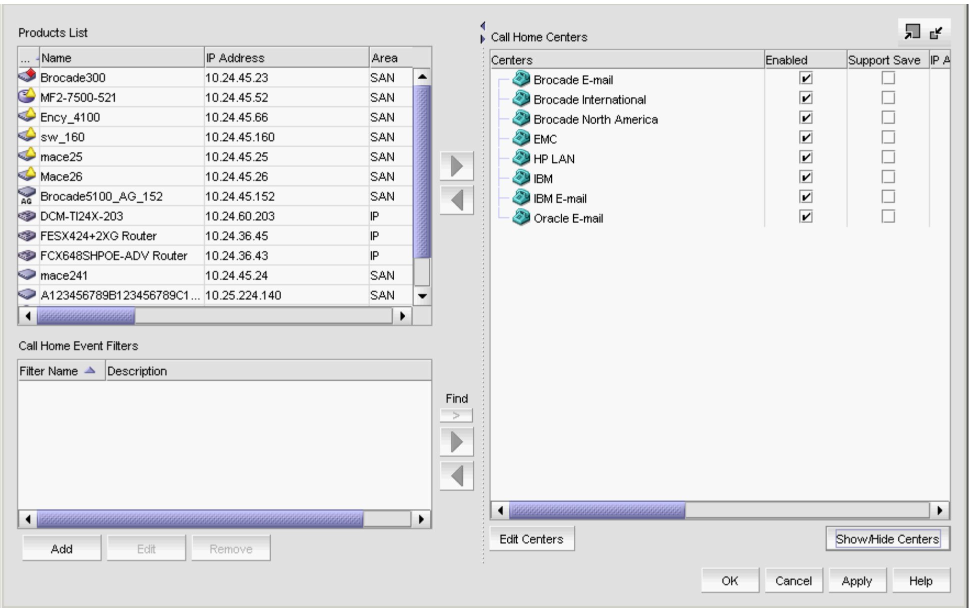
- Any Windows Server with an internal / external modem connection
- Analog phone line

Showing a call home center

To show a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays (Figure 55).



...	Name	IP Address	Area
	Brocade300	10.24.45.23	SAN
	MF2-7500-521	10.24.45.52	SAN
	Ency_4100	10.24.45.66	SAN
	sw_160	10.24.45.160	SAN
	mace25	10.24.45.25	SAN
	Mace26	10.24.45.26	SAN
	Brocade5100_AG_152	10.24.45.152	SAN
	DCM-TI24X-203	10.24.60.203	IP
	FESX424+2XG Router	10.24.36.45	IP
	FCX648SHPOE-ADV Router	10.24.36.43	IP
	mace241	10.24.45.24	SAN
	A123456789B123456789C1...	10.25.224.140	SAN

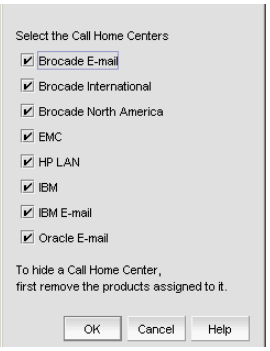
Filter Name	Description

Centers	Enabled	Support Save	IP A
Brocade E-mail	☑	□	
Brocade International	☑	□	
Brocade North America	☑	□	
EMC	☑	□	
HP LAN	☑	□	
IBM	☑	□	
IBM E-mail	☑	□	
Oracle E-mail	☑	□	

FIGURE 55 Call Home dialog box

2. Click **Show/Hide Centers** (beneath the **Call Home Centers** table).

   The **Centers** dialog box displays with a predefined list of call home centers (Figure 56).



Select the Call Home Centers

☑ Brocade E-mail
☑ Brocade International
☑ Brocade North America
☑ EMC
☑ HP LAN
☑ IBM
☑ IBM E-mail
☑ Oracle E-mail

To hide a Call Home Center,
first remove the products assigned to it.

FIGURE 56 Centers dialog box

3. Select the check boxes of the call home centers you want to display and click **OK**.

   The **Call Home** dialog box displays with the selected call home center listed in the **Call Home Centers** table.

Hiding a call home center

NOTE
Before you can hide a call home center, you must remove all assigned products.

To hide a call home center, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Click **Show/Hide Centers** (beneath the **Call Home Centers** table).

   The **Centers** dialog box displays with a predefined list of call home centers.

3. Clear the check boxes of the call home centers you want to hide and click **OK**.

   The **Call Home** dialog box displays with only selected call home centers listed in the **Call Home Centers** table.

Editing a call home center

NOTE
Call Home is supported on Windows systems for all modem call home centers and is supported on Unix for the E-mail call home centers.

To edit a call home center, select from the following procedures:

Editing the Brocade International or IBM call home center

To edit a Brocade International or IBM call home center, complete the following steps.

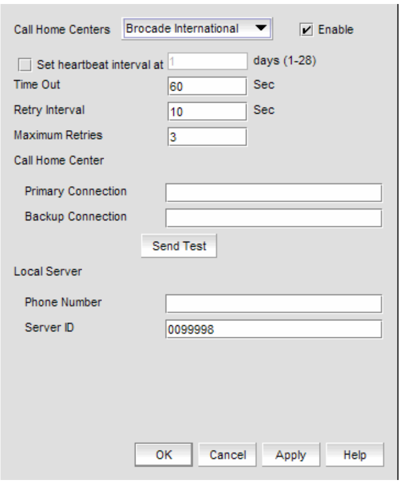
1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Select the call home center you want to edit (**Brocade International** or **IBM**) in the **Call Home Centers** table.

3. Click **Edit Centers** (beneath the **Call Home Centers** table).

   The **Configure Call Home Center** dialog box displays (Figure 57).



Call Home Centers: Brocade International ☑ Enable

☐ Set heartbeat interval at 1 days (1-28)

Time Out: 60 Sec

Retry Interval: 10 Sec

Maximum Retries: 3

Call Home Center

Primary Connection:

Backup Connection:

Local Server

Phone Number:

Server ID: 0099998

FIGURE 57 **Configure Call Home Center dialog box (Brocade International or IBM option)**

4. Make sure the call home center type you selected displays in the **Call Home Centers** list.
5. Select **Enable** to enable this call home center.
6. Set the time interval at which to check the call home center by selecting the **Set the heartbeat interval at ___ days (1-28)** check box and entering the interval in the field.
7. Enter the time out interval (default is 60 seconds) in the **Time Out** field.
8. Enter the retry interval (default is 10 seconds) in the **Retry Interval** field.
9. Enter the maximum number of retries (default is 3) in the **Maximum Retries** field.
10. Enter the primary phone number or extension of the call home center in the **Call Home Center - Primary Connection** field.
11. Enter the backup phone number or extension of the call home center in the **Call Home Center - Backup Connection** field.
12. Enter the phone number or extension of the local server in the **Local Server - Phone Number** field.
13. Enter the identification number of the local server in the **Local Server - Server ID** field.
14. Click **Send Test** to test the phone number.

    The selected call home center must be enabled to test the phone number.

    A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.
15. Click **OK**.

    The **Call Home** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.
16. Click **OK** to close the **Call Home** dialog box.

Editing the Brocade North America call home center

Modem call home centers are only available for Brocade. To edit this call home center, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Select **Brocade North America** in the **Call Home Centers** table.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).

   The **Configure Call Home Center** dialog box displays(Figure 58).

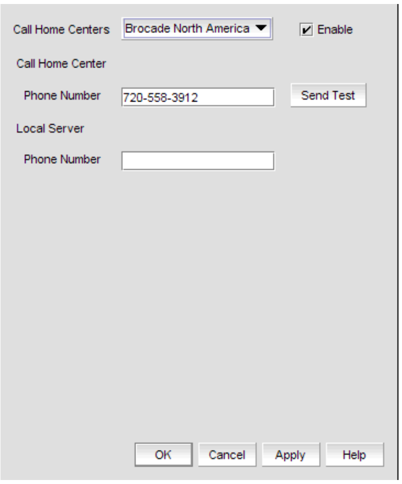

Call Home Centers: Brocade North America
☑ Enable
Call Home Center
Phone Number: 720-558-3912
Local Server
Phone Number:

FIGURE 58 Configure Call Home Center dialog box (Brocade North America option)

4. Make sure the call home center type you selected displays in the **Call Home Centers** list.
5. Select **Enable** to enable this call home center.
6. Enter the phone number or extension of the call home center in the **Call Home Center - Phone Number** field
7. Enter the phone number or extension of the local server in the **Local Server - Phone Number** field.
8. Click **Send Test** to test the phone number.

   The selected call home center must be enabled to test the phone number.

   A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

9. Click **OK**.

   The **Call Home** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

10. Click **OK** to close the **Call Home** dialog box.

Editing an E-mail call home center

E-mail call home centers are available for Brocade, IBM, and Oracle. To edit one of these call home centers, complete the following steps.

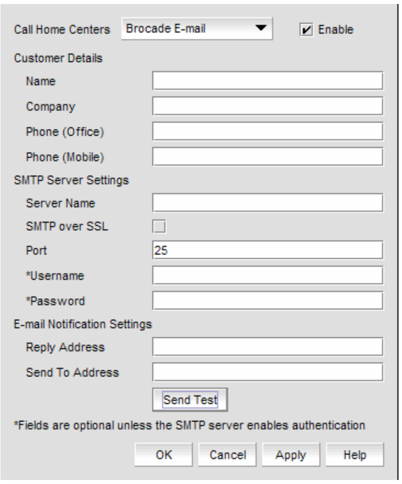
1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Select the call home center you want to edit (**Brocade E-mail**, **IBM E-mail**, or **Oracle E-mail**) in the **Call Home Centers** table.

3. Click **Edit Centers** (beneath the **Call Home Centers** table).

   The **Configure Call Home Center** dialog box displays (Figure 59).



Call Home Centers: Brocade E-mail

☑ Enable

☐ SMTP over SSL

Port: 25

*Fields are optional unless the SMTP server enables authentication

FIGURE 59 Configure Call Home Center dialog box (Brocade, IBM, or Oracle E-mail option)

4. Make sure the call home center type you selected displays in the **Call Home Centers** list.

5. Select the **Enable** check box to enable this call home center.

6. Enter the customer contact name in the **Customer Details - Name** field.

7. Enter the company name in the **Customer Details - Company** field.

8. Enter the phone number of the customer contact in the **Customer Details - Phone (Office)** field.

9. Enter the mobile phone number of the customer contact in the **Customer Details - Phone (Mobile)** field.

10. Enter the name of the server in the **SMTP Server Settings - Server Name** field.

11. Select the **SMTP over SSL** check box to enable secure communication between the SMTP server and the Management application.

12. Enter the port number (default is 465 if SMTP over SSL is enabled; otherwise, the default is 25) of the server in the **SMTP Server Settings - Port** field.

13. Enter a user name in the **SMTP Server Settings - Username** field.

    This is a required field when the SMTP server authentication is enabled.

14. Enter a password in the **SMTP Server Settings - Password** field.

    This is a required field when the SMTP server authentication is enabled.

15. Enter the e-mail address for replies in the **E-mail Notification Settings - Reply Address** field.
16. Enter the customer e-mail address in the **E-mail Notification Settings - Send To Address** field.
17. Click **Send Test** to test the mail server.

    The selected call home center must be enabled to test the mail server.

    A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

18. Click **OK**.

    The **Call Home Configuration** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

19. Click **OK** to close the **Call Home Configuration** dialog box.

Editing the EMC call home center

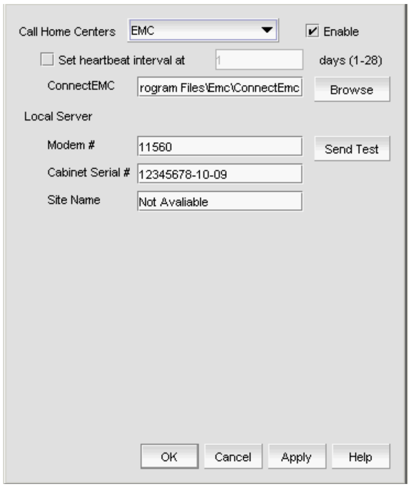
To edit an EMC call home center, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Select the **EMC** call home center you want to edit in the **Call Home Centers** table.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).

   The **Configure Call Home Center** dialog box displays (Figure 60).



Call Home Centers: EMC

☑ Enable

□ Set heartbeat interval at 1 days (1-28)

ConnectEMC: rogram Files\Emc\ConnectEmc

Local Server

Modem #: 11560

Cabinet Serial #: 12345678-10-09

Site Name: Not Avaliable

FIGURE 60 Configure Call Home Center dialog box (EMC option)

4. Make sure the **EMC** call home center type displays in the **Call Home Centers** list.
5. Select **Enable** to enable this call home center.
6. Set the time interval at which to check the call home center by selecting the **Set the heartbeat interval at ___ days (1-28)** check box and entering the interval in the field.

7. Enter the path to the ConnectEMC application in the **ConnectEMC** field or browse to the ConnectEMC application location.
8. Enter the phone number or extension of the local server in the **Local Server - Modem #** field.
9. Enter the identification number of the local server in the **Local Server - Cabinet Serial #** field.
10. Enter the site name for the local server in the **Local Server - Site Name** field.
11. Click **Send Test** to test the Connect EMC application.

    The selected call home center must be enabled to test the Connect EMC application.

    A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.
12. Click **OK**.

    The **Call Home** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.
13. Click **OK** to close the **Call Home** dialog box.

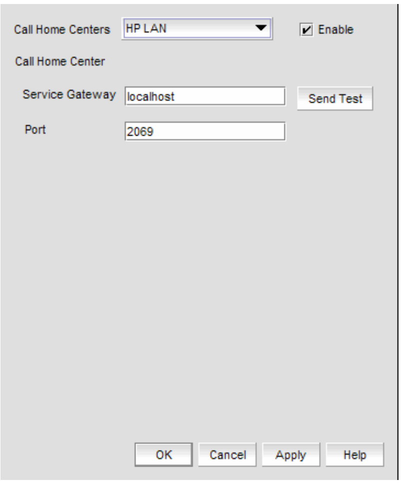
Editing the HP LAN call home center

To edit an HP LAN call home center, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

    The **Call Home** dialog box displays.
2. Select the **HP LAN** call home center you want to edit in the **Call Home Centers** table.
3. Click **Edit Centers** (beneath the **Call Home Centers** table).

    The **Configure Call Home Center** dialog box displays (Figure 61).



Call Home Centers: HP LAN

☑ Enable

Service Gateway: localhost

Port: 2069

FIGURE 61 Configure Call Home Center dialog box (HP LAN option)

4. Make sure the **HP LAN** call home center type displays in the **Call Home Centers** list.
5. Select **Enable** to enable this call home center.
6. Enter the IP address of the call home center in the **Service Gateway** field.

7. Enter the port number (default is 2069) of the call home center in the **Port** field
8. Click **Send Test** to test the address.

   The selected call home center must be enabled to test the IP address.

   A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.

   NOTE
   The HP LAN Call Home alert displays the directory separation characters with a double backslash (\\) instead of a single backslash (\).

9. Click **OK**.

   The **Call Home** dialog box displays with the call home center you edited highlighted in the **Call Home Centers** table.

10. Click **OK** to close the **Call Home** dialog box.

Enabling a call home center

To enable a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the **Enable** check box of the call home center you want to enable in the **Call Home Centers** table.
3. Click **OK** to close the **Call Home** dialog box.

Enabling support save

NOTE
Only supported on Fabric OS switches with Fabric OS 5.2 or later.

When you enable Support Save through the call home center, all call home events trigger the Support Save operation and the Support Save stored location on the FTP server is transmitted with the call home event.

To enable a support save for a call home center, complete the following steps.

1. Select **Monitor > Event Notification > Call Home**.

   The **Call Home** dialog box displays.

2. Select the **Support Save** check box of the call home center or device for which you want to enable support save in the **Call Home Centers** table.
3. Click **OK** to close the **Call Home** dialog box.

Testing the call home center connection

Once you add and enable a call home center, you should verify that call home is functional.

To verify call home center functionality, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.
2. Click **Edit Centers** (beneath the **Call Home Centers** table).

   The **Configure Call Home Center** dialog box displays.
3. Select the center you want to check in the **Call Home Centers** list.
4. Make sure that the **Enabled** check box is selected.

   NOTE
   You must configure the call home center before you test the connection. To configure a call home center, refer to "Editing a call home center" on page 165.
5. Click **Send Test**.

   A faked event is generated and sent to the selected call home center. You must contact the call home center to verify that the event was received and in the correct format.
6. Click **OK** to close the 'Test Event Sent' message.
7. Click **OK** to close the **Configure Call Home Center** dialog box.
8. Click **OK** to close the **Call Home** dialog box.

Disabling a call home center

When a call home center is disabled, no devices can send call home events to the call home center. However, the devices and event filters assigned to the disabled call home center are not removed. You can still perform the following actions on a disabled call home center:

- Edit call home center configuration.
- Add devices and event filters to the call home center.

To disable a call home center, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.
2. Clear the **Enable** check box of the call home center you want to disable in the **Call Home Centers** table.

   The selected call home center and its devices and event filters become grayed out. However, the call home center is not actually disabled until you save your changes. When a device is assigned to the call home center, a confirmation message displays.
3. Click **OK** to confirm.
4. Click **OK** to close the **Call Home** dialog box.

Viewing Call Home status

You can view call home status from the main Management application window or from the **Call Home Notification** dialog box.

The Management application enables you to view the call home status at a glance by providing a call home status icon on the Status Bar. The following table illustrates and describes the icons that indicate the current status of the call home function.

TABLE 15 Call Home Icons

Icon	Description
☎	Normal— Displays when call home is enabled on all devices and no filters are applied.
☎⚠	Degraded— Displays when call home is enabled on all devices and at least one filter is active.
☎✗	Disabled— Displays when any of the following conditions are met: • At least one device's call home is disabled. • At least one non-manageable device. • At least one device does not have the Management server registered as a trap recipient.

To view more detail regarding call home status, click the **Call Home** icon. The **Call Home Notification** dialog box displays the list of devices that have assigned filters or call home disabled.

The following table explains the statuses that may be displayed in the **Call Home Notification** dialog box.

TABLE 16 Call Home Status

Status	Description
Enabled	The device is manageable, call home is enabled, and a filter is applied.
Disabled	Call home is disabled on at least one device or call home is disabled from the **Call Home** dialog box.
Not Manageable	Manageability is lost.
Server Not Registered	The Server is not registered to receive Call Home events from this device. **Note:** Fabric OS switches only.

Assigning a device to the call home center

Discovered devices (switches, routers, and directors) are not assigned to a corresponding call home center automatically. You must manually assign each device to a call home center before you use call home.

To assign a device or multiple devices to a call home center, complete the following steps.

1. Select Monitor > Event Notification > Call Home.

   The Call Home dialog box displays.

2. Select the devices you want to assign to a call home center in the Products List table.
3. Select the call home center to which you want to assign the devices in the Call Home Center table.

   You can only assign a device to one call home center at a time.

   If you do not select a call home center, the selection defaults to the first call home center in the Call Home Center table.

   If you have made a previous selection on an assigned device or filter and you do not select a call home center, the selection defaults to the previous selection's call home center.

4. Click the right arrow button.

   The selected devices display beneath the selected call home center. Devices assigned to a call home center do not display in the Products List table.

5. Click OK to close the Call Home dialog box.

Removing a device from a call home center

To remove a device or multiple devices from a call home center, complete the following steps.

1. Select Monitor > Event Notification > Call Home.

   The Call Home dialog box displays.

2. Select the call home center from which you want to remove devices in the Call Home Center table.
3. Select the devices you want to remove from the selected call home center.
4. Click the left arrow button.

   A confirmation message displays.

5. Click OK.

   The selected devices are removed from the call home center and display in the Products List table.

6. Click OK to close the Call Home dialog box.

Removing all devices and filters from a call home center

To remove all devices and filters from a call home center, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Select the call home center from which you want to remove devices and filters in the **Call Home Center** table.
3. Click the left arrow button.

   A confirmation message displays.

4. Click **OK**.

   All devices assigned to the selected call home center display in the **Products List** table. Any assigned filters are also removed.

5. Click **OK** to close the **Call Home** dialog box.

Defining an event filter

To define an event filter, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Click **Add** beneath the **Call Home Event Filter** table.

   The **Call Home Event Filter** dialog box displays.

3. Enter a name for the filter in the **Name** field.
4. Enter a name for the description in the **Description** field.
5. Select the events you want to include in the filter in the **Available Call Home Event Types** table.

   Click **Select All** to select all event types in the table or select **Unselect All** to clear the selected event types in the table. For more information about Call Home events, refer to Appendix B, “Call Home Event Tables”.

6. Click **OK**.

   The Event Filter name and the description are displayed in the **Call Home** dialog box.

7. Click **OK** to close the **Call Home** dialog box.

   To assign event filters to a call home center or a device, refer to “Assigning an event filter to a call home center” on page 176 or “Assigning an event filter to a device” on page 176.

Call Home for virtual switches

For virtual switches, there are two types of Call Home events:

- FRU-based Call Home events which are triggered at the chassis level.
- Port-based Call Home events, which are triggered for each virtual switch.

Assigning an event filter to a call home center

Event filters allow call home center users to log in to a Management server and assign specific event filters to the devices. This limits the number of unnecessary or 'acknowledge' events and improves the performance and effectiveness of the call home center.

You can only select one event filter at a time; however, you can assign the same event filter to multiple devices or call home centers. When you assign an event filter to a call home center, the event filter is assigned to all devices in the call home center. For more information about Call Home events, refer to Appendix B, "Call Home Event Tables".

NOTE
You cannot assign an event filter to a call home center that does not contain devices.

To assign an event filter to a call home center, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Select the event filters you want to assign in the **Call Home Event Filters** table.
3. Select the call home centers to which you want to assign the event filters in the **Call Home Centers** table.
4. Click the right arrow button.

   The selected event filters are assigned to the selected call home centers.

5. Click **OK** to close the **Call Home** dialog box.

Assigning an event filter to a device

To assign an event filter to a device, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Select the event filter you want to assign in the **Call Home Event Filters** table.

   For more information about Call Home events, refer to Appendix B, "Call Home Event Tables".

3. Select one or more devices to which you want to assign the event filter in the **Call Home Centers** table.
4. Click the right arrow button.

   The selected event filter is assigned to the selected devices. The event filter displays beneath the specified device or all of the devices under the specified call home center.

5. Click **OK** to close the **Call Home** dialog box.

Overwriting an assigned event filter

A device can only have one event filter at a time; therefore, when a new filter is applied to a device that already has a filter, you must confirm the new filter assignment.

To overwrite an event filter, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Select the event filter you want to apply in the **Call Home Event Filters** table.

   For more information about Call Home events, refer to Appendix B, “Call Home Event Tables”.

3. Select the devices to which you want to apply the event filter in the **Call Home Centers** table.

4. Click the right arrow button.

   For existing event filters, a confirmation messages displays.

5. Click **Yes**.

   The selected event filter is applied to the selected devices. The event filter displays beneath the specified device or all of the devices under the specified call home center.

6. Click **OK** to close the **Call Home** dialog box.

Removing an event filter from a call home center

To remove all event filters from a call home center, complete the following steps.

1. Select **Monitor** > **Event Notification** > **Call Home**.

   The **Call Home** dialog box displays.

2. Choose one of the following options in the **Call Home Centers** table:

   - Right-click a call home center and select **Remove Filters**.
   - Select the call home center and click the left arrow button.

     All event filters assigned to the call home center are removed.

3. Click **OK** to close the **Call Home** dialog box.

Removing an event filter from a device

To remove an event filter from a device, complete the following steps.

1. Select Monitor > Event Notification > Call Home.

   The Call Home dialog box displays.

2. Choose one of the following options in the Call Home Centers table:

   - Right-click an event filter assigned to a device and select Remove Filter.
   - Right-click a device to which the event filter is assigned and select Remove Filter.
   - Select an event filter assigned to a device and click the left arrow button. Press CTRL and click to select multiple event filters assigned to multiple devices.

   All event filters assigned to the device are removed.

3. Click OK to close the Call Home dialog box.

Removing an event filter from the Call Home Event Filters table

1. Select Monitor > Event Notification > Call Home.

   The Call Home dialog box displays.

2. Select the event filter you want to remove in the Call Home Event Filters table.
3. Click Remove.

   - If the event filter is not assigned to any devices, a confirmation message displays asking if you want to remove the event filter. Click Yes.
   - If the event filter is assigned to any devices, a confirmation message displays informing you that removing this event filter will remove it from all associated devices. Click Yes.

     The event filter is removed from any associated devices and the Call Home Event Filters table.

     To determine to which devices the event filter is assigned, select the event filter and then click the find button (>).

4. Click OK to close the Call Home dialog box.

Searching for an assigned Event Filter

To find all devices to which an event filter is assigned, complete the following steps.

1. Select Monitor > Event Notification > Call Home.

   The Call Home dialog box displays.

2. Select the event filter you want to find in the Call Home Event Filters table.
3. Click > (find button).
4. All instances of the event filter are highlighted in the Call Home Centers table.

   If the selected event filter is not assigned to any devices in the Call Home Centers table, a not found message displays.

Chapter

View Management 8

In this chapter

View management overview

You can customize the topology by creating views that include certain fabrics or devices and then switch between the views to see specific information about those fabrics or devices.

If you discover or import a network with more than approximately 2000 devices, the devices display on the Product List, but not on the Topology Map. Instead, the Topology Map shows a message stating that the topology cannot be displayed. To resolve this issue, create a new view to filter the number of devices being discovered. Refer to “Creating a customized view” on page 180 for instructions.

Creating a customized view

You may want to customize the Product List and Connectivity Map to simplify management of large SANs by limiting the topology size or Product List columns.

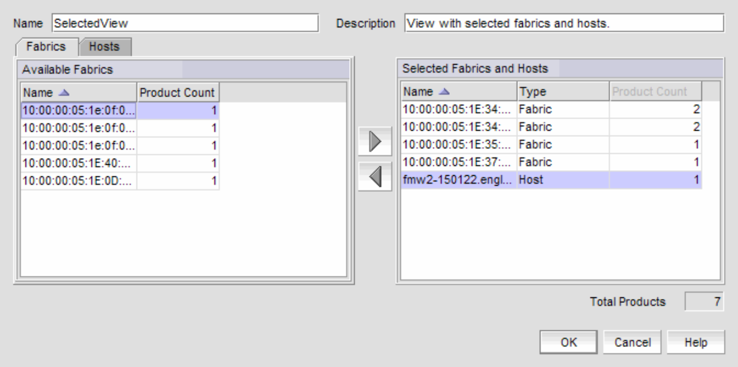
For each customized view, you can specify the fabrics and hosts that display on the Connectivity Map, as well as the columns and device groupings that display on the Product List.

Customized view settings reside on the server. Only users with the same login to the same server can see and select the view settings. No individual user can have access to the views created by another user.

If you select a customized view and new devices are discovered, those new devices display in the customized view if they belong in that view category or fabric.

1. Use one of the following methods to open the **Create View** dialog box:
   - Select **View** > **Manage View** > **Create View.**
   - Select **Create View** from the **View All** list. The **View All** list does not display until you discover a fabric or host.

     The **Create View** dialog box displays.



Name: SelectedView

Description: View with selected fabrics and hosts.

Available Fabrics

Name	Product Count
10:00:00:05:1e:0f:0...	1
10:00:00:05:1e:0f:0...	1
10:00:00:05:1e:0f:0...	1
10:00:00:05:1E:40:...	1
10:00:00:05:1E:0D:...	1

Selected Fabrics and Hosts

Name	Type	Product Count
10:00:00:05:1E:34:...	Fabric	2
10:00:00:05:1E:34:...	Fabric	2
10:00:00:05:1E:35:...	Fabric	1
10:00:00:05:1E:37:...	Fabric	1
fmw2-150122.engl...	Host	1

Total Products: 7

FIGURE 62 **Create View dialog box - Fabrics tab**

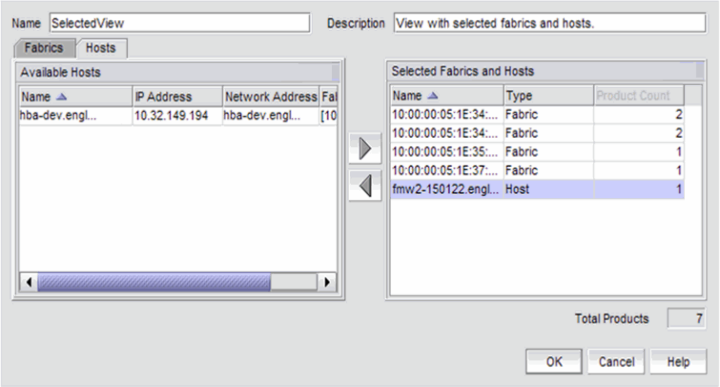
2. Enter a name (128-character maximum) in the **Name** field and a description (126-character maximum) in the **Description** field for the view.

NOTE
You cannot use the name “View” or “View All” in the **Name** field.

NOTE
You cannot use an existing name in the **Name** field.

3. Click the **Fabrics** tab.
4. In the **Available Fabrics** table, select the fabrics you want to include in the view and click the right arrow button to move your selections to the **Selected Fabrics and Hosts** table.

   To select more than one row, press CTRL and click individual rows. To select muliple sequental rows, press SHIFT and click on a sequence of rows.
5. Click the **Hosts** tab.



Name: SelectedView

Description: View with selected fabrics and hosts.

Available Hosts

Name	IP Address	Network Address	Fal
hba-dev.engl...	10.32.149.194	hba-dev.engl...	[10

Selected Fabrics and Hosts

Name	Type	Product Count
10:00:00:05:1E:34:...	Fabric	2
10:00:00:05:1E:34:...	Fabric	2
10:00:00:05:1E:35:...	Fabric	1
10:00:00:05:1E:37:...	Fabric	1
fmw2-150122.engl...	Host	1

Total Products: 7

FIGURE 63 Create View dialog box - Hosts tab

6. In the **Available Hosts** table, select the hosts you want to include in the view and click the right arrow button to move your selections to the **Selected Fabrics and Hosts** table.
7. Click **OK** to save the customized view and close the **Create View** dialog box.

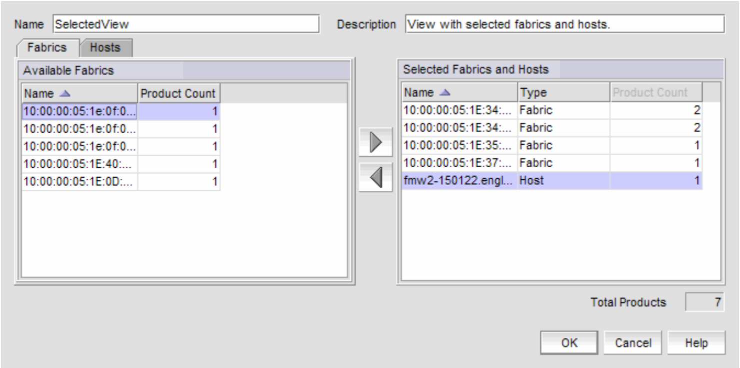
   The new view displays automatically in the main window of the Management application.

Editing a customized view

You can only edit customized views that you have created.

1. Use one of the following methods to open the **Edit View** dialog box:
   - Select **View** > **Manage View** > **Edit View** > *View_Name*.
   - Select **Edit View** from the **View All** list. The **View All** list does not display until you discover a fabric or host.

     The **Edit View** dialog box displays.



Name: SelectedView

Description: View with selected fabrics and hosts.

Fabrics | Hosts

Available Fabrics

Name	Product Count
10:00:00:05:1e:0f:0...	1
10:00:00:05:1e:0f:0...	1
10:00:00:05:1e:0f:0...	1
10:00:00:05:1E:40:...	1
10:00:00:05:1E:0D:...	1

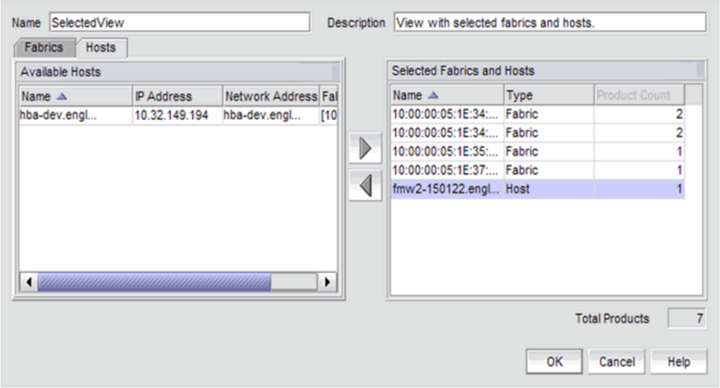
Selected Fabrics and Hosts

Name	Type	Product Count
10:00:00:05:1E:34:...	Fabric	2
10:00:00:05:1E:34:...	Fabric	2
10:00:00:05:1E:35:...	Fabric	1
10:00:00:05:1E:37:...	Fabric	1
fmw2-150122.engl...	Host	1

Total Products: 7

FIGURE 64 Edit View dialog box - Fabrics tab

2. Click the **Fabrics** tab.
3. In the **Available Fabrics** table, select the fabrics you want to include in the view and use the right arrow button to move your selections to the **Selected Fabrics and Hosts** table.
4. Click the **Hosts** tab.



Name: SelectedView

Description: View with selected fabrics and hosts.

Fabrics | Hosts

Available Hosts

Name	IP Address	Network Address	Fal
hba-dev.engl...	10.32.149.194	hba-dev.engl...	[10

Selected Fabrics and Hosts

Name	Type	Product Count
10:00:00:05:1E:34:...	Fabric	2
10:00:00:05:1E:34:...	Fabric	2
10:00:00:05:1E:35:...	Fabric	1
10:00:00:05:1E:37:...	Fabric	1
fmw2-150122.engl...	Host	1

Total Products: 7

FIGURE 65 Edit View dialog box - Hosts tab

5. In the **Available Hosts** table, select the fabrics you want to include in the view and use the right arrow button to move your selections to the **Selected Fabrics and Hosts** table.
6. To remove fabrics and hosts from a view, select the fabrics and hosts you want to remove in the **Selected Fabrics and Hosts** table and click the left arrow button.
7. Click **OK** to save your changes and close the **Edit View** dialog box.
8. Verify your changes on the main window of the Management application.

Deleting a customized view

To delete a customized view, use the following procedure.

1. Select **View** > **Manage View** > **Delete View** > *View_Name*.
2. Click **Yes** on the message.

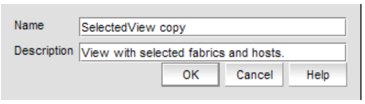
   If you delete the current view, the view changes to the default view (View All).

Copying a view

To copy a customized view, use the following procedure.

1. Use one of the following methods to open the **Copy View** dialog box:
   - Select **View** > **Manage View** > **Copy View** > *View_Name*.
   - Select **Copy View** from the **View All** list. The **View All** list does not display until you discover a fabric or host.

     The **Copy View** dialog box displays the name of the view you are copying.



Name SelectedView copy

Description View with selected fabrics and hosts.

FIGURE 66 **Copy View dialog box**

2. Enter a name (128-character maximum) in the **Name** field and a description (126-character maximum) in the **Description** field for the view.

NOTE
You cannot use the name “View” or “View All” in the **Name** field.

NOTE
You cannot use an existing name in the **Name** field.

3. Click **OK** to save your changes and close the **Copy View** dialog box.
4. Verify that the copied view displays on the main window of the Management application.

SAN topology layout

You can customize various parts of the topology, including the layout of devices and connections and 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.** Select to specify a new layout for the desktop icons, background color for groups, and line type for connections between icons.
- **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 user and attached port numbers in decimal format.
  - **Hex.** Select to display all domain IDs and user and attached port numbers in hex format.
- **Product Label**. Select to configure which product labels display.

  NOTE
  Changes apply to all fabrics present in the topology when the **Product Label** option is selected.

  - **Name (Product).** Displays the product name as the product label.
  - **Node WWN.** Displays the world wide 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.
  - **Zone Alias.** Displays the zone alias as the product label.
- **Port Label.** Select to configure which port labels display.

  NOTE
  Changes apply to the selected fabric or the fabric to which the selected item belongs.

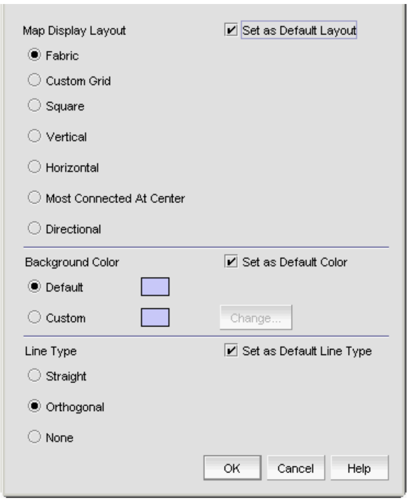
  - **Name.** Displays the name as the port label. If the port has not been given a name, the WWN of the port displays.
  - **Port Number.** Displays the port number as the port label.
  - **Port Address.** Displays the port address as the port label.
  - **Port WWN.** Displays the port world wide name as the port label.
  - **User Port #.** Displays the user's port number as the port label.
  - **Slot/Port.** Displays the slot and port as the port label for a chassis switch and the port number for a switch.
  - **Zone Alias.** Displays the zone alias 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 Connectivity Map) that are connected to other devices.
  - **UnOccupied Product Ports.** Select to display the ports of the devices (shown in the Connectivity Map) that are not connected to any other device.
  - **Attached Ports.** Select to display the attached ports of the target devices.
  - **Switch to Switch Connections.** Select to display the switch-to-switch connections. Switch-to-switch connections only display when the **Attached Ports** option is also selected.

Customizing the layout of devices on the topology

You can customize the layout of devices by group type or for the entire Connectivity Map. Customizing the layout makes it easier to view the SAN and manage its devices. Group types include Fabric, Host, Storage, Router and Switch groups.

1. Right-click a group or the Connectivity Map and select **Map Display.**

   The **Map Display Properties** dialog box displays. The **Map Display Layout** list varies depending on what you selected (group type or Connectivity Map).



Map Display Layout ☑ Set as Default Layout
● Fabric
○ Custom Grid
○ Square
○ Vertical
○ Horizontal
○ Most Connected At Center
○ Directional

Background Color ☑ Set as Default Color
● Default
○ Custom

Line Type ☑ Set as Default Line Type
○ Straight
● Orthogonal
○ None

FIGURE 67 Map Display Properties dialog box

2. Select one of the following options from the **Map Display Layout** list:

   - **Free Form.** Select to display the devices in the default format for Switch Groups and Router Groups.
     When the **Free Form** map display layout is selected, the **View > Show Ports** menu command is unavailable.
   - **Fabric.** Only available for the group type “Fabric”. Select to display the devices in the default format.
   - **Custom Grid.** Select to be able 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. A device cannot be moved outside of its group.
   - **Square.** Select to display the device icons in a square configuration. Default for Host and Storage groups.
   - **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.

3. Select the **Set as Default Layout** check box to set your selection as the default.
4. Click **OK** on the **Map Display Properties** dialog box.

Customizing the layout of connections on the topology

You can change the way inter-device connections display on the topology.

1. Right-click a group or the Connectivity Map and select **Map Display.**

   The **Map Display Properties** dialog box displays.

2. Select one of the following options from the **Line Tepe** list:
   - **Straight.** Select to display connections using straight lines.
   - **Orthogonal.** Select to display connections in orthogonal grid lines. Disabled if **Free Form** is selected in **Map Display Layout** area.
   - **None.** Select to hide the connections between devices.
3. Select the **Set as Default Layout** check box to set your selection as the default.
4. Click **OK** on the **Map Display Properties** dialog box.

Changing a group background color

You can customize the topology by changing the background color of a group.

1. Right-click a group or the Connectivity Map and select **Map Display.**

   The **Map Display Properties** dialog box displays.

2. Select the **Custom** option and click **Change.**

   The **Choose a background color** dialog box displays (Figure 68).

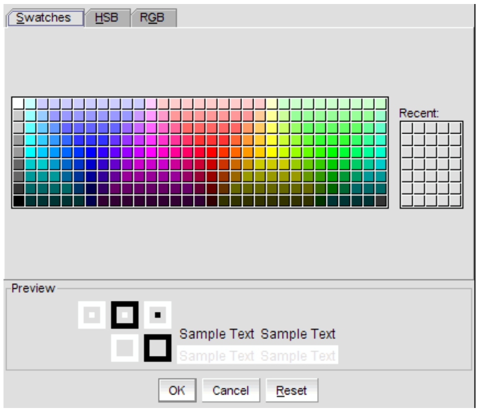


FIGURE 68 Choose a background color dialog box

3. Select or specify a color and preview it in the **Preview** pane.
   - To pick a color from a swatch, select the **Swatches** tab. Select a color from the display.
   - 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%).
   - 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).
4. Click **OK** to change the background color, or click **Reset** to return all settings to the color currently being displayed on the topology.
5. Click **OK** on the **Map Display Properties** dialog box.

Reverting to the default background color

To revert back to the default background color, complete the following steps.

1. Right-click a group and select **Map Display**.

   The **Map Display Properties** dialog box displays.
2. Select the **Default** option.
3. Click **OK** on the **Map Display Properties** dialog box.

Changing the product label

To change the product label, complete the following steps.

1. Select a product in the Connectivity Map or Product List.
2. Select **View > Product Label**, and select one of the following options:
   - **Name (Product).** Displays the product name as the product label.
   - **WWN.** Displays the world wide 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.
   - **Zone Alias.** Displays the zone alias as the product label.

   Changes apply to all fabrics present in the topology when the **Product Label** option is selected.

Changing the port label

To change the port label, complete the following steps.

1. Select a port in the Connectivity Map or Product List.
2. Select View > Port Label, and select one of the following options:
   - 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 WWN. Displays the port world wide name as the port label.
   - User Port #. Displays the user's port number as the port label.
   - Slot/Port. Displays the slot and port as the port label.
   - Zone Alias. Displays the zone alias 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
Connected (or occupied) 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 View > Port Display, and select one of the following options:
   - Occupied Product Ports. Select to display the ports of the devices in the fabrics (present in the Connectivity Map) that are connected to other devices.
   - Unoccupied Product Ports. Select to display the ports of the devices (shown in the Connectivity Map) that are not connected to any other device.
   - Attached Ports. Select to display the attached ports of the target devices.
   - Switch to Switch Connections. Select to display the connections between devices. Switc- t-switch connections only display when the Attached Ports option is also selected.
2. Repeat step 1 to select more than one port display option.

Grouping on the topology

To simplify management, devices display in groups. Groups are shown with background shading and are labeled appropriately. You can expand and collapse groups to easily view a large topology.

Collapsing groups

To collapse a single group on the topology, choose one of the following options:

- Click the icon at the top right-hand corner of the group on the topology (▬).
- Double-click in the group, but not on a device.
- Right-click in a group, but not on a device, and select Collapse from the shortcut menu.

To collapse all groups on the topology by one level, click the Collapse button on the Connectivity Map toolbar (↙).

Expanding groups

To expand a group on the topology, do one of the following:

- Double-click the group icon.
- Right-click the group icon and select Expand from the shortcut menu.

To expand all groups on the topology by one level, click the Expand button on the Connectivity Map toolbar (↗).

Viewing connections

You can view the connections in a fabric using one of the following methods:

- Select a fabric and then select View > Connected End Devices and select Include Virtual Devices, Hide All, Show All, or Custom.
- Right-click the fabric and select Connected End Devices > Include Virtual Devices, Hide All, Show All, or Custom from the shortcut menu.

NOTE
Selecting Hide All disables the Include Virtual Devices option.

Configuring custom connections

NOTE
Active zones must be available on the fabric.

To create a display of the connected end devices participating in a single zone or group of zones, complete the following steps.

1. Choose one of the following options:
   - Select a fabric on the topology and select **View** > **Connected End Devices** > **Custom**.
   - Right-click a fabric on the topology and select **Connected End Devices** > **Custom** from the shortcut menu.

   The **Connected End Devices - Custom display for** *Fabric* dialog box displays with a list of zones in the **Zones in** *Fabric* list.
2. Select the zones you want to include in the connection in the **Zones in** *Fabric* list.
3. Select the application to which you want to add the selected zones in the **Application** list.
4. Click the right arrow button to move the zones to the **Selected Zones** list.
5. Click **OK**.

Saving a custom connection configuration

NOTE
Active zones must be available on the fabric.

To save a new custom connection configuration, complete the following steps.

1. Choose one of the following options:
   - Select a fabric on the topology and select **View** > **Connected End Devices** > **Custom**.
   - Right-click a fabric on the topology and select **Connected End Devices** > **Custom** from the shortcut menu.

   The **Connected End Devices - Custom display for** *Fabric* dialog box displays with a list of zones in the **Zones in** *Fabric* list.
2. Select the zones you want to include in the connection in the **Zones in** *Fabric* list.
3. Click the right arrow button to move the selected zones to the **Selected Zones** list.
4. Click **Save**.

   The **Save Application** dialog box displays.
5. Enter a new name in the **Application Name** field.
6. Click **OK** on the **Save Application** dialog box.
7. Click **OK** on the **Connected End Devices - Custom display for** *Fabric* dialog box.

   The saved custom connection configuration displays in the **Connected End Devices** menu.

Deleting a custom connection configuration

NOTE
Active zones must be available on the fabric.

To delete a custom connection configuration, complete the following steps.

1. Choose one of the following options:
   - Select a fabric on the topology and select **View** > **Connected End Devices** > **Custom**.
   - Right-click a fabric on the topology and select **Connected End Devices** > **Custom** from the shortcut menu.

   The **Connected End Devices - Custom display for** *Fabric* dialog box displays.
2. Select the configuration you want to delete in the **Application** list.
3. Click **Delete**.
4. Click **OK** on the confirmation message.
5. Click **OK** on the **Connected End Devices - Custom display for** *Fabric* dialog box.

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 Connectivity Map (topology) or Product List.

Zooming in and out of the Connectivity Map

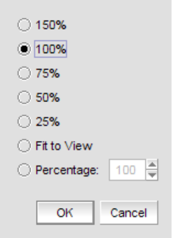
You can zoom in or out of the Connectivity Map to see products and ports.

Zooming in

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

- Click the zoom-in icon (🔍) on the Connectivity Map toolbar.
- Press CTRL and the plus sign on the number pad on the keyboard.
- Use the **Zoom** dialog box.
  a. Select **View** > **Zoom**.

     The **Zoom** dialog box displays.



○ 150%
● 100%
○ 75%
○ 50%
○ 25%
○ Fit to View
○ Percentage: 100

FIGURE 69 Zoom dialog box

b. Select a zoom percentage.

c. Click **OK** to save your changes and close the **Zoom** dialog box.

Zooming out

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

- Click the zoom-out icon (🔍) on the Connectivity Map toolbar.
- Press CTRL and the minus sign on the number pad on the keyboard.
- Use the **Zoom** dialog box.

  a. Select **View > Zoom**.

  The **Zoom** dialog box displays.

  b. Select a zoom percentage.

  c. Click **OK** to save your changes and close the **Zoom** dialog box.

Showing levels of detail on the Connectivity Map

You can configure different levels of detail on the Connectivity Map, making device management easier.

Viewing fabrics

To view only fabrics, without seeing groups, products, or ports, select **View > Show> Fabrics Only.**

Viewing groups

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

Viewing products

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

Viewing ports

To view all ports, select **View > Show> All Ports.**

Exporting the topology

You can save the topology to an image (PNG format).

1. Click **Export** in the toolbar.

   The **Export Topology To PNG File** dialog box displays.

2. Browse to the directory where you want to export the image.
3. Edit the name in the **File Name** field, if necessary.

4. Click **Save**.

   If the file name is a duplicate, a message displays. Click **Yes** to replace the image or click **No** to go back to the **Export Topology To PNG File** dialog box and change the file name.

   The **File Download** dialog box displays.

5. Click **Open** to view the image or click **Cancel** to close the dialog box.

Customizing application tables

You can customize any table in the Management application main interface (for example, the Master Log or the Product List) or in individual dialog boxes in the following ways:

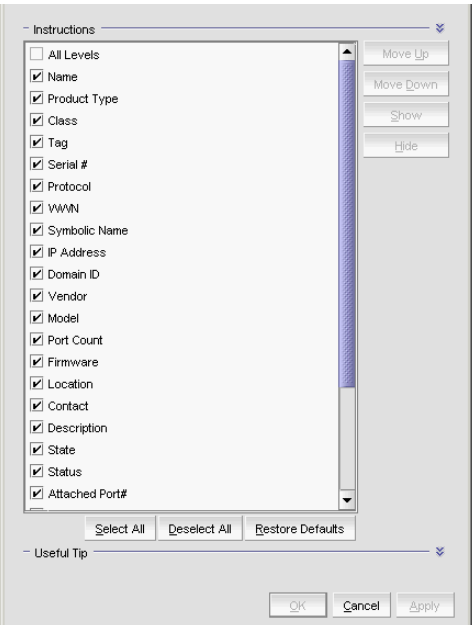
- Display only specific columns
- Display columns in a specific order
- Resize the columns to fit the contents
- Sort the table by a specific column or multiple columns
- Copy information from the table to another application
- Export information from the table
- Search for information
- Expand the table to view all information
- Collapse the table

Displaying columns

To only display specific columns, complete the following steps.

1. Right-click anywhere in the table and select **Customize** or **Table > Customize**.

   The **Customize Columns** dialog box displays.



□ All Levels
☑ Name
☑ Product Type
☑ Class
☑ Tag
☑ Serial #
☑ Protocol
☑ WWN
☑ Symbolic Name
☑ IP Address
☑ Domain ID
☑ Vendor
☑ Model
☑ Port Count
☑ Firmware
☑ Location
☑ Contact
☑ Description
☑ State
☑ Status
☑ Attached Port#

FIGURE 70 Customize Columns dialog box

2. Choose from the following options:
    - Select the check box to display a column.
      OR
      Select the column name and click **Show**.
    - Clear the check box to hide a column.
      OR
      Select the column name and click **Hide**.
    - Click **Select All** to select all check boxes.
    - Click **Deselect All** to clear all check boxes.
    - Click **Restore Defaults** to restore the table to the original settings.
3. Click **OK**.

Changing the order of columns

To change the order in which columns display, choose from one of the following options.

Rearrange columns in a table by dragging and dropping the column to a new location.

OR

1. Right-click anywhere in the table and select **Customize** or **Table > Customize**.

   The **Customize Columns** dialog box displays.
2. Select the name of the column you want to move and use the **Move Up** button and **Move Down** button to move it to a new location.
3. Click **OK**.

Resizing the columns

You can resize a single column or all columns in the table.

To resize a single column, right-click the column header and select Size Column to Fit or Table > Size Column to Fit.

To resize all columns in the table, right-click anywhere in the table and select Size All Columns to Fit or Table > Size All Columns to Fit.

Sorting table information

To sort the table by a single column, click the column header.

To reverse the sort order, click the column header again.

To sort the table by multiple columns, complete the following steps.

1. Click the primary column header.
2. Press CTRL and click a secondary column header.

Copying table information

You can copy the entire table or a specific row to another application (such as Notepad, Excel, Word, and so on).

1. Choose from one of the following options:
   - Right-click anywhere in the table and select Table > Copy Table.
   - Select the table row that you want to export and select Table > Copy Row.
2. Open the application to which you want to copy the Product List information.
3. Select Edit > Paste (or press CTRL + V).
4. Save the file.

Exporting table information

You can export the entire table or a specific row to a text file.

1. Choose from one of the following options:
   - Right-click anywhere in the table and select Table > Export Table.
   - Select the table row that you want to export and select Table > Export Row.

   The Save table to a tab delimited file dialog box displays.
2. Browse to the location where you want to save the file.
3. Enter the file name in the File Name field.
4. Click Save.

Searching for information in a table

You can search for information in the table by any of the values found in the table.

1. Right-click anywhere in the table and select **Table > Search.**

   The focus moves to the Search field.

   FIGURE 71 Search field

2. Enter all or part of the search text in the Search field and press **Enter.**

   The first instance is highlighted in the table.

3. Press **Enter** to go to the next instance of the search text.

Expanding and collapsing tables

You can expand a table to display all information or collapse it to show only the top level.

To expand the entire table, right-click anywhere in the table and select **Expand All** or **Table > Expand All.**

To collapse the entire table, right-click anywhere in the table and select **Collapse All** or **Table > Collapse All.**

Search

You can search for a device by text or regular expression.

- **Text**—Enter a text string in the search text box. This search is case sensitive.

  For example, you can enter the first five characters in a device name. All products in the Product List that contain the search text display highlighted.

- **Regular Expression**—Enter a Unicode regular expression in the search text box. (For hints, refer to "Regular Expressions" on page 961.) All products in the Product List that contain the search text display highlighted. This search is case insensitive.

  For example, you might need to search ports. To search for a port using a Unicode regular expressions, enter "2/1|2/2|2/3". This search will find Ports 2/1, 2/2, and 2/3 on all devices.

Searching for a device

You can search for a device by name, WWN, or device type. When searching in the Connectivity Map, make sure you search the right view (**View** > **Manage View** > **Display View** > *View_Name*) with the appropriate options of port display (**View** > **Port Display** > *Display_Option*) and connected end devices (**View** > **Port Display** > **Show All**) enabled.

To search for a device, complete the following steps.

1. Enter your search criteria in the search field.

   NOTE
   To search for a device, the device must be discovered and display in the topology.

2. Choose one of the following options:
   - Select **Text** from the search list and enter a text string in the search text box.

     This search is case sensitive.
   - Select **Regular Expression** from the search list and enter a Unicode regular expression in the search text box.

     This search is case insensitive
3. Press **Enter** or click the search icon.

   The search results display highlighted.

   If the search finds more than one match, a message displays, advising you to restrict the search by restricting the search by node (refer to "Restricting a search by node" on page 197) or by looking for exact matches (refer to "Searching for an exact match" on page 198).

Restricting a search by node

When a device is assigned to a product group, it may be listed in the Product node, as well as Product Groups node. Therefore the search results include the device under both the Product node and the Product Group node.

NOTE
To search for a device, the device must be discovered and display in the topology.

To restrict the search only to specific nodes, complete the following steps.

1. Select the Product node or Product Group node that you want to search.
2. Choose one of the following options:
   - Select **Text** from the search list.
   - Select **Regular Expression** from the search list.

3. Enter your search criteria in the search field.
   - **Text**—Enter a text string in the search text box. This search is case sensitive.

     For example, you can enter the first five characters in a device name. All products in the Product List that contain the search text display highlighted.
   - **Regular Expression**—Enter a Unicode regular expression in the search text box. (For hints, refer to "Regular Expressions" on page 961.) All products in the Product List that contain the search text display highlighted. This search is case insensitive.
4. Press **Enter** or click the search icon.

   The search results display highlighted.

Searching for an exact match

To search for an exact match, complete the following steps.

1. Choose one of the following options:
   - Select **Text** from the search list.
   - Select **Regular Expression** from the search list.
2. Enter your search criteria in the search field.
   - **Text**—Enter a text string in the search text box. This search is case sensitive.

     For example, you can enter the first five characters in a device name. All products in the Product List that contain the search text display highlighted.
   - **Regular Expression**—Enter a Unicode regular expression in the search text box. (For hints, refer to "Regular Expressions" on page 961.) All products in the Product List that contain the search text display highlighted. This search is case insensitive.
3. Press **Ctrl** and click the search icon.

   The search results display highlighted.

   Example

   If you search for IP address "192.1.1.101" and then press CTRL and click the search icon, the application only highlights "192.1.1.101". This search does not highlight "SI-101 [192.1.1.101]".

   If you search for port "1/2" and then press CTRL and click the search icon, the application only highlights port "1/2". This search does not highlight ports "1/2", "1/20", "1/21", "1/22", and so forth.

Clearing search results

To clear search results, select **Clear Search** from the search list.

Chapter

Third-party tools

9

In this chapter

About third-party tools

NOTE
Installing tools is only available with the Trial and Licensed version versions.

You can open other software products (such as, Firefox, Windows Explorer, Web Tools, Element Managers, FCR Configuration, HCM Agent and so on) you frequently use from the **Tools** menu or shortcut menus.

You can add third-party tools to the **Tools** menu or shortcut menus to open other software products (such as, Firefox, Windows Explorer, Web Tools, Element Managers, FCR Configuration, HCM Agent and so on) you frequently use.

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 the device's shortcut menu.

NOTE
Installing tools is only available with the Trial and Licensed version versions.

To open an application, perform the following steps.

1. Select the device.
2. Use one of the following techniques:
   - Select **Tools** > **Product Menu** > *Tool_Name*.
   - Select **Tools** > *Tool_Name*.
   - Right-click the device, and select the tool from the menu.

     If the third-party tool is a web-based application, you must enter the IP address of the applications server as a parameter to be able to open the application. For step-by-step instructions about entering the IP address of the server, refer to "Entering the server IP address of a tool" on page 211.

Launching a Telnet session

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

NOTE
The device 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.

Launching an Telnet session from the SAN tab

To launch a telnet session, complete the following steps.

On the Connectivity Map, right-click a device and select **Telnet** or **Telnet through Server.**

NOTE
Telnet through Server is only supported on Windows systems.

OR

1. Select the switch to which you want to connect.
2. Select **Tools** > **Product 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 Fibre Channel switches and directors. You can open a device's Element Manager directly from the application.

To launch a device's Element Manager, complete the following steps.

On the Connectivity Map, double-click the device you want to manage.

The Element Manager displays.

OR

On the Connectivity Map, right-click the device you want to manage and select **Element Manager > Hardware**.

The Element Manager displays.

OR

1. Select a device.
2. Select **Configure > Element Manager > Hardware**.

   The Element Manager displays.

OR

1. Select a device.
2. Click the Element Manager icon on the toolbar.

   The Element Manager displays.

Launching Web Tools

Use Web Tools to enable and manage Fabric OS access gateway, switches, and directors. You can open Web Tools directly from the application. For more information about Web Tools, refer to the *Brocade Web Tools Administrator's Guide.* For more information about Fabric OS access gateway, switches, and directors, refer to the documentation for the specific device.

To launch a device's Element Manager, complete the following steps.

NOTE
You must have Element Manager - Product Administration privileges for the selected device to launch Web Tools. If you do not have Element Manager - Product Administration privileges, you will need to enter those credentials to launch Web Tools.

On the Connectivity Map, double-click the Fabric OS device you want to manage.

Web Tools displays.

OR

On the Connectivity Map, right-click the Fabric OS device you want to manage and select **Element Manager > Hardware**.

Web Tools displays.

OR

1. Select a Fabric OS device.
2. Select **Configure > Element Manager > Hardware**.

   Web Tools displays.

OR

1. Select a Fabric OS device.
2. Click the Element Manager icon on the toolbar.

   Web Tools displays.

   NOTE
   When you close the Management application client, any Web Tools instance launched from the clients closes as well.

Launching FCR configuration

Use FCR Configuration to launch the FC Routing module, which enables you to share devices between fabrics without merging the fabrics. You can open the FC Routing module directly from the Management application. For more information about FC Routing, refer to the *Brocade Web Tools Administrator's Guide*.

The FCR Configuration option is available only for the following devices with Fabric OS 5.0 or later:

- Fabric OS extension switch
- Fabric OS Directors configured with an extension blade
- Fabric OS 1U, 40-port, 8 Gbps FC Switch (with Integrated Routing license)
- Fabric OS 2U, 80-port, 8 Gbps FC Switch (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 16-port Blade (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 32-port Blade (with Integrated Routing license)
- Fabric OS directors configured with a FC 8 GB 48-port Blade (with Integrated Routing license)

  Note that on the FC 8 GB 48-port Blade, the Shared Area ports, for example, 16-47, cannot be configured as EX_ports

NOTE
You must have Element Manager - Product Administration privileges for the selected device to launch Web Tools. If you do not have Element Manager - Product Administration privileges, you will need to enter those credentials to launch Web Tools.

On the Connectivity Map, right-click the Fabric OS device you want to configure and select **Element Manager > Router Admin**.

OR

1. Select a Fabric OS device.
2. Select **Configure > Element Manager > Router Admin**.

   The FC Routing module displays.

   NOTE
   When you close the Management application client, any Web Tools instance launched from the clients closes as well.

Launching Name Server

Use Name Server to view entries in the Simple Name Server database. You can open the Name Server module directly from the Management application. For more information about Name Server, refer to the *Brocade Web Tools Administrator's Guide*.

NOTE
You must have Element Manager - Product Administration privileges for the selected device to launch Web Tools. If you do not have Element Manager - Product Administration privileges, you will need to enter those credentials to launch Web Tools.

On the Connectivity Map, right-click the Fabric OS device you want to configure and select Element Manager > Name Server.

The Name Server module displays.

OR

1. Select a Fabric OS device.
2. Select Configure > Element Manager > Name Server.

   The Name Server module displays.

   NOTE
   When you close the Management application client, any Web Tools instance launched from the clients closes as well.

Launching HCM Agent

Use Fabric OS HCM Agent to enable and manage Fabric OS HBAs. You can open HCM Agent directly from the application. For more information about HCM Agent, refer to the *HCM Agent Administrator's Guide.* For more information about Fabric OS HBAs, refer to the documentation for the specific device.

To launch a Fabric OS HBA's Element Manager, complete the following steps.

NOTE
You must have Element Manager - Product Administration privileges for the selected device to launch HCM Agent. If you do not have Element Manager - Product Administration privileges, you will need to enter those credentials to launch HCM Agent.

On the Connectivity Map, double-click the Fabric OS HBA or CNA device you want to manage.

HCM Agent displays.

OR

On the Connectivity Map, right-click the Fabric OS HBA or CNA device you want to manage and select **Element Manager**.

HCM Agent displays.

OR

1. Select a Fabric OS HBA or CNA.
2. Select **Configure > Element Manager > HCM**.

   HCM Agent displays.

OR

1. Select a Fabric OS HBA or CNA device.
2. Click the Element Manager icon on the toolbar.

   HCM Agent displays.

Launching Fabric Watch

Use Fabric Watch as an health monitor that allows you to enable each switch to constantly monitor its SAN fabric for potential faults and automatically alerts you to problems long before they become costly failures.. For more information about Fabric Watch, refer to the Fabric Watch *Administrator's Guide.* For more information about Fabro OS access gateway, switches, and directors, refer to the documentation for the specific device.

To launch Fabric Watch, complete the following steps.

NOTE
You must have Fabric Watch privileges for the selected device to launch Fabric Watch. If you do not have Fabric Watch privileges, you will need to enter those credentials to launch Fabric Watch.

NOTE
You must have the Fabric Watch license for the selected device.

On the Connectivity Map, right-click the Fabric OS device you want to monitor and select **Fabric Watch > Configure.**

Fabric Watch displays.

OR

1. Select a Fabric OS device.
2. Select **Monitor > Fabric Watch > Configure.**

   Fabric Watch displays.

Single sign on support for IBM

The Management application supports single sign on (SSO) for IBM products such as IBM Tivoli Storage Productivity Center (TPC) or IBM Systems Director. Although SSO is not required, it creates a more seamless experience between the Management application server and IBM TPC or IBM Systems Director. There are several functions within the IBM TPC that launch the Management application client. If SSO is not enabled, each time the Management application client is launched, you must verify your Management application credentials. By enabling SSO, the Management application can authenticate against IBM TPC and launch the specified dialog box directly. This reduces the number of authentication steps required by you.

To configure the Management application to support SSO, complete the following steps.

1. Create the trust store on the IBM product.

   The trust store is used to establish SSL communication between the Management application and the IBM product for authentication. For instructions, refer to the IBM Systems Director or TPC documentation about configuring users.

2. Configure the Management application by completing the following steps.
   a. Copy the trust store to the Management application directory (*Install_Home*\bin\tpc).

      The Management application directory is located in *Install_Home*\bin\tpc (Windows systems) or *Install_Home*/bin/tpc (UNIX systems).

      The trust store is located where you specified in step 1.

b. Open a **Command Prompt** window.

c. Type **cd** *Install_Home***\bin\tpc** and press **Enter** to go to the tpc directory.

d. Type **tpcssosetup.bat** (Windows systems) or **sh tpcssosetup** (UNIX systems) with the following parameters:

```
IP of the host where IBM product is running as the 1st parameter,
The port number as the 2nd parameter, the default is 16311,
The trust store name as the 3rd parameter,
The password for the trust store as the 4th parameter,
Basic authentication user name, this is a user in the LDAP server where IBM
product authenticate with, as the 5th parameter, and basic authentication
user's password the 6th parameter
```

Example (Windows systems)

```
tpcssosetup 10.32.1.1 16311 ibm_higgins_sso_10.32.1.1.jks password
tipadmin super123
```

Example (UNIX systems)

```
sh tpcssosetup 10.32.1.1 16311 ibm_higgins_sso_10.32.1.1.jks password
tipadmin super123
```

e. Press **Enter** to configure single sign on for the Management application.

3. Create a new user account in the Management application, including user name, password, and resource group.

   This account must match the IBM Systems Director or TPC user account. To create a user account, refer to "Creating a new user account" on page 140.

4. Make sure any switches you need to manage are discovered by the Management application. Add switch/fabric into the Management applciation by selecting Discovery > Setup > Add Fabric.

   To discover a switch or fabric, refer to "Discovering fabrics" on page 53.

5. Restart the Management application.

Launch in context support for IBM

This Management application supports launch in context (LIC) for IBM products such as IBM Tivoli Storage Productivity Center (TPC) or IBM Systems Director. The Management application includes a package to deploy and remove the LIC menus for IBM TPC on Windows systems.

1. Copy tpc_*Application_Name*_ldf.zip to any directory on the TPC host.

   This procedure uses the *Install_Home*\conf\tpc\Win32 directory as an example.

2. Unzip the file and choose one of the following options:

   - To deploy the package, complete the following steps.

     a. Open the *Install_Home*`\conf\tpc` directory.

     a. Select **Start** > **Programs** > **Accessories** > **Command Prompt.**

        The **Command Prompt** window displays.

     b. Type **cd** *Install_Home***\conf\tpc** and press **Enter** to go to the tpc directory.

c. Type **tpc***Application_Name***ldfdeployer.bat** with the following the parameters and press **Enter** to to deploy the package.

```
TIP install directory, no space, as the 1st parameter,
Application_Name server domain as the 2nd parameter,
Application_Name server name as the 3rd parameter, and
Application_Name server port number, default 80, as the 4th parameter
```

Example of deployment parameters

```
tpcldfdeployer C:\Progra~1\IBM\tivoli\tip brocade.com myhost.engliab
80
```

- To undeploy the package, complete the following steps.

a. Open the *Install_Home*\conf\tpc directory.

d. Select **Start > Programs > Accessories > Command Prompt.**

The **Command Prompt** window displays.

e. Type **cd** *Install_Home***\conf\tpc** and press **Enter** to go to the tpc directory.

f. Type **tpc***Application_Name***ldfundeployer.bat** with the first parameter and **Enter** to remove the package.

First parameter is as follows:

```
TIP install directory, no space, as the 1st parameter,
```

Example

```
tpcApplication_Nameldfundeployer  C:\Progra~1\IBM\tivoli\tip
```

3. Open the WSADMIN for TIP on the TPC server (C:\Program Files\IBM\tivoli\tip\bin\wsadmin.bat).
4. Type `$AdminTask modifyESSWSFedConfiguration {-domain ".domainname.com" –secure false}` and press **Enter**.

NOTE
The dot (.) in front of domainname is mandatory.

5. Restart the TCP data server for the menu to display.

Available LIC points

NOTE
LIC requires a Trial or Licensed version.

LIC enables you to launch the following dialog boxes:

- **Audit Log** dialog box
- **Bottleneck Detection** dialog box
- **CEE Configuration** dialog box
- *DCB_Name* **Edit Switch** dialog box, **QoS** tab
- **Configure Names** dialog box
- **Create View** dialog box
- **Device Connectivity Troubleshooting** dialog box

- **E-mail Event Notification Setup** dialog box
- **Encryption Center** dialog box
- **Event Log** dialog box
- **Fabric Binding** dialog box
- **Fabric Device Sharing Diagnosis** dialog box
- *Fabric_Name* **Historical Performance Graph** dialog box
- **FCIP Tunnels** dialog box
- **FCoE Configuration** dialog box
- **FICON Log** dialog box
- **Firmware Management** dialog box
- **Logical Switches** dialog box
- Main Interface
- **Port Fencing** dialog box
- **Product Status Log** dialog box
- **Real Time Port Picker** dialog box
- **Router Configuration - Connect Edge Fabric** *Fabric_Name* dialog box
- **Save Switch Configuration** dialog box
- **Security Log** dialog box
- **Set End-to-End Monitors** dialog box
- **Set Threshold Policies** dialog box
- **SMIA Configuration Tool** dialog box
- **Switch Configuration Repository** dialog box
- **Syslog Log** dialog box
- **Syslog Forwarding** dialog box
- **Technical Support Data** dialog box
- **Trace Route** dialog box
- **View Reports** dialog box (**Fabric Ports Report**)
- **View Reports** dialog box (**Historical Performance Report**)
- **VLAN Configuration** dialog box
- **Zoning** dialog box

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.

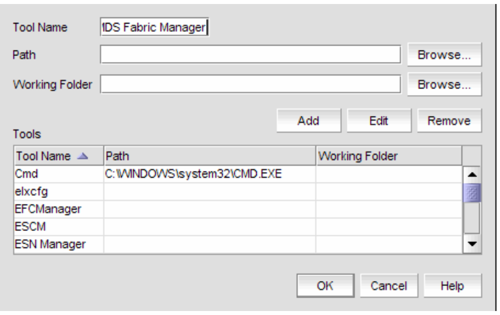
To add a tool, complete the following steps.

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 (Figure 72).



Tool Name: IDS Fabric Manager

Path:

Working Folder:

Tool Name	Path	Working Folder
Cmd	C:\WINDOWS\system32\CMD.EXE	
elxcfg		
EFCManager		
ESCM		
ESN Manager		

FIGURE 72 Define Tools dialog box

4. Type the tool's name in the **Tool Name** field as you want it to appear on the **Tools** menu.
5. Type or browse to the path of the executable file in the **Path** field.
6. Type or browse to the path of the folder that you want to set as your working folder in the **Working Folder** field.
7. Click **Add** to add the tool.

   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 **Define Tools** dialog box.

   To add this tool to the **Tools** menu, refer to "Adding an option to the Tools menu" on page 211.

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

Entering the server IP address of a tool

If the third-party tool is a web-based application, you must enter the IP address of the applications server as a parameter to be able to open the application.

To enter the server IP address, complete the following steps.

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, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts.

3. Select the tool you want to edit in the **Tool Menu Items** table.

   The settings for the selected tool display in the fields at the top of the dialog box.

4. Edit the IP address of the server (for example, `http://`*IP_Address* or `http://`*IP_Address*`:`*Port_Number*) in the **Parameters** field.

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.

Adding an option to the Tools menu

You can add third-party tools to the **Tools** menu which enables you to launch tools directly from the application.

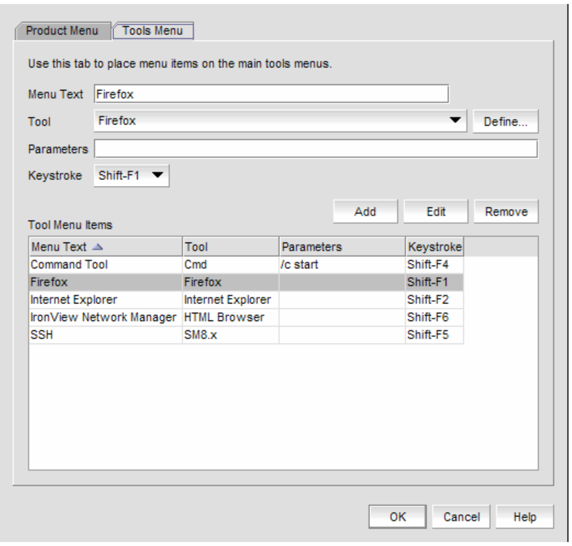
To add a option to the tools menu, complete the following steps.

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, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts (Figure 73).



Use this tab to place menu items on the main tools menus.

Menu Text: Firefox

Tool: Firefox

Parameters:

Keystroke: Shift-F1

Tool Menu Items

Menu Text	Tool	Parameters	Keystroke
Command Tool	Cmd	/c start	Shift-F4
Firefox	Firefox		Shift-F1
Internet Explorer	Internet Explorer		Shift-F2
IronView Network Manager	HTML Browser		Shift-F6
SSH	SM8.x		Shift-F5

FIGURE 73 Setup Tools dialog box (Tools menu tab)

3. Type a label for the option as you want it to appear on the **Tools** menu in the **Menu Text** field.

4. Select the application from the **Tool** list, or click **Define** if you want to specify a new tool.

   To specify a new tool, refer to "Adding a tool" on page 210.

5. (Optional) Enter parameters, such as a URL, in the **Parameters** field.

6. (Optional) Select a keyboard shortcut in the **Keystroke** list.

   NOTE
   You cannot assign the same keyboard shortcut to two different tools.

7. Click **Add**.

   The new tool displays in the **Tool Menu Items** table.

   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.

To edit a option to the tools menu, complete the following steps.

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, including the tool name as it displays on the **Tools** menu, parameters, and keystroke shortcuts.

3. Select the tool you want to edit in the **Tool Menu Items** table.

   The settings for the selected tool display in the fields at the top of the dialog box.

4. Edit the label for the option as you want it to appear on the **Tools** menu in the **Menu Text** field.
5. Select the application from the **Tool** list.
6. Edit the parameters, such as a URL, in the **Parameters** field.
7. Select a new keyboard shortcut in the **Keystroke** list.
8. Click **Edit**.

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

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

Removing an option from the Tools menu

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

To remove a option to the tools menu, complete the following steps.

1. Select **Tools > Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Tools Menu** tab.
3. Select the row of the tool you want to remove in the **Tools Menu Items** table.
4. Click **Remove**.

   If the tool is not being utilized, no confirmation message displays.

5. Click **Update** to remove the tool.
6. 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.

To add an option to the device’s shortcut menu, complete the following steps.

1. Select **Tools** > **Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Product Menu** tab.

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

3. Type or select the text in the **Menu Text** list as you want it to appear on the menu.

4. Choose one of the following options:

   - To display the menu option only for devices that meet the conditions listed, select the **Match Conditions** option.
   - To display the menu option on the shortcut menus for all devices, select the **All** option.

     If you select **All**, skip to step 8. Otherwise, continue to step 5.

5. Select the appropriate type in the **Condition 1 Property** name list.

6. Enter the appropriate value for the selected property in the **Condition 1 Value** field.

7. (Optional) Select the **Condition 2 Property** type and enter the **Value** for that property type (Condition 1 AND Condition 2 must be true) to define a second condition to be simultaneously true.

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

8. Select the tool that you want to launch from the **Tool** list, or click **Define** to add a tool.

   To specify a new tool, refer to “Adding a tool” on page 210.

9. Select the **Append device ID** check box to specify the parameter used when opening the tool.

   - To specify that the device’s IP address should be used when opening the tool, select the **IP Address** option.
   - To specify that the device’s Node WWN should be used when opening the tool, select the **Node WWN** option.

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

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

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

11. 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.

To edit an option to the device's shortcut menu, complete the following steps.

1. Select **Tools** > **Setup**.

   The **Setup Tools** dialog box displays.

2. Click the **Product Menu** tab.

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

3. Select the menu item you want to change in the **Product Popup Menu Items** table.

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

4. Edit or select the text in the **Menu Text** list as you want it to appear on the menu.

5. Choose one of the following options:

   - To display the menu option only for devices that meet the conditions listed, select the **Match Conditions** option.
   - To display the menu option on the shortcut menus for all devices, select the **All** option.

     If you select **All**, skip to step 8. Otherwise, continue to step 5.

6. Change the type in the **Condition 1 Property** name list.

7. Change the value for the selected property in the **Condition 1 Value** field.

8. (Optional) Change the **Condition 2 Property** type or edit the **Value** for that property type (Condition 1 AND Condition 2 must be true) to edit a second condition to be simultaneously true.

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

9. Select the tool from the **Tool** list that you want to launch, or click **Define** to add a tool.

   To specify a new tool, refer to "Adding a tool" on page 210.

10. Select the **Append device ID** check box to specify the parameter used when opening the tool.

    - To specify that the device's IP address should be used when opening the tool, select the **IP Address** option.
    - To specify that the device's Node WWN should be used when opening the tool, select the **Node WWN** option.

11. Click **Edit**.

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

12. 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.

To remove an option to the device's shortcut menu, complete the following steps.

1. Select Tools > Setup.

   The Setup Tools dialog box displays.

2. Click the Product Menu tab.

   The Product Popup Menu Items table displays all configured menu options.

3. Select the menu item you want to remove in the Product Popup Menu Items table.
4. Click Remove.
5. Click OK to save your work and close the Setup Tools dialog box.

Microsoft System Center Operations Manager (SCOM) plug-in

NOTE
The System Center Operations Manager (SCOM) plug-in is only supported on Windows.

NOTE
The SCOM plug-in is only available on Professional Plus and Enterprise.

NOTE
You must have SCOM Management privileges to access the Plug-in for SCOM dialog box.

The SCOM plug-in allows fabric inventory information collected by the Management application to be displayed on the Microsoft SCOM console. The SCOM plug-in uses the SCOM SDK services to extend the SCOM console and present fabric inventory information. The SCOM plug-in serves dynamic HTML pages to the SCOM console.

The SCOM console displays the folloiwng information:

- Fabric and switch details
- End-to-end monitor statistics
- Events from the Management application when Critical events for switches in the fabric trigger CallHome in the Management application

The SCOM plug-in is supported on the following configurations:

- SCOM 2007 R2
- Professional Plus and Enterprise Trial and Licensed version 11.0.0 and later

SCOM plug-in requirements

- Make sure you import the Management application management pack (*Management_Application_Name*.FabricView.xml) to the SCOM Server prior to registering the SCOM Plug-in. The management pack is located in the following directory on the DVD scom/OEM_Name.
- Make sure the Management application server host is managed by the SCOM Server in agent managed mode.
- Make sure the SCOM HealthService agent is running on the Management application server.
- Make sure you install the SCOM Console 2007 R2 software on the Management application server.
- (Optional) Enable SSL on the *Management_Application_Name* to use HTTPS Communication between SCOM Console and the Management application.
- Make sure that the fabric or switch is managed by the the Management application to view fabric and switch details.
- Make sure to enable performance monitoring at the SAN or fabric level to collect end-to-end monitor statistics. Refer to “SAN end-to-end monitoring” on page 771.

Registering a SCOM server

To register the SCOM server, complete the following steps.

1. Select **Tools > Plug-in for SCOM**.

   The **Plug-in for SCOM** dialog box displays.

2. Click **Add**.

   The **Add SCOM Server** dialog box displays.

3. Enter an IP address or fully qualified domain name for the SCOM host in the **Host** field.

   The Management application accepts IP addresses in IPv4 and IPv6 formats. The IPv4 format is valid when the operating system has IPv4 mode only or dual stack mode. The IPv6 format is valid when the operating system has IPv6 mode only or dual stack mode.

4. Enter the domain name in the **Domain** field.
5. Enter your user ID and password.
6. Click **OK**.
7. Click **Close**.

Editing a SCOM server

To edit the SCOM server, complete the following steps.

1. Select **Tools > Plug-in for SCOM.**

   The **Plug-in for SCOM** dialog box displays.

2. Select the server you want to edit and click **Edit.**

   The **Edit SCOM Server** dialog box displays. The **Host** field is not editable in the **Edit SCOM Server** dialog box.

3. Edit the domain name in the **Domain** field.
4. Enter your user ID and password.
5. Click **OK.**
6. Click **Close.**

Removing a SCOM server

To configure the SCOM plug-in, complete the following steps.

1. Select **Tools > Plug-in for SCOM.**

   The **Plug-in for SCOM** dialog box displays.

2. Select the SCOM server you want to delete in the SCOM Servers table.
3. Click **Remove.**
4. Click OK on the confirmation message.
5. Click **Close.**

Chapter

Server Management Console 10

In this chapter

Server Management Console overview

The Server Management Console (SMC) is an automatically installed, stand-alone application for managing the Management application server. You can perform the following tasks using the SMC:

- From the **Services** tab, you can start, stop, refresh, and restart services on the server.
- From the **Ports** tab, you can change the Management application server or web server port number.
- From the **AAA Settings** tab (Enterprise Licensed version only), you can configure an authentication server (LDAP or Radius server), and establish authentication policies.
- From the **Restore** tab, you can restore server application data.
- From the **Technical Support Information** tab, you can collect information for technical support.
- From the **HCM Upgrade** tab, you can upgrade the Management application to use a new version of Host Connectivity Manager (HCM).
- From the **Performance Data Aging** tab, you can define the performance data collection interval..
- From the **SMI Agent Configuration Tool** dialog box, you can configure the SMI Agent settings, such as security, CIMOM, and certificate management as well as launch Management application dialog boxes.

Launching the SMC on Windows

Open the **Server Management Console** from the **Start** menu on the Management application server.

You can also drag the SMC icon onto your desktop as a short cut.

Launching the SMC on Linux

Perform the following steps to launch the Server Management Console on Linux systems.

1. On the Management application server, go to the following directory:

   Install_Directory/bin

2. Type the following at the command line:

```
./smc
OR
sh smc
```

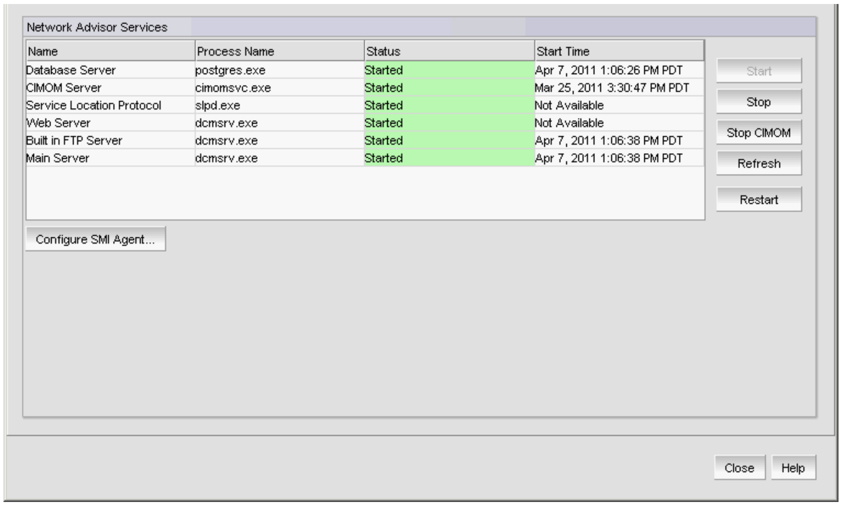
Services

You must be logged in at the administrator (Windows systems) or root (UNIX systems) level to stop, start, and restart the Management application services. Stopping and restarting the Management application services causes clients connected to the server to lose connection, and they must re-log in to the server.

Monitoring and managing Management application services

To monitor the status of the Management application services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab (Figure 74).



Network Advisor Services

Name	Process Name	Status	Start Time
Database Server	postgres.exe	Started	Apr 7, 2011 1:06:26 PM PDT
CIMOM Server	cimomsvc.exe	Started	Mar 25, 2011 3:30:47 PM PDT
Service Location Protocol	slpd.exe	Started	Not Available
Web Server	dcmsrv.exe	Started	Not Available
Built in FTP Server	dcmsrv.exe	Started	Apr 7, 2011 1:06:38 PM PDT
Main Server	dcmsrv.exe	Started	Apr 7, 2011 1:06:38 PM PDT

FIGURE 74 Services tab

3. Review the following information for each available service.
   - **Name**—The name of the server; for example, FTP Server or Database Server.
   - **Process Name**—The name of the process; for example, postgres.exe (Database Server).
   - **Status**—The status of the service; for example, started or stopped.
   - **Start Time**—The date and time the service started. The Start Time for Service Location Protocol displays as ‘Not Available’.
4. Click **Close** to close the Server Management Console.

Refreshing the server status

To refresh the server status for each of the Management application services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Refresh** to update the table with the latest status of the services in case the services were stopped or restarted outside of the Server Management Console.
4. Click **Close** to close the Server Management Console.

Stopping all services

To stop all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Stop** to stop all services.

   Note that clicking **Restart** stops and then restarts all services.
4. Click **Close** to close the Server Management Console.

Stopping the CIMOM services

To stop the CIMOM (Common Information Model Object Manager) services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Stop CIMOM**.
4. Click **Close** to close the Server Management Console.

Starting all services

NOTE
The **Start** button restarts running services in addition to starting stopped services which causes client-server disconnect.

To start all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Start** to start all services.

   NOTE
   If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.

4. Click **Close** to close the Server Management Console.

Restarting all services

To stop and restart all services, complete the following steps.

1. Launch the Server Management Console.
2. Click the **Services** tab.
3. Click **Restart** to stop then restart all services.

   NOTE
   If the server is configured to use an external FTP server, the Server Management Console does not attempt to start the built-in FTP service.

4. Click **Close** to close the Server Management Console.

Changing server port numbers

Use the **Ports** tab of the Server Management Console to change the Management application server and Web server port numbers. The default Web Server port number is 80. The Management application server default port number is 24600.

To change the Management application server or web server port number, complete the following steps.

1. Click the **Ports** tab.
2. Type a new port number in the *Management_Application_Name* **Server** or **Web Server port** field.

   For Trial or Licensed version versions, do not use port 2638.
3. Click **Apply** to save the changes.

   The server automatically restarts if you change the server port number. You must manually restart the server if you change only the web server port number.

NOTE
You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **11.X.X** > **Server Management Console**).

AAA Settings

The Authentication function enables you to configure an authentication server and establish authentication policies. Authentication is configured to the local database by default. If you configure primary authentication to a Radius server, a TACACS+ server, an LDAP server, or switch authentication, you can also configure secondary authentication to the local server. When you log in to the Management application, if the primary server is unavailable, the Management application attempts with the next configured primary server. If all primary servers are unavailable, then the Management application falls back to the secondary authentication. Fall back can occur when the server is unavailable, authentication fails, or the user is not found.

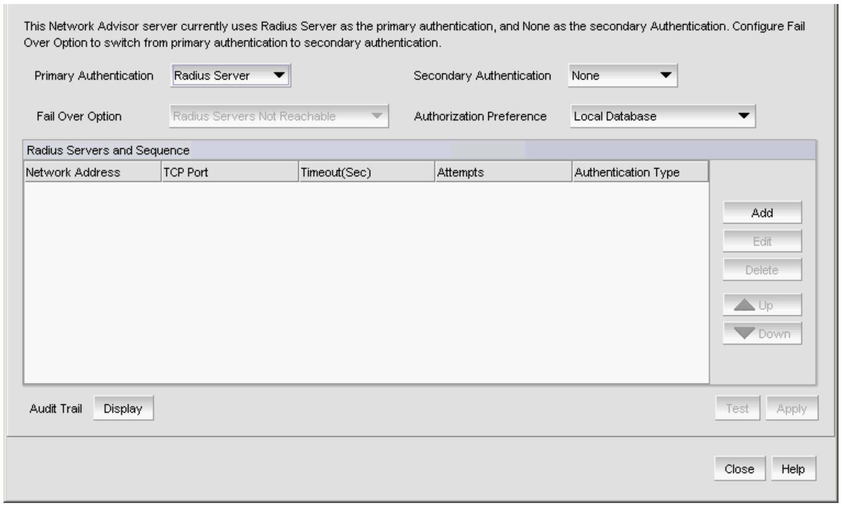
Configuring a Radius server

If you are using a Radius server for authentication, make the following preparations first:

- Select an **Authentication Type** (you will be prompted to provide a type in the **Add or Edit Radius Server** dialog box). The **Authentication Type** is the authentication policy you choose for handling authentication. The options are PAP and CHAP.
  - PAP, password protected protocol, is based on password verification. Passwords are not encrypted, and are not secure from eavesdroppers during transmission.
  - CHAP, challenge handshake protocol, uses a three-way handshake method of verification based on a shared secret. If you are using CHAP, have the shared secret available to you. You will need to type it in as a configuration parameter.
- Know the Shared Secret.
- Have the IP address of the server available.

- Know the TCP port you are using. For Radius servers, ports 1812 or 1645 (actually UDP ports) are commonly used. Check with the Radius server vendor if you are not sure which port to specify.
- Know how long you want to wait between attempts to reach the server if it is busy. This is expressed as a timeout value (default is 3 seconds) in seconds. Values are between 1 and 15.
- Determine how many attempts (default is 3 times) to make to reach the server before stopping and assuming it is unreachable. Values are between 1 and 5.
- If possible, establish an active connection with the Radius server before configuration. This enables you to test the connection as part of the configuration procedure.

1. Select the **AAA Settings** tab (Figure 75).



This Network Advisor server currently uses Radius Server as the primary authentication, and None as the secondary Authentication. Configure Fail Over Option to switch from primary authentication to secondary authentication.

Primary Authentication: Radius Server

Secondary Authentication: None

Fail Over Option: Radius Servers Not Reachable

Authorization Preference: Local Database

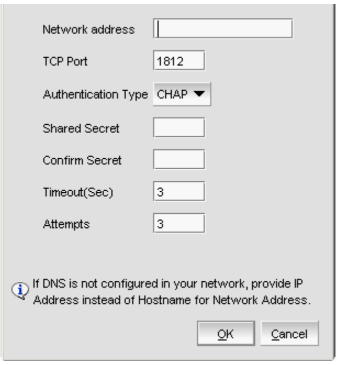
Radius Servers and Sequence

Network Address	TCP Port	Timeout(Sec)	Attempts	Authentication Type

FIGURE 75 AAA Settings tab

2. For **Primary Authentication**, select **Radius Server.**
3. Click **Add.**

   The **Add or Edit Radius Server** dialog box displays (Figure 76).



Network address:

TCP Port: 1812

Authentication Type: CHAP

Shared Secret:

Confirm Secret:

Timeout(Sec): 3

Attempts: 3

If DNS is not configured in your network, provide IP Address instead of Hostname for Network Address.

FIGURE 76 Add or Edit Radius Server

4. Enter the radius server’s IP address in the **IP Address** field.
5. Enter the TCP port, if necessary, used by the Radius server in the **TCP Port** field.

   Default is 1812.

6. Select the authentication policy (PAP or CHAP) from the **Authentication Type** field.

   Default is CHAP.

7. Enter the shared secret in the **Shared Secret** and **Confirm Secret** fields.

8. Enter the timeout timer value (in seconds) that specifies the amount of time to wait between retries when the server is busy in the **Timeout (Sec)** field.

   Default is 3 seconds.

9. Enter the number of attempts to be made to reach a server before assuming it is unreachable in the **Attempts** field.

   Default is 3 attempts.

10. Click **OK** to return to the **AAA Settings** tab.

11. If you have established an active connection with the Radius server, click **Test**.

    Test attempts to contact the Radius server by issuing a **ping** command.

12. Set secondary authentication by selecting one of the following options from the **Secondary Authentication** list:

    - **Local Database**
    - **None**

13. Set the fall back condition to secondary authentication by selecting one of the following options from the **Switch to secondary authentication when** list:

    - **Radius Servers Not Reachable**
    - **Radius Authentication Failed**

14. Set the authorization preference by selecting one of the following options from the **Authorization Preference** list:

    - **Local Database**
    - **Primary Authentication Server**

15. Click **Apply** to save the configuration.

Configuring an LDAP server

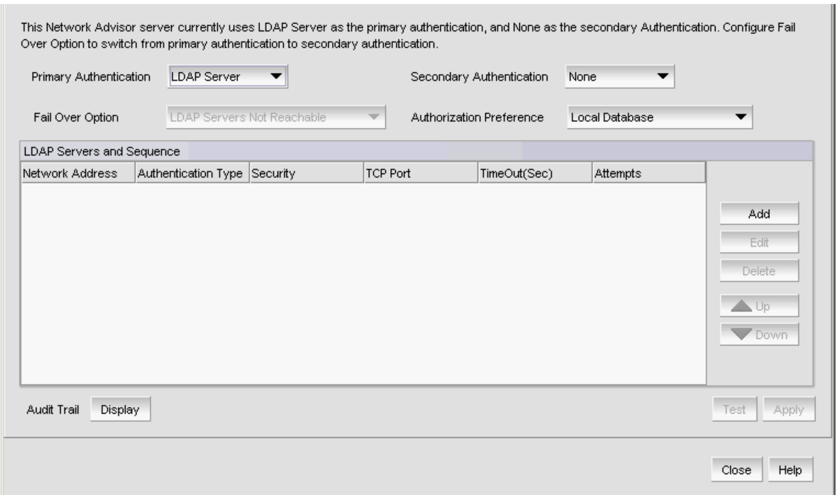
If you are using an LDAP server for authentication, make the following preparations first:

- Have the IP address of the server available.
- Know the TCP port you are using. The LDAP server uses Transport Layer Security (TLS). LDAP over TLS generally uses port 389. Check with the LDAP server administrator if you are not sure which port to specify.
- Know how long you want to wait between attempts (default is 3 seconds) to reach the server if it is busy. This is expressed as a timeout value in seconds. Values are between 1 and 15.
- Determine how many attempts (default is 3 times) to make to reach the server before stopping and assuming it is unreachable. Values are between 1 and 5.

NOTE
If the LDAP server's IP address is entered in the Management application, the LDAP server's hostname (if any) must still be known to the Management application host OS. The Management application server must be using a DNS server that knows the LDAP server's hostname, or you must manually add the LDAP server's hostname to the local hosts file (for Linux the file is located in /etc/hosts and for Windows the file is located in C:\Windows\System32\drivers\etc\hosts for Windows).

To configure an LDAP server for authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. Select **LDAP Server** from the **Primary Authentication** list.



This Network Advisor server currently uses LDAP Server as the primary authentication, and None as the secondary Authentication. Configure Fail Over Option to switch from primary authentication to secondary authentication.

Primary Authentication: LDAP Server

Secondary Authentication: None

Fail Over Option: LDAP Servers Not Reachable

Authorization Preference: Local Database

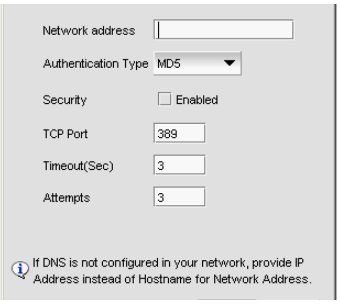
LDAP Servers and Sequence

Network Address	Authentication Type	Security	TCP Port	TimeOut(Sec)	Attempts

FIGURE 77 AAA Settings tab - LDAP server

3. Click **Add**.

   The **Add or Edit LDAP Server** dialog box displays (Figure 78).



Network address	
Authentication Type	MD5
Security	□ Enabled
TCP Port	389
Timeout(Sec)	3
Attempts	3

If DNS is not configured in your network, provide IP Address instead of Hostname for Network Address.

FIGURE 78 Add or Edit LDAP server

4. Enter the LDAP server's IP address in the **IP Address** field.
5. Enter the TCP port used by the LDAP server in the **TCP Port** field.

   Default is 389.

6. Enter the timeout timer value (in seconds) that specifies the amount of time to wait between retries when the server is busy in the **Timeout (Sec)** field.

   Default is 3 seconds.

7. Enter the number of attempts to be made to reach a server before assuming it is unreachable in the **Attempts** field.

   Default is 3 attempts.

8. Click **OK** to return to the **AAA Settings** tab.
9. If you have established an active connection with the LDAP server, click **Test**.

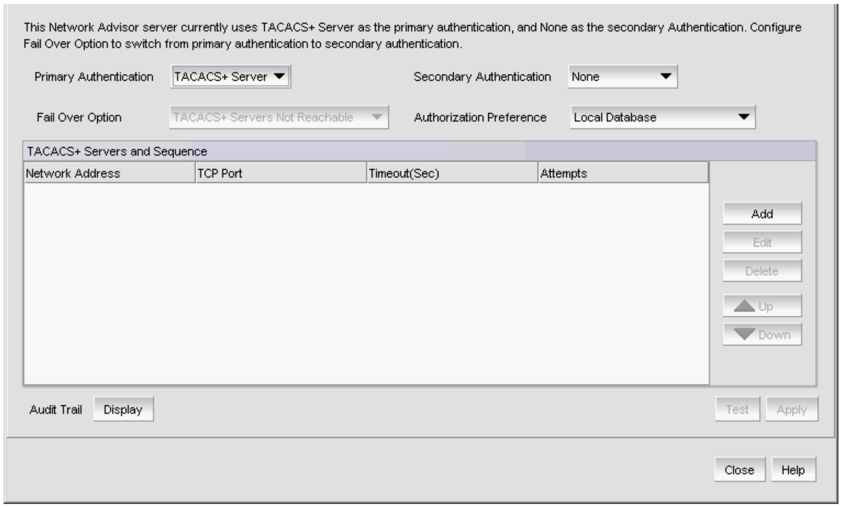
   Test attempts to contact the LDAP server by issuing a **ping** command.

10. Set secondary authentication by selecting one of the following options from the **Secondary Authentication** list:
    - Local Database
    - None
11. Set the fall back condition to secondary authentication by selecting one of the following options from the **Switch to secondary authentication when** list:
    - LDAP Servers Not Reachable
    - LDAP Authentication Failed
    - User Not Found in LDAP
12. Set the authorization preference by selecting one of the following options from the **Authorization Preference** list:
    - Local Database
    - Primary Authentication Server
    - LDAP Authorization
13. Click **Apply** to save the configuration.

Configuring a TACACS+ server

To configure TACACS+ server authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. For **Primary Authentication**, select **TACACS+ Server.**



This Network Advisor server currently uses TACACS+ Server as the primary authentication, and None as the secondary Authentication. Configure Fail Over Option to switch from primary authentication to secondary authentication.

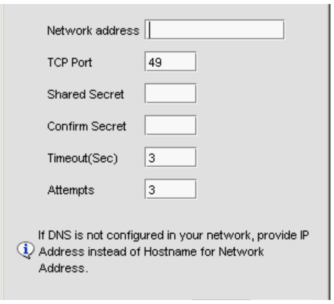
Primary Authentication	TACACS+ Server
Secondary Authentication	None
Fail Over Option	TACACS+ Servers Not Reachable
Authorization Preference	Local Database

TACACS+ Servers and Sequence

Network Address	TCP Port	Timeout(Sec)	Attempts

FIGURE 79 AAA Settings tab - TACACS+ server

3. Click **Add.**



Network address	
TCP Port	49
Shared Secret	
Confirm Secret	
Timeout(Sec)	3
Attempts	3

If DNS is not configured in your network, provide IP Address instead of Hostname for Network Address.

FIGURE 80 Add or Edit TACACS+ server

4. Enter the TACACS+ server's IP address in the **Network Address** field.
5. Enter the TCP port used by the TACACS+ server in the **TCP Port** field.

   Default is 49.
6. Enter the shared secret in the **Shared Secret** and **Confirm Secret** fields.
7. Enter the timeout timer value (in seconds) that specifies the amount of time to wait between retries when the server is busy in the **Timeout (Sec)** field.

   Default is 3 seconds.
8. Enter the number of attempts to be made to reach a server before assuming it is unreachable in the **Attempts** field.

   Default is 3 attempts.

9. Click **OK** to return to the **AAA Settings** tab.
10. Set secondary authentication by selecting one of the following options from the **Secondary Authentication** list:
    - **Local Database**
    - **None**
11. Set the fall back condition to secondary authentication by selecting one of the following options from the **Fail Over Option** list:
    - **TACACS+ Server Not Reachable**
    - **TACACS+ Server Authentication Failed**
12. Set the authorization preference by selecting one of the following options from the **Authorization Preference** list:
    - **Local Database**
    - **Primary Authentication Server**
13. Click **Test**.

    The **Test Authentication** dialog box displays.
14. Enter your user ID and password and click **Test**.

    Test verifies your user ID and password for the local database and verifies user privileges on the Management application server.
15. Click **Apply** to save the configuration.

Configuring switch authentication

Switch authentication enables you to authenticate a user account against the switch database and the Management application server. You can configure up to three switches and specify the fall back order if one or more of the switches is not available.

NOTE
Switch authentication is only supported on Fabric OS devices.

To configure switch authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. For **Primary Authentication**, select **Switch**.
3. Enter the switch IP address and click **Add**.

   Repeat step 3 as needed. You can add up to three switches.
4. Set up the fall back order by completing the following steps.
   a. Select the IP address of the switch you want to move.
   b. Click **Move Up** or **Move Down** to move the switch where you want it.
5. Select a switch and click **Remove** to remove a switch from the list.
6. Click **Test**.

   The **Test Authentication** dialog box displays.

7. Enter your user ID and password and click **Test**.

   Test verifies your user ID and password on the switch and verifies user privileges on the Management application server.

8. Click **Apply** to save the configuration.

Configuring Windows authentication

Windows authentication enables you to authenticate a user account against the Windows user accounts and the Management application server when running on Windows hosts.

The following list details the supported Windows authentication types and the associated platforms:

- NT domain authentication (multiple domains)—supported on Windows XP/2003/2008 platforms only
- Windows Workgroup authentication—supported on Windows XP/2003/2008 platforms only
- Windows local user accounts—supported on Windows XP/2003/2008 platforms only.

To configure Windows authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. For **Primary Authentication**, select **Windows Domain**.
3. Enter the domain name in the **Windows Domain Name** field.
4. Click **Test**.

   The **Test Authentication** dialog box displays.

5. Enter your user ID and password and click **Test**.

   Test verifies your user ID and password on the Windows domain and verifies user privileges on the Management application server.

6. Click **Apply** to save the configuration.

Configuring local database authentication

Local database authentication enables you to authenticate a user account against the local database and the Management application server.

To configure local database authentication, complete the following steps.

1. Select the **AAA Settings** tab.
2. For **Primary Authentication**, select **Local Database**.
3. Click **Test**.

   The **Test Authentication** dialog box displays.

4. Enter your user ID and password and click **Test**.

   Test verifies your user ID and password for the local database and verifies user privileges on the Management application server.

5. Click **Apply** to save the configuration.

Displaying the client authentication audit trail

All responses to authentication requests coming from clients are logged to an audit trail log file. This file is automatically backed up on the first day of every month.

1. Select the **AAA Settings** tab.
2. Click **Display** next to **Authentication Audit Trail**.

   The **Login** dialog box displays.
3. Enter your username and password in the appropriate fields and click **OK**.

   The defaults are Administrator and password, respectively.

   The **Authentication Audit Trail** log displays.

   The audit trail shows user names that have attempted to log in to the Management application, and changes to user authentication.
4. Click the **Client to Server Authentication** tab to view the client to server authentication status.
5. Click the **Authentication Settings Changes** tab to view the previous authentication changes.

Restoring the database

To restore application data files, you must know the path to the backup files. This path is configured from the **Server > Options** dialog box. For more information about backup, refer to "Server Data backup" on page 86.

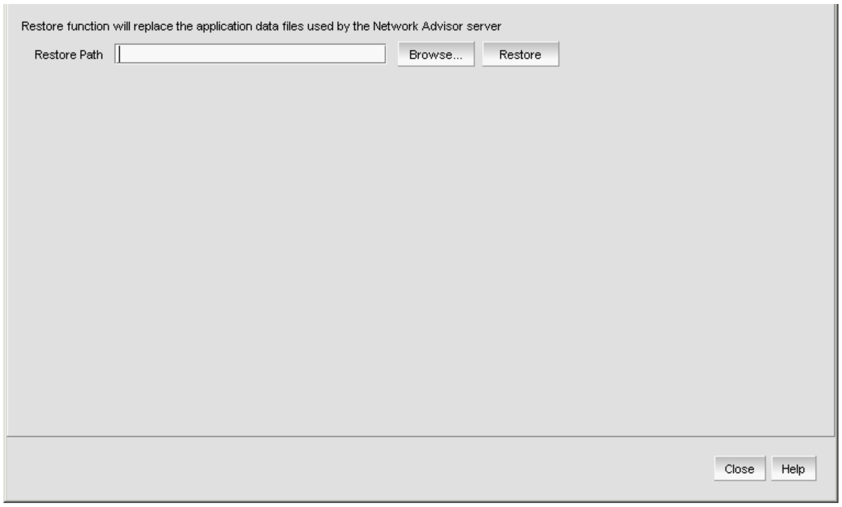
NOTE
You cannot restore data from a previous version of the Management application.

NOTE
You cannot restore data from a higher or lower configuration (Trial or Licensed version) of the Management application.

NOTE
You cannot restore data from a different package of the Management application.

To restore the application data files, complete the following steps.

1. Click the **Services** tab.
2. Stop all services.
3. Click the **Restore** tab (Figure 81).



Restore function will replace the application data files used by the Network Advisor server

FIGURE 81 Restore tab

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

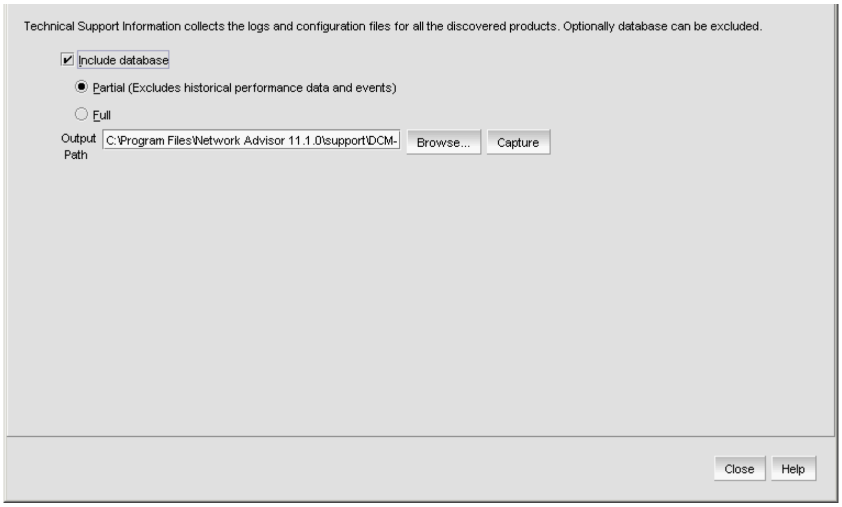
   Upon completion, a message displays the status of the restore operation. Click **OK** to close the message and the Server Management Console. For the restored data to take effect, re-launch the Configuration Wizard using the instructions in “Launching the Configuration Wizard” on page 27.

Capturing technical support information

The **Technical Support Information** tab of the SMC allows you to capture technical support information for the Management application as well as the configuration files for all switches in discovered fabrics. This information is saved in a *zip* file in a location that you specify.

To capture technical support information, complete the following steps.

1. Select the **Technical Support Information** tab.



Technical Support Information collects the logs and configuration files for all the discovered products. Optionally database can be excluded.

☑ Include database

● Partial (Excludes historical performance data and events)

○ Full

Output Path: C:\Program Files\Network Advisor 11.1.0\support\DCM-

FIGURE 82 Technical Support Information tab

2. Select the **Include database** check box to capture database server support save files and choose one of the following options:

   - Select the **Partial** option to exclude historical data and events from the database capture.
   - Select the **Full** option to include historical data and events from the database capture.

NOTE
It is recommended that you only capture the partial database.

NOTE
You should only capture the full database when you need to debug Historical Performance Management or Historical Events issues.

3. Enter the path where you want to save the support data and a name for the support save file in the **Output Path** field.

   For example, *Full_Path**Support_Save_File_Name*.zip. You can also browse to the location you want to save the support data and append the file name to the path when you return to the **Techncial Support Information** tab.

   If you do not specify an output path, the Management application automatically saves the data to the *Install_Home*/support directory. The default name of the Server Support Save is DCM-SS-*Time_Stamp*.

   NOTE
   For Linux systems, you cannot have blank spaces in the output path (target directory). If the output path contains blank spaces, the supportShow files are not complete.

4. Click **Capture**.

   A confirmation message displays when the capture is complete.

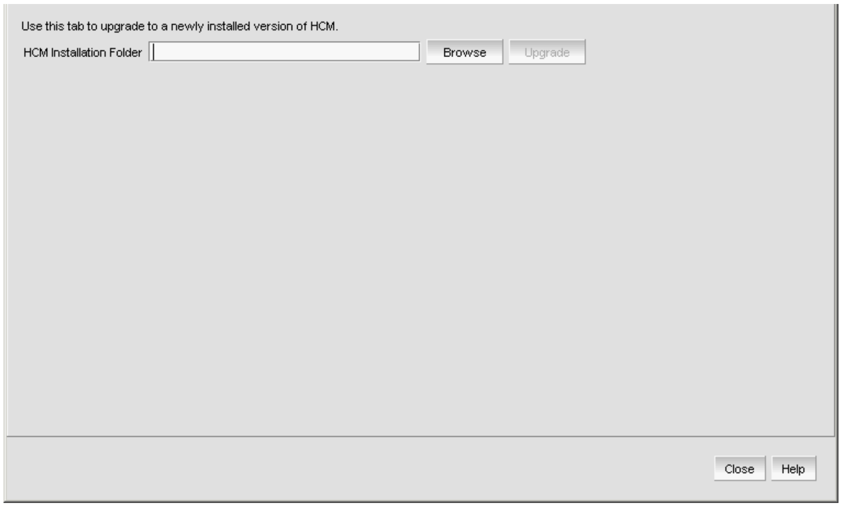
5. Click **OK**.

Upgrading HCM on the Management server

The **HCM Upgrade** tab enables you to upgrade the Management application to include a new version of HCM.

To upgrade HCM, complete the following steps.

1. Select the **HCM Upgrade** tab.



Use this tab to upgrade to a newly installed version of HCM.

HCM Installation Folder

FIGURE 83 HCM Upgrade tab

2. Click **Browse** to select the HCM installation folder location (for example, C:\Program Files\BROCADE\Adapter on Windows systems and /opt/brocade/adapter on Linux systems).
3. Click **Upgrade**.
4. Click **Close**.

Defining the performance data aging interval

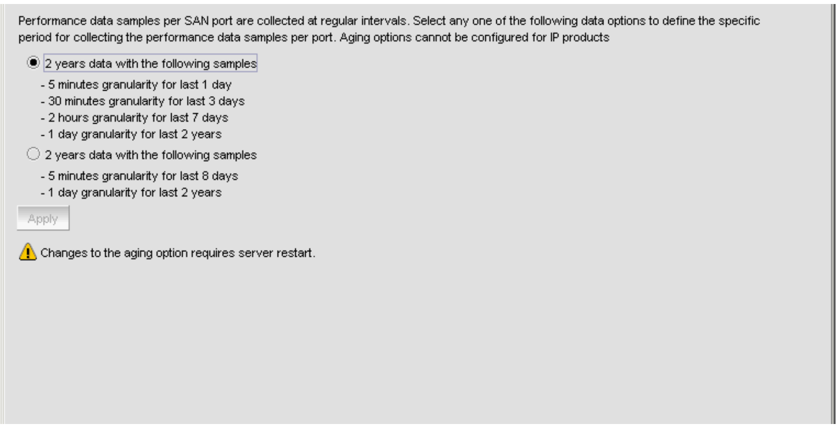
The **Performance Data Aging** tab enables you to define the performance data collection interval.

NOTE
Changes to the performance data aging option requires a server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **11.X.X > Server Management Console**).

To define the performance data collection interval, complete the following steps.

1. Click the **Performance Data Aging** tab.



Performance data samples per SAN port are collected at regular intervals. Select any one of the following data options to define the specific period for collecting the performance data samples per port. Aging options cannot be configured for IP products

● 2 years data with the following samples
- 5 minutes granularity for last 1 day
- 30 minutes granularity for last 3 days
- 2 hours granularity for last 7 days
- 1 day granularity for last 2 years

○ 2 years data with the following samples
- 5 minutes granularity for last 8 days
- 1 day granularity for last 2 years

⚠ Changes to the aging option requires server restart.

FIGURE 84 **Performance Data Aging tab**

2. Select one of the following options:
   - Option 1—**2 years data with the following samples**
     - 5 minutes granularity for last 1 day (288 samples)
     - 30 minutes granularity for last 3 days (144 samples)
     - 2 hour granularity for last 7 days (84 samples)
     - 1 day granularity for last 2 years (730 samples)
   - Option 2—**2 years data with the following samples**
     - 5 minutes granularity for last 8 days (2304 samples)
     - 1 day granularity for last 2 years (730 samples)

   If you change from the Option 1 to the Option 2, you will lose existing performance data for the following intervals:

   - 30 minutes granularity for last 3 days (144 samples)
   - 2 hour granularity for last 7 days (84 samples)
3. Click **Apply.**

   The **Login** dialog box displays.
4. Enter your user name and password in the appropriate fields and click **OK.**

5. Click **Yes** on the confirmation message.

   The server automatically restarts.

6. Click **Close**.

SMI Agent configuration

The SMIA Configuration Tool enables you to configure SMI Agent settings, such as security, CIMOM, and certificate management. This tool is automatically installed with the Management application as part of the Server Management Console. This SMIA Configuration Tool consists of the following tabs:

- **Home**—enables you to launch the following Management application dialog boxes: **Fabric Discovery**, **Host Discovery**, **Users**, **Options**, **Server**, and **About**.
- **Authentication**—enables you to configure mutual authentication for Client,CIMMOM server, and Indication using a secure protocol.
- **CIMOM**—enables you to configure the CIMOM server port, the Bind Network Address, and the CIMOM log.
- **Certificate Management**—enables you to import Client and Indication certificates, export Server certificates, as well as view and delete current certificates.
- **Summary**—enables you to view the CIMOM server configuration and current configuration.

Launching the SMIA configuration tool on Windows

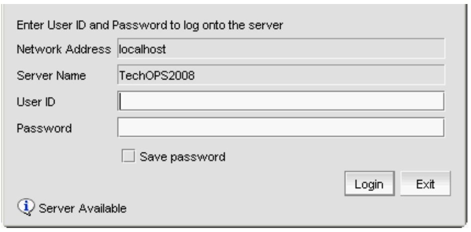
NOTE
All Management application services must be running before you can log into the **SMIA Configuration Tool**. To start the Management application services, click **Start** on the **Server Management Console** dialog box.

1. Launch the **Server Management Console** from the **Start** menu on the Management application server.

   You can also drag the SMC icon onto your desktop as a short cut.

2. Click **Configure SMI Agent** on the **Server Management Console** dialog box.

   The **Log In** dialog box displays.


Enter User ID and Password to log onto the server

Network Address localhost

Server Name TechOPS2008

User ID

Password

□ Save password

Server Available

FIGURE 85 Log In dialog box

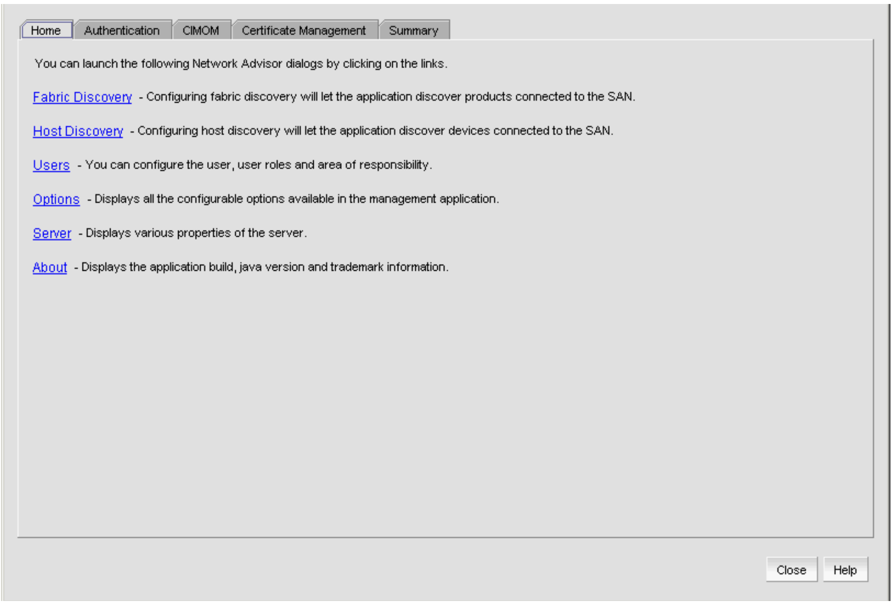
3. Enter your username and password in the appropriate fields.

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

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

5. Click **Login**.

   The **SMIA Configuration Tool** dialog box displays.



You can launch the following Network Advisor dialogs by clicking on the links.

Fabric Discovery - Configuring fabric discovery will let the application discover products connected to the SAN.

Host Discovery - Configuring host discovery will let the application discover devices connected to the SAN.

Users - You can configure the user, user roles and area of responsibility.

Options - Displays all the configurable options available in the management application.

Server - Displays various properties of the server.

About - Displays the application build, java version and trademark information.

FIGURE 86 SMIA Configuration Tool dialog box

Launching the SMIA configuration tool on Unix

NOTE
All Management application services must be running before you can log into the **SMIA Configuration Tool**. To start the Management application services, click **Start** on the **Server Management Console** dialog box.

Perform the following steps to launch the Server Management Console on Unix systems.

1. On the Management application server, go to the following directory:

   Install_Directory/bin

2. Type the following at the command line:

```
./smc
OR
sh smc
```

3. Click **Configure SMI Agent** on the Server Management Console dialog box.

   The **Login** dialog box displays.

4. Enter your username and password in the appropriate fields and click **OK**.

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

   The **SMIA Configuration Tool** dialog box displays.

Launching a remote SMIA configuration tool

To launch a remote SMIA configuration tool, complete the following steps.

1. Open a web browser and enter the IP address of the Management application server in the **Address** bar.

   If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address*:*Web_Server_Port_Number*.

   The Management application web start screen displays.

2. Click the SMIA configuration tool application web start link.

   The **Log In** dialog box displays.

3. Enter your user name and password.

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

4. Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in.

5. Click **Login**.

   The **SMIA Configuration Tool** dialog box displays

Service Location Protocol (SLP) support

The Management application SMI Agent uses Service Location Protocol (SLP) to allow applications to discover the existence, location, and configuration of WBEM services in enterprise networks.

You do not need a WBEM client to use SLP discovery to find a WBEM Server; that is, SLP discovery might already know about the location and capabilities of the WBEM Server to which it wants to send its requests. In such environments, you do not need to start the SLP component of the Management application SMI Agent.

However, in a dynamically changing enterprise network environment, many WBEM clients might choose to use SLP discovery to find the location and capabilities of other WBEM Servers. In such environments, start the SLP component of the Management application SMI Agent to allow advertisement of its existence, location, and capabilities.

SLP installation is optional and you can configure it during Management application configuration. Once installed, SLP starts whenever the Management application SMI Agent starts.

SLP support includes the following components:

- slpd script starts the slpd platform
- slpd program acts as a Service Agent (SA). A different slpd binary executable file exists for UNIX and Windows systems.
- slptool script starts the slptool platform-specific program
- slptool program can be used to verify whether SLP is operating properly or not. A different slptool exists for UNIX and Windows.

  By default, the Management application SMI Agent is configured to advertise itself as a Service Agent (SA). The advertised SLP template shows its location (IP address) and the WBEM Services it supports. The default advertised WBEM services show the Management application SMI Agent:

  - accepts WBEM requests over HTTP without SSL on TCP port 5988
  - accepts WBEM requests over HTTPS using SSL on TCP port 5989

slptool commands

Use the following slptool commands to verify whether the SLP is operating properly.

- slptool findsrvs service:service-agent

  Use this command to verify that the Management application SMI Agent SLP service is properly running as a Service Agent (SA).

  Example output: service:service-agent://127.0.0.1,65535

- slptool findsrvs service:wbem

  Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM services.

  Example outputs:

  service:wbem:https://10.0.1.3:5989,65535

  service:wbem:http://10.0.1.3:5988,65535

  This output shows the functionalities of the Management application SMI Agent:

  - accepts WBEM requests over HTTP using SSL on TCP port 5989
  - accepts WBEM requests over HTTP without SSL on TCP port 5988

- slptool findattrs service:wbem:https://*IP_Address*:*Port*

NOTE
Where *IP_Address*:*Port* is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

Use this command to verify that Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTP protocol.

Example output:

```
Install_Home\cimom\bin>slptool findattrs service:wbem:http://10.24.35.61:5988
(template-type=wbem),(template-version=1.0),(template-description=This
template describes the attributes used for advertising WBEM Servers),
(template-url-syntax=http://10.24.35.61:5988),(service-hi-name=WBEM Solutions
J WBEM Server),(service-hi-description=WBEM Solutions J WBEM Server),
(service-id=WBEMSolutions:f1f65c3b-27f1-4b70-9ced-e412e93a8d5e),(Communicatio
nMechanism=CIM-XML),(OtherCommunicationMechanismDescription =null),
(InteropSchemaNamespace=interop),(ProtocolVersion=1.2),
(FunctionalProfilesSupported=Basic Read,Basic Write,Schema Manipulation,
Instance Manipulation,Association Traversal,Query Execution,Qualifier
Declaration,Indications),(FunctionalProfileDescriptions=null),(MultipleOperat
ionsSupported=true),(AuthenticationMechanismsSupported=Basic),(Authentication
MechanismDescriptions=null),(Namespace=root/brocade1,interop),(Classinfo=0,0)
,(RegisteredProfilesSupported=SNIA:SMI-S,DMTF:Profile Registration,SNIA:FC
HBA,DMTF:LaunchInContext,SNIA:Fan,SNIA:Fabric,SNIA:Switch,DMTF:Role Based
Authorization,SNIA:Power Supply,SNIA:Sensors,SNIA:Server)
```

- slptool findattrs service:wbem:http://*IP_Address*:*Port*

NOTE
Where *IP_Address*:*Port* is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

Use this command to verify that the Management application SMI Agent SLP service is properly advertising its WBEM SLP template over the HTTPS protocol.

Example output:

```
Install_Home\cimom\bin>slptool findattrs service:wbem:
https://10.24.35.61:5989(template-type=wbem),(template-version=1.0),(template
-description=This template describes the attributes used for advertising WBEM
Servers),(template-url-syntax=https://10.24.35.61:5989),(service-hi-name=WBEM
Solutions J WBEM Server),(service-hi-description=WBEM Solutions J WBEM
Server),(service-id=WBEMSolutions:f1f65c3b-27f1-4b70-9ced-e412e93a8d5e),(Comm
unicationMechanism=CIM-XML),(OtherCommunicationMechanismDescription
=null),(InteropSchemaNamespace=interop),(ProtocolVersion=1.2),(FunctionalProf
ilesSupported=Basic Read,Basic Write,Schema Manipulation,Instance
Manipulation,Association Traversal,Query Execution,Qualifier Declaration,
Indications),(FunctionalProfileDescriptions=null),
(MultipleOperationsSupported=true),(AuthenticationMechanismsSupported=Basic),
(AuthenticationMechanismDescriptions=null),(Namespace=root/brocade1,interop),
(Classinfo=0,0),(RegisteredProfilesSupported=SNIA:SMI-S,DMTF:Profile
Registration,SNIA:FC HBA,DMTF:LaunchInContext,SNIA:Fan,SNIA:Fabric,
SNIA:Switch,DMTF:Role Based Authorization,SNIA:Power Supply,SNIA:Sensors,
SNIA:Server)
```

SLP on UNIX systems

This section describes how to verify the SLP daemon on UNIX systems.

SLP file locations on UNIX systems

- SLP log—*Install_Home*/cimom /cfg/slp.log
- SLP daemon—*Install_Home*/cimom /cfg/slp.conf

  You can reconfigure the SLP daemon by modifying this file.
- SLP register—*Install_Home*/cimom /cfg/slp.reg

  You can statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to http://www.openslp.org/doc/html/UsersGuide/index.html.

Verifying SLP service installation and operation on UNIX systems

1. Open a command window.
2. Type % su root and press **Enter** to become the root user.
3. Type # *Install_Home*/cimom/bin/slptool findsrvs service:service-agent and press **Enter** to verify the SLP service is running as a Service Agent (SA).
4. Type # *Install_Home*/cimom/bin/slptool findsrvs service:wbem and press **Enter** to verify the SLP service is advertising its WBEM services.
5. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
   - Type # *Install_Home*/cimom /bin/slptool findattrs service:wbem:http://*IP_Address:Port* and press **Enter**.
   - Type # *Install_Home*/cimom /bin/slptool findattrs service:wbem:https://*IP_Address:Port* and press **Enter**.

NOTE
Where *IP_Address:Port* is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

SLP on Windows systems

This section describes how to verify the SLP daemon on Windows systems.

SLP file locations on Windows systems

- SLP log—*Install_Home*\cimom \cfg\slp.log
- SLP daemon—*Install_Home*\cimom\cfg\slp.conf

  You can reconfigure the SLP daemon by modifying this file.
- SLP register—*Install_Home*\cimom\cfg\slp.reg

  You can statically register an application that does not dynamically register with SLP using SLPAPIs by modifying this file. For more information about these files, read the comments contained in them, or refer to http://www.openslp.org/doc/html/UsersGuide/index.html.

Verifying SLP service installation and operation on Windows systems

1. Launch the Server Management Console from the **Start** menu.
2. Click **Start** to start the SLP service.
3. Open a command window.
4. Type cd c:\Install_Home\cimom \bin and press **Enter** to change to the directory where slpd.bat is located.
5. Type > slptool findsrvs service:service-agent and press **Enter** to verify the SLP service is running as a Service Agent.
6. Type > slptool findsrvs service:wbem and press **Enter** to verify the SLP service is advertising its WBEM services.
7. Choose one of the following options to verify the SLP service is advertising the WBEM SLP template over its configured client protocol adapters.
   - Type > slptool findattrs service:wbem:http://*IP_Address:Port* and press **Enter**.
   - Type > slptool findattrs service:wbem:https://*IP_Address:Port* and press **Enter**.

NOTE
Where *IP_Address:Port* is the IP address and port number that display when you use the slptool findsrvs service:wbem command.

Home tab

The **Home** tab of the **SMIA Configuration Tool** enables you to access the following Management application features or information:

- **Fabric Discovery**—enables you to view discovered fabrics, discover new fabrics, as well as edit the default SNMP configuration. For step-by-step instructions, refer to "Discovering fabrics" on page 53.
- **Host Discovery**—enables you to view discovered hosts, discover new hosts, as well as edit the default SNMP configuration. For step-by-step instructions, refer to "Host discovery" on page 70.
- **Users**—enables you to create or delete Management application users with System Administrator privileges. For step-by-step instructions, refer to "User accounts" on page 140.
- **Options**—enables you to configure the Management application settings. For step-by-step instructions, refer to "Application Configuration" on page 85.
- **Server**—enables you to view server properties. For step-by-step instructions, refer to "Viewing server properties" on page 33.
- **About**—enables you to display information about the Management application, including the build number, Java version, and trademark information.
- **Upgrade** button (Trial version only)—enables you to upgrade from managing 2560 switch ports to 9000 switch ports. For step-by-step instructions, refer to "Upgrading the application" on page 46.

Accessing Management application features

To access Management application features such as, fabric and host discovery, role-based access control, application configuration and display options, server properties, as well as the application name, build, and copyright, complete the following steps.

1. Click the Home tab, if necessary.
2. Select from the following to access the feature or dialog box.
   - Fabric Discovery
   - Host Discovery
   - Users
   - Options
   - Server
   - About
   - Upgrade (Trial version only)
3. Click Close to close the SMIA Configuration Tool dialog box.

Authentication

NOTE
You must have User Management Read and Write privileges to make changes on the CIMOM tab.

The **Authentication** tab enables you to configure mutual authentication for Client and Indication using a secure protocol.

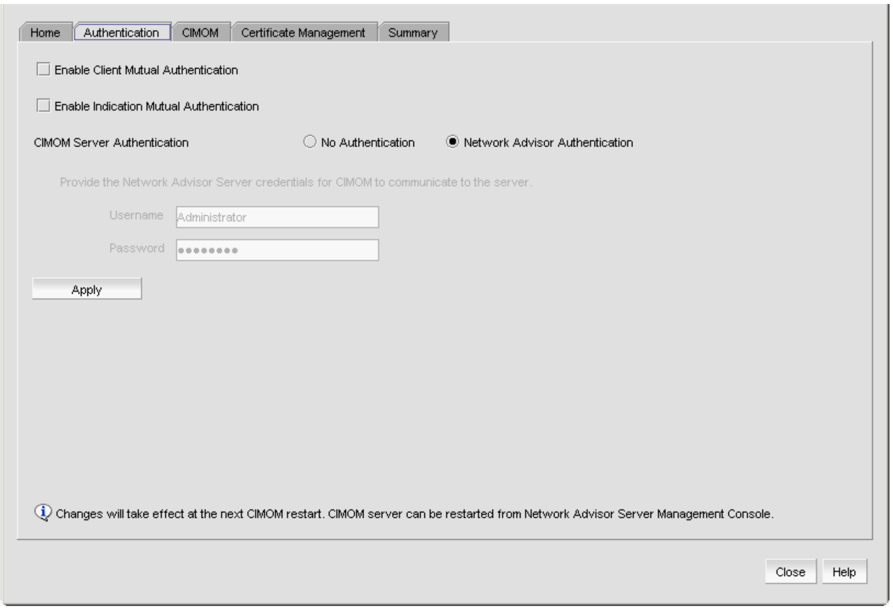
Enabling or disabling CIM client and indication mutual authentication

When you enable client mutual authentication, all CIM client and indication requests to the SMI Agent must pass credentials (KeyStore and TrustStore) to validate the requests. The KeyStore file provides the credentials and the TrustStore file verifies the credentials. When you enable indication mutual authentication, both the CIM client and the CIMOM server maintain the TrustStore files.

The CIM client KeyStore file sends credentials to be validated by the CIMOM server TrustStrore file for any communication from the CIM client to the CIMOM server and the CIMOM server KeyStore file sends credentials to be validated by the CIM client TrustStrore file for any communication from the CIMOM server to the CIM client

To enable or disable CIM client and indication mutual authentication, complete the following steps.

1. Click the **Authentication** tab.



☐ Enable Client Mutual Authentication

☐ Enable Indication Mutual Authentication

CIMOM Server Authentication ○ No Authentication ● Network Advisor Authentication

Provide the Network Advisor Server credentials for CIMOM to communicate to the server.

Username: Administrator

Password: ••••••••

Changes will take effect at the next CIMOM restart. CIMOM server can be restarted from Network Advisor Server Management Console.

FIGURE 87 Authentication tab

2. Select the **Enable Client Mutual Authentication** check box, as needed.

   If the check box is checked, CIM client mutual authentication is enabled. If the check box is clear (default), client mutual authentication is disabled.

3. Select the **Enable Indication Mutual Authentication** check box, as needed.

   If the check box is checked, indication mutual authentication is enabled. If the check box is clear (default), indication mutual authentication is disabled.

4. Click **Apply**.

NOTE
Changes on this tab take effect after the next CIMOM server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **11.X.X > Server Management Console**).

5. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Configuring CIMOM server authentication

CIMOM server authentication is the authentication mechanism between the CIM client and the CIMOM Server. You can configure the CIMOM server to allow the CIM client to query the CIMOM server without providing credentials; however, the CIMOM server requires the Management application credentials to connect to the Management application server to retrieve the required data. Therefore, if you select no authentication, you must provide Management application credentials to retrieve data from the Management application server.

To configure CIMOM server authentication, complete the following steps.

1. Click the **Authentication** tab.
2. Choose from one of the following options:
   - Select **No Authentication** to allow the CIM client to query the CIMOM server without providing credentials; however, note that the CIMOM server requires the Management application credentials to connect to the Management application server to retrieve the required data. To provide Management application credentials, complete the following steps.
     a. Enter the Management application user name in the **Username** field.
     b. Enter the Management application user password in the **Password** field.
   - Select *Management_Application* **Authentication** to allow the CIM client to query the CIMOM server and the Management application server using the credentials configured on the **Users** tab.
3. Click **Apply**.

NOTE
Changes on this tab take effect after the next CIMOM server restart.

NOTE
You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **11.X.X > Server Management Console**).

4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

CIMOM configuration

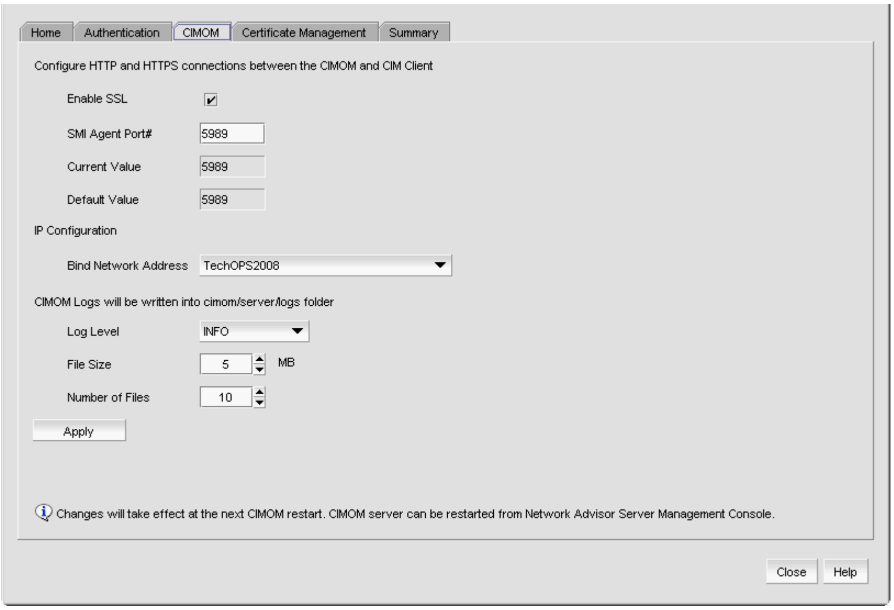
NOTE
You must have SAN - SMI Operation Read and Write privileges to view or make changes on the CIMOM tab.

The **CIMOM** tab enables you to configure the CIMOM server port, the Bind Network Address, and the CIMOM log.

Configuring the SMI Agent port number

To configure the SMI Agent port number, complete the following steps.

1. Click the **CIMOM** tab.



Configure HTTP and HTTPS connections between the CIMOM and CIM Client

Enable SSL ☑

SMI Agent Port# 5989

Current Value 5989

Default Value 5989

IP Configuration

Bind Network Address TechOPS2008

CIMOM Logs will be written into cimom/server/logs folder

Log Level INFO

File Size 5 MB

Number of Files 10

Changes will take effect at the next CIMOM restart. CIMOM server can be restarted from Network Advisor Server Management Console.

FIGURE 88 CIMOM tab

2. Select or clear the **Enable SSL** check box, to enable or disable SSL for the SMI Agent.

   NOTE
   Disabling SSL will disable Indication and Client Mutual Authentication.

   If the check box is checked (default), SSL is enabled. If the check box is clear, SSL is disabled.

3. Enter the SMI Agent port number in the **SMI Agent Port #** field.

   This port number must be within the range of 1 through 65535. Defaults are 5989 with SSL enabled and 5988 with SSL disabled.

4. Click **Apply**.

   NOTE
   Changes on this tab take effect after the next CIMOM server restart.

   NOTE
   You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **11.X.X** > **Server Management Console**).

   If you disabled SSL, a confirmation message displays. Click **Yes** to continue.

5. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Configuring the Bind Network Address

NOTE
You must have SAN - SMI Operation Read and Write privileges to view or make changes on the CIMOM tab.

To configure the network bind address, complete the following steps.

1. Click the **CIMOM** tab.
2. Select a network address from the **IP Configuration Bind Network Address** list to which you want to bind the CIMOM server.

   The default network address is the host system name.

3. Click **Apply**.

   NOTE
   Changes on this tab take effect after the next CIMOM server restart.

   NOTE
   You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **11.X.X** > **Server Management Console**).

4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Configuring the CIMOM log

NOTE
You must have SAN - SMI Operation Read and Write privileges to view or make changes on the **CIMOM** tab.

To configure the CIMOM log, complete the following steps.

1. Click the **CIMOM** tab.
2. Select a log category from the **Log Level** list to start logging support data for the server.

   Options include the following:

   - Off—select to turn off logging support data.
   - Severe—select to only log support data that indicates serious failures which prevent normal program operation.
   - Warning—select to only log support data that indicates a potential problem.
   - Info (default)—select to only log support data for informational messages.
   - Config—select to only log support data for static configuration messages used to assist in debugging problems associated with particular configurations.
   - Fine—select to only log message data used to provide trace information.
   - Finer—select to only log message data used to provide detailed trace information.
   - Finest—select to only log message data used to provide highly detailed trace information.
   - All—select to log support data for all messages.
3. Click **Apply**.

   NOTE
   Changes on this tab take effect after the next CIMOM server restart.

   NOTE
   You can only restart the server using the Server Management Console (**Start > Programs >** *Management_Application_Name* **11.X.X > Server Management Console**).
4. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Certificate management

NOTE
You must have SMI Operation Read and Write privileges to view or make changes on the **Certificate Management** tab.

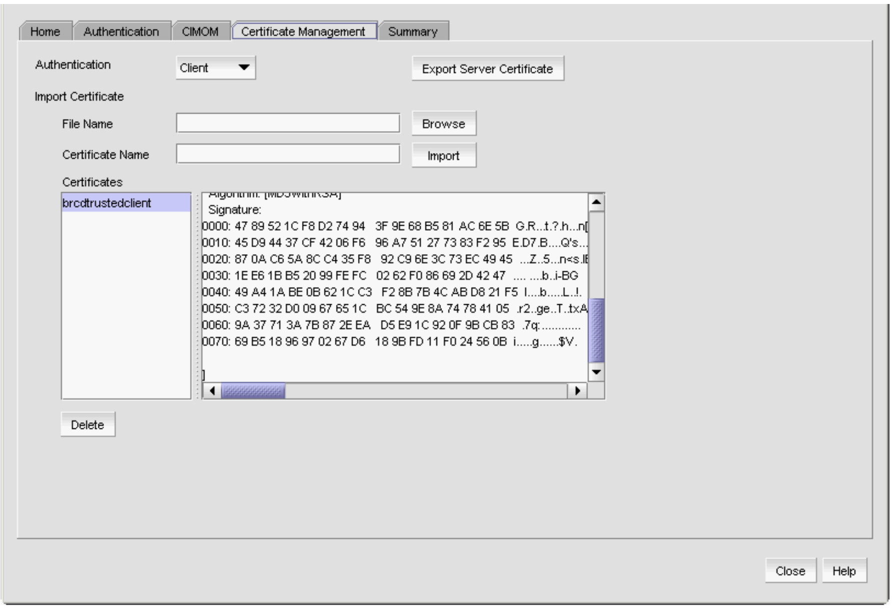
The **Certificate Management** tab enables you to manage your CIM client and Indication authentication certificates. Using this tab, you can perform the following operations:

- “Importing a certificate”
- “Viewing a certificate”
- “Exporting a certificate”
- “Deleting a certificate”

Importing a certificate

To import a certificate, complete the following steps.

1. Click the **Certificate Management** tab.



Authentication: Client

Certificates: brcdtrustedclient

```
 Algorithm: [MD5withRSA]
 Signature:
0000: 47 89 52 1C F8 D2 74 94   3F 9E 68 B5 81 AC 6E 5B  G.R...t.?.h...n[
0010: 45 D9 44 37 CF 42 06 F6   96 A7 51 27 73 83 F2 95  E.D7.B....Q's...
0020: 87 0A C6 5A 8C C4 35 F8   92 C9 6E 3C 73 EC 49 45  ...Z..5...n<s.IE
0030: 1E E6 1B B5 20 99 FE FC   02 62 F0 86 69 2D 42 47  .... ....b..i-BG
0040: 49 A4 1A BE 0B 62 1C C3   F2 8B 7B 4C AB D8 21 F5  I....b.....L..!.
0050: C3 72 32 D0 09 67 65 1C   BC 54 9E 8A 74 78 41 05  .r2..ge..T..txA
0060: 9A 37 71 3A 7B 87 2E EA   D5 E9 1C 92 0F 9B CB 83  .7q:............
0070: 69 B5 18 96 97 02 67 D6   18 9B FD 11 F0 24 56 0B  i.....g......$V.

]
```

FIGURE 89 Certificate Management tab

2. Select the **Client** or **Indication** from the **Authentication** list.

   The appropriate certificates display in the **Certificates** list.

3. Enter the full path or browse to the certificate you want to import (for example, on Windows the path is C:\Certificates\cimom-indication-auth2.cer and on Linux the path is opt/Certificates/cimom-indication-auth2.cer).

   You can only import certificate files with the CER extension (.cer).

4. Enter a name for the certificate in the **Certificate Name** field.

5. Click **Import.**

   The new certificate displays in the **Certificates** list and text box.

   If the certificate location is not valid, an error message displays. Click **OK** to close the message and reenter the full path to the certificate location.

   If you did not enter a certificate name, an error message displays. Click **OK** to close the message and enter a name for the certificate.

   If the certificate file is empty or corrupted, an error message displays. Click **OK** to close the message.

6. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Viewing a certificate

NOTE
You must have SMI Operation Read and Write privileges to view the **Certificate Management** tab.

To view a certificate, complete the following steps.

1. Select **Client** or **Indication** from the **Authentication** list.

   The appropriate certificates display in the **Certificates** list.

2. Select the certificate you want to view in the **Certificates** list.

   The certificate details display in the **Certificates** text box.

3. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Exporting a certificate

NOTE
You must have SMI Operation Read and Write privileges to view or make changes to the **Certificate Management** tab.

To export a certificate, complete the following steps.

1. Click the **Certificate Management** tab.
2. Select **Client** or **Indication** from the **Authentication** list.

   The appropriate certificates display in the **Certificates** list.

3. Select the certificate you want to export in the **Certificates** list.
4. Click **Export Server Certificate.**

   The **Save As** dialog box displays.

5. Browse to the directory where you want to export the certificate.
6. Edit the certificate name in the **File Name** field, if necessary.
7. Click **Save**.
8. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Deleting a certificate

NOTE
You must have SMI Operation Read and Write privileges to view or make changes to the **Certificate Management** tab.

To delete a certificate, complete the following steps.

1. Click the **Certificate Management** tab.
2. Select **Client** or **Indication** from the **Authentication** list.

   The appropriate certificates display in the **Certificates** list.
3. Select the certificate you want to delete in the **Certificates** list.
4. Click **Delete**.
5. Click **Yes** on the confirmation message.

   The selected certificate is removed from the **Certificates** list.
6. Click **Close** to close the **SMIA Configuration Tool** dialog box.

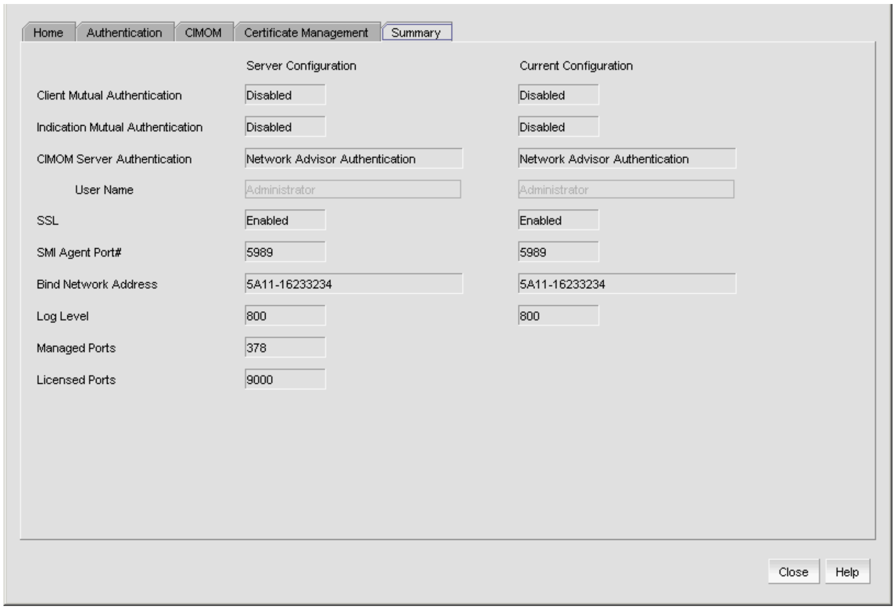
Viewing the configuration summary

To view summary information about the Server configuration and the current configuration, complete the following steps.

NOTE
Server configuration changes in the **Summary** tab only take effect after the CIMOM restart.

NOTE
You can only restart the server using the Server Management Console (**Start** > **Programs** > *Management_Application_Name* **11.X.X** > **Server Management Console**).

1. Click the **Summary** tab.



	Server Configuration	Current Configuration
Client Mutual Authentication	Disabled	Disabled
Indication Mutual Authentication	Disabled	Disabled
CIMOM Server Authentication	Network Advisor Authentication	Network Advisor Authentication
User Name	Administrator	Administrator
SSL	Enabled	Enabled
SMI Agent Port#	5989	5989
Bind Network Address	5A11-16233234	5A11-16233234
Log Level	800	800
Managed Ports	378	
Licensed Ports	9000	

FIGURE 90 Summary tab

2. Review the summary.

   NOTE
   When the CIMOM server is stopped, the server configuration information does not display on the **Summary** tab.

   The following information is included in the summary.

Field/Component	Description
Client Mutual Authentication	Displays whether or not the client mutual authentication is enabled or disabled for the Server Configuration and the Current Configuration.
Indication Mutual Authentication	Displays whether or not the indication mutual authentication is enabled or disabled for the Server Configuration and the Current Configuration.
CIMOM Server Authentication	Displays whether or not the CIMOM server authentication is enabled or disabled for the Server Configuration and the Current Configuration.

Field/Component	Description
User Name	Displays the user name for the Server Configuration and the Current Configuration. Only enabled if **CIMOM Server Authentication** is No Authentication.
SSL	Displays whether or not the SSL is enabled or disabled for the Server Configuration and the Current Configuration.
SMI Agent Port #	Displays the SMI Agent port number for the Server Configuration and the Current Configuration.
Bind Network Address	Displays the Bind Network address for the Server Configuration and the Current Configuration.
Log Level	Displays the log level for the Server Configuration and the Current Configuration. Options include the following: • 10000—Off • 1000—Severe • 900—Warning • 800—Info (default) • 700—Config • 500—Fine • 400—Finer • 300—Finest • 0—All
Managed Ports	Displays the number of managed ports. For more information about managed port count rules, refer to "Managed count" on page 44.
Licensed Ports	Displays the number of licensed ports.

3. Click **Close** to close the **SMIA Configuration Tool** dialog box.

Chapter

SAN Device Configuration 11

In this chapter

Configuration repository management

(Trial and Licensed version) Configuration files are stored in an Postgress database on the Management application server. You can save entire configurations of switch configuration files and use them to ensure consistent switch settings in your fabric, propagate configuration settings to additional switches in the fabric, and troubleshoot the switches.

For Windows platforms the default location is
Install_Home\data\database\*Management_Application_Name*.db

For more information about the database fields, refer to "Database Fields" on page 967.

Saving switch configurations

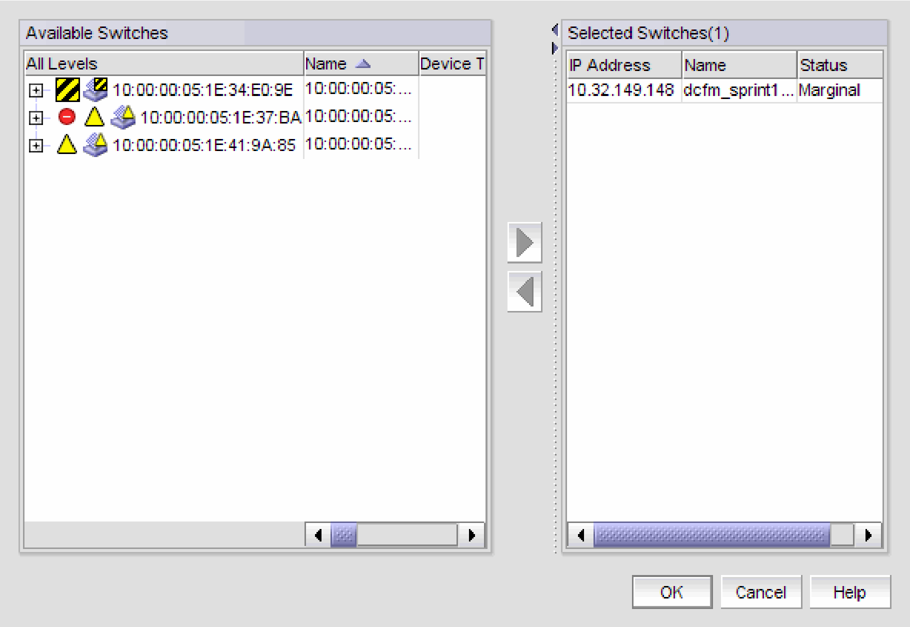
NOTE
Save switch configuration is only supported on Fabric OS switches.

NOTE
To save switch configuration on more than one switch at a time, you must have the Enhanced Group Management license.

Configuration files are uploaded from the selected switches and stored in individual files. Files are named with the convention *cfg_fabricName_switchName_domainID*.

1. Select **Configure** > **Configuration** > **Save**.

   The **Save Switch Configurations** dialog box displays.



All Levels	Name	Device T
10:00:00:05:1E:34:E0:9E	10:00:00:05:...	
10:00:00:05:1E:37:BA	10:00:00:05:...	
10:00:00:05:1E:41:9A:85	10:00:00:05:...	

IP Address	Name	Status
10.32.149.148	dcfm_sprint1...	Marginal

FIGURE 91 Save switch configurations

2. Select the switches for which you want to save configuration files from **Available Switches**.
3. Click the right arrow to move the selected switches to **Selected Switches**.
4. Click **OK**.

   Configuration files from the selected switches are saved to the repository.

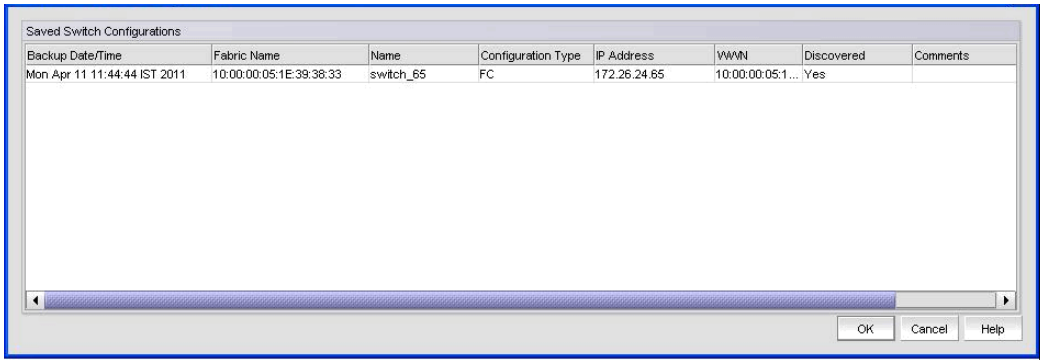
Restoring a switch configuration for a selected device

The **Restore Switch Configuration** dialog box enables you to download a previously saved switch configuration to a selected device.

To restore a switch configuration, complete the following steps.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Restore**.

   The **Restore Switch Configuration** dialog box displays.



Saved Switch Configurations

Backup Date/Time	Fabric Name	Name	Configuration Type	IP Address	WWN	Discovered	Comments
Mon Apr 11 11:44:44 IST 2011	10:00:00:05:1E:39:38:33	switch_65	FC	172.26.24.65	10:00:00:05:1...	Yes	

FIGURE 92 Restore Switch Configuration dialog box

2. Select the switch configuration you want to download from the **Saved Switch Configurations** table.

3. Click **OK**.

   The configuration is downloaded to the device. If necessary, the restoration process prompts you to disable and reboot the device before the configuration begins. This lets you determine whether the configuration backup should be performed immediately or at a later time.

   When you restore a switch configuration on a Virtual Fabrics-configured chassis, the configuration data for the logical switches is downloaded to the switch as configured in the file. When you restore a switch configuration on a logical switch, only the selected logical switch configuration data is downloaded to the switch.

Backing up a switch configuration

NOTE
The Enhanced Group Management (EGM) license must be activated on a switch to perform this procedure and to use the supportSave module.

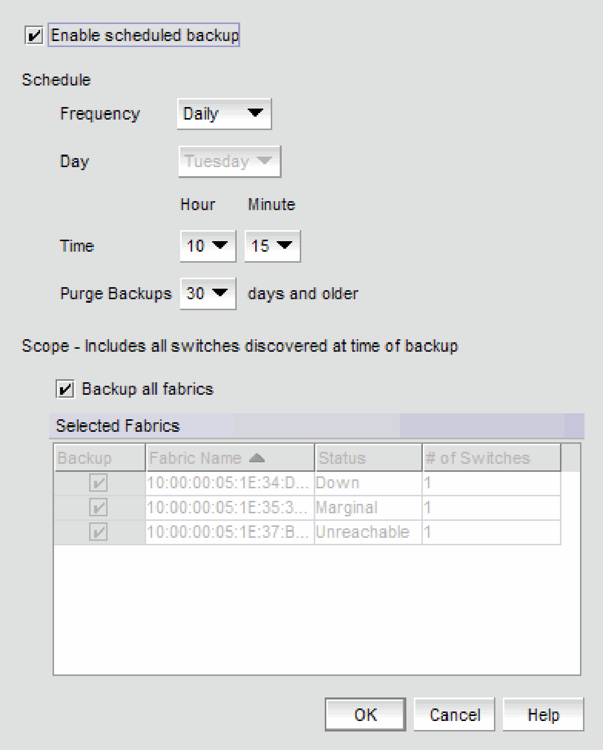
If a periodic backup is scheduled at the SAN level, that backup will apply to all switches from all fabrics discovered. Any new fabrics being discovered are automatically added to the list of fabrics to be backed up.

NOTE
If a backup is scheduled for more than one fabric and some of the fabrics contain common members, the backup will include the unique switch configuration values obtained from the fabrics.

You can schedule a backup of one or more switch configurations. The configuration files are stored in the Management application database.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Schedule Backup**.

   The **Schedule Backup of Switch Configurations** dialog box displays.



☑ Enable scheduled backup

Schedule

Frequency: Daily

Day: Tuesday

Time: Hour 10, Minute 15

Purge Backups: 30 days and older

Scope - Includes all switches discovered at time of backup

☑ Backup all fabrics

Selected Fabrics

Backup	Fabric Name	Status	# of Switches
☑	10:00:00:05:1E:34:D...	Down	1
☑	10:00:00:05:1E:35:3...	Marginal	1
☑	10:00:00:05:1E:37:B...	Unreachable	1

FIGURE 93 Schedule backup of switch configurations

2. Click the **Enable scheduled backup** check box.

3. Set the **Schedule** parameters. These include the following:
   - The desired **Frequency** for backup operations (daily, weekly, monthly).
   - The **Day** you want back up to run.

     If **Frequency** is **Daily**, the Day list is grayed out.

     If **Frequency** is **Weekly**, choices are days of the week (Sunday through Saturday).

     If **Frequency** is **Monthly**, choices are days of the month (1 through 31).
   - The **Time** (hour, minute) you want back up to run.
   - The maximum age allowed before you **Purge Backups**.

     The number of purge days should be at least one day more than the selected backup frequency.

     The backup purge thread runs every day at 12:30 PM and deletes all back up configurations that exceed the maximum age allowed.
4. Choose one of the following options to determine the scope of the backup.
   - Select the **Backup all fabrics** check box, if necessary, to back up all switch configurations of discovered switches in all fabrics
   - Clear the **Backup all fabrics** check box and select the specific fabric check boxes in the **Selected Fabrics** table to back up individual fabrics.

     If any switches do not have the EGM license, a messages displays. Click **OK** to enable backup on the switches with the EGM license.
5. Click **OK**.

   Click **OK** on the confirmation message.

Restoring a configuration from the repository

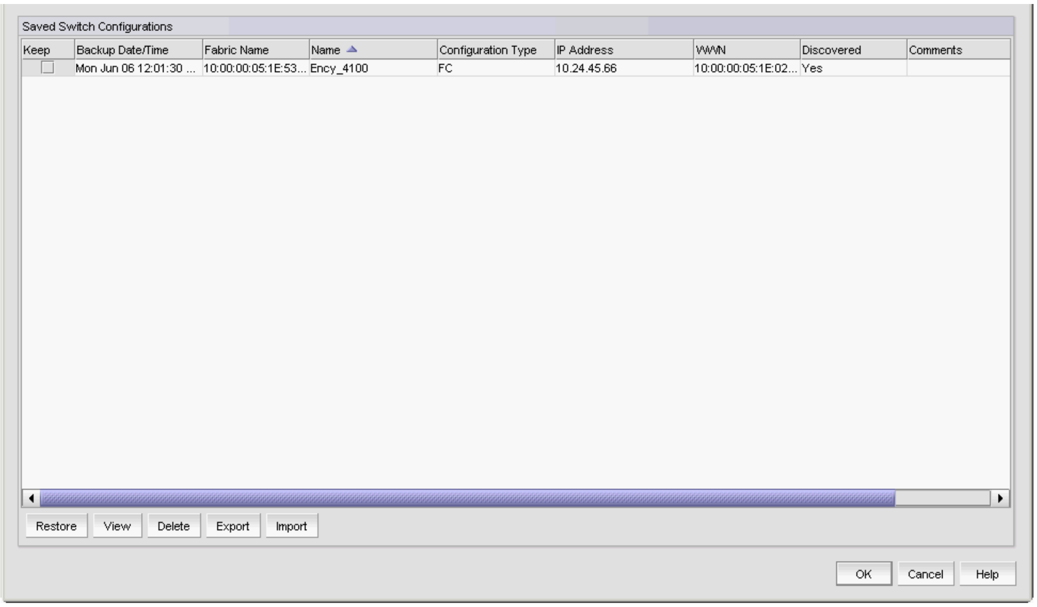
If you delete a fabric or switch from discovery, the configuration remains in the repository until you delete it manually. Stored configurations are linked to the switch WWN; therefore, if the IP address or switch name is changed and then rediscovered, the Switch Configuration Repository dialog box displays the new switch name and IP address for the old configuration.

NOTE
This feature requires a Trial or Licensed version.

---

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

   The **Switch Configuration Repository** dialog box displays (Figure 94).



Saved Switch Configurations

Keep	Backup Date/Time	Fabric Name	Name ▲	Configuration Type	IP Address	WWN	Discovered	Comments
□	Mon Jun 06 12:01:30 ...	10:00:00:05:1E:53...	Ency_4100	FC	10.24.45.66	10:00:00:05:1E:02...	Yes	

FIGURE 94 Switch Configuration Repository

2. Select the configuration you want to restore, and click **Restore**.

   The configuration is downloaded to the device. If necessary, the restoration process prompts you to disable and reboot the device before the configuration begins. This lets you determine whether the configuration backup should be performed immediately or at a later time.

   If you confirm the restoration, the entire configuration is restored; you cannot perform selective download for specific configuration sections.

Viewing configuration file content

NOTE
This feature requires a Trial or Licensed version.

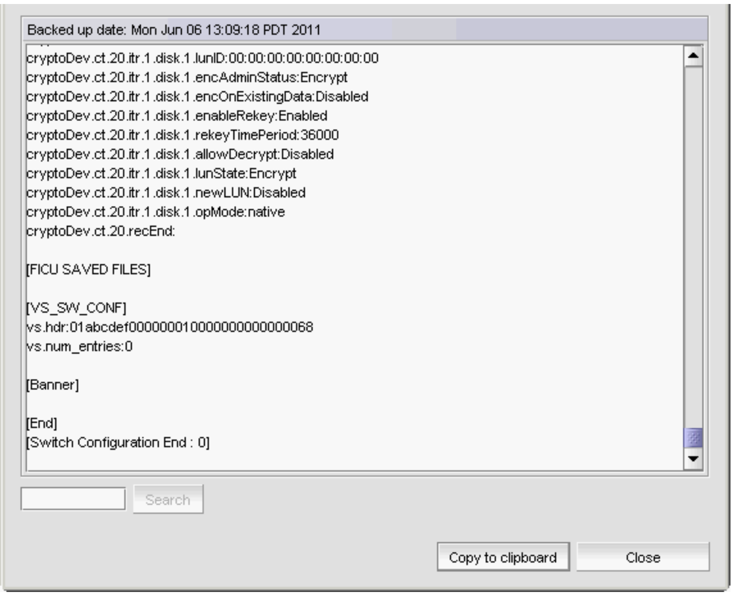
You can view switch configuration file content in a text file.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

   The **Switch Configuration Repository** dialog box displays.

2. Click **View**.

   The configuration details display. If you want to save the contents as a text file, click **Copy to Clipboard**, paste the copy into a text editor (Notepad or Wordpad on Windows systems), and save the file.



Backed up date: Mon Jun 06 13:09:18 PDT 2011

```
cryptoDev.ct.20.itr.1.disk.1.lunID:00:00:00:00:00:00:00:00
cryptoDev.ct.20.itr.1.disk.1.encAdminStatus:Encrypt
cryptoDev.ct.20.itr.1.disk.1.encOnExistingData:Disabled
cryptoDev.ct.20.itr.1.disk.1.enableRekey:Enabled
cryptoDev.ct.20.itr.1.disk.1.rekeyTimePeriod:36000
cryptoDev.ct.20.itr.1.disk.1.allowDecrypt:Disabled
cryptoDev.ct.20.itr.1.disk.1.lunState:Encrypt
cryptoDev.ct.20.itr.1.disk.1.newLUN:Disabled
cryptoDev.ct.20.itr.1.disk.1.opMode:native
cryptoDev.ct.20.recEnd:

[FICU SAVED FILES]

[VS_SW_CONF]
vs.hdr:01abcdef000000010000000000000068
vs.num_entries:0

[Banner]

[End]
[Switch Configuration End : 0]
```

FIGURE 95 Configuration file content

3. Click **Close** to close the dialog box.
4. Click **Yes** on the message.

Searching the configuration file content

NOTE
This feature requires a Trial or Licensed version.

To search the configuration file content, complete the following steps.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository.**

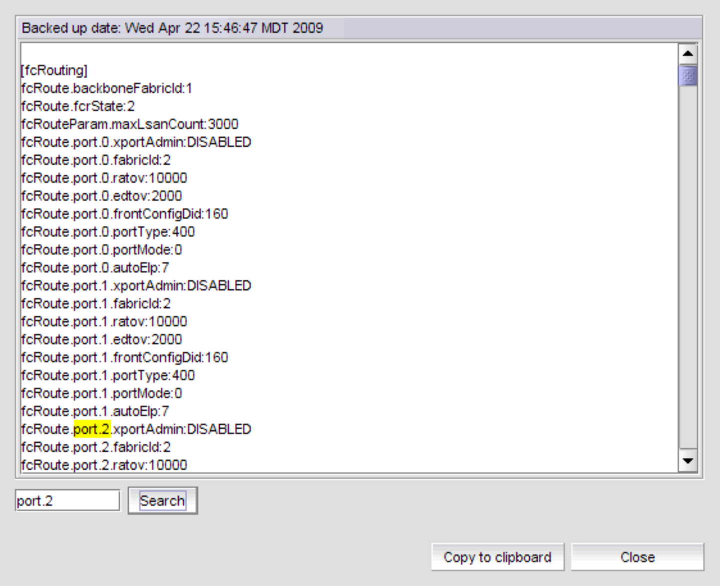
   The **Switch Configuration Repository** dialog box displays.

2. Click **View.**

   The configuration details display.

3. Enter the information you want to search for in the field and click **Search.**

   The text string you are searching for is highlighted in the dialog box. Continue clicking **Search** to scroll through the contents until you find the information you need. If the search item is not found a ‘not found’ message displays. Click **OK** to close the message.



Backed up date: Wed Apr 22 15:46:47 MDT 2009

```
[fcRouting]
fcRoute.backboneFabricId:1
fcRoute.fcrState:2
fcRouteParam.maxLsanCount:3000
fcRoute.port.0.xportAdmin:DISABLED
fcRoute.port.0.fabricId:2
fcRoute.port.0.ratov:10000
fcRoute.port.0.edtov:2000
fcRoute.port.0.frontConfigDid:160
fcRoute.port.0.portType:400
fcRoute.port.0.portMode:0
fcRoute.port.0.autoElp:7
fcRoute.port.1.xportAdmin:DISABLED
fcRoute.port.1.fabricId:2
fcRoute.port.1.ratov:10000
fcRoute.port.1.edtov:2000
fcRoute.port.1.frontConfigDid:160
fcRoute.port.1.portType:400
fcRoute.port.1.portMode:0
fcRoute.port.1.autoElp:7
fcRoute.port.2.xportAdmin:DISABLED
fcRoute.port.2.fabricId:2
fcRoute.port.2.ratov:10000
```

port.2

FIGURE 96 **Configuration file content**

4. Click **Close** to close the dialog box.

5. Click **Yes** on the message.

Deleting a configuration

NOTE
This feature requires a Trial or Licensed version.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

   The **Switch Configuration Repository** dialog box displays.

2. Select the configuration you want to delete, and click **Delete**.

Exporting a configuration

NOTE
This feature requires a Trial or Licensed version.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

   The **Switch Configuration Repository** dialog box displays.

2. Select the configuration you want to export, and click **Export**.

   The file chooser appropriate to your operating system displays.

3. Use the file chooser to select the location into which you want to export the configuration.

4. Click **Export**.

   The configuration is automatically named (*Device_Name_Date_and_Time)* and exported to the location you selected.

Importing a configuration

NOTE
This feature requires a Trial or Licensed version.

1. Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

   The **Switch Configuration Repository** dialog box displays.

2. Click **Import**.

   The file chooser appropriate to your operating system displays.

3. Use the file chooser to select the file from which you want to import the configuration, and click **Import**.

Keeping a copy past the defined age limit

NOTE
This feature requires a Trial or Licensed version.

1. Right click a device in the Product List or the Connectivity Map, and select **Configuration > Configuration Repository**.

   The **Switch Configuration Repository** dialog box displays.

2. Select the check box under **Keep** for the configuration you want to preserve. The configuration will be kept until it is manually deleted, or until the **Keep** check box is cleared to enable the age limit again.
3. Click **OK**.

Replicating configurations

NOTE
This feature requires a Trial or Licensed version.

You can replicate a switch SNMP configuration, the Fabric Watch configuration, Trace Destination configuration, or the entire configuration.

Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Replicate > Configuration**.

A wizard is launched to guide you through the process.

Replicating security configurations

NOTE
This feature requires a Trial or Licensed version.

You can replicate an AD/LDAP Server, DCC, IP, RADIUS Server, or SCC security policy.

Right-click a device in the Product List or the Connectivity Map, and select **Configuration > Replicate > Security.**

A wizard is launched to guide you through the process.

Enhanced group management

Use Enhanced Group Management (EGM), a separate licensed feature, to control access to specific features on Fabric OS devices. The features affected include the following:

- Firmware Download - enables you to perform group firmware download.

  For specific instructions for firmware download, refer to "Firmware management" on page 265.
- Security - enables you to perform Group Security Policy Replication.

  For specific instructions for security, refer to "Configuration repository management" on page 255.
- Configuration Management - enables you to perform Group Configuration Upload and Replication.

  For specific instructions for configuration management, refer to "Replicating configurations" on page 264.

Firmware management

A firmware file repository (Windows systems only) is maintained on the server in the following location: C:\Program Files*Install_Directory*\data\ftproot\Firmware\Switches\7.0\n.n.n\n.n.n

The firmware repository is used by the internal FTP server that is delivered with the Management application software, and may be used by an external FTP server if it is installed on the same platform as the Management application software. The repository is not available to FTP servers on external platforms. The repository is used only for Fabric OS firmware. M-EOS firmware is handled through the Element Manager specific to the switch or director model.

NOTE
Non-disruptive firmware download (HCL) is not supported when downgrading from Fabric OS version 7.0 to 6.4. You must remove all non-default logical switches and disable Virtual Fabrics before downgrading.

NOTE
Firmware download is not supported in pure IPv6 mode.

NOTE
You cannot use Fabric OS firmware download with command line options in the Management application.

Displaying the firmware repository

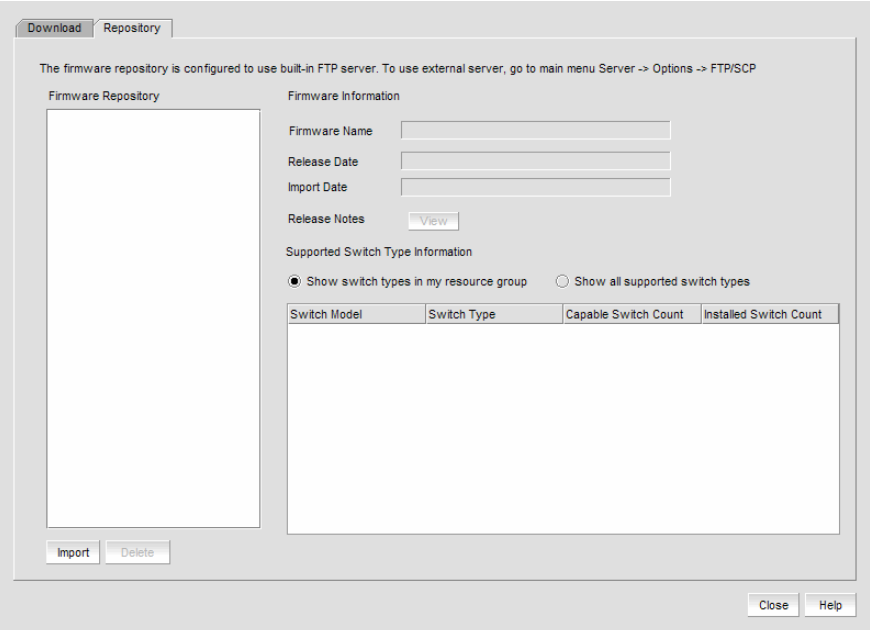
The firmware repository is available on the **Firmware Management** dialog box. The Management application supports .zip and .gz compression file types for firmware files.

1. Select **Configure** > **Firmware Management**.

   The **Firmware Management** dialog box displays.

2. Select the **Repository** tab (Figure 97).

   Initially, the repository is empty. You must import firmware files into the repository. Imported firmware files are then displayed under **Firmware Repository**.



The firmware repository is configured to use built-in FTP server. To use external server, go to main menu Server -> Options -> FTP/SCP

● Show switch types in my resource group ○ Show all supported switch types

Switch Model	Switch Type	Capable Switch Count	Installed Switch Count

FIGURE 97 Firmware repository

3. View information about a specific firmware file by selecting the firmware file in the **Firmware Repository**.

   The **Firmware Name**, **Release Date**, and **Import Date** are displayed. You may also view the **Release Notes**, if the release notes were imported.

Importing a firmware file and release notes

Firmware files and release notes can be imported into the Firmware Repository.

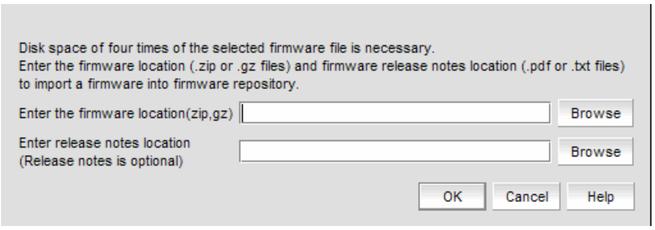
1. Select **Configure** > **Firmware Managemen**t.

   The **Firmware Management** dialog box displays.

2. Select the **Repository** tab (Figure 97).

3. Click **Import**.

   The **Import Firmware from File** dialog box displays (Figure 98).



Disk space of four times of the selected firmware file is necessary.
Enter the firmware location (.zip or .gz files) and firmware release notes location (.pdf or .txt files) to import a firmware into firmware repository.

Enter the firmware location(zip,gz)

Enter release notes location
(Release notes is optional)

FIGURE 98 **Import firmware**

4. Type in the location of the firmware file and release notes, or use **Browse** to select the location.

   The Management application supports .zip and .gz compression file types for firmware files.

5. Click **OK**.

   You return to the **Repository** tab. The file is listed in the Firmware Repository when the import is complete and successful.

Deleting a firmware file

Firmware files can be deleted from the Firmware Repository.

1. Select **Configure** > **Firmware Managemen**t.

   The **Firmware Management** dialog box displays.

2. Select the **Repository** tab (Figure 97).

3. Select one or more firmware files from the Firmware Repository for deletion.

4. Click **Delete**.

   A confirmation dialog displays. Click **Yes** to confirm. The firmware file is deleted from the repository.

Download firmware

NOTE
Non-disruptive firmware download (HCL) is not supported when downgrading from Fabric OS version 6.2 to 6.1. You must remove all non-default logical switches and disable Virtual Fabrics before downgrading.

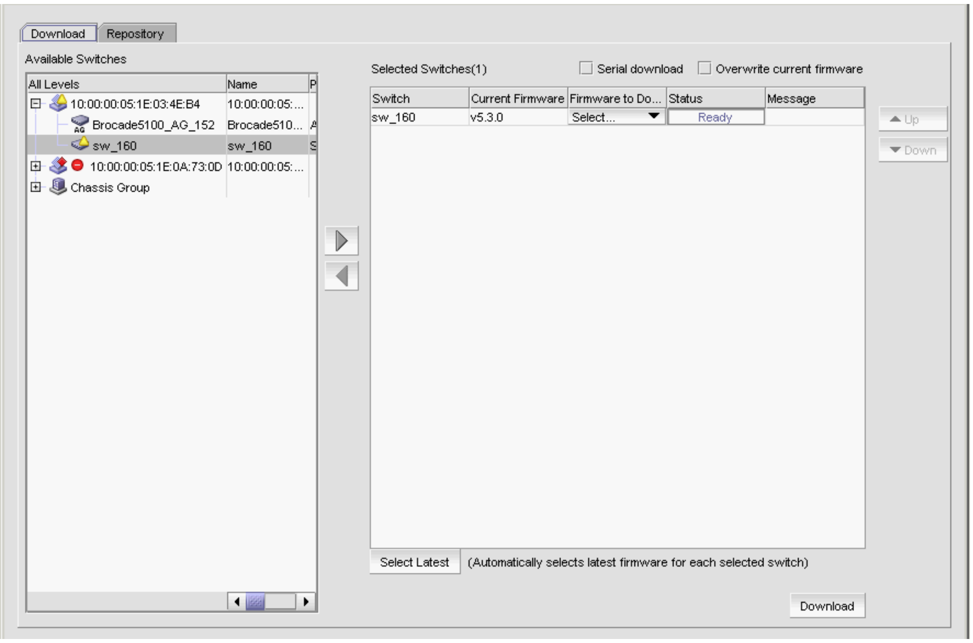
NOTE
You cannot use Fabric OS firmware download with command line options in the Management application.

You can download firmware using the **Firmware Management** dialog box.

1. Select **Configure** > **Firmware Managemen**t.

   The **Firmware Management** dialog box displays.

2. Select the **Download** tab (Figure 99).



Available Switches

All Levels	Name	P
⊟ 10:00:00:05:1E:03:4E:B4	10:00:00:05:...	
Brocade5100_AG_152	Brocade510...	A
sw_160	sw_160	S
⊞ 10:00:00:05:1E:0A:73:0D	10:00:00:05:...	
⊞ Chassis Group		

Selected Switches(1) ☐ Serial download ☐ Overwrite current firmware

Switch	Current Firmware	Firmware to Do...	Status	Message
sw_160	v5.3.0	Select...	Ready	

(Automatically selects latest firmware for each selected switch)

FIGURE 99 Firmware download

3. Select one or more switches from the **Available Switches** table.

4. Click the right arrow to move the switches to the **Selected Switches** table.

   If you selected any switches that do not support firmware download, a message displays. Click **OK** on the message.

   The switches that support firmware download display in the **Selected Switches** table.

5. Select a specific version from the **Firmware to Download** column, or use **Select Latest** to automatically select the latest version.

   If you have your FTP or SCP Server configured to use an external FTP or SCP Server, the **Firmware to Download** column is empty.

6. To download the firmware to the selected switches one at a time, select the **Serial download** check box.

   Use the **Up** and **Down** buttons to determine the order in which the firmware is downloaded to the switches. If firmware download fails on one switch, all other switches in the queue will be skipped.

   If the **Serial download** check box is cleared, the download occurs in parallel on the switches (up to 20 at a time).

7. To overwrite the current firmware, even if the selected version is the same as the version currently running on the switch, click the **Overwrite Current Firmwares** check box.

8. If you configured an external FTP server, choose from one of the following options:

   - Select **External FTP Server** to download from the external FTP server.

     If you select external FTP server, configure the following on the FTP server:

     - Create user and password.
     - Select the **Shared folders** link and set firmware location as the home directory and select all check boxes under the **Files** and **Directories** attributes.
   - Select **SCP Server** to download from the external SCP server.

   NOTE
   The Management application only supports WinSSHD as the third-party Windows external SCP server. Firmware upgrade and downgrade through WinSSHD is only supported on devices running Fabric OS 7.0 or later.

9. If you configured an external server, enter the path to the firmware directory in the **Firmware Directory** field.

   A confirmation message displays. Click **Yes** on the confirmation message.

   This field does not display if the external server is installed on the same machine as the Management application and occupies port 21.

10. Click **Download**.

    While the firmware is downloaded to the device, the **Status** column displays the current download status. Once firmware download is complete, the **Message** column displays whether the download was a success or failure.

Properties

You can customize the device and fabric **Properties** dialog boxes to display only the data you need by adding, editing, and deleting property labels. You can also edit property fields to change information.

Viewing Fabric properties

To view the properties for a fabric, complete the following step.

1. Right-click any fabric and select **Properties**.

   The *Fabric_Name* **Properties** dialog box displays, with information related to the selected fabric.

TABLE 17 Fabric properties

Field/Component	Description
Name	The name specified through the switch Element Manager.
FID Fabric Name	Enter a name for the fabric (up to 128 characters). Supported on seed switches running Fabric OS 7.0 or later.
Seed Switch	The IP address of the seed switch.
AD Enabled	Whether admin domain is enabled on the switch or not.
Status	The operational status.
Switch and AG Count	The number of switches and Access Gateway's in the fabric.
Description	A description of the customer site.
Principal Switch	The IP address of the principal switch.
Active Zone Configuration	Whether active zone configuration is activated on the fabric.
Last Discovery	The date and time of last discovery.
Tracked	Whether the fabric is tracked.
Location	The customer site location.
Contact	The primary contact at the customer site.

2. Click **OK** on the *Fabric_Name* **Properties** dialog box to close.

Viewing device properties

To view the properties for a device or, complete the following step.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays, with information related to the selected device (such as, switches, directors, HBAs, trunks, tunnels, and nodes).

   Depending on the device type, some of the properties listed in the following table may not be available for all products.

TABLE 18 Device properties

Field/Component	Description
Addressing Mode	The addressing mode of the switch.
Back to Edge Routing Supported	Whether back to edge routing is supported.
Bandwidth	The bandwidth of the FCIP tunnel.
Capability	The node capability.
Compression	Whether compression is On or Off for the FCIP tunnel.
Connected Virtual FCoE Port	The fabric name, switch name, and virtual FCoE port number of the connected virtual FCoE port.
Contact	The primary contact at the customer site.
Contributors	The device contributors.
Device Type	Whether the device is an initiator or target.
Description	A description of the customer site.
Destination IP Address	The IP address of the of the FCIP tunnel destination device.
Discovery Status	The discovery status of the switch. Examples include ‘Discovered: Seed Switch’ and ‘Discovered: Not Reachable’.
Domain ID	The device’s domain ID, which is the top-level addressing hierarchy of the domain.
Fabric	The fabric name.
Fabric Name	The name specified through the device Element Manager.
Fabric Watch	Whether Fabric Watch is up or down.
Fastwrite	Whether fastwrite is On or Off for the FCIP tunnel.
FC Port	The FC port of the FCIP tunnel.
FCoE Capable	Whether the device is Fibre Channel over Ethernet capable.
FCS Role	Whether FCS is supported.
Firmware	The firmware version.
GigE Port	The GigE port of the FCIP tunnel.
Host Name	The Host name.
IKE Policy #	The IKE policy number. Also includes the following information: • Authentication Algorithm • Encryption Algorithm • Diffie-Hellman • SA Life

TABLE 18 Device properties (Continued)

Field/Component	Description
IP Address	The device's IP address.
IPSec Policy #	The IPSec policy number. Also includes the following information: • Authentication Algorithm • Encryption Algorithm • SA Life
L2 Capable	Whether the device is Layer 2 capable.
L3 Capable	Whether the device is Layer 3 capable.
L2 Mode	The Layer 2 mode. Options include Access, Converged, or Trunk.
LAG ID	The link aggregation group identifier.
Last Discovery	The date and time of the last discovery.
Location	The customer site location.
MAC address	In a network, the Media Access Control (MAC) address is a unique number that identifies a specific hardware interface. It is a 12-digit hexadecimal number.
Managed By	The management program used to manage the fabric.
Master Port	The master port of the trunk.
Member Ports	The member ports of the trunk.
Model	The model number of the device.
Name	The user-defined name of the switch.
Node Name	The name of the node.
Node WWN	The world wide name of the node.
Physical/Logical	Whether the device is a physical device or a logical device.
Port Count	The number of ports.
Port Type	The port type.
Preshared key configured	Whether the preshared key is configured for the FCIP tunnel.
Reason	The device status.
Remote Switch Name	The remote switch name of the trunk.
Remote Switch IP	The remote switch IP address of the trunk.
Remote Switch WWN	The remote switch world wide name of the trunk.
Remote Slot #	The remote slot number of the trunk.
Remote Master Port	The remote master port of the trunk.
Remote Member Ports	The remote member port of the trunk.
Sequence number	The sequence number of the switch.
Serial #	The hardware serial number.
Slot #	The slot number of the trunk.
Source IP Address	The IP address of the of the FCIP tunnel source device.
Speed (Gb/s)	The speed of the port in gigabytes per second.

TABLE 18 Device properties (Continued)

Field/Component	Description
State	The device's state, for example, online or offline.
Status	The operational status.
Switch Name	The switch name.
Switch IP	The switch IP address.
Switch WWN	The switch world wide name.
Tape Pipelining	Whether tape pipelining is On or Off for the FCIP tunnel.
Tunnel ID	The tunnel identifier.
Type	The device type.
Unit Type	The unit type of the node.
Vendor	The product vendor.
# Virtual FCoE port count	The number of virtual FCoE ports on the device. There is a one-to-one mapping of TE ports to virtual FCoE ports. Therefore, the number of virtual session ports is one for directly connected devices.
VLAN #	The VLAN number of the FCIP tunnel.
VLAN Class of Service for Control Connection	The VLAN class of service for the control connection of the FCIP tunnel.
VLAN Class of Service for Data Connection	The VLAN class of service for the data connection of the FCIP tunnel.
VLAN ID	The VLAN identification number.
WWN	The world wide name of the device.

2. To view port properties, select one of the following tabs:

   The following port types are available depending on the selected device:

   - FC Ports
   - GigE Ports
   - IP Ports
   - iSCSI Ports
   - Virtual Sessions Ports
   - Virtual FCoE Ports
   - Virtual Machine Ports

3. If you selected the FC Ports tab, select the port type.

   - FC
   - ICL
   - GigE

   For a description of the port properties, refer to "Port properties" on page 283.

Adding a property label

You can add a new field to any of the tabs on the **Properties** dialog box.
To add a new field, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab to which you want to add a property.
3. Right-click on any label.

   The new property label displays above the one you select.

4. Select **Add**.

   The **Add Property** dialog box displays.

5. Type a label and description for the property.
6. Select the property type from the **Type** list, if available.
7. Click **OK**.

   The new property displays above the one you selected.

Editing a property label

You can edit any label that you create on the **Properties** dialog box.

To edit any field you create, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab on which you want to edit a property.
3. Right-click the label for the property you want to edit.
4. Select **Edit**.

   The **Edit Property** dialog box displays.

5. Change the label and description for the property, as needed.
6. Change the property type from the **Type** list, if available.
7. Click **OK**.

Deleting a property label

You can delete any label that you created on any of the tabs from the **Properties** dialog box. To delete a label, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab on which you want to delete a property.
3. Right-click the label for the property you want to delete.
4. Select **Delete**.
5. Click **Yes** on the confirmation message.

   The property you selected is deleted.

Editing a property field

You can edit fields on the **Properties** dialog box. To edit a field, complete the following steps.

1. Right-click any product icon and select **Properties**.

   The **Properties** dialog box displays.

2. Select the tab on which you want to edit a field.

   Fields containing a green triangle (◢) in the lower right corner are editable.

3. Click in an editable field and change the information.
4. Click **OK**.

Ports

You can enable and disable ports, as well as view port details, properties, type, status, and connectivity.

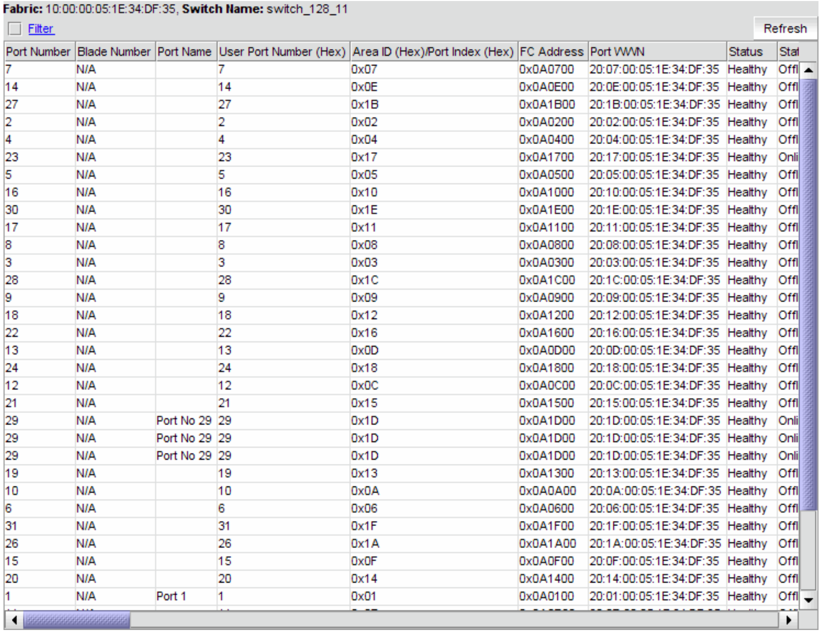
Viewing port connectivity

The connected switch and switch port information displays for all ports.

To view port connectivity, choose one of the following steps:

- Right-click a product icon and select **Port Connectivity.**
- Select a product icon and select **Monitor** > **Port Connectivity.**

  The **Port Connectivity View** dialog box displays (Figure 100).



Fabric: 10:00:00:05:1E:34:DF:35, **Switch Name:** switch_128_11

Port Number	Blade Number	Port Name	User Port Number (Hex)	Area ID (Hex)/Port Index (Hex)	FC Address	Port WWN	Status	Stat
7	N/A		7	0x07	0x0A0700	20:07:00:05:1E:34:DF:35	Healthy	Offl
14	N/A		14	0x0E	0x0A0E00	20:0E:00:05:1E:34:DF:35	Healthy	Offl
27	N/A		27	0x1B	0x0A1B00	20:1B:00:05:1E:34:DF:35	Healthy	Offl
2	N/A		2	0x02	0x0A0200	20:02:00:05:1E:34:DF:35	Healthy	Offl
4	N/A		4	0x04	0x0A0400	20:04:00:05:1E:34:DF:35	Healthy	Offl
23	N/A		23	0x17	0x0A1700	20:17:00:05:1E:34:DF:35	Healthy	Onli
5	N/A		5	0x05	0x0A0500	20:05:00:05:1E:34:DF:35	Healthy	Offl
16	N/A		16	0x10	0x0A1000	20:10:00:05:1E:34:DF:35	Healthy	Offl
30	N/A		30	0x1E	0x0A1E00	20:1E:00:05:1E:34:DF:35	Healthy	Offl
17	N/A		17	0x11	0x0A1100	20:11:00:05:1E:34:DF:35	Healthy	Offl
8	N/A		8	0x08	0x0A0800	20:08:00:05:1E:34:DF:35	Healthy	Offl
3	N/A		3	0x03	0x0A0300	20:03:00:05:1E:34:DF:35	Healthy	Offl
28	N/A		28	0x1C	0x0A1C00	20:1C:00:05:1E:34:DF:35	Healthy	Offl
9	N/A		9	0x09	0x0A0900	20:09:00:05:1E:34:DF:35	Healthy	Offl
18	N/A		18	0x12	0x0A1200	20:12:00:05:1E:34:DF:35	Healthy	Offl
22	N/A		22	0x16	0x0A1600	20:16:00:05:1E:34:DF:35	Healthy	Offl
13	N/A		13	0x0D	0x0A0D00	20:0D:00:05:1E:34:DF:35	Healthy	Offl
24	N/A		24	0x18	0x0A1800	20:18:00:05:1E:34:DF:35	Healthy	Offl
12	N/A		12	0x0C	0x0A0C00	20:0C:00:05:1E:34:DF:35	Healthy	Offl
21	N/A		21	0x15	0x0A1500	20:15:00:05:1E:34:DF:35	Healthy	Offl
29	N/A	Port No 29	29	0x1D	0x0A1D00	20:1D:00:05:1E:34:DF:35	Healthy	Onli
29	N/A	Port No 29	29	0x1D	0x0A1D00	20:1D:00:05:1E:34:DF:35	Healthy	Onli
29	N/A	Port No 29	29	0x1D	0x0A1D00	20:1D:00:05:1E:34:DF:35	Healthy	Onli
19	N/A		19	0x13	0x0A1300	20:13:00:05:1E:34:DF:35	Healthy	Offl
10	N/A		10	0x0A	0x0A0A00	20:0A:00:05:1E:34:DF:35	Healthy	Offl
6	N/A		6	0x06	0x0A0600	20:06:00:05:1E:34:DF:35	Healthy	Offl
31	N/A		31	0x1F	0x0A1F00	20:1F:00:05:1E:34:DF:35	Healthy	Offl
26	N/A		26	0x1A	0x0A1A00	20:1A:00:05:1E:34:DF:35	Healthy	Offl
15	N/A		15	0x0F	0x0A0F00	20:0F:00:05:1E:34:DF:35	Healthy	Offl
20	N/A		20	0x14	0x0A1400	20:14:00:05:1E:34:DF:35	Healthy	Offl
1	N/A	Port 1	1	0x01	0x0A0100	20:01:00:05:1E:34:DF:35	Healthy	Offl

FIGURE 100 Port Connectivity View dialog box

Loop devices are displayed in multiple rows, one row for each related device port.

If no switch or device is connected to the port, then the related fields are empty.

The following table details the information located (in alphabetical order) on the **Port Connectivity View** dialog box.

TABLE 19 Port connectivity properties

Field	Description
Actual Distance	The actual distance for -end port connectivity.
Area ID /Port Index	The area ID and the port index of the port.
Blade Number	The number of the blade.
Blocked	Whether the selected port is blocked.

TABLE 19 Port connectivity properties (Continued)

Field	Description
Buffer Limited	Whether buffers are limited.
Buffers Needed/Allocated	The ratio of buffers needed relative to the number of buffers allocated.
Calculated Status	The operational status. There are four possible operation status values: • Up - Operation is normal. • Down - The port is down or the route to the remote destination is disabled. • Disabled - The connection has been manually disabled. • Backup Active - The backup TCP port is active due to a failover.
Capability	The device capability of the connected device port. The value is mapped depending on whether it is a name server (NS) or a FICON device.
Connected Blade Number	The number of the connected blade.
Connected Port Area ID Port Index	The area ID and the port index of the connected port.
Connected Port Name	The name of the connected port.
Connected Port Number	The number of the connected port.
Connected Port Speed	The speed of the connected port.
Connected Port Status	The connection status. There are four possible operation status values: • Up - Operation is normal. • Down - The port is down or the route to the remote destination is disabled. • Disabled - The connection has been manually disabled. • Backup Active - The backup TCP port is active due to a failover.
Connected Port State	The connected port's state; for example, online or offline.
Connected Port WWN	The world wide name of the connected port.
Connected User Port Number	The port number of the connected user port.
COS	The class of service (CoS) value, which ranges between zero (low priority) and seven (high priority).
Device Node WWN	The world wide name of the device node.
Device Symbolic Name	The symbolic name of the device node.
Device Port/Switch Domain ID	The device port and switch domain ID.
Device Port/Switch WWN	The device port and switch world wide name.
Device Port/Switch Name	The device port and switch name.
Device Port/Switch State	The device port and switch state.
Device Port/Switch Manufacturer	The device port and manufacturer of the switch.
Device Port/Switch Manufacturing Plant	The device port and switch manufacturing plant.
Device Port / Switch Type Number	The device port and switch type number.
Device Type	The device type; for example, target or initiator.

TABLE 19 **Port connectivity properties (Continued)**

Field	Description
FC4 Type	The active FC4 type; for example, SCSI.
FC Address	The Fibre Channel address. Each FC port has both an address identifier and a world wide name (WWN).
Flag	Whether a flag is on or off.
Hard Address	The hard address of the device.
Host Name	The name of the Host.
Long Distance	Whether the connection is considered to be normal or longer distance.
Model	The model name and number of the device.
Parameter	Device parameters.
Physical/Virtual/NPIV	Whether the port is a physical port, a virtual port, or an NPIV_port.
Port Address	The port's address.
Port IP Address	The port's IP address.
Port Module	The port's module.
Port Name	The port's name.
Port Number	The port's number.
Port Type	The type of port; for example, U_Port (universal port) or FL_Port (Fabric loop port).
Port WWN	The world wide name of the port.
Prohibited	Whether the allow/prohibit matrix is activated.
Serial #	The port's serial number.
Speed	The current port speed, in gigabits per second.
State	The port's state; for example, online or offline.
Switch Dynamic Load Sharing	Whether switch dynamic load sharing is enabled.
Switch FCS Role	Whether the Fabric Configuration Server (FCS), which is the primary point of control that manages all the switches within a fabric, is enabled.
Switch FMS mode	Whether the File Management Solution (FMS) mode is enabled.
Switch Has Certificate	Whether the switch has a certificate (true or false).
Switch IDID	Whether the switch's insistent domain ID (IDID) is enabled. If it is enabled, the IDID is the same ID that is requested during switch reboots, power cycles, CP failovers, firmware downloads, and fabric reconfiguration.
Switch in Order Delivery	Whether switch in-order delivery is enabled.
Switch IP	The switch's IP address.
Switch Port Count	The number of ports on the switch.
Switch Role	The role of the switch; for example, subordinate.

TABLE 19 Port connectivity properties (Continued)

Field	Description
Switch Routing Policy	Whether a routing policy, for example, port-based routing policy, is enabled.
Switch Secure Mode	Whether switch secure mode is enabled.
Switch Status	The operational status. There are four possible operation status values: • Up - Operation is normal. • Down - The port is down or the route to the remote destination is disabled. • Disabled - The connection has been manually disabled. • Backup Active - The backup TCP port is active due to a failover.
Switch Supplier Serial Number	The serial number of the switch supplier.
Switch Version	The switch's version number.
Tag	The tag number of the port.
Unit Type	The switch unit type.
User Port Number	The port number of the user's device.
Vendor	The hardware vendor's name.

Refreshing the port connectivity view

To obtain configuration changes that occurred since the Port Connectivity View dialog box opened, click Refresh.

Enabling a port

To enable a port from the port connectivity view, right-click the port you want to enable from the Port Connectivity View dialog box and select Disable/Enable Port > Enable.

Disabling a port

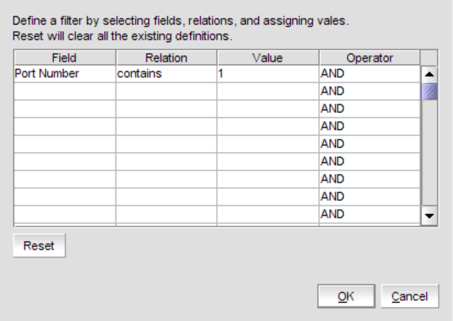
To disable a port from the port connectivity view, right-click the port you want to disable from the Port Connectivity View dialog box and select Disable/Enable Port > Disable.

Filtering port connectivity

To filter results from the port connectivity view, complete the following steps.

1. Click the **Filter** link from the **Port Connectivity View** dialog box

   The **Filter** dialog box displays (Figure 101).



Define a filter by selecting fields, relations, and assigning vales.
Reset will clear all the existing definitions.

Field	Relation	Value	Operator
Port Number	contains	1	AND
			AND
			AND
			AND
			AND
			AND
			AND
			AND
			AND

FIGURE 101 **Filter dialog box**

2. Click a blank cell in the **Field** column to select the property from which to filter the results.
3. Click a blank cell in the **Relation** column to select an action operation.

   The following actions are available:

   - ==
   - !=
   - <
   - >
   - <=
   - >=
   - contains
   - matches

4. Define a filter by entering a value that corresponds to the selected property in the **Value** column.
5. Repeat steps 2 through 4 as needed to define more filters.
6. Click **OK**.

   The **Port Connectivity View** dialog box displays. If filtering is already enabled, only those ports that meet the filter requirements display. To enable the filter, select the **Filter** check box.

Resetting the filter

Reset immediately clears all existing definitions. You cannot cancel the reset.

To reset the **Filter** dialog box, complete the following steps.

1. Click the **Filter** link from the **Port Connectivity View** dialog box.

   The **Filter** dialog box displays.

2. Click **Reset**.

   All existing definitions are cleared automatically. You cannot cancel the reset.

Enabling the filter

To enable the filter, select the **Filter** check box.

Disabling the filter

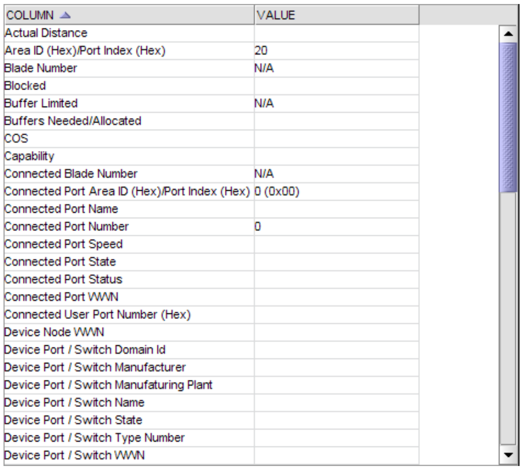
To disable the filter, clear the **Filter** check box.

Viewing port details

To view port details, complete the following steps.

1. Right-click the port for which you want to view more detailed information on the **Port Connectivity View** dialog box and select **Show Details**.

   The **Port Details** dialog box displays (Figure 102).



COLUMN ▲	VALUE
Actual Distance	
Area ID (Hex)/Port Index (Hex)	20
Blade Number	N/A
Blocked	
Buffer Limited	N/A
Buffers Needed/Allocated	
COS	
Capability	
Connected Blade Number	N/A
Connected Port Area ID (Hex)/Port Index (Hex)	0 (0x00)
Connected Port Name	
Connected Port Number	0
Connected Port Speed	
Connected Port State	
Connected Port Status	
Connected Port WWN	
Connected User Port Number (Hex)	
Device Node WWN	
Device Port / Switch Domain Id	
Device Port / Switch Manufacturer	
Device Port / Switch Manufaturing Plant	
Device Port / Switch Name	
Device Port / Switch State	
Device Port / Switch Type Number	
Device Port / Switch WWN	

FIGURE 102 Port Details dialog box

2. Review the port information.

   For the list of fields on the **Port Details** dialog box, refer to Table 20 on page 283.

3. Sort the results by clicking on the column header.

4. Rearrange the columns by dragging and dropping the column header.

5. Click the close (X) button to close this dialog box.

Viewing ports and port properties

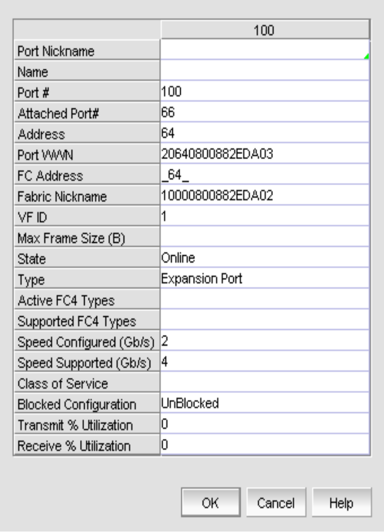
To view ports on the Connectivity Map, right-click a product icon and select **Show Ports.**

NOTE
Show Ports is not applicable when the map display layout is set to **Free Form** (default).

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.

The port **Properties** dialog box displays (Figure 103).



	100
Port Nickname	
Name	
Port #	100
Attached Port#	66
Address	64
Port WWN	20640800882EDA03
FC Address	_64_
Fabric Nickname	10000800882EDA02
VF ID	1
Max Frame Size (B)	
State	Online
Type	Expansion Port
Active FC4 Types	
Supported FC4 Types	
Speed Configured (Gb/s)	2
Speed Supported (Gb/s)	4
Class of Service	
Blocked Configuration	UnBlocked
Transmit % Utilization	0
Receive % Utilization	0

FIGURE 103 Port Properties dialog box

The following port types are available depending on the selected device:

- FC Ports
- GigE Ports
- IP Ports
- iSCSI Ports

NOTE
iSCSI ports that have an FC Address of all zeros are inactive. All others are active.

- Virtual Sessions Ports
- Virtual FCoE Ports

Depending on the port type, some of the following properties (Table 20) may not be available for all products.

TABLE 20 **Port properties**

Field	Description
# Virtual Session Ports	The number of virtual session ports associated with the GE port.
Additional Port Info	Additional error information relating to the selected port.
Address	The address of the port.
Active FC4 Types	The active FC4 types.
Active Tunnels	The number of active tunnels.
Area ID (hex)/Port Index (hex)	The area identifier, in hexadecimal, of the switch-to-product connection.
Associated GE Port	The port number of the associated GE port.
Attached Port #	The port number of the attached product.
Blocked	The configuration of the switch (blocked or unblocked).
Buffers Desired	The number of buffers desired but not allocated.
Buffers Allocated	The number of buffers allocated.
Class	The class of the port.
Class of Service	The class of service.
Connected Devices	The number of connected devices. Click the icon in the right side of the field to open the **Virtual FCoE Port <Number> Connected Devices** dialog box.
Connected Switch	The name of the connected switch.
Delete button	Click to delete.
Device Type	Whether the device is an initiator or target.
Distance Actual (km)	The actual distance (in km) for -end port connectivity.
Distance Estimated (km)	The estimated distance (in km) for -end port connectivity.
Fabric	The fabric’s IP address.
Fabric Name	The name of the fabric.
FCIP Capable	Whether the port is FCIP capable.
FC Port Count	The number of FC ports on the device.
Flag (FICON related)	Whether a flag is on or off.
GigE Port Count	The number of GigE ports on the device.
Inband Management Status	The inband management status (online or offline).
Index	The index of the Virtual FCoE Port.
Interface Count	The interface count.
iSCSI button	Click to launch the Element Manager.
iSCSI Capable	Whether the port is iSCSI capable or not.
Locked Port Type	The port type of the locked product.
Long Distance Setting	Whether the connection is considered to be normal or longer distance.

TABLE 20 Port properties (Continued)

Field	Description
MAC Address	The Media Access Control address assigned to a network adapters or network interface cards (NICs).
Manufacturer Plant	The name of the manufacturer plant.
Modify button	Click to launch the Element Manager.
Model	The model number of the device.
Name	The name of the port (up to 128 characters). This field is editable.
Performance list	Select to launch the dialog box of one of the following performance options: • Real Time Graph • HIstorical Graph • HIstorical Report
Physical/Logical	Whether the port is a physical port or a logical port.
Port Address	The address of the port.
Port #	The number of the port.
Port ID	The identifier of the port.
Port Module	The port’s module.
Port NPIV	Number of NPIV ports.
Port Speed (Gb/s)	The port speed, in Gbits per second.
Port State	The port state (online or offline).
Port Status	The port’s operational status (online or offline).
Port WWN	The port’s world wide name.
Prohibited	Whether the port is prohibited.
Protocol	The network protocol, for example, Fibre Channel.
Serial #	The hardware serial number.
Slot #	The location (slot) of the port.
Speed (Gb/s)	The port speed, in Gbits per second.
State	The port state (online or offline).
Status	The port’s operational status (online or offline).
Switch	The name of the switch.
Symbolic Name	The symbolic name of the port.
Tag	The tag number of the port.
Troubleshooting list	Select to launch the dialog box of one of the following troubleshooting options: • IP Ping • IP Traceroute • IP Performance
Type	The type of port, for example, U_port.
Tunnel Count	The number of tunnels.
User Port #	The number of the user port.

TABLE 20 Port properties (Continued)

Field	Description
Vendor	The product vendor.
Virtual FCoE Port Count	The number of FC ports on the device.

Port types

On the Connectivity 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 not applicable when the map display layout is set to Free Form (default).

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 21 Port types

Port Type	Description
D	A port in diagnostic mode.
E	An expansion port connecting two Fibre Channel switches.
EX	On a Fibre Channel Router, a connection between a fibre channel router and a fibre channel switch
F	On a Fibre Channel switch, a port that supports an N_Port.
FL	An N_port or F_port that supports arbitrated loop functions associated with arbitrated loop topology.
VE	A virtual E_port configured for an FCIP Tunnel.
VEX	A virtual EX_port configured in an FCIP Tunnel.

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 Show 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.

Viewing port connection properties

You can view the information about products and ports on both sides of the connection.

1. Right-click the connection between two end devices on the Connectivity Map and select **Properties**.

   OR

   Double-click the connection between two devices on the Connectivity Map.

   The **Connection Properties** dialog box displays.

   NOTE
   If one of the devices is in an unknown state, the Product 1 and Product 2 information displays; however, the **Connections** table information does not display.

2. Review the following information:
   - Product properties for both devices.
   - Connection properties.
   - Selected connection port properties.

   Depending on the device type at either end of the connection, some of the following fields (Table 22) may not be available for all products.

TABLE 22 Port connection properties

Field	Description
Product Properties table	The product information for the two connected switches.
Domain ID	The domain ID of the selected switch and product in xxs(yy) format, where *xx* is the normalized value and *yy* is the actual value.
Fabric Name	The world wide name of the fabric.
IP Address	The IP address of the switch.
Name	The name of the switch.
WWN	The world wide name of the switch.
Connections table	One row for each circuit.
1-Port #	The port number of the first switch.
1-Port Type	The port type of the first switch.
1-WWPN	The world wide port number of the first switch.
1-MAC Address	The media access control (MAC) address of the first switch.
1-IP Address	The IP address of the first switch.
1-Speed (Gbps)	The speed of the first switch.
1-Trunk	Whether there is a trunk on the first switch.
1-Tunnel ID	The tunnel ID of the first switch.
1-Circuit ID	The circuit ID of the first switch.
2-Port #	The port number of the second switch.
2-Port Type	The port type of the second switch.

TABLE 22 Port connection properties (Continued)

Field	Description
2-WWPN	The world wide port number of the second switch.
2-MAC Address	The MAC address of the second switch.
2-IP Address	The IP address of the second switch.
2-Trunk	Whether there is a trunk on the second switch.
2-Speed (Gbps)	The speed of the second switch.
2-Tunnel ID	The tunnel ID of the second switch.
2-Circuit ID	The circuit ID of the second switch.
Selected Connection Properties table	The connected device port information.
Area ID (hex)/Port Index (hex)	The area identifier, in hexadecimal, of the switch-to-product connection.
Blocked	The configuration of the switch (blocked or unblocked).
Buffers Allocated	The number of buffers allocated.
Buffers Desired	The number of buffers required but not allocated.
Circuits	The circuit number of the connected switch.
Connected Switch	The name of the connected switch.
Cost	The cost of the ISL link.
Distance Actual (km)	The actual distance (in km) for -end port connectivity.
Distance Estimated (km)	The estimated distance (in km) for -end port connectivity.
ED TOV	The Error Detect timeout value, in milliseconds, of the connected switch. This variable is used to flag a potential error condition when an unexpected response is not received.
Fabric	The fabric name.
FC Address	The Fibre Channel (FC) address of the switch.
FC Port #	The FC port number of the switch.
FCIP Capable	Whether the switch is FCIP capable or not.
Flag (FICON related)	Whether a FICON-related flag is on or off.
GE Port #	The GE port number of the switch.
InBand Management State	Whether inband management is enabled or disabled.
iSCSI Capable	Whether the switch is iSCSI capable or not.
L2 Mode	Whether the switch is in L2 mode or not.
LAG ID	The LAG identifier.
Locked Port Type	The port type of the locked product.
Long Distance Setting	Whether the connection is considered to be normal or longer distance.
MAC Address	The MAC address of the switch.
Manufacturer	The name of the manufacturer.
Manufacturer Plant	The name of the manufacturing plant.

TABLE 22 Port connection properties (Continued)

Field	Description
Name	The name of the switch.
NPIV Enabled	Whether the NPIV port is enabled.
Parameter	The parameter of the switch.
Physical/Logical	Whether the port is a physical port or a logical port.
PID Format	The port ID format of the switch.
Port #	The port number.
Port Address	The address of the port.
Port Module	The port’s module.
Port NPIV	The number of NPIV ports.
Port Type	The type of port.
Port State	Whether the port is online or offline.
Port Status	Whether the port is enabled or disabled.
Prohibited	Whether the port is prohibited.
Protocol	The network protocol, for example, Fibre Channel.
RA TOV	The resource allocation time out value, in milliseconds, of the connected switch. This variable works with the E D TOV variable to determine switch actions when presented with an error condition.
Sequence #	The sequence number of the switch.
Serial #	The serial number of the switch.
Slot #	The slot number of the switch.
Speed (Gb/s)	The speed in gigabytes per second.
State	The operational status of the port.
Status	The operational status of the switch
Switch	The switch name.
Tag	The tag number of the switch.
Trunking Enabled	Whether trunking is enabled on the switch.
Tunnel Count	The number of tunnels on the switch.
Tunnel ID	The tunnel ID number of the switch.
User Port #	The user port number of the switch.
VLAN ID	The VLAN identifier.
VPWWN State	Whether the VPWWN state is enabled or disabled.
VPWWN Type	The VPWWN type: Auto or User.
Auto VPWWN	The automatically generated VPWWN.
User VPWWN	The user-defined VPWWN.

3. Click **Close** to close the dialog box.

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. Select View All, Levels, and then Ports Only from the main window.
2. Use the scroll bar to view the columns to the right and locate the FC Address column in the Ports Only list.
3. Click the column label to sort the column in ascending order, if needed.

   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 Connectivity Map or the Product List. On the Connectivity Map, right-click on the product whose ports you want to view and select Show Ports.

To determine a port's status through the Product List, scroll down the Product List to the product whose ports you want to see and click the added icon (⊕).

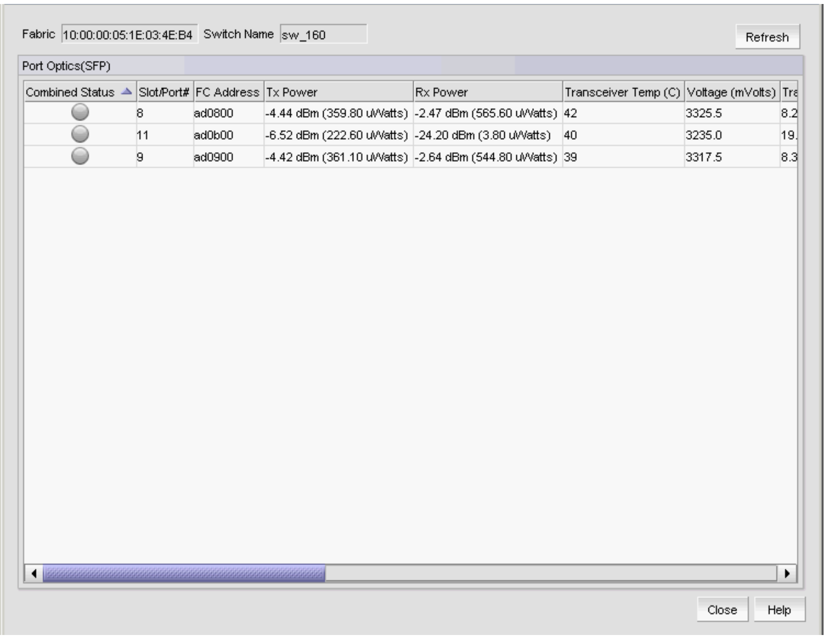
Viewing port optics

NOTE
QSFP ports do not display in the **Port Optics** dialog box.

To view port optics, complete the following steps.

1. Right-click the switch for which you want to view port optic information on the Connectivity Map and select **Port Optics (SFP)**.

   The **Port Optics (SFP)** dialog box displays(Figure 104).



Fabric 10:00:00:05:1E:03:4E:B4 Switch Name sw_160

Port Optics(SFP)

Combined Status	Slot/Port#	FC Address	Tx Power	Rx Power	Transceiver Temp (C)	Voltage (mVolts)	Tra
●	8	ad0800	-4.44 dBm (359.80 uWatts)	-2.47 dBm (565.60 uWatts)	42	3325.5	8.2
●	11	ad0b00	-6.52 dBm (222.60 uWatts)	-24.20 dBm (3.80 uWatts)	40	3235.0	19.
●	9	ad0900	-4.42 dBm (361.10 uWatts)	-2.64 dBm (544.80 uWatts)	39	3317.5	8.3

FIGURE 104 **Port Optics dialog box**

2. Review the port optics information.

   - **Combined Status**—Displays the current status of the port.

     NOTE
     Requires a 16 Gbps capable port running Fabric OS 7.0 or later.

     NOTE
     The device must have a Fabric Watch license and threshold monitoring configured for the port. For more information, refer to the Fabric Watch Administrator’s Guide.

     If the port is online and port monitoring is active, displays the current status of the port based on these five parameters: **Transceiver Temp (C)**, **Rx Power**, **Tx Power**, **Transceiver Current (mAmps)**, and **Voltage (mVolts)**.

     If the port is offline, displays the current status of the port based on these two parameters: **Transceiver Temp (C)** and **Voltage (mVolts)**.

Status icons:

- Warning icon—One of the five parameters exceeds the threshold of that parameter. The corresponding parameter field displays with a yellow background.
- No icon—No parameters exceed the threshold of that parameter.
- Unknown icon—The port is not a 16 Gbps capable port or the device is running Fabric OS 6.4.X or earlier.
- Error icon—Unable to retrieve status of the supported port.

- Slot/Port #—The slot and port number of the selected fabric.
- FC Address—The Fibre Channel address of the port.
- TX Power—The power transmitted to the SFP in dBm and uWatts.

NOTE
The uWatts display requires devices with Fabric OS 6.1.0 and later. Devices running Fabric OS 6.0.0 and earlier only display dBm.

- RX Power—The power received from the port in dBm and uWatts.

NOTE
The uWatts display requires devices with Fabric OS 6.1.0 and later. Devices running Fabric OS 6.0.0 and earlier only display dBm.

- Transceiver Temp (C)—The temperature of the SFP transceiver.
- Voltage (mVolts)—The voltage across the port in mVolts.
- Transceiver Current (mAmps)—The laser bias current value in mAmps.
- Powered on Years (Hours)—The powered on time in years and hours for 16 Gbps capable ports. Empty for unsupported ports.

NOTE
Requires a 16 Gbps capable port running Fabric OS 7.0 or later.

- FC Speed (GB/s) (Fabric OS 7.0 or later)—The FC port speed; for example, 4 Gbps.
- FC Speed (MB/s) (Fabric OS 6.4 or earlier)—The FC port speed; for example, 400 Mbps.
- Distance—The length of the fiber optic cable.
- Vendor—The vendor of the SFP.
- Vendor OUI—The vendor’s organizational unique identifier (OUI).
- Vendor PN—The part number of the SFP.
- Vendor Rev—The revision number of the SFP.
- Serial #—The serial number of the SFP.
- Data Code—The data code.
- Media Form Factor—The type of media for the transceiver; for example, single mode.
- Connector—The type of port connector.
- Wave Length—The wave length.
- Encoding—Displays how the fiber optic cable is encoded.

3. Sort the results by clicking on the column header.
4. Rearrange the columns by dragging and dropping the column header.
5. Click **Close** to close the **Port Optics (SFP)** dialog box.

Refreshing port optics

To refresh port optics, click **Refresh**.

The Management application retrieves updated port optic information.

Port Auto Disable

The **Port Auto Disable** dialog box allows you to enable and disable the port auto disable flag on individual FC_ports or on all ports on a selected device, as well as unblock currently blocked ports. Enabling the port auto disable on a port or device configures a port to become blocked when any of the following five events occur:

- Loss Of Sync
- Loss OF Signal
- OLS (Offline Primitive Sequence)
- NOS (Not Operational Primitive Sequence)
- LIP (Loop Initialization Primitive Sequence)

NOTE
To enable or disable the port auto disable flag, the device must be running Fabric OS 6.3 or later.

You can also configure ports to become blocked when one or more of the events listed above occur.

NOTE
To configure the specific events that trigger the port auto disable flag, the device must be running Fabric OS 7.0 or later.

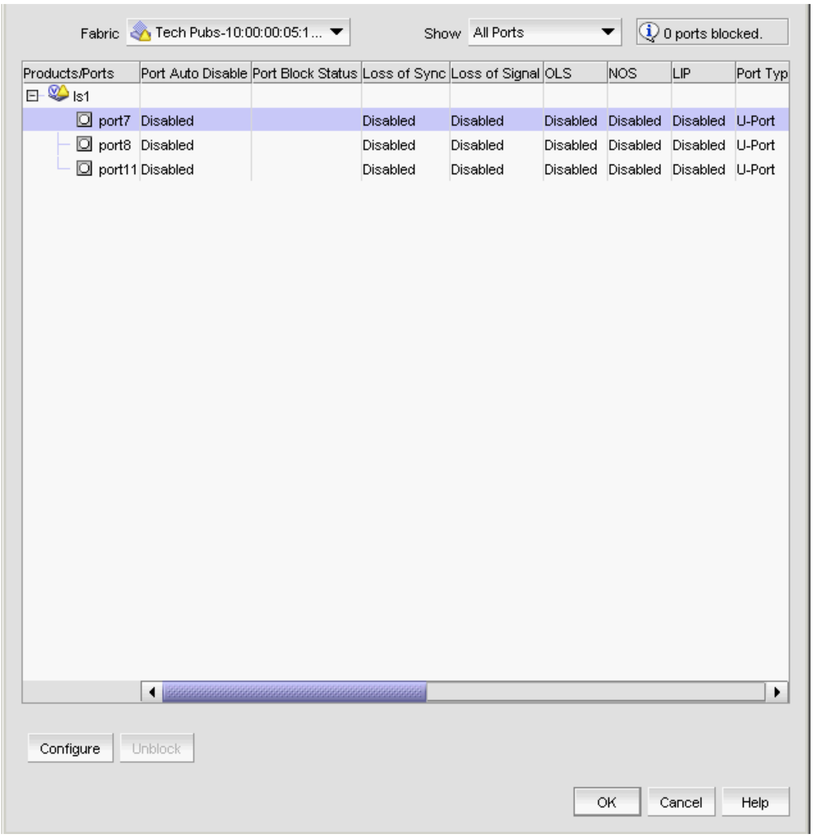
Viewing the port auto disable status

NOTE
The device must be running Fabric OS 6.3 or later.

To view the port auto disable status, complete the following steps.

1. Select **Configure** > **Port Auto Disable.**

   The **Port Auto Disable** dialog box displays.



Fabric Tech Pubs-10:00:00:05:1...

Show All Ports

0 ports blocked.

Products/Ports	Port Auto Disable	Port Block Status	Loss of Sync	Loss of Signal	OLS	NOS	LIP	Port Typ
ls1								
port7	Disabled		Disabled	Disabled	Disabled	Disabled	Disabled	U-Port
port8	Disabled		Disabled	Disabled	Disabled	Disabled	Disabled	U-Port
port11	Disabled		Disabled	Disabled	Disabled	Disabled	Disabled	U-Port

FIGURE 105 Port Auto Disable dialog box

2. Select one of the followingfrom the **Show** list to determine what ports to display:

   - **All Ports** (default)
   - **Disabled PAD Ports**
   - **Enabled PAD Ports**
   - **Blocked Ports**

3. Review the port status and other information:

   - **Products/Ports** tree—Displays devices and associated ports. Also, displays a Warning icon for blocked FC ports (displayed with the port icon).
   - **Port Auto Disable**—Displays whether Port Auto Disable is currently enabled or disabled.
   - **Port Block Status**—Displays whether the port is currently blocked.

- Loss of Sync—Whether the Loss of Sync event is enabled or disabled in port auto disable.
- Loss of Signal—Whether the Loss of Signal event is enabled or disabled in port auto disable.
- OLS—Whether the Offline Primitive Sequence event is enabled or disabled in port auto disable.
- NOS—Whether the Not Operational Primitive Sequence event is enabled or disabled in port auto disable.
- LIP—Whether the Loop Initialization Primitive Sequence event is enabled or disabled in port auto disable.
- Port Type—Displays the port type.
- Port Number—Displays the port number.
- Port WWN—Displays the port world wide name.
- Port Name—Displays the port name.
- User Port #—Displays the user port number.
- PID—Displays the port identifier.
- Connected Port #—Displays the connected port number.
- Connected Port WWN—Displays the connected port world wide name.
- Connected Port Name—Displays the connected port name.

4. Click OK on the Port Auto Disable dialog box.

Configuring port auto disable triggers

NOTE
The device must be running Fabric OS 7.0 or later.

You can configure a port to become blocked when one or more of the following events occur on the configured port:

- Loss Of Sync
- Loss OF Signal
- OLS (Offline Primitive Sequence)
- NOS (Not Operational Primitive Sequence)
- LIP (Loop Initialization Primitive Sequence)

To configure the port auto disable events, complete the following steps.

1. Select Configure > Port Auto Disable.

   The Port Auto Disable dialog box displays.

2. Select the fabric on which you want to enable port auto disable (PAD) from the Fabric list.
3. Select All Ports from the Show list to filter the port list:
4. Select one or more ports or devices on which you want to enable PAD.
5. Click Configure.

   The Configure Port Auto Disable dialog box displays.

6. Select one or more of the following event types:
   - **Port Auto Disable**
   - **Loss Of Sync**—Requires devices running Fabric OS 7.0 or later.
   - **Loss Of Signal**—Requires devices running Fabric OS 7.0 or later.
   - **OLS** (Offline Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
   - **NOS** (Not Operational Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
   - **LIP** (Loop Initialization Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
7. Click **OK** on the **Configure Port Auto Disable** dialog box.
8. Click **OK** on the **Port Auto Disable** dialog box.

Enabling port auto disable on individual ports

NOTE
The device must be running Fabric OS 6.3 or later.

To enable port auto disable on individual ports, complete the following steps.

1. Select **Configure** > **Port Auto Disable.**

   The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Choose one of the following options from the **Show** list to filter the port list:
   - **All Ports** (default)—Displays all ports in the fabric.
   - **Disabled PAD**—Displays only ports where PAD is disabled.
4. Select the ports on which you want to enable PAD.
5. Click **Configure**.

   The **Configure Port Auto Disable** dialog box displays.
6. Select one or more of the following event types:
   - **Port Auto Disable**
   - **Loss Of Sync**—Requires devices running Fabric OS 7.0 or later.
   - **Loss Of Signal**—Requires devices running Fabric OS 7.0 or later.
   - **OLS** (Offline Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
   - **NOS** (Not Operational Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
   - **LIP** (Loop Initialization Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
7. Click **OK** on the **Configure Port Auto Disable** dialog box.
8. Click **OK** on the **Port Auto Disable** dialog box.

Enabling port auto disable on all ports on a device

NOTE
The device must be running Fabric OS 6.3 or later.

To enable port auto disable on all ports on a device, complete the following steps.

1. Select **Configure > Port Auto Disable**.

   The **Port Auto Disable** dialog box displays.

2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Select **All Ports** from the **Show** list.
4. Select the device on which you want to enable PAD on all ports.
5. Click **Configure**.

   The **Configure Port Auto Disable** dialog box displays.

6. Select one or more of the following event types:
   - **Port Auto Disable**
   - **Loss Of Sync**—Requires devices running Fabric OS 7.0 or later.
   - **Loss Of Signal**—Requires devices running Fabric OS 7.0 or later.
   - **OLS** (Offline Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
   - **NOS** (Not Operational Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
   - **LIP** (Loop Initialization Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
7. Click **OK** on the **Configure Port Auto Disable** dialog box.
8. Click **OK** on the **Port Auto Disable** dialog box.

Disabling port auto disable on individual ports

NOTE
The device must be running Fabric OS 6.3 or later.

To disable port auto disable on individual ports, complete the following steps.

1. Select **Configure > Port Auto Disable**.

   The **Port Auto Disable** dialog box displays.

2. Select the fabric on which you want to disable port auto disable (PAD) from the **Fabric** list.
3. Choose one of the following options from the **Show** list to filter the port list:
   - **All Ports** (default)—Displays all ports in the fabric.
   - **Enabled PAD**—Displays only ports where PAD is enabled.
4. Select the ports on which you want to disable PAD.
5. Click **Configure**.

   The **Configure Port Auto Disable** dialog box displays.

6. Clear any of the following selected event types.
    - **Port Auto Disable**
    - **Loss Of Sync**—Requires devices running Fabric OS 7.0 or later.
    - **Loss Of Signal**—Requires devices running Fabric OS 7.0 or later.
    - **OLS** (Offline Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
    - **NOS** (Not Operational Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
    - **LIP** (Loop Initialization Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
7. Click **OK** on the **Configure Port Auto Disable** dialog box.
8. Click **OK** on the **Port Auto Disable** dialog box.

Disabling port auto disable on all ports on a device

NOTE
The device must be running Fabric OS 6.3 or later.

To disable port auto disable on all ports on a device, complete the following steps.

1. Select **Configure > Port Auto Disable.**

    The **Port Auto Disable** dialog box displays.
2. Select the fabric on which you want to disable port auto disable (PAD) from the **Fabric** list.
3. Select **All Ports** from the **Show** list.
4. Select the device on which you want to disable PAD on all ports.
5. Click **Configure**.

    The **Configure Port Auto Disable** dialog box displays.
6. Clear any of the following selected event types.
    - **Port Auto Disable**
    - **Loss Of Sync**—Requires devices running Fabric OS 7.0 or later.
    - **Loss Of Signal**—Requires devices running Fabric OS 7.0 or later.
    - **OLS** (Offline Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
    - **NOS** (Not Operational Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
    - **LIP** (Loop Initialization Primitive Sequence)—Requires devices running Fabric OS 7.0 or later.
7. Click **OK** on the **Configure Port Auto Disable** dialog box.
8. Click **OK** on the **Port Auto Disable** dialog box.

Unblocking ports

NOTE
The device must be running Fabric OS 6.3 or later.

To unblock ports, complete the following steps.

1. Select **Configure > Port Auto Disable.**

   The **Port Auto Disable** dialog box displays.

2. Select the fabric on which you want to enable port auto disable (PAD) from the **Fabric** list.
3. Select **Blocked Ports** from the **Show** list.
4. Click **Unblock.**
5. Click **OK** on the **Port Auto Disable** dialog box.

Chapter

Host Port Mapping 12

In this chapter

Host port mapping overview

HBAs and Hosts discovered through a fabric can be easily identified in the topology by their product icons. For a list of products and their icons, refer to “SAN product icons” on page 18. Once identified in the topology, you can create Hosts and assign the HBAs to them and import an externally created Host port mapping file (.CSV) to the Management application.

NOTE
The Management application now enables you to map HBAs from multiple fabrics (previous versions limited HBA mapping to one fabric).

The Management application also enables you to discover Hosts directly using Host discovery (for step-by-step instructions, refer to “Host discovery” on page 70). If you discover a Host directly, when you open the **Host Port Mapping** dialog box the Management application automatically groups all HBAs under the discovered Host.

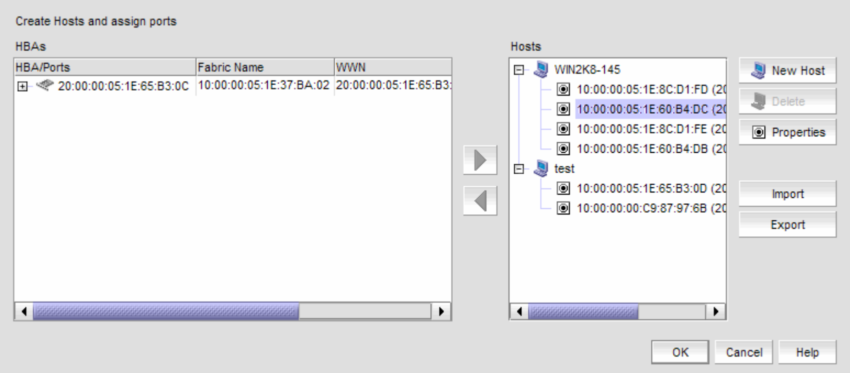
If you create a new Host and associate HBAs to it, then you try to discover a Host with the same HBAs using Host discovery, the HBA’s discovered using Host discovery must match the HBAs associated to the Host exactly; otherwise, Host discovery will fail.

Creating a new Host

To create a new Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

   The **Host Port Mapping** dialog box displays.



Create Hosts and assign ports

HBAs

HBA/Ports	Fabric Name	WWN
20:00:00:05:1E:65:B3:0C	10:00:00:05:1E:37:BA:02	20:00:00:05:1E:65:B3:

Hosts

```
WIN2K8-145
    10:00:00:05:1E:8C:D1:FD (2(
    10:00:00:05:1E:60:B4:DC (2(
    10:00:00:05:1E:8C:D1:FE (2(
    10:00:00:05:1E:60:B4:DB (2(
test
    10:00:00:05:1E:65:B3:0D (2(
    10:00:00:00:C9:87:97:6B (2(
```

FIGURE 106 Host Port Mapping dialog box

2. Click **New Host**.

   A new Host displays in the **Hosts** table in edit mode.

3. Double-click the new Host name to make it editable, type a name for the new Host, and press **Enter**.

   The name of the new Host appears in the **Hosts** table in alphabetical order. To assign HBAs to this Host, refer to "Associating an HBA with a Host" on page 301.

4. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

Renaming an HBA Host

To rename a Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

   The **Host Port Mapping** dialog box displays.

2. Click the Host you want to rename in the **Hosts** table, wait a moment, and then click it again.

   The Host displays in edit mode.

3. Type a new name for the Host.

   The name of the Host appears in the **Hosts** table in alphabetical order with the new name. To assign HBAs to this Host, refer to "Associating an HBA with a Host" on page 301.

4. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

Deleting an HBA Host

To delete a Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

   The **Host Port Mapping** dialog box displays.

2. Select the Host you want to delete in the **Hosts** table.
3. Click **Delete**.

   The selected Host is deleted. Any HBAs associated with the Host are automatically moved from the **Host** table to the **HBAs** table.

4. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

Viewing Host properties

To view Host properties, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

   The **Host Port Mapping** dialog box displays.

2. Select the HBA Host port you want to view in the **Hosts** table.
3. Click **Properties**.

   The **Properties** dialog box for the selected port displays.

4. Click **OK** to close the **Properties** dialog box.
5. Click **OK** to close the **Host Port Mapping** dialog box.

Associating an HBA with a Host

ATTENTION
Discovered information overwrites your user settings.

To associate an HBA with a Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

   The **Host Port Mapping** dialog box displays.

2. Select the Host to which you want to assign HBAs in the **Hosts** table or click **New Host** to create a new Host.
3. Select the HBA from the **HBAs** table on the left and click the right arrow.

   The HBA displays in the **Hosts** table. The HBA is now associated with the selected Host.

4. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

   On the Connectivity Map, the HBA displays in the Host.

Importing HBA-to-Host mapping

The **Host Port Mapping** dialog box enables you to import externally created HBA ports-to-Host mapping information into the application. The imported file must be in CSV format. The first row must contain the headers (wwn, name) for the file.

Example

```
wwn,name
20:00:00:00:C9:69:D5:27, s1
20:00:00:05:1E:0A:35:0E, s2
```

When the import is complete a result summary displays with the information listed in Table 23.

TABLE 23 Import Results

Value	Definition
Total Valid Input Records	Number of lines identified in the CSV file without any errors (excluding the Header).
Unique HBA WWNs Recognized	Number of unique HBAs identified in the CSV file.
Hosts Created or Identified	Number of Hosts identified in the CSV file already discovered, and which are either online or offline but not deleted.
Conflicting HBA Mappings	Number of occurrences where you were asked to decide whether to override previously discovered information. If you select Yes to All, or No to All, each occurrence where conflict resolution occurs automatically is counted as one conflict.
Overwritten HBA Mappings	Number of times a previously discovered mapping is overwritten during the import process.
Importing Errors	Number of errors encountered during the import.
Details	Tabulates the error information with respect to the line number where it occurred.

To import Host port mapping, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

   The **Host Port Mapping** dialog box displays.

2. Click **Import**.

   The **Import** dialog box displays.

3. Browse to the file (CSV format only) you want to import.

4. Click **Open** on the **Import** dialog box.

   The file imports, reads, and applies all changes line-by-line and performs the following:

   - Checks for correct file structure and well-formed WWNs, and counts number of errors.

     If more than 5 errors occur, import fails and a 'maximum error count exceeded' message displays. Edit the Host port mapping file and try again.

   - Checks for duplicate HBAs.

     If duplicates exist, a message displays with the duplicate mappings detailed. Click **Yes** to continue. Click **No** to edit the Host port mapping file and try again.

- Checks for existing mappings in the current map.

  If a mapping already exists, a message displays with the current mapping information. Click **Yes** to overwrite the current mapping. Click **Yes to All** to overwrite all mapping conflicts. Click **No** to leave the current mapping. Click **No to All** to leave all current mappings when conflict occurs. Click **Cancel** to cancel the import.

5. Click **OK** to close the **Import Results** dialog box.
6. Click **OK** to close the **Host Port Mapping** dialog box.

Removing an HBA from a Host

To remove an HBA from a Host, complete the following steps.

1. Right-click an HBA icon and select **Host Port Mapping**.

   The **Host Port Mapping** dialog box displays.

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

   The HBA you selected is removed from the **Hosts** table and the HBA is no longer associated with the Host.

3. Click **OK** to save your changes and close the **Host Port Mapping** dialog box.

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

Exporting Host port mapping

The **Host Port Mapping** dialog box enables you to export a Host port. The export file uses the CSV format. The first row contains the headers (HBA/Ports WWN, Host Name) and the switch to which the port is connected.

Example

```
HBA World Wide Name, Host Name
5005076717011E7D, Server1
50050767170A5AAF, Server1
```

To export a Host port, complete the following steps.

1. Open the **Host Port Mapping** dialog box by performing one of the following actions:
   - Select an HBA port icon in the topology view, then select **Discover > Host Port Mapping**.
   - Right-click any HBA port icon in the topology view and select **Host Port Mapping**.
   - Right-click any HBA port in the Device Tree and select **Host Port Mapping**.

     The **Host Port Mapping** dialog box displays.

2. Select the Host port you want to export from the **HBA/Ports** list.

   To configure Host port mapping, refer to “Creating a new Host” on page 300 and “Associating an HBA with a Host” on page 301.

3. Click **Export**.

   The **Export** dialog box displays.

4. Browse to the location where you want to save the export file.

   Depending on your operating system, the default export location are as follows:

   - Desktop\My documents (Windows)
   - \root (Linux)

5. Enter a name for the files and click **Save**.
6. Click **OK** to close the **Host Port Mapping** dialog box.

Chapter

Storage Port Mapping 13

In this chapter

Storage port mapping overview

The Management 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 Management application cannot see the relationship between ports attached to the same storage device. Therefore, the Management application allows you to manually associate the connections that the system is unable to make.

The Management 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.

NOTE
When you open the **Storage Port Mapping** dialog box, Discovery is automatically turned off. When you close the **Storage Port Mapping** dialog box, Discovery automatically restarts.

During Discovery, if a previously mapped Storage Port is found to have a relationship with a port just discovered, the Management 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 Management 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.

Creating a storage array

To create a storage array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
   - 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 **New Storage**.

   A new storage array displays in the **Storage Array** list in edit mode.
3. Rename the new storage array and press **Enter**.
4. Add storage ports to the new storage array.

   NOTE
   You must add at least one storage ports to the new storage array to save the new array in the system.

   For step-by-step instructions about adding ports to an array, refer to "Adding storage ports to a storage array" on page 306.
5. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

Adding storage ports to a storage array

To add storage ports to a storage array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
   - 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 Ports** table.

   To select more than one port, hold down the **CTRL** key while selecting multiple storage ports.
3. Select the storage array to which you want to assign the storage port in the **Storage Array** list.
4. Click the right arrow.

   The storage port is added to the Storage Array.
5. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

Unassigning a storage port from a storage array

To unassign a storage port from a storage array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
   - 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 port you want to unassign from the **Storage Array** list.
3. Click the left arrow button.

   The selected storage port is removed from the **Storage Array** list and added to the **Storage Ports** table.
4. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

Reassigning mapped storage ports

To reassign a storage port, complete the following steps.

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 port you want to unassign from the **Storage Array** list.
3. Click the left arrow button.

   The selected storage port is removed from the **Storage Array** list and added to the **Storage Ports** table.
4. Make sure the storage port you want to reassign is still selected.
5. Select the storage array to which you want to reassign the storage port in the **Storage Array** list.
6. Click the right arrow button.

   The storage port moves from the **Storage Ports** table to the selected storage array.
7. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

Editing storage array properties

To edit storage array properties, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
   - 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.**

   The **Properties** dialog box appears.
3. Edit the property fields, as needed.

   Depending on which tab you select (Properties tab, Storage tab, Port tab), different fields will be available for editing. Editable fields have a green triangle in the lower right corner of the field.
4. Click **OK** on the **Properties** dialog box to save the storage array properties.
5. Click **OK** to save your work and close the **Storage Port Mapping** dialog box.

Deleting a storage array

To delete a storage array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
   - 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 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** to save your work and close the **Storage Port Mapping** dialog box.

Viewing storage port properties

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
   - 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

To view storage array properties, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
   - 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.**

   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.

Importing storage port mapping

The **Storage Port Mapping** dialog box enables you to import externally created storage port mapping information into the application. The imported file must be in CSV format. The first row must contain the headers (wwn, name) for the file, which is ignored during the import.

Example

```
wwn,name
20:00:00:04:CF:BD:89:6E,name1
20:00:00:04:CF:BD:6F:32,name2
20:00:00:04:CF:BD:70:2F,name1
20:00:00:04:CF:BD:6F:52,name2
```

To import storage port mapping, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:

   - 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 **Import.**

   The **Import** dialog box displays.

3. Browse to the file (CSV format only) you want to import.

4. Click **Open** on the **Import** dialog box.

   The file imports, reads, and applies all changes line-by-line and performs the following:

   - Checks for correct file structure (first entry must be the storage node name (WWN) and second entry must be the storage array name), well formed WWNs, and counts number of errors

     If more than 5 errors occur, import automatically cancels. Edit the storage port mapping file and try again.

   - Checks for duplicate storage ports (the same storage port mapped to more than one storage array)

     If duplicates exist, a message displays with the duplicate mappings detailed. Click **Yes** to continue. Click **No** to edit the storage port mapping file and try again.

   - Checks if mapping exists in current map

     If mappings already exist, a message displays with the current mapping information. Click **Yes** to overwrite the current mapping. Click **Yes to All** to overwrite all mapping conflicts. Click **No** to leave the current mapping. Click **No to All** to leave all current mappings when conflict occurs. Click **Cancel** to cancel the import.

When import is complete a result summary displays with the following information ("Import Results" on page 311).

TABLE 24 Import Results

Value	Definition
Total Valid Input Records	Number of lines identified in the CSV file without any errors (excluding the Header).
Unique storage port WWN's Recognized	Number of unique storage ports identified in the CSV file.
Storage Arrays Created or Identified	Number of storage ports identified in the CSV file already discovered and are either online or offline but not deleted.
Conflicting Port Mappings	Number of occurrences where you were asked to decide whether to override previously discovered information. If a you select Yes to All, or No to All, each occurrence where conflict resolution occurs automatically is counted as one conflict.
Overwritten Port Mappings	Number of times a previously discovered mapping is overwritten during the import process.
Importing Errors	Number of errors encountered during the import.
Details	Tabulates the error information with respect to the line number where it occurred.

5. Click **OK** to close the **Import Results** dialog box.
6. Click **OK** to close the **Storage Port Mapping** dialog box.

Exporting storage port mapping

The **Storage Port Mapping** dialog box enables you to export a storage port array. The export file uses the CSV format. The first row contains the headers (Storage Node Name (WWNN), Storage Array Name) for the file.

Example

```
Storage Node Name (WWNN), Storage Array Name
20000004CFBD7100,New Storage Array
20000004CFBD896E,New Storage Array
2000002037E19CED,New Storage Array
```

To export a storage port array, complete the following steps.

1. Open the **Storage Port Mapping** dialog box by performing one of the following actions:
   - 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 port array you want to export port from the **Storage Array** list.

3. Click **Export**.

   The **Export** dialog box displays.

4. Browse to the location where you want to save the export file.

   Depending on your operating system, the default export location are as follows:

   - Desktop\My documents (Windows)
   - \root (Linux)

5. Enter a name for the files and click **Save**.

6. Click **OK** to close the **Storage Port Mapping** dialog box.

Chapter

Host management 14

In this chapter

Host management

Extensive management operations are supported on the switches and fabrics of the SAN using the Management application. Adapters and hosts are visible as part of the fabrics managed by the Management application. The management operations that are currently available using the Management application are discussed in this chapter.

The Management application integrates with another manageability application called the Host Connectivity Manager (HCM) to provide complete management of the host bus adapters (HBAs) and converged network adapters (CNAs).

- The Management application focuses on operations such as fault management, performance management, and configuration management for multiple adapters and adapter ports and security configuration using Fibre Channel Security Protocol (FC-SP) that is set up on the adapter port and the switch.

- HCM supports management for individual adapters (1/4/8 Gbps HBAs), 10 Gbps CNAs, 16 Gbps FC adapters, and other devices, such as the host, DCB ports, FCoE ports, and Ethernet ports.

The Management application, in conjunction with HCM, provides end-to-end management capability. For information about configuring, monitoring, and managing individual adapters using the HCM GUI or the Brocade Command Utility (BCU), refer to the *Adapters Administrator's Guide*.

HCM software

The Host Connectivity Manager (HCM) is a management software application for configuring, monitoring, and troubleshooting Brocade host bus adapters (HBAs) and converged network adapters (CNAs) in a storage area network (SAN) environment.

The information in this guide is intended for OEMs, field service personnel, and customers who are installing Brocade hardware and HCM software. For instructions about how to install the HCM software, refer to the *Adapters Installation and Reference Manual.*

You can manage the software on the host or remotely from another host. The communication between the management console and the agent is managed using JSON-RPC over HTTPS.

NOTE
All HCM, utility, SMI-S Provider, boot software, and driver installation packages, as well as the Driver Update Disk (DUD), are described in the *Adapters Installation and Reference Manual*.

HCM features

Common HBA and CNA management software features include the following:

- Discovery using the agent software running on the servers attached to the SAN, which enables you to contact the devices in your SAN.
- Configuration management , which enables you to configure local and remote systems. With HCM you can configure the following items:
  - Brocade 4 Gbps and 8 Gbps HBAs
  - HBA ports (including logical ports, base ports, remote ports, and virtual ports) associated with the local host
  - Brocade 10 Gbps single-port and 10 Gbps dual-port converged network adapters (CNAs)
  - Brocade 16 Gbps FC adapters
  - DCB ports (CNA only)
  - FCoE ports (CNA only)
  - Ethernet ports (CNA only)

- Diagnostics, which enables you to test the adapters and the devices to which they are connected:
  - Link status of each adapter and its attached devices
  - Loopback test, which is external to the adapter, to evaluate the ports (transmit and receive transceivers) and the error rate on the adapter
  - Read/write buffer test, which tests the link between the adapter and its devices
  - FC protocol tests, including echo, ping, and traceroute
  - Ethernet loopback test (CNA only)
- Monitoring, which provides statistics for the SAN components.
- Security, which enables you to specify a CHAP secret and configure authentication parameters.
- Event notifications, which provide asynchronous notification of various conditions and problems through a user-defined event filter.

Host bus adapters

There are five models of Fibre Channel Host Bus Adapters (HBAs). These models provide reliable, high-performance host connectivity for mission-critical SAN environments. The Brocade HBAs are listed in Table 25.

TABLE 25 Brocade Fibre Channel HBA models

Model Number	Description	Number of Ports
825	Dual-port stand-up HBA with a per-port maximum of 8 Gbps using a 8 Gbps SFP.[1]	2
815	Single-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.[1]	1
804	Dual-port mezzanine HBA with a per-port maximum of 8 Gbps. This HBA installs in server blades that install in supported blade system enclosures.	2
425	Dual-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.[2]	2
415	Single-port stand-up HBA with a per-port maximum of 4 Gbps using a 4 Gbps SFP.[2]	1

[1] A 4 Gbps SFP installed in 815 or 825 HBAs allows 4, 2, or 1 Gbps speed only.

[2] An 8 Gbps SFP installed in 425 or 415 HBAs allows 2 or 4 Gbps speed only.

Using Brocade HBAs, you can connect your server (host system) to devices on the Fibre Channel SAN. The combined high performance and proven reliability of a single-ASIC design makes these HBAs ideal for connecting hosts to SAN fabrics based on Fabric or M-Enterprise operating systems.

Converged network adapters

Table 26 describes available Brocade Converged Network Adapters (CNAs) for PCIe x 8 host bus interfaces, hereafter referred to as Brocade CNAs. These adapters provide reliable, high-performance host connectivity for mission-critical SAN environments.

TABLE 26 Brocade Fibre Channel CNA models

Model Number	Port Speed	Number of Ports	Adapter Type
1741M	10 Gbps maximum	2	Expansion
1020	10 Gbps maximum	2	Stand-up
1010	10 Gbps maximum	1	Stand-up
1007[1]	10 Gbps maximum	2	Expansion

[1] The Brocade 1007 is a two-port CNA mezzanine or expansion card adapter that mounts on a blade server that installs in a blade system enclosure. The adapter uses FCoE to converge standard data and storage networking data onto a shared Ethernet link. Ethernet and Fibre Channel communication are routed through the DCB ports on the adapter to the blade system enclosure midplane and onto the installed switch modules installed in the enclosure.

For information on installing the Brocade 1007 CNA on a blade server, refer to the *Adapters Installation and Reference Guide*.

Brocade CNAs combine the functions of a Host Bus Adapter (HBA) and Network Interface Card (NIC) on one PCIe x8 card. The CNAs even appear as network adapters (NIC) and Fibre Channel adapters to the host. These CNAs fully support FCoE protocols and allow Fibre Channel traffic to converge onto 10 Gbps Data Center Bridging (DCB) networks. FCoE and 10 Gbps DCB operations are simultaneous.

The combined high performance and proven reliability of a single-ASIC design makes these CNAs ideal for connecting host systems on Ethernet networks to SAN fabrics based on Brocade or M-EOS.

NOTE

The Brocade 1007 and 1741M CNA expansion cards connect to the embedded switch modules or embedded interconnect modules on the Blade System chassis by way of an internal backplane and, therefore, no optical modules (SFPs) are involved. With the exception of no SFPs, the Brocade 1007 CNA expansion cards function the same as the other Brocade CNAs.

Fabric adapters

Table 27 describes available Brocade 1860 Fabric Adapter models. The BR-1860 provides dual mode support for the port.

TABLE 27 Brocade Fabric adapter models

Model Number	Port Speed	Number of Ports	Adapter Type
BR-1860-1F	16 Gbps FC HBA or 10 Gbps CNA	1	Fabric
BR-1860-2F	16 Gbps FC HBA or 10 Gbps CNA	2	Fabric
BR-1860-1P	16 Gbps FC HBA or 10 Gbps CNA	1	Fabric
BR-1860-2P	16 Gbps FC HBA and/or 10 Gbps CNA	2	Fabric

Host adapter discovery

The Management application enables you to discover individual hosts, import a group of hosts from a CSV file, or import host names from discovered fabrics. The maximum number of host discovery requests that can be accepted is 1000. Host discovery requires HCM Agent 2.0 or later. SMI and WMI discovery are not supported.

NOTE
Pure Fabric discovery alone shows adapters behind Access Gateway and all adapter ports as virtual. When you discover an adapter and ports using Host discovery, the adapter and all its ports are shown as physical.

Instructions for discovering hosts are detailed in Chapter 4, “Discovery” and include information about the following:

“Discovering Hosts by Network address or host name” on page 70

- “Importing Hosts from a CSV file” on page 72
- “Importing Hosts from a Fabric” on page 73
- “Importing Hosts from a VM manager” on page 74
- “Editing Host adapter credentials” on page 75
- “Removing a host from active discovery” on page 76
- “Viewing the host discovery state” on page 77
- “Troubleshooting host discovery” on page 77
- “VM Manager Discovery” on page 78

Connectivity map

The Connectivity Map, which displays in the upper right area of the main widow, is a grouped map that shows physical and logical connectivity of Fabric OS components, including discovered and monitored devices and connections. These components display as icons in the Connectivity Map. For a list of icons that display in the Connectivity Map, refer to the following tables in Chapter 1, "Getting Started":

- "Host product icons" on page 19
- "Host group icons" on page 20
- "SAN port icons" on page 20

The Management application displays all discovered fabrics in the Connectivity Map by default. To display a discovered Host in the Connectivity Map, you must select the Host in the Product List. You can only view one Host and physical and logical connections at a time.

View management

You can customize the topology by creating views at the managed host level in addition to the fabric level views. If you discover or import a Fabric with more than approximately 2000 devices, the devices display on the Product List, but not on the Connectivity Map. Instead, the topology area shows a message stating that the topology cannot be displayed. To resolve this issue, create a new view to filter the number of devices being discovered.

Instructions for managing customized views of the topology are detailed in Chapter 8, "View Management" and include information about the following:

- "Creating a customized view"
- "Editing a customized view"
- "Deleting a customized view"
- "Copying a view"
- "Grouping on the topology"

Host port mapping

Host bus adapters (HBAs) and hosts discovered through one or more fabrics can be easily identified in the topology by their product icons. For a list of products and their icons, refer to "Host product icons" on page 19. Once identified in the topology, you can create hosts and assign the HBAs to them and import an externally created host port mapping file (.CSV) to the Management application.

NOTE
The Management application now enables you to map HBAs from multiple fabrics (previous versions limited HBA mapping to one fabric).

The Management application also enables you to discover hosts directly using Host discovery (for step-by-step instructions, refer to "Host discovery" on page 70). If you discover a host directly, when you open the **Host Port Mapping** dialog box, the Management application automatically groups all HBAs under the host.

If you create a new Host and associate HBAs to it, and then you try to discover a host with the same HBAs using Host discovery, the HBA's discovered using host discovery must match the HBAs associated to the Host exactly; otherwise, Host discovery will fail.

Instructions for mapping a Host to HBAs are detailed in Chapter 12, "Host Port Mapping" and include information about the following:

- "Creating a new Host" on page 300
- "Renaming an HBA Host" on page 300
- "Deleting an HBA Host" on page 301
- "Viewing Host properties" on page 301
- "Associating an HBA with a Host" on page 301
- "Importing HBA-to-Host mapping" on page 302
- "Removing an HBA from a Host" on page 303
- "Exporting Host port mapping" on page 303

Adapter software

The **Adapter Software** dialog box allows you to perform the following tasks:

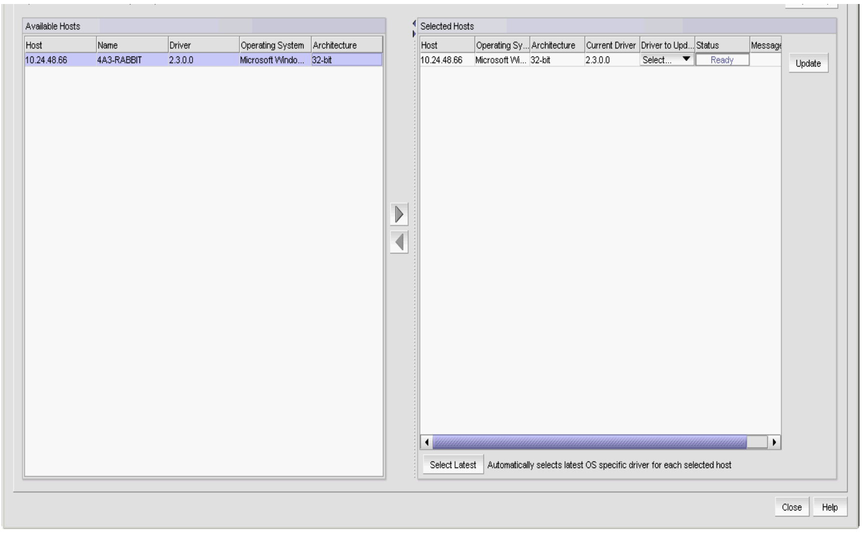
- Select and import a driver file or delete existing drivers from the driver repository
- Update the driver to the hosts.

This feature is available for hosts that are disovered through the Host Connectivity Manager (HCM) agent with driver version 2.3.0.0 and higher.

To update the drivers to selected hosts, complete the following steps:

1. Select **Host > Adapter Software** from the **Configure** menu.

   The **Adapter Software** dialog box, Driver tab, shown in Figure 107, displays.



Available Hosts

Host	Name	Driver	Operating System	Architecture
10.24.48.66	4A3-RABBIT	2.3.0.0	Microsoft Windo...	32-bit

Selected Hosts

Host	Operating Sy...	Architecture	Current Driver	Driver to Upd...	Status	Message
10.24.48.66	Microsoft Wi...	32-bit	2.3.0.0	Select...	Ready	

Automatically selects latest OS specific driver for each selected host

FIGURE 107 Adapter Software dialog box, Driver tab

2. Select one or more hosts from the **Available Hosts** list and click the right arrow button to move the selected hosts to the **Selected Hosts** list.
3. Select one or more hosts from the **Selected Hosts** list. You can select mutliple hosts, but if the selected host count is greater than 20, a batch of 20 hosts is initiated for the driver update first and the remaining hosts are queued.
4. Select the host's corresponding driver to update from the **Driver to Update** list. Once the driver has been selected for each host, click **Update** .

   Alternatively, you can select one or more hosts from the **Selected Hosts** list and click **Select Latest** to automatically select the latest operating system-specific driver for each selected host. If you want to import a driver from another location, follow the instructions in "Driver repository" on page 321.

Driver repository

You can access the Driver Repository dialog box from the **Adapter Software** dialog box. Initially, the repository is empty. You must import files into the repository. Imported driver files are then displayed in the **Available Driver Files** list in the **Driver Repository** dialog box.

Importing a driver into the repository

To import drivers into the Management application, perform the following tasks.

1. From the **Adapter Software** dialog box, click the **Repository** button.

   The **Driver Repository** dialog box, shown in Figure 108, displays.

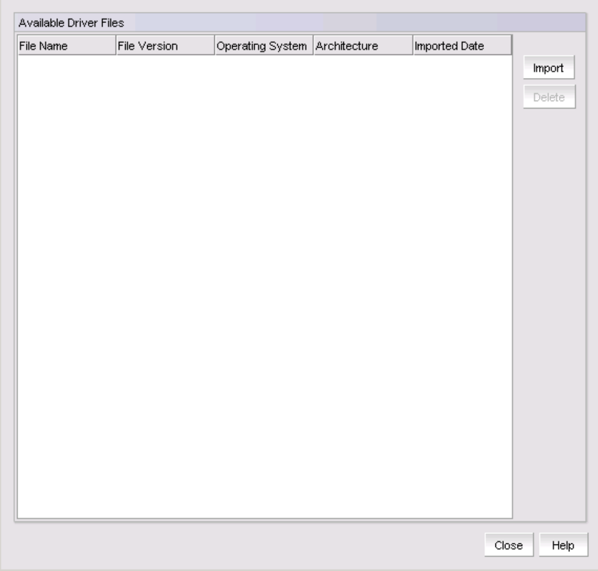


FIGURE 108 Driver Repository dialog box

2. Click **Import** on the **Driver Repository** dialog box.

   The **Import Driver Repository** dialog box displays.

3. Locate the driver file using one of the following methods:

   - Search for the file you want from the **Look In** list.
   - Enter the name of the image file you want to import in the **File Name** field.

4. Click **Open**.

   After the import completes successfully, you see a message that the boot image imported successfully.

5. Click **OK**.

Deleting a driver file from the repository

1. Select one or more driver files from the **Available Driver Files** list on the **Driver Repository** dialog box.
2. Click **Delete.**

   The driver file is removed from the Driver Repository dialog box.

NOTE
Windows drivers (.exe files) cannot be imported into the server repository when the Management application server is running on Linux or Solaris platforms.

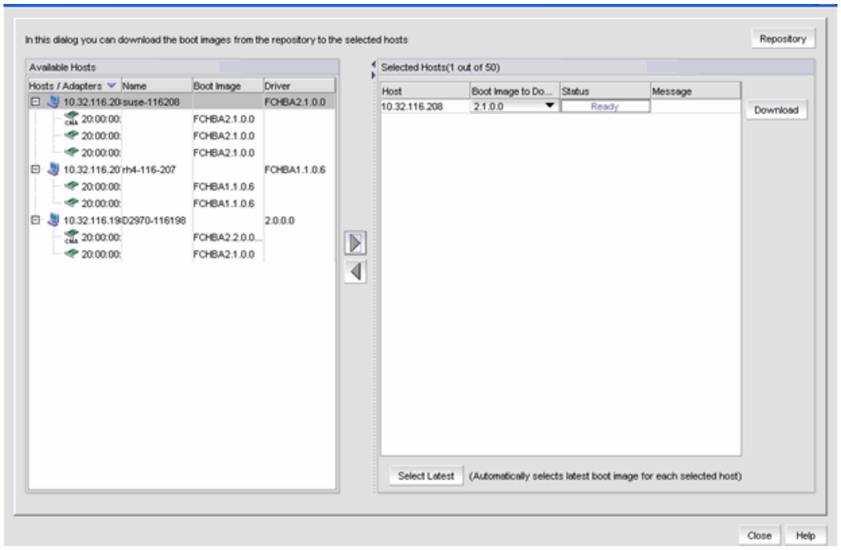
Boot Image Repository

The boot code image stored in the adapter's flash contains the instructions that enable the server to locate the boot disk in SAN. The boot code image contains basic input/output system (BIOS), extensible firmware interface (EFI), and open firmware which enable the adapters to be compatible with any system platform.

Boot images are required for adapters that are shipped without a boot image or when it is necessary to overwrite images on adapters that contain older or corrupted boot image versions.

1. From the Management application menu bar, select **Configure** > **Host** > **Adapter Software.**
2. Click the **Boot Image** tab.

   The **Boot Image Management** dialog box, shown in Figure 109, displays.



In this dialog you can download the boot images from the repository to the selected hosts

Available Hosts

Hosts / Adapters	Name	Boot Image	Driver
10.32.116.20	suse-116208		FCHBA2.1.0.0
20:00:00:		FCHBA2.1.0.0	
20:00:00:		FCHBA2.1.0.0	
20:00:00:		FCHBA2.1.0.0	
10.32.116.20	rh4-116-207		FCHBA1.1.0.6
20:00:00:		FCHBA1.1.0.6	
20:00:00:		FCHBA1.1.0.6	
10.32.116.19	D2970-116198		2.0.0.0
20:00:00:		FCHBA2.2.0.0...	
20:00:00:		FCHBA2.1.0.0	

Selected Hosts(1 out of 50)

Host	Boot Image to Do...	Status	Message
10.32.116.208	2.1.0.0	Ready	

(Automatically selects latest boot image for each selected host)

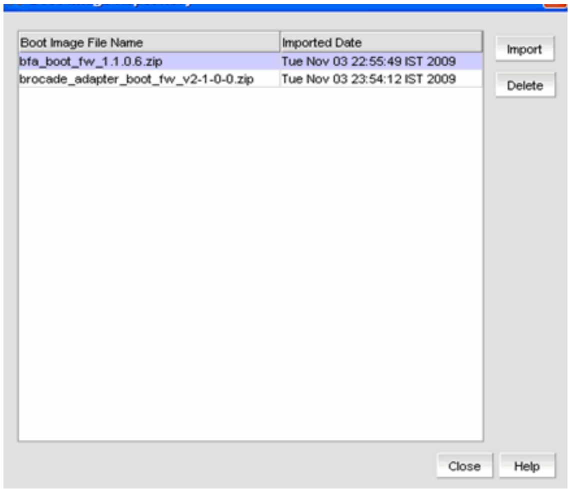
FIGURE 109 Boot Image Management dialog box

Importing a boot image into the repository

To import boot images into the Management application, perform the following tasks.

1. From the **Boot Image Management** dialog box, click the **Repository** button.

   The **Boot Image Repository** dialog box, shown in Figure 110, displays.



Boot Image File Name	Imported Date
bfa_boot_fw_1.1.0.6.zip	Tue Nov 03 22:55:49 IST 2009
brocade_adapter_boot_fw_v2-1-0-0.zip	Tue Nov 03 23:54:12 IST 2009

FIGURE 110 Boot Image Repository dialog box

2. Click **Import** on the **Boot Image Repository** dialog box.
3. The **Import Boot Image** dialog box displays.
4. Locate the boot image file using one of the following methods:
   - Search for the file you want from the **Look In** list. Boot image files version 2.0.0.0 and 2.1.0.0 are .zip files and other boot image files are tar files.
   - Enter the name of the image file you want to import in the **File Name** field.
5. Click **Open**.

   After the import completes successfully, you see a message that the boot image imported successfully.

NOTE
The boot image file is imported to *Install_Server_Home*/data/adapter_boot_images.

6. Click **OK**.

Downloading a boot image to a selected host

To download boot images to a selected host, perform the following tasks.

1. Select one or more hosts from the **Available Hosts** list on the **Boot Image Management** dialog box, and click the right arrow button to move the selected hosts to the **Selected Hosts** list.

   You can select up to 50 hosts. The first 20 hosts execute the download concurrently. If you select more than 20 hosts, they will be queued and will start when the previous download completes.

   NOTE
   The driver version of the host must be 2.0.0.0 or higher.

2. Click **Select Latest** to make sure the lastest imported boot images display in the **Boot Image to Download** list for hosts corresponding to driver installed.
3. From the **Boot Image Management** dialog box, click the **Download** button.

   One of the following download status messages displays in the **Status** column of the **Selected Hosts** list:

   - Ready
   - Queued
   - In progress
   - Failed—If the download failed, the failure reason displays in the **Message** column of the **Selected Hosts** list; for example, failed to connect to HCM agent, a checksum error occurred, or the file is invalid.
   - Finished

Deleting a boot image from the repository

1. Select one or more boot images from the **Boot Image File Name** list on the **Boot Image Repository** dialog box.
2. Click **Delete**.

   The boot image is removed from the boot image repository.

Backing up boot image files

You can back up the boot image files from the repository using the **Options** dialog box. Refer to "Backup support" on page 330 for instructions.

Role-based access control

The Management application enables you to create resource groups and assign users to the selected role within that group. This enables you to assign users to a role within the resource group.

The Management application provides one pre-configured resource group (All Fabrics). When you create a resource group, all available roles are automatically assigned to the resource group. Once the resource group is available you can assign a user to a role within the resource group.

Host adapter management privileges

You can launch the Host Connectivity Manager (HCM) if you have read and write permissions to the Host Adapter Management privilege. Other HBA-related operations are controlled by the following privileges:

- The HBA technical support launch point is controlled by the Technical Support Data Collection privilege.
- The Fibre Channel Security Protocol (FCSP) launch point is controlled by the Security privilege. Read write (RW) and read only (RO) permissions are required.
- The HBA performance monitoring launch point is controlled by the Performance privilege.

Host adapter administrator privileges

The Host Adapter Administrator role has the following privileges:

- Add and delete properties
- Discovery setup
- Host management
- Performance
- Properties edit
- Security
- Servers
- View management

Instructions for managing resource groups and users using roles and privileges are detailed in "User accounts,""Roles," and "Areas of responsibility," in "User Account Management,".

Host performance management

Real-time performance enables you to collect data from managed HBA and CNA ports. You can use real-time performance to configure the following options:

- Select the polling rate from 20 seconds up to 1 minute.
- Select up to 32 ports total from a maximum of 10 devices for graphing performance.
- Choose to display the same Y-axis range for both the Tx MB/Sec and Rx MB/Sec measure types for easier comparison of graphs.

Table 28 lists the counters that are supported for the FC ports and for the HBA and CNA ports.

TABLE 28 Counters

FC port measures	HBA port measures	CNA port measures
Tx % utilization	Tx % utilization	Tx % utilization
Rx % utilization	Rx % utilization	Rx % utilization
Tx MBps	Tx MBps	Tx MBps
Rx MBps	Rx MBps	Rx MBps
CRC errors	CRC errors	
Signal losses	Signal losses	
Sync losses	Sync losses	
Link failures	Link failures	
Sequence errors	Primitive sequence protocol errors	
Invalid transmissions		
Rx link resets		
Tx link resets		
	NOS count	
	Error frames	
	Dropped frames	
	Undersized frames	
	Oversized frames	
	Bad EOF frames	
	Invalid ordered sets	
	Non-frame coding error	
		Received paused frames
		Transmitted paused frames
		Received FCoE pause frames
		Transmitted FCoE pause frames
		Received FCS error frames
		Transmitted FCS error frames
		Received alignment error frames

TABLE 28 Counters (Continued)

FC port measures	HBA port measures	CNA port measures
		Received length error frames
		Received code error frames

Instructions for generating real-time performance data are detailed in "Generating a real-time performance graph" on page 761.

Host security authentication

Fibre Channel Security Protocol (FC-SP) is a mechanism used to secure communication between two switches or between a switch and a device such as an HBA port.

You can use either the Management application or the HCM GUI to display the authentication settings and status. When you enable FC-SP authentication using the Management application, you can also set the authentication settings on the attached 8 Gbps 8-FC port.

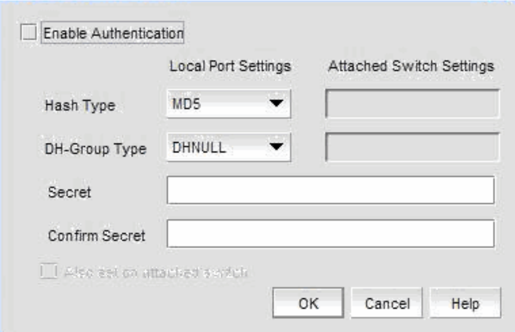
NOTE
FC-SP is only available for Brocade HBAs that are managed using the HCM agent. FC-SP is not available for virtual ports or unmanaged HBA ports. The user must have the Security privilege to use this feature.

Configuring security authentication using the Management application

Access the **Fibre Channel Security Protocol Configuration** (FCSP) dialog box by selecting an adapter port from the device tree.

1. Select the appropriate device based on how you want to configure security authentication:
2. Right-click the HCM HBA port and select the **FC Security Protocol** menu item.

   The **Fibre Channel Security Protocol Configuration** (adapter level) dialog box displays. The **Fibre Channel Security Protocol Configuration** dialog at the host level displays.



□ Enable Authentication

	Local Port Settings	Attached Switch Settings
Hash Type	MD5	
DH-Group Type	DHNULL	
Secret		
Confirm Secret		

□ Also set on attached switch

FIGURE 111 Fibre Channel Security Protocol Configuration - host level dialog box

3. Configure the following parameters on the **FCSP Authentication** dialog box:

a. Select the **Enable Authentication** check box to enable or disable the authentication policy.

   If authentication is enabled, the port attempts to negotiate with the switch. If the switch does not participate in the authentication process, the port skips the authentication process.

   The Hash type list shows the following options, but only one option, DHNULL, is supported.

   - **MD5** - A hashing algorithm that verifies a message's integrity using Message Digest version 5. MD5 produces a 128-bit digest and is the required authentication mechanism for LDAP v3 servers.
   - **SHA1** - A secure hashing algorithm that computes a 160-bit message digest for a data file that is provided as input.
   - **MD5SHA1** - Similar to the MD5 hashing algorithm, but used for DH-CHAP authentication.
   - **SHA1MD5** - Similar to the SHA1 hashing algorithm, but used for DH-CHAP authentication.

b. Select **DHNULL** as the DH-group type value.

c. Type and retype the secret.

   The length of the secret must be between eight and 41 characters and the secret field cannot be blank.

d. Select the **Also set on attached switch** check box to set or not set the CHAP secret on the attached switch.

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

   FC Security Protocol settings are also applied to the attached switch.

supportSave on adapters

Host management features support capturing support information for managed Brocade adapters, which are discovered in the Management application. You can trigger supportSave for multiple adapters at the same time.

NOTE
You cannot schedule Host supportSave information

Instructions for scheduling and capturing technical support files are detailed in Chapter 31, "Technical Support".

Host fault management

Fault management enables you to monitor your SAN using the following methods:

- Monitor logs for specified conditions and notify you or run a script when the specified condition is met.
- Create event-based policies, which contain an event trigger and action.
- Configure E-mail event notification.
- Receive and forward Syslog messages from Brocade switches and Brocade HBAs, managed using the Host Connectivity Manager (HCM).

Adapter events

You can configure triggers and actions for the following event types that are:

- Product Audit Event — occurs when a target product is audited.
- Product Status Event — occurs when a device or connection changes to Up or Down.
- Product Threshold Alert Event — notifies you when a threshold alert has been reached.

You can configure event policies for events you want to monitor. A policy is the mechanism defined by you that identifies the response to specific event types. You can customize the event management policy using triggers and actions, which are explained in "Fault Management" on page 823.

Event actions

You can create actions for events you want to monitor. A event action is the mechanism defined by you that identifies the response to specific event types. You can customize the event management policy using triggers and actions, which are explained "Event action definitions" on page 847. This section also provides information about the following topics:

Filtering event notifications

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

NOTE
The e-mail filter in the Management application is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box. See "Setting up advanced event filtering" on page 827 for more information.

To configure event notifications, use the instructions in "Configuring e-mail notification" on page 824.

Syslog forwarding

NOTE
Syslog messages are only available on Brocade devices and HBAs (managed using the HCM Agent).

Syslog forwarding is the process by which you can configure the Management application to send Syslog messages to other computers. Switches only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you must configure the Management application to listen on a different port. Then you must configure another Syslog server to listen for Syslog messages and forward the messages to the Management application Syslog listening port. Brocade HBAs only send the Syslog information through port 514; therefore, if port 514 is being used by another application, you the management application cannot send Syslog messages to another computer.

Syslog messages are persisted in the database. You can view the Syslog messages from the Management application. However, the Management application does not convert the Syslog messages into event objects except for the audit syslog messages.

For more information about Syslog forwarding, refer to "Syslog forwarding" on page 844.

Backup support

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

Configuring backup to a hard drive

NOTE
This procedure requires a hard drive. The drive should not be the same physical drive on which your Operating System or the Management application is installed.

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

1. Click the **SAN** tab.
2. Select **Server** > **Options**.

   The **Options** dialog box displays.
3. Select **Server Backup** in the **Category** list.

   The currently defined directory displays in the **Output Directory** field.
4. Select the **Enable Backup** check box, if necessary.
5. Choose one or more of the following options:
   - Select the **Include Adapter Boot Image** directory to back up boot image files from the boot image repository.
   - Select the **Include FTP Root directory** check box.

     If you select the FTP Root directory, the FTP Root sub-directories, Technical Support and Trace Dump are selected automatically and you cannot clear the sub-directory selections. If you do not select the FTP Root directory, the sub-directories can be selected individually.

6. Enter the time (using a 24-hour clock) you want the backup process to begin in the Next Backup Start Time Hours and Minutes fields.
7. Select an interval from the Backup Interval drop-down list to set how often backup occurs.
8. Browse to the hard drive and directory to which you want to back up your data.
9. 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.

Enabling backup

Backup is enabled by default. However, if it has been disabled, complete the following steps to enable the function.

1. Click the SAN tab.
2. Select Server > Options.

   The Options dialog box displays.
3. Select Server Backup in the Category list.
4. Select the Enable Backup check box.
5. Click Apply or OK.

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. Click the SAN tab.
2. Select Server > Options.

   The Options dialog box displays.
3. Select Server Backup in the Category list.
4. Clear the Enable Backup check box.
5. Click Apply or OK.

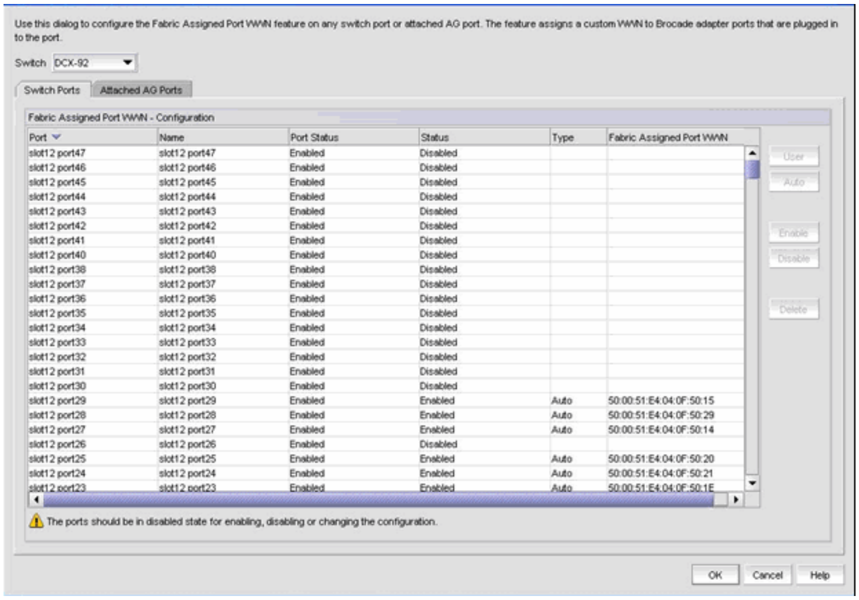
Adapter port WWN virtualization

Adapter port world wide name (WWN) virtualization enables the adapter port to use a switch-assigned WWN rather than the physical port WWN for communication, allowing you to pre-provision the server with the following configuration tasks:

- Create the zones with the Fabric Assigned WWN before the servers and devices are connected to the switches, before they are exposed to the SAN network.
- Create LUN mapping and LUN masking without the devices present in the network.
- Pre-configure boot LUN zoning. You can configure Solaris ports or Linux ports on the switch, enabling the server to boot automatically with the pre-defined boot LUNs.

NOTE
Fabric Assigned WWN (FAWWN) is not supported for base switches or FICON-enabled switches.

Configuring fabric-assigned port WWNs on switch ports



Use this dialog to configure the Fabric Assigned Port WWN feature on any switch port or attached AG port. The feature assigns a custom WWN to Brocade adapter ports that are plugged in to the port.

Switch: DCX-92

Fabric Assigned Port WWN - Configuration

Port	Name	Port Status	Status	Type	Fabric Assigned Port WWN
slot12 port47	slot12 port47	Enabled	Disabled		
slot12 port46	slot12 port46	Enabled	Disabled		
slot12 port45	slot12 port45	Enabled	Disabled		
slot12 port44	slot12 port44	Enabled	Disabled		
slot12 port43	slot12 port43	Enabled	Disabled		
slot12 port42	slot12 port42	Enabled	Disabled		
slot12 port41	slot12 port41	Enabled	Disabled		
slot12 port40	slot12 port40	Enabled	Disabled		
slot12 port38	slot12 port38	Enabled	Disabled		
slot12 port37	slot12 port37	Enabled	Disabled		
slot12 port36	slot12 port36	Enabled	Disabled		
slot12 port35	slot12 port35	Enabled	Disabled		
slot12 port34	slot12 port34	Enabled	Disabled		
slot12 port33	slot12 port33	Enabled	Disabled		
slot12 port32	slot12 port32	Enabled	Disabled		
slot12 port31	slot12 port31	Enabled	Disabled		
slot12 port30	slot12 port30	Enabled	Disabled		
slot12 port29	slot12 port29	Enabled	Enabled	Auto	50:00:51:E4:04:0F:50:15
slot12 port28	slot12 port28	Enabled	Enabled	Auto	50:00:51:E4:04:0F:50:29
slot12 port27	slot12 port27	Enabled	Enabled	Auto	50:00:51:E4:04:0F:50:14
slot12 port26	slot12 port26	Enabled	Disabled		
slot12 port25	slot12 port25	Enabled	Enabled	Auto	50:00:51:E4:04:0F:50:20
slot12 port24	slot12 port24	Enabled	Enabled	Auto	50:00:51:E4:04:0F:50:21
slot12 port23	slot12 port23	Enabled	Enabled	Auto	50:00:51:E4:04:0F:50:1E

⚠ The ports should be in disabled state for enabling, disabling or changing the configuration.

FIGURE 112 Configure Fabric Assigned WWNs dialog box

The **Configure Fabric Assigned WWNs** dialog box enables you to perform the following tasks:

- Enable and disable the Fabric Assigned WWN feature status on a switch or AG port.
- Set the type value to *auto* or *user-defined*. When the **User** button is selected, the WWN is cleared from the table and editing is enabled.
- Delete the Fabric Assigned WWN from the **Fabric Assigned WWN - Configuration** table.

Instructions for performing the Fabric Assigned WWN configuration tasks are detailed in the following sections.

Enabling the FAWWN feature on a switch or AG ports

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Select a switch port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **Enable** button.

   The selected switch's Port status is enabled.
4. Click **OK**.

   The **Fabric Assigned WWN Confirmation and Status** dialog box displays.
5. Click **Start** to save the changes to the switch.
6. Click **Close** on the **Fabric Assigned WWN Configuration** dialog box.

Disabling the fabric assigned WWN feature on a switch or AG port

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Select a switch port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **Disable** button.

   The selected switch's FAWWN feature status is disabled.
4. Click **OK**.

Auto-assigning a switch or AG port 's fabric assigned WWN

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Select a switch port or AG port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **User** button.

   The systems sets the type to **User** and the Fabric Assigned WWN column cells are now editable.
4. Enter a valid world wide name on the selected switch.
5. Click **OK**.

Manually assigning a FAWWN to a switch or AG port

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.

2. Select a switch port or AG port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **Auto** button.

   If the switch port does not have an Auto FAWWN map type and the FAWWN feature is not yet enabled on the port, a <To Be Generated> message displays.

4. Click **OK**.

Modifying a switch or AG port WWN

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.

2. Select a switch port or AG port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **User** button.

   The Fabric Assigned WWNs parameters are now editable.

Deleting a switch port WWN

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.

2. Select a switch port or AG port from the **Fabric Assigned WWN - Configuration** list.
3. Click the **Delete** button.

   The Fabric Assigned WWN row is cleared from the **Fabric Assigned WWNs** list.

Configuring Fabric Assigned WWNs on attached AG ports

The **Add AG Fabric Assigned WWN Configuration** dialog box, shown in Figure 113, enables you to configure the Fabric Assigned WWN feature on a selected attached Access Gateway (AG) port.

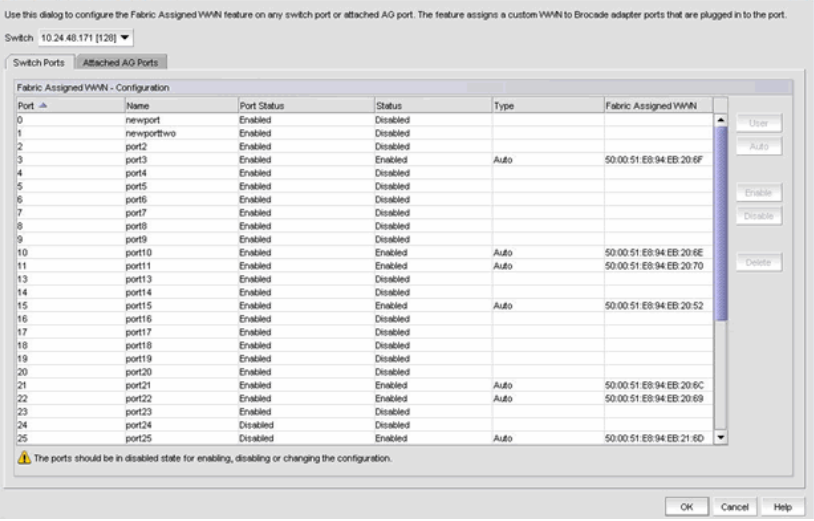
1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.

2. Click the **Attached AG Ports** tab.



Use this dialog to configure the Fabric Assigned WWN feature on any switch port or attached AG port. The feature assigns a custom WWN to Brocade adapter ports that are plugged in to the port.

Switch 10.24.48.171 [128]

Fabric Assigned WWN - Configuration

Port	Name	Port Status	Status	Type	Fabric Assigned WWN
0	newport	Enabled	Disabled		
1	newporttwo	Enabled	Disabled		
2	port2	Enabled	Disabled		
3	port3	Enabled	Enabled	Auto	50:00:51:E8:94:EB:20:6F
4	port4	Enabled	Disabled		
5	port5	Enabled	Disabled		
6	port6	Enabled	Disabled		
7	port7	Enabled	Disabled		
8	port8	Enabled	Disabled		
9	port9	Enabled	Disabled		
10	port10	Enabled	Enabled	Auto	50:00:51:E8:94:EB:20:6E
11	port11	Enabled	Enabled	Auto	50:00:51:E8:94:EB:20:70
13	port13	Enabled	Disabled		
14	port14	Enabled	Disabled		
15	port15	Enabled	Enabled	Auto	50:00:51:E8:94:EB:20:52
16	port16	Enabled	Disabled		
17	port17	Enabled	Disabled		
18	port18	Enabled	Disabled		
19	port19	Enabled	Disabled		
20	port20	Enabled	Disabled		
21	port21	Enabled	Enabled	Auto	50:00:51:E8:94:EB:20:6C
22	port22	Enabled	Enabled	Auto	50:00:51:E8:94:EB:20:69
23	port23	Enabled	Disabled		
24	port24	Disabled	Disabled		
25	port25	Disabled	Enabled	Auto	50:00:51:E8:94:EB:21:6D

⚠ The ports should be in disabled state for enabling, disabling or changing the configuration.

FIGURE 113 Configure Fabric Assigned WWNs on attached AG ports dialog box

Adding AG port Fabric assigned WWNs

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

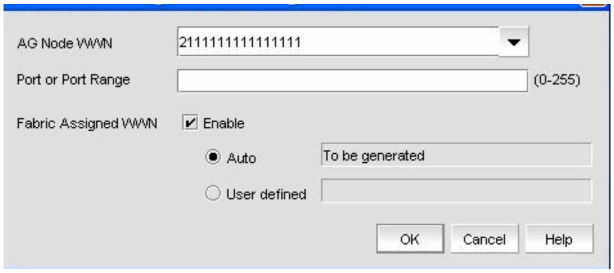
   The **Configure Fabric Assigned WWNs** dialog box displays.

2. Click the **Attached AG Ports** tab.

3. Select a row in the **Fabric Assigned WWN Configuration - AG Ports** list.

4. Click **Add**.

   The **Add AG Fabric Assigned WWN Configuration** dialog box, shown in Figure 114, displays.



AG Node WWN 2111111111111111

Port or Port Range (0-255)

Fabric Assigned WWN ☑ Enable

● Auto To be generated

○ User defined

FIGURE 114 Add AG Fabric Assigned WWN Configuration dialog box

5. Enter a valid world wide name (WWN), with or without colons, for the Access Gateway node. Optionally, you can select an existing AG Node WWN from the list. The AG Node WWN combo box includes all discovered AG Node WWNs that are connected to the selected switch.
6. Enter a port or a port range using numbers or a hyphen (-). For example, you can enter a range as 1-6 or you can separate values with a comma; for example: 1, 2, 5, 7-10, 20.
7. Click the **Enable** checkbox to enable the Fabric Assigned WWN.
8. Set the fabric assigned WWN type to one of the following map types:
   - Auto—If the switch port does not have an Auto FAWWN map type and the FAWWN feature is not yet enabled on the port, a <To Be Generated> message displays.
   - User defined—If this option is selected, you must enter a valid world wide name, with or without colons. The User defined text box cannot be empty.
9. Click **OK** to add the rows for this configuration to the **Fabric Assigned WWN Configuration - AG Ports** list.

Deleting AG port FAWWNs

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Click the **Attached AG Ports** tab.
3. Select an online AG Fabric Assigned WWN row and click the **Delete** button.

   The AG FAWWN row is cleared from the **Fabric Assigned WWN Configuration - AG Ports** list.

Moving an AG port 's FAWWN across switches

The AG port FAWWN can be online or offline when moved across switches.

1. Select **Configure > Fabric Assigned WWN**.

   or

   Right-click the switch and select Fabric Assigned WWN.

   The **Configure Fabric Assigned WWNs** dialog box displays.
2. Click the **Attached AG Ports** tab.

3. Select the WWN row you want to move by right-clicking it, select the **Copy Row** option, and paste the contents into a text editor.
4. Select an online AG FAWWN row and click the **Delete** button.
5. Select a switch from the **Switch** list and click **Add** to launch the **Add AG Fabric Assigned WWN Configuration** dialog box.
6. Using the information you copied to the text editor, configure the AG port WWN information to be moved to the selected switch.
7. Click **OK**.

   The specified AG FAWWN row is added to the new switch.

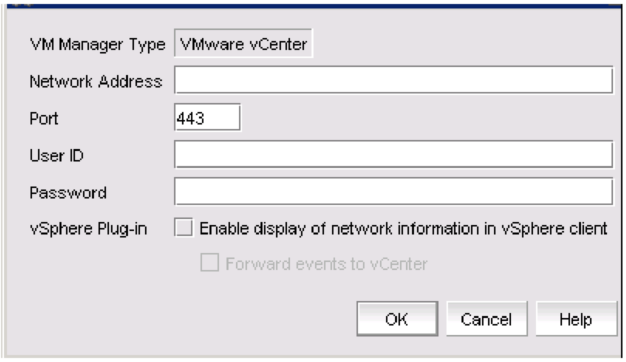
VM Manager

A vCenter server can be discovered by adding a VM Manager tor to the Management application. See "VM Manager Discovery" on page 78 for information about discovering VM Managers.

Adding a VM Manager

1. Click **Add** on the **Discover VM Managers** dialog box.

   The **Add VM Manager** dialog box displays.



VM Manager Type: VMware vCenter

Port: 443

Network Address
User ID
Password
vSphere Plug-in
☐ Enable display of network information in vSphere client
☐ Forward events to vCenter
OK
Cancel
Help

FIGURE 115 Add VM Manager dialog box

2. Enter the IP address or host name of the VM Manager (VMM) into the **Network Address** text box. The maximum number of supported characters is 256.
3. Enter the VMM server port number into the **Port** text box. The valid port number range is 0 through 65536.
4. Enter the user ID into the **User ID** text box to identify the user of the VMM. The maximum number of supported characters is 64.
5. Enter the password into the **Password** text box. The maximum number of supported characters is 64.

6. Enable or disable the vSphere client plug-in registration. If you enable this plug-in, events are forwarded from the Management application to the vCenter server.
7. Click **OK**.

   The VMM discovery process begins. When complete, the vCenter server and all ESX hosts managed by that vCenter display in the Host product tree.

Editing VM Manager

The fields in the **Edit VM Manager** dialog box are identical to the fields in the **Add VM Manager** dialog box except for the **Network Address** field, which you cannot edit.

1. Click **Edit** on the **Discover VM Managers** dialog box.

   The **Edit VM Manager** dialog box displays.
2. Enter the VMM server port number into the **Port** text box. The valid port number range is 0 through 65536.
3. Enter the user ID into the **User ID** text box to identify the user of the VMM. The maximum number of supported characters is 64.
4. Enter the password into the **Password** text box. The maximum number of supported characters is 64.
5. Enable or disable the vSphere client plug-in registration. If you enable this plug-in, events are forwarded from the Management application to the vCenter server.
6. Click **OK**.

   The VMM discovery process begins. When complete, the vCenter server and all ESX hosts managed by that vCenter display in the Host product tree.

Deleting VM Manager

You cannot delete a VM Manager host. Hosts can only be excluded or included. If you select a host from the **Discovered VM Managers** list in the **Discover VM Managers** dialog box and click **Delete**, the host displays in the **Previously Discovered Addresses** list.

Chapter

Fibre Channel over Ethernet 15

In this chapter

FCoE overview

Fibre Channel over Ethernet (FCoE) leverages Ethernet enhancements, called *Data Center Bridging (DCB),* to transport encapsulated Fibre Channel frames over Ethernet. Ethernet is the physical layer over which the encapsulated FC frames are transported.

One of the barriers to using Ethernet as the basis for a converged network has been the limited bandwidth that Ethernet has historically provided. However, with 10 Gbps Ethernet, the available bandwidth now offers the potential to consolidate all the traffic types over the same link.

Unlike Fibre Channel, Ethernet is not a peer-to-peer protocol. The mechanism used to discover new ports, MAC address assignments and FC logins and logouts is called the FCoE Initialization Protocol (FIP).

DCB exchange protocol

DCB Exchange (DCBX) protocol allows enhanced Ethernet devices to convey and configure their DCB capabilities and ensures a consistent configuration across the network. DCBX protocol is used between data center bridging (DCB) devices, such as a converged network adapter (CNA) and a FCoE switch, to exchange configuration with directly-connected peers.

NOTE
When DCBX protocol is used, any other LLDP implementation must be disabled on the host systems.

Enhanced Ethernet features

Data Center Bridging (DCB) is a set of IEEE 802 standard Ethernet enhancements that enable Fibre Channel convergence with Ethernet. The two basic requirements in a lossless Ethernet environment are Enhanced Transmission Selection (ETS) and priority-based flow control. These capabilities allow the Fibre Channel frames to run directly over 10 Gbps Ethernet segments without adversely affecting performance.

Enhanced transmission selection

Enhanced transmission selection (ETS) allows lower priority traffic classes to use available bandwidth that is not be used by higher priority traffic classes and maximizes the use of available bandwidth.

ETS allows configuration of bandwidth per priority group.

Priority group ID usage is defined as follows:

- PGID = {0, 7} is used when the priority group is limited for its bandwidth use.
- PGID = {8, 14} is reserved.
- PGID = {15.0 - 15.7} is used for priorities that are not limited for their bandwidth use.

The configured priority group percentage refers to the maximum percentage of available link bandwidth after PGID 15.0 to 15.7 is serviced, assuming all priority groups are fully subscribed. If one of the priority groups does not consume its allocated bandwidth, then any unused portion is available for use by other priority groups.

Priority-based flow control

Priority-based flow control allows the network to selectively pause different classes of traffic and create lossless lanes for Fibre Channel, while retaining packet drop congestion management for IP traffic. A high-level pause example follows:

- During periods of heavy congestion, the receive buffers reach high threshold and generate a pause.
- The pause tells transmission (Tx) queues to stop transmitting.
- After the receive (Rx) buffers reach low threshold, a zero pause is generated.
- The zero pause signals the Tx queues to resume transmitting.

Ethernet jumbo frames

The basic assumption underlying FCoE is that TCP/IP is not required in a local data center network and the necessary functions can be provided with Enhanced Ethernet. The purpose of an “enhanced” Ethernet is to provide reliable, lossless transport for the encapsulated Fibre Channel traffic. Enhanced Ethernet provides support for jumbo Ethernet frames and in-order frame delivery.

The Fabric OS FCoE 10 Gbps converged network adapter supports jumbo packets of up to 9 KB, compared to the original 1,518-byte MTU for Ethernet. The frame size increase allows the same amount of data to be transferred with less effort.

FCoE protocols supported

The Fabric OS FCoE converged network adapter supports two layers of protocols: Ethernet link layer and FCoE layer. They are listed in the following sections.

Ethernet link layer protocols supported

The following protocols support the Ethernet link layer.

- 802.1q (VLAN)
- 802.1Qaz (enhanced transmission selection)
- 802.1Qbb (priority flow control)
- 802.3ad (link aggregation)
- 802.3ae (10 Gb Ethernet)
- 802.1p (priority encoding)
- IEEE 1149.1 (JTAG) for manufacturing debug and diagnostics
- IPv4 specification (RFC 793/768)
- IPv6 specification (RFC 2460)
- TCP/UDP specification (RFC 793/768)
- ARP specification (RFC 826)
- RSS with support for IPV4TCP, IPV4, IPV6TCP, IPV6 hash types
- HDS (Header-data split)

FCoE protocols

The following protocols support Fibre Channel over Ethernet.

- FIP (FC-BB5 compliant):
  - Support for FIP Discovery protocol for dynamic FCF discovery and FCoE link management
  - Support for FPMA and SPMA type FIP fabric login
- Support for Initiator mode only (FCP-3 compliant in Initiator mode)
- SCSI protection information support
- IP-over-FC
- NPIV support

FCoE Licensing

The FCoE license enables Fibre Channel over Ethernet (FCoE) functionality on the 8 Gbps 8-FC port, 10 GbE 24-DCB port Switch. Without the FCoE license, the 8 Gbps 8-FC port, 10 GbE 24-DCB port Switch is a pure L2 Ethernet switch and will not allow FCoE bridging capabilities.

With the FCoE license, the FCoE Configuration dialog displays virtual FCoE port information and enables you to manage the virtual port information. The topology displays directly-connected converged network adapters (CNAs) and the **Properties** dialog for the virtual FCoE port details.

Without the FCoE license, the virtual FCoE port displays in the device tree, but you cannot enable, disable, or view virtual FCoE port information.

Save running to startup

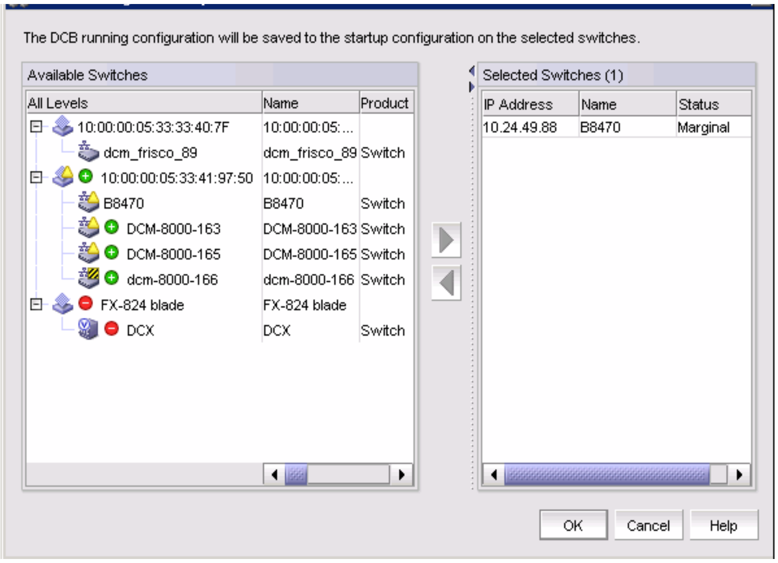
The **Save running to startup** dialog box lists discovered DCB switches with Fabric OS version 6.3x firmware or higher. You can select available switches and move them to the Selected Switches table. Upon startup, the DCB switch configuration is copied to the selected switches.

NOTE
This dialog box launches if there is at least one DCB switch discovered. If no DCB switches exist, a warning dialog displays.

Copying switch configurations to selected switches

1. To access the **Save running to startup** dialog box, select **Configure** > **Configuration** > **Save Running to Startup** from the menu bar.

   The **Save Running to Startup** dialog box displays.



The DCB running configuration will be saved to the startup configuration on the selected switches.

Available Switches

All Levels	Name	Product
10:00:00:05:33:33:40:7F	10:00:00:05:...	
dcm_frisco_89	dcm_frisco_89	Switch
10:00:00:05:33:41:97:50	10:00:00:05:...	
B8470	B8470	Switch
DCM-8000-163	DCM-8000-163	Switch
DCM-8000-165	DCM-8000-165	Switch
dcm-8000-166	dcm-8000-166	Switch
FX-824 blade	FX-824 blade	
DCX	DCX	Switch

Selected Switches (1)

IP Address	Name	Status
10.24.49.88	B8470	Marginal

FIGURE 116 Save running to startup dialog box

2. Highlight a discovered DCB switch from the **Available Switches** table, and click the right arrow button to move the switch to the **Selected Switches** Table.
3. Highlight the selected switch and click **OK** to start the configuration.

   The running configuration is saved to the selected switch, effective on the next system startup. If you restore the DCB switch using the **Restore Switch Configuration** dialog box, you are prompted to select one of two restoration methods:

   - As the running configuration and reboot

     ATTENTION
     Rebooting a switch connected to a fabric will stop all traffic to and from the switch. All ports on the switch will become inactive until the switch comes back online.

   - As the startup configuration (no reboot)

   For instructions on how to restore a saved switch configuration, refer to "Restoring a switch configuration for a selected device" on page 257.

DCB configuration

Depending on the platform, the DCB switch has the one of the following configurations:

- For the IBM blade server:
  - 14 internal 10 Gbps ports for BCH type
  - 12 internal 10 Gbps ports BCHT type
  - Eight external 10 Gbps DCB ports
  - Eight 8-Gbps FC ports
- For the Dell embedded switch module:
  - 16 10-Gbps internal ports
  - Eight 10-Gbps external ports
  - Four 8-Gbps FC ports

You must configure DCB interfaces and ports differently than you configure FC ports, in order to effectively use the converged network features.

For example, Priority-based flow control (PFC) and Enhanced transmission selection (ETS) are the two QoS policy enhancements you must configure to create a lossless Ethernet. You then use DCBX protocol on DCB-enabled devices to exchange configuration information.

The DCB/FC switch module for the IBM Blade Center has eight 8-Gbps FC ports and 22/20 10 Gbps Ethernet DCB ports. The DCB ports are categorized into two types:

- External ports - The eight external ports are the same as the original 10 Gbps Ethernet DCB ports. The default name in the device tree is ExT<slot>/<port>.
- Internal ports - The default name for the 12 or 14 internal ports is InT <slot>/<port>. 802.1x, LAG configuration, and spanning tree protocol (STP) are not supported on internal ports.

Switch policies

You can configure and enable a number of DCB policies on a switch, port, or link aggregation group (LAG).

The following switch policy configurations apply to all ports in a LAG:

- DCB map and Traffic Class map
- Link Layer Discovery Protocol (LLDP)

The switch policies are described in the following sections.

DCB map and Traffic Class map

With DCB, Fibre Channel uses a buffer management system based on buffer-to-buffer credits, with corresponding confirmation by the R-RDY frame. The flow control standard used for DCB is based on "pause" frames. Coupled with an appropriate input buffer, lossless transport of frames is possible.

Priority-based flow control (PFC) deals with the prioritization of frames. This standard IEEE 802.1Q allows application-specific bandwidth reservations in DCB. When you create a DCB map, you specify the precedence (priority) and then you map the priority groups with the Class of Service (CoS) and apply bandwidth percentages.

Refer to "QoS configuration" on page 358 for instructions on how to create DCB and Traffic Class maps.

LLDP profiles

Data Center Bridging Capability Exchange Protocol (DCBX) enables Enhanced Ethernet devices to discover whether a peer device supports particular features, such as Priority Flow Control or Class of Service (CoS). In a Data Center Bridging (DCB) environment, LLDP is enhanced with DCBX protocol to further share or change the configured DCB enhancements.

Refer to "LLDP-DCBX configuration" on page 372 for instructions on how to configure LLDP for FCoE.

802.1x policy

802.1x is a standard authentication protocol that defines a client-server-based access control and authentication protocol. 802.1x restricts unknown or unauthorized clients from connecting to a LAN through publicly accessible ports.

Refer to "802.1x authentication" on page 377 for information on setting 802.1x parameters.

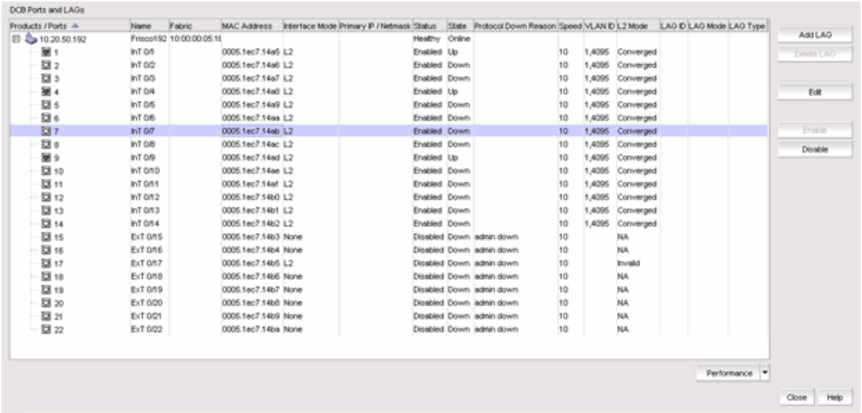
Opening the DCB Configuration dialog box

Launch the DCB Configuration dialog box using one of the following methods:

- Select **Configure** > **DCB** from the menu bar.
- Right-click the DCB switch from the device tree, and select **Configure** > **DCB**.
- Right-click the DCB switch from the topology map and select **Configure** > **DCB**.

The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

NOTE
The **Protocol Down Reason** column displays the values only for the external ports of embedded platforms but not for the internal ports.



DCB Ports and LAGs

Products / Ports	Name	Fabric	MAC Address	Interface Mode	Primary IP / Netmask	Status	State	Protocol Down Reason	Speed	VLAN ID	L2 Mode	LAG ID	LAG Mode	LAG Type
10.20.50.192	Frisco192	10:00:00:05:1				Healthy	Online							
1	InT 0/1		0005.1ec7.14a5	L2		Enabled	Up		10	1,4095	Converged			
2	InT 0/2		0005.1ec7.14a6	L2		Enabled	Down		10	1,4095	Converged			
3	InT 0/3		0005.1ec7.14a7	L2		Enabled	Down		10	1,4095	Converged			
4	InT 0/4		0005.1ec7.14a8	L2		Enabled	Up		10	1,4095	Converged			
5	InT 0/5		0005.1ec7.14a9	L2		Enabled	Down		10	1,4095	Converged			
6	InT 0/6		0005.1ec7.14aa	L2		Enabled	Down		10	1,4095	Converged			
7	InT 0/7		0005.1ec7.14ab	L2		Enabled	Down		10	1,4095	Converged			
8	InT 0/8		0005.1ec7.14ac	L2		Enabled	Down		10	1,4095	Converged			
9	InT 0/9		0005.1ec7.14ad	L2		Enabled	Up		10	1,4095	Converged			
10	InT 0/10		0005.1ec7.14ae	L2		Enabled	Down		10	1,4095	Converged			
11	InT 0/11		0005.1ec7.14af	L2		Enabled	Down		10	1,4095	Converged			
12	InT 0/12		0005.1ec7.14b0	L2		Enabled	Down		10	1,4095	Converged			
13	InT 0/13		0005.1ec7.14b1	L2		Enabled	Down		10	1,4095	Converged			
14	InT 0/14		0005.1ec7.14b2	L2		Enabled	Down		10	1,4095	Converged			
15	ExT 0/15		0005.1ec7.14b3	None		Disabled	Down	admin down	10		NA			
16	ExT 0/16		0005.1ec7.14b4	None		Disabled	Down	admin down	10		NA			
17	ExT 0/17		0005.1ec7.14b5	L2		Disabled	Down	admin down	10		Invalid			
18	ExT 0/18		0005.1ec7.14b6	None		Disabled	Down	admin down	10		NA			
19	ExT 0/19		0005.1ec7.14b7	None		Disabled	Down	admin down	10		NA			
20	ExT 0/20		0005.1ec7.14b8	None		Disabled	Down	admin down	10		NA			
21	ExT 0/21		0005.1ec7.14b9	None		Disabled	Down	admin down	10		NA			
22	ExT 0/22		0005.1ec7.14ba	None		Disabled	Down	admin down	10		NA			

FIGURE 117 DCB configuration dialog box

Minimum DCB configuration for FCoE traffic

You must complete the following procedures to create the basic configuration of DCB for FCoE traffic.

This section is applicable for the following Fabric OS (FOS) versions: 6.3.0, 6.3.1, 6.3.2, 6.4.1, and 6.4.2. This section is not applicable for FOS versions 6.3.1_dcb, 6.3.1_cee, 6.4.1_fcoe, or 7.0.0.

NOTE
The first two procedures in this section can be completed as a single procedure. They were broken into two separate procedures for clarity.

Creating a DCB map to carry the LAN and SAN traffic

To create a DCB map to carry the LAN and SAN traffic, complete the following steps. This procedure is applicable for FOS versions lower than FOS 7.0. For FOS versions 7.0 and higher, you can only edit the the default DCB map.

1. Select **Configure > DCB.**

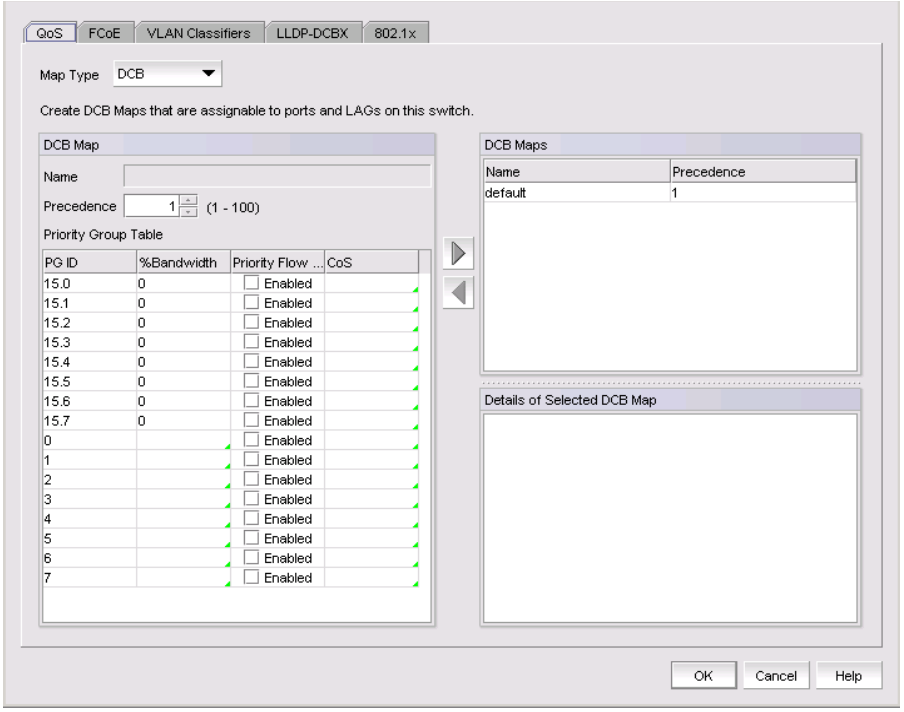
   The **DCB Configuration** dialog box displays.

2. Select the switch to edit in the **DCB Ports and LAGs** table and click **Edit.**

   The **Edit Switch** dialog box displays.

3. Click the **QOS** tab.

   The **Edit Switch - QoS tab dialog box** displays



Map Type DCB

Create DCB Maps that are assignable to ports and LAGs on this switch.

DCB Map

Name

Precedence 1 (1 - 100)

Priority Group Table

PG ID	%Bandwidth	Priority Flow ...	CoS
15.0	0	☐ Enabled	
15.1	0	☐ Enabled	
15.2	0	☐ Enabled	
15.3	0	☐ Enabled	
15.4	0	☐ Enabled	
15.5	0	☐ Enabled	
15.6	0	☐ Enabled	
15.7	0	☐ Enabled	
0		☐ Enabled	
1		☐ Enabled	
2		☐ Enabled	
3		☐ Enabled	
4		☐ Enabled	
5		☐ Enabled	
6		☐ Enabled	
7		☐ Enabled	

DCB Maps

Name	Precedence
default	1

Details of Selected DCB Map

FIGURE 118 Edit Switch dialog box - QOS tab

4. Use “Creating a DCB map” on page 359 to create a new DCB Map or edit an existing map to carry the traffic types, as shown in the dialog box above. Creating a new DCB map is applicable to Fabric OS versions 7.0 and higher.

5. Click **Close** on the **DCB Configuration** dialog box.

Configuring LLDP for FCoE

To configure LLDP for FCoE, complete the following steps.

1. Select **Configure > DCB**.

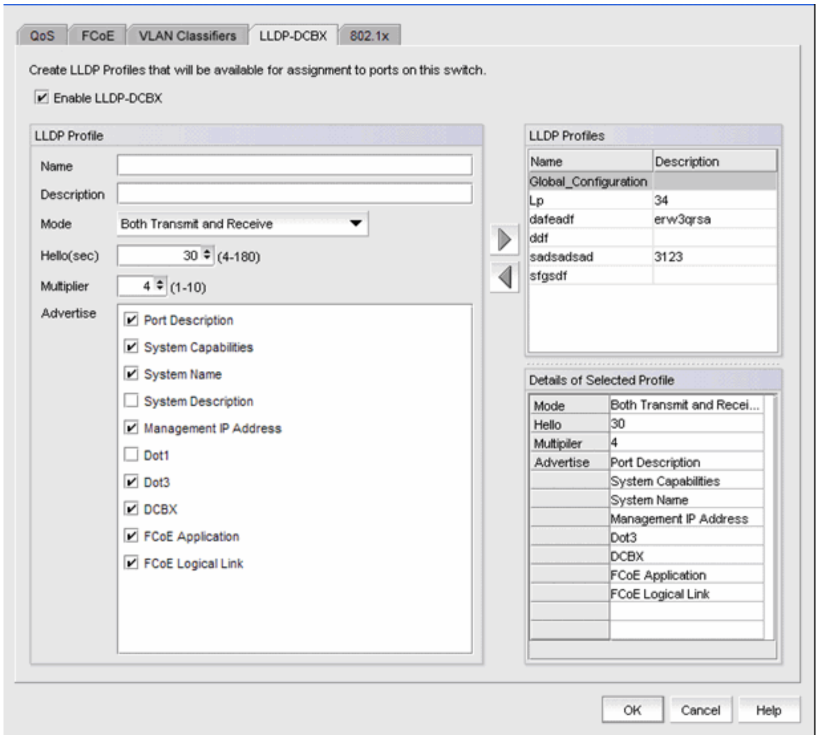
   The **DCB Configuration** dialog box displays.

2. Select the switch to edit in the **DCB Ports and LAGs** table and click **Edit**.

   The **Edit Switch** dialog box displays.

3. Click the **LLDP-DCBX** tab.

4. The **Edit Switch - LLDP-DCBX** tab dialog box displays.



Create LLDP Profiles that will be available for assignment to ports on this switch.

☑ Enable LLDP-DCBX

LLDP Profile

Name

Description

Mode: Both Transmit and Receive

Hello(sec): 30 (4-180)

Multiplier: 4 (1-10)

Advertise:
☑ Port Description
☑ System Capabilities
☑ System Name
□ System Description
☑ Management IP Address
□ Dot1
☑ Dot3
☑ DCBX
☑ FCoE Application
☑ FCoE Logical Link

LLDP Profiles

Name	Description
Global_Configuration	
Lp	34
dafeadf	erw3qrsa
ddf	
sadsadsad	3123
sfgsdf	

Details of Selected Profile

Mode	Both Transmit and Recei...
Hello	30
Multipiler	4
Advertise	Port Description
	System Capabilities
	System Name
	Management IP Address
	Dot3
	DCBX
	FCoE Application
	FCoE Logical Link

FIGURE 119 DCB Edit Switch dialog box - LLDP-DCBX tab

5. Select the **<Global Configuration>** LLDP profile in the **LLDP Profiles** table.

6. Click the left arrow button to edit.

7. Select the **FCoE Application** and **FCoE Logical Link** check boxes in the **Advertise** table to advertise them on the network.

8. Click **OK** after changing the attributes of the current deployment.

   The **Deploy to Products** dialog box displays.

   The **Deployment Status** dialog box launches.

9. Click **Start** on the **Deployment Status** dialog box to save the changes to the switch.

10. Click **Close** to close the dialog box.

Configuring the DCB interface with the DCB Map and Global LLDP profile

To configure the DCB interface, complete the following steps.

1. Select **Configure** > **DCB**.

   The **DCB Configuration** dialog box displays.

2. Select the Te port connected to the CNA in the **DCB Ports and LAGs** table and click **Edit**.
3. Select the **Port** tab, if necessary, and select the **Enable** check box.
4. Select **L2** from the **Interface Mode** list.
5. Select **Converged** (for a Brocade CNA) or **Access** (for QLogic CNA) from the **L2 Mode** list.
6. Click the **QOS** tab and select the **Assign a map** check box.
7. Select **DCB** from the **Map Type** list.
8. Select the DCB map you created in "Creating a DCB map to carry the LAN and SAN traffic" on page 346 from the **Available DCB Maps** list.
9. Click the **LLDP-DCBX** tab and select the **Enable LLDP-DCBX on Te** *Port Number* check box.
10. Select **Assign the Global Configuration**.
11. Click **OK**.

    The **Deploy to Ports** dialog box displays.

12. Click **OK** after changing the attributes of the current deployment.

    The **Deployment Status** dialog box launches.

13. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected ports.
14. Click **Close** to close the **Deployment Status** dialog box.

Create the FCoE VLAN to carry FCoE traffic

NOTE
This procedure is completed using Web Tools.

To create the FCoE VLAN, complete the following steps. This procedure is applicable for FOS versions lower than FOS 7.0.

1. Select the Fabric OS FCoE switch in the Product Tree or Connectivity Map.
2. Select **Configure** > **Element Manager** > **Admin**.

   Web Tools displays. You can also launch Web Tools by clicking the **Element Manager** button on the DCB Configuration dialog box.

3. Click the **DCB** tab.
4. Click the **VLAN** tab.
5. Click **Add**.

   The **VLAN Configuration** dialog box displays.

6. Enter the VLAN identifier in the VLAN ID field.

7. Click **OK** on the **VLAN Configuration** dialog box.

   The **VLAN Configuration** dialog box displays.

8. Select the VLAN you created and click **Edit** to convert the VLAN to FCoE VLAN.
9. Select the **FCoE** check box.
10. Select the DCB interface to carry the FCoE traffic from the **Selection List** and click **Add** to add it to the **Selected List**.
11. Click **OK** on the **VLAN Configuration** dialog box to save your changes.
12. Close Web Tools.

Creating VLAN classifiers and activating on the DCB interface

---

NOTE
This procedure is completed using the CLI. This procedure is applicable for FOS versions lower than FOS 7.0.

To create and activate the VLAN classifiers on the DCB interface, complete the following steps.

1. Log into the switch and enter global configuration mode.

   Example

   ```
   switch:<userid>>cmsh
   switch#configure terminal
   ```

2. Create and apply VLAN Classifiers to the DCB interface to classify Ethernet frames on an untagged interface to VLAN.

   Example

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

3. Apply the VLAN classifier Group to the DCB interface.

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

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

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

   Example

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

Adding a LAG

Link aggregation is a mechanism to bundle several physical ports together to form a single logical channel or trunk. The collection of ports is called a link aggregation group (LAG).

NOTE
An internal port cannot be part of a LAG. You can create LAGs with external ports only.

The **Add LAG** button is enabled when a single DCB switch or ports of a single DCB switch are selected. The **Add LAG** button is disabled when multiple switches are selected, ports from different switches are selected, or LAGs are selected.

The **Edit button** is enabled when a single LAG, port, or switch is selected.

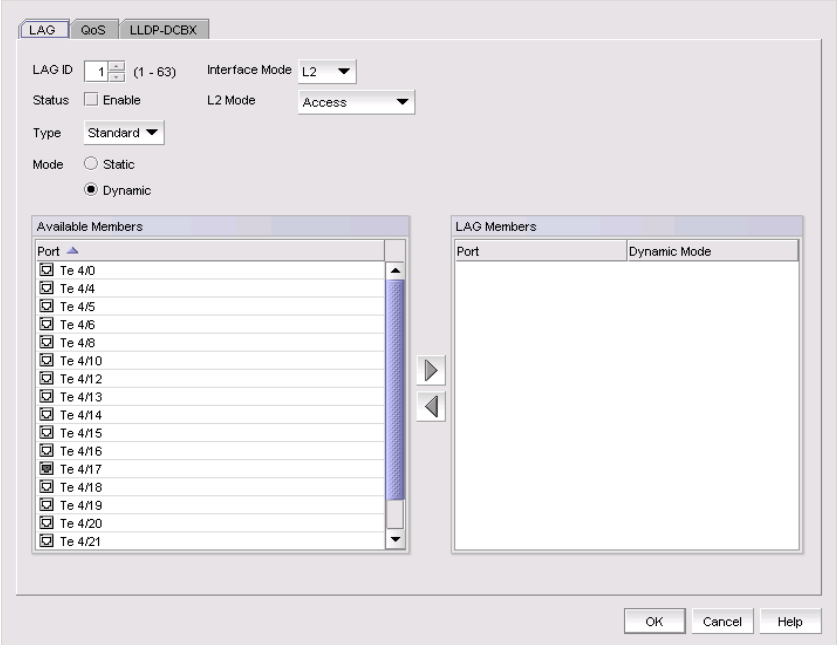
1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select the DCB switch or one or more DCB ports to add to a link aggregation group (LAG).

3. Click **Add LAG**.

   The **Add LAG** dialog box displays.



LAG ID 1 (1 - 63)   Interface Mode L2

Status □ Enable   L2 Mode Access

Type Standard

Mode ○ Static
● Dynamic

Available Members

Port
Te 4/0
Te 4/4
Te 4/5
Te 4/6
Te 4/8
Te 4/10
Te 4/12
Te 4/13
Te 4/14
Te 4/15
Te 4/16
Te 4/17
Te 4/18
Te 4/19
Te 4/20
Te 4/21

LAG Members

Port	Dynamic Mode

FIGURE 120 Add LAG dialog box

4. Configure the following LAG parameters:

   NOTE
   Ports with 802.1x authentication or ports that are L2 or L3 mode-enabled are not supported in a LAG.

   - **Status** - Enabled or Disabled. You must enable the LAG to use the DCB functionality.
   - **LAG ID** - Enter the LAG identifier, using a value between 1-63. Duplicate LAG IDs are not allowed.
   - **Interface mode** - none or L2.
     - The L3 interface mode option is displayed in the Edit LAG dialog box only.
   - **L2 interface mode** - Select the L2 mode (Access or Trunk):
     - Access mode allows only one VLAN and allows only untagged frames.
     - Trunk mode allows more than one VLAN association and allows tagged frames.
     - A converged mode interface can be native (Access, untagged frames) in one VLAN and non-native (Trunk, tagged frames) in another VLAN.
   - **IP/Netmask** - The netmask is used to divide an IP address into subnets. It specifies which portion of the IP address represents the network and which portion represents the host, and can only be configured if the interface mode is L3.
     - Primary - The primary IP address assigned to a 10 Gbps DCB/FC switch module.
     - Secondary - The secondary IP address is optional. Secondary IP addresses are helpful when the interface port is part of multiple subnets.

5. Select at least one available DCB port from the **Available Members** table and click the right arrow button to move them to the **LAG Members** table.

   The DCB ports are now part of the link aggregation group.

6. Continue to configure the following LAG parameters. These parameters are always enabled.

   - **Mode** - Sets all ports added to the LAG members table in either Static or Dynamic mode. The default is Dynamic, Active, but LAG members can be Active or Passive if the LAG member is Dynamic.
   - **Type** - Sets the limit on the size of the LAG. The type values include Standard, where the LAG is limited to 16 ports, and Brocade LAG, where the LAG is limited to four ports. The default is Standard.

     NOTE
     The 8 Gbps 16-FC-port, 10 GbE 8-Ethernet Port have three anvil chips and each anvil chip supports eight 10 Gbps Ethernet ports. You cannot create Fabric OS-type LAGs from different anvil chips. If you do, an error message displays and only the first port is considered as part of the LAG.

7. When you have finished configuring the policies, click **OK**.

   The **Deploy to LAGs** dialog box displays.

8. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.

9. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected LAG or LAGs.
10. Click **Close** to close the **Deployment Status** dialog box.

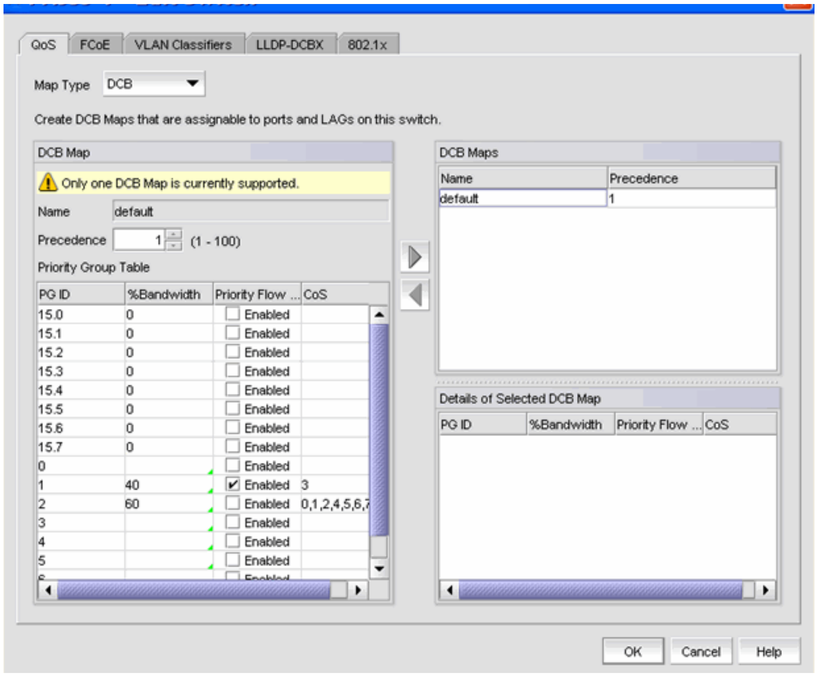
Editing a DCB switch

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select the DCB switch from the **Products/Ports** table.
3. Click **Edit**.

   The **Edit Switch** dialog box displays (Figure 121).



Map Type: DCB

Create DCB Maps that are assignable to ports and LAGs on this switch.

⚠ Only one DCB Map is currently supported.

Name: default

Precedence: 1 (1 - 100)

Priority Group Table

PG ID	%Bandwidth	Priority Flow ...	CoS
15.0	0	□ Enabled	
15.1	0	□ Enabled	
15.2	0	□ Enabled	
15.3	0	□ Enabled	
15.4	0	□ Enabled	
15.5	0	□ Enabled	
15.6	0	□ Enabled	
15.7	0	□ Enabled	
0		□ Enabled	
1	40	☑ Enabled	3
2	60	□ Enabled	0,1,2,4,5,6,7
3		□ Enabled	
4		□ Enabled	
5		□ Enabled	

Name	Precedence
default	1

PG ID	%Bandwidth	Priority Flow ...	CoS

FIGURE 121 Edit Switch dialog box

4. Configure the policies for the Edit Switch tabs, which are described in the following sections:
   - "QoS configuration" on page 358
   - "FCoE provisioning" on page 365
   - "VLAN classifier configuration" on page 368
   - "LLDP-DCBX configuration" on page 372
   - "802.1x authentication" on page 377
5. When you have finished configuring the policies, apply the settings to the switch.

NOTE
Clicking **Cancel** when there are pending changes launches a pop-up dialog.

6. Click **OK**.

   The **Deploy to Products** dialog box displays.

7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.

8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.

9. Click **Close** to close the **Deployment Status** dialog box.

Editing a DCB port

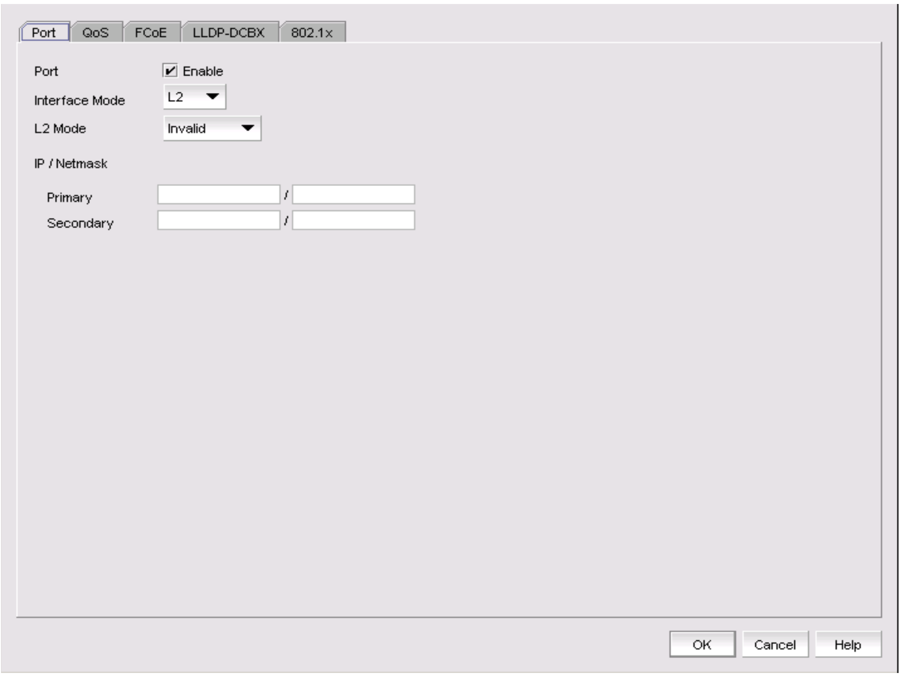
1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a DCB port from the Products/Ports table.

3. Click **Edit**.

   The **Edit Port** dialog box displays.



Port ☑ Enable

Interface Mode L2

L2 Mode Invalid

FIGURE 122 **Edit Port dialog box**

4. Modify the following DCB Port parameters as required:
   - **Status** - Enable or Disable. You must enable the LAG to use the DCB functionality.
   - **Interface Mode** - None or L2. For external ports, the **L3** interface mode displays, in addition to None or L2. If you select L3 as the interface mode, the IP/Netmask field is enabled and you can then assign the primary and secondary IP addresses.
     - L2 Mode - This is enabled if you select L2 as the Interface Mode. If a DCB port is enabled on the 10 Gbps DCB/FC switch module, the L2 mode is disabled.
     - L3 Mode appears only for the external ports of embedded platforms.

     NOTE
     You can change the Interface Mode from **L2** to **None** only if the port is assigned to the default VLAN 1.
   - **IP/Netmask** - The netmask is used to divide an IP address into subnets. It specifies which portion of the IP address represents the network and which portion represents the host, and can only be configured if the interface mode is L3.
     - Primary - The primary IP address assigned to a 10 Gbps DCB/FC switch module.
     - Secondary - The secondary IP address is optional. Secondary IP addresses are helpful when the interface port is part of multiple subnets.
5. When you have finished configuring the policies, apply the settings to the DCB port.

   NOTE
   Clicking **Cancel** when there are pending changes launches a pop-up dialog.
6. Click **OK** when you have finished modifying the DCB port parameters.

   The **Deploy to Ports** dialog box displays.
7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected port or ports.
9. Click **Close** to close the **Deployment Status** dialog box.

Editing a LAG

Use the following procedure to change members and policies in a link aggregation group (LAG).

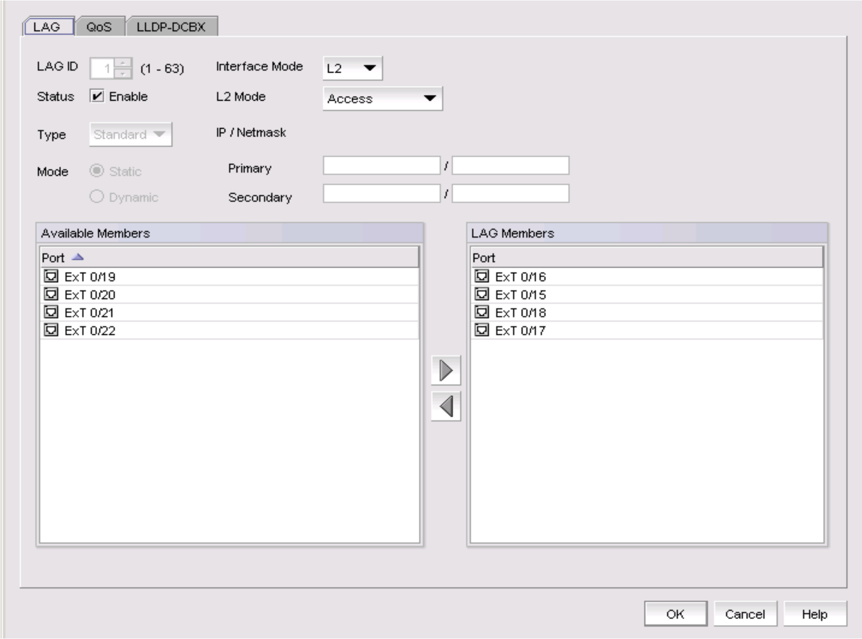
1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select the link aggregation group (LAG) from the **Products/Ports** table.

3. Click **Edit**.

   The **Edit LAG** dialog box displays.



LAG ID 1 (1 - 63)
Interface Mode L2
Status ☑ Enable
L2 Mode Access
Type Standard
IP / Netmask
Mode ● Static ○ Dynamic
Primary /
Secondary /

Available Members

Port
ExT 0/19
ExT 0/20
ExT 0/21
ExT 0/22

LAG Members

Port
ExT 0/16
ExT 0/15
ExT 0/18
ExT 0/17

FIGURE 123 Edit LAG dialog box

4. Configure the following LAG parameters, as required:

NOTE
Ports with 802.1x authentication or ports that are L2/L3 mode enabled are not supported in a LAG.

- **Status** - Enabled or Disabled. You must enable the LAG to use the DCB functionality.
- **LAG ID** - The LAG identifier, which is not an editable field.
- **Interface Mode** - L2 or none. For external ports, the **L3** interface mode displays, in addition to None or L2. If you select L3 as the interface mode, the IP/Netmask field is enabled and you can then assign the primary and secondary IP addresses.
  - A port must be in non-L2 Mode if you are adding the port as a member of a LAG.
  - You cannot change the Interface Mode from **L2** to **none** if the LAG is assigned to a VLAN.

- **L2 Mode** - Select the L2 mode (Access or Trunk).
  - Access mode allows only one VLAN and allows only untagged frames.
  - Trunk mode allows more than one VLAN association and allows tagged frames.
- **Primary** - Enter the primary IP address assigned to an L3 port.

  NOTE
  Primary and secondary IP fields are applicable only to the external ports and the interface mode must be L3 to enable these fields.

- **Secondary** - Enter the secondary IP address (optional). Multiple (secondary) IP addresses help when the interface and port are part of multiple subnets.

5. Continue to configure the following LAG parameters. These parameters are disabled until you add a DCB port to the **LAG members** table.
   - **Mode** - The ports that are LAG members are in either Static or Dynamic mode. You cannot change the mode on existing members of a LAG.

     If the mode is set as Dynamic, you can change the dynamic mode type (to Active or Passive) only for newly-added ports, not for existing port members of a LAG.
   - **Type** - The type value options are **Standard**, where the LAG is limited to 16 ports, and **Brocade**, where the LAG is limited to four ports. The default is **Standard**. The type is set when you add a LAG; you cannot edit the type using the **Edit LAG** dialog box.
6. Click **OK** .

   The **Deploy to LAGs** dialog box displays.
7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected LAG or LAGs.

   NOTE
   If the primary or secondary IP address already exists on another interface, an error message displays in the **Status** area.
9. Click **Close** to close the **Deployment Status** dialog box.

Enabling a DCB port or LAG

If you select multiple switches or multiple ports and LAGs from two or more switches, both the **Enable** button and the **Disable** button are disabled.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select one or more DCB ports or LAGs (which can span multiple switches) that you want to enable.

   NOTE
   All selected LAGs must be in the same state (enabled or disabled); otherwise, both the **Enable** and **Disable** buttons are disabled.

3. Click **Enable.**

   The **Confirmation and Status** dialog box launches with the selected Ports or LAGs.

4. Click **Start** on the **Confirmation and Status** dialog box to save the changes to the selected ports or LAGs.

   The selected DCB ports or LAGs are enabled in the **DCB Configuration** dialog box.

5. Click **Close** to close the **Confirmation and Status** dialog box.

Deleting a LAG

You can only delete a link aggregation group (LAG) that is selected from a single switch. If you select multiple switches or multiple ports from two or more switches, the **Delete** button is disabled.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select one or more LAGs (that can span multiple switches) that you want to delete from the **Products/Ports** table.

3. Click **Delete.**

   The **Confirmation and Status** dialog box launches with the selected LAGs.

4. Click **Start** on the **Confirmation and Status** dialog box to save the changes to the DCB switches.

   The selected LAGs are deleted in the **DCB Configuration** dialog box.

5. Click **Close** to close the **Confirmation and Status** dialog box.

QoS configuration

QoS configuration involves configuring packet classification, mapping the priority and traffic class, controlling congestion, and scheduling. The configuration of these QoS entities consist of DCB Map and Traffic Class Map configuration.

In a Data Center Bridging (DCB) configuration, Enhanced Transmission Selection (ETS) and Priority-based flow control (PFC) are configured by utilizing a priority table, a priority group table, and a priority traffic table. The Traffic Class Map is the mapping of user priority to traffic class.

Enhanced Transmission Selection

Enhanced Transmission Selection (ETS) allows lower priority traffic classes to use available bandwidth not being used by higher priority traffic classes and maximizes the use of available bandwidth.

Priority-based flow control

Priority based flow control (PFC) is an enhancement to the existing pause mechanism in Ethernet. PFC creates eight separate virtual links on the physical link and allows any of these links to be paused and restarted independently, enabling the network to create a no-drop class of service for an individual virtual link.

Table 29 shows examples of how priority grouping might be allocated in a 15-priority group scenario.

TABLE 29 Ppriority grouping allocated in a 15-priority group example

Priority group ID	Bandwidth (%)	Priority flow control
0	55	on
1	25	on
2	0	off
3	0	off
4	5	off
5	0	off
6	15	on
7	0	off
15.0-15.7	Strict priority No bandwidth % configuration allowed	on

Creating a DCB map

This procedure is applicable only for FOS versions lower than FOS 7.0.

When you create a DCB map, each of the Class of Service (CoS) options (0-7) must be mapped to at least one of the Priority Group IDs (0-7) and the total bandwidth must equal 100. All QoS, DCB map, and Traffic map configurations apply to all ports in a LAG.

There can be, at the most, 16 entries in the Priority Group table. Eight of the entries are Strict Priority entries with a Priority Group ID of 15.0 to 15.7 and eight are user-definable entries with a Priority Group ID of 0-7. See Table 29 for an example of priority group configuration.

NOTE
The 10 Gbps DCB/FC switch module can have only one DCB map.

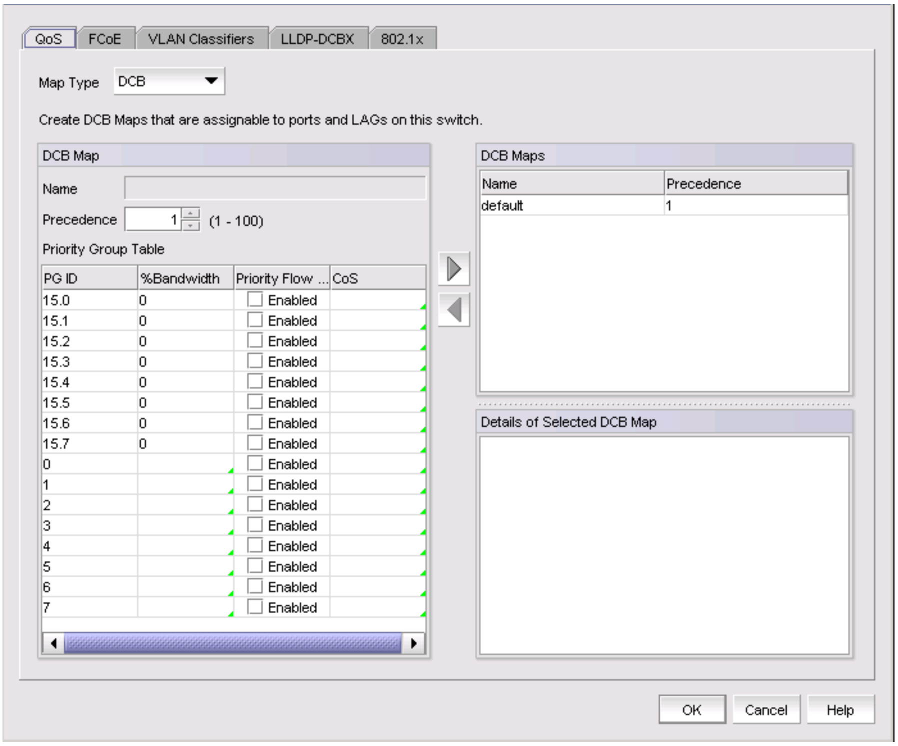
1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit.**

3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.



Map Type DCB

Create DCB Maps that are assignable to ports and LAGs on this switch.

DCB Map

Name

Precedence 1 (1 - 100)

Priority Group Table

PG ID	%Bandwidth	Priority Flow ...	CoS
15.0	0	☐ Enabled	
15.1	0	☐ Enabled	
15.2	0	☐ Enabled	
15.3	0	☐ Enabled	
15.4	0	☐ Enabled	
15.5	0	☐ Enabled	
15.6	0	☐ Enabled	
15.7	0	☐ Enabled	
0		☐ Enabled	
1		☐ Enabled	
2		☐ Enabled	
3		☐ Enabled	
4		☐ Enabled	
5		☐ Enabled	
6		☐ Enabled	
7		☐ Enabled	

DCB Maps

Name	Precedence
default	1

Details of Selected DCB Map

FIGURE 124 QoS, Create DCB Map dialog box

4. Select DCB from the **Map Type** list.
5. Configure the following DCB Map parameters in the **DCB Map** table:
   - **Name** - Enter a name to identify the DCB map. If the switch is a 10 Gbps DCB/FC switch module, you cannot change the name.
   - **Precedence** - Enter a value between 1 - 100. This number determines the map's priority.
   - **Priority Flow Control** check box - Check to enable priority flow control on individual priority groups.
   - **CoS** - Click the CoS cell to launch the **Edit CoS** dialog box, where you can select and assign one or more priorities (PG ID 15.0 through 15.7).

     All of the eight CoS values (0-7) must be used in a DCB map. Duplicate CoS values in two or more priority groups are not allowed.

     NOTE
     You can only edit CoS fields that are displayed with a green tick mark.

     % Bandwidth *(optional)* - While in the **Edit CoS** dialog box, enter a bandwidth value for priority group (PG) IDs 15.00 to 15.7. You must map each CoS to at least one of the PG IDs.

     Note the following points:

     - You cannot define a bandwidth percentage for Strict Priorities (PG ID 15.0 - 15.7). The total % Bandwidth for PG ID 15.0-15.7 must equal 0%.
     - If you set a CoS value to one or more of the PG IDs 0-7, you must also enter a non-0% bandwidth percentage. The total % Bandwidth must equal 100%.
     - For PG IDs 0-7 that do not have an assigned CoS value or PFC enabled, the % Bandwidth must be 0%.
6. Click the right arrow button to add the map to the DCB Maps table.

   If a DCB map exists with the same name, a validation dialog box launches and you are asked if you want to overwrite the map.
7. Click **OK**.
8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Editing a DCB map

1. Select **Configure** > **DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.
4. Select a DCB Map from the **DCB Maps** table, and click the left arrow button to load its values to the left pane. The fields are now editable.

5. Keep the same DCB Map name and modify the following values, as required. See Table 29 for an example of priority group configuration.
    - **Name** - Enter a name to identify the DCB map. If the switch is a 10 Gbps DCB/FC switch module, you cannot change the name.
    - **Precedence** - Enter a value between 1 - 100. This number determines the map's priority.
    - **% Bandwidth** - Enter a bandwidth value for priority group IDs 0-7. The total of all priority groups must equal 100%.
    - **Priority Flow Control** check box - Check to enable priority flow control on individual priority groups.
    - **CoS** - Click the CoS cell to launch the **Edit CoS** dialog box, where you can select and assign one or more priorities (PG ID 15.0 through 15.7).
    - All of the eight CoS values (0-7) must be used in a DCB map. Duplicate CoS values in two or more priority groups are not allowed.
6. Click the right arrow button to re-add the map to the DCB Maps table.

    If the DCB Map already exists, an overwrite message displays.
7. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Deleting a DCB map

You cannot delete the DCB map of a 10 Gbps DCB/FC switch module. To delete the DCB map of an 8 Gbps DCB switch, complete the following steps.

1. Select **Configure** > **DCB** from the menu bar.

    The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

    The **QoS** dialog box displays.
4. Select one or more DCB maps.
5. Click the left arrow button.

    The selected DCB Map row is removed from the table.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.

    NOTE
    With Fabric OS (FOS) version 7.0 and higher, there is only one DCB Map (the default), which you cannot delete.
7. Click **OK** after changing the attributes of the current deployment.

    The **Deployment Status** dialog box launches.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.
9. Click **Close** to close the **Deployment Status** dialog box.

Assigning a DCB map to a port or link aggregation group

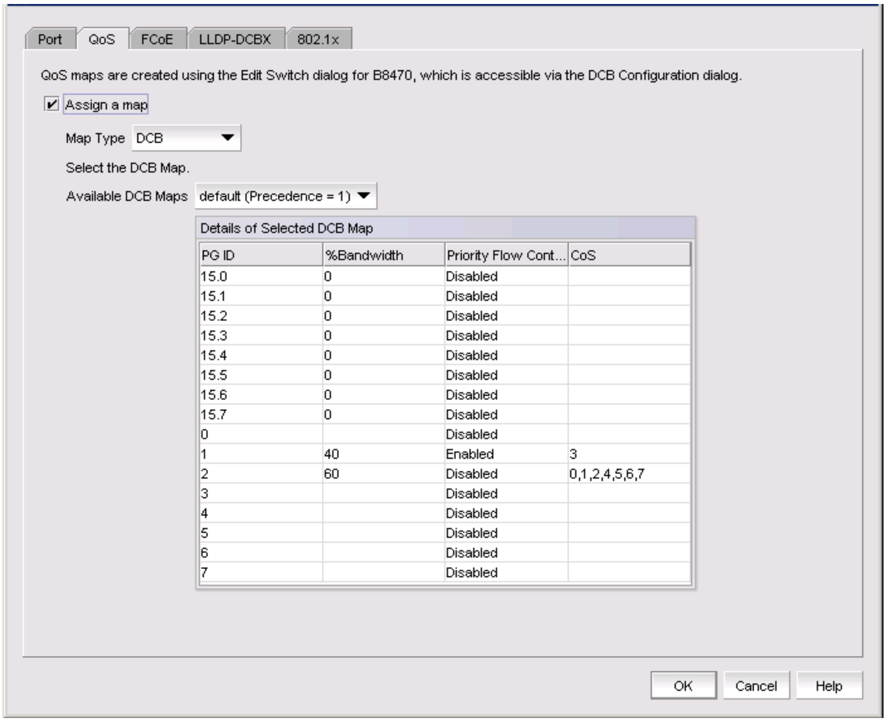
A port can have either a DCB map or a Traffic Class map assigned to it, but it cannot have both.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the **QoS** tab on the **Edit Port** dialog box.

   The **QoS** dialog box displays.



QoS maps are created using the Edit Switch dialog for B8470, which is accessible via the DCB Configuration dialog.

☑ Assign a map

Map Type: DCB

Select the DCB Map.

Available DCB Maps: default (Precedence = 1)

Details of Selected DCB Map

PG ID	%Bandwidth	Priority Flow Cont...	CoS
15.0	0	Disabled	
15.1	0	Disabled	
15.2	0	Disabled	
15.3	0	Disabled	
15.4	0	Disabled	
15.5	0	Disabled	
15.6	0	Disabled	
15.7	0	Disabled	
0		Disabled	
1	40	Enabled	3
2	60	Disabled	0,1,2,4,5,6,7
3		Disabled	
4		Disabled	
5		Disabled	
6		Disabled	
7		Disabled	

FIGURE 125 QoS, Assign a DCB Map to a port dialog box

4. Click the **Assign a map** check box.

   If you do not enable this check box, all QoS edit features are disabled.

5. Select **DCB Map** in the **Map Type** list.
6. Select a DCB Map in the **Available DCB Maps** list.

   If no DCB maps were created on the switch, the **Available DCB Maps** list is empty.

7. When you have finished the configuration, click **OK** to launch the **Deploy to Ports/LAGs** dialog box, shown in Figure 134.

Creating a traffic class map

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select **Traffic Class** from the **Map Type** list.
5. Name the Traffic Class map.
6. Click the Traffic Class cell in a CoS row and directly enter a value from 0-7. You can leave the cell empty to indicate zero (0).
7. Click the right arrow button to add the map to the **Traffic Class Maps** table.

   If the name of the Traffic Class map already exists, an overwrite warning message displays. Click **Yes** to overwrite the existing Traffic Class map.

8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Editing a traffic class map

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a Traffic Class Map from the **Traffic Class Maps** table, and click the left arrow button to load its values to the left pane. The fields are now editable.

   If the name of the Traffic Class map already exists, an overwrite warning message displays. Click **Yes** to overwrite the existing Traffic Class map.

5. Keep the same Traffic Class Map name and modify the values, as required.
6. Click the right arrow button to re-add the map to the Traffic Class Maps table.
7. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Deleting a traffic class map

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.

4. Select a Traffic Class Map that you want to delete from the **Traffic Class Maps** table.
5. Click the left arrow button.

   The selected DCB Map row is removed from the table.

6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.
7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.

8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.

Assigning a traffic class map to a port or link aggregation group

You can assign a Traffic Class map to a port or ports under the LAG; however, a port does not *require* a Traffic Class map be assigned to it. A port can have either a DCB map or a Traffic Class map assigned to it, but it cannot have both.

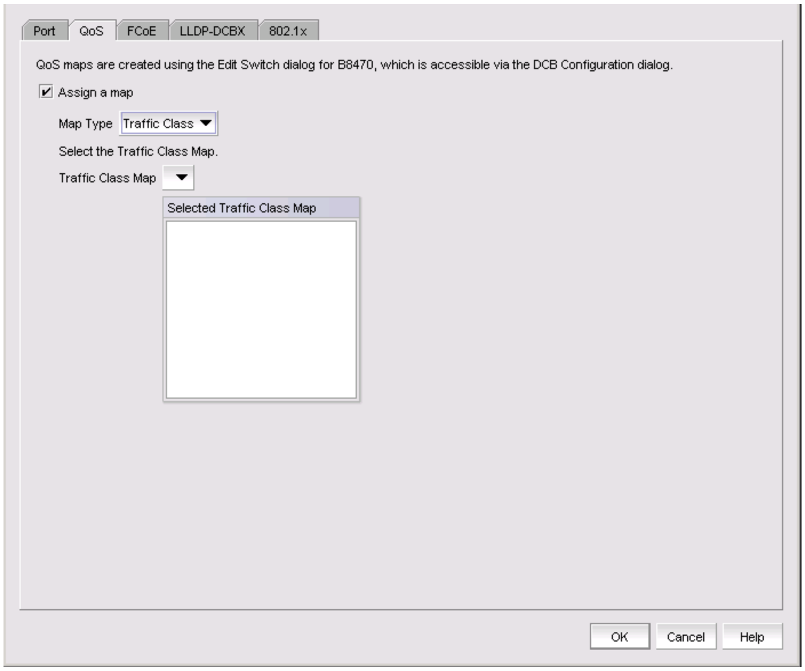
NOTE
You cannot configure QoS or LLDP-DCBX on a LAG.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a port or LAG, and click **Edit**.
3. Click the **QoS** tab on the **Edit Switch** dialog box.

   The **QoS** dialog box displays.



QoS maps are created using the Edit Switch dialog for B8470, which is accessible via the DCB Configuration dialog.

☑ Assign a map

Map Type Traffic Class

Select the Traffic Class Map.

Traffic Class Map

Selected Traffic Class Map

FIGURE 126 QoS, assign a traffic class map to a port dialog box

4. Click the **Assign a map** check box.
5. Select **Traffic Class** in the **Map Type** list.
6. Select a Traffic Class Map in the **Traffic Class Map** list.
7. When you have finished the configuration, click **OK** to launch the **Deploy to Ports/LAGs** dialog box. Refer to “Product, Port, and LAG Deployment” on page 379 for more information.

FCoE provisioning

The Management application supports FCoE provisioning only on Fabric OS (FOS) version 6.3.1_dcb. However, the Brocade command line interface supports FCoE provisioning for the following versions of FOS: FOS 6.3.1_cee, FOS 6.4.1_fcoe, and FOS 7.0.0. Refer to the *Fabric OS Command Reference Manual* for CLI procedures.

FCoE provisioning simplifies the number of steps required to configure a DCB port to carry the FCoE traffic. The FCoE map contains the default DCB Map and the VLAN ID. You can change the default VLAN ID using the FCoE tab of the Edit Switch dialog box, shown in Figure 127.

NOTE
The default DCB map associated with the default FCoE map can be edited on the switch from the QoS tab.

Changing the VLAN ID on the default FCoE map

You can change the VLAN ID on the default FCoE map only when no ports or LAGs are participating as members of the switch. You must first manually remove the FCoE Map option for each of the port members before you change the VLAN ID on the switch.

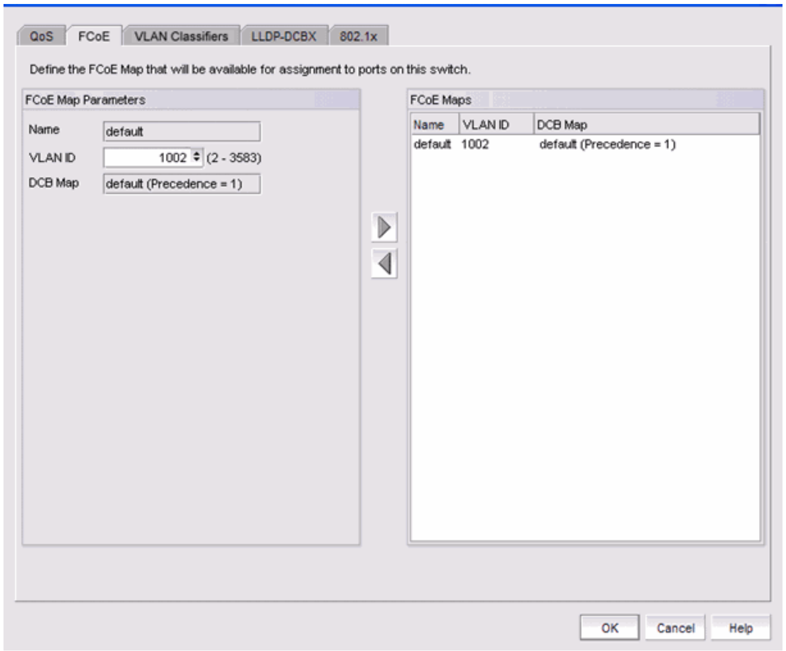
1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit**.

3. Click the **FCoE tab** on the **Edit Switch** dialog box.

   The **Edit Switch** dialog box, FCoE tab displays, as shown in Figure 127.



Define the FCoE Map that will be available for assignment to ports on this switch.

FCoE Map Parameters

Name: default

VLAN ID: 1002 (2 - 3583)

DCB Map: default (Precedence = 1)

FCoE Maps

Name	VLAN ID	DCB Map
default	1002	default (Precedence = 1)

FIGURE 127 Edit Switch dialog box - FCoE tab

4. Accept the default VLAN ID of 1002, or change the value. The valid VLAN ID range is from 2 through 3583.

5. Click the right arrow button to move the FCoE map parameters into the FCoE Maps list.

6. When you have finished the configuration, click OK to launch the **Deploy to Products** dialog box.

7. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.

8. Click **Start** on the Deployment Status dialog box to save the changes to the selected devices.

Enabling or disabling the FCoE map on the port

You must first manually disable an FCoE map-enabled port if you want to edit the VLAN ID of the FCoE map. See "Changing the VLAN ID on the default FCoE map" on page 366 for information on editing the VLAN ID using the Edit Switch dialog box, FCoE tab.

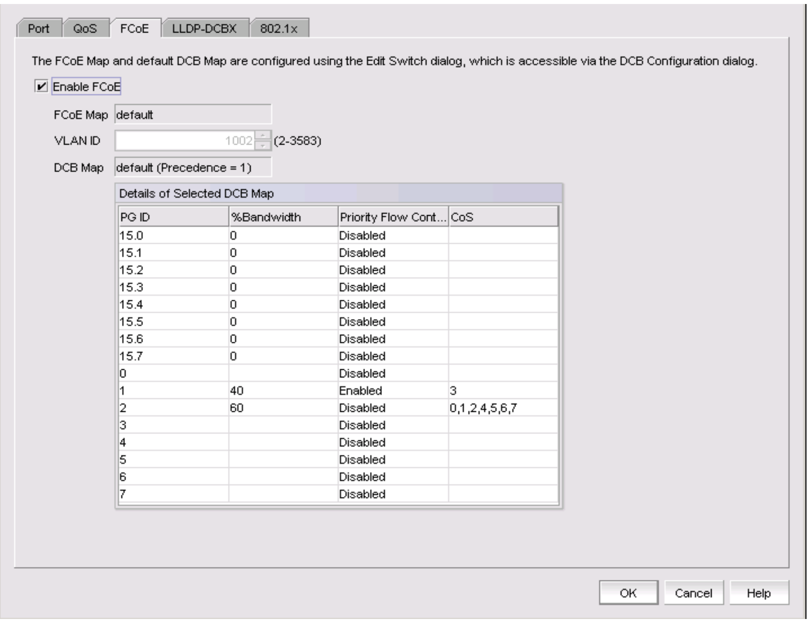
1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a port and click **Edit.**

3. Click the **FCoE tab** on the **Edit Port** dialog box.

   The **Edit Port** dialog box, **FCoE** tab displays, as shown in Figure 128.



The FCoE Map and default DCB Map are configured using the Edit Switch dialog, which is accessible via the DCB Configuration dialog.

☑ Enable FCoE

FCoE Map: default

VLAN ID: 1002 (2-3583)

DCB Map: default (Precedence = 1)

Details of Selected DCB Map

PG ID	%Bandwidth	Priority Flow Cont...	CoS
15.0	0	Disabled	
15.1	0	Disabled	
15.2	0	Disabled	
15.3	0	Disabled	
15.4	0	Disabled	
15.5	0	Disabled	
15.6	0	Disabled	
15.7	0	Disabled	
0		Disabled	
1	40	Enabled	3
2	60	Disabled	0,1,2,4,5,6,7
3		Disabled	
4		Disabled	
5		Disabled	
6		Disabled	
7		Disabled	

FIGURE 128 Edit Port dialog box - FCoE tab

4. If enabled, click the **Enable FCoE** check box to disable the port's membership on the FCoE map.

5. When you have finished the configuration, click **OK** to launch the **Deploy to Ports** dialog box.

6. Click **OK** after changing the attributes of the current deployment.

   The **Deployment Status** dialog box launches.

7. Click **Start** on the Deployment Status dialog box to save the changes to the selected devices.

VLAN classifier configuration

The Management application supports VLAN classifier management only on Fabric OS (FOS) version 6.3.1_dcb and FOS 7.0.0.

VLAN classifier rules are used to define specific rules for classifying untagged packets to selected VLANs based on protocol and MAC addresses. The classified frames are then tagged with a VLAN ID.

VLAN classifier rules can be categorized into the following areas:

- 802.1Q protocol-based classifier rules
- MAC address-based classifier rules

VLAN classifiers are created on per-switch basis. The **VLAN Classifiers** tab of the **Edit Switch** dialog box allows you to create rules and group them into VLAN classifiers, which can then be applied to access port and LAG VLAN members and converged port VLAN members.

NOTE
The **VLAN Classifiers** tab on the **Edit Switch** dialog box displays only on switches with Fabric OS (FOS) versions 7.0.0 and later.

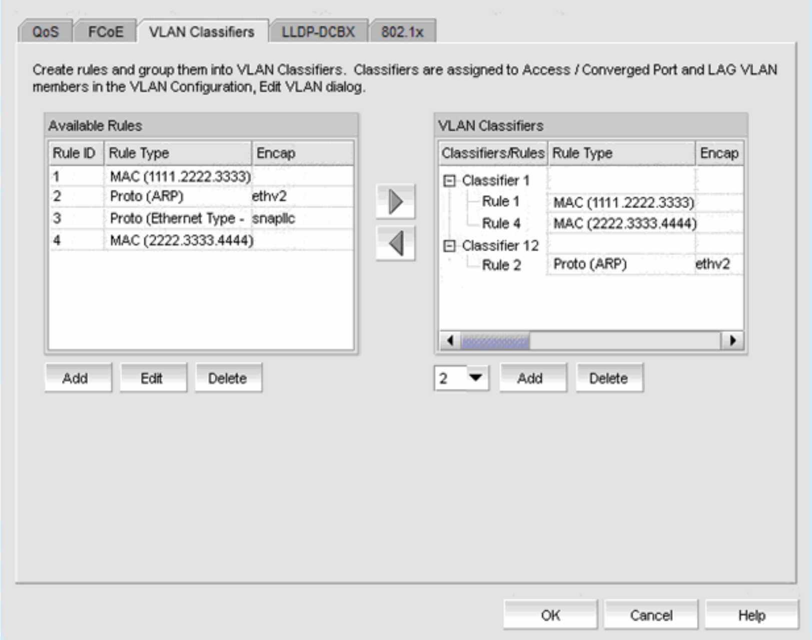
Adding a VLAN classifier rule

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit**.
3. Click the **VLAN Classifiers tab** on the **Edit Switch** dialog box.

   The **Edit Switch** dialog box, **VLAN Classifiers** tab displays, as shown in Figure 129.



Create rules and group them into VLAN Classifiers. Classifiers are assigned to Access / Converged Port and LAG VLAN members in the VLAN Configuration, Edit VLAN dialog.

Available Rules

Rule ID	Rule Type	Encap
1	MAC (1111.2222.3333)	
2	Proto (ARP)	ethv2
3	Proto (Ethernet Type -	snapllc
4	MAC (2222.3333.4444)	

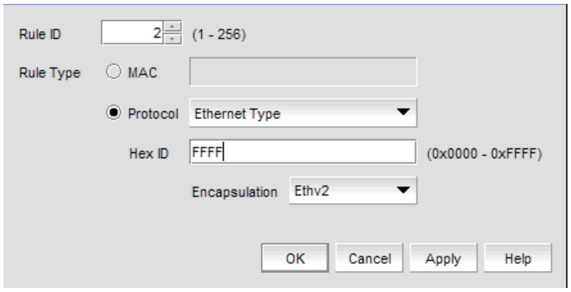
VLAN Classifiers

Classifiers/Rules	Rule Type	Encap
⊟ Classifier 1		
Rule 1	MAC (1111.2222.3333)	
Rule 4	MAC (2222.3333.4444)	
⊟ Classifier 12		
Rule 2	Proto (ARP)	ethv2

FIGURE 129 Edit Switch dialog box, VLAN Classifiers tab

4. Click the **Add** button under the **Available Rule** list.

   The **Add Rules** dialog box displays, as shown in Figure 130.



Rule ID 2 (1 - 256)

Rule Type ○ MAC

● Protocol Ethernet Type

Hex ID FFFF (0x0000 - 0xFFFF)

Encapsulation Ethv2

FIGURE 130 Add Rules dialog box

The **Rule ID** field is pre-populated with the next available Rule ID number.

5. Keep the Rule ID number as it is, or change the number using a value between 1 through 256.
6. Select a rule type. Valid rule types are MAC (MAC address-based rule) and Proto (802.1Q protocol-based rule).
7. If **Ethernet Type** is selected as the Protocol rule type, enter any valid four-digit hexadecimal value within the allowed range of 0x0000 through 0xFFFF. For the other Proto options, the hex ID value is hard-coded as follows:
   - ARP—0x0808
   - IP—0x8881
   - IPv6—0x86DD
8. Select an encapsulation type from the list. Options include Ethv2, nosnapllc, and snapllc. Encap only accepts a value when Protocol is selected as the rule type.

9. Click **OK** to add the rule to the **Available Rules** list on the **VLAN Classifiers** dialog box and close the **Add Rules** dialog box.

NOTE
Clicking **Apply** also adds the rule to the **Available Rules** list on the **VLAN Classifiers** dialog box, and in addition, the **Add Rules** dialog box remains open and clears all entries for you to define the next rule.

10. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Editing a VLAN classifier rule

1. From the **VLAN Classifiers** dialog box, select a row in the **Available Rules** table and click **Edit**.

   The **Edit Rule** dialog box displays with the fields pre-populated with the rule details. The **Rule ID** field is disabled.

2. Edit the rule type and protocol type as required. If Ethernet is selected as the rule type, enter any valid four-digit hexadecimal value within the allowed range of 0x0000 through 0xFFFF. For the other Proto options, the hex ID value is hard-coded as follows:

   - ARP—0x0808
   - IP—0x8881
   - IPv6—0x86DD

3. Select an encapsulation type from the list. Options include Ethv2, nosnapllc, and snapllc. Encap only accepts a value when Protocol is selected as the rule type.

4. Click **OK** to add the edited rule to the **Available Rules** list on the **VLAN Classifiers** dialog box and close the **Edit Rules** dialog box.

5. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Deleting a VLAN classifier rule

1. From the **VLAN Classifiers** dialog box, select a row in the **Available Rules** table and click **Delete**.

   A message displays if the rules are participating in VLAN classifier groups that are currently associated with VLAN port or LAG members.

2. Click **Yes** to remove the selected rule row from the table.

3. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Creating a VLAN classifier group

You can assign existing rules to a selected VLAN classifier and form a VLAN classifier group. If no rules are available, you can add rules to a selected switch using the **Add Rules** dialog box.

1. Select **Configure** > **DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit.**
3. Click the **VLAN Classifiers tab** on the **Edit Switch** dialog box.

   The **Edit Switch** dialog box, **VLAN Classifiers** tab displays, as shown in Figure 129.

4. Select a Classifier ID from the VLAN Classifier list. Values range from 1 through 16.
5. Click the **Add** button under the VLAN Classifier list.

   The classifier with the selected ID is displayed in the VLAN Classifier list.

6. Select the classifier from the VLAN Classifier list and then select the rules you want to add under this classifier from the VLAN Classifier Rules list.
7. Click the right arrow button.

   The selected rules are assigned to the selected VLAN Classifier ID in the VLAN Classifier list.

8. When you have finished the configuration, click OK to launch the **Deploy to Products** dialog box, shown in Figure 134.

Deleting a VLAN classifier group

1. Click the **VLAN Classifiers tab** on the **Edit Switch** dialog box.

   The **Edit Switch** dialog box, **VLAN Classifiers** tab displays, as shown in Figure 129.

2. Select a classifier from the **VLAN Classifiers** list.
3. Click **Delete.**

   The VLAN Classifier group is deleted.

4. When you have finished the configuration, click OK to launch the **Deploy to Products** dialog box, shown in Figure 134.

LLDP-DCBX configuration

Link Layer Discovery Protocol (LLDP) provides a solution for the configuration issues caused by increasing numbers and types of network devices in a LAN environment, because, with LLDP, you can statically monitor and configure each device on a network.

Data Center Bridging Capability Exchange Protocol (DCBX) enables Enhanced Ethernet devices to discover whether a peer device supports particular features, such as Priority Flow Control or Class of Service (CoS). In a Data Center Bridging (DCB) environment, LLDP is enhanced with DCBX protocol to further share or change the configured DCB enhancements. You must enable the DCBX protocol and configure certain parameters in order to effectively utilize the benefits of a converged network.

Using the **LLDP-DCBX** dialog box, you can create and manage LLDP profiles and assign a LLDP profile to a port or link aggregation group (LAG).

Configuring LLDP for FCoE

To configure LLDP for FCoE, complete the following steps.

NOTE
When a TE port is selected to assign to an LLDP profile, a yellow banner displays with the following error message: “LLDP-DCBX is disabled on this switch. The configuration becomes functional when LLDP-DCBX is enabled on the switch.”

1. Select **Configure > DCB**.

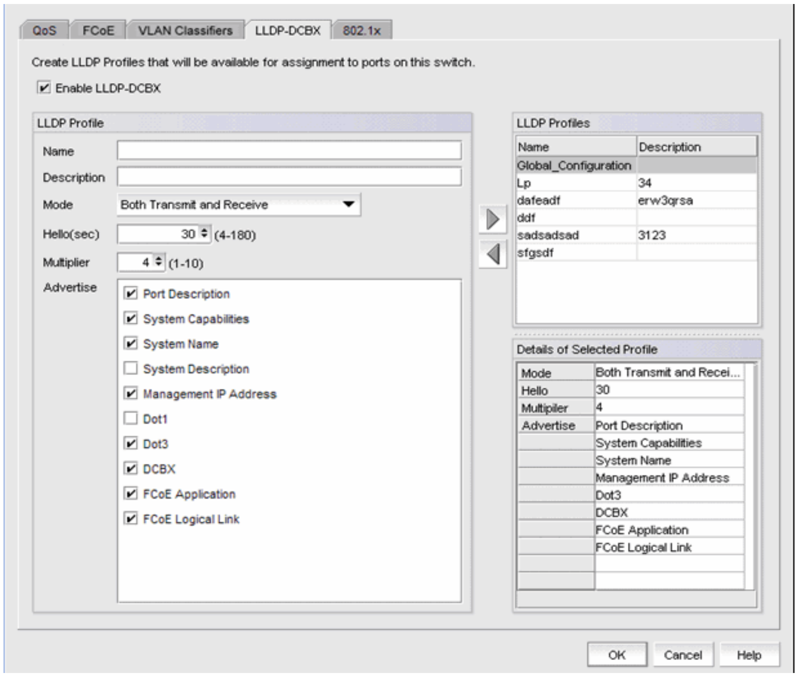
   The **DCB Configuration** dialog box displays.

2. Select the switch to edit in the **DCB Ports and LAGs** table and click **Edit**.

   The **Edit Switch** dialog box displays.

3. Click the **LLDP-DCBX** tab.

4. Click the **Enable LLDP-DCBX** check box.



Create LLDP Profiles that will be available for assignment to ports on this switch.

☑ Enable LLDP-DCBX

LLDP Profile

Name

Description

Mode: Both Transmit and Receive

Hello(sec): 30 (4-180)

Multiplier: 4 (1-10)

Advertise:
- ☑ Port Description
- ☑ System Capabilities
- ☑ System Name
- □ System Description
- ☑ Management IP Address
- □ Dot1
- ☑ Dot3
- ☑ DCBX
- ☑ FCoE Application
- ☑ FCoE Logical Link

LLDP Profiles

Name	Description
Global_Configuration	
Lp	34
dafeadf	erw3qrsa
ddf	
sadsadsad	3123
sfgsdf	

Details of Selected Profile

Mode	Both Transmit and Recei...
Hello	30
Multipiler	4
Advertise	Port Description
	System Capabilities
	System Name
	Management IP Address
	Dot3
	DCBX
	FCoE Application
	FCoE Logical Link

FIGURE 131 **Edit Switch dialog box - LLDP-DCBX tab**

5. Select the **Global Configuration** LLDP profile in the **LLDP Profiles** table.
6. Click the left arrow button to edit.
7. Select the **FCoE Application** and **FCoE Logical Link** check boxes in the **Advertise** table to advertise them on the network.
8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Adding an LLDP profile

NOTE
When a TE port is selected to assign to an LLDP profile, a yellow banner displays with the following error message: "LLDP-DCBX is disabled on this switch. The configuration becomes functional when LLDP-DCBX is enabled on the switch."

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

   The **LLDP-DCBX** dialog box displays.
4. Click the **Enable LLDP-DCBX** checkbox.

5. Configure the LLDP Profile parameters:
   - **Name** - Type a name for the LLDP profile.

     If the name of the LLDP profile already exists on the switch, an overwrite warning displays.
   - **Description** - Type a meaningful description of the LLDP profile.
   - **Mode** - Select a mode from the list: Tx (transmitted) or Rx (received).
   - **Hello** - Enter a hello interval time for the bridge. The value range is 4-180 and the default value is 30.
   - **Multiplier** - Enter a multiplier. The value range is 1-10 and the default is 4.
   - **Advertise** - Check the profile parameters that you want to display as part of the LLDP profile:
     - Port description - The user-configured port description.
     - System name - The user-configured name of the local system.
     - System capabilities - The system capabilities running on the system.
     - System description - The system description containing information about the software running on the system.
     - Management IP address - The IP management address of the local system.
     - Dot 1..Dot 3 -
     - DCBX - The DCBX profiles.
     - FCoE application - The FCoE application feature.
     - FCoE logical link - The logical link level for the SAN network.
6. Click the right arrow button to move the newly created profile into the DBCX Profiles table.
7. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Editing an LLDP profile

1. Select **Configure** > **DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.

   The **LLDP Profile** dialog box displays.
4. Select an LLDP Profile in the **LLDP Profile** table.

   NOTE
   You can edit the <Global Configuration> profile. You cannot, however, delete or duplicate global configurations.
5. Click the left arrow to load the LLDP Profile's values to the left pane.
6. Modify the values, as described in "Adding an LLDP profile" on page 373. You are not allowed to modify the LLDP Profile's name.

7. Click the right arrow to update the LLDP Profile parameters.
8. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Deleting an LLDP profile

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a switch, and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Switch** dialog box.
4. Select an existing LLDP Profile from the **LLDP Profiles** table in the upper right pane.

   NOTE
   You cannot delete <Global Configurations>. You can, however, edit global configurations. For more information, see “” on page 374.
5. Click the left arrow button.

   The selected LLDP profile is removed from the table.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box.
7. Click **OK**.

   The **Deployment Status** dialog box launches.
8. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.
9. Click **Close** to close the **Deployment Status** dialog box.

Assigning an LLDP profile to a port or ports in a LAG

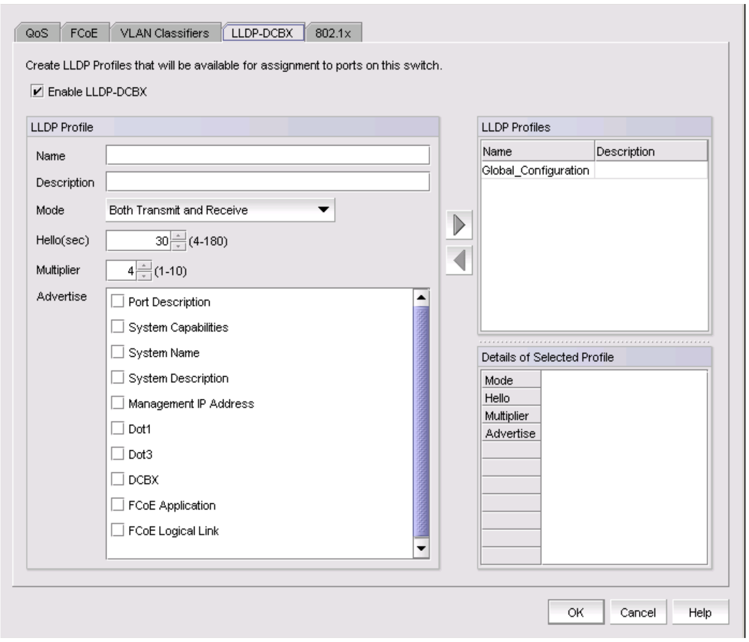
You create LLDP profiles using the **Edit Switch** dialog box, which you access from the **DCB Configuration** dialog box. Global configuration parameters, which is the default selection, are displayed in the Assigned Profile table shown in Figure 132.

NOTE
A yellow banner displayed on the **LLDP-DCBX** dialog box indicates that LLDP-DCBX is disabled on the switch. The configuration options become functional when LLDP-DCBX is enabled on the switch.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.
2. Select a port or link aggregation group (LAG), and click **Edit**.
3. Click the **LLDP-DCBX** tab on the **Edit Port/Edit LAG** dialog box.

   The **Assign an LLDP profile** dialog box displays.



Create LLDP Profiles that will be available for assignment to ports on this switch.

☑ Enable LLDP-DCBX

Name

Description

Mode: Both Transmit and Receive

Hello(sec): 30 (4-180)

Multiplier: 4 (1-10)

Advertise:
- ☐ Port Description
- ☐ System Capabilities
- ☐ System Name
- ☐ System Description
- ☐ Management IP Address
- ☐ Dot1
- ☐ Dot3
- ☐ DCBX
- ☐ FCoE Application
- ☐ FCoE Logical Link

Name	Description
Global_Configuration	

Mode	
Hello	
Multiplier	
Advertise	

FIGURE 132 Assign an LLDP profile dialog box

4. Click **Assign an LLDP profile to <port name>** button to enable the feature.

NOTE
Assign the Global Configuration is the default. The **Available Profiles** list is disabled if global configuration is selected. In addition, the **Assign an LLDP profile** button is disabled if no LLDP profiles exist on the switch.

5. Select an LLDP profile from the **Available Profiles** list.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Ports/LAGs** dialog box. Refer to "Product, Port, and LAG Deployment" on page 379 for more information.

802.1x authentication

802.1x is a standard authentication protocol that defines a client-server-based access control and authentication protocol. 802.1x restricts unknown or unauthorized clients from connecting to a LAN through publicly accessible ports.

NOTE
802.1x is not supported for internal ports.

A switch must be enabled for 802.1x authentication before you configure its parameters. See "Setting 802.1x parameters for a port" for more information.

Enabling 802.1x authentication

802.1x authentication is enabled or disabled globally on the switch using the **Edit Switch** dialog box.

1. Select **Configure** > **DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit.**
3. Click the 802.1x tab on the **Edit Switch** dialog box.
4. Click the **Enable 802.1x** check box to enable 802.1x authentication, and click **OK.**
5. Configure the 802.1x parameters, which are described in "Setting 802.1x parameters for a port" on page 378.
6. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Disabling 802.1x authentication

1. Select **Configure** > **DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch and click **Edit.**
3. Click the 802.1x tab on the **Edit Switch** dialog box.
4. Clear the **Enable 802.1x** check box to disable 802.1x authentication.
5. When you have finished the configuration, click **OK** to launch the **Deploy to Products** dialog box, shown in Figure 134.

Setting 802.1x parameters for a port

The 802.1x parameters can be configured whether the feature is enabled on the switch. The default parameters are initially populated when 802.1x is enabled, but you can change the default values as required.

1. Select **Configure > DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

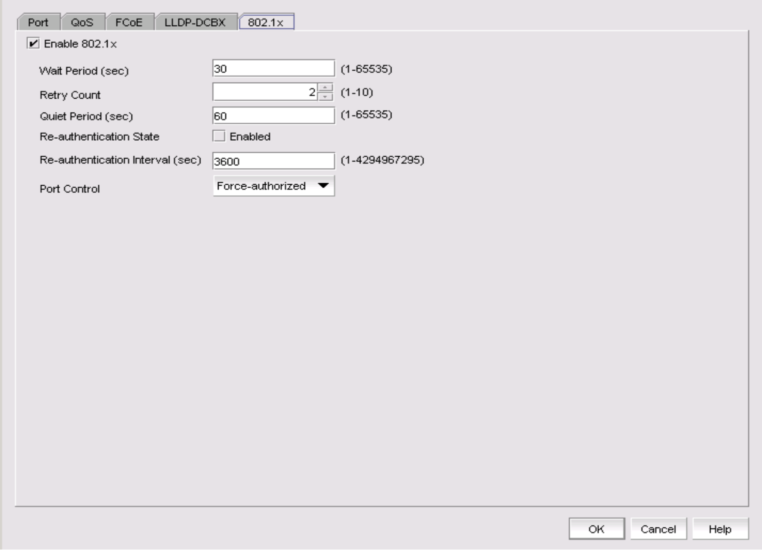
2. Select a port and click **Edit.**

3. Click the 802.1x tab on the **Edit Port** dialog box.

   The **Enable 802.1x** dialog box displays.

4. Click the **Enable 802.1x** check box to enable 802.1x authentication.

   The **802.1x** parameters are enabled for editing.



☑ Enable 802.1x

Wait Period (sec) 30 (1-65535)

Retry Count 2 (1-10)

Quiet Period (sec) 60 (1-65535)

Re-authentication State □ Enabled

Re-authentication Interval (sec) 3600 (1-4294967295)

Port Control Force-authorized

FIGURE 133 802.1x dialog box

5. Configure the following 802.1x parameters:

   - **Wait Period** - The number of seconds the switch waits before sending an EAP request. The value range is 15 to 65535 seconds. The default value is 30.
   - **Retry Count** - The maximum number of times that the switch restarts the authentication process before setting the switch to an unauthorized state. The value range is 1 to 10. The default value is 2.
   - **Quiet Period** - The number of seconds that the switch remains in the quiet state after a failed authentication exchange with the client. The value range is 1 to 65535 seconds. The default value is 60.
   - **Re-authentication State** - Enable or disable the periodic re-authentication of the client. The default is Disable.

- **Re-authentication Interval** - The number of seconds between re-authentication attempts. The value range is 1 to 4294967295. The default value is 3600 seconds. This feature is not dependent on the re-authentication state being enabled.
- **Port Control** - Select an authorization mode from the list to configure the ports for authorization. Options include auto, force-authorized, or force-unauthorized and the default value is auto.

6. When you have finished the configuration, click **OK** to launch the **Deploy to Ports** dialog box. Refer to "Product, Port, and LAG Deployment" on page 379 for more information.

Product, Port, and LAG Deployment

The **Deploy to Products**, **Deploy to Ports**, and **Deploy to LAGs** dialog boxes provide the flexibility to commit DCB configurations either right away or at a scheduled time. These dialog boxes also allow you to commit the switch-level configuration changes to one or more target switches.

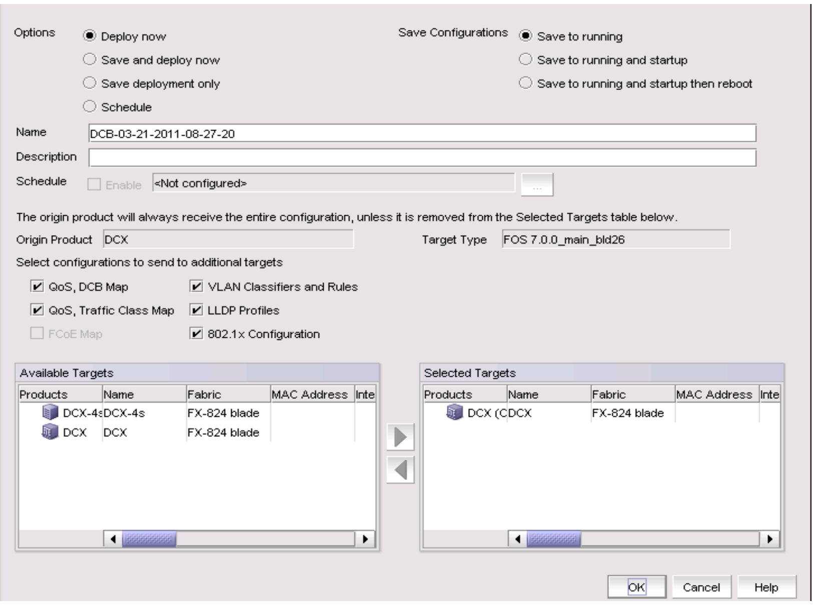
Deploying DCB product, port, and LAG configurations

The switch, port, and LAG deployment dialog boxes provide common deployment options, save configuration options, and schedule options. Depending on which product, port, or LAG you select, the **Deploy to Products**, **Deploy to Ports**, or **Deploy to LAGs** dialog box displays upon deployment.

1. Select **Configure** > **DCB** from the menu bar.

   The **DCB Configuration** dialog box displays, showing the status of all DCB-related hardware and functions.

2. Select a switch, port, or LAG, and click **Edit**.
3. Configure the switch, port, or LAG. When you have finished the configuration, click **OK** to launch the appropriate dialog box. Refer to "Product, Port, and LAG Deployment" on page 379.



Options
● Deploy now
○ Save and deploy now
○ Save deployment only
○ Schedule

Save Configurations
● Save to running
○ Save to running and startup
○ Save to running and startup then reboot

Name: DCB-03-21-2011-08-27-20
Description:
Schedule: □ Enable <Not configured>

The origin product will always receive the entire configuration, unless it is removed from the Selected Targets table below.

Origin Product: DCX
Target Type: FOS 7.0.0_main_bld26

Select configurations to send to additional targets
☑ QoS, DCB Map
☑ QoS, Traffic Class Map
□ FCoE Map
☑ VLAN Classifiers and Rules
☑ LLDP Profiles
☑ 802.1x Configuration

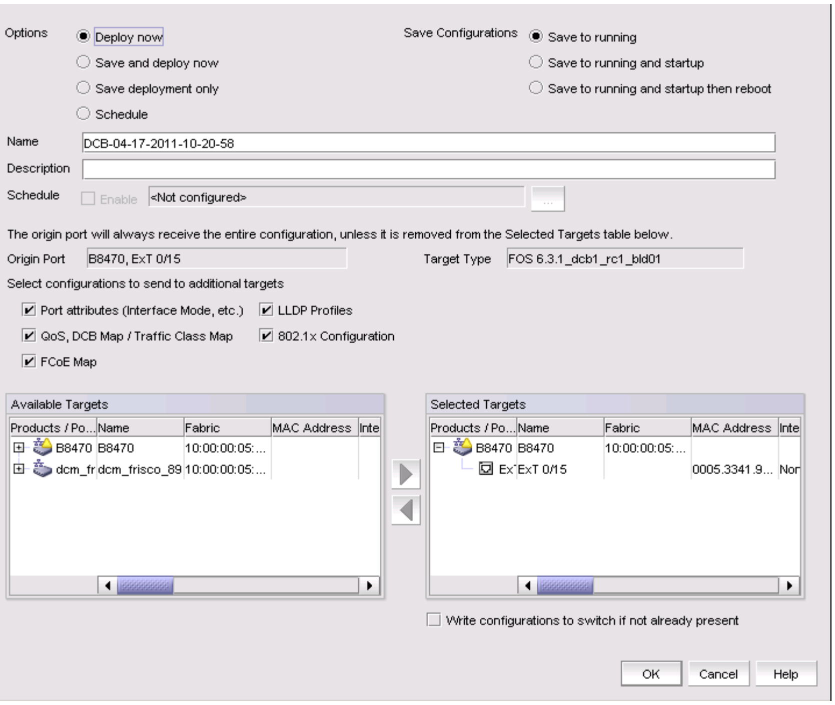
Available Targets

Products	Name	Fabric	MAC Address	Inte
DCX-4s	DCX-4s	FX-824 blade		
DCX	DCX	FX-824 blade		

Selected Targets

Products	Name	Fabric	MAC Address	Inte
DCX (CDCX		FX-824 blade		

FIGURE 134 Deploy to Products dialog box



Options
● Deploy now
○ Save and deploy now
○ Save deployment only
○ Schedule

Save Configurations
● Save to running
○ Save to running and startup
○ Save to running and startup then reboot

Name: DCB-04-17-2011-10-20-58
Description:
Schedule: □ Enable <Not configured>

The origin port will always receive the entire configuration, unless it is removed from the Selected Targets table below.

Origin Port: B8470, ExT 0/15
Target Type: FOS 6.3.1_dcb1_rc1_bld01

Select configurations to send to additional targets
☑ Port attributes (Interface Mode, etc.)
☑ QoS, DCB Map / Traffic Class Map
☑ FCoE Map
☑ LLDP Profiles
☑ 802.1x Configuration

Available Targets

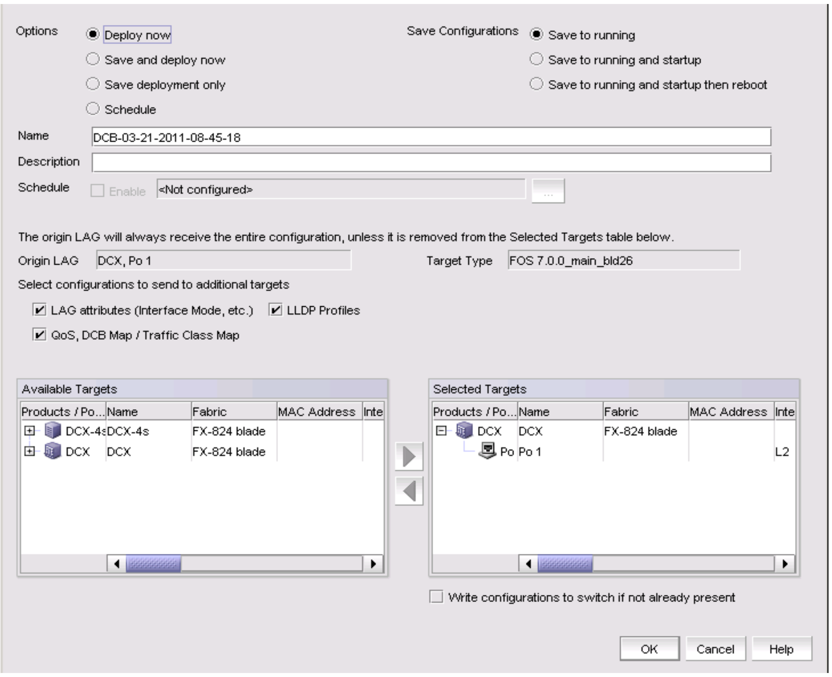
Products / Po...	Name	Fabric	MAC Address	Inte
⊞ B8470	B8470	10:00:00:05:...		
⊞ dcm_fr	dcm_frisco_89	10:00:00:05:...		

Selected Targets

Products / Po...	Name	Fabric	MAC Address	Inte
⊟ B8470	B8470	10:00:00:05:...		
Ex	ExT 0/15		0005.3341.9...	Nor

□ Write configurations to switch if not already present

FIGURE 135 Deploy to Ports dialog box



Options ● Deploy now ○ Save and deploy now ○ Save deployment only ○ Schedule

Save Configurations ● Save to running ○ Save to running and startup ○ Save to running and startup then reboot

Name: DCB-03-21-2011-08-45-18

Description:

Schedule: □ Enable <Not configured>

The origin LAG will always receive the entire configuration, unless it is removed from the Selected Targets table below.

Origin LAG: DCX, Po 1   Target Type: FOS 7.0.0_main_bld26

Select configurations to send to additional targets

☑ LAG attributes (Interface Mode, etc.) ☑ LLDP Profiles

☑ QoS, DCB Map / Traffic Class Map

Available Targets

Products / Po...	Name	Fabric	MAC Address	Inte
⊞ DCX-4s	DCX-4s	FX-824 blade		
⊞ DCX	DCX	FX-824 blade		

Selected Targets

Products / Po...	Name	Fabric	MAC Address	Inte
⊟ DCX	DCX	FX-824 blade		
Po	Po 1			L2

□ Write configurations to switch if not already present

FIGURE 136 Deploy to LAGs dialog box

4. Click one of the following deployment options:
   - Deploy now
   - Save and deploy now
   - Save deployment only
   - Schedule
5. Click one of the following save configuration options:
   - Save to running
   - Save to running and startup
   - Save to running and startup then reboot

   The name for the scheduled product deployment is pre-populated with a “DCB-MM-DD-YYYY-HR-MIN-SS” prefix. This is an editable field.
6. Provide a description for the product/port/LAG deployment.
7. If the **Schedule** option is selected, click the **Use** check box for one-time deployment. One-time deployment is the only option.

   The name of the origin product is a read-only field. The origin product receives the entire configuration, unless it is removed from the **Selected Targets** list.

8. Select one or more of the following configurations, to be deployed on the selected targets:

   For switches:

   - QoS, DCB Map
   - QoS, Traffic Class Map
   - FCoE Map
   - VLAN Classifiers and Rules
   - LLDP Profiles
   - 802.1x Configuration

   NOTE
   See "Source to target switch FOS version compatibility for deployment" for restrictions.

   For ports:

   - Port attributes (interface mode, etc.)
   - QoS, DCB Map / Traffic Class Map
   - FCoE Map
   - LLDP Profiles
   - 802.1x Configuration

   NOTE
   On the **Deploy to Ports** dialog box, you can write port configurations to the switch by enabling the check box at the bottom of the dialog box.

   For LAGs:

   - LAG attributes (Interface Mode, etc.)
   - QoS, DCB Map / Traffic Class Map
   - LLDP Profiles

9. Click to move the available targets selected for configuration deployment to the **Selected Targets** list.
10. Click **OK**.

    The **Deployment Status** dialog box launches.

11. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected devices.
12. Click **Close** to close the **Deployment Status** dialog box.

Source to target switch FOS version compatibility for deployment

Table 30 lists the restrictions that exist when deploying source switches to target switches.

TABLE 30 Source to target switch FOS version compatibility

Source FOS version and device	Target FOS version supported	Comments
Brocade 8000 DCB switch and FCOE10-24 DCB blade with FOS version 6.4.2 or earlier.	Allows Brocade 8000 DCB switch and FCOE10-24 DCB blade with FOS version 6.4.2 or earlier. Excludes Brocade Converged 10 Gbe switch module for IBM BladeCenter with FOS 6.3.1_cee, FOS 6.4.1_fcoe, and FOS 6.3.1_dcb.	You cannot copy legacy configurations to FOS version 7.0 switches, because these switches support FCoE maps and can have only one default DCB map. Legacy FOS switches, however, can have more than one default map.
Brocade FCOE10-24 DCB blade with FOS 6.4.1_fcoe	Allows FCOE10-24 DCB blade with FOS 6.4.1_fcoe or FOS 7.0.0 . Allows Brocade Converged 10 Gbe switch module for IBM BladeCenter with FOS 6.3.1_cee or FOS 6.3.1_dcb. Excludes Brocade 8000 DCB switch and FCOE10-24 DCB blade with FOS 6.4.2 or earlier.	Both the source and the target support only one default DCB map. You can copy QoS, LLDP, and 802.1x configurations from the source to the target.
Brocade 8000 DCB switch FCOE10-24 CEE blade with FOS 7.0.	Allows Brocade 8000 DCB switch and FCOE10-24 DCB blade with FOS 7.0.0. Excludes all others.	VLAN classifiers are supported, but the FCoE map is not supported on FOS 7.0.0.
Brocade Converged 10 GbE switch module for IBM BladeCenter with FOS 6.3.1_cee and 6.3.1_dcb	Allows Brocade Converged 10 Gbe switch module for IBM BladeCenter with FOS 6.3.1_cee, FOS 6.3.1_dcb. Allows Dell M8428-k switch with FOS 6.3.1_dell, FOS 6.3.1_dcb.	Both source and target switches must support the FCoE map and VLAN classifiers.
Dell M8428-k switch with FOS 6.3.1_dell and 6.3.1_dcb	Allows Brocade Converged 10 Gbe switch module for IBM BladeCenter with FOS 6.3.1_cee, FOS 6.3.1_dcb. Allows Dell M8428-k switch with FOS 6.3.1_dell, FOS 6.3.1_dcb.	Both source and target switches must support the FCoE map and VLAN classifiers.

DCB Performance

Performance monitoring provides details about the quantity of traffic and errors a specific port or device generates on the fabric over a specific time frame. You can also use Performance features to indicate the devices that create the most traffic and to identify the ports that are most congested.

The Performance menu items launch either SAN or IP performance dialog boxes based on which tab you select. Note the following points:

- The DCB configuration dialog box can be launched from either the SAN or IP tab.
- The Historical Report menu item is disabled on the Performance list from the DCB configuration dialog box on the IP tab.
- The appropriate IP Performance tab launches depending on whether you selected a port or a switch.

Real Time Performance Graph

You can monitor a device's performance through a performance graph that displays transmit and receive data. The graphs can be sorted by the column headers. You can create multiple real-time performance graph instances.

Generating a real-time performance graph.

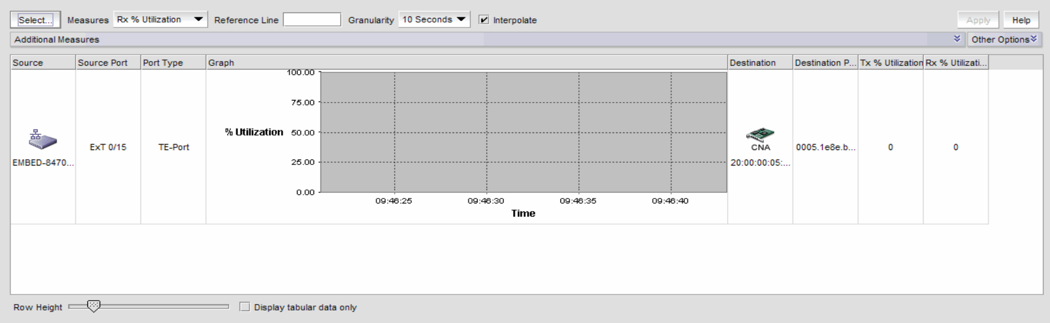
To generate a real-time performance graph for a device, complete the following steps.

1. Select a DCB port from the **DCB Configuration** dialog box, and select **Real Time Graph** from the Performance list.

   A message displays, prompting you to close the **DCB Configuration** dialog box.

2. Click **OK** to close the **DCB Configuration** dialog and open the Performance dialog box.

   The **Real Time Performance Graphs** dialog box displays.



Measures Rx % Utilization

Reference Line

Granularity 10 Seconds

☑ Interpolate

Source	Source Port	Port Type	Graph	Destination	Destination P...	Tx % Utilization	Rx % Utilizati...
EMBED-8470...	ExT 0/15	TE-Port		CNA 20:00:00:05:...	0005.1e8e.b...	0	0

Row Height

□ Display tabular data only

FIGURE 137 Real Time Performance Graphs dialog box

For complete information about Real Time Performance Graphs, refer to "SAN real-time performance data" on page 760.

Historical Performance Graph

The **Historical Performance Graph** dialog box enables you to customize how you want the historical performance information to display.

Generating a historical performance graph

1. Select a DCB port from the **DCB Configuration** dialog box, and select **Historical Graph** from the Performance list.

   A message displays, prompting you to close the **DCB Configuration** dialog.

2. Click **OK** to close the **DCB Configuration** dialog and open the Performance dialog box.

   The **Historical Performance Graph** dialog box displays.

For complete information about Real Time Performance Graphs, refer to “SAN real-time performance data” on page 760.

Historical Performance Report

The **Historical Performance Report** dialog box enables you to customize how you want the historical performance information to display.

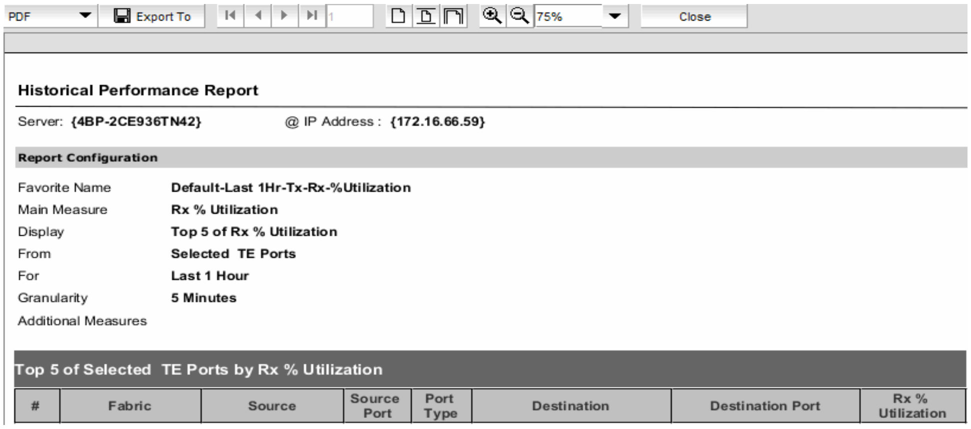
Generating a historical performance report.

1. Select a DCB port from the **DCB Configuration** dialog box, and select **Historical Report** from the Performance list.

   A message displays, prompting you to close the **DCB Configuration** dialog box.

2. Click **OK** to close the **DCB Configuration** dialog and open the Performance dialog box.

   The **Historical Performance Report** dialog box displays.



Historical Performance Report

Server: {4BP-2CE936TN42} @ IP Address : {172.16.66.59}

Report Configuration

Favorite Name	Default-Last 1Hr-Tx-Rx-%Utilization
Main Measure	Rx % Utilization
Display	Top 5 of Rx % Utilization
From	Selected TE Ports
For	Last 1 Hour
Granularity	5 Minutes
Additional Measures	

Top 5 of Selected TE Ports by Rx % Utilization

#	Fabric	Source	Source Port	Port Type	Destination	Destination Port	Rx % Utilization

FIGURE 138 Historical Performance Report dialog box

For complete information about Historical Performance Graphs, refer to “SAN Historical performance data” on page 764.

FCoE login groups

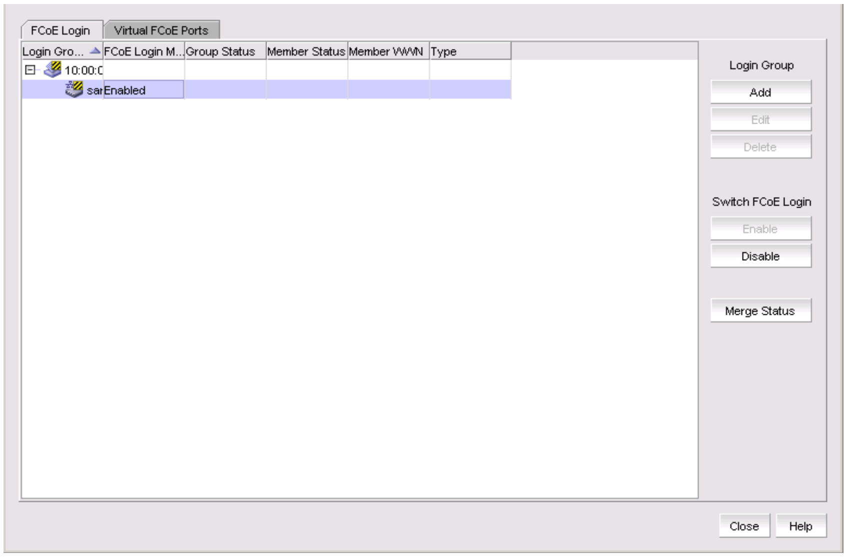
The FCoE Configuration dialog box allows you to manage the FCoE login configuration parameters on the DCB switches in all discovered fabrics. FCoE login configuration is created and maintained as a fabric-wide configuration.

1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

   The **FCoE Configuration** dialog box displays, shown in Figure 139.



Login Gro...	FCoE Login M...	Group Status	Member Status	Member WWN	Type
10:00:0					
sar	Enabled				

FIGURE 139 FCoE Configuration dialog box

2. Perform one of the following tasks:

   Under Login Group:

   - Click **Add** to launch the Add Login Group dialog box. See "Adding an FCoE login group" on page 387.
   - Click **Edit** to launch the Edit Login Group dialog box. See "Editing an FCoE login group" on page 388.
   - Click **Delete** to delete a login group. See "Deleting one or more FCoE login groups" on page 389.

Adding an FCoE login group

Complete the following steps to add switches to a login group. You can manually add ports by entering the world wide name (WWN) or select available managed CNAs from all discovered hosts. Only directly-connected devices are supported.

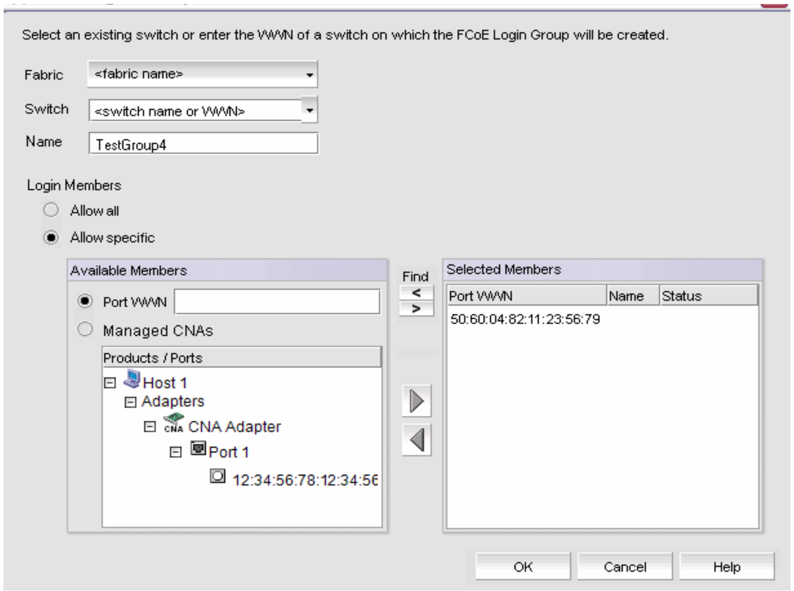
1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

2. Click **Add**.

   The **Add Login Group** dialog box, shown in Figure 140, displays.



Select an existing switch or enter the WWN of a switch on which the FCoE Login Group will be created.

Fabric: <fabric name>

Switch: <switch name or WWN>

Name: TestGroup4

Login Members

○ Allow all

● Allow specific

Available Members

● Port WWN

○ Managed CNAs

Products / Ports

- Host 1
  - Adapters
    - CNA Adapter
      - Port 1
        - 12:34:56:78:12:34:56

Selected Members

Port WWN	Name	Status
50:60:04:82:11:23:56:79		

FIGURE 140 Add Login Group dialog box

3. Select an existing switch from the **Switch** list, or enter the WWN of the switch that will be added to the FCoE login group.

4. Select one of the following Login Members options:

   - Allow all—Click to allow all login members into the Available Members list.
   - Allow specific—Click to allow specific login members into the Available Members list. If you select this option, you can add specific login members using the options in the **Available Members** area.

5. Select one of the following Available Member options:

   - Port WWN—Click to enter the world wide name (WWN) of the port to associate with the selected switch. The member port WWN text field allows a maximum of 16 digits.
   - Managed CNAs—Click to show a list of products and ports which can be selected as login group members.

6. Select available members from the **Products/Ports** list and click the right arrow button to move the available members to the **Selected Members** list.

7. Click **OK**.

   The **FCoE Login Group Confirmation and Status** dialog displays.

8. Review the changes carefully before you accept them.

9. Click **Start** to apply the changes, or click **Close** to abort the operation.

   On closing the FCoE Login Group Confirmation and Status dialog box, the **FCoE Configuration** Dialog refreshes the data and the latest information is displayed.

Editing an FCoE login group

Complete the following steps to edit the name of a login group. You can manually add ports by entering the world wide name (WWN) or select available managed CNAs from all discovered hosts. Only directly-connected devices are supported.

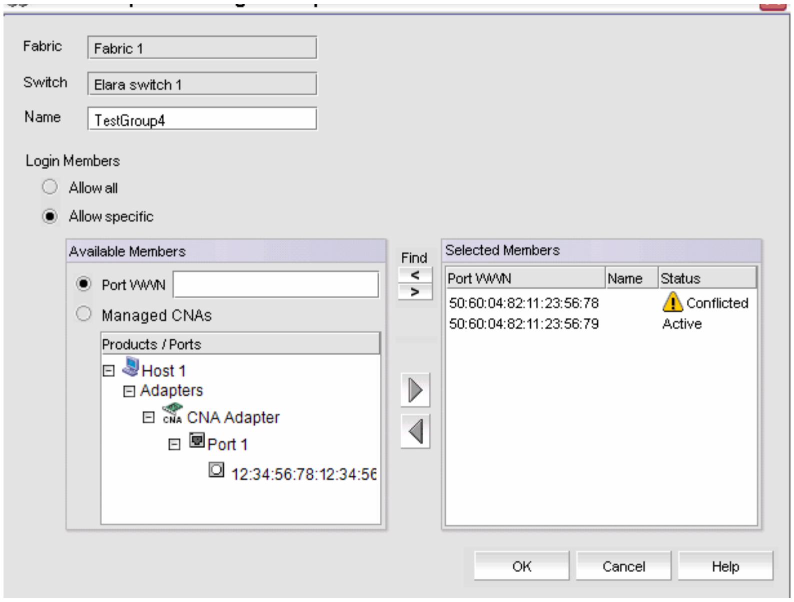
1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

2. Select a group from the Login Groups list and click **Edit**.

   The **Edit Login Group** dialog box, shown in Figure 141, displays.



Fabric: Fabric 1

Switch: Elara switch 1

Name: TestGroup4

Login Members

○ Allow all

● Allow specific

Available Members

● Port WWN

○ Managed CNAs

Products / Ports

- Host 1
  - Adapters
    - CNA Adapter
      - Port 1
        - 12:34:56:78:12:34:56

Selected Members

Port WWN	Name	Status
50:60:04:82:11:23:56:78		⚠ Conflicted
50:60:04:82:11:23:56:79		Active

FIGURE 141 Edit Login Group dialog box

3. Change the name of the login group.

   NOTE
   The **Fabric** field and the **Switch** field are read-only fields.

4. Perform one of the following editing tasks:
   - Rename the login group by entering the new name into the **Name** field. The **Allow All** option must be selected to rename the login group.
   - Select one of the following options to add or remove login members into the **Available Members** list. The **Allow Specific** option must be selected to add or remove login members.
     - Port WWN—Click to enter the world wide name (WWN) of the port to associate with the selected switch. The member port WWN text field allows a maximum of 16 digits.
     - Managed CNAs—Click to show a list of products and ports which can be selected as login group members.
5. Select available members from the **Products/Ports** list and click the right arrow button to move the available members to the **Selected Members** list.
6. Click **OK**.

   The **FCoE Login Group Confirmation and Status** dialog displays.
7. Review the changes carefully before you accept them.
8. Click **Start** to apply the changes, or click **Close** to abort the operation.

   On closing the FCoE Login Group Confirmation and Status dialog box, the **FCoE Configuration** Dialog refreshes the data and the latest information is displayed.

Deleting one or more FCoE login groups

1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

   The **FCoE Configuration** dialog box displays.
2. Select a group from the Login Groups list and click **Delete**.

   The **FCoE Login Group Confirmation and Status** dialog displays.
3. Review the changes carefully before you accept them.
4. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The login group is removed from the **Login Group** table.

Disabling the FCoE login management feature on a switch

1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

   The **FCoE Configuration** dialog box displays.

2. Select an FCoE-enabled switch from the Login Groups list and click **Disable**.

   The **FCoE Login Group Confirmation and Status** dialog displays.

3. Review the changes carefully before you accept them.

4. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The FCoE login management feature is disabled and all login groups on the selected switch are deleted.

   The value in the FCoE Login Management State column for the selected switch is **Disabled** and no login groups appear under the switch after the FCoE Configuration dialog box refresh operation.

Enabling the FCoE login management feature on a switch

1. Select **Configure > FCoE** from the menu bar.

   or

   Right-click the DCB device and select **FCoE**.

   The **FCoE Configuration** dialog box displays.

2. Select an FCoE-disabled switch from the Login Groups list and click **Enable**.

3. The FCoE Login Group Configuration and Status dialog box displays.

4. Review the changes carefully before you accept them.

5. Click **Start** to apply the changes, or click **Close** to abort the operation.

   The FCoE login management feature is enabled on the selected switch.

   The value in the FCoE Login Management State column is **Enabled** after the **FCoE Configuration** dialog box refresh operation.

Virtual FCoE port configuration

The virtual FCoE port has the following configuration features:

- Displays the virtual FCoE ports on each of the DCB devices, which provides the Ethernet with bridging capability.
- One-to-one mapping of FCoE ports with 10 Gbps Ethernet ports.
- Option to enable or disable the virtual FCoE ports.
- Option to view the end devices connected to a virtual FCoE port.

Viewing virtual FCoE ports

Configuration of virtual FCoE ports requires installation of the FCoE license on the switch.

1. Select **Configure > FCoE** from the menu bar.

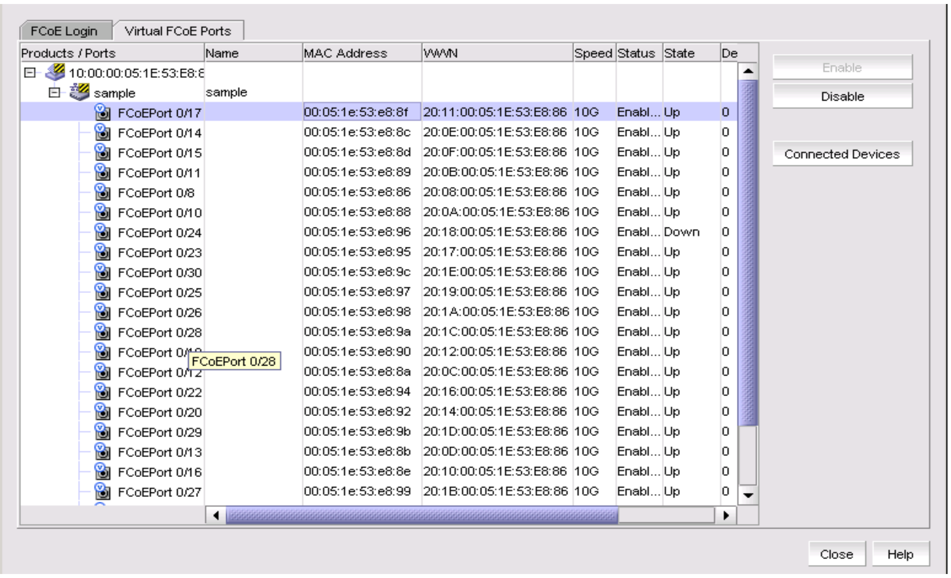
   or

   Right-click the DCB device and select **FCoE**.

   The **FCoE Configuration** dialog box displays.

2. Select the **Virtual FCoE Ports** tab.

   The **Virtual FCoE Ports** tab displays.



Products / Ports	Name	MAC Address	WWN	Speed	Status	State	De
10:00:00:05:1E:53:E8:8							
sample	sample						
FCoEPort 0/17		00:05:1e:53:e8:8f	20:11:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/14		00:05:1e:53:e8:8c	20:0E:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/15		00:05:1e:53:e8:8d	20:0F:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/11		00:05:1e:53:e8:89	20:0B:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/8		00:05:1e:53:e8:86	20:08:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/10		00:05:1e:53:e8:88	20:0A:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/24		00:05:1e:53:e8:96	20:18:00:05:1E:53:E8:86	10G	Enabl...	Down	0
FCoEPort 0/23		00:05:1e:53:e8:95	20:17:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/30		00:05:1e:53:e8:9c	20:1E:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/25		00:05:1e:53:e8:97	20:19:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/26		00:05:1e:53:e8:98	20:1A:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/28		00:05:1e:53:e8:9a	20:1C:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/18		00:05:1e:53:e8:90	20:12:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/12		00:05:1e:53:e8:8a	20:0C:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/22		00:05:1e:53:e8:94	20:16:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/20		00:05:1e:53:e8:92	20:14:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/29		00:05:1e:53:e8:9b	20:1D:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/13		00:05:1e:53:e8:8b	20:0D:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/16		00:05:1e:53:e8:8e	20:10:00:05:1E:53:E8:86	10G	Enabl...	Up	0
FCoEPort 0/27		00:05:1e:53:e8:99	20:1B:00:05:1E:53:E8:86	10G	Enabl...	Up	0

FIGURE 142 Virtual FCoE Ports dialog box

3. Select one or more virtual ports from the **Products/Ports** list.

4. Perform one of the following tasks:
   - Click **Enable** to enable a selected virtual FCoE port for DCB configuration.
   - Click **Disable** to disable a selected virtual FCoE port from DCB configuration.
   - Click **Connected Devices** to view a list of FCoE virtual ports and to what they are directly connected.
5. Click **Close** to close the dialog box.

Clearing a stale entry

A stale entry is a device that logged in and logged off but, because a port went down after an FLOGI was received, the device failed to receive the message. The entry in the **FCoE Connected Devices** table becomes stale and you must clear it manually.

1. Select a virtual FCoE port from the **FCoE Configuration** dialog box and click **Connected Devices**.

   The **Connected Devices** dialog box displays.
2. Select one or more rows from the **Connected Devices** table and click **Disconnect**.

   The **DCB Confirmation and Status** dialog displays.

   The selected connected device should be cleared from the switch cache and from the table. Note, however, that the connected devices might still be active and this operation could potentially stop traffic between the connected devices and the switch.
3. Review the changes carefully before you accept them.
4. Click **Start** to apply the changes, or click **Close** to abort the operation.

   On closing the DCB Confirmation and Status dialog box, the **FCoE Configuration** Dialog refreshes the data and the latest information about the FCoE ports are displayed.

Chapter

Security Management 16

In this chapter

Layer 2 access control list management

A Layer 2 access control list (L2 ACL) enables you to filter traffic based on the information in the IP packet header using the MAC address and Ethernet type.

NOTE
L2 ACLs can filter traffic for both Fabric OS and Internetwork OS FCoE devices.

An ACL is a unique collection of permit and deny statements (rules) that apply to frames. You can use ACLs to permit or deny incoming frames from passing through an interface to which you assigned the ACLs. When the interface receives the frame, the device compares the fields in the frame against any ACLs assigned to the interface to verify that the frame has the required permissions to be forwarded. The device compares the frame, sequentially, against each rule in the assigned ACL. If the frame matches the ‘permit’ rule, the traffic is forwarded; otherwise, the traffic is dropped.

You should configure the ACL on the device before you assign the ACL to an interface. You can create multiple ACLs and save them to the device configuration. However, the ACL does not filter traffic until you assign it to an interface. You can assign an ACL on the following interface types: physical port , Virtual LAN (VLAN), or Link Aggregation Group (LAG).

You can create two types of ACLs:

- Standard ACL—Use to permit and deny traffic based on the source MAC address of incoming frames. You should use standard ACLs when you only need to filter traffic based the source address.
- Extended ACL—Use to permit and deny traffic based on the source and destination MAC addresses and EtherType, of incoming frames.

Fabric OS L2 ACL configuration

This section provides procedures for configuring a standard for extended L2 ACL on a device, assigning the L2 ACL to an interface, as well as clearing L2 ACL assignments from a device.

Creating a standard L2 ACL configuration

To create a standard L2 ACL configuration, complete the following steps.

1. Select the device and select **Configure** > **Security** > **L2 ACL** > **Product.**

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

2. Select **New** from the **Add** list.

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

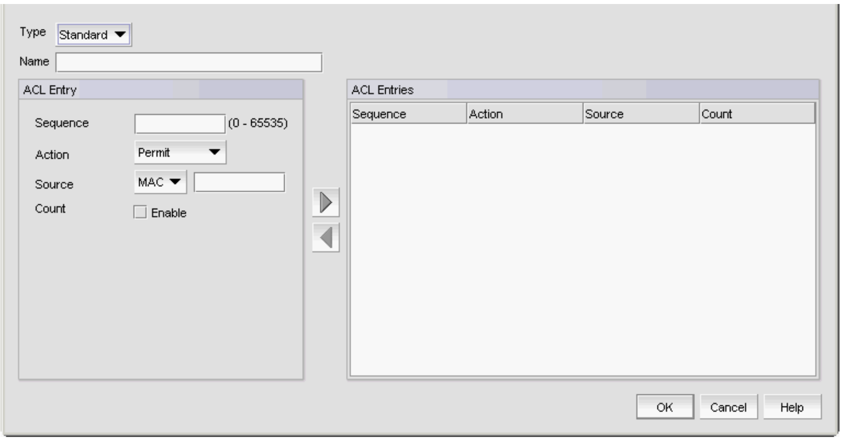


FIGURE 143 *Device_Name* - **L2 ACL Configuration (Standard) dialog box**

3. Select **Standard** from the **Type** list.
4. Enter a name for the ACL in the **Name** field.
5. Enter a sequence number for the ACL in the **Sequence** field.
6. Select **Permit** or **Deny** from the Action list.
7. In the **Source** list, select one of the following options:
   - **Any**
   - **MAC**

     Selecting MAC enables the **Source** field. Enter the source MAC address on which the configuration filters traffic in the **Source** field.
8. Select the **Count** check box to enable counting.

   Count specifies the number of packets filtered (allowed or denied) for the ACL rule.
9. Click the right arrow button.

   The new ACL entry displays in the **ACL Entries** table. To create additional ACL entries, repeat step 3 through step 9.

10. Click **OK** on the **Add - L2 ACL Configuration** dialog box.

    The new ACL configuration displays in the **ACLs** table. To create additional ACLs, repeat step 2 through step 10.

11. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

    The **Deploy to Products - L2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 407

Editing a standard L2 ACL configuration

To create a standard L2 ACL configuration on a Fabric OS device, complete the following steps.

1. Select the device and select **Configure > Security > L2 ACL > Product.**

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

2. Select the ACL you want to edit in the **ACLs** table and click **Edit.**

   The *Configuration_Name* **Edit Standard L2 ACL Configuration** dialog box displays.

3. To edit an existing ACL rule, complete the following steps.

   a. Select the rule you want to edit in the **ACL Entries** table and click the left arrow button.

   b. Change the sequence number for the ACL in the **Sequence** field.

   c. Select **Permit** or **Deny** from the Action list.

   d. In the **Source** list, select one of the following options:

      - Any
      - MAC
        Selecting MAC enables the **Source** field. Enter the source MAC address on which the configuration filters traffic in the **Source** field.

   e. Select the **Count** check box to enable counting.

      Count specifies the number of packets filtered (allowed or denied) for the ACL rule.

   f. Click the right arrow button.

      The updated ACL entry displays in the **ACL Entries** table. To edit additional ACL entries, repeat step 3.

4. To delete an existing ACL rule, select the rule you want to edit in the **ACL Entries** table and click the left arrow button.

5. To add a new ACL rule, complete the following steps.

   a. Enter the sequence number for the ACL in the **Sequence** field.

   b. Select **Permit** or **Deny** from the Action list.

   c. In the **Source** list, select one of the following options:

      - Any
      - MAC
        Selecting MAC enables the **Source** field. Enter the source MAC address on which the configuration filters traffic in the **Source** field.

d. Select the **Count** check box to enable counting.

Count specifies the number of packets filtered (allowed or denied) for the ACL rule.

e. Click the right arrow button.

The new ACL entry displays in the **ACL Entries** table. To add additional ACL entries, repeat step 5.

6. Click **OK** on the **Add - L2 ACL Configuration** dialog box.

The updated ACL configuration displays in the **ACLs** table. To edit additional ACLs, repeat step 2 through step 5.

7. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

The **Deploy to Products - L2 ACL** dialog box displays. To save the configuration, refer to “Saving a security configuration deployment” on page 407

Copying a standard L2 ACL configuration

To copy a standard L2 ACL configuration on a Fabric OS device, complete the following steps.

1. Select the device and select **Configure > Security > L2 ACL > Product.**

The *Device_Name* - **L2 ACL Configuration** dialog box displays.

2. Select the ACL you want to duplicate in the **ACLs** table and click **Duplicate.**

The **Duplicate - L2 ACL Configuration** dialog box displays with the default name ‘Copy of *Original_Name*’.

3. Enter a new name for the ACL in the **Name** field.

4. To edit an existing ACL rule, complete the following steps.

a. Select the rule you want to edit in the **ACL Entries** table and click the left arrow button.

b. Change the sequence number for the ACL in the **Sequence** field.

c. Select **Permit** or **Deny** from the Action list.

d. In the **Source** list, select one of the following options:

- **Any**
- **MAC**
Selecting MAC enables the **Source** field. Enter the source MAC address on which the configuration filters traffic in the **Source** field.

e. Select the **Count** check box to enable counting.

Count specifies the number of packets filtered (allowed or denied) for the ACL rule.

f. Click the right arrow button.

The updated ACL entry displays in the **ACL Entries** table. To edit additional ACL entries, repeat step 4.

5. To delete an existing ACL rule, select the rule you want to edit in the **ACL Entries** table and click the left arrow button.

6. To add a new ACL rule, complete the following steps.

   a. Enter the sequence number for the ACL in the **Sequence** field.

   b. Select **Permit** or **Deny** from the Action list.

   c. In the **Source** list, select one of the following options:

      - Any
      - MAC
        Selecting MAC enables the **Source** field. Enter the source MAC address on which the configuration filters traffic in the **Source** field.

   d. Select the **Count** check box to enable counting.

      Count specifies the number of packets filtered (allowed or denied) for the ACL rule.

   e. Click the right arrow button.

      The new ACL entry displays in the **ACL Entries** table. To add additional ACL entries, repeat step 6.

7. Click **OK** on the **Duplicate - L2 ACL Configuration** dialog box.

   The new ACL configuration displays in the **ACLs** table. To copy additional ACLs, repeat step 2 through step 10.

8. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

   The **Deploy to Products - L2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 407

Creating an extended L2 ACL configuration

To create an extended L2 ACL configuration on a Fabric OS device, complete the following steps.

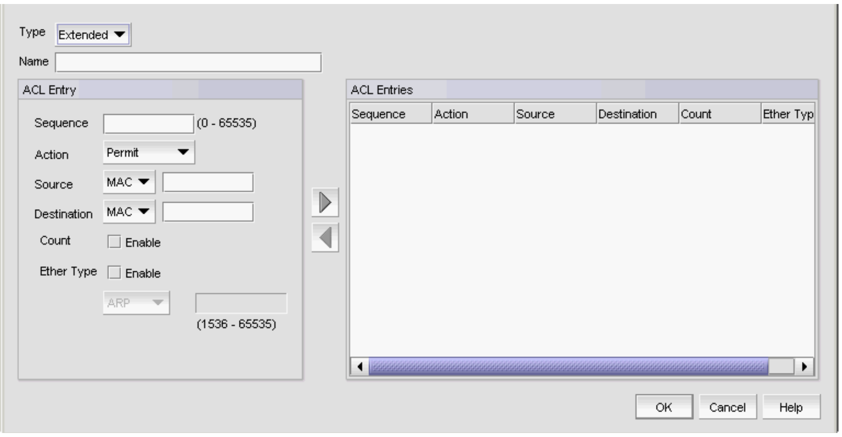
1. Select the device and select **Configure > Security > L2 ACL > Product.**

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

2. Select **New** from the **Add** list.

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

3. Select **Extended** from the **Type** list.



Type Extended

Action Permit

Source MAC

Destination MAC

Ether Type ARP

FIGURE 144 *Device_Name* **- L2 ACL Configuration (Extended) dialog box**

4. Enter a name for the ACL in the **Name** field.
5. Enter a sequence number for the ACL in the **Sequence** field.
6. Select **Permit** or **Deny** from the Action list.
7. In the **Source** list, select one of the following options:
   - **Any**
   - **Host**
   - **MAC**

     Selecting MAC or Host enables the **Source** field. Enter the source address on which the configuration filters traffic in the **Source** field.
8. In the **Destination Address** list, select one of the following options:
   - **Any**
   - **Host**
   - **MAC**

     Selecting MAC or Host enables the **Destination** field. Enter the destination address on which the configuration filters traffic in the **Destination** field.
9. Select the **Count** check box to enable counting.

   Count specifies the number of packets filtered (allowed or denied) for the ACL rule.
10. Select the **Ether Type** check box to specify the Ethernet protocol.
11. In the **Ether Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:
    - **ARP**—Address Resolution Protocol
    - **FCoE**—Fibre Channel over Ethernet
    - **IPV4**—Internet Protocol, version 4
    - **Custom**—enter a custom protocol. Valid values are 1536 through 65535.
12. Click the right arrow button.

    The new ACL entry displays in the **ACL Entries** table. To create additional ACL entries, repeat step 5 through step 12.
13. Click **OK** on the **Add - L2 ACL Configuration** dialog box.

    The new ACL displays in the **ACL Entries** table. To create additional ACL entries, repeat step 2 through step 13.
14. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

    The **Deploy to Products - L2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 407

Editing an extended L2 ACL configuration

To edit an extended L2 ACL configuration on a Fabric OS device, complete the following steps.

1. Select the device and select **Configure** > **Security** > **L2 ACL** > **Product**.

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

2. Select the ACL you want to edit in the **ACLs** table and click **Edit**.

   The *Configuration_Name* **Edit Extended L2 ACL Configuration** dialog box displays.

3. To edit an existing rule, complete the following steps.

   a. Select the rule you want to edit in the **ACL Entries** table and click the left arrow button.

   b. Change sequence number for the ACL in the **Sequence** field.

   c. Select **Permit** or **Deny** from the Action list.

   d. In the **Source** list, select one of the following options:

      - **Any**
      - **Host**
      - **MAC**

      Selecting MAC or Host enables the **Source** field. Enter the source address on which the configuration filters traffic in the **Source** field.

   e. In the **Destination Address** list, select one of the following options:

      - **Any**
      - **Host**
      - **MAC**

      Selecting MAC or Host enables the **Destination** field. Enter the destination address on which the configuration filters traffic in the **Destination** field.

   f. Select the **Count** check box to enable counting.

      Count specifies the number of packets filtered (allowed or denied) for the ACL rule.

   g. Select the **Ether Type** check box to specify the Ethernet protocol.

   h. In the **Ether Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:

      - **ARP**—Address Resolution Protocol
      - **FCoE**—Fibre Channel over Ethernet
      - **IPV4**—Internet Protocol, version 4
      - **Custom**—enter a custom protocol. Valid values are 1536 through 65535.

   i. Click the right arrow button.

      The updated ACL entry displays in the **ACL Entries** table. To update additional ACL entries, repeat step 3.

4. To delete a rule, select the rule you want to delete in the **ACL Entries** table and click the left arrow button.

5. To add a rule, complete the following steps.

   a. Enter sequence number for the ACL in the **Sequence** field.

   b. Select **Permit** or **Deny** from the Action list.

   c. In the **Source** list, select one of the following options:

      - **Any**
      - **Host**
      - **MAC**

      Selecting MAC or Host enables the **Source** field. Enter the source address on which the configuration filters traffic in the **Source** field.

   d. In the **Destination Address** list, select one of the following options:

      - **Any**
      - **Host**
      - **MAC**

      Selecting MAC or Host enables the **Destination** field. Enter the destination address on which the configuration filters traffic in the **Destination** field.

   e. Select the **Count** check box to enable counting.

      Count specifies the number of packets filtered (allowed or denied) for the ACL rule.

   f. Select the **Ether Type** check box to specify the Ethernet protocol.

   g. In the **Ether Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:

      - **ARP**—Address Resolution Protocol
      - **FCoE**—Fibre Channel over Ethernet
      - **IPV4**—Internet Protocol, version 4
      - **Custom**—enter a custom protocol. Valid values are 1536 through 65535.

   h. Click the right arrow button.

      The new ACL entry displays in the **ACL Entries** table. To create additional ACL entries, repeat step 5.

6. Click **OK** on the **Edit - L2 ACL Configuration** dialog box.

   The updated ACL displays in the **ACL Entries** table. To edit additional ACLs, repeat step 2 through step 6.

7. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

   The **Deploy to Products - L2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 407

Copying an extended L2 ACL configuration

To copy an extended L2 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > L2 ACL > Product**.

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

2. Select the ACL you want to copy in the **ACLs** table and click **Duplicate**.

   The **Duplicate - L2 ACL Configuration** dialog box displays with the default name 'Copy of *Original_Name*'.

3. Enter a new name for the ACL in the **Name** field.

4. To edit an existing rule, complete the following steps.

   a. Select the rule you want to edit in the **ACL Entries** table and click the left arrow button.

   b. Change sequence number for the ACL in the **Sequence** field.

   c. Select **Permit** or **Deny** from the Action list.

   d. In the **Source** list, select one of the following options:

      - **Any**
      - **Host**
      - **MAC**

      Selecting MAC or Host enables the **Source** field. Enter the source address on which the configuration filters traffic in the **Source** field.

   e. In the **Destination Address** list, select one of the following options:

      - **Any**
      - **Host**
      - **MAC**

      Selecting MAC or Host enables the **Destination** field. Enter the destination address on which the configuration filters traffic in the **Destination** field.

   f. Select the **Count** check box to enable counting.

      Count specifies the number of packets filtered (allowed or denied) for the ACL rule.

   g. Select the **Ether Type** check box to specify the Ethernet protocol.

   h. In the **Ether Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:

      - **ARP**—Address Resolution Protocol
      - **FCoE**—Fibre Channel over Ethernet
      - **IPV4**—Internet Protocol, version 4
      - **Custom**—enter a custom protocol. Valid values are 1536 through 65535.

   i. Click the right arrow button.

      The updated ACL entry displays in the **ACL Entries** table. To update additional ACL entries, repeat step 4.

5. To delete a rule, select the rule you want to delete in the **ACL Entries** table and click the left arrow button.

6. To add a rule, complete the following steps.

   a. Enter sequence number for the ACL in the **Sequence** field.

   b. Select **Permit** or **Deny** from the Action list.

   c. In the **Source** list, select one of the following options:

      - **Any**
      - **Host**
      - **MAC**

      Selecting MAC or Host enables the **Source** field. Enter the source address on which the configuration filters traffic in the **Source** field.

   d. In the **Destination Address** list, select one of the following options:

      - **Any**
      - **Host**
      - **MAC**

      Selecting MAC or Host enables the **Destination** field. Enter the destination address on which the configuration filters traffic in the **Destination** field.

   e. Select the **Count** check box to enable counting.

      Count specifies the number of packets filtered (allowed or denied) for the ACL rule.

   f. Select the **Ether Type** check box to specify the Ethernet protocol.

   g. In the **Ether Type** list, select one of the following to specify the Ethernet type being transferred in the Ethernet frame:

      - **ARP**—Address Resolution Protocol
      - **FCoE**—Fibre Channel over Ethernet
      - **IPV4**—Internet Protocol, version 4
      - **Custom**—enter a custom protocol. Valid values are 1536 through 65535.

   h. Click the right arrow button.

      The new ACL entry displays in the **ACL Entries** table. To create additional ACL entries, repeat step 6.

7. Click **OK** on the **Duplicate - L2 ACL Configuration** dialog box.

   The new ACL displays in the **ACL Entries** table. To copy additional ACLs, repeat step 2 through step 7.

8. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

   The **Deploy to Products - L2 ACL** dialog box displays. To save the configuration, refer to “Saving a security configuration deployment” on page 407

Assigning a L2 ACL configuration to an interface

To assign L2 ACL configuration to a interface, complete the following steps.

1. Select **Configure** > **Security** > **L2 ACL** > **Port**.

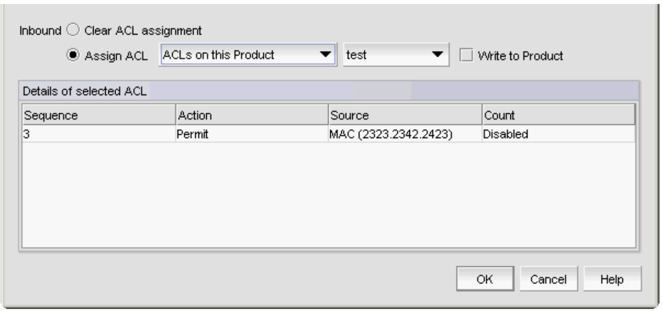
   The **Port Selection** - **L2 ACL** dialog box displays.

2. Select a port or Link Aggregation Group (LAG) in the **Available Ports** table and click the right arrow button.

   LAGs display in the **Available Ports** table using the following convention: Po *LAG_Number.*

3. Click **OK**.

   The *Device_Name* - *Port_Number/***LAG** *LAG_Number*- **Layer 2 ACL Configuration** dialog box displays.



Inbound ○ Clear ACL assignment

● Assign ACL ACLs on this Product ▼ test ▼ □ Write to Product

Details of selected ACL

Sequence	Action	Source	Count
3	Permit	MAC (2323.2342.2423)	Disabled

FIGURE 145 *Device_Name* - *Port_Number* - **Layer 2 ACL Configuration dialog box**

4. Select the **Assign ACL** option and choose one of the following options from the first **Assign ACL** list:

   - Select **ACLs on this Product** to assign ACLs deployed on the product to the port.

     The second list is populated with the ACLs deployed on the switch or associated with a save deployment object.

   - Select **ACLs bound to this interface** to assign ACLs bound to the interface to the port.

     The second list is populated with the ACLs bound to the interface.

5. Select the ACL you want to assign to the port from the second **Assign ACL** list.

6. Select the **Write to device** check box to configurecreate the selected ACL on the device if it does not already exist.

7. Click **OK** on the *Device_Name* - *Port_Number* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Ports** - **L2 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 405.

Clearing L2 ACL assignments

To clear L2 ACL configuration from interfaces, complete the following steps.

1. Select **Configure** > **Security** > **L2 ACL** > **Port.**

   The **Port Selection** - **L2 ACL** dialog box displays.

2. Select a port or LAG in the **Available Ports** table and click the right arrow button.

   LAGs display in the **Available Ports** table using the following convention: Po *LAG_Number.*

3. Click **OK.**

   The *Device_Name* - *Port_Number/***LAG** *LAG_Number* - **Layer 2 ACL Configuration** dialog box displays.

4. Select the **Clear ACL Assignment** option.

5. Click **OK** on the *Device_Name* - *Port_Number/***LAG** *LAG_Number* - **Layer 2 ACL Configuration** dialog box.

   The **Deploy to Ports** - **L2 ACL** dialog box displays. To deploy the configuration, refer to "Security configuration deployment" on page 405.

Creating a L2 ACL from a saved configuration

To create a L2 ACL from a saved configuration, complete the following steps.

1. Select the device and select **Configure** > **Security** > **L2 ACL** > **Product.**

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

2. Select **From Saved Configurations** from the **Add** list.

   The **L2 ACL Saved Configurations** dialog box displays.

3. Select one or more configurations to add to the new L2 ACL configuration.

4. Click **OK** on the **L2 ACL Saved Configurations** dialog box.

   The new ACL displays in the **ACLs** table.

5. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

   The **Deploy to Products** - **L2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 407

Deleting a L2 ACL configuration

To delete a L2 ACL configuration, complete the following steps.

1. Select the device and select **Configure > Security > L2 ACL > Product.**

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

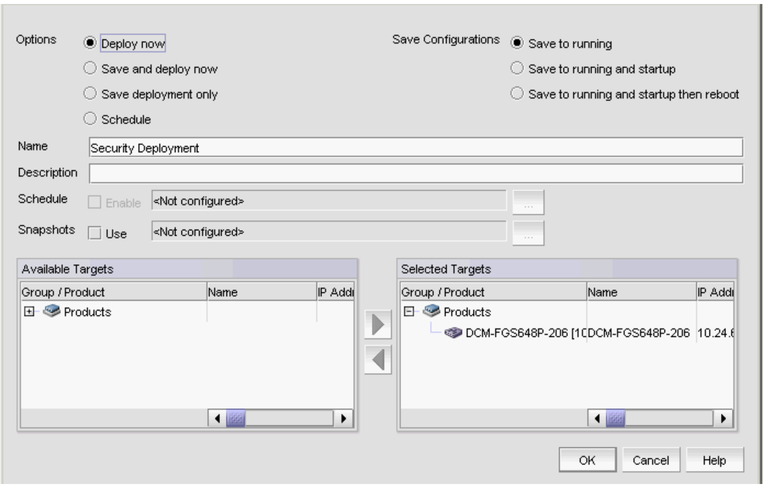
2. Select the L2 ACL you want to delete in the **ACLs** table and click **Delete.**
3. Click **Yes** on the confirmation message.
4. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

   NOTE
   The L2 ACL configuration is not deleted from the switch until you deploy the configuration to the switch.

   The **Deploy to Products - L2 ACL** dialog box displays. To save the configuration, refer to "Saving a security configuration deployment" on page 407

Security configuration deployment

Figure 146 shows the standard interface used to deploy security configurations.



Options
● Deploy now
○ Save and deploy now
○ Save deployment only
○ Schedule

Save Configurations
● Save to running
○ Save to running and startup
○ Save to running and startup then reboot

Name: Security Deployment
Description:
Schedule: □ Enable <Not configured>
Snapshots: □ Use <Not configured>

Available Targets

Group / Product	Name	IP Addı
⊞ Products		

Selected Targets

Group / Product	Name	IP Addı
⊟ Products		
DCM-FGS648P-206 [1(	DCM-FGS648P-206	10.24.(

FIGURE 146 Deploy to Product/Ports dialog box

Before you can deploy a security configuration, you must create the security configuration. For step-by-step instructions, refer to the following procedures:

- "Creating a standard L2 ACL configuration" on page 394
- "Editing a standard L2 ACL configuration" on page 395
- "Copying a standard L2 ACL configuration" on page 396
- "Creating an extended L2 ACL configuration" on page 397
- "Editing an extended L2 ACL configuration" on page 399
- "Copying an extended L2 ACL configuration" on page 401
- "Creating a L2 ACL from a saved configuration" on page 404

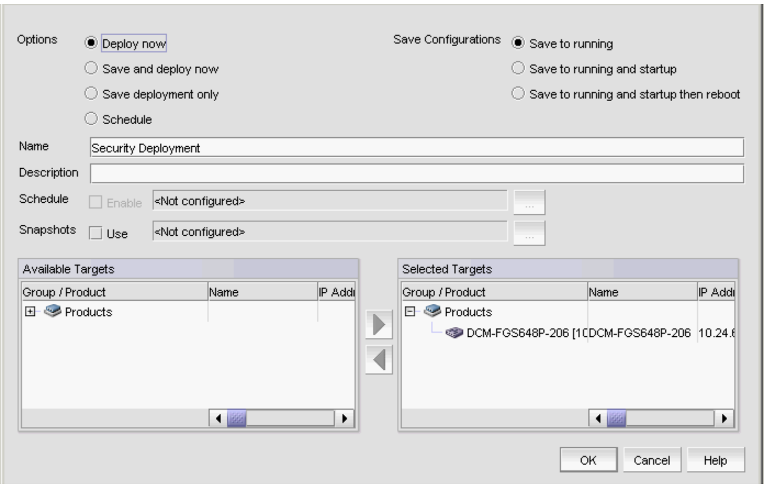
Security Management enables you to configure, persist, and manage a security configuration as a “deployment configuration object”. A deployment configuration object is comprised of the following parts:

- Security configuration (L2 ACL)
- Target information
- Deployment option
- Persistence option
- Scheduling option
- Snapshot option

To create a deployment configuration object, you must save the deployment. Once you create a deployment configuration object, you can access the security configuration from the Deployment manager. For more information about the Deployment manager, refer to “Deployment Manager” on page 723.

Deploying a security configuration on demand

To deploy a security configuration immediately, complete the following steps.



Options
● Deploy now
○ Save and deploy now
○ Save deployment only
○ Schedule

Save Configurations
● Save to running
○ Save to running and startup
○ Save to running and startup then reboot

Name: Security Deployment
Description:
Schedule: □ Enable <Not configured>
Snapshots: □ Use <Not configured>

Available Targets		
Group / Product	Name	IP Addı
⊞ Products		

Selected Targets		
Group / Product	Name	IP Addı
⊟ Products		
DCM-FGS648P-206 [1(	DCM-FGS648P-206	10.24.ε

FIGURE 147 Deploy to Product/Ports dialog box

1. Choose one of the following options:
   - Deploy now—Select to deploy the configuration immediately on the product or port without saving the deployment definition.
   - Save and deploy now—Select to deploy the configuration immediately on the product or port and save the deployment definition for future deployment.

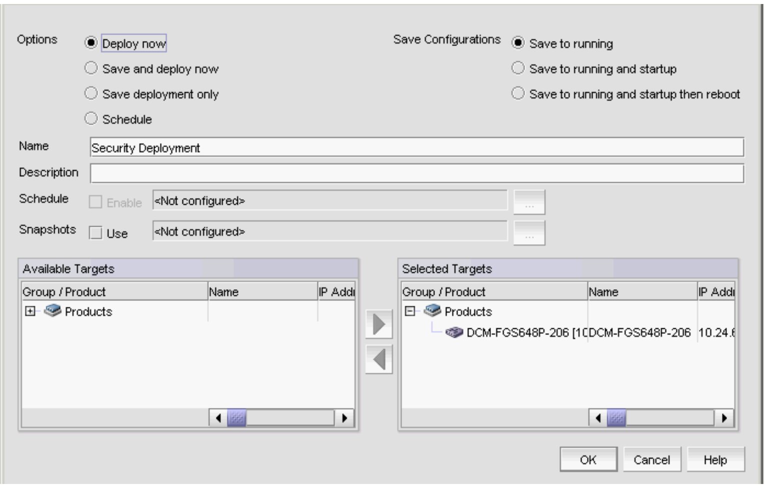
2. Select one of the following save configuration options:

   - **Save to running**—Select to update the running configuration; however, the deployment is not saved to the product’s flash memory.
   - **Save to running and startup**—Select to update the running configuration as well as save the deployment configuration to the product’s flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.
   - **Save to running and startup then reboot**—Select to update the running configuration, save the deployment configuration to the product’s flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.

3. Enter a name for the deployment in the **Name** field.
4. Enter a description for the deployment in the **Description** field.
5. Select one or more ports or products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
6. Click **OK** on the **Deploy to Products - L2 ACL** dialog box.

Saving a security configuration deployment

To save a security configuration deployment, complete the following steps.



Options ● Deploy now ○ Save and deploy now ○ Save deployment only ○ Schedule

Save Configurations ● Save to running ○ Save to running and startup ○ Save to running and startup then reboot

Name: Security Deployment

Description:

Schedule □ Enable <Not configured>

Snapshots □ Use <Not configured>

Available Targets

Group / Product	Name	IP Addr
⊞ Products		

Selected Targets

Group / Product	Name	IP Addr
⊟ Products		
DCM-FGS648P-206 [1(	DCM-FGS648P-206	10.24.6

FIGURE 148 Deploy to Product/Ports dialog box

1. Select the **Save deployment only** option to save the deployment definition for future deployment.
2. Select one of the following save configuration options:

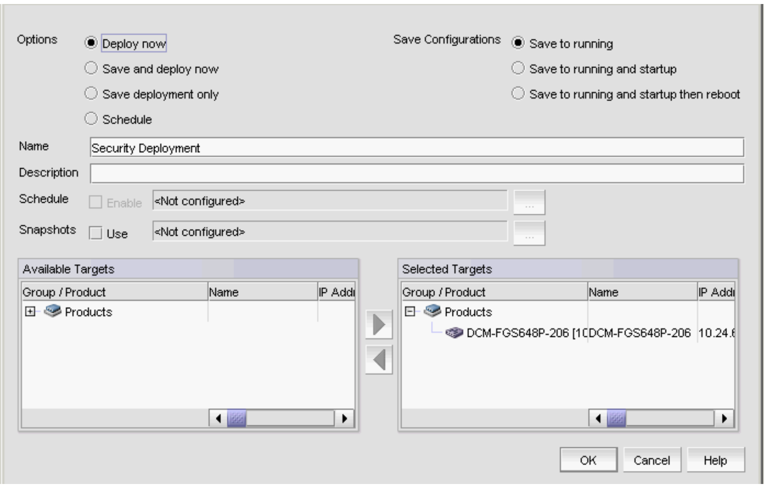
   - **Save to running**—Select to update the running configuration; however, the deployment is not saved to the product’s flash memory.
   - **Save to running and startup**—Select to update the running configuration as well as save the deployment configuration to the product’s flash memory. Selecting this option is the equivalent to a write memory command on the product CLI.

- **Save to running and startup then reboot**—Select to update the running configuration, save the deployment configuration to the product's flash memory, and reboot the product. Selecting this option is the equivalent to entering a write memory and a reload command on the product CLI.

3. Enter a name for the deployment in the **Name** field.
4. Enter a description for the deployment in the **Description** field.
5. Select one or more ports or products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
6. Click **OK** on the **Deploy to Products - L2 ACL** dialog box.

Scheduling a security configuration deployment

To schedule a security configuration deployment, complete the following steps.



Options ● Deploy now ○ Save and deploy now ○ Save deployment only ○ Schedule

Save Configurations ● Save to running ○ Save to running and startup ○ Save to running and startup then reboot

Name: Security Deployment

Description:

Schedule □ Enable <Not configured>

Snapshots □ Use <Not configured>

Group / Product	Name	IP Addr
Products		

Group / Product	Name	IP Addr
Products		
DCM-FGS648P-206 [1(	DCM-FGS648P-206	10.24.6

FIGURE 149 Deploy to Product/Ports dialog box

1. Select **Configure > Security > L2 ACL > Product.**

   The *Device_Name* - **L2 ACL Configuration** dialog box displays.

2. Choose one of the following options:

   - Select **New** from the **Add** list.

     The **Add - L2 ACL Configuration** dialog box displays.

   - Select an ACL in the list and click **Edit.**

     The **Edit - L2 ACL Configuration** dialog box displays.

3. Configure the L2 ACL and click **OK** on the **Add/Edit - L2 ACL Configuration** dialog box.
4. Click **OK** on the *Device_Name* - **L2 ACL Configuration** dialog box.

   The **Deploy to Products - L2 ACL** dialog box displays.

5. Select the **Schedule** option.

6. Select one of the following save configuration options:
   - **Save to running**
   - **Save to running and startup**
   - **Save to running and startup then reboot**
7. Enter a name for the deployment in the **Name** field.
8. Enter a description for the deployment in the **Description** field.
9. Click the **Schedule Enable** check box and click the ellipsis button to schedule deployment.

   The **Schedule Properties** dialog box displays.
10. Choose one of the following options to configure the frequency at which deployment runs for the schedule:
    - To configure deployment to run only once, refer to "Configuring a one-time deployment schedule" on page 409.
    - To configure hourly deployment, refer to "Configuring an hourly deployment schedule" on page 410.
    - To configure daily deployment, refer to "Configuring a daily deployment schedule" on page 410.
    - To configure weekly deployment, refer to "Configuring a weekly deployment schedule" on page 410.
    - To configure monthly deployment, refer to "Configuring a monthly deployment schedule" on page 411.
11. Click **OK** on the **Schedule Properties** dialog box.
12. Select one or more ports or products to which you want to deploy the configuration in the **Available Targets** list and click the right arrow button to move them to the **Selected Targets** list.
13. Click **OK** on the **Deploy to Products - L2 ACL** dialog box.

Configuring a one-time deployment schedule

To configure a one-time schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.

   To finish configuring the deployment schedule, return to one of the following procedures:

   To configure security configuration schedule, refer to step 11 of "Scheduling a security configuration deployment" on page 408.

Configuring an hourly deployment schedule

To configure an hourly schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.
2. Select the minute past the hour you want deployment to run from the **Minutes past the hour** list.

   Where the minute value is from 00 through 59.

   To finish configuring the deployment schedule, return to one of the following procedures:

   To configure security configuration schedule, refer to step 11 of “Scheduling a security configuration deployment” on page 408.

Configuring a daily deployment schedule

To configure a daily deployment schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.

   To finish configuring the deployment schedule, return to one of the following procedures:

   To configure security configuration schedule, refer to step 11 of “Scheduling a security configuration deployment” on page 408.

Configuring a weekly deployment schedule

To configure a weekly schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Select the day you want deployment to run from the **Day of the Week** list.

   To finish configuring the deployment schedule, return to one of the following procedures:

   To configure security configuration schedule, refer to step 11 of “Scheduling a security configuration deployment” on page 408.

Configuring a monthly deployment schedule

To configure a monthly schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Select the day you want deployment to run from the **Day of the Month** list (1 through 31).

   To finish configuring the deployment schedule, return to one of the following procedures:

   To configure security configuration schedule, refer to step 11 of "Scheduling a security configuration deployment" on page 408.

Chapter

FC-FC Routing Service Management 17

In this chapter

Devices that support Fibre Channel routing

The FC-FC Routing Service is supported only on the following devices:

- 40-port, 8 Gbps FC Switch
- 80-port, 8 Gbps FC Switch
- 48-port, 16 Gbps FC Switch
- 4 Gbps Router, Extension Switch
- 8 Gbps Extension Switch
- Any of the following blades on a Director chassis:
  - 4 Gbps Router, Extension Blade
  - FC 8 GB 16-port Blade
  - FC 8 GB 32-port Blade
  - FC 8 GB 48-port Blade - The shared ports area (ports 16-47) cannot be used as EX_Ports.
  - 8 Gbps Extension Blade
- Any of the following blades on a Backbone chassis:
  - 4 Gbps Router, Extension Blade
  - FC 8 GB 16-port Blade
  - FC 8 GB 32-port Blade
  - FC 8 GB 48-port Blade - The shared ports area (ports 16-47) cannot be used as EX_Ports.
  - FC 8 GB 64-port Blade
  - 8 Gbps Extension Blade
  - 16 Gbps 32-port Blade
  - 16 Gbps 48-port Blade

Fibre Channel routing overview

Fibre Channel (FC) routing provides connectivity to devices in different fabrics without merging the fabrics. Using Fibre Channel routing, you can share tape drives across multiple fabrics without the administrative overhead, such as change management and network management, and scalability issues that might result from merging the fabrics.

Fibre Channel routing allows you to create logical storage area networks (LSANs) that can span fabrics. These LSANs allow Fibre Channel zones to cross physical SAN boundaries without merging the fabrics and while maintaining the access controls of zones.

Refer to the *Fabric OS Administrator's Guide* for detailed information about Fibre Channel routing.

The following terminology is used in this chapter:

FC router	A switch running the FC-FC Routing Service.
Interfabric link (IFL)	The link between an E_Port and an EX_Port, or a VE_Port and a VEX_Port.
Edge fabric	A standard Fibre Channel fabric with targets and initiators connected through an FC router to another Fibre Channel fabric.
Backbone fabric	The fabric to which the FC router belongs. An FC router connects two or more edge fabrics; a *backbone fabric* connects FC routers. A backbone fabric consists of at least one FC router and possibly a number of Fabric OS-based Fibre Channel switches. Initiators and targets in the edge fabric can communicate with devices in the backbone fabric through the FC router.
LSAN	A logical SAN that spans fabrics. An LSAN is defined by zones in two or more edge or backbone fabrics that contain the same devices. LSANs enable Fibre Channel zones to cross physical SAN boundaries without merging the fabrics while maintaining the access controls of zones.
metaSAN	The collection of all SANs interconnected with FC routers.

Figure 150 on page 415 shows a metaSAN with a backbone fabric and three edge fabrics. The backbone consists of one 4 Gbps Router, Extension Switch connecting hosts in Edge fabrics 1 and 3 with storage in Edge fabric 2 and the backbone fabric. LSANs provide device sharing between the following pairs of fabrics:

- The backbone fabric and Edge fabric 1
- Edge fabric 1 and Edge fabric 2
- Edge fabric 2 and Edge fabric 3

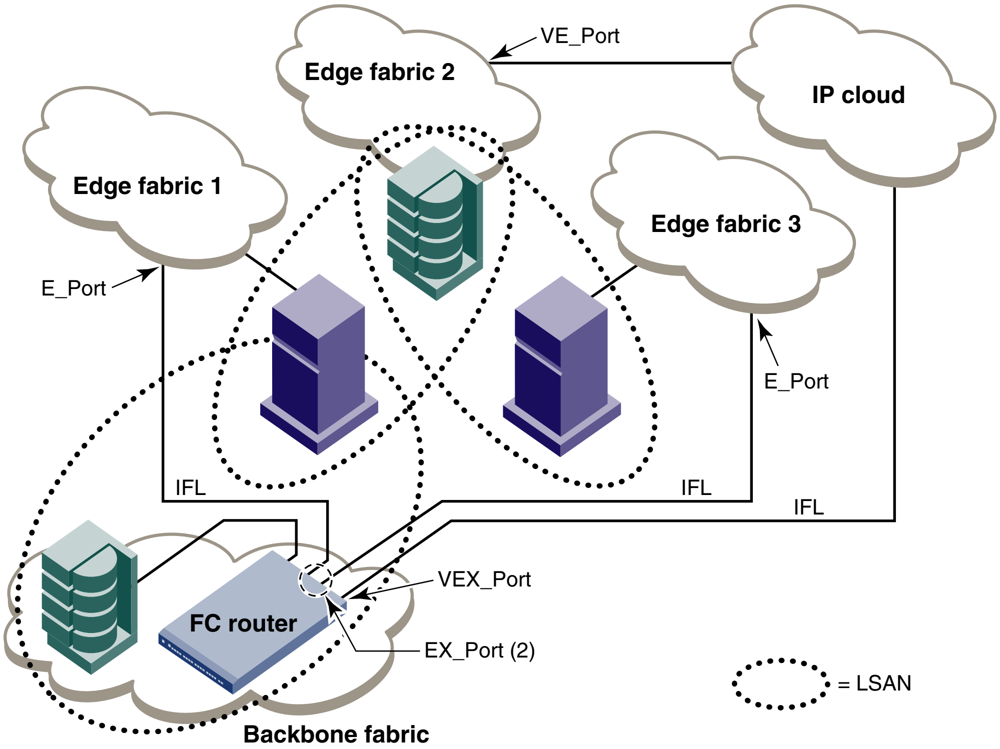


FIGURE 150 A metaSAN with edge-to-edge and backbone fabrics

Guidelines for setting up Fibre Channel routing

The following are some general guidelines for setting up Fibre Channel routing:

- Ensure that the backbone fabric ID of the FC router is the same as that of other FC routers in the backbone fabric.
- On the FC router, ensure that the ports to be configured as EX_Ports are either disabled or not connected.
- When configuring EX_Ports, supply a fabric ID for the fabric to which the port will be connected. You can choose any unique fabric ID as long as it is consistent for all EX_Ports that connect to the same edge fabric.
- For Virtual Fabric (VF)-enabled fabrics, only the base switch can be configured as the FC router; for example, EX_Ports can be configured only on a base switch for a VF-enabled switch.

Connecting edge fabrics to a backbone fabric

The following procedure explains how to set up FC-FC routing on two edge fabrics connected through an FC router using E_Ports and EX_Ports.

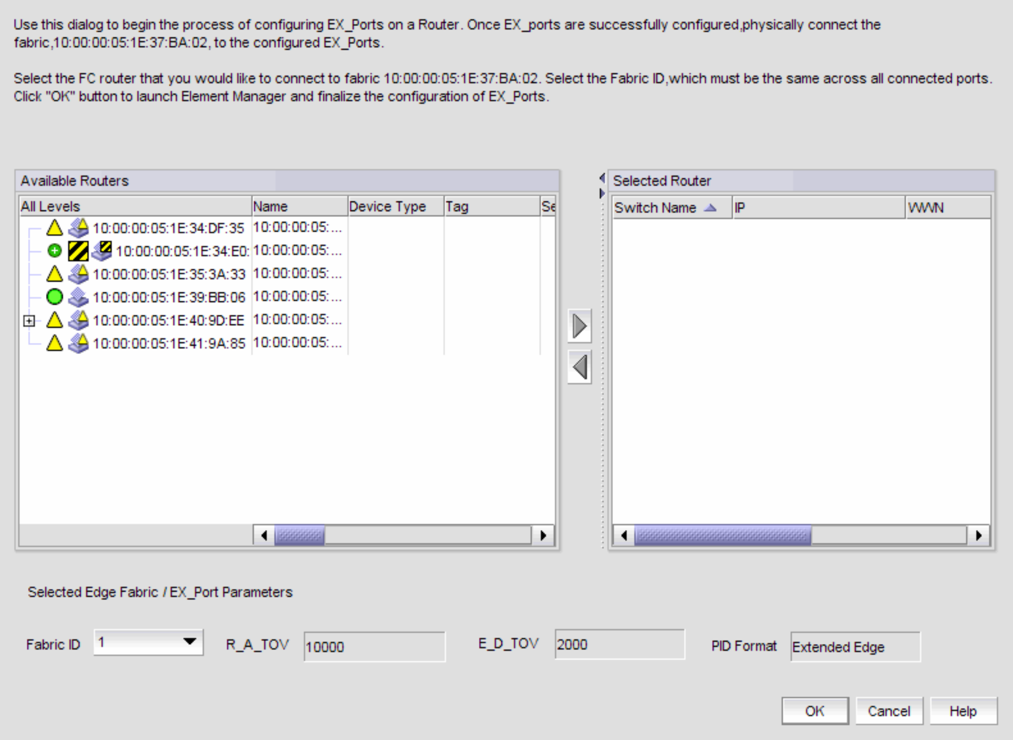
For Enterprise Edition only: If you are connecting Fibre Channel SANs through an IP-based network, see "Configuring an FCIP tunnel" on page 644 for instructions on setting up an FCIP tunnel between a VE_Port and a VEX_Port.

ATTENTION
Be sure that you do not physically connect a port to the remote fabric before configuring it as an EX_Port; otherwise, the two fabrics merge and you lose the benefit of FC-FC routing.

1. Select the edge fabric you want to connect to an FC router from the Connectivity Map or Product List.
2. Right-click the edge fabric in the Connectivity Map or Product List and select **Router Configuration.**

   The **Router Configuration-Connect Edge Fabric** dialog box is displayed (Figure 151). The edge fabric you selected is also displayed in the title of the dialog box. Discovered extension switches capable of FC routing are displayed in the **Available Routers** list.

   NOTE
   If the configuration includes virtual fabrics, only the base switch displays in the **Available Routers** list.



Use this dialog to begin the process of configuring EX_Ports on a Router. Once EX_ports are successfully configured,physically connect the fabric,10:00:00:05:1E:37:BA:02, to the configured EX_Ports.

Select the FC router that you would like to connect to fabric 10:00:00:05:1E:37:BA:02. Select the Fabric ID,which must be the same across all connected ports. Click "OK" button to launch Element Manager and finalize the configuration of EX_Ports.

Available Routers

All Levels	Name	Device Type	Tag	Se
⚠ 10:00:00:05:1E:34:DF:35	10:00:00:05:...			
⊕ 10:00:00:05:1E:34:E0:	10:00:00:05:...			
⚠ 10:00:00:05:1E:35:3A:33	10:00:00:05:...			
● 10:00:00:05:1E:39:BB:06	10:00:00:05:...			
⊞ ⚠ 10:00:00:05:1E:40:9D:EE	10:00:00:05:...			
⚠ 10:00:00:05:1E:41:9A:85	10:00:00:05:...			

Selected Router

Switch Name ▲	IP	WWN

Selected Edge Fabric / EX_Port Parameters

Fabric ID: 1
R_A_TOV: 10000
E_D_TOV: 2000
PID Format: Extended Edge

FIGURE 151 Router Configuration-Connect Edge Fabric dialog box

3. Select the FC router from the **Available Routers** list.

4. Click the right arrow button to move the FC router you selected to the **Selected Router** list.
5. Select a valid fabric ID (1 through 128) from the **Fabric ID** list.

   You can choose any unique fabric ID as long as it is consistent for all EX_Ports that connect to the same edge fabric. If the edge fabric is already configured with the backbone fabric, the **Fabric ID** list is disabled and populated with the pre-selected value.
6. Click **OK** on the **Router Configuration-Connect Edge Fabric** dialog box.

   The Element Manager launches automatically and opens the **FC Router** dialog box and Port Configuration wizard. For more information, refer to the *Web Tools Administrator's Guide.*
7. Follow the instructions in the Port Configuration wizard to configure the EX_Port:
   a. Select the port to be configured as an EX_Port.
   b. Ensure the backbone fabric ID of the switch is the same as that of other FC routers in the backbone fabric. The backbone fabric ID is the fabric ID that was selected in the **Router Configuration-Connect Edge Fabric** dialog box.
   c. Complete the wizard to configure the EX_Port.
   d. Physically connect the EX_Port to the edge fabric, if it is not already connected.
8. Repeat step 1 through step 7 to connect a second edge fabric to the FC router, if your configuration involves two edge fabrics.

   The front domain is added in the edge fabric and is given a name in the format fcr_fd_*domainID*. For example, if the domain ID is 3, the name of the front domain is fcr_fd_3.

   If the edge fabric is a pure M-EOS fabric, the front domain name is "Unknown" due to a limitation in M-EOS.
9. Configure LSAN zones in each fabric that will share devices.

   For specific instructions, refer to "Configuring LSAN zoning" on page 598.

Configuring routing domain IDs

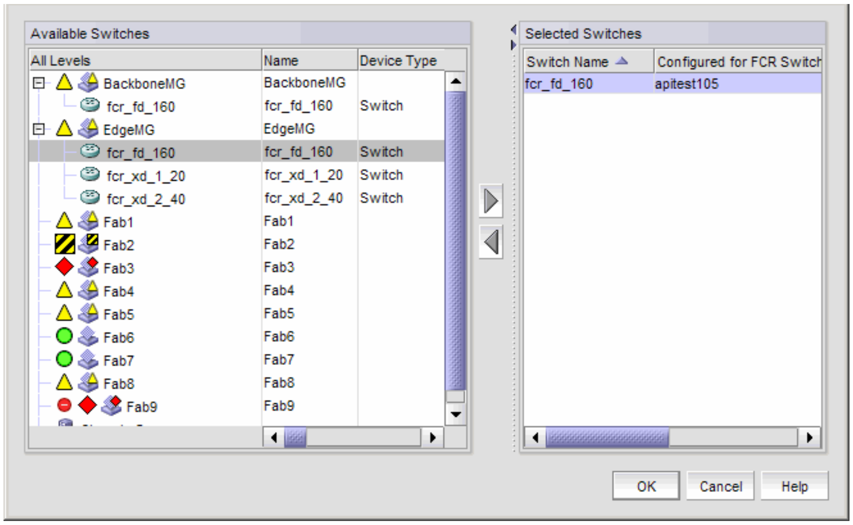
Logical (phantom) domains are created to enable routed fabrics. Two types of logical domains are created:

- A front domain is created in edge fabrics for every interfabric link (IFL).
- A translate (Xlate) domain is created in routed fabrics that share devices.

Use the following procedure to change the domain IDs of these logical domains.

1. In the Product List or Connectivity Map, right-click the fabric for which you want to configure logical domains, and select **Routing Domain IDs**.

   The **Configure Routing Domain IDs** dialog box is displayed (Figure 152).



All Levels	Name	Device Type
BackboneMG	BackboneMG	
fcr_fd_160	fcr_fd_160	Switch
EdgeMG	EdgeMG	
fcr_fd_160	fcr_fd_160	Switch
fcr_xd_1_20	fcr_xd_1_20	Switch
fcr_xd_2_40	fcr_xd_2_40	Switch
Fab1	Fab1	
Fab2	Fab2	
Fab3	Fab3	
Fab4	Fab4	
Fab5	Fab5	
Fab6	Fab6	
Fab7	Fab7	
Fab8	Fab8	
Fab9	Fab9	

Switch Name	Configured for FCR Switch
fcr_fd_160	apitest105

FIGURE 152 Configure Routing Domain IDs dialog box

2. Right-click anywhere in the **Available Switches** list and select **Expand All** in the right-click menu.

   The switch group for the fabric expands to display the logical domains.

3. Select a logical domain, and click the right arrow button to move the switch to the **Selected Switches** list.

4. Select a domain ID number from the **Domain ID** column in the **Selected Switches** list. The **Domain ID** column lists unused domain IDs.

   You may need to scroll right or drag the dialog box open further to see the **Domain ID** column.

5. Click **OK**.

Chapter

Virtual Fabrics 18

In this chapter

Virtual Fabrics overview

NOTE
Virtual Fabrics requires that you have at least one Virtual Fabrics-enabled physical chassis running Fabric OS 6.2.0 or later in your SAN.

Virtual Fabrics enables you to divide one physical chassis into multiple logical switches that can be managed by separate administrators. Logical switches consist of one or more ports that act as a single FC switch. You can interconnect logical switches to create a logical fabric.

The following lists the benefits of using the Management application to manage Virtual Fabrics:

- Enables you to view your entire SAN (both physical and virtual) at a glance.
- Enables you to easily determine which devices in your SAN are logical switches. Logical switches are shown with a Virtual Fabrics icon (Ⓥ).
- Enables you to manage a logical switch the same as a physical switch, so that fewer physical chassis are required for Management application deployment.
- Enables you to use a logical switch for discovery and eliminate the requirement for one physical chassis for each fabric.
- Enables you to manage multiple Virtual Fabrics-capable physical chassis from the same interface.
- Enables you to provide logical isolation of data, control, and management paths at the port level.

Before using the Management application to manage Virtual Fabrics, you should familiarize yourself with Virtual Fabrics concepts, as described in the *Fabric OS Administrator’s Guide*.

Terminology

Table 31 lists definitions of Virtual Fabrics terms.

TABLE 31 Virtual Fabrics terms

Term	Definition
Physical chassis	The physical switch or chassis from which you create logical switches and fabrics.
Logical switch	A collection of zero or more ports that act as a single Fibre Channel (FC) switch. When Virtual Fabrics is enabled on the chassis, there is always at least one logical switch: the default logical switch. You must assign each logical switch (default or general) in the same chassis to a different logical fabric. The logical switch supports all E_Ports and F_Ports. Note that EX_ports are only allowed on the base switch.
Default logical switch	A logical switch that is created automatically when the Virtual Fabrics feature is enabled in a physical chassis. Initially, all ports in a chassis belong to the default logical switch. The default logical switch always exists as long as Virtual Fabrics is enabled. You cannot delete the default logical switch. The default logical switch supports all E_Ports and F_Ports.
Base switch	A special logical switch used to communicate among different logical switches. The legacy EX_port is connected to the base logical switch. Inter-Switch Links (ISLs) connected to the base switch are used to communicate among different fabrics. The base switch supports E_Ports and EX_Ports.
Fabric ID (FID)	An identifier you assign to a logical switch (default or general) or a base switch to designate to which logical or base fabric it belongs.
Logical fabric	A fabric with at least one logical switch.
Base fabric	A fabric formed from base switches that have the same FID. The base fabric provides the physical connectivity across multiple segments of a fabric over which logical switches in the fabric can establish logical connectivity.
Extended ISL (XISL)	An ISL physically connected between two base switches that carries traffic for multiple logical fabrics. By default, logical switches are configured to not use XISLs. XISL use is not supported in the following cases: • FICON logical fabrics • Logical switches in an edge fabric connected to an FC router • Logical switch in InteropMode 2 or InteropMode 3 • Logical switch has VE_Ports and is running Fabric OS 6.4.x or earlier.

Virtual Fabrics requirements

To configure Virtual Fabrics, you must have at least one Virtual Fabrics-enabled physical chassis running Fabric OS 6.2.0 or later in your SAN. Use one of the following options to discover a Virtual Fabrics-enabled physical chassis on the Management application topology:

- Discover a Virtual Fabrics-capable seed physical chassis running Fabric OS 6.2.0 or later. Virtual Fabrics is disabled by default. This physical chassis displays as a legacy switch. Once discovered, you must enable Virtual Fabrics.
- Discover a Virtual Fabrics-enabled seed physical chassis running Fabric OS 6.2.0 or later with Virtual Fabrics enabled, and at least one logical switch defined on the core switch. The physical chassis displays as a virtual switch.
- Upgrade a physical chassis already in your SAN to Fabric OS 6.2.0 or later. Virtual Fabrics is disabled by default. This switch displays as a legacy switch. Once upgraded, you must enable Virtual Fabrics.

For more information about enabling Virtual Fabrics on a physical chassis, refer to "Enabling Virtual Fabrics" on page 423.

Table 32 lists the Virtual Fabric-capable physical chassis and the number of logical switches allowed for each of those physical chassis.

TABLE 32 Maximum number of logical switches per chassis

Physical chassis	Number of logical switches allowed
40-port, 8 Gbps FC Switch	3
80-port, 8 Gbps FC Switch	4
48-port, 16 Gbps FC Switch	4[1]
384-port Backbone Chassis	8
192-port Backbone Chassis	8

[1] The maximum is 3 logical switches if you are using FC-FC routing.

For the switches, any port can be assigned to any logical switch. However, depending on the partition type, the backbone chassis have the port requirements shown in Table 33.

TABLE 33 Blade and port types supported on logical switches for backbone chassis

Logical switch type	Ports
Default logical switch	• Extension Blade—E_, F_, GE_, and VE_Ports • FC 10-6 ISL Blade—E_ and F_Ports • FC 8 GB Port Blade—E_ and F_Ports • FC 16 GB Port Blade—E_ and F_Ports • 10 Gig FCoE port Blade—E_ and F_Ports • 8 Gbps Extension Blade • FC ports: E_, F_, and VE_Ports • GE ports: VE_Ports • 384-port and 192-port Backbone Chassis— ICL ports

TABLE 33 Blade and port types supported on logical switches for backbone chassis (Continued)

Logical switch	• Extension Blade—GE_ and VE_Ports • FC 8 GB Port Blade—E_ and F_Ports • FC 16 GB Port Blade—E_ and F_Ports • 8 Gbps Extension Blade • FC ports: E_, F_, and VE_Ports • GE ports: VE_Ports • 384-port and 192-port Backbone Chassis— ICL ports
Base switch	• Extension Blade—GE_ and VEX_Ports • FC 8 GB Port Blade—E_ and EX_Ports • FC 16 GB Port Blade—E_ and EX_Ports • 8 Gbps Extension Blade • FC ports: E_, EX_, VE_, and VEX_Ports • GE ports: VE_Ports • 384-port and 192-port Backbone Chassis— ICL Ports

NOTE

In the 384-port Backbone Chassis, ports 48–63 of the FC 8 GB 64-port Blade are not supported in the base switch, and ports 56–63 are not supported as E_Ports on the default logical switch. The 192-port Backbone Chassis does not have these limitations.

Configuring Virtual Fabrics

The Management application allows you to discover, enable, create, and manage Virtual Fabric-capable physical chassis from the same interface.

This procedure describes the general steps you take to enable the Virtual Fabrics feature and configure logical fabrics. The logical fabrics in this example span multiple physical chassis, and the logical switches in each fabric communicate using an XISL in the base fabric.

1. Enable Virtual Fabrics in each physical chassis.

   See “Enabling Virtual Fabrics” on page 423 for instructions.

2. Set up base switches in each physical chassis:

   a. Create base switches in each physical chassis and assign ports to them.

      See “Creating a logical switch or base switch” on page 424 for instructions.

   b. Disable the base switches in each physical chassis.

      Right-click each base switch in the Connectivity Map or Product List and select **Enable/Disable > Disable**.

   c. Physically connect ports in the base switches to form XISLs.

   d. Enable all of the base switches. This forms the base fabric.

      Right-click each base switch in the Connectivity Map or Product List and select **Enable/Disable > Enable**.

3. Set up logical switches in each physical chassis:

    a. Create logical switches in each physical chassis and assign ports to them. Make sure the logical switches are configured to allow XISL use.

       See “Creating a logical switch or base switch” on page 424 for instructions.

    b. Disable all of the logical switches in each physical chassis.

       Right-click each logical switch in the Connectivity Map or Product List and select **Enable/Disable > Disable**.

    c. Physically connect devices and ISLs to the ports on the logical switches.

       You can connect ISLs from one logical switch to another logical switch in a different physical chassis only if the two logical switches have the same FID (and are thus in the same logical fabric). Traffic between these logical switches can travel over either this ISL or the XISL in the base fabric. The physical ISL path is favored over the XISL path because it has a lower cost.

    d. Enable all logical switches in each chassis.

       Right-click each logical switch in the Connectivity Map or Product List and select **Enable/Disable > Enable**.

   The logical fabric is formed.

Enabling Virtual Fabrics

For a list of platforms that are Virtual Fabrics-capable, refer to “Virtual Fabrics requirements” on page 421.

ATTENTION
If the physical chassis is participating in a fabric, the affected fabric will be disrupted.

1. Select the physical chassis in the topology and click **Configure > Virtual Fabric > Enable**.

   Alternatively, you can right-click the physical chassis and select **Enable Virtual Fabric**.

2. Read the warning message and click **OK**.

Disabling Virtual Fabrics

ATTENTION
Disabling Virtual Fabrics deletes all logical switches, returns port management to the physical chassis, and reboots the physical chassis. If these logical switches are participating in a fabric, all affected fabrics will be disrupted.

1. Select the physical chassis in the Chassis Group and click **Configure > Virtual Fabric > Disable**.

   Alternatively, you can right-click the physical chassis in the Chassis Group and select **Disable Virtual Fabric**.

2. Read the warning message and click **OK**.

Creating a logical switch or base switch

NOTE
Virtual Fabrics must be enabled on at least one physical chassis in your fabric.

Optionally, you can define the logical switch to be a base switch. Each chassis can have only one base switch.

1. Select a switch with Virtual Fabrics enabled on the Product List or Connectivity Map and select **Configure > Virtual Fabric > Logical Switches**.

   The **Logical Switches** dialog box displays.

2. Select the physical chassis from which you want to create a logical switch in the **Chassis** list.

3. Select one of the following in the **Existing Logical Switches** table:

   - A physical chassis in the Discovered Logical Switches node.
   - A NewFabric logical switch template in the Discovered Logical Switches node.
   - The Undiscovered Logical Switches node.

   If you select a logical switch template, the fabric-wide settings for the logical switch are obtained from the settings in the template.

   If you select a physical chassis or the Undiscovered Logical Switches node, the fabric-wide settings for the logical switch are the default settings.

4. Click **New Switch.**

   The **New Logical Switch** dialog box displays.

5. Click the **Fabric** tab, if necessary.

6. Enter a fabric identifier in the **Logical Fabric ID** field.

   This assigns the new logical switch to a logical fabric.

   If the logical fabric does not exist, this creates a new logical fabric as well as assigning the new logical switch.

7. (*Optional*) Select the **Base Fabric for Transport** check box if you want to configure the switch to use XISLs.

   In the following cases, you should make sure the **Base Fabric for Transport** check box is cleared, because XISL use is not supported:

   - FICON logical fabrics
   - Logical switches in an edge fabric connected to an FC router
   - Logical switch in InteropMode 2 or InteropMode 3
   - Logical switch has VE_Ports and is running Fabric OS 6.4.x or earlier.

   NOTE
   For switches running Fabric OS 7.0.0 or later, VE_Ports on the 8 Gbps Extension Blade *are* supported on logical switches that use XISLs.

8. (*Optional*) Perform the following steps to make the logical switch a base switch:

   a. Clear the Base Fabric for Transport check box.

      This check box is not relevant for base switches because all base switches can use XISLs.

   b. Select the Base Switch check box.

9. (*Optional*) For Backbone Chassis only, select an option in the 256 Area Limit list to use 256-area addressing mode (zero-based or port-based) or to disable this mode (default).

   The 256-area addressing mode can be used in FICON environments, which have strict requirements for 8-bit area FC addresses.

10. (*Optional*) Enter new values for the fabric-wide parameters or leave unchanged to accept the current values.

    Click the Help button for detailed information on each parameter.

11. Click the Switch tab.

12. Enter a name for the logical switch in the Name field.

13. Select a domain ID in the Preferred Domain ID list.

    In a FICON environment, select a domain ID that is not in use by the default or another logical switch in the same chassis.

14. (*Optional*) Select the Insistent check box to not allow the domain ID to be changed when a duplicate domain ID exists.

    If you select this check box and a duplicate domain ID exists, the switch will segment from the fabric instead of changing the domain ID.

15. Click OK on the New Logical Switch dialog box.

    The new logical switch displays in the Existing Logical Switches table (already highlighted). This logical switch has no ports.

16. Select the ports you want to include in the logical switch from the Ports table.

17. Click the right arrow button.

    The ports display in the selected logical switch node in the Existing Logical Switches table.

18. Click OK on the Logical Switches dialog box.

    The Logical Switch Change Confirmation and Status dialog box displays with a list of all changes you made in the Logical Switches dialog box.

    The Re-Enable ports after moving them and QoS disable the ports while moving them check boxes are selected by default.

    NOTE
    Ports are automatically disabled before moving from one logical switch to another.

19. (*Optional*) Select the Unbind Port Addresses while moving them check box.

20. Click **Start** to send these changes to the affected chassis.

    NOTE
    Most changes to logical switches will disrupt data traffic in the fabric.

    The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

21. When the changes are complete, click **Close**.

22. If the newly created switch is not part of a discovered fabric, then you must discover the switch.

    a. Undiscover the physical chassis. See "Deleting a fabric" on page 60 for instructions.

    b. Rediscover the physical chassis. See "Discovering fabrics" on page 53 for instructions.

       When entering the IP address, use the IP address of the physical fabric.

Finding the physical chassis for a logical switch

The Management application enables you to locate the physical chassis in the Product List from which the logical switch was created.

To find the physical chassis for a logical switch, right-click the logical switch in the Connectivity Map or Product List and select **Chassis**.

The physical chassis is highlighted in the Product List.

Finding the logical switch from a physical chassis

The Management application enables you to locate the logical switch from the physical chassis.

To find the logical switch, right-click the physical chassis within the **Chassis Group** in the Product List and select **Logical Switches** > *Logical_Switch_Name*.

The logical switch you selected is highlighted in the Product List and Connectivity Map.

Assigning ports to a logical switch

A port can be assigned to only one logical switch.

All ports are initially assigned to the default logical switch. When you create a logical switch, it has no ports and you must explicitly assign ports to it.

When you assign a port to a logical switch, it is removed from the original logical switch and assigned to the new logical switch.

1. Select a switch on the Product List or Connectivity Map and select **Configure** > **Virtual Fabric** > **Logical Switches**.

   The **Logical Switches** dialog box displays.

2. Select the physical chassis from which you want to assign ports in the **Chassis** list.
3. Select the ports you want to include in the logical switch from the **Ports** table.
4. Right-click anywhere in the **Existing Logical Switches** table and select **Table** > **Expand All**.
5. Select the logical switch in the **Existing Logical Switches** table.

6. Click the right arrow button.

   The ports display in the selected logical switch node in the **Existing Logical Switches** table.

7. Click **OK** on the **Logical Switches** dialog box.

   The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

   The **Re-Enable ports after moving them** and **QoS disable the ports while moving them** check boxes are selected by default.

   NOTE
   Ports are disabled before moving from one logical switch to another.

8. (*Optional*) Select the **Unbind Port Addresses while moving them** check box.

9. Click **Start** to send these changes to the affected chassis.

   NOTE
   Most changes to logical switches will disrupt data traffic in the fabric.

   The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

10. When the changes are complete, click **Close**.

Removing ports from a logical switch

1. Select a switch on the Product List or Connectivity Map and select **Configure > Virtual Fabric > Logical Switches.**

   The **Logical Switches** dialog box displays.

2. Select the physical chassis to which the ports belong in the **Chassis** list.

3. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.

4. Select the ports you want to remove from the logical switches from the **Existing Logical Switches** table.

5. Click the left arrow button.

   A message displays indicating that the ports will be moved to the default logical switch.

6. Click **OK** on the warning message.

   The selected ports are removed from the logical switch and automatically reassigned to the default logical switch. The selected ports are highlighted in the **Ports** table.

7. (*Optional*) Perform the following steps to assign the ports to a logical switch other than the default logical switch:

   a. Select the destination logical switch in the **Existing Logical Switches** table.

   b. Click the right arrow button.

      The ports display in the selected logical switch node in the **Existing Logical Switches** table.

8. Click **OK** on the **Logical Switches** dialog box.

   The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

   The **Re-Enable ports after moving them** and **QoS disable the ports while moving them** check boxes are selected by default.

   NOTE
   Ports are disabled before moving from one logical switch to another.

9. (*Optional*) Select the **Unbind Port Addresses while moving them** check box.
10. Click **Start** to send these changes to the affected chassis.

    NOTE
    Most changes to logical switches will disrupt data traffic in the fabric.

    The status of each change is displayed in the **Status** column and **Status** area in the dialog box.
11. When the changes are complete, click **Close**.

Deleting a logical switch

1. Select a switch on the Product List or Connectivity Map and select **Configure > Virtual Fabric > Logical Switches**.

   The **Logical Switches** dialog box displays.
2. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.
3. Select the logical switch you want to delete from the **Existing Logical Switches** table and click **Delete**.

   All ports in the deleted logical switch are reassigned to the default logical switch.
4. Read the confirmation message and click **Yes**.
5. Click **OK** on the **Logical Switches** dialog box.

   The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

   The **Re-Enable ports after moving them** and **QoS disable the ports while moving them** check boxes are selected by default.

   NOTE
   Ports are disabled before moving from one logical switch to another.
6. (*Optional*) Select the **Unbind Port Addresses while moving them** check box.
7. Click **Start** to send these changes to the affected chassis.

   NOTE
   Most changes to logical switches will disrupt data traffic in the fabric.

   The status of each change is displayed in the **Status** column and **Status** area in the dialog box.
8. When the changes are complete, click **Close**.

Configuring fabric-wide parameters for a logical fabric

When you create a logical switch, you must assign it to a fabric and configure fabric-wide parameters. All the switches in a fabric must have the same fabric-wide settings.

Instead of configuring these settings separately on each logical switch, you can create a *logical fabric template*, which defines the fabric-wide settings for a logical fabric. Then, when you create logical switches for that fabric, these fabric-wide settings are used automatically and you do not have to re-enter them.

Creating a logical fabric template does *not* create a logical fabric. A logical fabric is created only when you assign logical switches to a fabric ID (FID).

The logical fabric template exists only in the lifetime and scope of the **Logical Switches** dialog box. When you exit this dialog box, the logical fabric templates are deleted.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Virtual Fabric > Logical Switches**.

   The **Logical Switches** dialog box displays.

2. Select the physical chassis from which you want to create a logical fabric in the **Chassis** list.
3. Click **New Fabric**.

   The **New Logical Fabric Template** dialog box displays.

4. Enter a new identifier in the **Logical Fabric ID** field to create a new logical fabric template.

   This identifier is how you distinguish among multiple logical fabric templates in the **Logical Switches** dialog box. If you create more than one logical fabric template, give them different fabric IDs.

5. Enter new values for the fabric parameters or leave unchanged to accept the default values.

   Click the **Help** button for detailed information on each parameter.

   NOTE
   If you set the long distance fabric, it must be set on all devices in the fabric.

6. Click the **Switch** tab.
7. Select the **Insistent Domain ID** check box to guarantee that a switch operates only with its preassigned domain ID. If a duplicate domain ID exists, the switch will segment from the fabric instead of changing the domain ID.

   Leave this check box blank to allow the domain ID to be changed if a duplicate address exists.

8. Click **OK** on the **New Logical Fabric Template** dialog box.

   The new logical fabric template displays under the **Discovered Logical Switches** node in the **Existing Logical Switches** table (already highlighted).

   All of the logical fabric templates have the same name, "NewFabric". You can differentiate among the templates by the FID number.

   You can now create logical switches using the fabric-wide settings in the logical fabric template. To assign logical switches, refer to "Creating a logical switch or base switch" on page 424.

NOTE
When you close the **Logical Switches** dialog box, the logical fabric templates are automatically deleted. Create the logical switches first, before closing the dialog box, to use the template.

Applying logical fabric settings to all associated logical switches

You can apply a selected logical switch configuration to all logical switches in the same fabric. This configures the fabric parameters for the selected logical switch to all logical switches in the fabric.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Virtual Fabric > Logical Switches**.

   The **Logical Switches** dialog box displays.

2. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.

3. Right-click the logical switch for which you have configured logical fabric settings from the **Existing Logical Switches** table and select **Configure All**.

   The logical fabric configuration settings (**Fabric** tab) are applied to all logical switches in the same fabric (determined by FID).

4. Click **OK** on the **Logical Switches** dialog box.

   The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

   The **Re-Enable ports after moving them** and **QoS disable the ports while moving them** check boxes are selected by default.

NOTE
Ports are disabled before moving from one logical switch to another.

5. (*Optional*) Select the **Unbind Port Addresses while moving them** check box.

6. Click **Start** to send these changes to the affected chassis.

NOTE
Most changes to logical switches will disrupt data traffic in the fabric.

   The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

7. When the changes are complete, click **Close**.

Moving a logical switch to a different fabric

You can move a logical switch from one fabric to another by assigning a different fabric ID.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Virtual Fabric > Logical Switches**.

   The **Logical Switches** dialog box displays.

2. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.
3. Select the logical switch you want to move to another logical fabric.
4. Click **Edit**.

   The **Edit Properties** dialog box displays.

5. Change the FID in the **Logical Fabric ID** field.
6. Click **OK** on the **Edit Properties** dialog box.

   The logical switch displays under the new logical fabric node in the **Existing Logical Switches** table.

7. Click **OK** on the **Logical Switches** dialog box.

   The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

   The **Re-Enable ports after moving them** and **QoS disable the ports while moving them** check boxes are selected by default.

   NOTE
   Ports are disabled before moving from one logical switch to another.

8. (*Optional*) Select the **Unbind Port Addresses while moving them** check box.
9. Click **Start** to send these changes to the affected chassis.

   NOTE
   Most changes to logical switches will disrupt data traffic in the fabric.

   The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

10. When the changes are complete, click **Close**.
11. If the newly created switch is not part of a discovered fabric, then you must discover the switch.
    a. Undiscover the physical chassis. See “Deleting a fabric” on page 60 for instructions.
    b. Rediscover the physical chassis. See “Discovering fabrics” on page 53 for instructions.

       When entering the IP address, use the IP address of the physical fabric.

Changing a logical switch to a base switch

The **Base Switch** column in the **Existing Logical Switches** table indicates whether a logical switch is a base switch.

1. Select a switch on the Product List or Connectivity Map and select **Configure > Virtual Fabric > Logical Switches**.

   The **Logical Switches** dialog box displays.

2. Right-click anywhere in the **Existing Logical Switches** table and select **Table > Expand All**.
3. Select the logical switch you want to change to a base switch.
4. Click **Edit**.

   The **Edit Properties** dialog box displays.

5. Clear the **Base Fabric for Transport** check box.

   This check box is applicable only to logical switches that are *not* base switches.

6. Select the **Base Switch** check box.
7. Click **OK** on the **Edit Properties** dialog box.

   The **Base Switch** column in the **Existing Logical Switches** table now displays **Yes** for the logical switch.

8. Click **OK** on the **Logical Switches** dialog box.

   The **Logical Switch Change Confirmation and Status** dialog box displays with a list of all changes you made in the **Logical Switches** dialog box.

   The **Re-Enable ports after moving them** and **QoS disable the ports while moving them** check boxes are selected by default.

   NOTE
   Ports are disabled before moving from one logical switch to another.

9. (*Optional*) Select the **Unbind Port Addresses while moving them** check box.
10. Click **Start** to send these changes to the affected chassis.

    NOTE
    Most changes to logical switches will disrupt data traffic in the fabric.

    The status of each change is displayed in the **Status** column and **Status** area in the dialog box.

11. When the changes are complete, click **Close**.

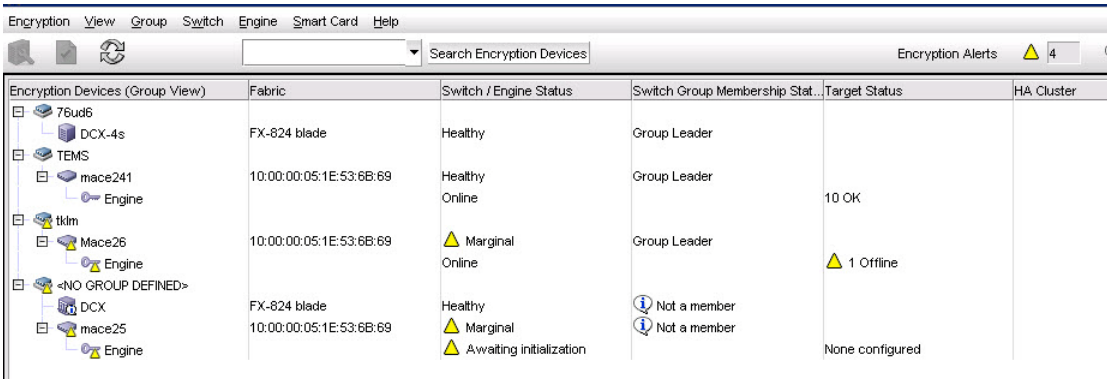
Chapter

SAN Encryption configuration 19

In this chapter

Encryption Center features

The **Encryption Center** dialog box is the single launching point for all encryption-related configuration in the Management application (Figure 153). It also provides a table that shows the general status of all encryption-related hardware and functions at a glance.



Encryption Devices (Group View)	Fabric	Switch / Engine Status	Switch Group Membership Stat...	Target Status	HA Cluster
76ud6					
DCX-4s	FX-824 blade	Healthy	Group Leader		
TEMS					
mace241	10:00:00:05:1E:53:6B:69	Healthy	Group Leader		
Engine		Online		10 OK	
tklm					
Mace26	10:00:00:05:1E:53:6B:69	⚠ Marginal	Group Leader		
Engine		Online		⚠ 1 Offline	
<NO GROUP DEFINED>					
DCX	FX-824 blade	Healthy	ⓘ Not a member		
mace25	10:00:00:05:1E:53:6B:69	⚠ Marginal	ⓘ Not a member		
Engine		⚠ Awaiting initialization		None configured	

FIGURE 153 Encryption Center dialog box

Beginning with Fabric OS 6.4, the Encryption Center is dynamically updated to reflect the latest changes based on any of the following events:

- Encryption group creation or deletion.
- A change in encryption group status.
- Addition or removal of an encryption group member.
- Addition or removal of an encryption engine.
- A change in encryption engine status.

If you are using the Encryption Center for the first time, please read the following topics before you begin to perform encryption operations:

- "Encryption user privileges" on page 435 describes the Role-based Access Control privileges that are specific to encryption.
- "Smart card usage" on page 436 and the topics that follow describe the options available for the use of Smart Cards for user authentication, system access control, and storing backup copies of data encryption master keys.
- "Network connections" on page 445 describes the network connections that must be in place to enable encryption.
- "Configuring blade processor links" on page 445 describes the steps for interconnecting encryption switches or blades in an encryption group through a dedicated LAN. This must be done before their encryption engines are enabled. Security parameters and certificates cannot be exchanged if these links are not configured and active.
- "Encryption node initialization and certificate generation" on page 446 lists the security parameters and certificates that are generated when an encryption node is initialized.
- "Supported encryption key manager appliances" on page 447 lists the supported key manager appliances, and lists topics that provide additional detail.

Encryption user privileges

In the Management application, resource groups are assigned privileges, roles, and fabrics. Privileges are not directly assigned to users; users get privileges because they belong to a role in a resource group. A user can only belong to one resource group at a time.

The Management application provides three pre-configured roles:

- Storage encryption configuration.
- Storage encryption key operations.
- Storage encryption security.

Table 34 lists the associated roles and their read/write access to specific operations. The functions are enabled from the **Encryption Center** dialog box:

TABLE 34

Privilege	Read/Write
Storage Encryption Configuration	• Launch the Encryption center dialog box. • View switch, group, or engine properties. • View the Encryption Group Properties Security tab. • View encryption targets, hosts, and LUNs. • View LUN centric view • View all re-key sessions • Add/remove paths and edit LUN configuration on LUN centric view • Re-balance encryption engines. • Clear tape LUN statistics • Create a new encryption group or add a switch to an existing encryption group. • Edit group engine properties (except for the Security tab) • Add targets. • Select encryption targets and LUNs to be encrypted or edit LUN encryption settings. • Edit encryption target hosts configuration. • Show tape LUN statistics.
Storage Encryption Key Operations	• Launch the Encryption center dialog box. • View switch, group, or engine properties, • View the Encryption Group Properties Security tab. • View encryption targets, hosts, and LUNs. • View LUN centric view. • View all re-key sessions. • Initiate manual re-keying of all disk LUNs. • Initiate refresh DEK. • Enable and disable an encryption engine. • Decommission LUNs. • Zeroize an encryption engine. • Restore a master key. • Edit key vault credentials. • Show tape LUN statistics.

TABLE 34

Privilege	Read/Write
Storage Encryption Security	• Launch the Encryption center dialog box. • View switch, group, or engine properties. • View Encryption Group Properties Security tab. • View LUN centric view. • View all re-key sessions. • View encryption targets, hosts, and LUNs. • Create a master key. • Backup a master key. • Edit smart card. • View and modify settings on the Encryption Group Properties Security tab (quorum size, authentication cards list and system card requirement). • Establish link keys for LKM key managers. • Show tape LUN statistics.

Smart card usage

Smart Cards are credit card-sized cards that contain a CPU and persistent memory. Smart cards can be used as security devices. You must have *Storage Encryption Security* user privileges to activate, register, and configure smart cards.

Smart cards can be used to do the following:

- Control user access to the Management application security administrator roles.
- Control activation of encryption engines.
- Securely store backup copies of master keys.

Smart card readers provide a plug-and-play interface that allows you to read and write to a smart card. The following smart card readers are supported:

- GemPlus GemPC USB

  http://www.gemalto.com/readers/index.html

- SCM MicrosystemsSCR331

  http://www.scmmicro.com/security/view_product_en.php?PID=2

NOTE
Only the Brocade smart cards that are included with the encryption switches are supported.

See the following procedures for instructions about how to manage smart cards:

- "Registering authentication cards from a card reader" on page 437
- "Registering system cards from a card reader" on page 442
- "Tracking smart cards" on page 443
- "Saving a master key to a smart card set" on page 541
- "Restoring a master key from a smart card set" on page 545

Registering authentication cards from a card reader

When authentication cards are used, one or more authentication cards must be read by a card reader attached to a Management application PC to enable certain security-sensitive operations. These include the following:

- Master key generation, backup, and restore operations.
- Replacement of authentication card certificates.
- Enabling and disabling the use of system cards.
- Changing the quorum size for authentication cards.
- Establishing a trusted link with the NetApp LKM key manager.
- Decommissioning LUNs.

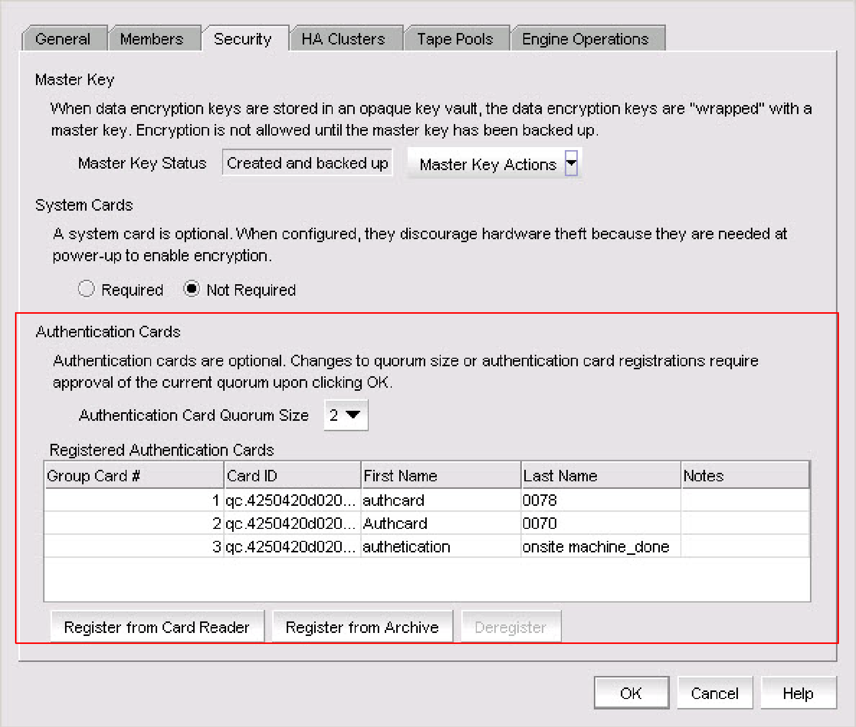
To register an authentication card or a set of authentication cards from a card reader, you must have the cards physically available. Authentication cards can be registered during encryption group or member configuration when running the configuration wizard, or they can be registered using the following procedure:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select an encryption group from the **Encryption Center Devices** table, then select **Group > Security** from the menu task bar, or right-click an encryption group and select **Security.**

   The **Encryption Group Properties** dialog box displays, with the **Security** tab selected (Figure 154).



Master Key

When data encryption keys are stored in an opaque key vault, the data encryption keys are "wrapped" with a master key. Encryption is not allowed until the master key has been backed up.

Master Key Status: Created and backed up

System Cards

A system card is optional. When configured, they discourage hardware theft because they are needed at power-up to enable encryption.

○ Required ● Not Required

Authentication Cards

Authentication cards are optional. Changes to quorum size or authentication card registrations require approval of the current quorum upon clicking OK.

Authentication Card Quorum Size: 2

Registered Authentication Cards

Group Card #	Card ID	First Name	Last Name	Notes
1	qc.4250420d020...	authcard	0078	
2	qc.4250420d020...	Authcard	0070	
3	qc.4250420d020...	authetication	onsite machine_done	

FIGURE 154 Encryption Group Properties dialog box - registering authentication cards

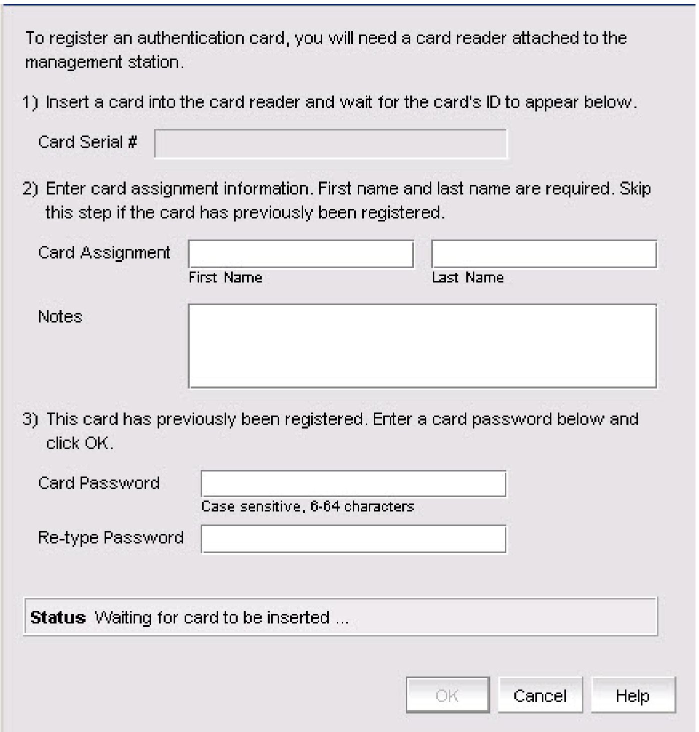
3. Locate the **Authentication Card Quorum Size** and select the quorum size from the list.

   The quorum size is the minimum number of cards necessary to enable the card holders to perform the security sensitive operations listed above. The maximum quorum size is five cards. The actual number of authentication cards registered is always more than the quorum size, so if you set the quorum size to five, for example, you will need to register at least six cards in the subsequent steps.

   NOTE
   Ignore the **System Cards** setting. Refer to "Tracking smart cards" on page 443 for information on its usage.

4. Click **Register from Card Reader** to register a new card.

   The **Add Authentication Card** dialog box displays (Figure 155).



To register an authentication card, you will need a card reader attached to the management station.

1) Insert a card into the card reader and wait for the card's ID to appear below.

Card Serial #

2) Enter card assignment information. First name and last name are required. Skip this step if the card has previously been registered.

Card Assignment: First Name, Last Name

Notes

3) This card has previously been registered. Enter a card password below and click OK.

Card Password — Case sensitive, 6-64 characters

Re-type Password

Status Waiting for card to be inserted ...

FIGURE 155 Add Authentication Card dialog box

5. Insert a smart card into the card reader. Wait for the card serial number to appear, then enter card assignment information as directed.
6. Click **OK**.
7. Wait for the confirmation dialog box indicating initialization is done, then click **OK**.

   The card is added to the **Registered Authentication Cards** table in the **Encryption Group Properties** dialog box.

8. Repeat step 5 through step 7 until you have successfully registered all cards. Ensure that the number of cards registered equals at least the quorum size plus one.

Registering authentication cards from the database

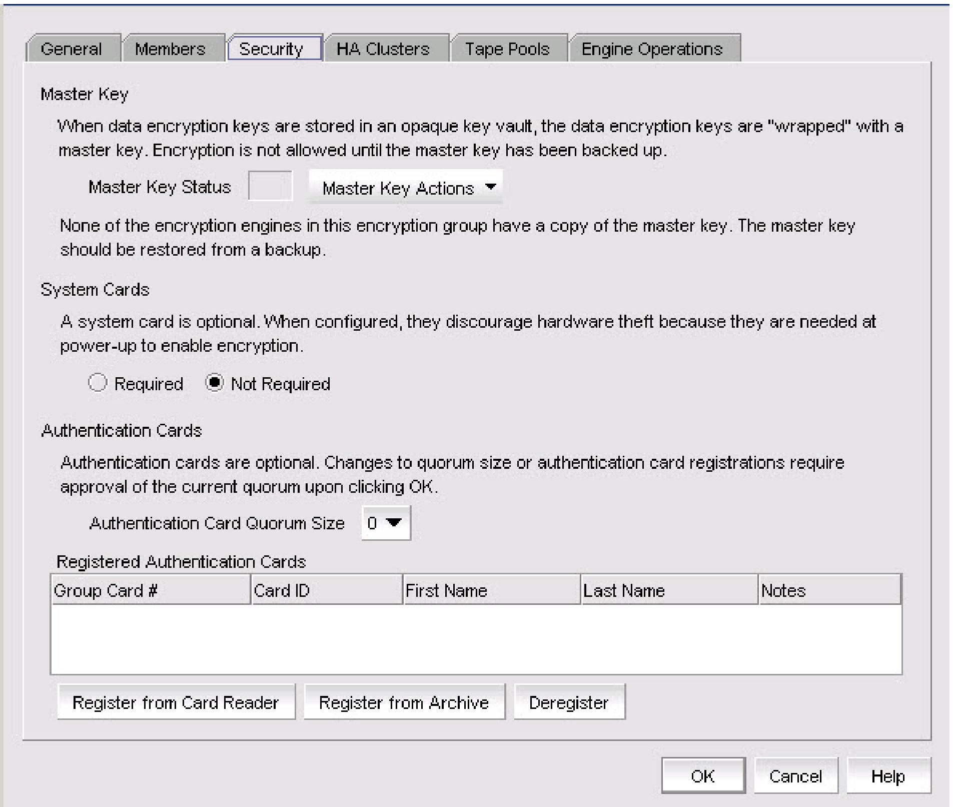
Smart cards that are already in the Management program's database can be registered as authentication cards.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select an encryption group from the **Encryption Center Devices** table, then select **Security** from the menu task bar, or right-click an encryption group and select **Security.**

   The **Encryption Group Properties** dialog box displays with the **Security** tab selected (Figure 156).



Master Key

When data encryption keys are stored in an opaque key vault, the data encryption keys are "wrapped" with a master key. Encryption is not allowed until the master key has been backed up.

Master Key Status

None of the encryption engines in this encryption group have a copy of the master key. The master key should be restored from a backup.

System Cards

A system card is optional. When configured, they discourage hardware theft because they are needed at power-up to enable encryption.

○ Required ● Not Required

Authentication Cards

Authentication cards are optional. Changes to quorum size or authentication card registrations require approval of the current quorum upon clicking OK.

Authentication Card Quorum Size 0

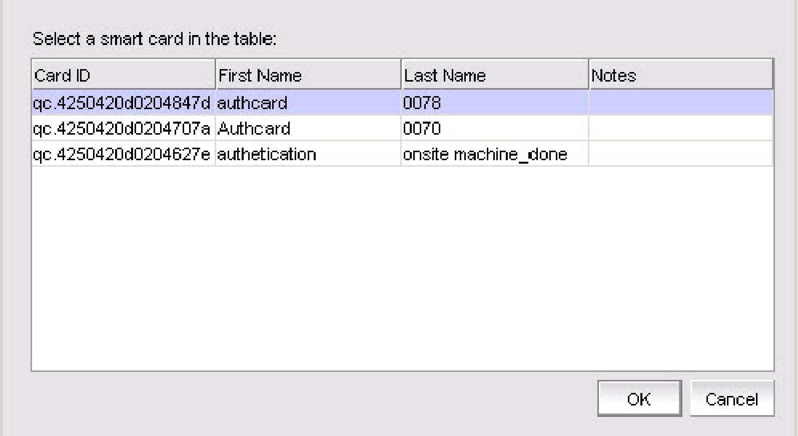
Registered Authentication Cards

Group Card #	Card ID	First Name	Last Name	Notes

FIGURE 156 Encryption Group Properties dialog box - Security tab

3. Click **Register from Archive.**

   The **Authentication Cards** dialog box displays (Figure 157). The dialog box lists the smart cards that are in the database.



Select a smart card in the table:

Card ID	First Name	Last Name	Notes
qc.4250420d0204847d	authcard	0078	
qc.4250420d0204707a	Authcard	0070	
qc.4250420d0204627e	authetication	onsite machine_done	

FIGURE 157 **Authentication Cards dialog box - registering smart cards from archive**

4. Select a card from the table, then click **OK.**
5. Wait for the confirmation dialog box indicating initialization is done, then click **OK.**

   The card is added to the **Registered Authentication Cards** table in the **Encryption Group Properties** dialog box. (Figure 154.)

Deregistering an authentication card

Authentication cards can be removed from the database and the switch by deregistering them. Use the following procedure to deregister an authentication card.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).
2. Select an encryption group from the **Encryption Center Devices** table, then select **Group > Security** from the menu task bar, or right-click an encryption group and select **Security.**

   The **Encryption Group Properties** dialog box displays, with the **Security** tab selected (Figure 154).
3. Select the authentication card in the **Registered Authentication Cards** table.
4. Click **Deregister.**
5. A confirmation dialog box displays. Click **Yes** to confirm deregistration.

   The registered authentication card is removed from the table.
6. Click **OK.**

   The card is deregistered from the group.

Using authentication cards

When a quorum of authentication cards is registered for use, an **Authenticate** dialog box is displayed to grant access to the following:

- The **Encryption Group Properties** dialog box **Link Keys** tab (for NetApp LKM only).
- The **Encryption Group Properties** dialog box **Security** tab, which provides access to the following:
  - **Master Key Actions**, which includes **Backup Master Key**, **Restore Master Key, and Create Master Key.**
  - **System Cards** radio buttons used to specify whether a system card is **Required** or **Not Required**.
  - **Authentication Card Quorum Size** selector.
  - **Register from Card Reader**, **Register From Archive**, and **Deregister** buttons.
- The **Master Key Backup** dialog box.
- The **Master Key Restore** dialog box.
- The **Decommission LUNs** dialog box.

To authenticate using a quorum of authentication cards, complete the following steps:

1. When the **Authenticate** dialog box is displayed, gather the number of cards needed, per instructions in the dialog box. The currently registered cards and the assigned owners are listed in the table near the bottom of the dialog box.
2. Insert a card, then wait for the ID to appear in the **Card ID** field.
3. Enter the assigned password.
4. Click **Authenticate**.
5. Wait for the confirmation dialog box, then click **OK**.
6. Repeat step 2 through step 5 for each card until at least the quorum plus one is reached.
7. Click **OK**.

Enabling or disabling the system card requirement

To use a system card to control activation of an encryption engine on a switch, you must enable the system card requirement. You can use the following procedure to enable or disable the system card requirement.

1. Select an encryption group from the **Encryption Center Devices** table, then select **Group > Security** from the menu task bar, or right-click a group and select **Security**.

   The **Encryption Group Properties** dialog box displays, with the **Security** tab selected (Figure 156).
2. Do one of the following:
   - Set **System Cards** to **Required** to require the use of a system card for controlling activation of the encryption engine. Click **OK** after reading the message in the encryption message dialog box.
   - Set **System Cards** to **Not Required** to permit activation of the encryption engine without the need to read a system card first.

Registering system cards from a card reader

System cards are smart cards that can be used to control activation of encryption engines. Encryption switches and blades have a card reader that enables the use of a system card. System cards discourage theft of encryption switches or blades by requiring the use of a system card at the switch or blade to enable the encryption engine. When the switch or blade is powered off, the encryption engine will not work without first inserting a system card into its card reader. If someone removes a switch or blade with the intent of accessing the encryption engine, it will function as an ordinary FC switch or blade when it is powered up, but use of the encryption engine is denied.

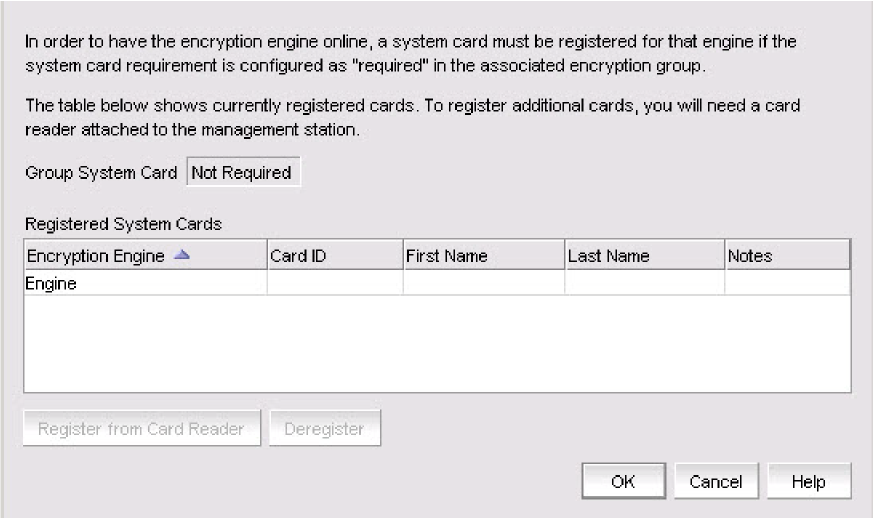
To register a system card from a card reader, a smart card must be physically available. System cards can be registered during encryption group creation or member configuration when running the configuration wizard, or they can be registered using the following procedure:

1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a switch from the **Encryption Center Devices** table, then select **Switch** > **System Cards** from the menu task bar, or right-click a switch and select **System Cards.**

   The **System Cards** dialog box displays (Figure 158).



In order to have the encryption engine online, a system card must be registered for that engine if the system card requirement is configured as "required" in the associated encryption group.

The table below shows currently registered cards. To register additional cards, you will need a card reader attached to the management station.

Group System Card: Not Required

Registered System Cards

Encryption Engine ▲	Card ID	First Name	Last Name	Notes
Engine				

FIGURE 158 System Cards dialog box

3. Insert a smart card into the card reader. Wait for the card serial number to appear, then enter card assignment information as directed.

4. Click **OK.**

5. Wait for the confirmation dialog box indicating initialization is done, then click **OK.**

   The card is added to the **Registered System Cards** table.

6. Store the card in a secure location, not in proximity to the switch or blade.

Deregistering a system card

System cards can be removed from the database by deregistering them. Use the following procedure to deregister a system card:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select the switch from the **Encryption Center Devices** table, then select **Switch > System Cards** from the menu task bar, or right-click the switch and select **System Cards.**

   The **System Cards** dialog box displays (Figure 158).

3. Select the system card to deregister.
4. Click **Deregister.**
5. A confirmation dialog box displays. Click **OK** to confirm deregistration.

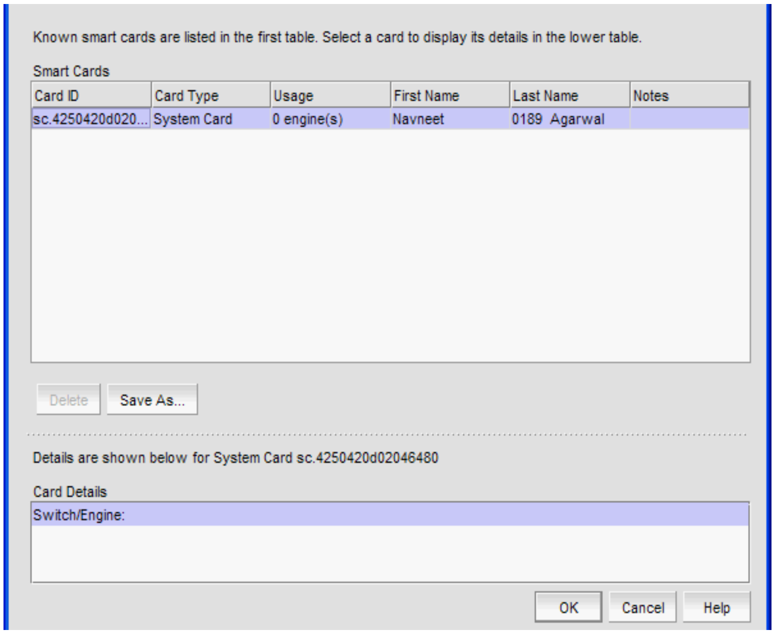
   The card is removed from the **Registered System Cards** table.

Tracking smart cards

Use the **Smart Card Tracking** dialog box to track smart card details.

1. From the **Encryption Center**, select **Smart Card > Smart Card Tracking**.

   The **Smart Card Asset Tracking** dialog box displays (Figure 159).



Known smart cards are listed in the first table. Select a card to display its details in the lower table.

Smart Cards

Card ID	Card Type	Usage	First Name	Last Name	Notes
sc.4250420d020...	System Card	0 engine(s)	Navneet	0189 Agarwal	

Details are shown below for System Card sc.4250420d02046480

Card Details

Switch/Engine:

FIGURE 159 Smart Card asset tracking dialog box

2. Select a smart card from the table, then do one of the following:

   - Click **Delete** to remove the smart card from the Management application database. Deleting smart cards from the Management application database keeps the **Smart Cards** table at a manageable size, but does not invalidate the smart card. The smart card can still be used. You must deregister a smart card to invalidate its use.

     NOTE
     The **Delete** operation applies only to recovery cards.

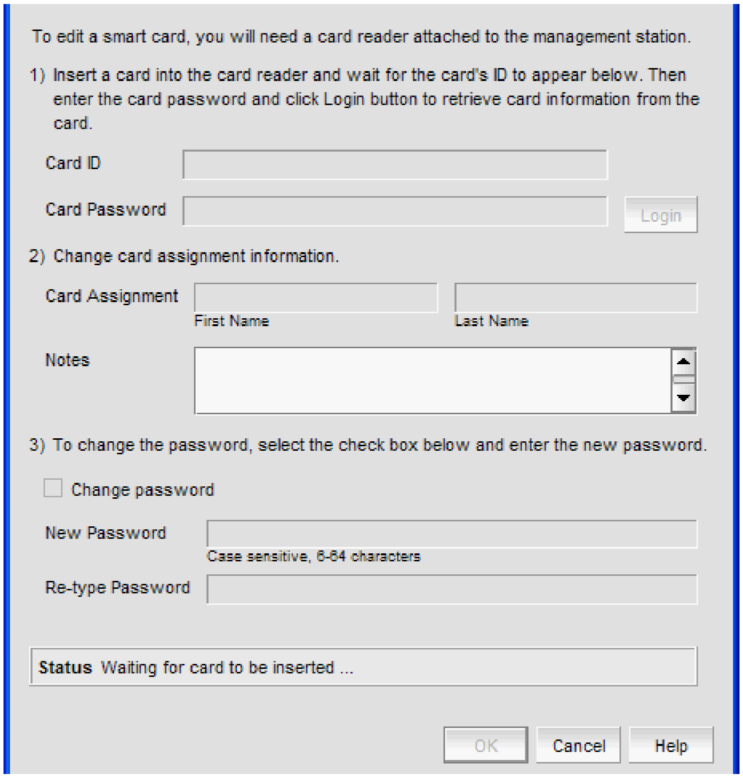
   - Click **Save As** to save the entire list of smart cards to a file. The available formats are comma-separated values (.csv) and HTML files (.html).

Editing smart cards

Use the **Edit Smart Card** dialog box to edit smart card details.

1. From the **Encryption Center** dialog box, select **Smart Card > Edit Smart Card** from the menu task bar.

   The **Edit Smart Card** dialog box displays (Figure 160).



To edit a smart card, you will need a card reader attached to the management station.

1) Insert a card into the card reader and wait for the card's ID to appear below. Then enter the card password and click Login button to retrieve card information from the card.

Card ID

Card Password

2) Change card assignment information.

Card Assignment

Notes

3) To change the password, select the check box below and enter the new password.

□ Change password

New Password

Case sensitive, 6-64 characters

Re-type Password

Status Waiting for card to be inserted ...

FIGURE 160 Edit Smart Card dialog box

2. Insert the smart card into the card reader.
3. After the card's ID is displayed in the **Card ID** field, enter the **Card Password**, then click **Login**.

4. Edit the card assignment user information as needed.
5. Click **OK**.

Network connections

Before you use the encryption setup wizard for the first time, you must have the following required network connections:

- The management ports on all encryption switches and 384-port Backbone Chassis CPs that have encryption blades installed must have a LAN connection to the SAN management program, and must be available for discovery.
- A supported key management appliance must be connected on the same LAN as the management port of the encryption switches, 384-port Backbone Chassis CPs, and the SAN Management program.
- In some cases, you might want to have an external host available on the LAN to facilitate certificate exchange between encryption nodes and the key management appliance. You may use the SAN management program host computer rather than an external host.
- All switches in the planned encryption group must be interconnected on a private LAN. This LAN is used to exchange security parameters and certificates, and to synchronize encryption engine operations. Refer to "Configuring blade processor links" on page 445 for details.

Configuring blade processor links

Each encryption switch or blade has two GbE ports labeled Ge0 and Ge1. The Ge0 and Ge1 ports are Ethernet ports that connect encryption switches and blades to other encryption switches and blades. Both ports of each encryption switch or blade must be connected to the same IP network and the same subnet. Static IP addresses should be assigned. Neither VLANs nor DHCP should be used. These two ports are bonded together as a single virtual network interface to provide link layer redundancy.

All encryption switches and blades in an encryption group must be interconnected by these links through a dedicated LAN before their encryption engines are enabled. Security parameters and certificates cannot be exchanged if these links are not configured and active.

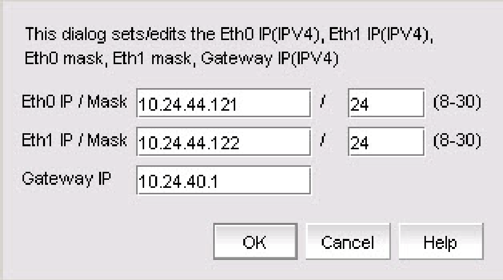
To configure blade processor links, complete the following steps:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select the encryption engine from the **Encryption Center Devices** table, then select **Engine > Blade Processor Link** from the menu task bar, or right-click the encryption engine and select **Blade Processor Link**.

   The **Blade Processor Link** dialog box displays (Figure 161).



This dialog sets/edits the Eth0 IP(IPV4), Eth1 IP(IPV4), Eth0 mask, Eth1 mask, Gateway IP(IPV4)

Eth0 IP / Mask 10.24.44.121 / 24 (8-30)

Eth1 IP / Mask 10.24.44.122 / 24 (8-30)

Gateway IP 10.24.40.1

FIGURE 161 Blade Processor Link dialog box

3. Enter the link IP address and mask, and the gateway IP address.
4. Click **OK**.

   The **Blade Processor Link** dialog box can also be launched from the following locations:

   - Select an encryption group from the **Encryption Center Devices** table, then select **Group > HA Clusters** from the menu task bar, or right-click a group and select **HA Clusters**. The Properties dialog box displays with the **HA Clusters** tab selected. Select a device from the **Non-HA Encryption Engines** table, then click **Configure Blade Processor Link**.
   - Select a group, switch, or engine from the **Encryption Center Devices** table, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets**. Select a container from the **Encryption Targets** table, click **LUNs**, then click **Configure Blade Processor Link**.

Encryption node initialization and certificate generation

When an encryption node is initialized, the following security parameters and certificates are generated:

- FIPS crypto officer
- FIPS user
- Node CP certificate
- A signed Key Authentication Center (KAC) certificate
- A KAC Certificate Signing Request (CSR)

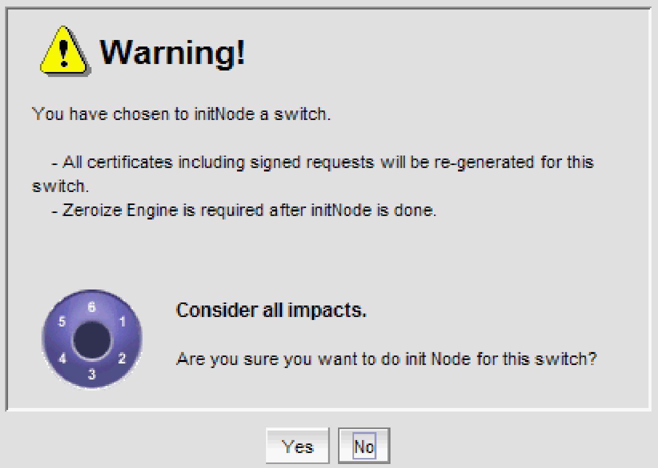
From the standpoint of external SAN management application operations, the FIPS crypto officer, FIPS user, and node CP certificates are transparent to users. The KAC certificates are required for operations with key managers. In most cases, KAC certificate signing requests must be sent to a Certificate Authority (CA) for signing to provide authentication before the certificate can be used. In all cases, signed KACs must be present on each switch.

Encryption nodes are initialized by the **Configure Switch Encryption** wizard when you confirm a configuration.

Encryption nodes may also be initialized from the **Encryption Center** dialog box.

1. Select a switch from the **Encryption Center Devices** table, then select **Switch > Init Node** from the menu task bar, or right-click a switch and select **Init Node**.

   A warning displays (Figure 162).



Warning!

You have chosen to initNode a switch.

- All certificates including signed requests will be re-generated for this switch.
- Zeroize Engine is required after initNode is done.

Consider all impacts.

Are you sure you want to do init Node for this switch?

FIGURE 162 Warning message

2. Select **Yes** to initialize the node.

Supported encryption key manager appliances

As stated under “Network connections”, a supported key management appliance must be connected on the same LAN as the management port of the encryption switches, or of the Backbone Chassis Control Processors (CPs) in the case of the encryption blade.

Secure communication between encryption nodes in an encryption group, and between encryption nodes and key manager appliances requires an exchange of certificates that are used for mutual authentication. Each supported key manager appliance has unique requirements for setting up a secure connection and exchanging certificates.

The following key manager appliances are supported:

- The RSA Key Manager (RKM)
- The NetApp Lifetime Key Manager (LKM)
- The HP StorageWorks Secure Key Manager (SKM)
- The Thales Encryption Manager for Storage (TEMS)
- The Tivoli Key Lifecycle Manager (TKLM)

Refer to the following topics for specific information:

- “Steps for Connecting to an RKM appliance” on page 448.
- “Connecting to an LKM appliance” on page 452.
- “Connecting to an SKM appliance” on page 457.
- “Connecting to a TEMS appliance” on page 466.
- “Connecting to a TKLM appliance” on page 469.

Steps for Connecting to an RKM appliance

All switches you plan to include in an encryption group must have a secure connection to the RSA Key Manager (RKM). The following is a suggested order of steps needed to create a secure connection to RKM:

1. Export the KAC CSR to a location accessible to a CA for signing.
2. Submit the KAC CSR for signing by a CA.
3. Import the signed certificate into the Fabric OS encryption node.
4. Upload the signed KAC and CA certificates onto the RKM appliance, and select the appropriate key classes.
5. If dual RKM appliances are used for high availability, the RKM appliances must be clustered, and must operate in maximum availability mode, as described in the RKM appliance user documentation.

These steps are described in more detail in the following sections:

- "Exporting the KAC certificate signing request (CSR)" on page 448
- "Submitting the CSR to a certificate authority" on page 449
- "Importing the signed KAC certificate" on page 449
- "Uploading the KAC and CA certificates onto the RKM appliance" on page 450
- "RKM key vault high availability deployment" on page 451

Exporting the KAC certificate signing request (CSR)

1. Export the KAC CSR to a temporary location prior to submitting the KAC CSR to a CA for signing.
2. Synchronize the time on the switch and the key manager appliance. They should be within one minute of each other. Differences in time can invalidate certificates and cause key vault operations to fail.
3. Select a switch from the **Encryption Center Devices** table, then select **Switch > Properties** from the menu task bar, or right-click the switch and select **Properties.**

   NOTE
   You can also select a switch from the **Encryption Center Devices** table, then click the **Properties** icon.

   The **Properties** dialog box displays.
4. Do one of the following:
   - If a CSR is present, click **Export.**
   - If a CSR is not present, select a switch from the **Encryption Center Devices** table, then select **Switch > Init Node** from the menu task bar, or right-click a switch and select **Init Node.** This generates switch security parameters and certificates, including the KAC CSR.

5. Save the file. The default location for the exported file is in the **Documents** folder.

NOTE
The CSR is exported in Privacy Enhanced Mail (.pem) format. This is the format required in exchanges with certificate authorities.

Submitting the CSR to a certificate authority

The CSR must be submitted to a CA to be signed. The certificate authority is a trusted third-party entity that signs the CSR. There are several CAs available and procedures vary, but the general steps are as follows:

1. Open an SSL connection to an X.509 server.
2. Submit the CSR for signing.
3. Request the signed certificate.

   Generally, a public key, the signed KAC certificate, and a signed CA certificate are returned.
4. Download and store the signed certificates.

The following example submits a CSR to the demoCA from RSA:

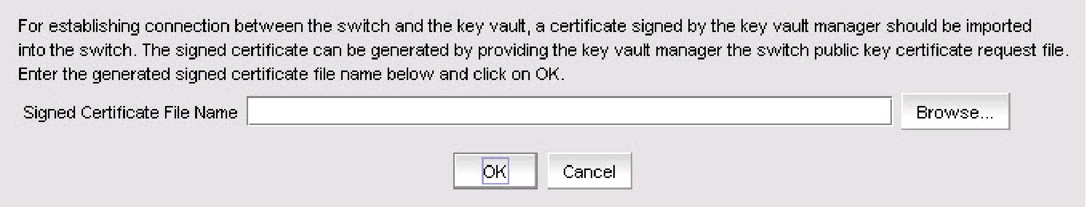
```
cd /opt/CA/demoCA
openssl x509 -req -sha1 -CAcreateserial -in certs/<Switch CSR Name> -days 365
-CA cacert.pem -CAkey private/cakey.pem -out newcerts/<Switch Cert Name>
```

Importing the signed KAC certificate

After a KAC CSR has been submitted and signed by a CA, the signed certificate must be imported into the switch.

1. Select a switch from the **Encryption Center Devices** table, then select **Switch > Import Certificate** from the menu task bar, or right-click a switch and select **Import Certificate.**

   The **Import Signed Certificate** dialog box displays (Figure 163).



For establishing connection between the switch and the key vault, a certificate signed by the key vault manager should be imported into the switch. The signed certificate can be generated by providing the key vault manager the switch public key certificate request file. Enter the generated signed certificate file name below and click on OK.

FIGURE 163 Import Signed Certificate dialog box

2. Browse to the location where the signed certificate is stored.
3. Click **OK.**

   The signed certificate is stored on the switch.

Uploading the KAC and CA certificates onto the RKM appliance

After an encryption group is created, you need to install the switch public key certificate (KAC certificate) and signing authority certificate (CA certificate) on the RKM appliance.

1. Open a web browser and connect to the RKM appliance setup page. You will need the URL and have the proper authority level, user name, and password.
2. Select the **Operations** tab.
3. Select **Certificate Upload**.
4. In the **SSLCAcertificateFile** field, enter the full local path of the CA certificate. Do not use the UNC naming convention format.
5. Select **Upload**, **Configure SSL**, and **Restart Webserver.**
6. After the web server restarts, enter the root password.
7. Open another web browser window, and start the RSA management user interface.

   You will need the URL, and have the proper authority level, user name, and password.

   NOTE
   The Identity Group name used in the next step might not exist in a freshly installed RKM. To establish an Identity Group name, click the **Identity Group** tab, and create a name. The name **Hardware Retail Group** is used as an example in the following steps.

8. Select the **Key Classes** tab. The key classes must be created only once, regardless of the number of nodes in your encryption group or the number of encryption groups that will be sharing this RKM.

   kcn.1998-01.com.brocade:DEK_AES_256_XTS

   kcn.1998-01.com.brocade:DEK_AES_256_CCM

   kcn.1998-01.com.brocade:DEK_AES_256_GCM

   kcn.1998-01.com.brocade:DEK_AES_256_ECB

   a. Click **Create.**
   b. Type the key name string into the **Name** field.
   c. Select **Hardware Retail Group** for **Identity Group.**
   d. Deselect **Activated Keys Have Duration.**
   e. Select **AES** for **Algorithm.**
   f. Select **256** for **Key Size.**
   g. Select the **Mode** for the respective key classes as follows:

      XTS for Key Class "kcn.1998-01.com.brocade:DEK_AES_256_XTS"

      CBC for Key Class "kcn.1998-01.com.brocade:DEK_AES_256_CCM"

      CBC for Key Class "kcn.1998-01.com.brocade:DEK_AES_256_GCM"

      ECB for Key Class "kcn.1998-01.com.brocade:DEK_AES_256_ECB"

   h. Click **Next.**
   i. Repeat step a through step h for each key class.

j. Click **Finish**.

9. For each encryption node, create an identity as follows:

   a. Select the **Identities** tab.

   b. Click **Create**.

   c. Enter a label for the node in the **Name** field. This is a user-defined identifier.

   d. Select the **Hardware Retail Group** in the **Identity Groups** field.

   e. Select the **Operational User** role in the **Authorization** field.

   f. Click **Browse** and select the imported certificate as the **Identity certificate**.

   g. Click **Save**.

RKM key vault high availability deployment

When dual RKM appliances are used for high availability, the RKM appliances must be clustered and must operate in maximum availability mode, as described in the RKM appliance user documentation.

When dual RKM appliances are clustered, they are accessed using an IP load balancer. For a complete high availability deployment, the multiple IP load balancers are clustered, and the IP load balancer cluster exposes a virtual IP address called a floating IP address. The floating IP address must be registered on the encryption group leader.

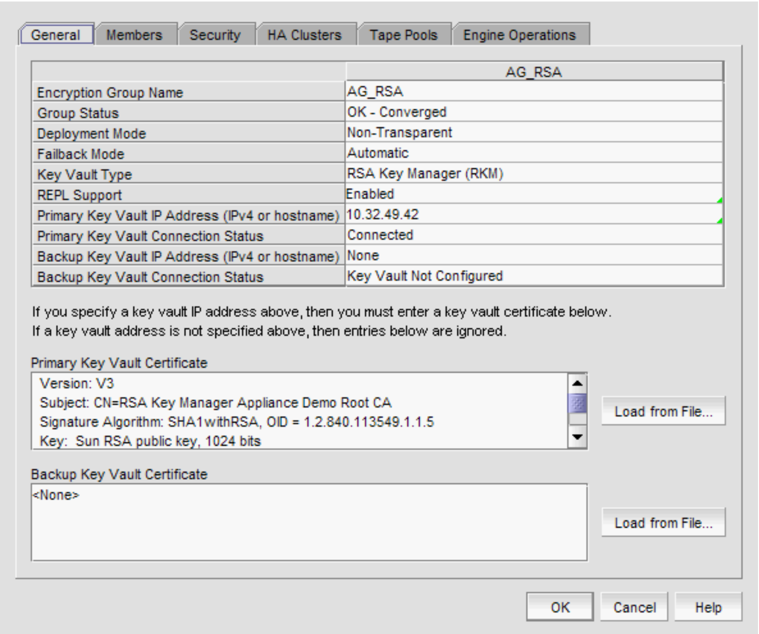
Neither the secondary RKM appliance nor individual RKM appliance IP addresses should be registered.

Loading the CA certificate onto the encryption group leader

The certificate for the CA that signed the switch KAC CSRs must be loaded onto the encryption group leader. The group leader can then distribute the CA certificate to the encryption group members.

1. From the **Encryption Center**, select a group from the **Encryption Center Devices** table, then select **Group > Properties** from the menu task bar, or right-click the group and select **Properties**. (If groups are not visible in the **Encryption Devices** table, select **View > Groups** from the menu bar first).

   The **Encryption Group Properties** dialog box displays with the **General** tab selected (Figure 164).



	AG_RSA
Encryption Group Name	AG_RSA
Group Status	OK - Converged
Deployment Mode	Non-Transparent
Failback Mode	Automatic
Key Vault Type	RSA Key Manager (RKM)
REPL Support	Enabled
Primary Key Vault IP Address (IPv4 or hostname)	10.32.49.42
Primary Key Vault Connection Status	Connected
Backup Key Vault IP Address (IPv4 or hostname)	None
Backup Key Vault Connection Status	Key Vault Not Configured

If you specify a key vault IP address above, then you must enter a key vault certificate below.
If a key vault address is not specified above, then entries below are ignored.

Primary Key Vault Certificate

```
Version: V3
Subject: CN=RSA Key Manager Appliance Demo Root CA
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5
Key:  Sun RSA public key, 1024 bits
```

Backup Key Vault Certificate

```
<None>
```

FIGURE 164 Encryption Group Properties with Key Vault Certificate

2. Select **Load from File**.

   A dialog box opens that allows you to browse to a location on your client PC that contains the downloaded CA certificate in .pem format.

Connecting to an LKM appliance

The NetApp Lifetime Key Manager (LKM) resides on an FIPS 140-2 Level 3-compliant network appliance. The encryption engine and LKM appliance communicate over a trusted link. A trusted link is a secure connection established between the Encryption switch or blade and the NetApp LKM appliance, using a shared secret called a link key.

The following configuration steps are performed from the NetApp DataFort Management Console and from the Management application:

- Install and launch the NetApp DataFort Management Console.
- Establish the trusted link.
- Obtain and import the LKM certificate.
- Export and register encryption node certificates on LKM.
- If required, create an LKM cluster for high availability.

These steps are described in more detail in the following sections:

- "The NetApp DataFort Management Console" on page 453
- "Establishing the trusted link" on page 453
- "Obtaining and importing the LKM certificate" on page 454
- "Exporting and registering the switch KAC certificates on LKM" on page 455
- "LKM key vault high availability deployment" on page 455

- “Disk keys and tape pool keys (Brocade native mode support)” on page 456
- “Tape LUN and DF -compatible tape pool support” on page 456
- “LKM Key Vault Deregistration” on page 456

The NetApp DataFort Management Console

The NetApp DataFort Management Console (DMC) must be installed on your PC or workstation to complete certain procedures described in this chapter. Refer to the appropriate DMC product documentation for DMC installation instructions. After you install DMC, complete the following steps:

1. Launch the DMC.
2. Click the **Appliance** tab on the top panel.
3. Add the NetApp LKM appliance IP address or hostname.
4. Right-click the added IP address and log in to the NetApp LKM key vault.

Establishing the trusted link

You must generate the trusted link establishment package (TEP) on all nodes to obtain a trusted acceptance package (TAP) before you can establish a trusted link between each node and the NetApp LKM appliance.

1. Select an LKM group from the **Encryption Center Devices** table, then select **Group > Link Keys** from the menu task bar, or right-click an LKM group and select **Link Keys.**

   The switch name displays in the link status table under **Switch**, with a **Link Key Status** of **Link Key requested, pending LKM approval**.

2. Select the switch, then click **Establish.**

   This results in a Trusted link establishment package (TEP), which is needed to establish the trusted link between the switch and the LKM appliance.

3. Launch the NetApp DataFort Management Console (DMC) and click the **View Unapproved Trustees** tab.

   The switch is listed as openkey_trustee_<ip address>, where the IP address is the switch IP address.

4. Select the switch, then click **Approve and Create TAP.**

   The **Approve TEP** dialog box displays. The TEP must be approved before a TAP can be created.

5. Provide a label in the dialog box, then click **Approve** to approve the TEP.

   A list of recovery cards and recovery officers is displayed. TEP approval is done by a quorum of recovery officers, using assigned recovery cards. Each recovery officer must individually insert one of the listed recovery cards into a card reader attached to the PC or workstation, then enter the password for that card and click **Start.** The procedure is repeated until a quorum of recovery officers has approved the TEP.

6. Save the TAP to a file (location does not matter).
7. Select the **Link Keys** tab from the **Encryption Group Properties** dialog box.

8. Select the switch in the link key status table, then click **Accept** to retrieve the TAP from the LKM appliance.
9. Repeat the above steps for each of the remaining member nodes.

Obtaining and importing the LKM certificate

Certificates must be exchanged between LKM and the encryption switch to enable mutual authentication. You must obtain a certificate from LKM, and import it into the encryption group leader. The encryption group leader exports the certificate to other encryption group members.

To obtain and import an LKM certificate, complete the following steps:

1. Open an SSH connection to the NetApp LKM appliance and log in.

```
host$ssh admin@10.33.54.231
admin@10.33.54.231's password:

Copyright (c) 2001-2009 NetApp, Inc.
All rights reserved
+-------------------------------+
| NetApp Appliance Management CLI |
|      Authorized use only!      |
+-------------------------------+
Cannot read termcapdatabase;
using dumb terminal settings.
Checking system tamper status:
No physical intrusion detected.
```

2. Add the group leader to the LKM key sharing group. Enter **lkmserver add --type third-party --key-sharing-group "/"** followed by the group leader IP address.

```
lkm-1>lkmserver add --type third-party --key-sharing-group \
    "/" 10.32.244.71
NOTICE: LKM Server third-party 10.32.244.71 added.
Cleartext connections not allowed.
```

3. On the NetApp LKM appliance terminal, enter **sys cert getcert-v2** to display the LKM certificate content.

```
lkm-1> sys cert getcert-v2
-----BEGIN CERTIFICATE-----
[content removed]
-----END CERTIFICATE-----
```

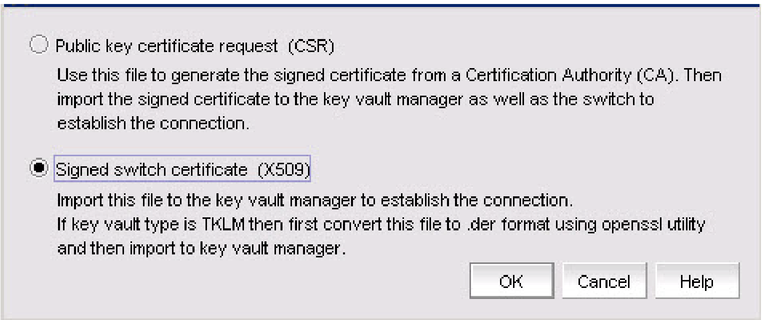
4. Copy and paste the LKM certificate content from the NetApp LKM appliance terminal into an editor buffer. Save the file as **lkmcert.pem** on the SCP-capable host. Save the entire certificate, including the lines `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----`.
5. If you are using the Management application, the path to the file must be specified on the **Select Key Vault** dialog box when creating a group leader. If the proper path is entered, the file is imported.

Exporting and registering the switch KAC certificates on LKM

The encryption switch signed KAC certificates must be exported and registered on the LKM appliance.

1. Select a switch from the **Encryption Center Devices** table, then select **Switch** > **Export Certificate** from the menu task bar, or right-click a switch and select **Export Certificate.**

   The **Export Switch Certificate** dialog box displays (Figure 165).



○ Public key certificate request (CSR)
Use this file to generate the signed certificate from a Certification Authority (CA). Then import the signed certificate to the key vault manager as well as the switch to establish the connection.

● Signed switch certificate (X509)
Import this file to the key vault manager to establish the connection.
If key vault type is TKLM then first convert this file to .der format using openssl utility and then import to key vault manager.

FIGURE 165 Export switch certificate dialog box

2. Select **Signed switch certificate** (X.509), then click **OK**.

   You are prompted to save the CSR, which can be saved to your SAN Management Program client PC, or an external host of your choosing.

3. Register the signed KAC certificate you exported from the member node with the NetApp LKM appliance.

LKM key vault high availability deployment

LKM appliances can be clustered to provide high availability capabilities. You can deploy and register one LKM with an encryption switch or blade and later deploy and register another LKM at any time if LKMs are clustered or linked together. Please refer to LKM documentation to link or cluster the LKMs.

When LKM appliances are clustered, both LKMs in the cluster must be registered and configured with the link keys before starting any crypto operations. If two LKM key vaults are configured, they must be clustered. If only a single LKM key vault is configured, it may be clustered for backup purposes, but it is not directly used by the switch.

When dual LKMs are used with the encryption switch or blade, the dual LKMs must be clustered. There is no enforcement done at the encryption switch or blade to verify whether or not the dual LKMs are clustered, but key creation operations will fail if you register non-clustered dual LKMs with the encryption switch or blade.

Regardless of whether you deploy a single LKM or clustered dual LKMs, register only the primary key vault with the encryption switch or blade. You do not need to register a secondary key vault.

Disk keys and tape pool keys (Brocade native mode support)

DEK creation, retrieval, and update for disk and tape pool keys in Brocade native mode are as follows:

- DEK creation - The DEK is archived into the primary LKM. Upon successful archival of the DEK onto the primary LKM, the DEK is read from the secondary LKM until it is either synchronized to the secondary LKM, or a timeout of 10 seconds occurs (2 seconds with 5 retries).
  - If key archival of the DEK to the primary LKM is successful, the DEK that is created can be used for encrypting disk LUNs or tape pools in Brocade native mode.
  - If key archival of the DEK to the primary LKM fails, an error is logged and the operation is retried. If the failure occurs after archival of the DEK to the primary LKM, but before synchronization to the secondary LKM, a VAULT_OFFLINE error is logged and the operation is retried. Any DEK archived to the primary LKM in this case is not used.
- DEK retrieval - The DEK is retrieved from the primary LKM if the primary LKM is online and reachable. If the registered primary LKM is not online or not reachable, the DEK is retrieved from a clustered secondary LKM.
- DEK Update - DEK update behavior is the same as DEK creation.

Tape LUN and DF -compatible tape pool support

- DEK creation - The DEK is created and archived to the primary LKM only. Upon successful archival of the DEK to the primary LKM, the DEK can be used for encryption of a Tape LUN or DF-Compatible tape pool. The DEK is synchronized to a secondary LKM through LKM clustering.

  If DEK archival to the primary LKM fails, DEK archival is retried to the clustered secondary LKM. If DEK archival also fails to the secondary LKM, an error is logged and the operation is retried.
- DEK retrieval - The DEK is retrieved from the primary LKM if the primary LKM is online and reachable. If the primary LKM is not online or reachable, the DEK is retrieved from the clustered secondary LKM.
- DEK update - DEK update behavior is the same as DEK creation.

LKM Key Vault Deregistration

Deregistration of either the primary or secondary LKM key vault from an encryption switch or blade is allowed independently.

- Deregistration of Primary LKM - You can deregister the Primary LKM from an encryption switch or blade without de-registering the backup or secondary LKM for maintenance or replacement purposes. However, when the primary LKM is de-registered, key creation operations will fail until either the primary LKM is re-registered, or the secondary LKM is de-registered and re-registered as the primary LKM.

  When the primary LKM is replaced with a different LKM, you must first synchronize the DEKs from the secondary LKM before re-registering the primary LKM.

- **Deregistration of Secondary LKM** - You can deregister the secondary LKM independently. Future key operations will use only the primary LKM until the secondary LKM is re-registered on the encryption switch or blade.

  When the secondary LKM is replaced with a different LKM, you must first synchronize the DEKs from the primary LKM before re-registering the secondary LKM.

Connecting to an SKM appliance

The SKM management web console can be accessed from any web browser with Internet access to the SKM appliance. The URL for the appliance is as follows:

```
https://<appliance hostname>:<appliance port number>
```

Where:

- `<appliance hostname>` is the hostname or IP address when installing the SKM appliance.
- `<appliance port number>` is 9443 by default. If a different port number was specified when installing the SKM appliance, use that port number.

The following configuration steps are performed from the SKM management web console and from the Management application:

- Configure a Brocade group on the SKM.
- Register the Brocade group user name and password on the encryption node.
- Set up a local CA on the SKM.
- Download the CA certificate.
- Create and install an SKM server certificate.
- Enable an SSL connection.
- Configure a cluster of SKM appliances for high availability.
- Export and sign the encryption node certificate signing requests.
- Import the signed certificates into the encryption node.

These steps are described in more detail in the following sections:

- “Configuring a Brocade group on SKM” on page 458
- “Registering the SKM Brocade group user name and password” on page 459
- “Setting up the local Certificate Authority (CA) on SKM” on page 460
- “Downloading the local CA certificate from SKM” on page 461
- “Creating and installing the SKM server certificate” on page 461
- “Enabling SSL on the Key Management System (KMS) Server” on page 462
- “Creating an SKM High Availability cluster” on page 463
- “Copying the local CA certificate for a clustered SKM appliance” on page 463
- “Adding SKM appliances to the cluster” on page 464
- “Signing the encryption node KAC certificates” on page 465
- “Importing a signed KAC certificate into a switch” on page 465

Configuring a Brocade group on SKM

A Brocade group is configured on SKM for all keys created by encryption switches and blades. This needs to be done only once for each key vault.

1. Log in to the SKM management web console using the admin password.
2. Select the **Security** tab.
3. Select **Local Users & Groups** under **Users and Groups**.

   The **User & Group Configuration** page displays.
4. Select **Add** under **Local Users.**
5. Create a Brocade user name and password.
6. Select the **User Administration Permission** and **Change Password Permission** check boxes.
7. Select **Save** to save this user data.
8. Select **Add** under **Local Groups**.
9. Add a Brocade group under **Group.**
10. Select **Save**.
11. Select the new Brocade group name, then select **Properties**.

    Local **Group Properties** and a **User List** are displayed.
12. In the **User List** section, select or type the Brocade user name under **Username**.
13. Select **Save**.

    The Brocade user name and password are now configured on SKM.

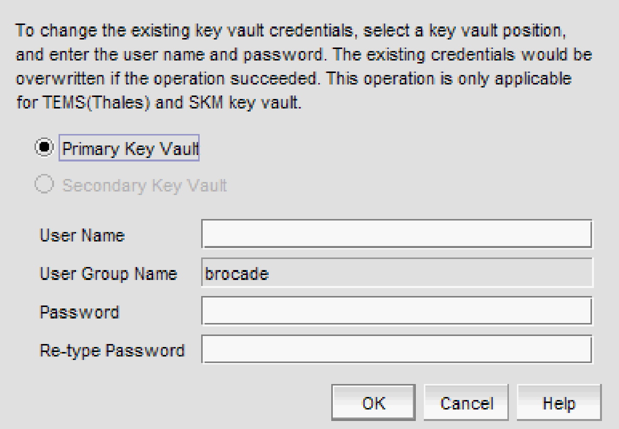
NOTE
Fabric OS 6.2.0 uses brcduser1 as a standard user name when creating a Brocade group on SKM. If you downgrade to version 6.2.0, the user name is overwritten to brcduser1, and the Brocade group user name must be changed to brcduser1.

Registering the SKM Brocade group user name and password

The Brocade group user name and password you created when configuring a Brocade group on SKM must also be registered on each encryption node.

1. Select the switch from the **Encryption Center Devices** table, then select **Switch > Key Vault Credentials** from the menu task bar, or right-click the switch and select **Key Vault Credentials**.

   The **Key Vault Credentials** dialog box displays (Figure 166).



To change the existing key vault credentials, select a key vault position, and enter the user name and password. The existing credentials would be overwritten if the operation succeeded. This operation is only applicable for TEMS(Thales) and SKM key vault.

● Primary Key Vault

○ Secondary Key Vault

User Name	
User Group Name	brocade
Password	
Re-type Password	

FIGURE 166 Key Vault Credentials dialog box

2. Enter the Brocade group user name and password.

   Keep the following rules in mind when registering the Brocade user name and password:

   - The user name and password must match the user name and password specified for the Brocade group.
   - The same user name and password must be configured on all nodes in an encryption group. This is not enforced or validated by the encryption group members, so care must be taken when configuring the user name and password to ensure they are the same on each node.
   - Different user names and passwords can never be used within the same encryption group, but each encryption group may have its own user name and password.
   - If you change the user name and password, the keys created by the previous user become inaccessible. The Brocade group user name and password must also be changed to the same values on SKM to make the keys accessible.
   - When storage is moved from one encryption group to another and the new encryption group uses a different user name and password, the Brocade group user name and password must also be changed to the same values on SKM to make the keys accessible.

3. Repeat the procedure for each node.

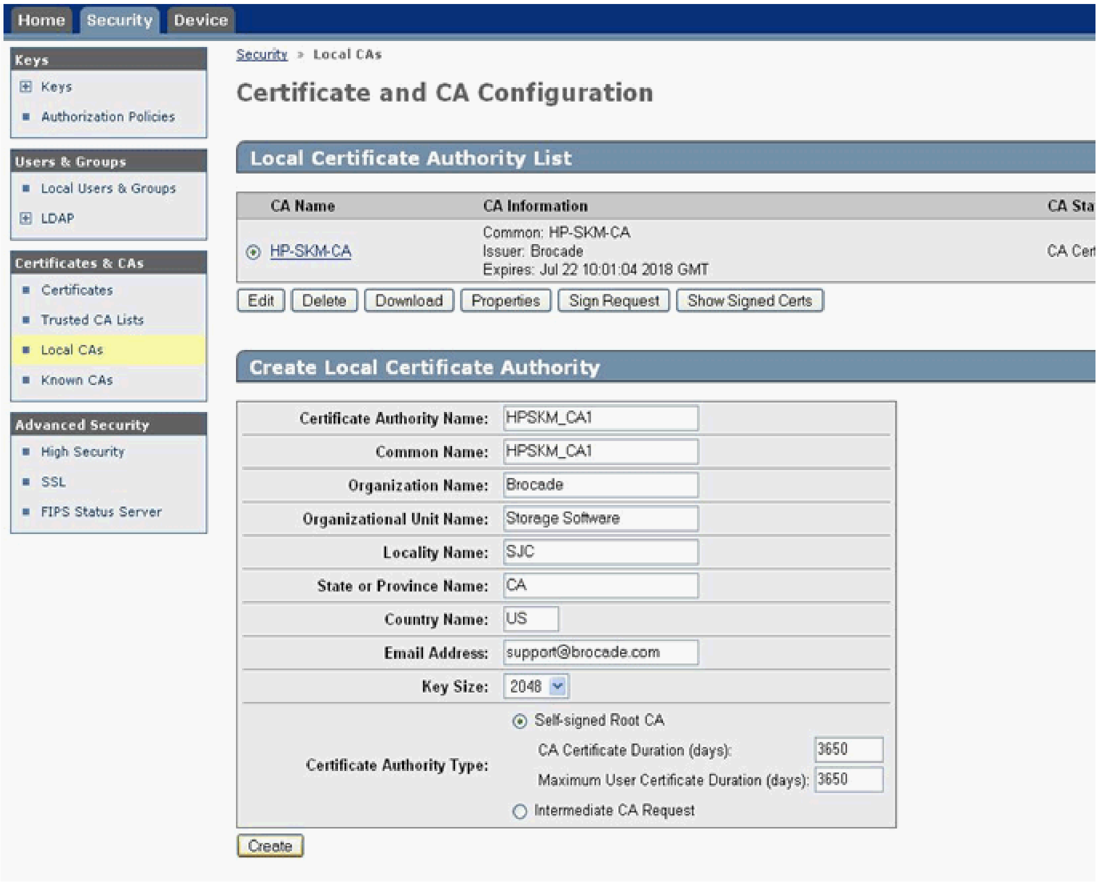
Setting up the local Certificate Authority (CA) on SKM

To create and install a local CA, complete the following steps:

1. Log in to the SKM management web console using the admin password.
2. Select the **Security** tab.
3. Under **Certificates & CAs**, click **Local CAs**.
4. Enter information required by the **Create Local Certificate Authorit**y section of the window to create your local CA.
   - Enter a **Certificate Authority Name** and **Common Name.** These may be the same value.
   - Enter your organizational information.
   - Enter the **Email Address** to receive messages for the Security Officer.
   - Enter the **Key Size.** HP recommends using 2048 for maximum security.
   - Select **Self-signed Root CA**.
   - Enter the **CA Certification Duration** and **Maximum User Certificate Duration.** These values determine when the certificate must be renewed and should be set in accordance with your company's security policies. The default value for both is 3650 days or 10 years.

5. Click **Create**.

   The new local CA displays under **Local Certificate Authority List** (Figure 167).



Certificate and CA Configuration

Local Certificate Authority List

CA Name	CA Information	CA Sta
⦿ HP-SKM-CA	Common: HP-SKM-CA Issuer: Brocade Expires: Jul 22 10:01:04 2018 GMT	CA Cert

Create Local Certificate Authority

Certificate Authority Name:	HPSKM_CA1
Common Name:	HPSKM_CA1
Organization Name:	Brocade
Organizational Unit Name:	Storage Software
Locality Name:	SJC
State or Province Name:	CA
Country Name:	US
Email Address:	support@brocade.com
Key Size:	2048
Certificate Authority Type:	⦿ Self-signed Root CA CA Certificate Duration (days): 3650 Maximum User Certificate Duration (days): 3650 ○ Intermediate CA Request

FIGURE 167 Creating an HP SKM Local CA

5. Under **Certificates & CAs**, select **Trusted CA Lists** to display the **Trusted Certificate Authority List Profiles.**
6. Click on **Default** under **Profile Name.**
7. In the **Trusted Certificate Authority List**, click **Edit.**
8. From the list of **Available CAs** in the right panel, select the CA you just created.

Repeat these steps any time another local CA is needed.

Downloading the local CA certificate from SKM

The local CA certificate you created using the procedure for "Setting up the local Certificate Authority (CA) on SKM" on page 460 must be saved to your local system. Later, this certificate must be imported onto the encryption group leader nodes.

1. From the **Security** tab, select **Local CAs** under **Certificates and CAs.**
2. Select the CA certificate you created.
3. Click **Download**, then save the certificate file on your local system.
4. Rename the downloaded file, changing the .cert extension to a .pem extension.

Creating and installing the SKM server certificate

To create the SKM server certificate, complete the following steps:

1. Click the **Security** tab.
2. Under **Certificates and CAs**, select **Certificates.**
3. Enter the required information under **Create Certificate Request.**
   - Enter a **Certificate Name** and **Common Name.** The same name may be used for both.
   - Enter your organizational information.
   - Enter the **E-mail Address** where you want messages to the Security Officer to go.
   - Enter the **Key Size.** HP recommends using the default value: 1024.
4. Click **Create Certificate Request.**

   Successful completion is indicated when the new entry for the server certificate appears on the **Certificate List** with a **Certificate Status** of **Request Pending.**
5. Select the newly created server certificate from the **Certificate List.**
6. Select **Properties.**

   The pending request displays under **Certificate Request Information.**
7. Copy the certificate data from ----BEGIN CERTIFICATE REQUEST---- to -----END CERTIFICATE REQUEST–––– lines. Be careful to exclude extra carriage returns or spaces after the data.
8. Under **Certificates & CAs**, select **Local CAs.**

   The **Certificate and CA Configuration** page is displayed.
9. From the **CA Name** column, select the name of the local CA you just created in "Setting up the local Certificate Authority (CA) on SKM" on page 460.

10. Click **Sign Request.**
11. Enter the required data in the **Sign Certificate Request** section of the window.
    - Select the CA name from the **Sign with Certificate Authority** drop down box.
    - Select **Server** as the **Certificate Purpose**.
    - Enter the number of days before the certificate must be renewed based on your site's security policies. The default value is 3649 or 10 years.
12. Paste the copied certificate request data into the **Certificate Request** box.
13. Click **Sign Request.**

    The signed certificate request data displays under **Sign Certificate Request.**
14. Click **Download** to download the signed certificate to your local system.
15. Copy the signed certificate data, from ----BEGIN to END...---- lines. Be careful to exclude extra carriage returns or spaces after the data.
16. From the **Security** tab select **Certificates** under **Certificates & CAs.**
17. Select the server certificate name you just created from the certificate list, and select **Properties.**

    The **Certificate Request Information** window displays.
18. Click **Install Certificate.**

    The **Certificate Installation** window displays.
19. Paste the signed certificate data you copied under **Certificate Response** and click **Save.**

    The status of the server certificate should change from **Request Pending** to **Active.**

Enabling SSL on the Key Management System (KMS) Server

The KMS Server provides the interface to the client. Secure Sockets Layer (SSL) must be enabled on the KMS Server before this interface will operate. After SSL is enabled on the first appliance, it will be enabled automatically on the other cluster members.

To configure and enable SSL, complete the following steps:

1. Select the **Device** tab.
2. In the **Device Configuration** menu, click **KMS Server** to display the **Key Management Services Configuration** window.
3. In the **KMS Server Settings** section of the window, click **Edit.**
4. Configure the KMS Server Settings. Ensure that the port and connection timeout settings are 9000 and 3600, respectively. For **Server Certificate**, select the name of the certificate you created in "Creating and installing the SKM server certificate" on page 461.
5. Click **Save.**

Creating an SKM High Availability cluster

The HP SKM key vault supports clustering of HP SKM appliances for high availability. If two SKM key vaults are configured, they must be clustered. If only a single SKM appliance is configured, it may be clustered for backup purposes, but the backup appliance will not be directly used by the switch. The procedures in this section will establish a cluster configuration on one SKM appliance and then transfer that configuration to the remaining appliances.

- Create the cluster on one SKM appliance that is to be a member of the cluster.
- Copy the local CA certificate from the first SKM appliance or an existing cluster member.
- Paste the local CA certificate into the management console for each of the SKM appliances added to the cluster.

To create a cluster, complete the following steps on one of the HP SKM appliances that is to be a member of the cluster:

1. From the SKM management console, click the **Device** tab.
2. In the **Device Configuration** menu, click **Cluster**.

   The **Create Cluster** section displays.
3. Select and note the **Local IP** address. You will need this address when you add an appliance to the cluster.
4. For **Local Port**, use the default value of 9001 unless you are explicitly directed to use a different value for your site.
5. Type the cluster password in the **Create Cluster** section of the main window to create the new cluster.
6. Click **Create**.
7. In the **Cluster Settings** section of the window, click **Download Cluster Key** and save the key to a convenient location, such as your computer's desktop. The cluster key is a text file and is only required temporarily. It may be deleted from your computer's desktop after all SKM appliances have been added to the cluster.

Copying the local CA certificate for a clustered SKM appliance

Before adding an SKM appliance to a cluster, you must obtain the local CA certificate from the original SKM or from an SKM that is already in the cluster.

1. Select the **Security** tab.
2. Select **Local CAs** under **Certificates & CAs**.
3. Select the name of the local CA from the **Local Certificate Authority** list.

   The **CA Certificate Information** is displayed.
4. Copy the certificate request, beginning with `---BEGIN CERTIFICATE REQUEST---` and ending with `---END CERTIFICATE REQUEST---`. Be careful not to include any extra characters.

Adding SKM appliances to the cluster

If you are adding an appliance to an existing cluster, select the Cluster Settings section of the window, click **Download Cluster Key**, then save the key to a convenient location, such as your computer's desktop.

To add SKM appliances to the cluster you are creating, you will need the original cluster member's local IP address and port number, and the location of the cluster key you downloaded, as specified in "Creating an SKM High Availability cluster" on page 463.

Complete the following steps on each SKM appliance you want to add to the cluster:

1. Open a new browser window, keeping the browser window from **Copying the Local CA certificate** open.
2. In the new browser window, log in to the management console of the SKM appliance that is being added to the cluster, then click the **Security** tab.
3. In the **Certificates & CAs** menu, click **Known CAs.**
4. Enter the information required in the **Install CA Certificate** section near the bottom of the page.
   - Enter the **Certificate Name** of the certificate being transferred from the first cluster member.
   - Paste the copied certificate data into the **Certificate** box.
5. Click **Install.**
6. In the **Certificates & CA** menu, click **Trusted CA Lists.**
7. Click **Default Profile Name.**
8. Click **Edit.**
9. Select the name of the CA from the list of **Available CAs** in the right panel.
10. Click **Add.**
11. Click **Save.**
12. Select the **Device** tab.
13. In the **Device Configuration** menu, click **Cluster.**
14. Click **Join Cluster.** In the **Join Cluster** section of the window, leave **Local IP** and **Local Port** set to their default settings.
15. Enter the original cluster member's local IP address into **Cluster Member IP.**
16. Enter the original cluster member's local Port into **Cluster Member Port.**
17. Click **Browse**, then select the **Cluster Key File** you saved.
18. Enter the cluster password into **Cluster Password.**
19. Click **Join.**
20. After adding all members to the cluster, delete the cluster key file from the desktop.
21. Create and install an SKM server certificate. Refer to "Creating and installing the SKM server certificate" on page 461 for a description of this procedure.

Signing the encryption node KAC certificates

The KAC certificate signing request generated when the encryption node is initialized must be exported for each encryption node and signed by the Brocade local CA on SKM. The signed certificate must then be imported back into the encryption node.

1. From the **Encryption Center**, select a switch, then select **Switch > Export Certificate.**

   The **Export Switch Certificate** dialog box displays.

2. Select **Public Key Certificate Request (CSR)**, then click **OK.**

   You are prompted to save the CSR, which can be saved to your SAN Management Program client PC, or an external host of your choosing.

   Alternatively, you may select a switch, then select **Switch > Properties**. Click the **Export** button beside the **Public Key Certificate Request**, or copy the CSR for pasting into the **Certificate Request Copy** area on the SKM **Sign Certificate Request** page.

3. Launch the SKM administration console in a web browser and log in.
4. Select the **Security** tab.
5. Select **Local CAs** under **Certificates & CAs.**

   The **Certificate and CA Configuration** page displays.

6. Under **Local Certificate Authority List**, select the Brocade CA name.
7. Select **Sign Request.**

   The **Sign Certificate Request** page displays.

8. Select **Sign with Certificate Authority** using the Brocade CA name and maximum of 3649 days.
9. Select **Client** as **Certificate Purpose.**
10. Allow Certificate **Duration** to default to 3649.
11. Paste the file contents that you copied in step 3 in the **Certificate Request Copy** area.
12. Select **Sign Request.**
13. Download the signed certificate to your local system as signed_kac_skm_cert.pem.

    This file is ready to be imported to the encryption switch or blade.

Importing a signed KAC certificate into a switch

After a KAC CSR has been submitted and signed by a CA, the signed certificate must be imported into the switch.

1. From the **Encryption Center**, select **Switch > Import Certificate.**

   The **Import Signed Certificate** dialog box displays.

2. Browse to the location where the signed certificate is stored.
3. Click **OK.**

   The signed certificate is stored on the switch.

Connecting to a TEMS appliance

TEMS provides a web user interface for management of clients, keys, admins, and configuration parameters. A Thales officer creates domains, groups, and managers (a type of administrator), assigns groups to domains, and assigns managers to manage groups. Managers are responsible for creating clients and passwords for the groups they manage.

The following configuration steps are performed from the TEMS web user interface and from the Management application:

- Set up network connections to TEMS.
- Create a TEMS client.
- Establish TEMS key vault credentials.
- Sign encryption node certificate signing requests.
- Import the signed requests onto the encryption nodes.

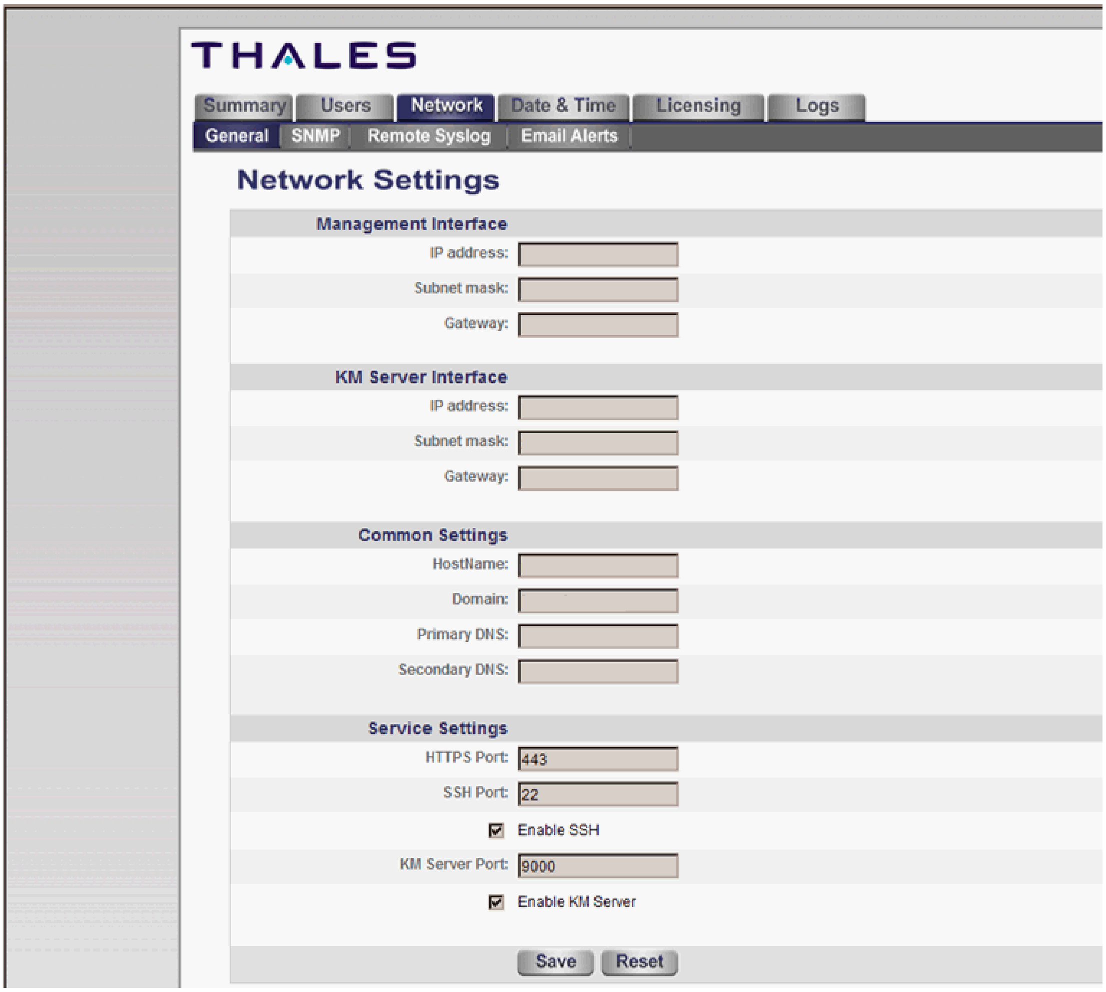
These steps are described in more detail in the following sections:

- "Setting up TEMS network connections" on page 466
- "Creating a client on TEMS" on page 468
- "Establishing TEMS key vault credentials on the switch" on page 469
- "Exporting the Fabric OS node self-signed KAC certificates" on page 470
- "Converting the KAC certificate format" on page 471

Setting up TEMS network connections

Communicating to TEMS is enabled over an SSL connection. Two IP addresses are needed. One IP address is used for the management interface, and a second IP address is used for communication with clients. These IP addresses are typically assigned during the initial setup of the TEMS appliance.

1. Log in to the Thales management program as admin and select the **Network** tab (Figure 168).



Network Settings

Management Interface

IP address:

Subnet mask:

Gateway:

KM Server Interface

IP address:

Subnet mask:

Gateway:

Common Settings

HostName:

Domain:

Primary DNS:

Secondary DNS:

Service Settings

HTTPS Port: 443

SSH Port: 22

☑ Enable SSH

KM Server Port: 9000

☑ Enable KM Server

FIGURE 168 TEMS Network Settings

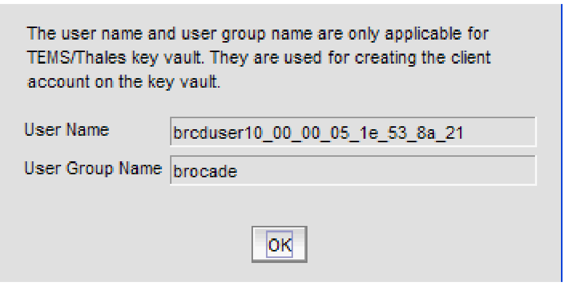
2. Enter the management IP address information under **Management Interface.**
3. Enter the client IP address information under **KM Server Interface.**
4. Enter a host name for the appliance, Internet or intranet domain, and, if used, the primary and secondary DNS IP address under **Common Settings.**
5. Set **Service Settings.**
   - HTTPS Port 433
   - SSH Port 22
   - Enable SSH
   - KM Server Port 9000
   - Enable KM Server

Creating a client on TEMS

This step assumes the group **brocade** has been created by an administrator. If the group **brocade** does not exist, you must log in to TEMS as **officer**, create the group, and assign the group to a manager.

1. From the **Encryption Center**, select a switch that needs to have a TEMS Client.
2. Select **Properties.**
3. Click **Key Vault User Name.**

   The **Key Vault User Information** dialog box displays (Figure 169).



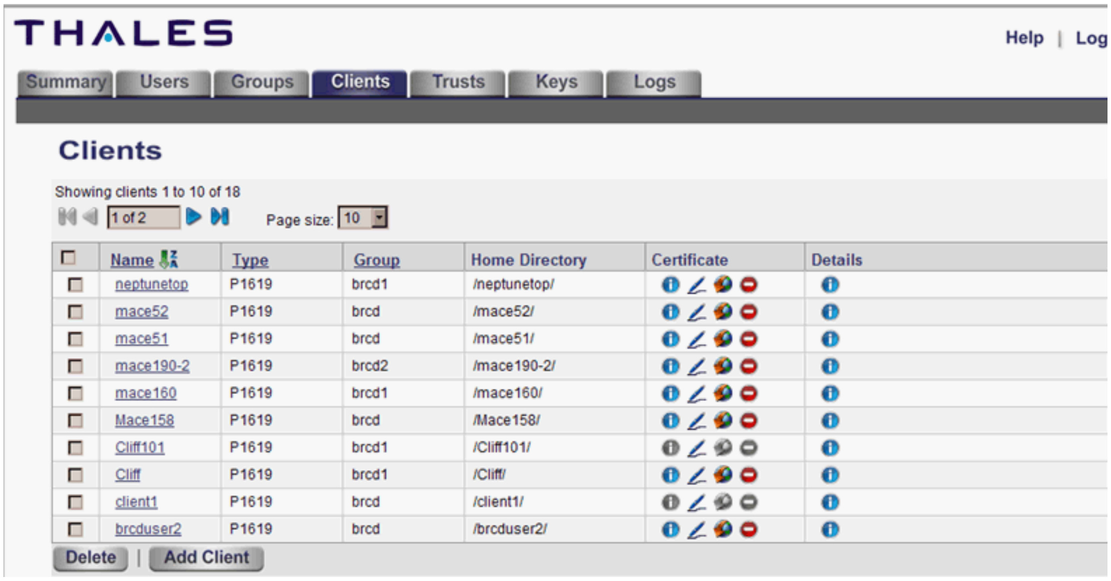
The user name and user group name are only applicable for TEMS/Thales key vault. They are used for creating the client account on the key vault.

User Name: brcduser10_00_00_05_1e_53_8a_21

User Group Name: brocade

FIGURE 169 TEMS Key Vault User Information

4. Copy the user name in the **User Name** field.
5. Log in to the Thales management program as a manager who has been assigned to the **brocade** group.
6. Select the **Clients** tab (Figure 170).



Clients

Showing clients 1 to 10 of 18

1 of 2 Page size: 10

□	Name	Type	Group	Home Directory	Certificate	Details
□	neptunetop	P1619	brcd1	/neptunetop/	ⓘ ✎ ● ⊖	ⓘ
□	mace52	P1619	brcd	/mace52/	ⓘ ✎ ● ⊖	ⓘ
□	mace51	P1619	brcd	/mace51/	ⓘ ✎ ● ⊖	ⓘ
□	mace190-2	P1619	brcd2	/mace190-2/	ⓘ ✎ ● ⊖	ⓘ
□	mace160	P1619	brcd1	/mace160/	ⓘ ✎ ● ⊖	ⓘ
□	Mace158	P1619	brcd	/Mace158/	ⓘ ✎ ● ⊖	ⓘ
□	Cliff101	P1619	brcd1	/Cliff101/	ⓘ ✎ ● ⊖	ⓘ
□	Cliff	P1619	brcd1	/Cliff/	ⓘ ✎ ● ⊖	ⓘ
□	client1	P1619	brcd	/client1/	ⓘ ✎ ● ⊖	ⓘ
□	brcduser2	P1619	brcd	/brcduser2/	ⓘ ✎ ● ⊖	ⓘ

FIGURE 170 TEMS Clients tab

7. Click the **Add Client** tab.
8. Enter the user name from step 4 in the **Name** field.

9. Enter a password in the **Password** and **Verify Password** fields.
10. Select the group **brocade** from the group pull-down menu.
11. Click **Add Client.**

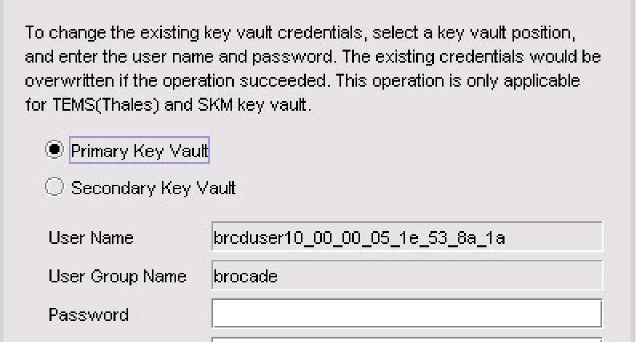
    A TEMS client user is created and is listed in the table.

Establishing TEMS key vault credentials on the switch

The credentials established for the TEMS client must be presented to TEMS by the switch.

1. From the Encryption Center, select a switch, then select **Switch** > **Key Vault Credentials** from the menu task bar, or right-click a switch and select **Key Vault Credentials.**

The Key Vault Credentials dialog box displays (Figure 171).



To change the existing key vault credentials, select a key vault position, and enter the user name and password. The existing credentials would be overwritten if the operation succeeded. This operation is only applicable for TEMS(Thales) and SKM key vault.

● Primary Key Vault

○ Secondary Key Vault

User Name: brcduser10_00_00_05_1e_53_8a_1a

User Group Name: brocade

Password:

FIGURE 171 Key Vault Credentials dialog box

2. Copy the user name and password used when creating the TEMS client.

   You may create different credentials, but if you do, you must change the TEMS client credentials to match the new credentials.

3. Click **OK.**

Connecting to a TKLM appliance

All switches you plan to include in an encryption group must have a secure connection to the Tivoli Key Lifecycle Manager (TKLM). A local LINUX host must be available to transfer certificates.

NOTE
Ensure that the time zone and clock time setting on the TKLM server and encryption nodes are the same. A difference of only a few minutes can cause the TLS connectivity to fail.

Repeat the same steps for configuring both the primary and secondary key vaults.

NOTE
The primary and secondary key vaults should be registered *before* you export the master key or encrypting LUNs. If the secondary key vault is registered *after* encryption is done for some of the LUNs, then the key database should be backed up and restored on the secondary TKLM from the registered primary TKLM before registering the secondary TKLM.

The following is a suggested order for the steps needed to create a secure connection to TKLM:

- Initialize all encryption nodes to generate KAC certificates and export the signed KAC certificates to a local LINUX host.
- Obtain the necessary user credentials and log in to the TKLM server appliance from the TKLM management web console.
- Create a default key store on TKLM.
- Create a device group named BRCD_ENCRYPTOR with device family LTO.
- Add devices to the group.
- Create a certificate for the TKLM server.
- Import the node KAC certificates.
- Export the server CA certificate to a LINUX or Windows host.
- Add encryption group members as needed. The first node added to an encryption group functions as the group leader. It is valid to have only one node in an encryption group.
- Import the server CA certificate and register TKLM on the encryption group leader nodes.
- Enable the encryption engines.

These configuration steps are described in the following sections:

- "Establishing a default key store and device group on TKLM" on page 471
- "Creating a self-signed certificate for TKLM" on page 471
- "Importing the Fabric OS encryption node KAC certificates to TKLM" on page 472
- "Exporting the TKLM self-signed server certificate" on page 473
- "Importing the TKLM certificate into the group leader" on page 474

Exporting the Fabric OS node self-signed KAC certificates

Each Fabric OS node generates a self-signed KAC certificate as part of the node initialization process as described under "Encryption node initialization and certificate generation". These certificates must be exported from each switch and stored on a local LINUX host to make them available for importing to TKLM.

1. Select a switch from the **Encryption Center Devices** table, then select **Switch > Export Certificate** from the menu task bar, or right-click the switch and select **Export Certificate.**

   The **Export Signed Certificate** dialog box displays.

2. Select **Signed switch certificate**, then click **OK.**

   A dialog box displays allowing you to save the signed certificate in .pem format in My Documents on your work station.

3. Make a note of this location.

Converting the KAC certificate format

The KAC certificate exported from the encryption switch is in .pem format. It is automatically converted to a .der format during the export process; however, if you need to manually convert the file before importing it to the TKLM server, you can do so by completing the following steps:

1. Go to openssl utility.
2. Run `openssl x509 -outform der -in KAC_Certificate_Name.pem -out KAC_Certificate_Name.der`.

Establishing a default key store and device group on TKLM

To establish a default key store and Fabric OS device group on TKLM, complete the following steps:

1. Obtain the necessary user credentials, then log in to the TKLM user interface.
2. Select Advanced Configuration > Keystore.

   The Keystore page displays.
3. Click OK to accept the default keystore settings.

Adding a device to the device group

After you have established a default key store and Fabric OS device group on TKLM, add a Fabric OS device to the device group.

1. Select Tivoli Key Lifecycle Manager > Welcome.

   The device group BRCD_ENCRYPTOR you just created is displayed in the Administration panel.
2. Click Go.

   The Configure Keys page displays. This page identifies this step as Step Two: Identify Drives.
3. Click Add on the Encryption Center Devices table menu task bar.

   An entry is added to the table.
4. Under Device Serial Number, enter the serial number that is displayed for each node that you are adding to the device group.

Creating a self-signed certificate for TKLM

You must create a self-signed certificate for TKLM that can be downloaded to the Fabric OS encryption engines to verify the authenticity of TKLM.

1. Select Tivoli Key Lifecycle Manager > Configuration.

   The Configuration page displays.
2. Select Create self-signed certificate.
3. Under Certificate label in key store, enter a certificate label.
4. Under Certificate description (common name), enter a descriptive name.
5. Under Validity period of new certificate, enter the desired life time for the certificate.

6. Select **Tivoli Key Lifecycle Manager** > **Advanced Configuration** > **Server Certificates** to verify that the certificate label is listed on **Administer Server Certificates** under **Certificates.**

7. Reboot the TKLM server.

Importing the Fabric OS encryption node KAC certificates to TKLM

The KAC certificates previously exported from the Fabric OS encryption nodes to an external LINUX host must now be imported into the TKLM server file system. You must import the KAC certificate in .der format. To do this, refer to "Converting the KAC certificate format" on page 471.

1. Import the KAC certificate from the external host into the TKLM server file system using a binary file transfer mechanism using FTP, USB, or SCP.

2. Select **Tivoli Key Lifecycle Manager** > **Advanced Configuration** > **Client Certificates.**

   The **Client Certificates** page displays.

3. Select **Import** > **SSL Certificate.**

   The **Import SSL/KMIP Certificates for Clients** page displays.

4. Enter the Fabric OS KAC certificate name in the **Certificate** field.

5. Under **File name and location**, enter or browse to the location where the imported KAC certificate is stored.

6. Select **Trust.**

7. Select **Import.**

8. Verify that the imported certificate is valid and active.

Exporting the TKLM self-signed server certificate

The TKLM self-signed server certificate must be exported in preparation for importing and registering the certificate on a Fabric OS encryption group leader node.

1. Enter the TKLM server wsadmin CLI.

   For Linux (in ./wsadmin.sh):

   ```
   <installed directory>/IBM/tivoli/tiptklmV2/bin/wsadmin.sh -username TKLMAdmin
   -password <password> -lang jython
   ```

   For Windows:

   ```
   <installed directory>\ibm\tivoli\tiptklmV2\bin\wsadmin.bat -username
   TKLMAdmin -password <password> -lang jython
   ```

2. Check the certificate list using the following command:

   ```
   print AdminTask.tklmCertList('[]')
   ```

   The listing will contain the uuid for all certificates. Use the uuid of the server certificate to export the server certificate from the database to the file system.

   ```
   print AdminTask.tklmCertExport('[
   -uuid <UUID of the certificate>
   -fileName <filename> -format DER]')
   ```

3. Exit the wsadmin CLI

   After export, the TKLM server certificate is at the following location:

   For LINUX:

   ```
   <installed directory>/ibm/tivoli/tiptklmV2/products/tklm/
   ```

   For Windows:

   ```
   <installed directory>\ibm\tivoli\tiptklmV2\products\tklm\
   ```

4. Transfer the TKLM certificate that was previously exported into the TKLM server file system to the Management application host using any binary file transfer mechanism via SCP, USB, or FTP.

Importing the TKLM certificate into the group leader

The TKLM certificate must be imported from the location on the LINUX host to the encryption group leader node. The encryption group leader exports the certificate to group member switches.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a switch from the **Encryption Center Devices** table, then select **Switch > Import Certificate** from the menu task bar, or right-click the switch and select **Import Certificate**.

   The **Import Signed Certificate** dialog box displays.

3. Browse to the location where the signed certificate is stored.

4. Click **OK**.

   The signed certificate is stored on the switch.

Encryption Preparation

Before you use the encryption setup wizard for the first time, you should have a detailed configuration plan in place and available for reference. The encryption setup wizard assumes the following:

- You have a plan in place to organize encryption devices into encryption groups.
- If you want redundancy and high availability in your implementation, you have a plan to create high availability (HA) clusters of two encryption switches or blades to provide failover support.
- All switches in the planned encryption group are interconnected on an I/O synch LAN.
- The management ports on all encryption switches and 384-port Backbone Chassis CPs that have encryption blades installed, have a LAN connection to the SAN management program and are available for discovery.
- A supported key management appliance is connected on the same LAN as the encryption switches, 384-port Backbone Chassis CPs, and the SAN Management program.
- An external host is available on the LAN to facilitate certificate exchange.
- Switch KAC certificates have been signed by a CA and stored in a known location.
- Key management system (key vault) certificates have been obtained and stored in a known location.

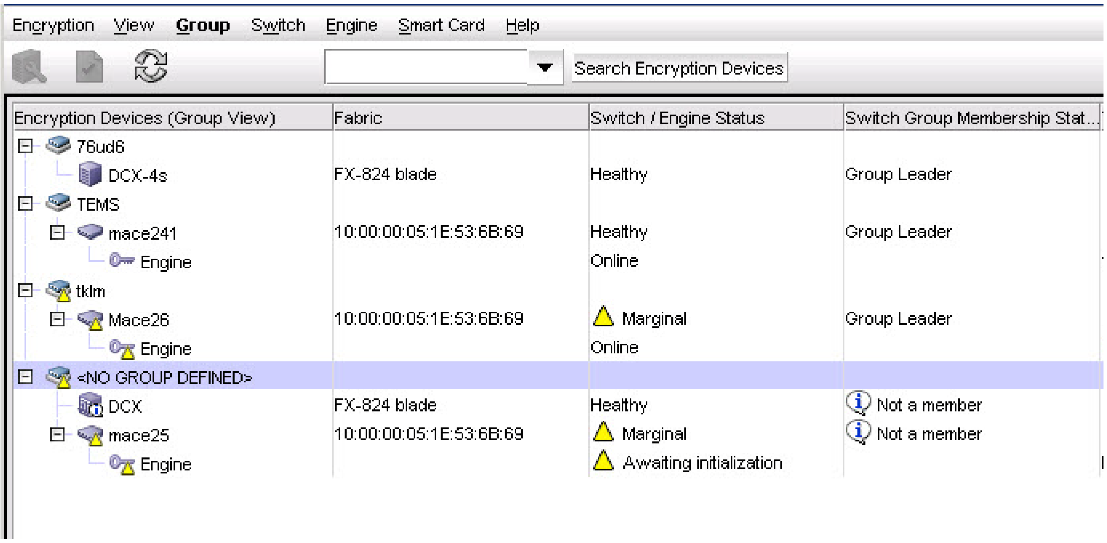
Creating a new encryption group

The following steps describe how to start and run the encryption setup wizard and create a new encryption group.

NOTE
When a new encryption group is created, any existing tape pools in the switch are removed.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 172).



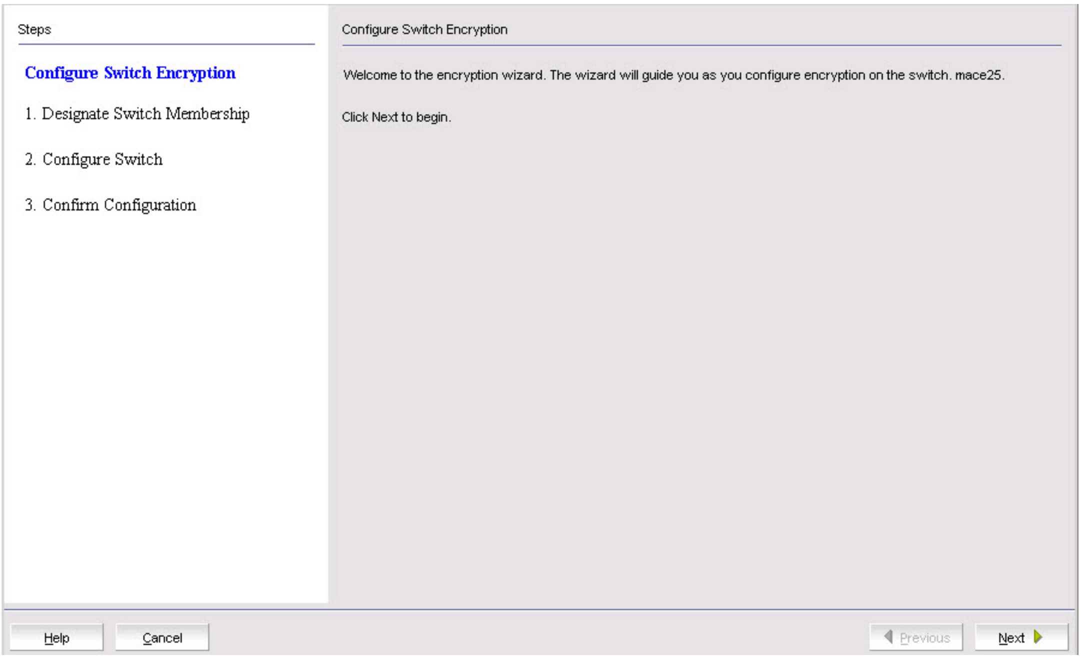
Encryption Devices (Group View)	Fabric	Switch / Engine Status	Switch Group Membership Stat...
76ud6			
DCX-4s	FX-824 blade	Healthy	Group Leader
TEMS			
mace241	10:00:00:05:1E:53:6B:69	Healthy	Group Leader
Engine		Online	
tklm			
Mace26	10:00:00:05:1E:53:6B:69	Marginal	Group Leader
Engine		Online	
<NO GROUP DEFINED>			
DCX	FX-824 blade	Healthy	Not a member
mace25	10:00:00:05:1E:53:6B:69	Marginal	Not a member
Engine		Awaiting initialization	

FIGURE 172 Encryption Center dialog box - No group defined

2. Select a switch from the **<NO GROUP DEFINED>** encryption group. (The switch must not be assigned to an encryption group.)

3. Select **Encryption > Create/Add to Group**, from the menu task bar, or right-click the switch and select **Create/Add to Group.**

   The **Configure Switch Encryption** wizard welcome panel displays(Figure 173).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
3. Confirm Configuration
Configure Switch Encryption

Welcome to the encryption wizard. The wizard will guide you as you configure encryption on the switch. mace25.

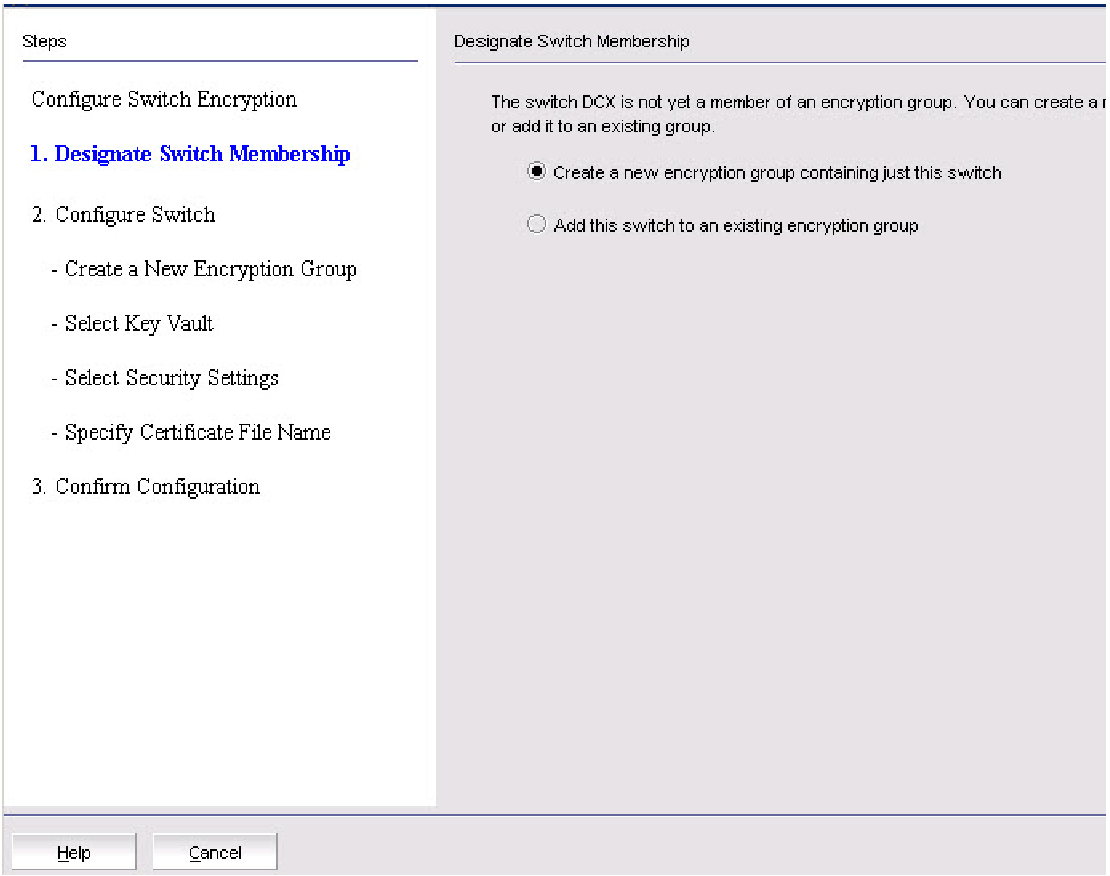
Click Next to begin.

Help
Cancel
Previous
Next

FIGURE 173 Configure Switch Encryption wizard - welcome panel

4. Click **Next.**

   The **Designate Switch Membership** dialog box displays (Figure 174).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Select Security Settings
- Specify Certificate File Name
3. Confirm Configuration
Designate Switch Membership
Help
Cancel

The switch DCX is not yet a member of an encryption group. You can create a r
or add it to an existing group.

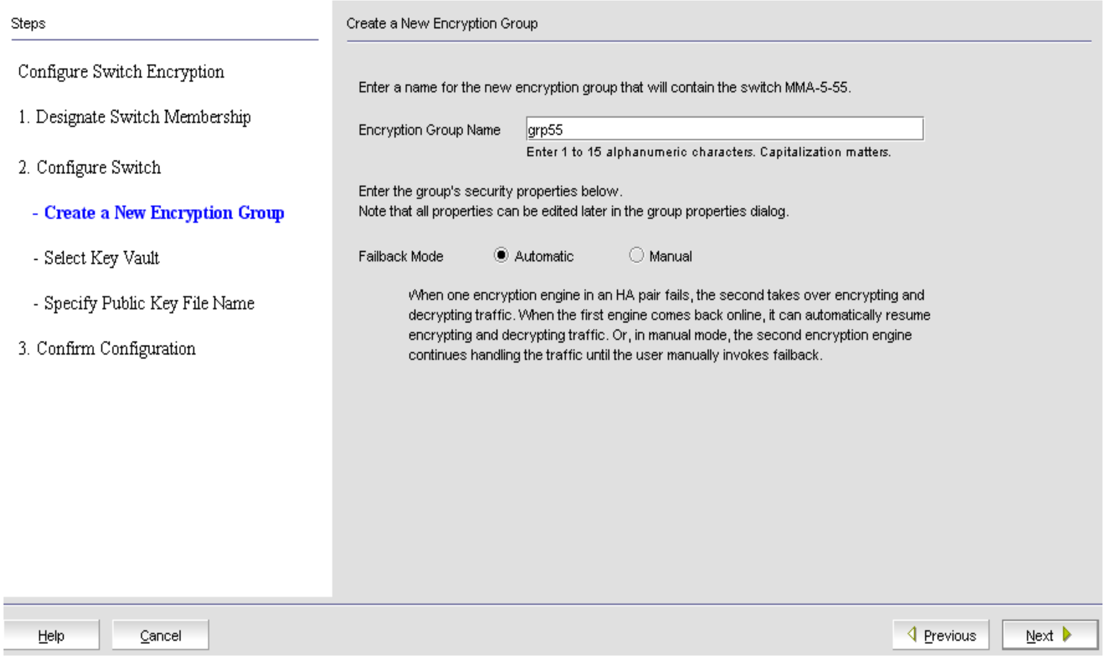
● Create a new encryption group containing just this switch

○ Add this switch to an existing encryption group

FIGURE 174 Designate Switch Membership dialog box

5. Verify that **Create a new encryption group containing just this switch** is selected.
6. Click **Next.**

   The **Create a New Encryption Group** dialog box displays (Figure 175).



Steps

Configure Switch Encryption

1. Designate Switch Membership

2. Configure Switch

- Create a New Encryption Group

- Select Key Vault

- Specify Public Key File Name

3. Confirm Configuration

Create a New Encryption Group

Enter a name for the new encryption group that will contain the switch MMA-5-55.

Encryption Group Name: grp55

Enter 1 to 15 alphanumeric characters. Capitalization matters.

Enter the group's security properties below.
Note that all properties can be edited later in the group properties dialog.

Failback Mode ● Automatic ○ Manual

When one encryption engine in an HA pair fails, the second takes over encrypting and decrypting traffic. When the first engine comes back online, it can automatically resume encrypting and decrypting traffic. Or, in manual mode, the second encryption engine continues handling the traffic until the user manually invokes failback.

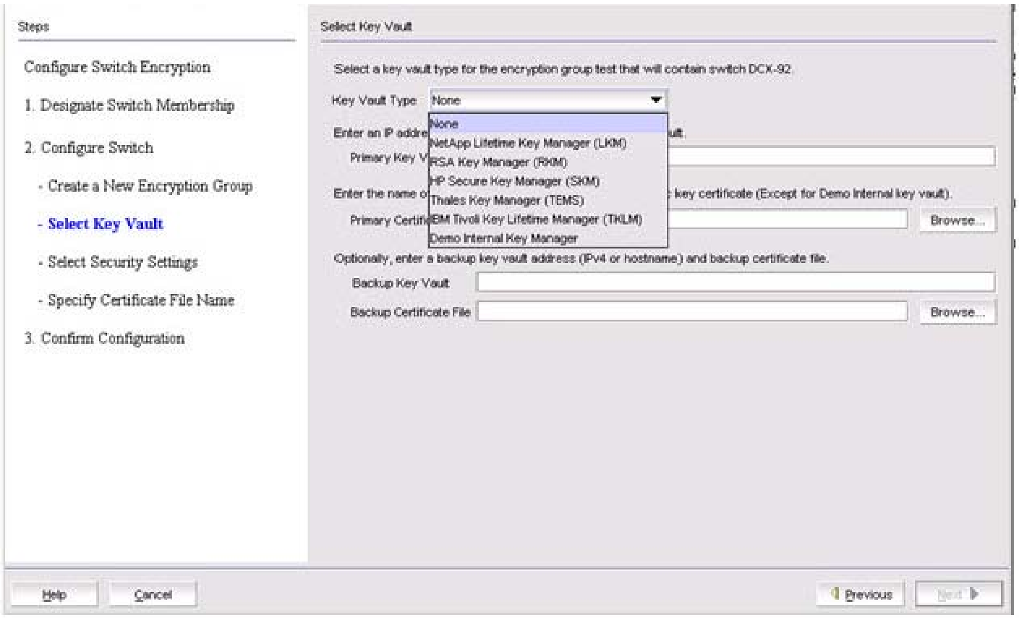
FIGURE 175 Create a New Encryption Group dialog box

7. Enter an **Encryption Group Name** for the encryption group and select **Automatic** failback mode. Encryption group names can have up to 15 characters. Letters, digits, and underscores are allowed.

   If the name for the encryption group already exists, a pop-up warning message displays. Although unique group names avoid confusion while managing multiple groups, you are not prevented from using duplicate group names. Click **Yes** to use the same name for the new encryption group, or click **No** to enter another name.

8. Click **Next.**

   The **Select Key Vault** dialog box displays (Figure 176).



Select a key vault type for the encryption group test that will contain switch DCX-92.

Key Vault Type: None

Enter an IP addre… …ult.

Enter the name o… …key certificate (Except for Demo Internal key vault).

Optionally, enter a backup key vault address (IPv4 or hostname) and backup certificate file.

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Select Security Settings
- Specify Certificate File Name
3. Confirm Configuration
Select Key Vault
None
NetApp Lifetime Key Manager (LKM)
RSA Key Manager (RKM)
HP Secure Key Manager (SKM)
Thales Key Manager (TEMS)
IBM Tivoli Key Lifetime Manager (TKLM)
Demo Internal Key Manager
Primary Key V
Primary Certifi
Browse...
Backup Key Vault
Backup Certificate File
Browse...
Help
Cancel
Previous
Next

FIGURE 176 Select Key Vault dialog box

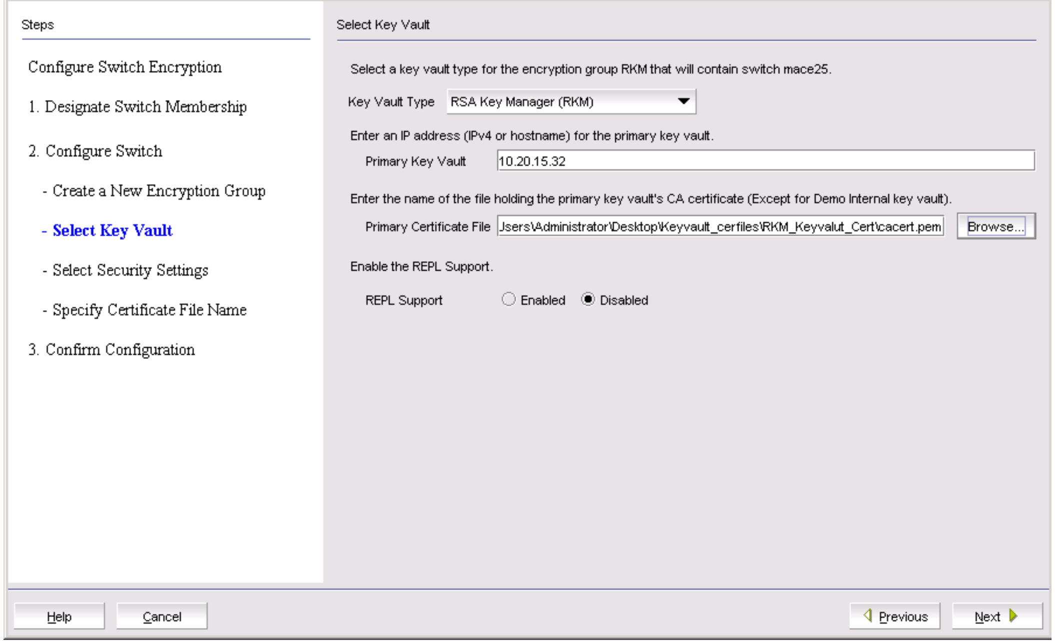
9. Select the **Key Vault Type**. Configuration options vary based on the key vault type you choose. To complete the wizard steps, proceed to the section that describes your particular key vault type. Key vault types are:

   - RSA Key Manager (RKM). For RKM key vault setting instructions, see "Configuring key vault settings for RSA Key Manager (RKM)" on page 480.
   - NetApp Link Key Manager (LKM). For LKM key vault setting instructions, see "Configuring key vault settings for NetApp Link Key Manager (LKM)" on page 485.
   - HP Secure Key Manager (SKM). For SKM key vault setting instructions, see "Configuring key vault settings for HP Secure Key Manager (SKM)" on page 490.
   - Thales Encryption Manager for Storage (TEMS). For TEMS key vault setting instructions, see "Configuring key vault settings for Thales Key Manager (TEMS)" on page 495.
   - Tivoli Key Lifetime Manager (TKLM). For TKLM key vault setting instructions, see "Configuring key vault settings for IBM Tivoli Key Lifetime Manager (TKLM)" on page 500.

Configuring key vault settings for RSA Key Manager (RKM)

The following procedure assumes you have already configured the initial steps in the **Configure Switch Encryption** wizard. If you have not already done so, go to "Creating a new encryption group" on page 475.

Figure 177 shows the key vault selection dialog box for RKM.



Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Select Security Settings
- Specify Certificate File Name
3. Confirm Configuration
Select Key Vault
Browse...
Help
Cancel
Previous
Next

Select a key vault type for the encryption group RKM that will contain switch mace25.

Key Vault Type: RSA Key Manager (RKM)

Enter an IP address (IPv4 or hostname) for the primary key vault.

Primary Key Vault: 10.20.15.32

Enter the name of the file holding the primary key vault's CA certificate (Except for Demo Internal key vault).

Primary Certificate File: Jsers\Administrator\Desktop\Keyvault_cerfiles\RKM_Keyvalut_Cert\cacert.pem

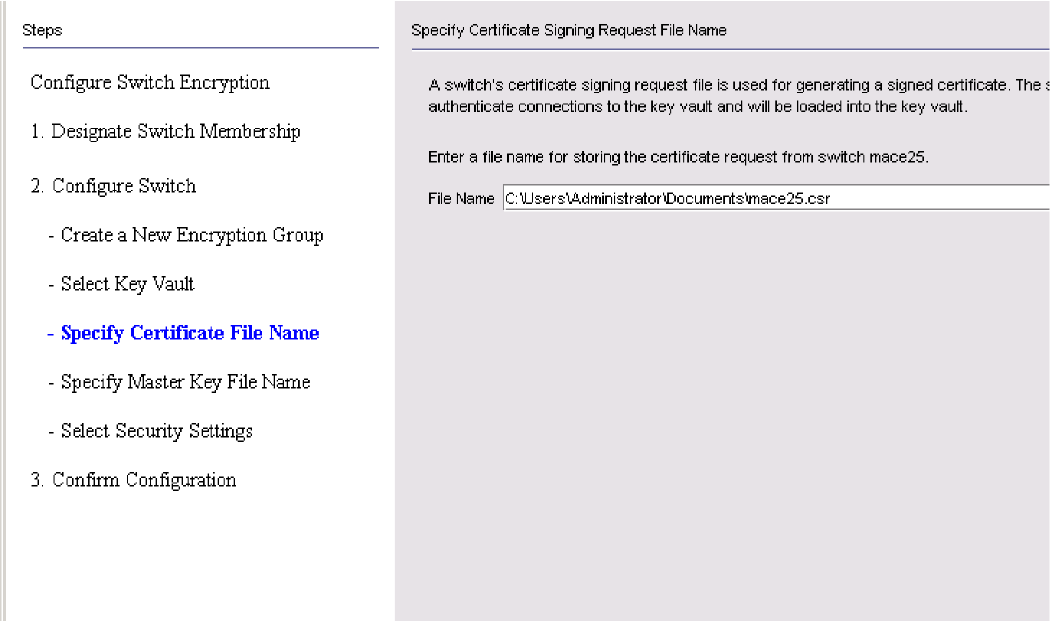
Enable the REPL Support.

REPL Support ○ Enabled ● Disabled

FIGURE 177 Select Key Vault dialog box for RKM

1. Enter the IP address or host name for the primary key vault. If you are clustering RKM appliances for high availability, IP load balancers are used to direct traffic to the appliances. Use the IP address of the load balancer.
2. Enter the name of the file that holds the Primary Key Vault's CA Key Certificate or browse to the desired location.
3. If you are implementing encryption on data replication LUNs used by the EMC Symmetrix Remote Data Facility (SRDF), you must select **Enabled** for **REPL Support**.
4. Click **Next**.

   The **Specify Certificate Signing Request File Name** dialog box displays (Figure 178).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration

Specify Certificate Signing Request File Name

A switch's certificate signing request file is used for generating a signed certificate. The s
authenticate connections to the key vault and will be loaded into the key vault.

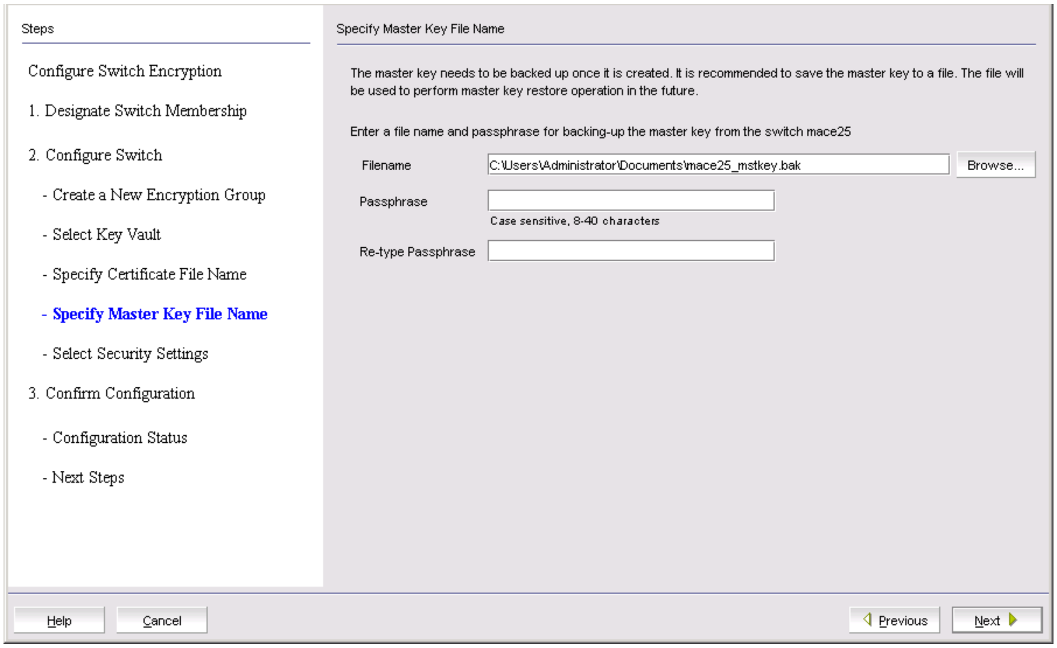
Enter a file name for storing the certificate request from switch mace25.

File Name C:\Users\Administrator\Documents\mace25.csr

FIGURE 178 Specify Certificate Signing Request File Name dialog box

5. Enter the location of the file where you want to store the certificate information, or browse to the desired location.
6. Click **Next**.

   The **Specify Master Key File Name dialog box** displays (Figure 179).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Browse...
Help
Cancel
Previous
Next

Specify Master Key File Name

The master key needs to be backed up once it is created. It is recommended to save the master key to a file. The file will be used to perform master key restore operation in the future.

Enter a file name and passphrase for backing-up the master key from the switch mace25

Filename C:\Users\Administrator\Documents\mace25_mstkey.bak

Passphrase

Case sensitive, 8-40 characters

Re-type Passphrase

FIGURE 179 Specify Master Key File Name dialog box

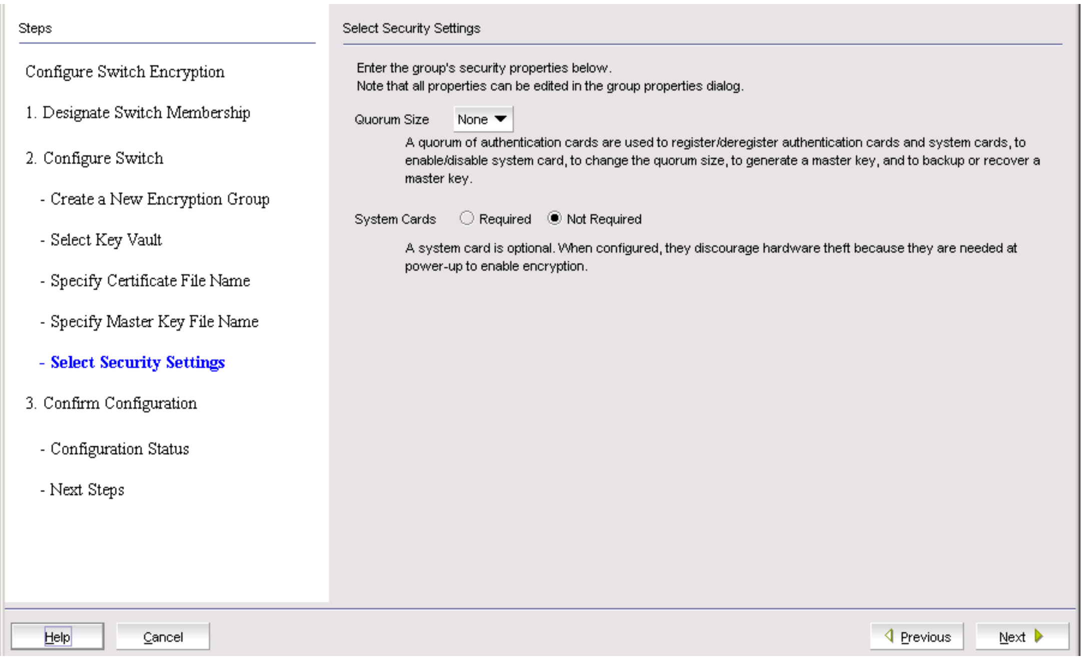
7. Enter the location of the file where you want to store back up master key information, or browse to the desired location.

8. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.

9. Re-enter the passphrase for verification.

10. Click **Next**.

    The **Select Security Settings** dialog box displays (Figure 180).



Steps

Configure Switch Encryption

1. Designate Switch Membership

2. Configure Switch

- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- **Select Security Settings**

3. Confirm Configuration

- Configuration Status
- Next Steps

Select Security Settings

Enter the group's security properties below.
Note that all properties can be edited in the group properties dialog.

Quorum Size None

A quorum of authentication cards are used to register/deregister authentication cards and system cards, to enable/disable system card, to change the quorum size, to generate a master key, and to backup or recover a master key.

System Cards ○ Required ● Not Required

A system card is optional. When configured, they discourage hardware theft because they are needed at power-up to enable encryption.

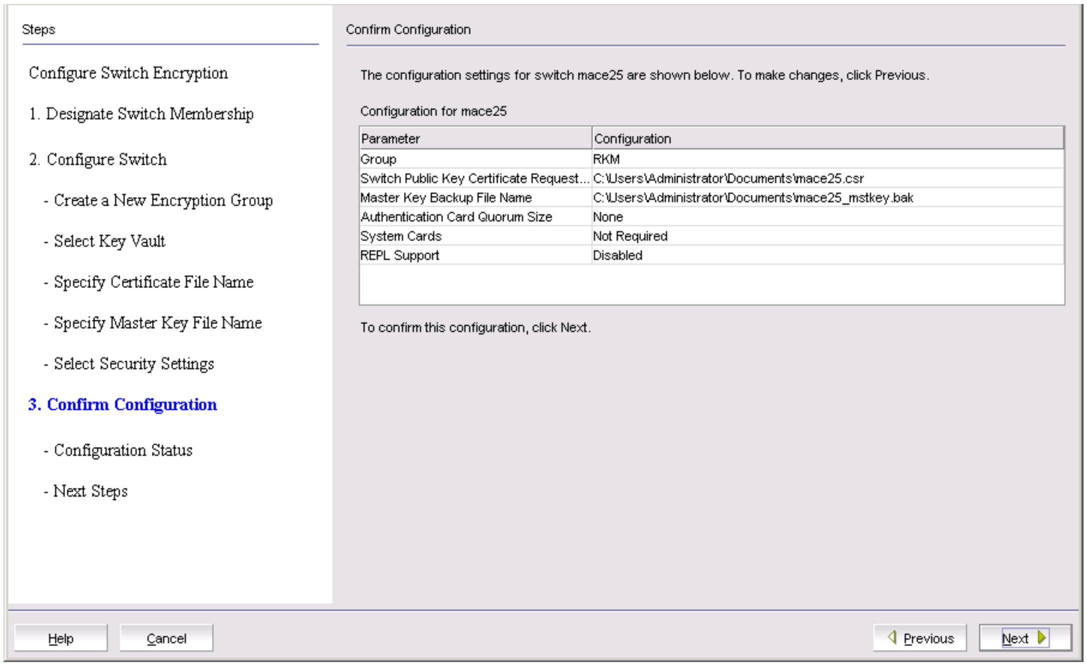
FIGURE 180 Select Security Settings dialog box

11. Set quorum size and system card requirements.

    The quorum size is the minimum number of cards necessary to enable the card holders to perform the security sensitive operations listed above. The maximum quorum size is five cards. The actual number of authentication cards registered is always more than the quorum size, so if you set the quorum size to five, for example, you will need to register at least six cards in the subsequent steps.

12. Click **Next**.

    The **Confirm Configuration** dialog box displays (Figure 181). The dialog box displays the encryption group name and switch public key certificate file name you specified.



Steps

Configure Switch Encryption

1. Designate Switch Membership

2. Configure Switch

- Create a New Encryption Group

- Select Key Vault

- Specify Certificate File Name

- Specify Master Key File Name

- Select Security Settings

3. Confirm Configuration

- Configuration Status

- Next Steps

Confirm Configuration

The configuration settings for switch mace25 are shown below. To make changes, click Previous.

Configuration for mace25

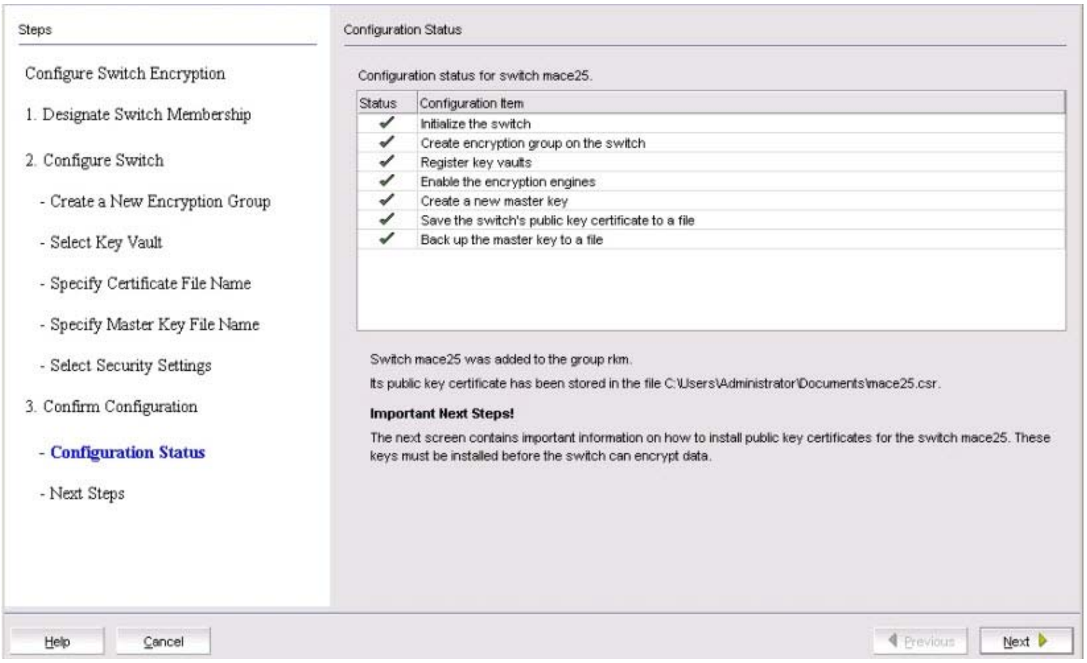
Parameter	Configuration
Group	RKM
Switch Public Key Certificate Request...	C:\Users\Administrator\Documents\mace25.csr
Master Key Backup File Name	C:\Users\Administrator\Documents\mace25_mstkey.bak
Authentication Card Quorum Size	None
System Cards	Not Required
REPL Support	Disabled

To confirm this configuration, click Next.

FIGURE 181 Confirm Configuration dialog box

13. Verify the information, then click **Next**.

14. The **Configuration Status** dialog box displays (Figure 182).



Steps

Configure Switch Encryption

1. Designate Switch Membership

2. Configure Switch

- Create a New Encryption Group

- Select Key Vault

- Specify Certificate File Name

- Specify Master Key File Name

- Select Security Settings

3. Confirm Configuration

- Configuration Status

- Next Steps

Configuration Status

Configuration status for switch mace25.

Status	Configuration Item
✓	Initialize the switch
✓	Create encryption group on the switch
✓	Register key vaults
✓	Enable the encryption engines
✓	Create a new master key
✓	Save the switch's public key certificate to a file
✓	Back up the master key to a file

Switch mace25 was added to the group rkm.

Its public key certificate has been stored in the file C:\Users\Administrator\Documents\mace25.csr.

Important Next Steps!

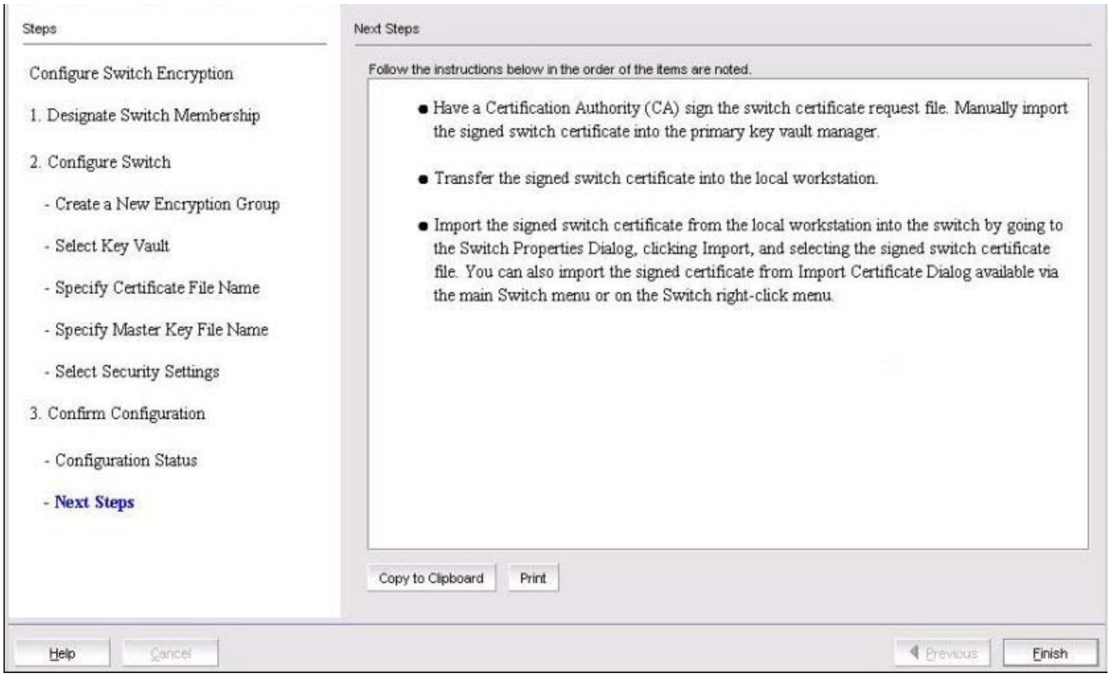
The next screen contains important information on how to install public key certificates for the switch mace25. These keys must be installed before the switch can encrypt data.

FIGURE 182 Configuration Status dialog box

15. Review the post-configuration instructions, which you can copy to a clipboard or print for later.

16. Click **Next**.

    The **Next Steps** dialog box displays (Figure 183).



Steps

Configure Switch Encryption

1. Designate Switch Membership

2. Configure Switch

- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings

3. Confirm Configuration

- Configuration Status
- **Next Steps**

Next Steps

Follow the instructions below in the order of the items are noted.

- Have a Certification Authority (CA) sign the switch certificate request file. Manually import the signed switch certificate into the primary key vault manager.
- Transfer the signed switch certificate into the local workstation.
- Import the signed switch certificate from the local workstation into the switch by going to the Switch Properties Dialog, clicking Import, and selecting the signed switch certificate file. You can also import the signed certificate from Import Certificate Dialog available via the main Switch menu or on the Switch right-click menu.

FIGURE 183 Next Steps dialog box

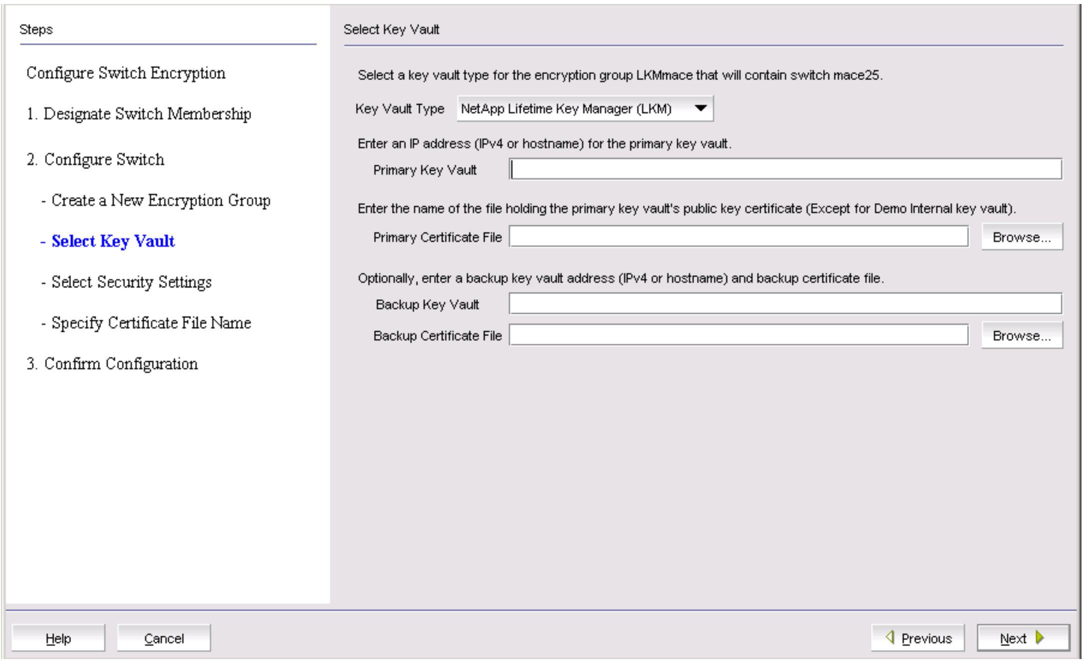
Instructions for installing public key certificates for the encryption switch are displayed.

17. Review the post-configuration instructions, which you can copy to a clipboard or print for later.
18. Click **Finish** to exit the **Configure Switch Encryption** wizard.
19. Review "Understanding configuration status results" on page 504.

Configuring key vault settings for NetApp Link Key Manager (LKM)

The following procedure assumes you have already configured the initial steps in the **Configure Switch Encryption** wizard. If you have not already done so, go to "Creating a new encryption group" on page 475.

Figure 184 shows the key vault selection dialog box for LKM.



Select a key vault type for the encryption group LKMmace that will contain switch mace25.

Key Vault Type: NetApp Lifetime Key Manager (LKM)

Enter an IP address (IPv4 or hostname) for the primary key vault.

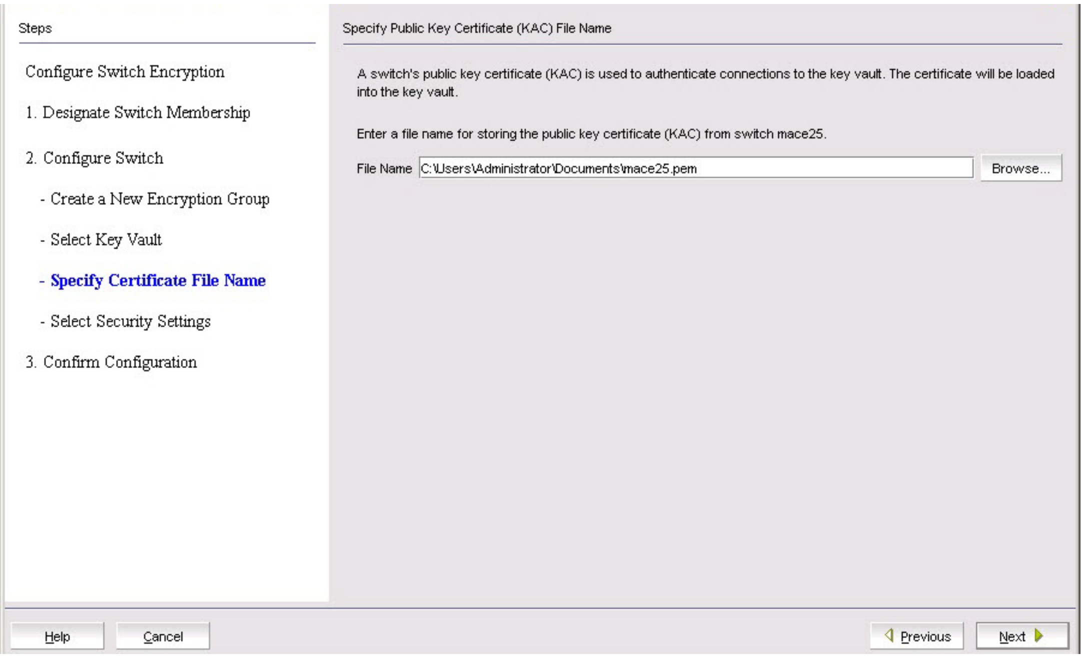
Enter the name of the file holding the primary key vault's public key certificate (Except for Demo Internal key vault).

Optionally, enter a backup key vault address (IPv4 or hostname) and backup certificate file.

FIGURE 184 Select Key Vault dialog box for LKM

1. Enter the IP address or host name for the primary key vault.
2. Enter the name of the file that holds the primary key vault's public key certificate or browse to the desired location.
3. If you are using a backup key vault, enter the IP address or host name, and the name of the file holding the backup key vault's public key certificate in the fields provided.
4. Click **Next.**

   The **Specify Public Key Certificate (KAC) File Name** dialog box displays (Figure 185).



Specify Public Key Certificate (KAC) File Name

A switch's public key certificate (KAC) is used to authenticate connections to the key vault. The certificate will be loaded into the key vault.

Enter a file name for storing the public key certificate (KAC) from switch mace25.

File Name C:\Users\Administrator\Documents\mace25.pem

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Select Security Settings
3. Confirm Configuration
Browse...
Help
Cancel
Previous
Next

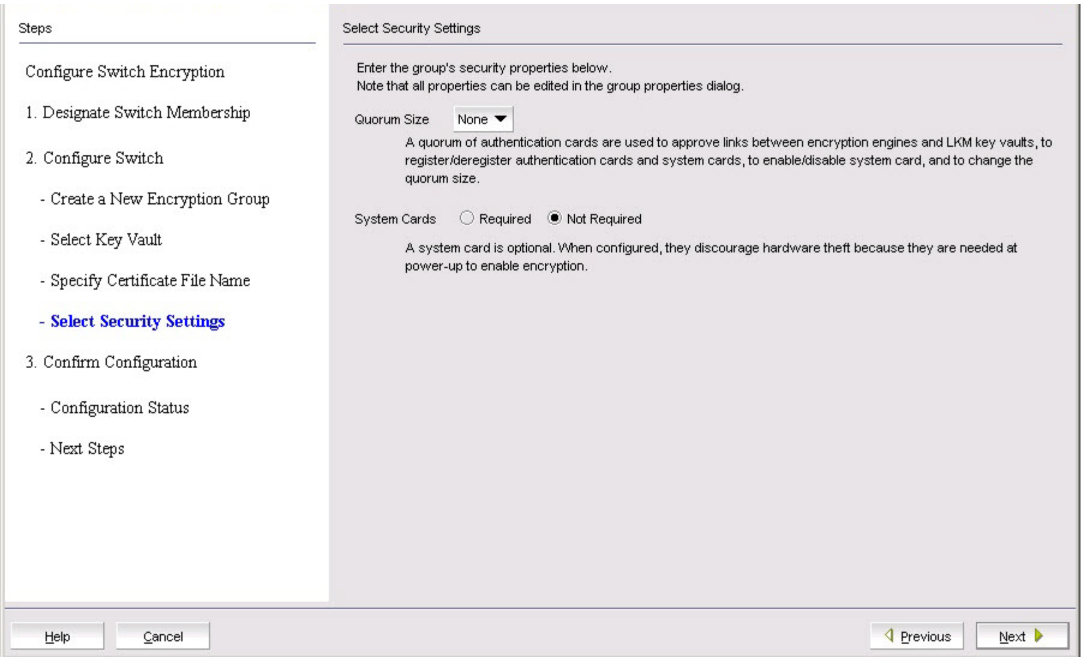
FIGURE 185 Specify Public Key Certificate (KAC) File Name dialog box

5. Specify the location of the file where you want to store the public key certificate that is used to authenticate connections to the key vault.

   The certificate stored in this file is the switch's public key certificate. You will need to know this path and file name to install the switch's public key certificate on the key management appliance.

6. Click **Next**.

   The **Select Security Settings** dialog box displays (Figure 186).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Help
Cancel
Previous
Next

Select Security Settings

Enter the group's security properties below.
Note that all properties can be edited in the group properties dialog.

Quorum Size: None

A quorum of authentication cards are used to approve links between encryption engines and LKM key vaults, to register/deregister authentication cards and system cards, to enable/disable system card, and to change the quorum size.

System Cards: ○ Required ● Not Required

A system card is optional. When configured, they discourage hardware theft because they are needed at power-up to enable encryption.

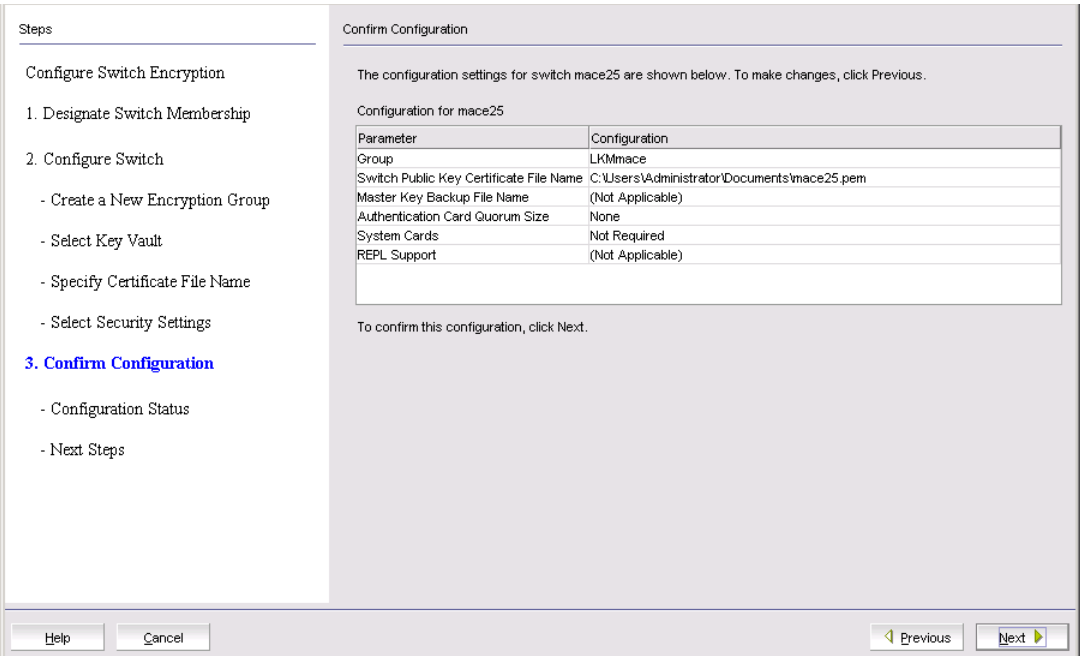
FIGURE 186 Select Security Settings dialog box

7. Set quorum size and system card requirements.

   The quorum size is the minimum number of cards necessary to enable the card holders to perform the security sensitive operations listed above. The maximum quorum size is five cards. The actual number of authentication cards registered is always more than the quorum size, so if you set the quorum size to five, for example, you will need to register at least six cards in the subsequent steps.

8. Click **Next**.

   The **Confirm Configuration** dialog box displays (Figure 187). The dialog box displays the encryption group name and switch public key certificate file name you specified.


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Confirm Configuration
Help
Cancel
Previous
Next

The configuration settings for switch mace25 are shown below. To make changes, click Previous.

Configuration for mace25

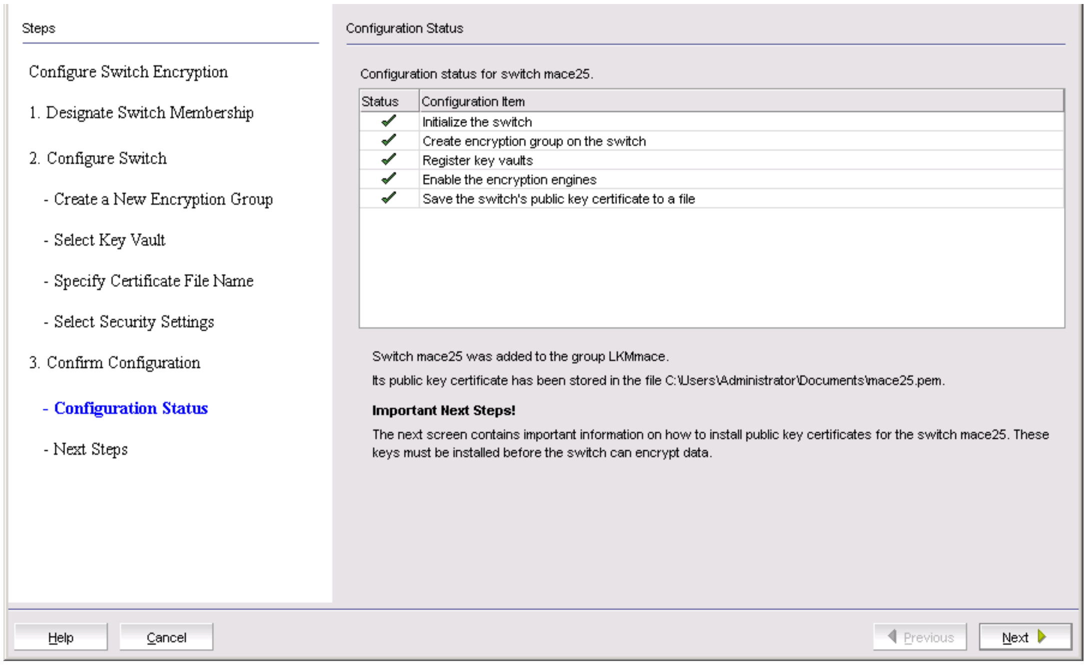
Parameter	Configuration
Group	LKMmace
Switch Public Key Certificate File Name	C:\Users\Administrator\Documents\mace25.pem
Master Key Backup File Name	(Not Applicable)
Authentication Card Quorum Size	None
System Cards	Not Required
REPL Support	(Not Applicable)

To confirm this configuration, click Next.

FIGURE 187 Confirm Configuration dialog box

9. Click **Next.**

   The **Configuration Status** dialog box displays (Figure 188).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Configuration Status
Help
Cancel
Previous
Next

Configuration status for switch mace25.

Status	Configuration Item
✓	Initialize the switch
✓	Create encryption group on the switch
✓	Register key vaults
✓	Enable the encryption engines
✓	Save the switch's public key certificate to a file

Switch mace25 was added to the group LKMmace.

Its public key certificate has been stored in the file C:\Users\Administrator\Documents\mace25.pem.

Important Next Steps!

The next screen contains important information on how to install public key certificates for the switch mace25. These keys must be installed before the switch can encrypt data.

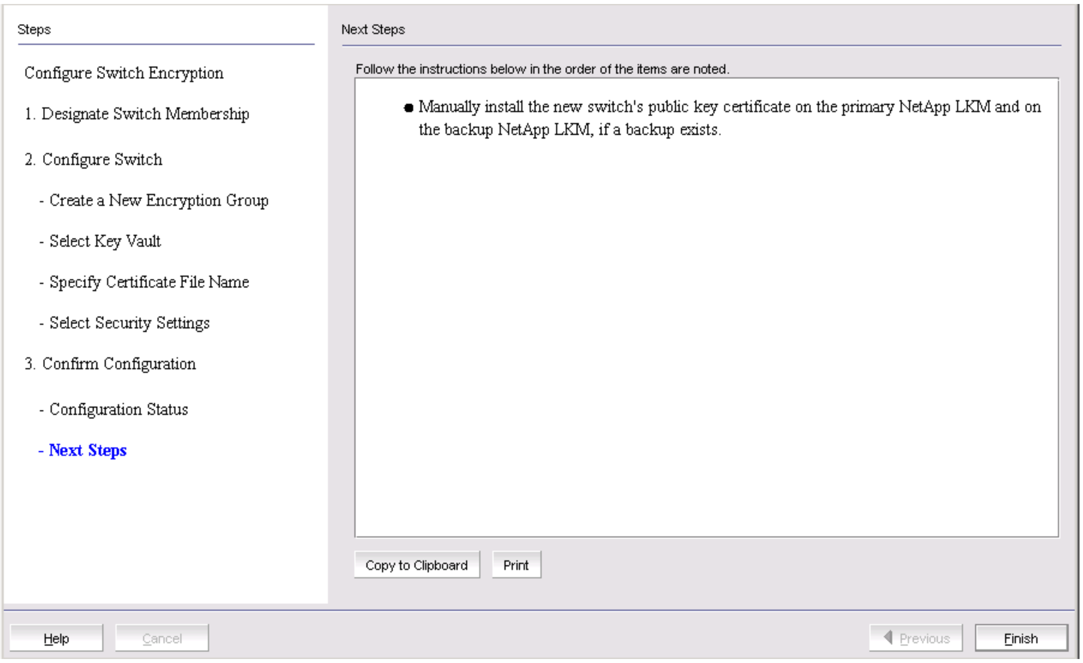
FIGURE 188 Configuration Status dialog box

All configuration items have green check marks if the configuration is successful. A red stop sign indicates a failed step. A message displays below the table, indicating the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.

After configuration of the encryption group is completed, the Management application sends API commands to verify the switch configuration. See "Understanding configuration status results" on page 504 for more information.

10. Verify the information, then click **Next**.

    The **Next Steps** dialog box displays (Figure 189).



Follow the instructions below in the order of the items are noted.

- Manually install the new switch's public key certificate on the primary NetApp LKM and on the backup NetApp LKM, if a backup exists.

FIGURE 189 Next Steps dialog box

Instructions for installing public key certificates for the encryption switch are displayed. These instructions are specific to the key vault type.

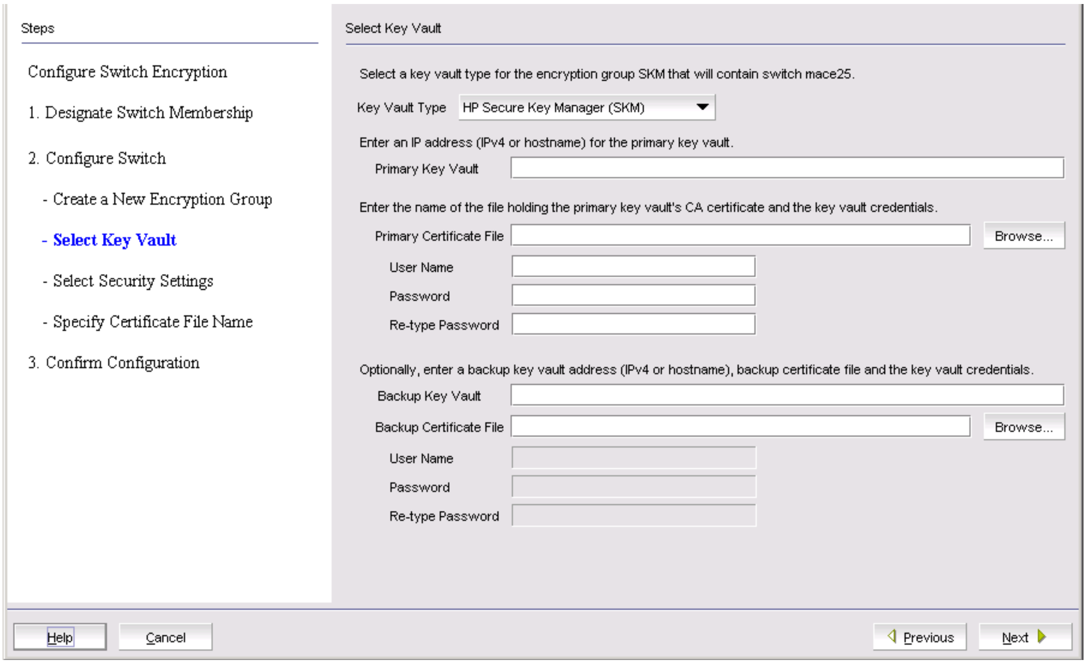
11. Review the post-configuration instructions, which you can copy to a clipboard or print for later.

12. Click **Finish** to exit the **Configure Switch Encryption** wizard.

Configuring key vault settings for HP Secure Key Manager (SKM)

The following procedure assumes you have already configured the initial steps in the **Configure Switch Encryption** wizard. If you have not already done so, go to "Creating a new encryption group" on page 475.

Figure 190 shows the key vault selection dialog box for LKM.



Select a key vault type for the encryption group SKM that will contain switch mace25.

Key Vault Type: HP Secure Key Manager (SKM)

Enter an IP address (IPv4 or hostname) for the primary key vault.

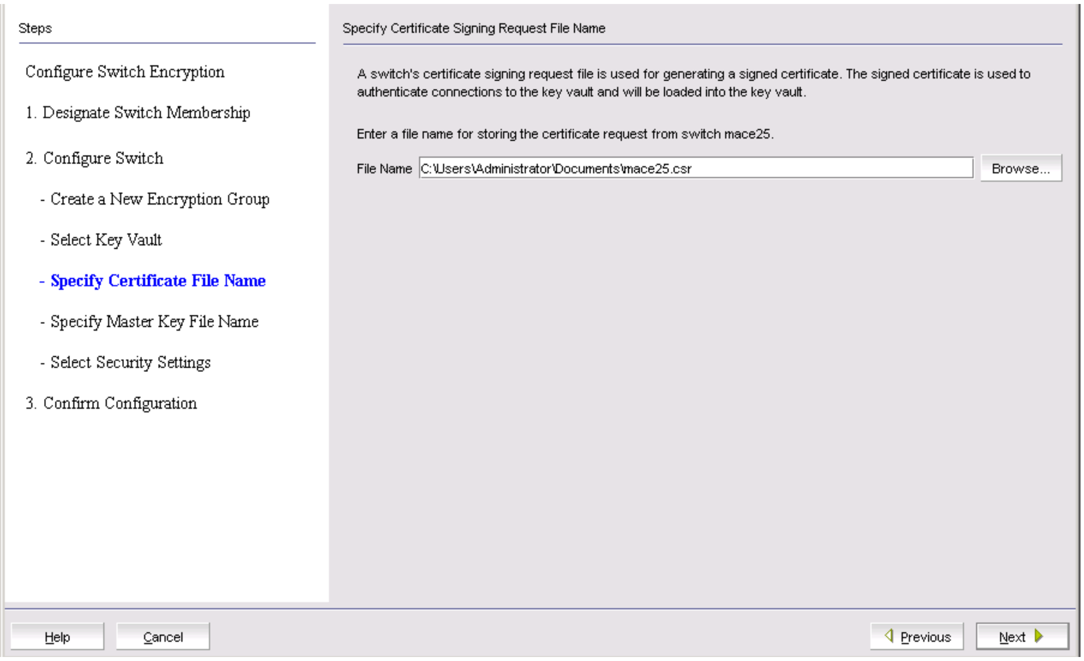
Enter the name of the file holding the primary key vault's CA certificate and the key vault credentials.

Optionally, enter a backup key vault address (IPv4 or hostname), backup certificate file and the key vault credentials.

FIGURE 190 Select Key Vault dialog box for SKM

1. Enter the IP address or host name for the primary key vault.
2. Enter the name of the file that holds the primary key vault's CA key certificate or browse to the desired location.
3. Enter the password you established for the Brocade user group.
4. If you are using a backup key vault, enter the IP address or host name, and the name of the file holding the backup key vault's public key certificate in the fields provided. The same user name and password used for the primary key vault are automatically applied to the backup key vault.
5. Click **Next**.

   The **Specify Certificate Signing Request File Name** dialog box displays (Figure 191).



Specify Certificate Signing Request File Name

A switch's certificate signing request file is used for generating a signed certificate. The signed certificate is used to authenticate connections to the key vault and will be loaded into the key vault.

Enter a file name for storing the certificate request from switch mace25.

File Name C:\Users\Administrator\Documents\mace25.csr

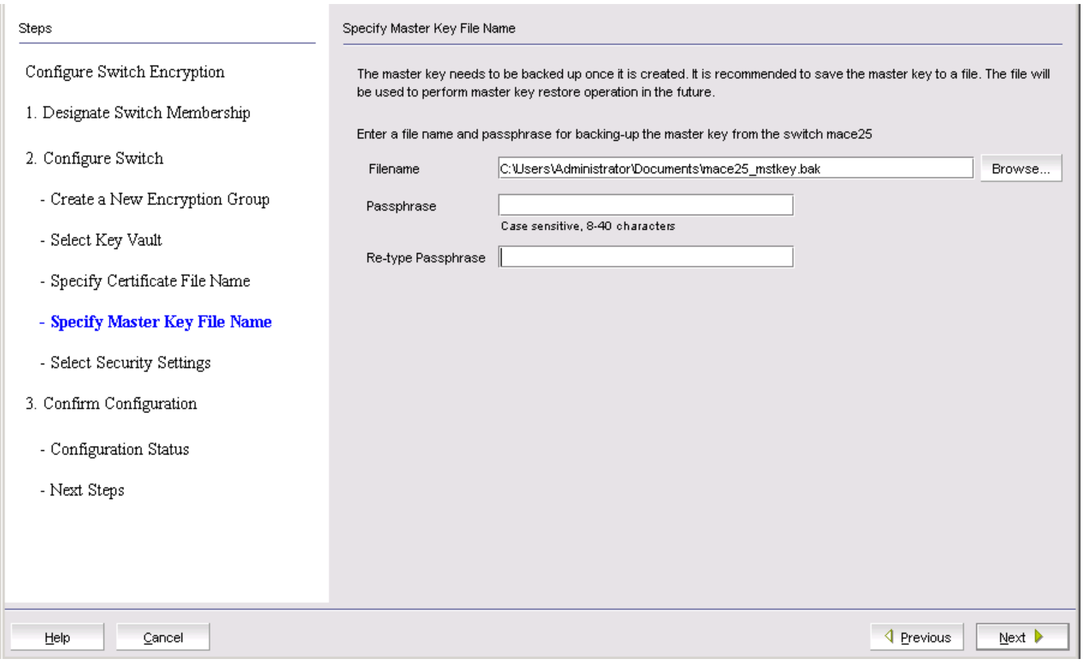
Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
Browse...
Help
Cancel
Previous
Next

FIGURE 191 Specify Certificate Signing Request File Name dialog box

6. Enter the location of the file where you want to store the certificate information, or browse to the desired location.

7. Click **Next**.

   The **Specify Master Key File Name** dialog box displays (Figure 192).



Specify Master Key File Name

The master key needs to be backed up once it is created. It is recommended to save the master key to a file. The file will be used to perform master key restore operation in the future.

Enter a file name and passphrase for backing-up the master key from the switch mace25

Filename C:\Users\Administrator\Documents\mace25_mstkey.bak

Passphrase

Case sensitive, 8-40 characters

Re-type Passphrase

Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Browse...
Help
Cancel
Previous
Next

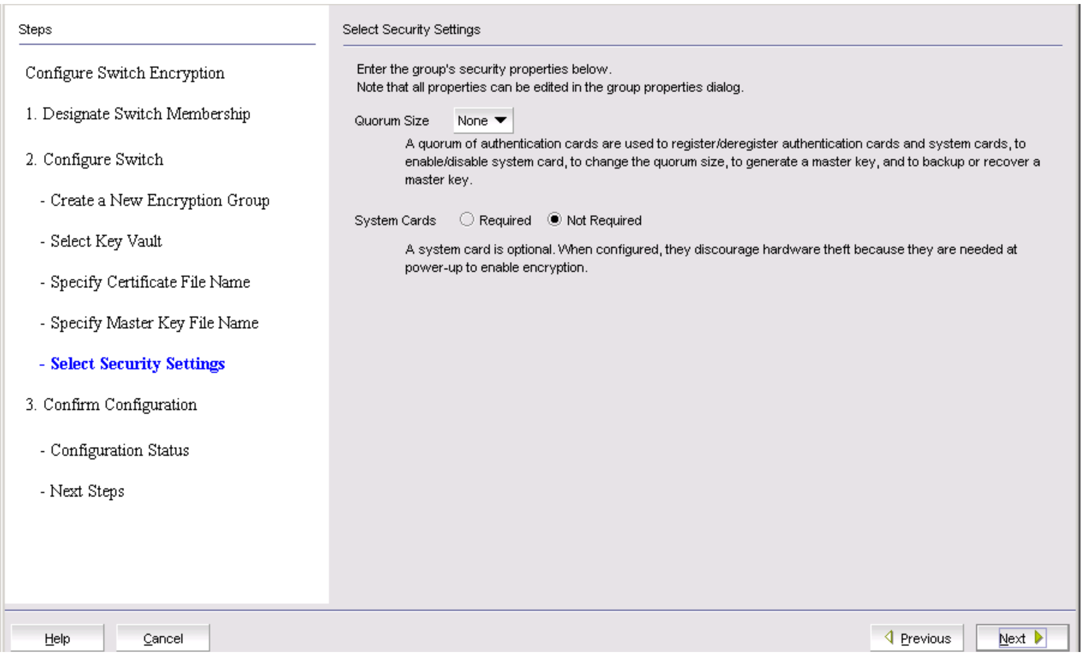
FIGURE 192 Specify Master Key File Name dialog box

8. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.

9. Re-enter the passphrase for verification.

10. Click **Next**.

11. The **Select Security Settings** dialog box displays (Figure 193).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Help
Cancel
Previous
Next

Select Security Settings

Enter the group's security properties below.
Note that all properties can be edited in the group properties dialog.

Quorum Size: None

A quorum of authentication cards are used to register/deregister authentication cards and system cards, to enable/disable system card, to change the quorum size, to generate a master key, and to backup or recover a master key.

System Cards ○ Required ● Not Required

A system card is optional. When configured, they discourage hardware theft because they are needed at power-up to enable encryption.

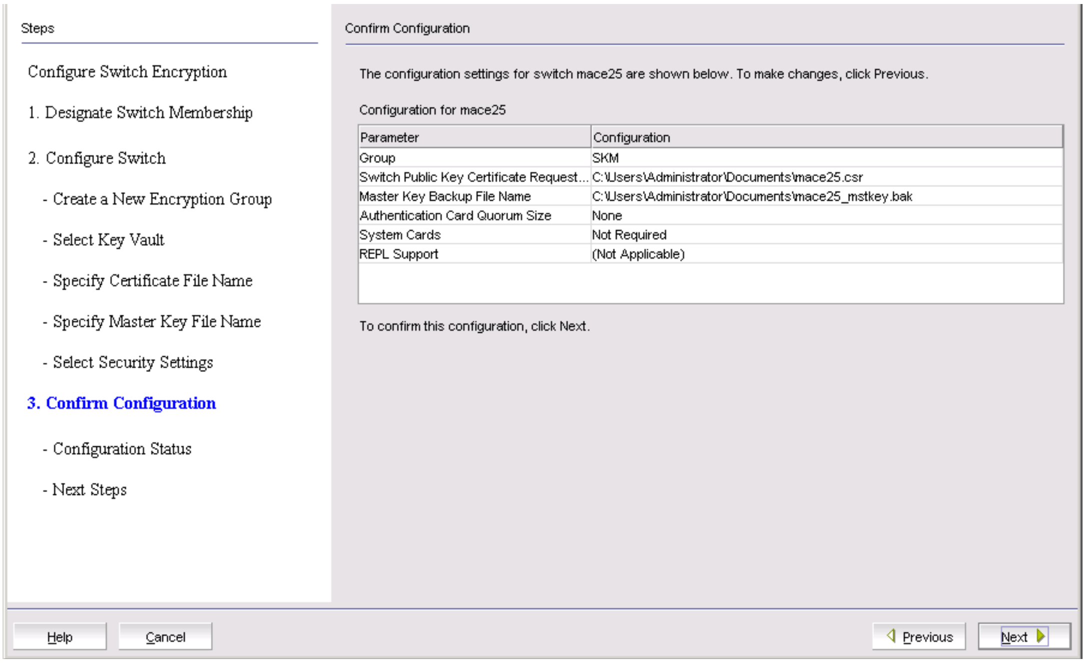
FIGURE 193 Select Security Settings dialog box

12. Set quorum size and system card requirements.

    The quorum size is the minimum number of cards necessary to enable the card holders to perform the security sensitive operations listed above. The maximum quorum size is five cards. The actual number of authentication cards registered is always more than the quorum size, so if you set the quorum size to five, for example, you will need to register at least six cards in the subsequent steps.

13. Click **Next**.

    The **Confirm Configuration** dialog box displays (Figure 194). The dialog box displays the encryption group name and switch public key certificate file name you specified.


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Help
Cancel
Previous
Next

Confirm Configuration

The configuration settings for switch mace25 are shown below. To make changes, click Previous.

Configuration for mace25

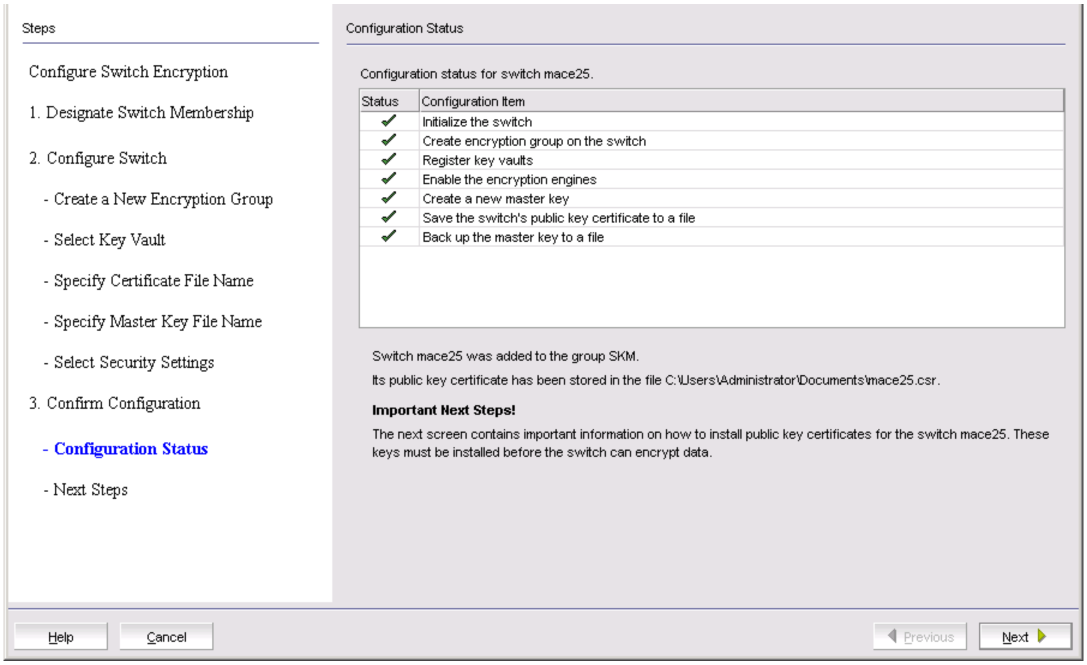
Parameter	Configuration
Group	SKM
Switch Public Key Certificate Request...	C:\Users\Administrator\Documents\mace25.csr
Master Key Backup File Name	C:\Users\Administrator\Documents\mace25_mstkey.bak
Authentication Card Quorum Size	None
System Cards	Not Required
REPL Support	(Not Applicable)

To confirm this configuration, click Next.

FIGURE 194 Confirm Configuration dialog box

14. Verify the information, then click **Next**.

    The **Configuration Status** dialog box displays (Figure 195).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Help
Cancel
Previous
Next

Configuration Status

Configuration status for switch mace25.

Status	Configuration Item
✓	Initialize the switch
✓	Create encryption group on the switch
✓	Register key vaults
✓	Enable the encryption engines
✓	Create a new master key
✓	Save the switch's public key certificate to a file
✓	Back up the master key to a file

Switch mace25 was added to the group SKM.

Its public key certificate has been stored in the file C:\Users\Administrator\Documents\mace25.csr.

Important Next Steps!

The next screen contains important information on how to install public key certificates for the switch mace25. These keys must be installed before the switch can encrypt data.

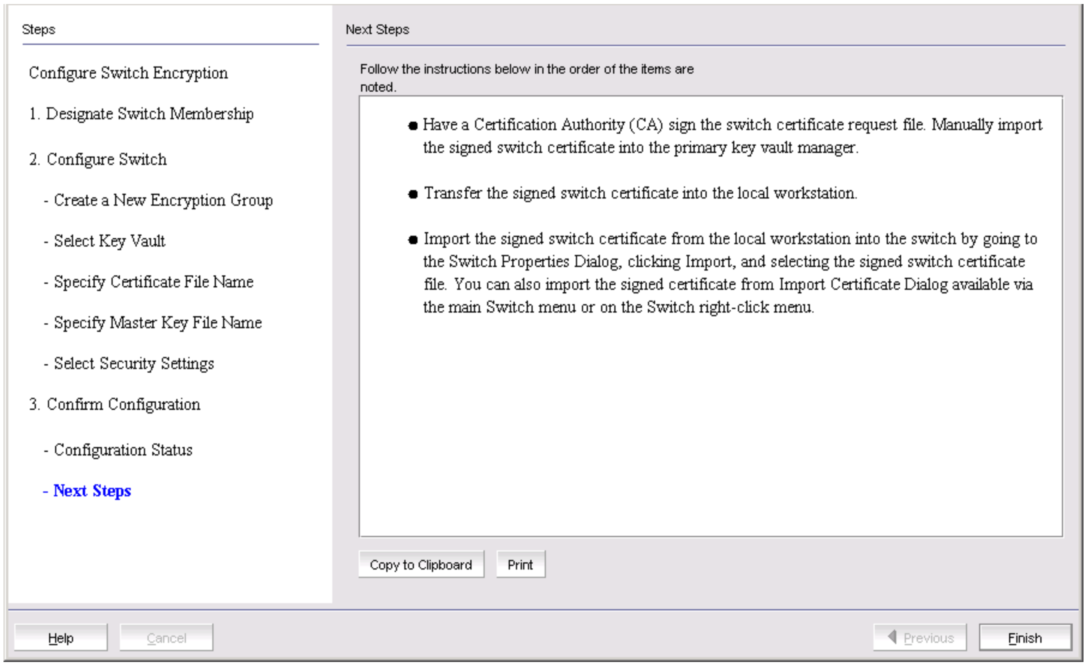
FIGURE 195 Configuration Status dialog box

All configuration items have green check marks if the configuration is successful. A red stop sign indicates a failed step. A message displays below the table, indicating the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.

After configuration of the encryption group is completed, the Management application sends API commands to verify the switch configuration. See "Understanding configuration status results" on page 504 for more information.

15. Verify the information and review important messages, then click **Next**.

    The **Next Steps** dialog box displays (Figure 196).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Next Steps
Copy to Clipboard
Print
Help
Cancel
Previous
Finish

Follow the instructions below in the order of the items are noted.

- Have a Certification Authority (CA) sign the switch certificate request file. Manually import the signed switch certificate into the primary key vault manager.
- Transfer the signed switch certificate into the local workstation.
- Import the signed switch certificate from the local workstation into the switch by going to the Switch Properties Dialog, clicking Import, and selecting the signed switch certificate file. You can also import the signed certificate from Import Certificate Dialog available via the main Switch menu or on the Switch right-click menu.

FIGURE 196 Next Steps dialog box

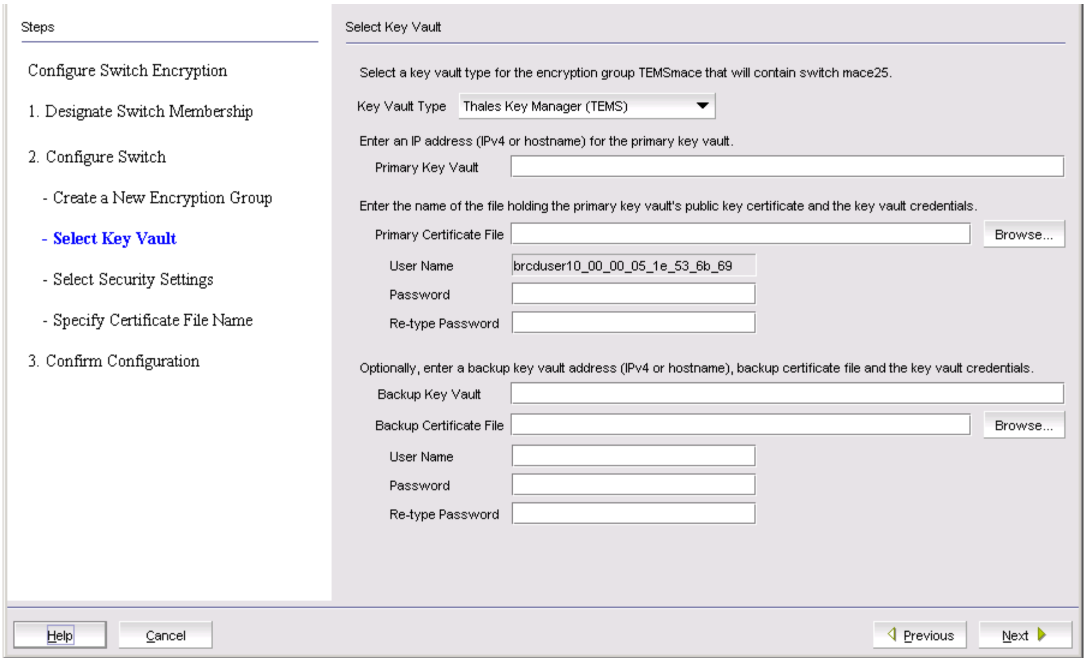
Instructions for installing public key certificates for the encryption switch are displayed.

16. Review post-configuration instructions, which you can copy to a clipboard or print for later.
17. Click **Finish** to exit the **Configure Switch Encryption** wizard.
18. Review "Understanding configuration status results" on page 504.

Configuring key vault settings for Thales Key Manager (TEMS)

The following procedure assumes you have already configured the initial steps in the **Configure Switch Encryption** wizard. If you have not already done so, go to "Creating a new encryption group" on page 475.

Figure 197 shows the key vault selection dialog box for TEMS.


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Select Security Settings
- Specify Certificate File Name
3. Confirm Configuration
Help
Cancel
Previous
Next

Select Key Vault

Select a key vault type for the encryption group TEMSmace that will contain switch mace25.

Key Vault Type: Thales Key Manager (TEMS)

Enter an IP address (IPv4 or hostname) for the primary key vault.

Primary Key Vault:

Enter the name of the file holding the primary key vault's public key certificate and the key vault credentials.

Primary Certificate File: Browse...

User Name: brcduser10_00_00_05_1e_53_6b_69

Password:

Re-type Password:

Optionally, enter a backup key vault address (IPv4 or hostname), backup certificate file and the key vault credentials.

Backup Key Vault:

Backup Certificate File: Browse...

User Name:

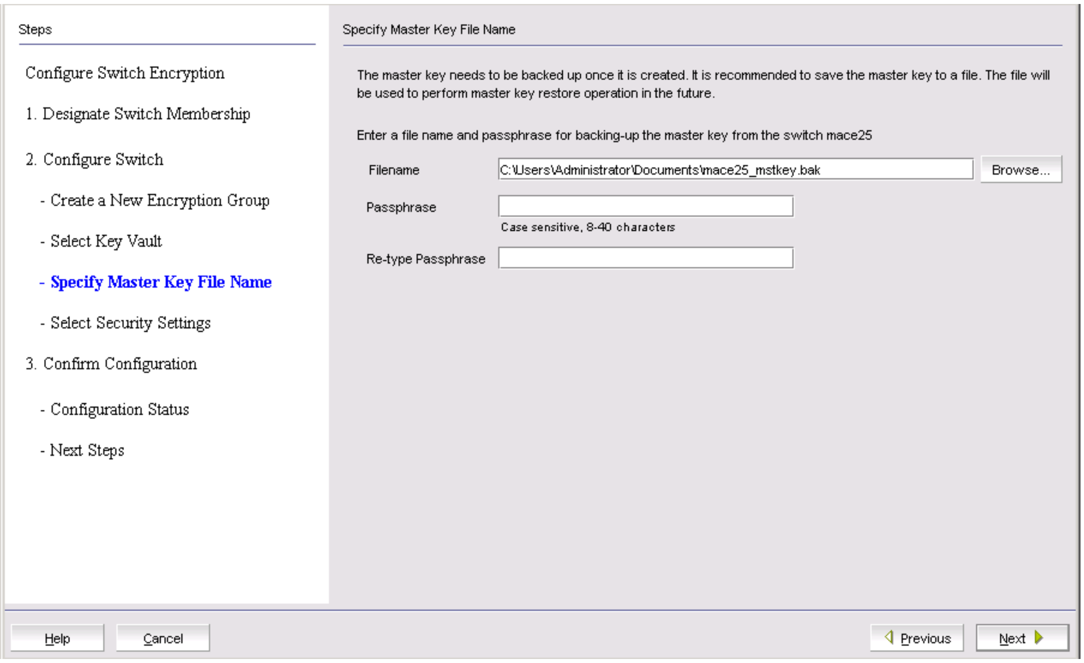
Password:

Re-type Password:

FIGURE 197 Select Key Vault dialog box for TEMS

1. Enter the IP address or host name for the primary key vault.
2. Enter the name of the file that holds the primary key vault's public key certificate, or browse to the desired location.
3. Enter the password you created for the Brocade group TEMS client.
4. If you are using a backup key vault, enter the IP address or host name, the name of the file holding the backup key vault's public key certificate in the fields provided, and the user name and password for the backup key vault.
5. Click **Next.**

   The **Specify Master Key File Name** dialog box displays (Figure 198).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Help
Cancel
Previous
Next
Browse...

Specify Master Key File Name

The master key needs to be backed up once it is created. It is recommended to save the master key to a file. The file will be used to perform master key restore operation in the future.

Enter a file name and passphrase for backing-up the master key from the switch mace25

Filename: C:\Users\Administrator\Documents\mace25_mstkey.bak

Passphrase:

Case sensitive, 8-40 characters

Re-type Passphrase:

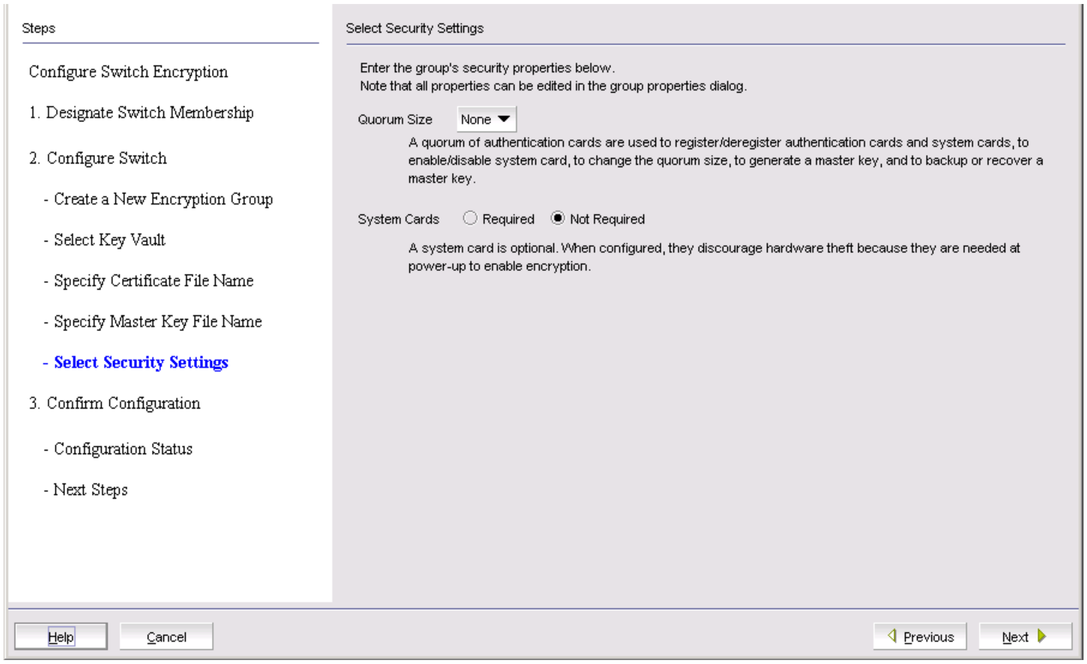
FIGURE 198 Specify Master Key File Name dialog box

6. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.

7. Re-enter the passphrase for verification.

8. Click **Next**.

   The **Select Security Settings** dialog box displays (Figure 199).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Help
Cancel
Previous
Next

Select Security Settings

Enter the group's security properties below.
Note that all properties can be edited in the group properties dialog.

Quorum Size: None

A quorum of authentication cards are used to register/deregister authentication cards and system cards, to enable/disable system card, to change the quorum size, to generate a master key, and to backup or recover a master key.

System Cards: ○ Required ● Not Required

A system card is optional. When configured, they discourage hardware theft because they are needed at power-up to enable encryption.

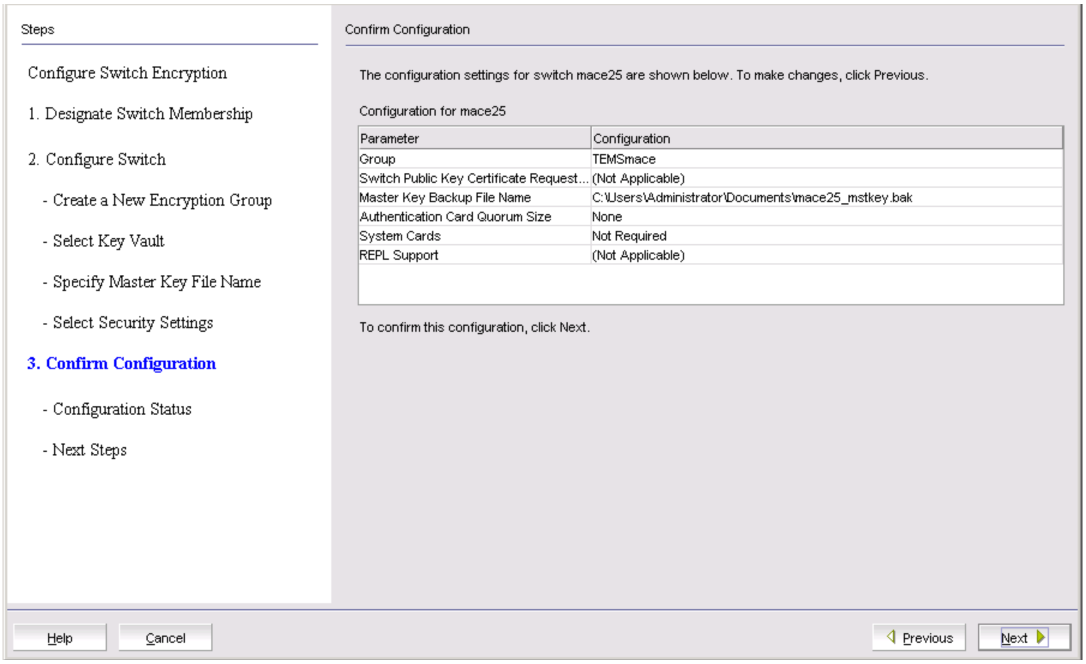
FIGURE 199 Select Security Settings dialog box

9. Set quorum size and system card requirements.

   The quorum size is the minimum number of cards necessary to enable the card holders to perform the security sensitive operations listed above. The maximum quorum size is five cards. The actual number of authentication cards registered is always more than the quorum size, so if you set the quorum size to five, for example, you will need to register at least six cards in the subsequent steps.

10. Click **Next**.

The **Confirm Configuration** dialog box displays (Figure 200).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Confirm Configuration
Help
Cancel
Previous
Next

The configuration settings for switch mace25 are shown below. To make changes, click Previous.

Configuration for mace25

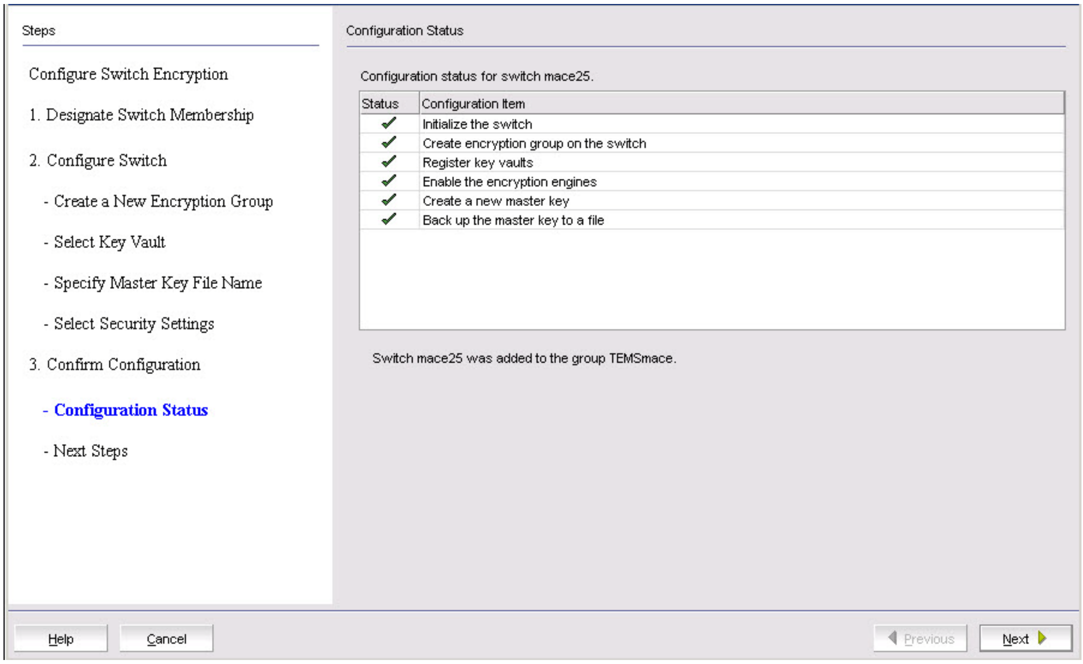
Parameter	Configuration
Group	TEMSmace
Switch Public Key Certificate Request...	(Not Applicable)
Master Key Backup File Name	C:\Users\Administrator\Documents\mace25_mstkey.bak
Authentication Card Quorum Size	None
System Cards	Not Required
REPL Support	(Not Applicable)

To confirm this configuration, click Next.

FIGURE 200 Confirm Configuration dialog box

11. Verify the contents, then click **Next**.

12. The **Configuration Status** dialog box displays (Figure 201).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Configuration Status
Help
Cancel
Previous
Next

Configuration status for switch mace25.

Status	Configuration Item
✓	Initialize the switch
✓	Create encryption group on the switch
✓	Register key vaults
✓	Enable the encryption engines
✓	Create a new master key
✓	Back up the master key to a file

Switch mace25 was added to the group TEMSmace.

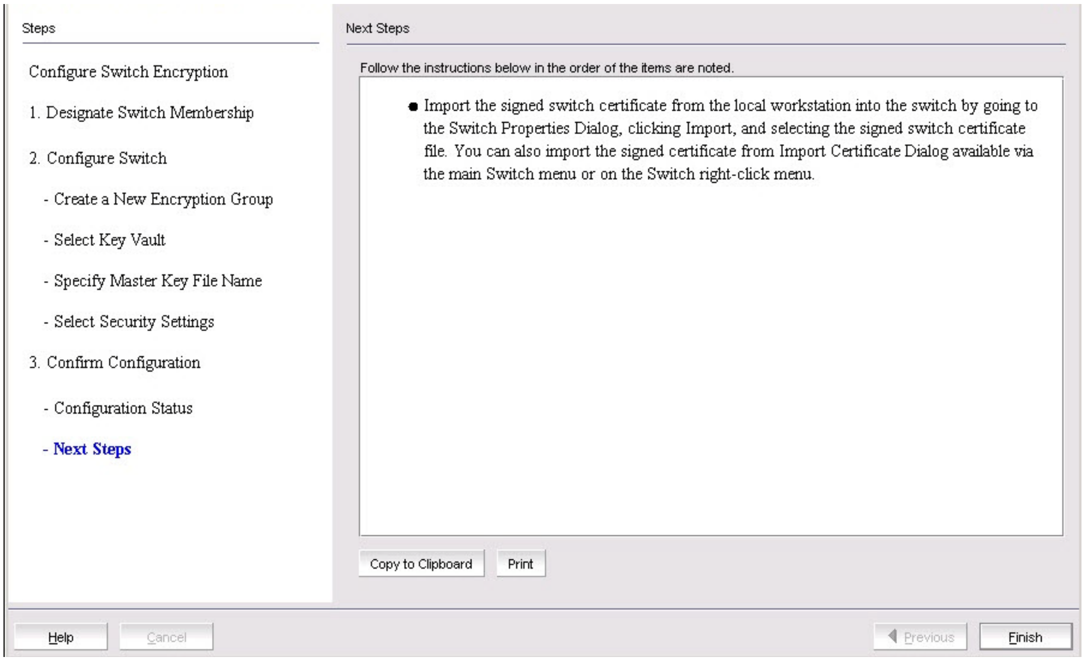
FIGURE 201 Configuration Status dialog box

All configuration items have green check marks if the configuration is successful. A red stop sign indicates a failed step. A message displays below the table, indicating the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.

After configuration of the encryption group is completed, the Management application sends API commands to verify the switch configuration. See "Understanding configuration status results" on page 504 for more information.

13. Click **Next.**

    The **Next Steps** dialog box displays (Figure 202).



Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Next Steps

Follow the instructions below in the order of the items are noted.

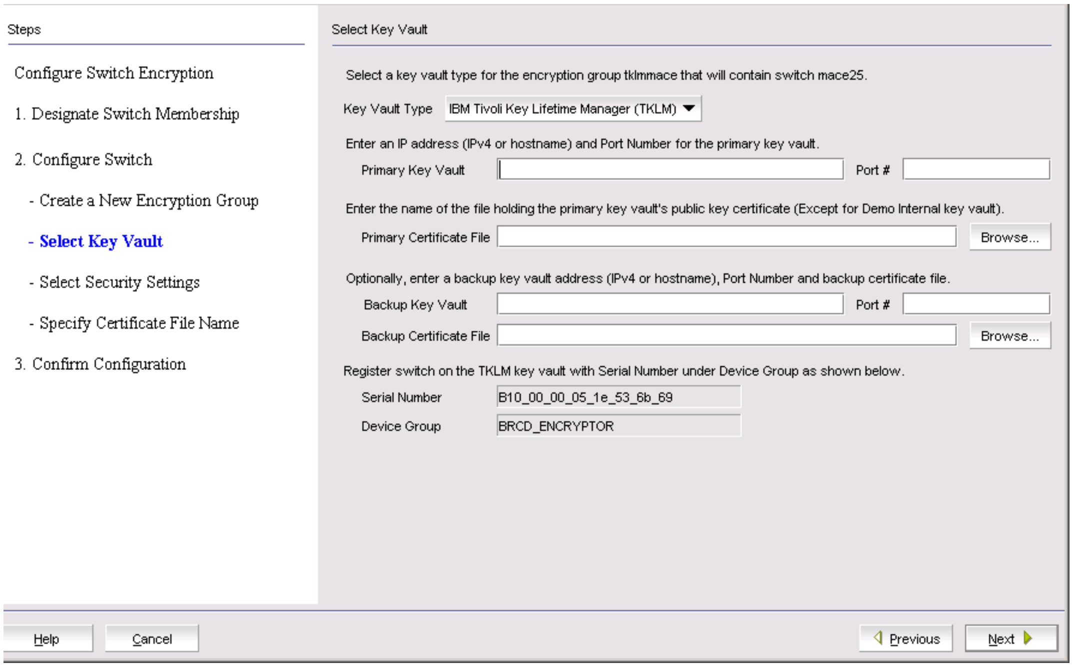
- Import the signed switch certificate from the local workstation into the switch by going to the Switch Properties Dialog, clicking Import, and selecting the signed switch certificate file. You can also import the signed certificate from Import Certificate Dialog available via the main Switch menu or on the Switch right-click menu.

FIGURE 202 Next Steps dialog box

Configuring key vault settings for IBM Tivoli Key Lifetime Manager (TKLM)

The following procedure assumes you have already configured the initial steps in the **Configure Switch Encryption** wizard. If you have not already done so, go to "Creating a new encryption group" on page 475.

Figure 203 shows the key vault selection dialog box for TKLM.



Steps

Configure Switch Encryption

1. Designate Switch Membership

2. Configure Switch

- Create a New Encryption Group

- **Select Key Vault**

- Select Security Settings

- Specify Certificate File Name

3. Confirm Configuration

Select Key Vault

Select a key vault type for the encryption group tklmmace that will contain switch mace25.

Key Vault Type: IBM Tivoli Key Lifetime Manager (TKLM)

Enter an IP address (IPv4 or hostname) and Port Number for the primary key vault.

Primary Key Vault | Port #

Enter the name of the file holding the primary key vault's public key certificate (Except for Demo Internal key vault).

Primary Certificate File | Browse...

Optionally, enter a backup key vault address (IPv4 or hostname), Port Number and backup certificate file.

Backup Key Vault | Port #

Backup Certificate File | Browse...

Register switch on the TKLM key vault with Serial Number under Device Group as shown below.

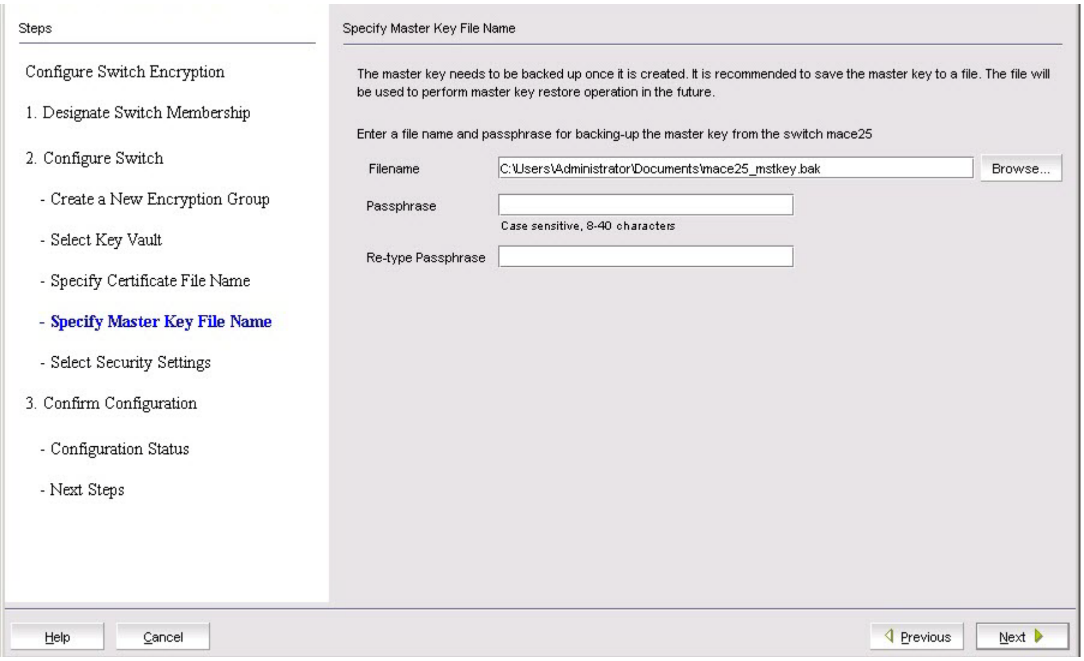
Serial Number: B10_00_00_05_1e_53_6b_69

Device Group: BRCD_ENCRYPTOR

FIGURE 203 **Select Key Vault dialog box for TKLM**

1. Enter the IP address or host name for the primary key vault.
2. Enter the name of the file that holds the primary key vault's public key certificate or browse to the desired location.
3. If you are using a backup key vault, enter the IP address or host name, and the name of the file holding the backup key vault's public key certificate in the fields provided.
4. Click **Next**.

   The **Specify Master Key Certificate File Name** dialog box displays (Figure 204).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Help
Cancel
Previous
Next
Browse...

Specify Master Key File Name

The master key needs to be backed up once it is created. It is recommended to save the master key to a file. The file will be used to perform master key restore operation in the future.

Enter a file name and passphrase for backing-up the master key from the switch mace25

Filename C:\Users\Administrator\Documents\mace25_mstkey.bak

Passphrase

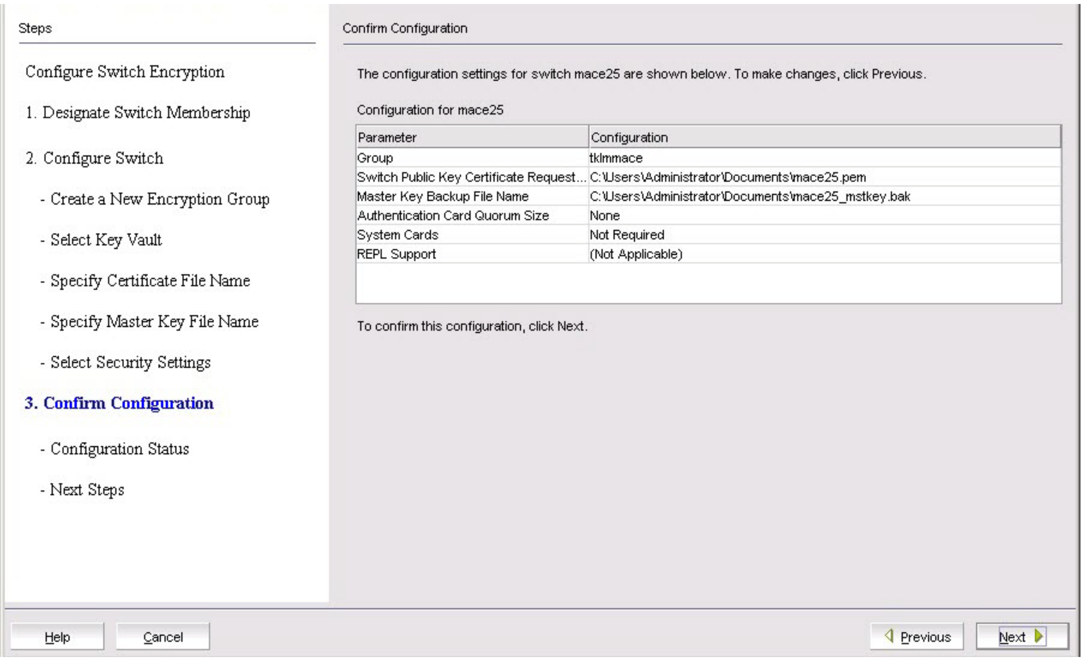
Case sensitive, 8-40 characters

Re-type Passphrase

FIGURE 204 Specify Master Key Certificate File Name dialog box

5. Enter a file name for backing up the master key or browse to the desired location.
6. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
7. Re-enter the passphrase for verification.
8. Click **Next**.

   The **Confirm Configuration** dialog box displays (Figure 205). The dialog box displays the encryption group name and switch public key certificate file name you specified.


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Confirm Configuration
Help
Cancel
Previous
Next

The configuration settings for switch mace25 are shown below. To make changes, click Previous.

Configuration for mace25

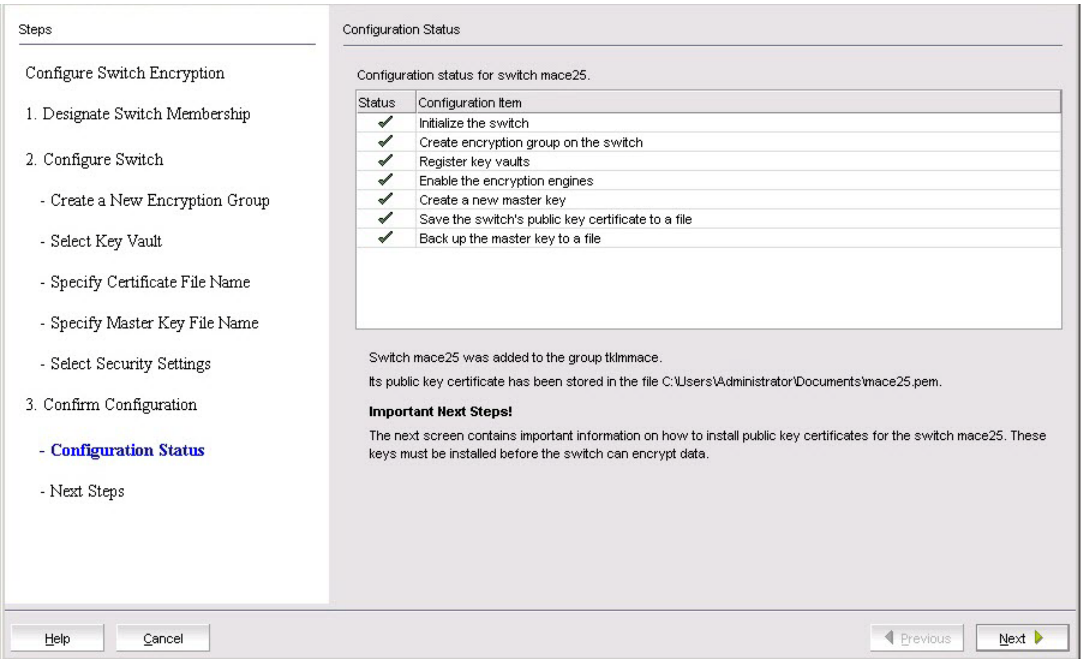
Parameter	Configuration
Group	tklmmace
Switch Public Key Certificate Request...	C:\Users\Administrator\Documents\mace25.pem
Master Key Backup File Name	C:\Users\Administrator\Documents\mace25_mstkey.bak
Authentication Card Quorum Size	None
System Cards	Not Required
REPL Support	(Not Applicable)

To confirm this configuration, click Next.

FIGURE 205 Confirm Configuration dialog box

9. Verify the information, then click **Next.**

   The **Configuration Status** dialog box displays (Figure 206).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Configuration Status
Help
Cancel
Previous
Next

Configuration status for switch mace25.

Status	Configuration Item
✓	Initialize the switch
✓	Create encryption group on the switch
✓	Register key vaults
✓	Enable the encryption engines
✓	Create a new master key
✓	Save the switch's public key certificate to a file
✓	Back up the master key to a file

Switch mace25 was added to the group tklmmace.

Its public key certificate has been stored in the file C:\Users\Administrator\Documents\mace25.pem.

Important Next Steps!

The next screen contains important information on how to install public key certificates for the switch mace25. These keys must be installed before the switch can encrypt data.

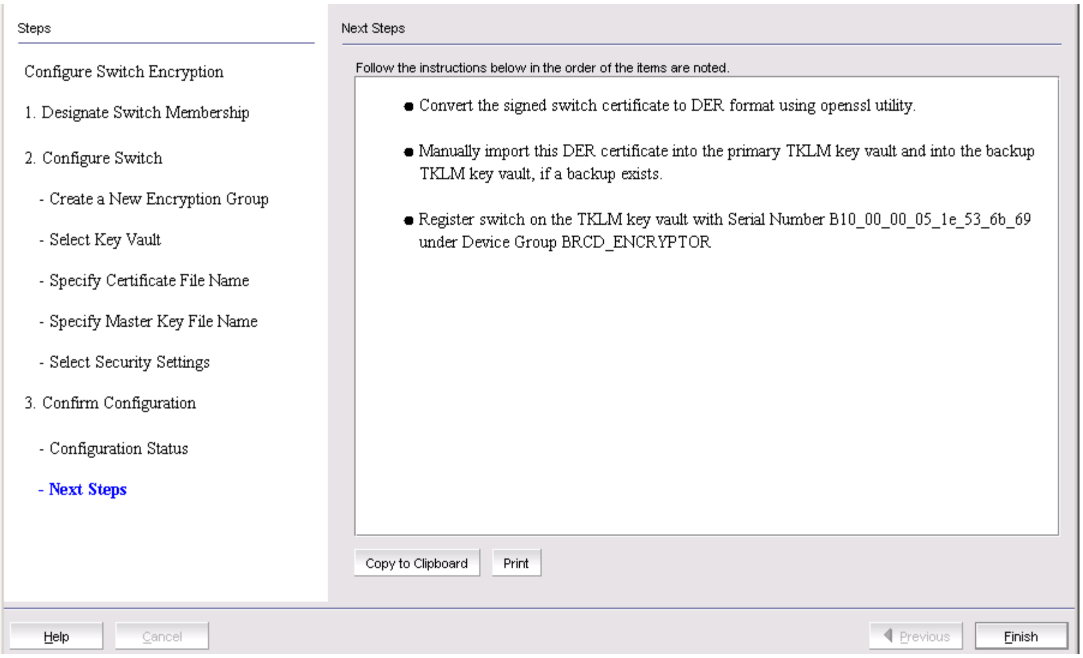
FIGURE 206 Configuration Status dialog box

All configuration items have green check marks if the configuration is successful. A red stop sign indicates a failed step. A message displays below the table, indicating the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.

After configuration of the encryption group is completed, the Management application sends API commands to verify the switch configuration. See "Understanding configuration status results" on page 504 for more information.

10. Review important messages, then click **Next**.

    The **Next Steps** dialog box displays (Figure 207).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Create a New Encryption Group
- Select Key Vault
- Specify Certificate File Name
- Specify Master Key File Name
- Select Security Settings
3. Confirm Configuration
- Configuration Status
- Next Steps
Next Steps

Follow the instructions below in the order of the items are noted.

- Convert the signed switch certificate to DER format using openssl utility.
- Manually import this DER certificate into the primary TKLM key vault and into the backup TKLM key vault, if a backup exists.
- Register switch on the TKLM key vault with Serial Number B10_00_00_05_1e_53_6b_69 under Device Group BRCD_ENCRYPTOR

FIGURE 207 Next Steps dialog box

Instructions for installing public key certificates for the encryption switch are displayed. These instructions are specific to the key vault type.

11. Review the post-configuration instructions, which you can copy to a clipboard or print for later.
12. Click **Finish** to exit the **Configure Switch Encryption** wizard.

Understanding configuration status results

After configuration of the encryption group is completed, the Management application sends API commands to verify the switch configuration. The CLI commands are detailed in encryption administrator's guide for your key vault management system.

- **Initialize the switch.** If the switch is not already in the initiated state, the Management application performs the `cryptocfg --initnode` command.
- **Create an encryption group on the switch.** The Management application creates a new group using the `cryptocfg --create -encgroup` command, and sets the key vault type using the `cryptocfg --set -keyvault command`.
- **Register the key vault.** The Management application registers the key vault using the `cryptocfg --reg keyvault` command.
- **Enable the encryption engines.** The Management application initializes an encryption switch using the `cryptocfg --initEE [<slotnumber>]` and `cryptocfg --regEE [<slotnumber>]` commands.
- **Create a new master key.** (Opaque key vaults only). The Management application checks for a new master key. New master keys are generated from the Security tab located in the **Encryption Group Properties** dialog box. See "Creating a new master key" on page 546 for more information.
- **Save the switch's public key certificate to a file.** The Management application saves the KAC certificate into the specified file.
- **Back up the master key to a file.** (Opaque key vaults only). The Management application saves the master key into the specified file.

NOTE
A master key is not generated if the key vault type is LKM. LKM manages DEK exchanges through a trusted link, and the LKM appliance uses its own master key to encrypt DEKs.

Adding a switch to an encryption group

The setup wizard allows you to either create a new encryption group, or add an encryption switch to an existing encryption group. Use the following procedure to add a switch to an encryption group:

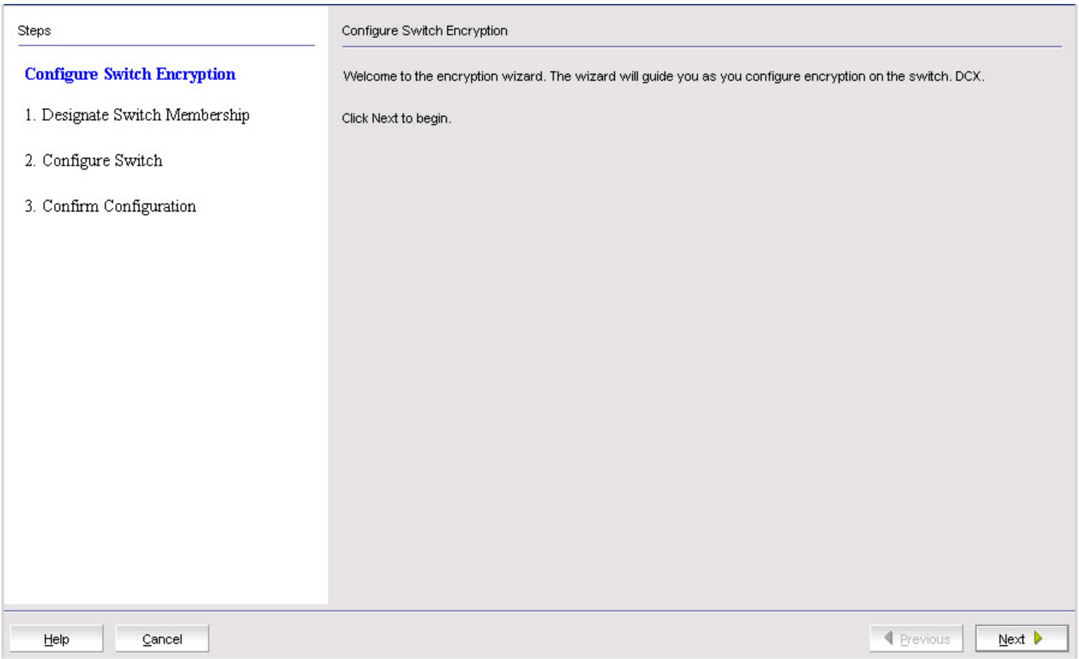
1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a switch to add from the **Encryption Center Devices** table, then select **Switch > Create/Add to Group** from the menu task bar, or right-click a switch and select **Create/Add to Group.**

   NOTE
   The switch must not already be in an encryption group.

   The **Configure Switch Encryption** wizard displays (step 208).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
3. Confirm Configuration
Configure Switch Encryption
Help
Cancel
Previous
Next

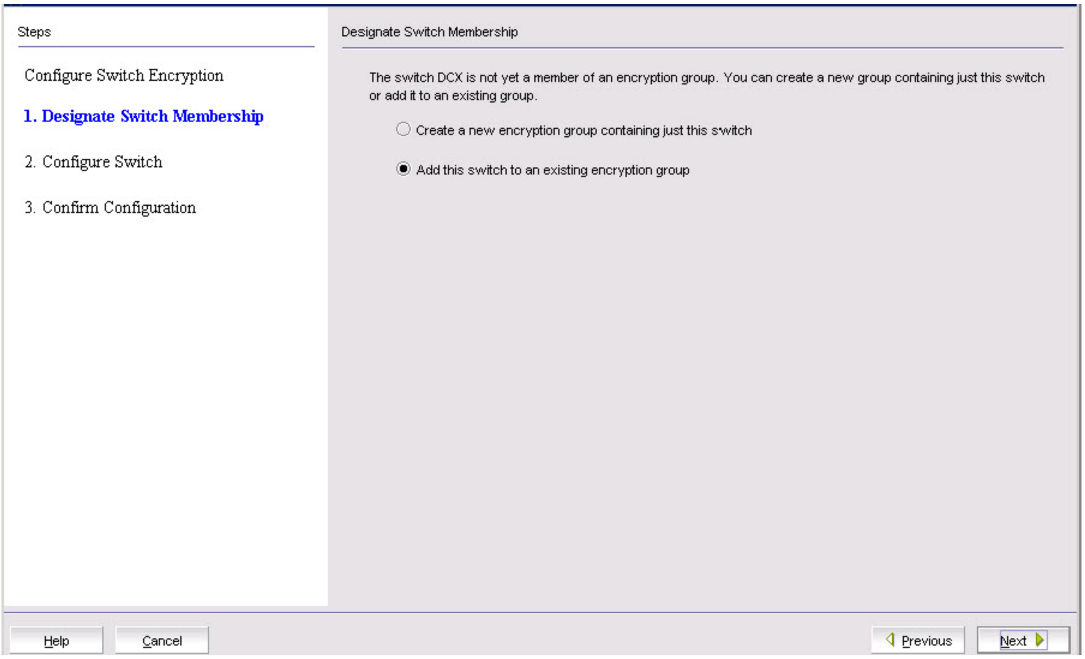
Welcome to the encryption wizard. The wizard will guide you as you configure encryption on the switch. DCX.

Click Next to begin.

FIGURE 208 Configure Switch Encryption wizard

3. Click **Next.**

   The **Designate Switch Membership** dialog box displays (Figure 209).


Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
3. Confirm Configuration
Designate Switch Membership
Help
Cancel
Previous
Next

The switch DCX is not yet a member of an encryption group. You can create a new group containing just this switch or add it to an existing group.

○ Create a new encryption group containing just this switch

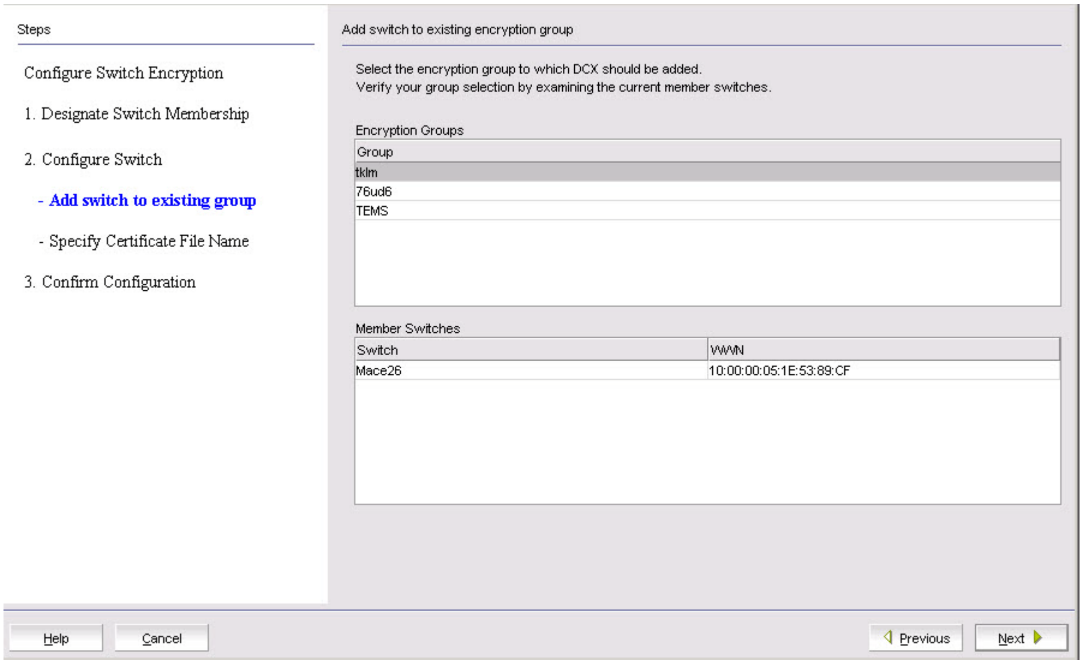
● Add this switch to an existing encryption group

FIGURE 209 Designate Switch Membership dialog box

4. Select **Add this switch to an existing encryption group.**

5. Click **Next.**

   The **Add Switch to Existing Encryption Group** dialog box displays.



Steps

Configure Switch Encryption

1. Designate Switch Membership

2. Configure Switch

   - **Add switch to existing group**

   - Specify Certificate File Name

3. Confirm Configuration

Add switch to existing encryption group

Select the encryption group to which DCX should be added.
Verify your group selection by examining the current member switches.

Encryption Groups

Group
tklm
76ud6
TEMS

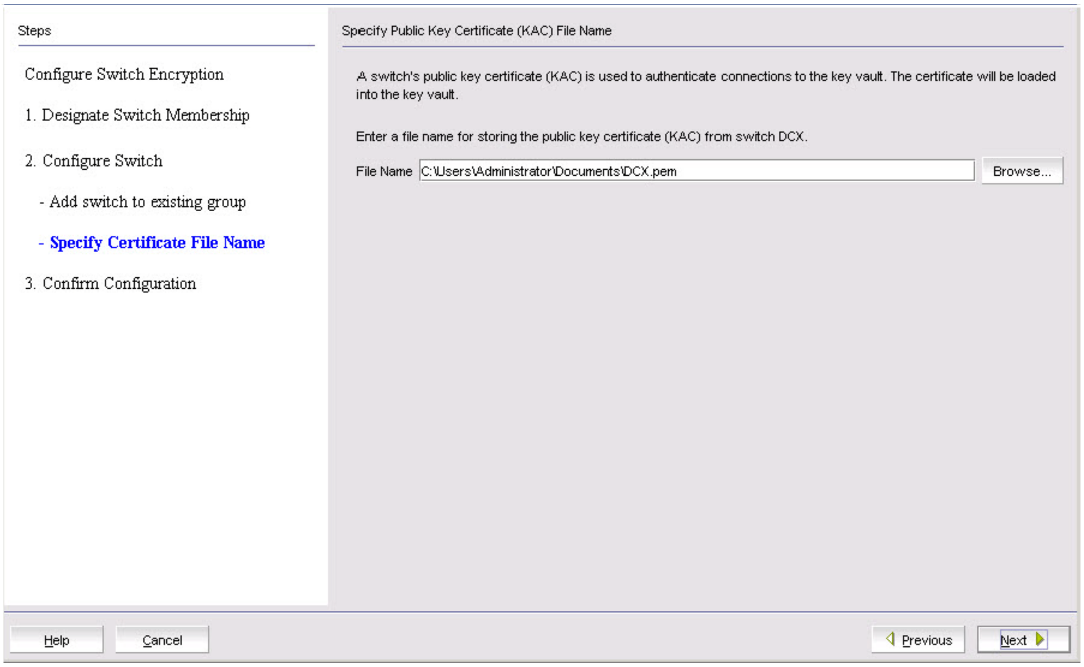
Member Switches

Switch	WWN
Mace26	10:00:00:05:1E:53:89:CF

FIGURE 210 Add Switch to Existing Encryption Group dialog box

6. Select the group in which to add the switch, then click **Next.**

   The **Specify Public Key Certificate File Name** dialog box displays (Figure 211).



Steps

Configure Switch Encryption

1. Designate Switch Membership

2. Configure Switch

   - Add switch to existing group

   - **Specify Certificate File Name**

3. Confirm Configuration

Specify Public Key Certificate (KAC) File Name

A switch's public key certificate (KAC) is used to authenticate connections to the key vault. The certificate will be loaded into the key vault.

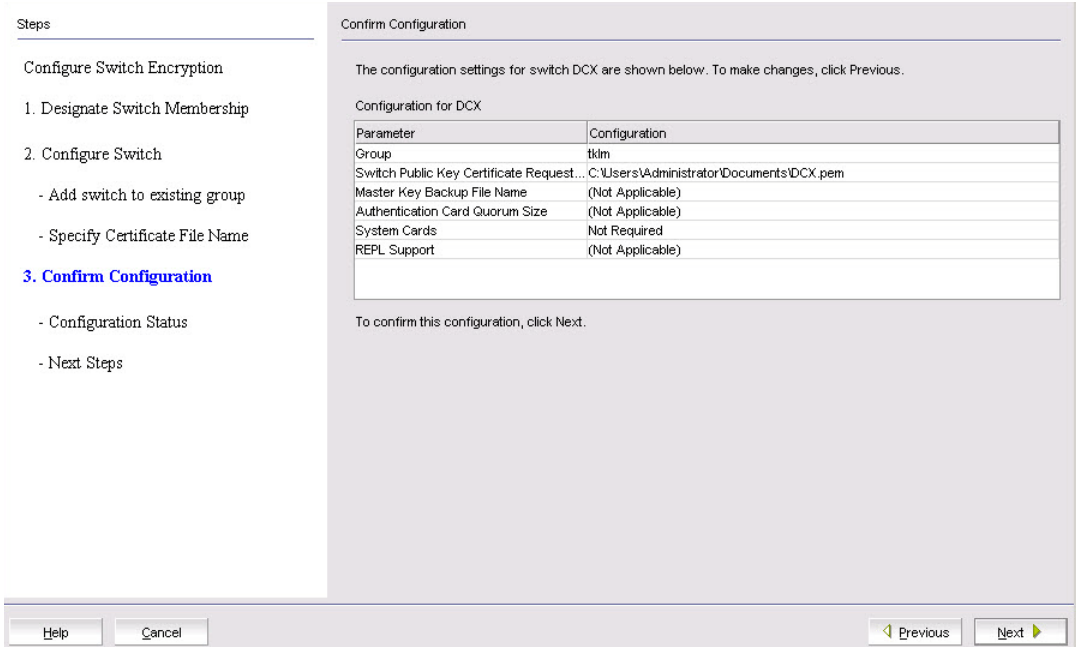
Enter a file name for storing the public key certificate (KAC) from switch DCX.

File Name C:\Users\Administrator\Documents\DCX.pem

FIGURE 211 Specify Public Key Certificate File Name dialog box

7. Specify the name of the file in which to store the public key certificate that is used to authenticate connections to the key vault, then click **Next**.

   The **Confirm Configuration** dialog box displays (Figure 212). The dialog box shows the encryption group name and switch public key certificate file name you specified.



The configuration settings for switch DCX are shown below. To make changes, click Previous.

Configuration for DCX

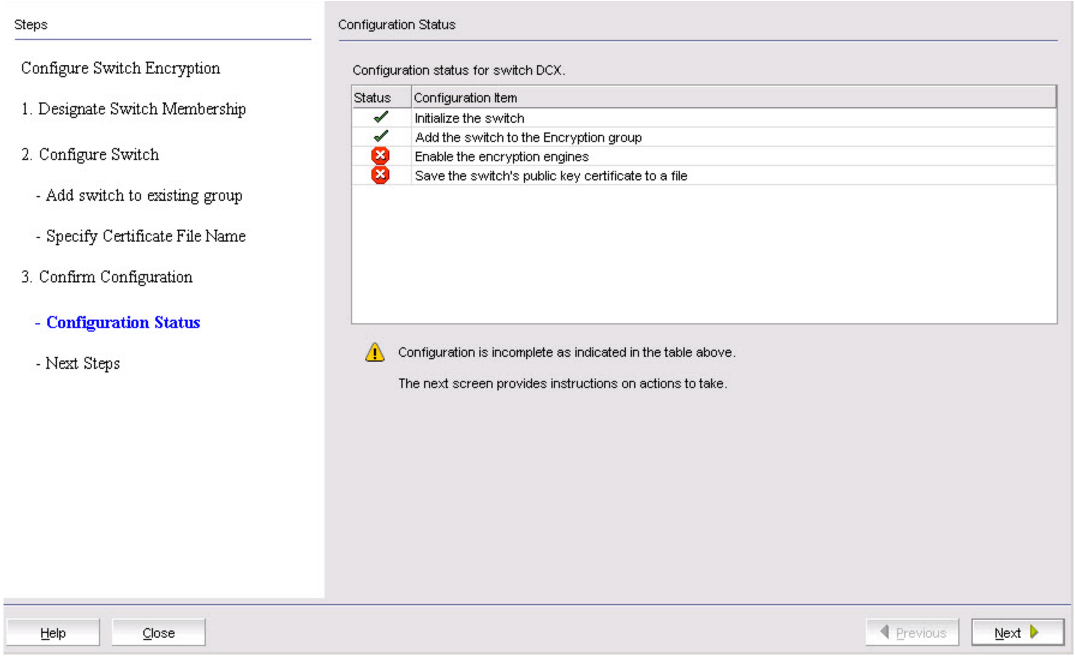
Parameter	Configuration
Group	tklm
Switch Public Key Certificate Request...	C:\Users\Administrator\Documents\DCX.pem
Master Key Backup File Name	(Not Applicable)
Authentication Card Quorum Size	(Not Applicable)
System Cards	Not Required
REPL Support	(Not Applicable)

To confirm this configuration, click Next.

FIGURE 212 Confirm Configuration dialog box

8. Click **Next**.

   The **Configuration Status** dialog box displays (Figure 213).



Steps
Configure Switch Encryption
1. Designate Switch Membership
2. Configure Switch
- Add switch to existing group
- Specify Certificate File Name
3. Confirm Configuration
- Configuration Status
- Next Steps

Configuration Status

Configuration status for switch DCX.

Status	Configuration Item
✓	Initialize the switch
✓	Add the switch to the Encryption group
☒	Enable the encryption engines
☒	Save the switch's public key certificate to a file

Configuration is incomplete as indicated in the table above.

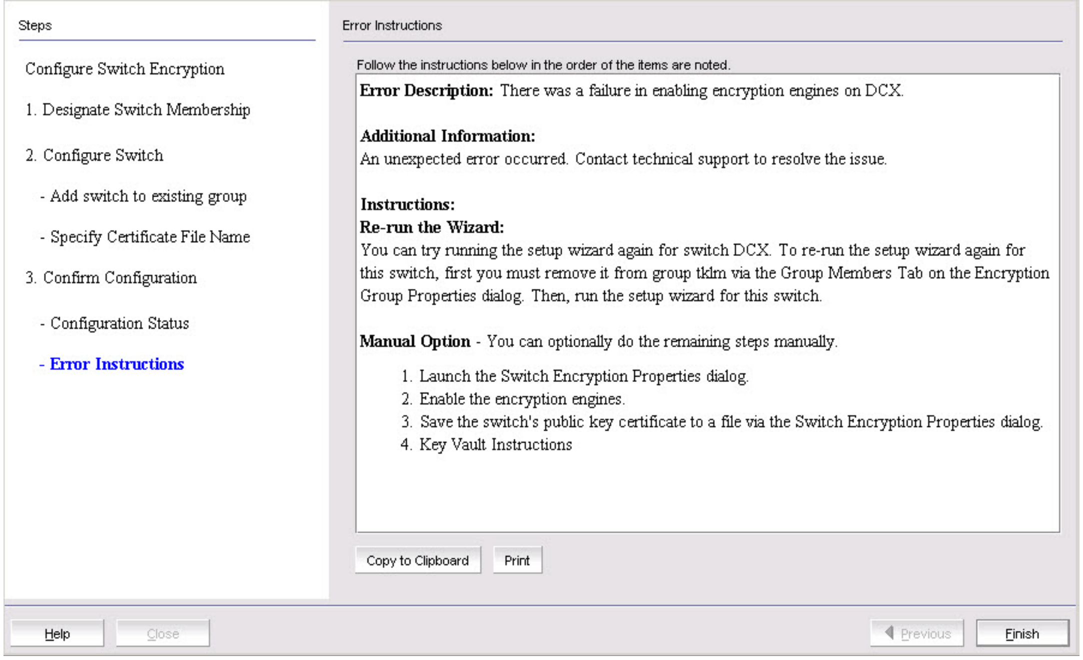
The next screen provides instructions on actions to take.

FIGURE 213 Configuration Status dialog box

All configuration items have green check marks if the configuration is successful. A red stop sign indicates a failed step. A message displays below the table, indicating the encryption switch was added to the group you named, and the public key certificate is stored in the location you specified.

9. Review important messages, then click **Next**.

   The **Error Instructions** dialog box displays (Figure 214).



Follow the instructions below in the order of the items are noted.

Error Description: There was a failure in enabling encryption engines on DCX.

Additional Information:
An unexpected error occurred. Contact technical support to resolve the issue.

Instructions:
Re-run the Wizard:
You can try running the setup wizard again for switch DCX. To re-run the setup wizard again for this switch, first you must remove it from group tklm via the Group Members Tab on the Encryption Group Properties dialog. Then, run the setup wizard for this switch.

Manual Option - You can optionally do the remaining steps manually.

1. Launch the Switch Encryption Properties dialog.
2. Enable the encryption engines.
3. Save the switch's public key certificate to a file via the Switch Encryption Properties dialog.
4. Key Vault Instructions

FIGURE 214 Error Instructions dialog box

Instructions for installing public key certificates for the encryption switch are displayed. These instructions are specific to the key vault type.

10. Review the post-configuration instructions, which you can copy to a clipboard or print for later.
11. Click **Finish** to exit the **Configure Switch Encryption** wizard.
12. Review “Understanding configuration status results” on page 504.

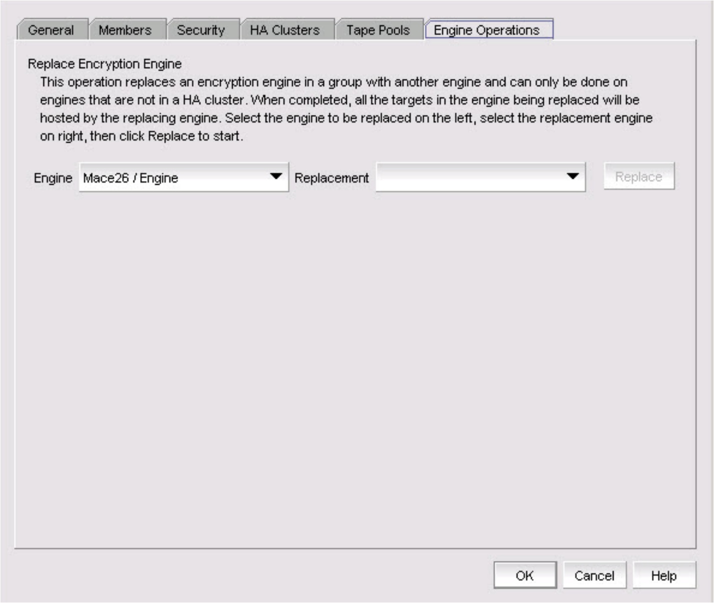
Replacing an encryption engine in an encryption group

To replace an encryption engine in an encryption group with another encryption engine within the same DEK Cluster, complete the following steps:

1. Select the engine from the **Encryption Center Devices** table, then select **Engine > Replace** from the menu task bar, or right-click the engine and select **Replace.**

   The **Encryption Group Properties** dialog box displays, with the **Engine Operations** tab selected (Figure 215).

   You can also display the **Engine Operations** tab by selecting an encryption group from the **Encryption Center Devices** table, selecting **Group > Properties** from the menu task bar, then selecting the **Engine Operations** tab, or right-click the group, select **Properties,** then select the **Engine Operations** tab.



Replace Encryption Engine

This operation replaces an encryption engine in a group with another engine and can only be done on engines that are not in a HA cluster. When completed, all the targets in the engine being replaced will be hosted by the replacing engine. Select the engine to be replaced on the left, select the replacement engine on right, then click Replace to start.

Engine: Mace26 / Engine

Replacement:

FIGURE 215 Engine Operations tab

2. Select the engine to replace from the **Engine** list.
3. Select the engine to use as the replacement from the **Replacement** list.
4. Click **Replace.**

   All containers hosted by the current engine (**Engine** list) are replaced by the new engine (**Replacement** list).

Creating high availability (HA) clusters

A high availability (HA) cluster is a group of exactly two encryption engines. One encryption engine can take over encryption and decryption tasks for the other encryption engine, if that member fails or becomes unreachable.

When creating a new HA Cluster, add one engine to create the cluster, then add the second engine. You can make multiple changes to the HA Clusters list; the changes are not applied to the switch until you click **OK**.

Both engines in an HA cluster must be in the same fabric, as well as the same encryption group.

NOTE
An IP address is required for the management port for any cluster-related operations.

1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

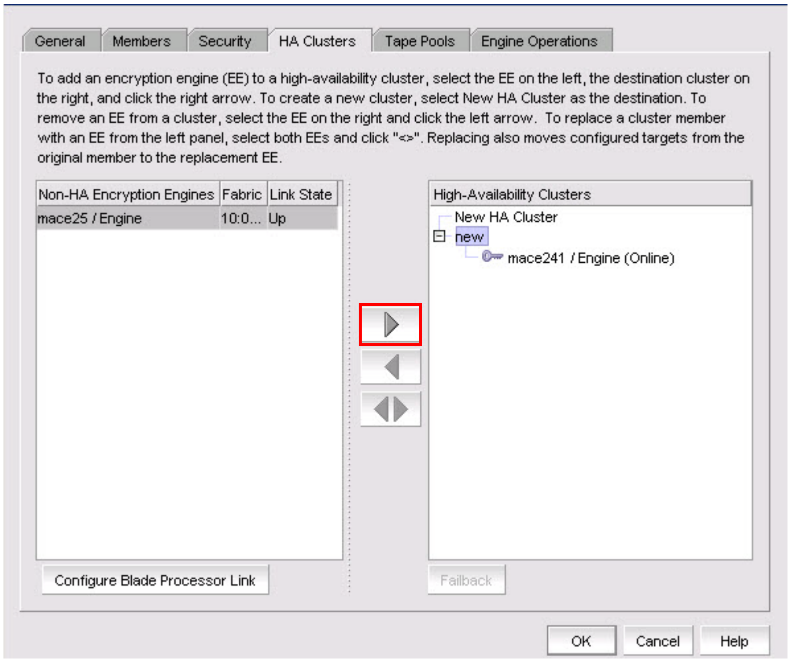
2. Select an encryption group from the **Encryption Center Devices** table, then select **Group** > **HA Cluster** from the menu task bar, or right-click an encryption group and select **HA Cluster.**

   NOTE
   If groups are not visible in the **Encryption Center Devices** table, select **View** > **Groups** from the menu task bar.

   The **Encryption Group Properties** dialog box displays, with the **HA Clusters** tab selected (Figure 216).

3. Select an available encryption engine from the **Non HA Encryption Engines** table and a destination HA cluster from the **High Availability Clusters** table**.** Select **New HA Cluster** if you are creating a new cluster.

4. Click the right arrow button to add the encryption engine to the selected HA cluster.



To add an encryption engine (EE) to a high-availability cluster, select the EE on the left, the destination cluster on the right, and click the right arrow. To create a new cluster, select New HA Cluster as the destination. To remove an EE from a cluster, select the EE on the right and click the left arrow. To replace a cluster member with an EE from the left panel, select both EEs and click "<>". Replacing also moves configured targets from the original member to the replacement EE.

Non-HA Encryption Engines	Fabric	Link State
mace25 / Engine	10:0...	Up

High-Availability Clusters
- New HA Cluster
- new
  - mace241 / Engine (Online)

FIGURE 216 Encryption Group Properties dialog box - HA Clusters tab

NOTE
If you are creating a new HA cluster, a dialog box displays requesting a name for the new HA cluster. HA Cluster names can have up to 31 characters. Letters, digits, and underscores are allowed.

Removing engines from an HA cluster

Removing the last engine from an HA cluster also removes the HA cluster.

If only one engine is removed from a two-engine cluster, you must either add another engine to the cluster, or remove the other engine.

1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select an encryption group from the **Encryption Center Devices** table, then select **Group** > **HA Cluster** from the menu task bar, or right-click an encryption group and select **HA Cluster**.

   The **Encryption Group Properties** dialog box displays, with the **HA Clusters** tab selected.

3. Select an engine from the **High Availability Clusters** table, then click the left arrow button. (Refer to Figure 216.)

4. Either remove the second engine or add a replacement second engine, making sure all HA clusters have exactly two engines.

5. Click **OK**.

Swapping engines in an HA cluster

Swapping engines is useful when replacing hardware. Swapping engines is different from removing an engine and adding another because when you swap engines, the configured targets on the former HA cluster member are moved to the new HA cluster member.

1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select an encryption group from the **Encryption Center Devices** table, then select **Group** > **HA Cluster** from the menu task bar, or right-click an encryption group and select **HA Cluster.**

   The **Encryption Group Properties** dialog box displays, with the **HA Clusters** tab selected.

To swap engines, select one engine from the **High Availability Clusters** table and one unclustered engine from encryption engine from the **Non HA Encryption Engines** table, then click the double-arrow button. (Refer to Figure 216.)

NOTE
The two engines being swapped must be in the same fabric.

Failback option

The **Failback** option determines the behavior when a failed encryption engine is restarted. When the first encryption engine comes back online, the encryption group's failback setting (auto or manual) determines how the encryption engine resumes encrypting and decrypting traffic to its encryption targets.

- In auto mode, when the first encryption engine restarts, it automatically resumes encrypting and decrypting traffic to its encryption targets.
- In manual mode, the second encryption engine continues handling the traffic until you manually invoke failback using the CLI or Management application, or until the second encryption engine fails.

Invoking failback

To invoke failback to the restarted encryption engine from the Management application, complete the following steps:

1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select an encryption group from the **Encryption Center Devices** table to which the encryption engine belongs, then click **Group** > **HA Clusters**, or right-click the group and select **HA Clusters**.

   The **Encryption Group Properties** dialog box displays, with the **HA Clusters** tab selected (Figure 216). Select the online encryption engine, then click **Failback**.

3. Click **OK.**

4. Click **Close** on the **Encryption Center** dialog box.

Adding encryption targets

Adding an encryption target maps storage devices and hosts to virtual targets and virtual initiators within the encryption switch.

NOTE
It is recommended that you configure the host and target in the same zone before configuring them for encryption. If the host and target are not already in the same zone, you can still configure them for encryption, but you will need to configure them in the same zone before you can commit the changes. If you attempt to close the Encryption Targets dialog box without committing the changes, you are reminded of uncommitted changes in the Management application.

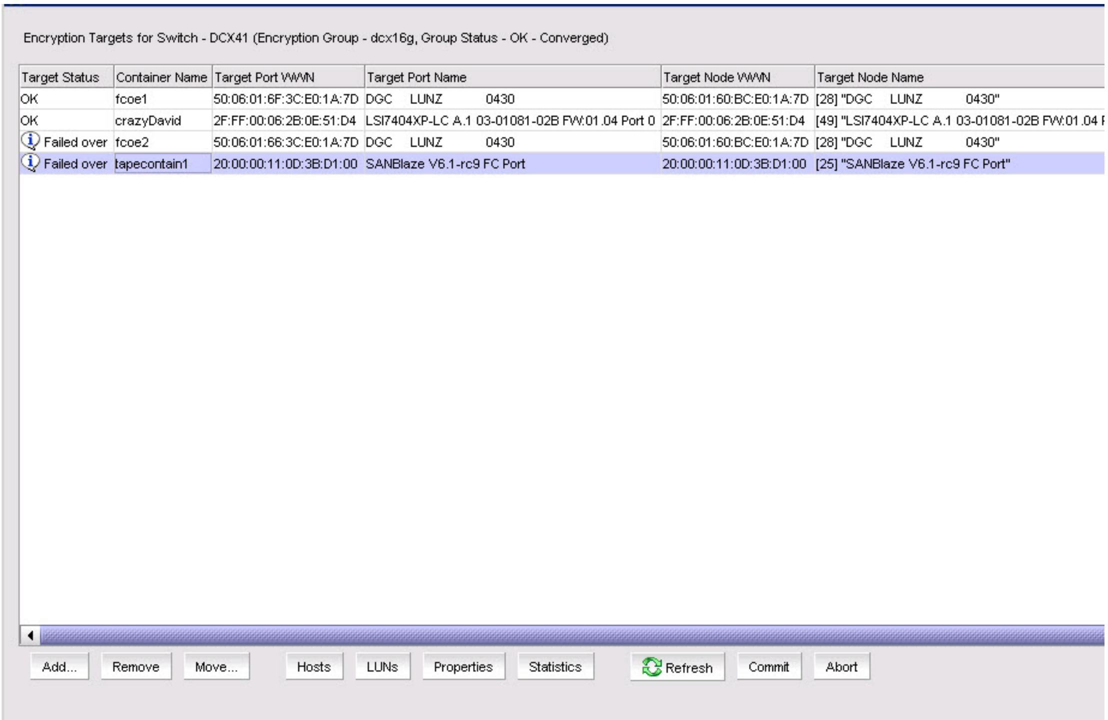
1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group, switch, or engine from the **Encryption Center Devices** table to which to add the target, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets**.

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   The **Encryption Targets** dialog box displays (Figure 217).



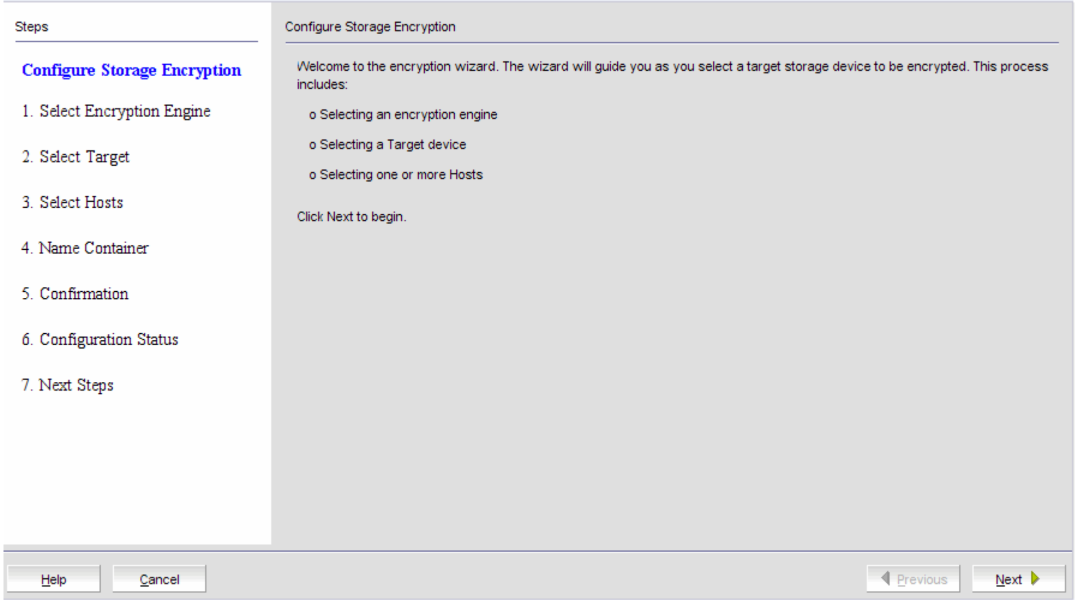
Encryption Targets for Switch - DCX41 (Encryption Group - dcx16g, Group Status - OK - Converged)

Target Status	Container Name	Target Port WWN	Target Port Name	Target Node WWN	Target Node Name
OK	fcoe1	50:06:01:6F:3C:E0:1A:7D	DGC LUNZ 0430	50:06:01:60:BC:E0:1A:7D	[28] "DGC LUNZ 0430"
OK	crazyDavid	2F:FF:00:06:2B:0E:51:D4	LSI7404XP-LC A.1 03-01081-02B FW:01.04 Port 0	2F:FF:00:06:2B:0E:51:D4	[49] "LSI7404XP-LC A.1 03-01081-02B FW:01.04 F
ⓘ Failed over	fcoe2	50:06:01:66:3C:E0:1A:7D	DGC LUNZ 0430	50:06:01:60:BC:E0:1A:7D	[28] "DGC LUNZ 0430"
ⓘ Failed over	tapecontain1	20:00:00:11:0D:3B:D1:00	SANBlaze V6.1-rc9 FC Port	20:00:00:11:0D:3B:D1:00	[25] "SANBlaze V6.1-rc9 FC Port"

FIGURE 217 Encryption Targets dialog box

3. Click **Add**, which launches the **Configure Switch Encryption** wizard.

   The **Configure Storage Encryption** dialog box displays. The dialog box explains the wizard's purpose, which is to configure encryption for a storage device (target).



Steps

Configure Storage Encryption

Welcome to the encryption wizard. The wizard will guide you as you select a target storage device to be encrypted. This process includes:

o Selecting an encryption engine

o Selecting a Target device

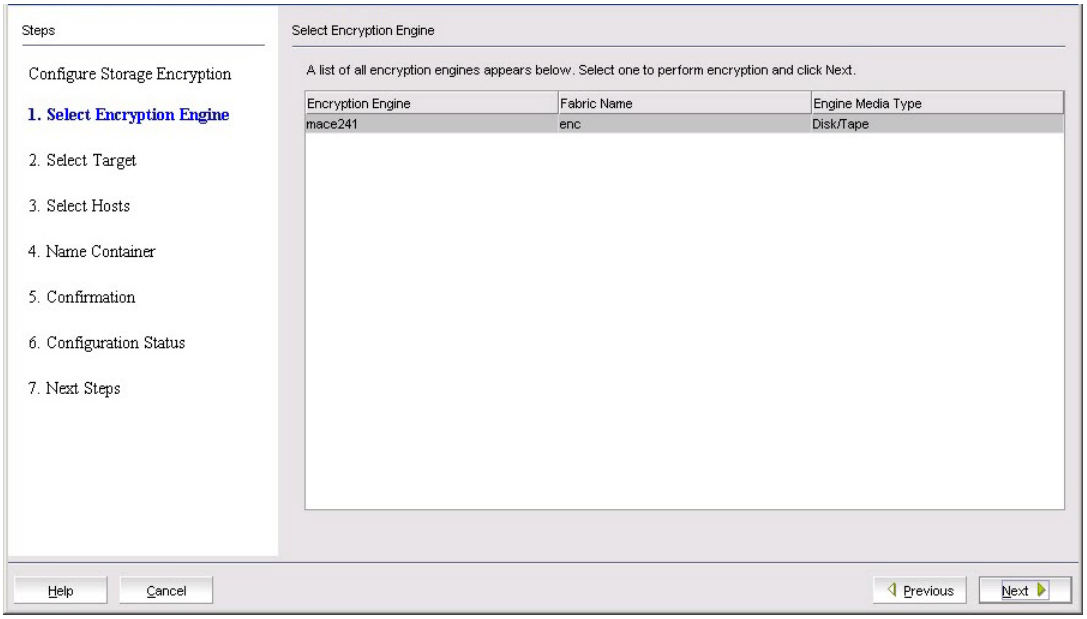
o Selecting one or more Hosts

Click Next to begin.

FIGURE 218 Configure Storage Encryption dialog box

4. Click **Next** to begin.

   The **Select Encryption Engine** dialog box displays (Figure 219).



Steps

Select Encryption Engine

A list of all encryption engines appears below. Select one to perform encryption and click Next.

Encryption Engine	Fabric Name	Engine Media Type
mace241	enc	Disk/Tape

FIGURE 219 Select Encryption Engine dialog box

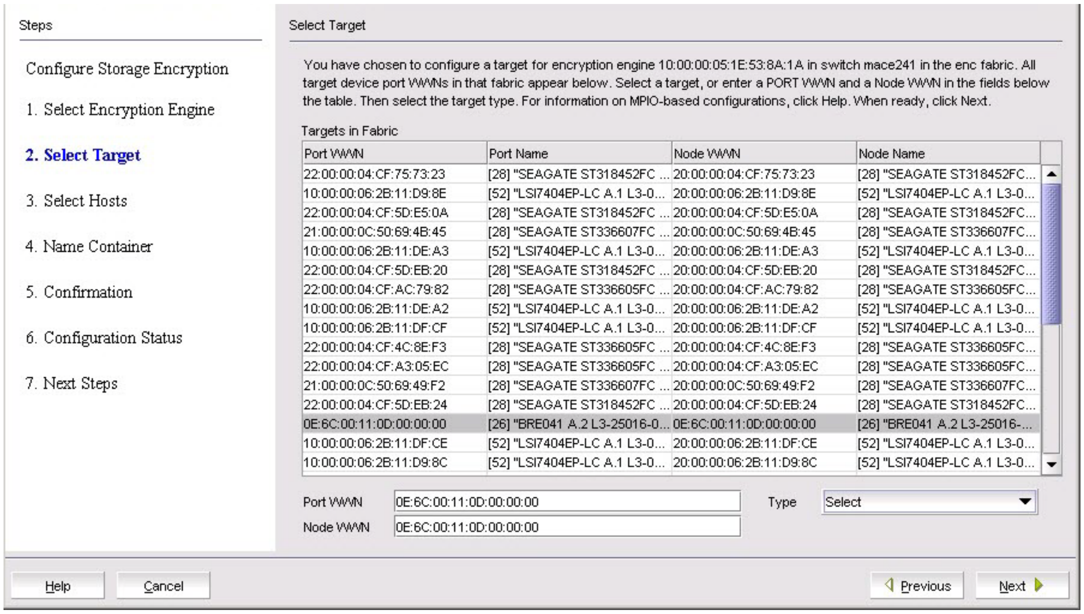
The list of engines depends on the scope being viewed.

- If the Targets dialog box is showing all targets in an encryption group, the list includes all engines in the group.
- If the Targets dialog box is showing all targets for a switch, the list includes all encryption engines for the switch.
- If the Targets dialog box is showing targets for a single encryption engine, the list contains only that engine.

5. Select the encryption engine (blade or switch) to configure, then click **Next.**

   The **Select Target** dialog box displays (Figure 220). The dialog box lists all target ports and target nodes in the same fabric as the encryption engine. The **Targets in Fabric** table does *not* show targets that are already configured in an encryption group.

   You can select targets from the list of known targets, or manually enter the port and node WWNs.



Select Target

You have chosen to configure a target for encryption engine 10:00:00:05:1E:53:8A:1A in switch mace241 in the enc fabric. All target device port WWNs in that fabric appear below. Select a target, or enter a PORT WWN and a Node WWN in the fields below the table. Then select the target type. For information on MPIO-based configurations, click Help. When ready, click Next.

Targets in Fabric

Port WWN	Port Name	Node WWN	Node Name
22:00:00:04:CF:75:73:23	[28] "SEAGATE ST318452FC ...	20:00:00:04:CF:75:73:23	[28] "SEAGATE ST318452FC...
10:00:00:06:2B:11:D9:8E	[52] "LSI7404EP-LC A.1 L3-0...	20:00:00:06:2B:11:D9:8E	[52] "LSI7404EP-LC A.1 L3-0...
22:00:00:04:CF:5D:E5:0A	[28] "SEAGATE ST318452FC ...	20:00:00:04:CF:5D:E5:0A	[28] "SEAGATE ST318452FC...
21:00:00:0C:50:69:4B:45	[28] "SEAGATE ST336607FC ...	20:00:00:0C:50:69:4B:45	[28] "SEAGATE ST336607FC...
10:00:00:06:2B:11:DE:A3	[52] "LSI7404EP-LC A.1 L3-0...	20:00:00:06:2B:11:DE:A3	[52] "LSI7404EP-LC A.1 L3-0...
22:00:00:04:CF:5D:EB:20	[28] "SEAGATE ST318452FC ...	20:00:00:04:CF:5D:EB:20	[28] "SEAGATE ST318452FC...
22:00:00:04:CF:AC:79:82	[28] "SEAGATE ST336605FC ...	20:00:00:04:CF:AC:79:82	[28] "SEAGATE ST336605FC...
10:00:00:06:2B:11:DE:A2	[52] "LSI7404EP-LC A.1 L3-0...	20:00:00:06:2B:11:DE:A2	[52] "LSI7404EP-LC A.1 L3-0...
10:00:00:06:2B:11:DF:CF	[52] "LSI7404EP-LC A.1 L3-0...	20:00:00:06:2B:11:DF:CF	[52] "LSI7404EP-LC A.1 L3-0...
22:00:00:04:CF:4C:8E:F3	[28] "SEAGATE ST336605FC ...	20:00:00:04:CF:4C:8E:F3	[28] "SEAGATE ST336605FC...
22:00:00:04:CF:A3:05:EC	[28] "SEAGATE ST336605FC ...	20:00:00:04:CF:A3:05:EC	[28] "SEAGATE ST336605FC...
21:00:00:0C:50:69:49:F2	[28] "SEAGATE ST336607FC ...	20:00:00:0C:50:69:49:F2	[28] "SEAGATE ST336607FC...
22:00:00:04:CF:5D:EB:24	[28] "SEAGATE ST318452FC ...	20:00:00:04:CF:5D:EB:24	[28] "SEAGATE ST318452FC...
0E:6C:00:11:0D:00:00:00	[26] "BRE041 A.2 L3-25016-0...	0E:6C:00:11:0D:00:00:00	[26] "BRE041 A.2 L3-25016-...
10:00:00:06:2B:11:DF:CE	[52] "LSI7404EP-LC A.1 L3-0...	20:00:00:06:2B:11:DF:CE	[52] "LSI7404EP-LC A.1 L3-0...
10:00:00:06:2B:11:D9:8C	[52] "LSI7404EP-LC A.1 L3-0...	20:00:00:06:2B:11:D9:8C	[52] "LSI7404EP-LC A.1 L3-0...

Port WWN: 0E:6C:00:11:0D:00:00:00
Node WWN: 0E:6C:00:11:0D:00:00:00
Type: Select

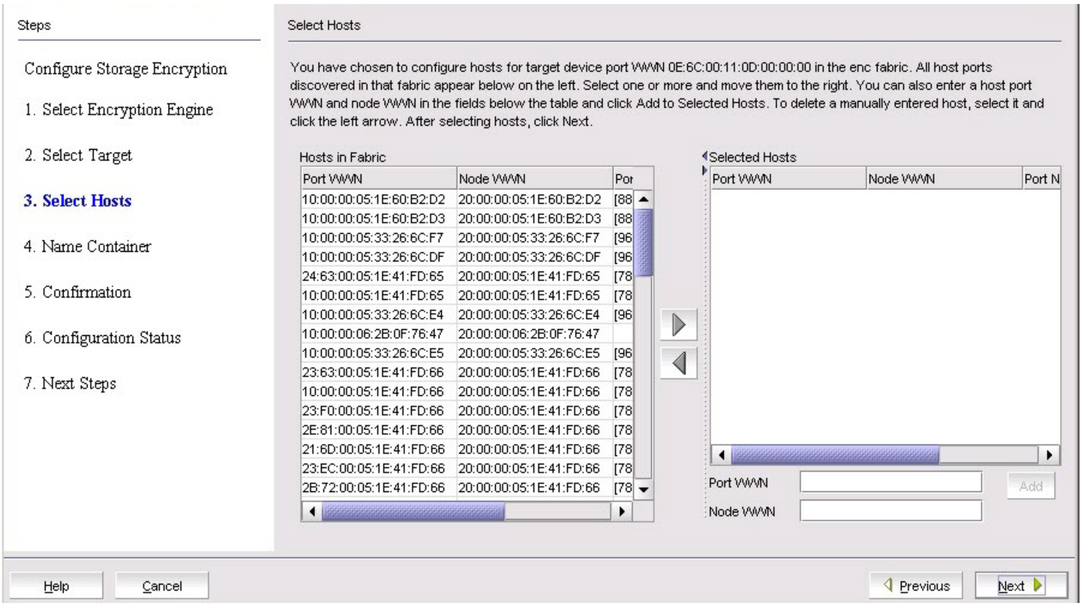
FIGURE 220 Select Target dialog box

   a. Select a target from the list. (The **Target Port WWN** and **Target Node WWN** fields contain all target information that displays when using the `nsshow` command.) You can also enter WWNs manually, for example, to specify a target that is not on the list.

   b. Select a target type from the **Type** list. If the target node is disk storage, choose **Disk**. If the target node is tape storage, choose **Tape**.

6. Click **Next.**

   The **Select Hosts** dialog box displays (Figure 221). The dialog box lists all hosts that are in the same fabric as the encryption engine.



Select Hosts

You have chosen to configure hosts for target device port WWN 0E:6C:00:11:0D:00:00:00 in the enc fabric. All host ports discovered in that fabric appear below on the left. Select one or more and move them to the right. You can also enter a host port WWN and node WWN in the fields below the table and click Add to Selected Hosts. To delete a manually entered host, select it and click the left arrow. After selecting hosts, click Next.

Hosts in Fabric

Port WWN	Node WWN	Por
10:00:00:05:1E:60:B2:D2	20:00:00:05:1E:60:B2:D2	[88
10:00:00:05:1E:60:B2:D3	20:00:00:05:1E:60:B2:D3	[88
10:00:00:05:33:26:6C:F7	20:00:00:05:33:26:6C:F7	[96
10:00:00:05:33:26:6C:DF	20:00:00:05:33:26:6C:DF	[96
24:63:00:05:1E:41:FD:65	20:00:00:05:1E:41:FD:65	[78
10:00:00:05:1E:41:FD:65	20:00:00:05:1E:41:FD:65	[78
10:00:00:05:33:26:6C:E4	20:00:00:05:33:26:6C:E4	[96
10:00:00:06:2B:0F:76:47	20:00:00:06:2B:0F:76:47	
10:00:00:05:33:26:6C:E5	20:00:00:05:33:26:6C:E5	[96
23:63:00:05:1E:41:FD:66	20:00:00:05:1E:41:FD:66	[78
10:00:00:05:1E:41:FD:66	20:00:00:05:1E:41:FD:66	[78
23:F0:00:05:1E:41:FD:66	20:00:00:05:1E:41:FD:66	[78
2E:81:00:05:1E:41:FD:66	20:00:00:05:1E:41:FD:66	[78
21:6D:00:05:1E:41:FD:66	20:00:00:05:1E:41:FD:66	[78
23:EC:00:05:1E:41:FD:66	20:00:00:05:1E:41:FD:66	[78
2B:72:00:05:1E:41:FD:66	20:00:00:05:1E:41:FD:66	[78

Selected Hosts

Port WWN	Node WWN	Port N

FIGURE 221 Select Hosts dialog box

7. Select hosts using either of the following methods:

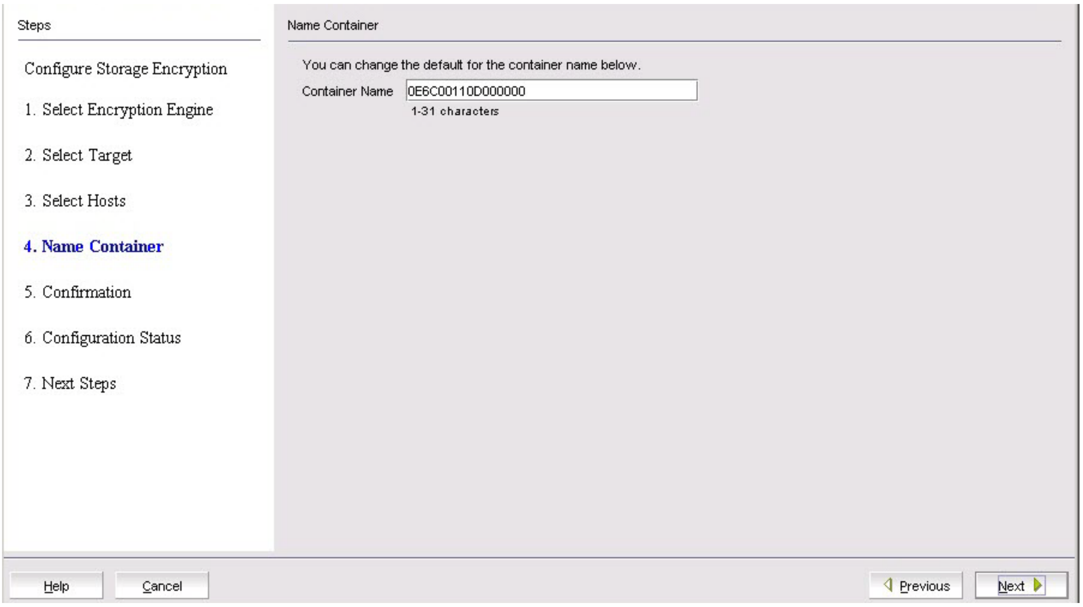
    a. Select a maximum of 1024 hosts from the **Hosts in Fabric** table, then click the right arrow to move the hosts to the **Selected Hosts** table. (The **Port WWN** column contains all target information that displays when using the `nsshow` command.)

    b. Manually enter world wide names in the **Port WWN** and **Node WWN** text boxes if the hosts are not included in the table. You must fill in both the Port WWN and the Node WWN. Click **Add** to move the host to the **Selected Hosts** table.

8. Click **Next.**

    The **Name Container** dialog box displays (Figure 222). The name container dialog box enables you to specify a name for the target container that is created in the encryption engine to hold the target configuration data.

    The container name defaults to the target WWPN. You can, however, rename the container name. Target container names can have up to 31 characters. Letters, digits, and underscores are allowed.



You can change the default for the container name below.

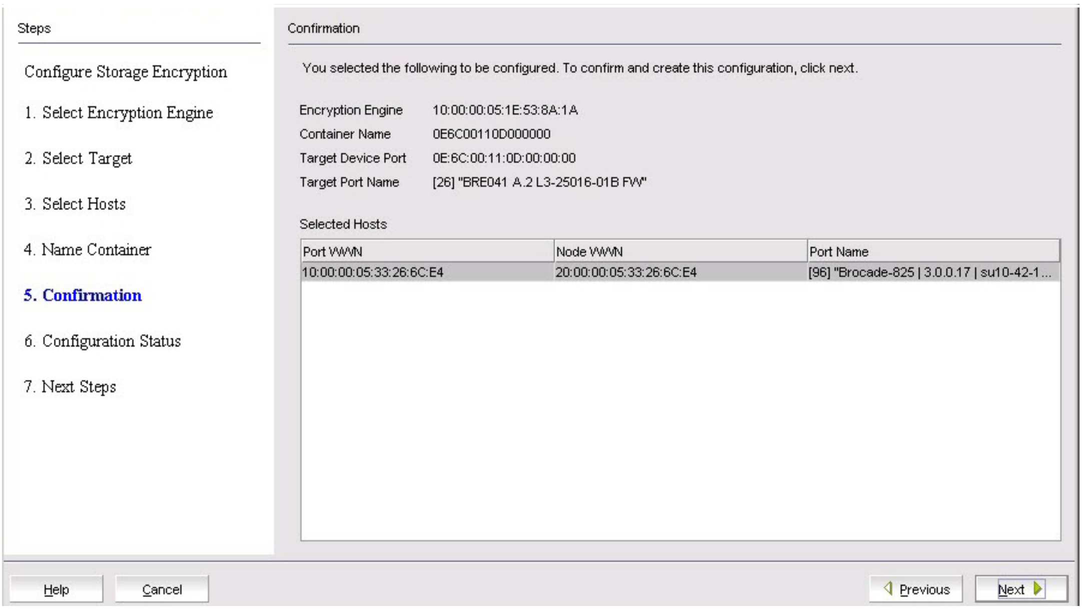
Container Name 0E6C00110D000000

1-31 characters

FIGURE 222 Name Container dialog box

9. Click **Next**.

   The **Confirmation** dialog box displays (Figure 223).



You selected the following to be configured. To confirm and create this configuration, click next.

Encryption Engine	10:00:00:05:1E:53:8A:1A
Container Name	0E6C00110D000000
Target Device Port	0E:6C:00:11:0D:00:00:00
Target Port Name	[26] "BRE041 A.2 L3-25016-01B FW"

Selected Hosts

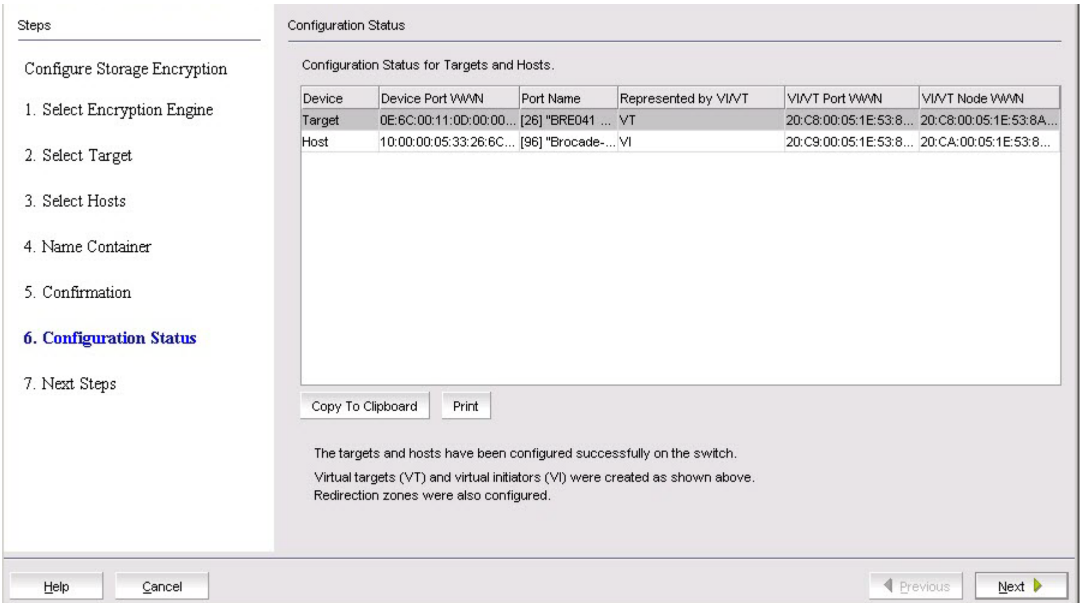
Port WWN	Node WWN	Port Name
10:00:00:05:33:26:6C:E4	20:00:00:05:33:26:6C:E4	[96] "Brocade-825 | 3.0.0.17 | su10-42-1...

FIGURE 223 Confirmation dialog box

10. Click **Next** after you have verified the contents. Clicking **Next** creates the configuration.

    The **Configuration Status** dialog box displays (Figure 224). The **Configuration Status** dialog box lists the target and host that are configured in the target container, as well as the virtual targets (VT) and virtual initiators (VI).

NOTE
If you can view the VI/VT Port WWNs and VI/VT Node WWNs, the container has been successfully added to the switch.



Configuration Status for Targets and Hosts.

Device	Device Port WWN	Port Name	Represented by VI/VT	VI/VT Port WWN	VI/VT Node WWN
Target	0E:6C:00:11:0D:00:00...	[26] "BRE041 ...	VT	20:C8:00:05:1E:53:8...	20:C8:00:05:1E:53:8A...
Host	10:00:00:05:33:26:6C...	[96] "Brocade-...	VI	20:C9:00:05:1E:53:8...	20:CA:00:05:1E:53:8...

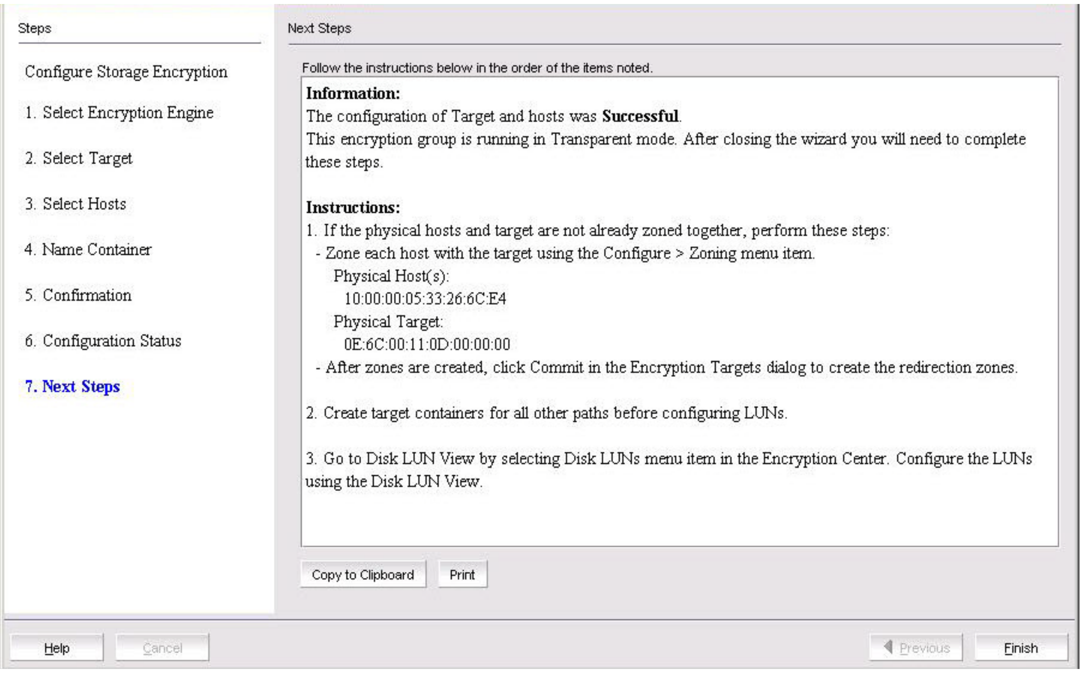
The targets and hosts have been configured successfully on the switch.
Virtual targets (VT) and virtual initiators (VI) were created as shown above.
Redirection zones were also configured.

FIGURE 224 Configuration Status dialog box

11. Review any post-configuration instructions or messages, which you can copy to a clipboard or print for later.

12. Click **Next**.

    The **Next Steps** dialog box displays (Figure 225).



Follow the instructions below in the order of the items noted.

Information:
The configuration of Target and hosts was **Successful**.
This encryption group is running in Transparent mode. After closing the wizard you will need to complete these steps.

Instructions:
1. If the physical hosts and target are not already zoned together, perform these steps:
- Zone each host with the target using the Configure > Zoning menu item.
Physical Host(s):
10:00:00:05:33:26:6C:E4
Physical Target:
0E:6C:00:11:0D:00:00:00
- After zones are created, click Commit in the Encryption Targets dialog to create the redirection zones.

2. Create target containers for all other paths before configuring LUNs.

3. Go to Disk LUN View by selecting Disk LUNs menu item in the Encryption Center. Configure the LUNs using the Disk LUN View.

FIGURE 225 Next Steps dialog box

Instructions for installing public key certificates for the encryption switch are displayed. These instructions are specific to the key vault type.

13. Review the post-configuration instructions, which you can copy to a clipboard or print for later.

14. Click **Finish** to exit the **Configure Switch Encryption** wizard.

15. Review "Understanding configuration status results" on page 504.

Configuring hosts for encryption targets

Use the **Encryption Target Hosts** dialog box to edit (add or remove) hosts for an encrypted target.

NOTE
Hosts are normally selected as part of the **Configure Switch Encryption** wizard, but you can also edit hosts later using the **Encryption Target Hosts** dialog box.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

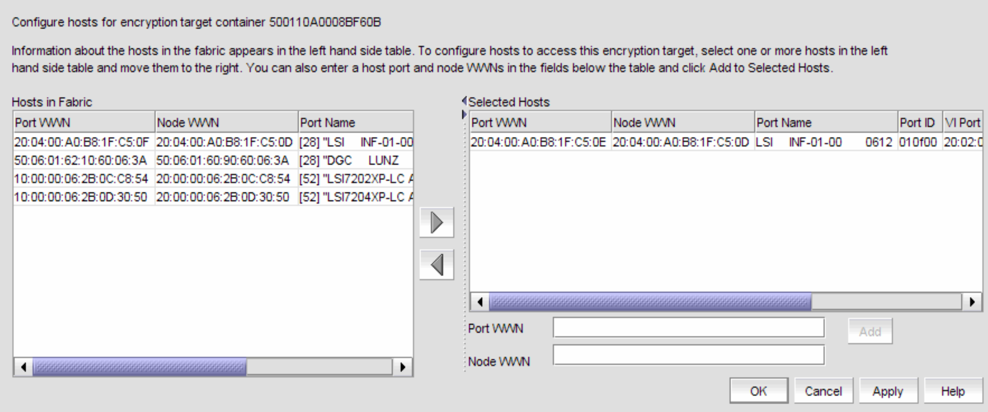
2. Select a group, switch, or engine from the **Encryption Center Devices** table that contains the storage device to be configured, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets.**

   The **Encryption Targets** dialog box displays (Figure 217).

3. Select a target storage device from the list, then click **Hosts.**

   The **Encryption Target Hosts** dialog box displays. The dialog box lists configured hosts in a fabric.

4. Select one or more hosts in a fabric, then move them to the **Selected Hosts** table using the right arrow, or manually enter world wide names in the **Port WWN** and **Node WWN** text boxes if the hosts are not included in the list. You must fill in both the Port WWN and the Node WWN. Click **Add** to move the host to the **Selected Hosts** list.



Configure hosts for encryption target container 500110A0008BF60B

Information about the hosts in the fabric appears in the left hand side table. To configure hosts to access this encryption target, select one or more hosts in the left hand side table and move them to the right. You can also enter a host port and node WWNs in the fields below the table and click Add to Selected Hosts.

Hosts in Fabric

Port WWN	Node WWN	Port Name
20:04:00:A0:B8:1F:C5:0F	20:04:00:A0:B8:1F:C5:0D	[28] "LSI INF-01-00
50:06:01:62:10:60:06:3A	50:06:01:60:90:60:06:3A	[28] "DGC LUNZ
10:00:00:06:2B:0C:C8:54	20:00:00:06:2B:0C:C8:54	[52] "LSI7202XP-LC A
10:00:00:06:2B:0D:30:50	20:00:00:06:2B:0D:30:50	[52] "LSI7204XP-LC A

Selected Hosts

Port WWN	Node WWN	Port Name	Port ID	VI Port
20:04:00:A0:B8:1F:C5:0E	20:04:00:A0:B8:1F:C5:0D	LSI INF-01-00 0612	010f00	20:02:0

Port WWN

Node WWN

FIGURE 226 Encryption Target Hosts dialog box

Adding target disk LUNs for encryption

You can add a new path to an existing disk LUN or add a new LUN and path by launching the **Add New Path** wizard. To launch the wizard, complete the following steps:

Before You Begin

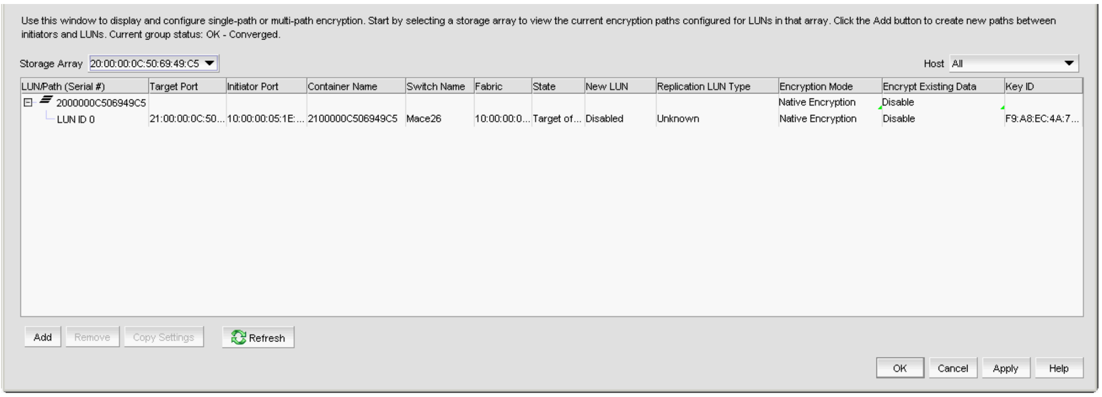
Before you can add a target disk LUN for encryption, you must first configure the Storage Arrays. For more information, see "Configuring Storage Arrays" on page 524.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group, switch, or engine from the **Encryption Center Devices** table, then select **Group/Switch/Engine > Disk LUNs** from the menu task bar, or right-click a group, switch, or engine and select **Disk LUNs.**

   The **Encryption Disk LUN View** dialog box displays (Figure 227).



Use this window to display and configure single-path or multi-path encryption. Start by selecting a storage array to view the current encryption paths configured for LUNs in that array. Click the Add button to create new paths between initiators and LUNs. Current group status: OK - Converged.

Storage Array 20:00:00:0C:50:69:49:C5

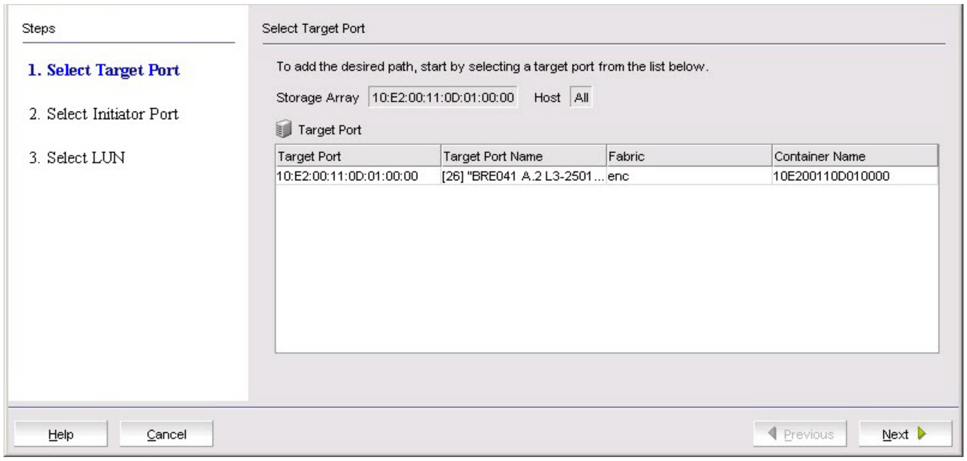
Host All

LUN/Path (Serial #)	Target Port	Initiator Port	Container Name	Switch Name	Fabric	State	New LUN	Replication LUN Type	Encryption Mode	Encrypt Existing Data	Key ID
2000000C506949C5									Native Encryption	Disable	
LUN ID 0	21:00:00:0C:50...	10:00:00:05:1E:...	2100000C506949C5	Mace26	10:00:00:0...	Target of...	Disabled	Unknown	Native Encryption	Disable	F9:A8:EC:4A:7...

FIGURE 227 Encryption Disk LUN View dialog box

3. Click **Add**.

   The **Select Target Port** dialog box displays (Figure 228).



To add the desired path, start by selecting a target port from the list below.

Storage Array 10:E2:00:11:0D:01:00:00 Host All

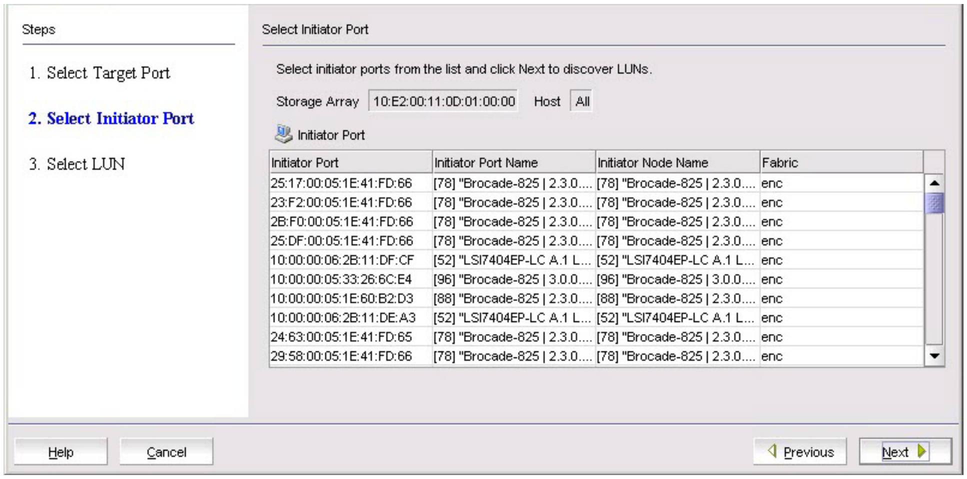
Target Port	Target Port Name	Fabric	Container Name
10:E2:00:11:0D:01:00:00	[26] "BRE041 A.2 L3-2501 ...	enc	10E200110D010000

FIGURE 228 Select Target Port dialog box

4. Select the target port from the **Target Port** table.

5. Click **Next**.

   The **Select Initiator Port** dialog box displays (Figure 229).



Select initiator ports from the list and click Next to discover LUNs.

Storage Array 10:E2:00:11:0D:01:00:00 Host All

Initiator Port	Initiator Port Name	Initiator Node Name	Fabric
25:17:00:05:1E:41:FD:66	[78] "Brocade-825 | 2.3.0....	[78] "Brocade-825 | 2.3.0....	enc
23:F2:00:05:1E:41:FD:66	[78] "Brocade-825 | 2.3.0....	[78] "Brocade-825 | 2.3.0....	enc
2B:F0:00:05:1E:41:FD:66	[78] "Brocade-825 | 2.3.0....	[78] "Brocade-825 | 2.3.0....	enc
25:DF:00:05:1E:41:FD:66	[78] "Brocade-825 | 2.3.0....	[78] "Brocade-825 | 2.3.0....	enc
10:00:00:06:2B:11:DF:CF	[52] "LSI7404EP-LC A.1 L...	[52] "LSI7404EP-LC A.1 L...	enc
10:00:00:05:33:26:6C:E4	[96] "Brocade-825 | 3.0.0....	[96] "Brocade-825 | 3.0.0....	enc
10:00:00:05:1E:60:B2:D3	[88] "Brocade-825 | 2.3.0....	[88] "Brocade-825 | 2.3.0....	enc
10:00:00:06:2B:11:DE:A3	[52] "LSI7404EP-LC A.1 L...	[52] "LSI7404EP-LC A.1 L...	enc
24:63:00:05:1E:41:FD:65	[78] "Brocade-825 | 2.3.0....	[78] "Brocade-825 | 2.3.0....	enc
29:58:00:05:1E:41:FD:66	[78] "Brocade-825 | 2.3.0....	[78] "Brocade-825 | 2.3.0....	enc

FIGURE 229 Select Initiator Port dialog box

6. Select the initiator port from the **Initiator Port** table.

7. Click **Next**.

LUN discovery is launched and a progress bar displays. There are four possible outcomes:

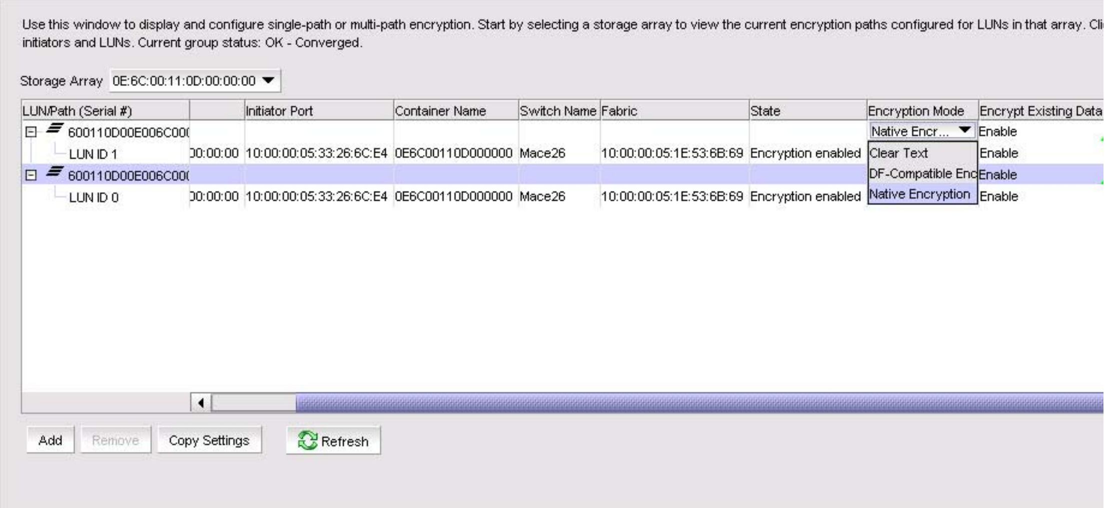
- A message displays indicating no LUNs were discovered. Click **OK** to dismiss the message and exit the wizard.
- A message displays indicating LUNs have been discovered, but are already configured. Click **OK** to dismiss the message and exit the wizard.
- A message displays indicating that the target is not in the right state for discovering LUNs. Click **OK** to dismiss the message and exit the wizard.
- The **Select LUN** dialog box displays, showing discovered LUNs that are available. Select the LUN from **LUN** list.

8. If **REPL Support** was enabled by the **Configure Switch Encryption** wizard, a **New LUN** check box is presented and enabled by default. If this LUN is to be paired with another LUN for SRDF data replication, the **New LUN** option must be enabled by selecting this check box. Refer to "Metadata requirements and remote replication" for information about how this option works. If **REPL support** was not enabled, this check box is not displayed.

9. Click **Finish**.

   The new LUN path is added to the **Encryption Disk LUN** view.

10. In environments where there are multiple paths to the same LUNs, it is critical that the same LUN policies are configured on all instances of the LUN. Be sure to return to the **Encryption Disk LUN View** dialog box to determine if there are configuration mismatches. Check under **Encryption Mode** for any entries showing **Mismatch.** To correct the mismatch, click the incorrect mode to display the choices, then select the correct mode (Figure 230).



Use this window to display and configure single-path or multi-path encryption. Start by selecting a storage array to view the current encryption paths configured for LUNs in that array. Cli
initiators and LUNs. Current group status: OK - Converged.

Storage Array 0E:6C:00:11:0D:00:00:00

LUN/Path (Serial #)		Initiator Port	Container Name	Switch Name	Fabric	State	Encryption Mode	Encrypt Existing Data
600110D00E006C00(							Native Encr...	Enable
LUN ID 1	)0:00:00	10:00:00:05:33:26:6C:E4	0E6C00110D000000	Mace26	10:00:00:05:1E:53:6B:69	Encryption enabled	Clear Text	Enable
600110D00E006C00(							DF-Compatible Enc	Enable
LUN ID 0	)0:00:00	10:00:00:05:33:26:6C:E4	0E6C00110D000000	Mace26	10:00:00:05:1E:53:6B:69	Encryption enabled	Native Encryption	Enable

FIGURE 230 Correcting an Encryption Mode Mismatch

When you correct a policy on a LUN, it is automatically selected for all paths to the selected LUN. When you modify LUN policies, a Modify icon appears to identify the modified LUN entry.

11. Click **OK** or **Apply** to apply the changes.

Configuring Storage Arrays

The Storage Array contains a list of storage ports that will be used later in the LUN centric view. You must assign storage ports from the same storage array for multi-path I/O purposes. On the LUN centric view, storage ports in the same storage array are used to get the associated CryptoTarget containers and initiators from the database. Storage ports that are not assigned to any storage array but are within the fabrics of the encryption group will be listed as a single target port on the LUN centric view. Storage Arrays are configured using the Storage Port Mapping dialog box. You will need to:

- Configure target and zone initiator ports in the same zone in order for the target container to come online and discover LUNs in the storage system.
- Create CryptoTarget containers for each target port in the storage array from the Target Container dialog box. Add initiator ports to the container. You must create target containers for those target ports in the configured storage arrays or unassigned target ports before mapping any LUN on the LUN centric view. If you do not create the container, LUN discovery will not function.

For more detailed information on creating a crypto target container, refer to the chapter describing storage arrays in this administrator’s guide.

Remote replication LUNs

The Symmetrix Remote Data Facility (SRDF) transmits data that is being written to both a local Symmetrix array and a remote symmetrix array. The replicated data facilitates a fast switchover to the remote site for data recovery.

SRDF supports the following methods of data replication:

- Synchronous Replication provides real-time mirroring of data between the source Symmetrix and the target Symmetrix systems. Data is written simultaneously to the cache of both systems in real time before the application I/O is completed, thus ensuring the highest possible data availability.
- Semi-Synchronous Replication writes data to the source system, completes the I/O, then synchronizes the data with the target system. Since the I/O is completed prior to synchronizing data with the target system, this method provides an added performance advantage. A second write will not be accepted on a Symmetrix source device until its target device has been synchronized.
- Adaptive Copy Replication transfers data from the source devices to the remote devices without waiting for an acknowledgment. This is especially useful when transferring large amounts of data during data center migrations, consolidations, and in data mobility environments.
- Asynchronous Replication places host writes into chunks and then transfers an entire chunk to the target system. When a complete chunk is received on the target system, the copy cycle is committed. If the SRDF links are lost during data transfer, any partial chunk is discarded, preserving consistency on the target system. This method provides a consistent point-in-time remote image that is not far behind the source system and results in minimal data loss if there is a disaster at the source site.

SRDF pairs

Remote replication is implemented by establishing a synchronized pair of SRDF devices connected by FC or IP links. A local source device is paired with a remote target device while data replication is taking place. While the SRDF devices are paired, the remote target device is not locally accessible for read or write operations. When the data replication operation completes, the pair may be split to enable normal read/write access to both devices. The pair may be restored to restore the data on the local source device.

Figure 231 shows the placement of encryption switches in an SRDF configuration. When encryption is enabled for the primary LUN, encrypted data written by the local application server to the primary LUN is replicated on the secondary LUN. The data is encrypted using a DEK that was generated on the local encryption switch and stored on the local RKM key vault. When each site has an independent key vault, as shown in Figure 231, the key vaults must be synchronized to ensure the availability of the DEK at the remote site. Refer to RKM user documentation for information about how to synchronize the key vaults. Both sites may share the same key vault, which eliminates the need for synchronization across sites. Depending on distance between sites, sharing a key vault may add some latency when retrieving a key.

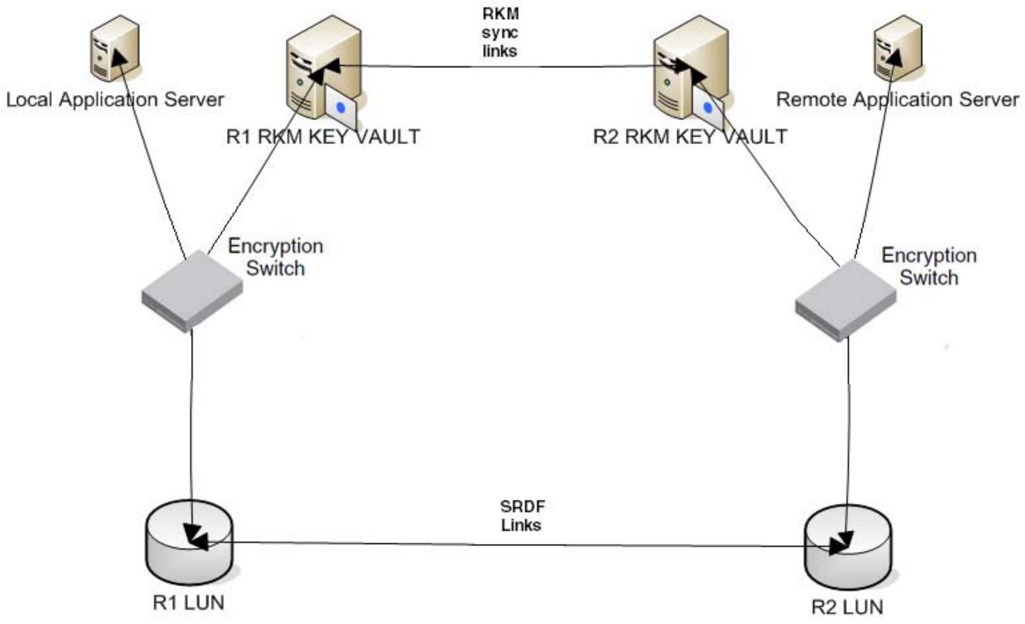


FIGURE 231 Basic SRDF configuration with encryption switches

Metadata requirements and remote replication

When the metadata and key ID are written, the primary metadata on blocks 1–16 is compressed and encrypted. However, there are scenarios whereby these blocks cannot be compressed, and the metadata is not written to the media. If blocks 1–16 are not compressible on the local source device and metadata is not written, obtaining the correct DEK for the remote target device becomes problematic. This problem is avoided by reserving the last three blocks of the LUN for a copy of the metadata. These blocks are not exposed to the host initiator. When a host reads the capacity of the LUN, the size reported is always three blocks less than the actual size. The behavior is enforced by selecting the **New LUN** check box on the **Select LUN** screen of the **Add New Path** wizard when adding LUNs for an SRDF pair (for example, R1 and R2 in Figure 231).

Note the following when using the **New LUN** option:

- Both LUNs that form an SRDF pair must be added to their containers using the **New LUN** option.
- For any site, all paths to a given SRDF device must be configured with the **New LUN** option.
- All LUNs configured with the **New LUN** option will report three blocks less than the actual size when host performs READ CAPACITY 10/READ CAPACITY 16.
- If a LUN is added with the **New LUN** option and with encryption enabled, it will always have valid metadata even if blocks 1–16 of the LUN is not compressible.
- LUNs configured as cleartext must also be added with the **New LUN** option if they are part of an SRDF pair. This is to handle scenarios whereby the LUN policy is changed to encrypted at some later time, and to verify formation of DEK clusters and LUN accessibility prior to enabling encryption for the LUN. When cleartext LUNs are configured with the **New LUN** option, no metadata is written to the last three blocks, but will still report three blocks less than the actual size when host performs READ CAPACITY 10/READ CAPACITY 16.
- The **New LUN** option is used only if an RKM key vault is configured for the encryption group.
- The **New LUN** option can be used only if replication is enabled for the encryption group.
- If the local LUN contains host data, configuring it with the **New LUN** option will cause the data on the last three blocks of the LUN to be lost. Before using the **New LUN** option, you must migrate the contents of the LUN to another LUN that is larger by at least three blocks. The new, larger LUN can then be used when creating the SRDF pair. The remote LUN of the SRDF pair must be of the same size. The original smaller LUN with user data can be decommissioned.

Adding target tape LUNs for encryption

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

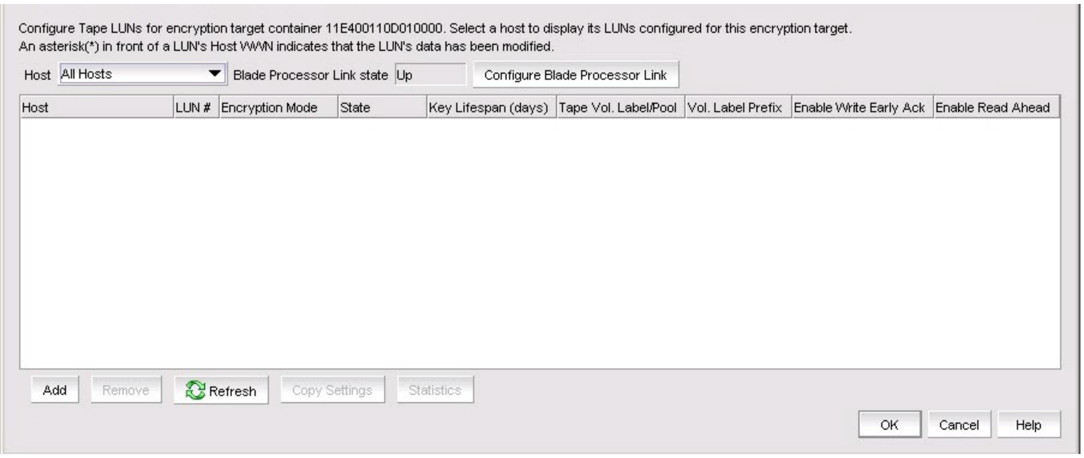
2. Select a group, switch, or engine from the **Encryption Center Devices** table that contains the storage device to be configured, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets**.

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   The **Encryption Targets** dialog box displays (Figure 217).

3. Select a target tape storage device from the **Encryption Targets** table, then click **LUNs**.

   The **Encryption Target Tape LUNs** dialog box displays (Figure 232).



Configure Tape LUNs for encryption target container 11E400110D010000. Select a host to display its LUNs configured for this encryption target.
An asterisk(*) in front of a LUN's Host WWN indicates that the LUN's data has been modified.

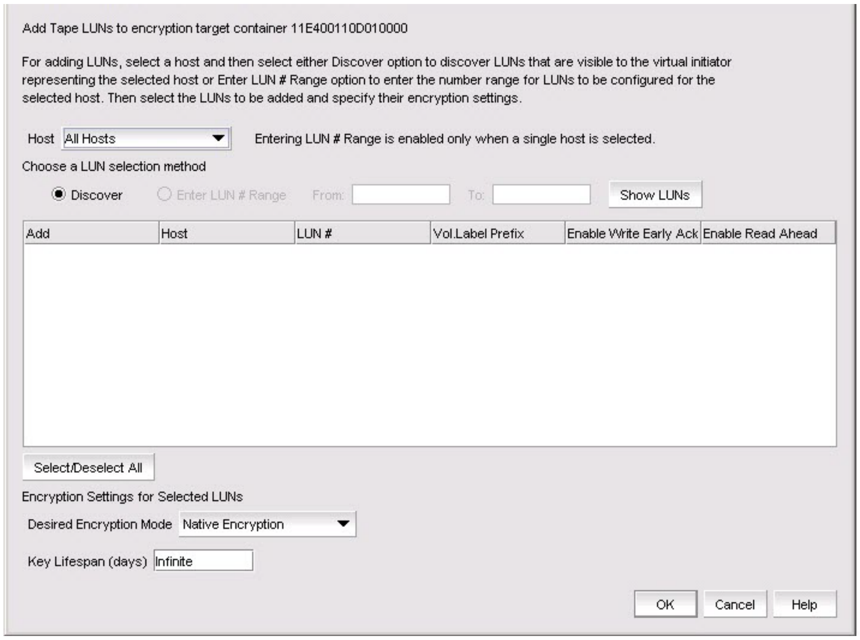
Host: All Hosts
Blade Processor Link state: Up

Host	LUN #	Encryption Mode	State	Key Lifespan (days)	Tape Vol. Label/Pool	Vol. Label Prefix	Enable Write Early Ack	Enable Read Ahead

FIGURE 232 Encryption Target LUNs dialog box

4. Click **Add**.

   The **Add Encryption Target Tape LUNs** dialog box displays (Figure 233).



Add Tape LUNs to encryption target container 11E400110D010000

For adding LUNs, select a host and then select either Discover option to discover LUNs that are visible to the virtual initiator representing the selected host or Enter LUN # Range option to enter the number range for LUNs to be configured for the selected host. Then select the LUNs to be added and specify their encryption settings.

Host: All Hosts

Entering LUN # Range is enabled only when a single host is selected.

Choose a LUN selection method

● Discover ○ Enter LUN # Range From: To:

Add	Host	LUN #	Vol.Label Prefix	Enable Write Early Ack	Enable Read Ahead

Encryption Settings for Selected LUNs

Desired Encryption Mode: Native Encryption

Key Lifespan (days): Infinite

FIGURE 233 Add Encryption Target Tape LUNs dialog box

The dialog box includes a table of all LUNs in the storage device that are visible to hosts. LUNs are identified by the **Host** world wide name, **LUN** number, **Volume Label Prefix** number, and **Enable Write Early ACK** and **Enable Read Ahead** status.

5. Select a host from the **Host** list.

   Before you encrypt a LUN, you must select a host, then either discover LUNs that are visible to the virtual initiator representing the selected host, or enter a range of LUN numbers to be configured for the selected host.

6. Choose a LUN to be added to an encryption target container using one of the two following methods:

   - Discover. Click to identify the exposed logical unit number for a specified initiator. If you already know the exposed LUNs for the various initiators accessing the LUN, you can enter the range of LUNs using the alternative method.
   - Enter a LUN number range. Click **Show LUNs** to add a range of LUNs to be configured for the selected host. The LUN needed for configuring a Crypto LUN is the LUN that is exposed to a particular initiator.

7. Select the desired encryption mode. Options are: **Native Encryption**, **DF-Compatible Encryption**, and **Cleartext**.
   - If you change a LUN policy from **Native Encryption** or **DF-Compatible Encryption** to **Clear Text**, you disable encryption.
   - The LUNs of the target that are not enabled for encryption must still be added to the CryptoTarget container with the **Clear Text** encryption mode option.

NOTE
The Re-keying interval can only be changed for disk LUNs. For tape LUNs, expiration of the re-keying interval simply triggers the generation of a new key to be used on future tape volumes. Tapes that are already made are not re-keyed. To re-key a tape, you need to read the tape contents using a host application that decrypts the tape contents using the old key, then rewrite the tape, which re-encrypts the data with the new key.

8. Click **OK**.

   The selected tape LUNs are added to the encryption target container.

Configuring encrypted tape storage in a multi-path environment

This example assumes one host is accessing one storage device using two paths:

- The first path is from Host Port A to Target Port A, using Encryption Engine A for encryption.
- The second path is from Host Port B to Target Port B, using Encryption Engine B for encryption.

Encryption Engines A and B are in switches that are already part of Encryption Group *X*.

The following procedure is used to configure this scenario using the Management application.

1. Configure Host Port A and Target Port A in the same zone by selecting **Configure > Zoning** from the Management application’s main menu.
2. Configure Host Port B and Target Port B in the same zone by selecting **Configure > Zoning** from the Management application’s main menu.
3. Select **Configure > Encryption** from the menu task bar to open the **Encryption Center** dialog box.
4. Click **View Groups** to display the encryption groups (if groups are not already displayed).
5. Select Encryption Group *X*, then click the **Targets** icon.
6. From the **Encryption Targets** dialog box, click **Add** to open the **Configure Switch Encryption** wizard. Use the wizard to create a target container for Encryption Engine A with Target Port A and Host Port A.
7. Repeat Step 6 to create a target container for Encryption Engine B with Target Port B and Host Port B.

   Up to this point, the Management application has been automatically committing changes as they are made. The targets and hosts are now fully configured; only the LUN configuration remains.

8. In the **Encryption Targets** dialog box, select Target Port A, click **LUNs**, then click **Add**. Select the LUNs to be encrypted and the encryption policies for the LUNs.

9. Select Target Port B, click **LUNs**, then click **Add**. Select the LUNs to be encrypted and the encryption policies for the LUNs, making sure that the encryption policies match the policies specified in the other path.
10. Click **Commit** to make the LUN configuration changes effective in both paths simultaneously.

The Management application does not automatically commit LUN configuration changes. This allows matching changes made in a multi-path environment to be committed together, preventing cases where one path may be encrypting and another path is not encrypting, resulting in corrupted data. You must manually commit any LUN configuration changes, even in non-multi-path environments. The **Encryption Targets** dialog box will display a reminder if you attempt to close the dialog box without committing your changes.

NOTE
There is a limit of 25 uncommitted LUN configuration changes. When adding more than eight LUNs in a multi-path environment, repeat step 8 through step 9 above, adding only eight LUNs to each target container at a time. Each commit operation will commit 16 LUNs, eight in each path.

Tape LUN write early and read ahead

The tape LUN write early and read ahead feature uses tape pipelining and prefetch to speed serial access to tape storage. These features are particularly useful when performing backup and restore operations, especially over long distances.

You can enable tape LUN write early and read ahead while adding the tape LUN for encryption, or you can enable or disable these features after the tape LUN has been added for encryption.

For more information, see the following topics:

“Adding target tape LUNs for encryption” on page 527

“Enabling and disabling tape LUN write early and read ahead” on page 530

Enabling and disabling tape LUN write early and read ahead

To enable or disable tape LUN write early and read ahead, follow these steps:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

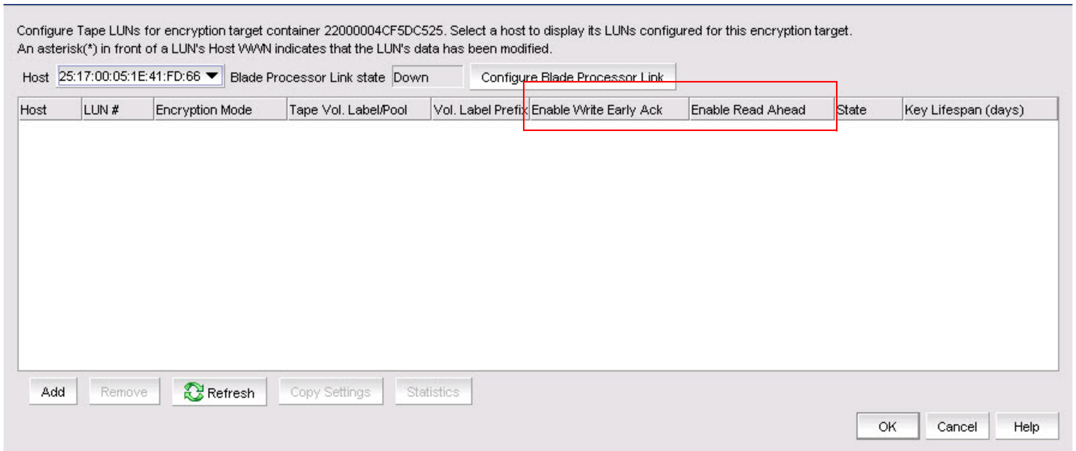
2. Select a group, switch, or engine from the **Encryption Center Devices** table, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click the group, switch, or engine and select **Targets**.

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   The **Encryption Targets** dialog box displays (Figure 217).

3. Select a target tape storage device from the table, then click **LUNs**.

   The **Encryption Target Tape LUNs** dialog box displays (Figure 234).



Configure Tape LUNs for encryption target container 22000004CF5DC525. Select a host to display its LUNs configured for this encryption target.
An asterisk(*) in front of a LUN's Host WWN indicates that the LUN's data has been modified.

Host: 25:17:00:05:1E:41:FD:66 Blade Processor Link state: Down

Host	LUN #	Encryption Mode	Tape Vol. Label/Pool	Vol. Label Prefix	Enable Write Early Ack	Enable Read Ahead	State	Key Lifespan (days)

FIGURE 234 Setting tape LUN pipelining and prefetch in the Encryption Target Tape LUNs dialog box

4. In the **Enable Write EarlyAck** and **Enable Read Ahead** columns, when the table is populated, you can set these features as desired for each LUN:
   - To enable write early for a specific tape LUN, select **Enable Write Early Ack** for that LUN.
   - To enable read ahead for a specific LUN, select **Enable Read Ahead** for that LUN.
   - To disable write early for a specific tape LUN, deselect **Enable Write Early Ack** for that LUN.
   - To disable read ahead for a specific LUN, deselect **Enable Read Ahead** for that LUN.
5. Click **OK.**
6. Commit the changes on the related crypto target container:
   a. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

   b. Select a group, switch, or engine from the **Encryption Center Devices** table that contains the storage device to be configured, then select **Group/Switch/Engine** > **Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets.**

NOTE
You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   c. Select the appropriate crypto target container.

   d. Click **Commit.**

Tape LUN statistics

This feature enables you to view and clear statistics for tape LUNs. These statistics include the number of compressed blocks, uncompressed blocks, compressed bytes and uncompressed bytes written to a tape LUN.

The tape LUN statistics are cumulative and change as the host writes more data on tape. You can clear the statistics to monitor compression ratio of ongoing host I/Os.

The encryption management application allows you to select tape LUN from either a tape LUN container through the **Encryption Targets** dialog box, or from the **Target Tape LUNs** dialog box.

For operational details, see the following topics:

- "Viewing and clearing tape container statistics" on page 532
- "Viewing and clearing tape LUN statistics for specific tape LUNs" on page 533
- "Viewing and clearing statistics for tape LUNs in a container" on page 535

Viewing and clearing tape container statistics

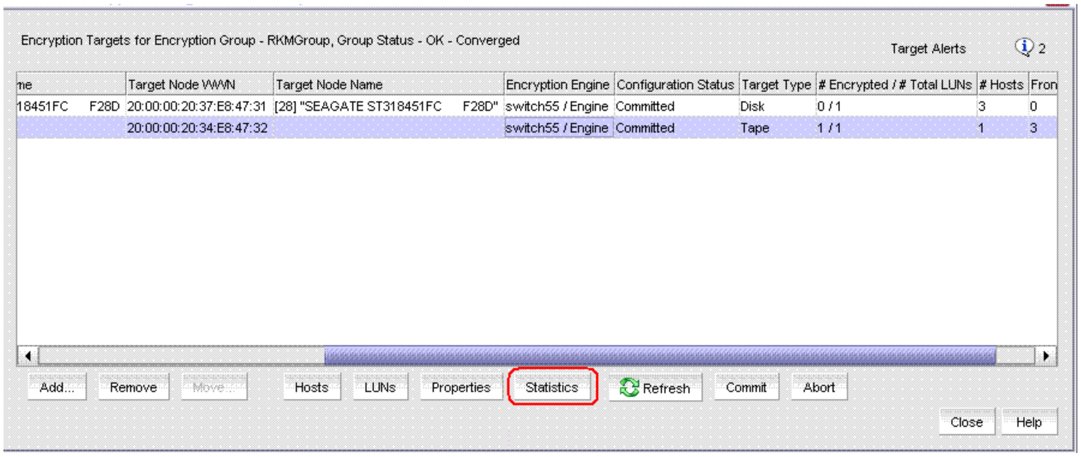
To view or clear statistics for tape LUNs in a container, follow these steps:

1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays.

2. Select a group from the **Encryption Center Devices** table, then select **Group** > **Targets** from the menu task bar, or right-click a group and select **Targets**.

   The **Encryption Targets** dialog box displays (Figure 235). The **Encryption Targets** dialog box lists the configured crypto target containers.



Encryption Targets for Encryption Group - RKMGroup, Group Status - OK - Converged

Target Alerts ⓘ 2

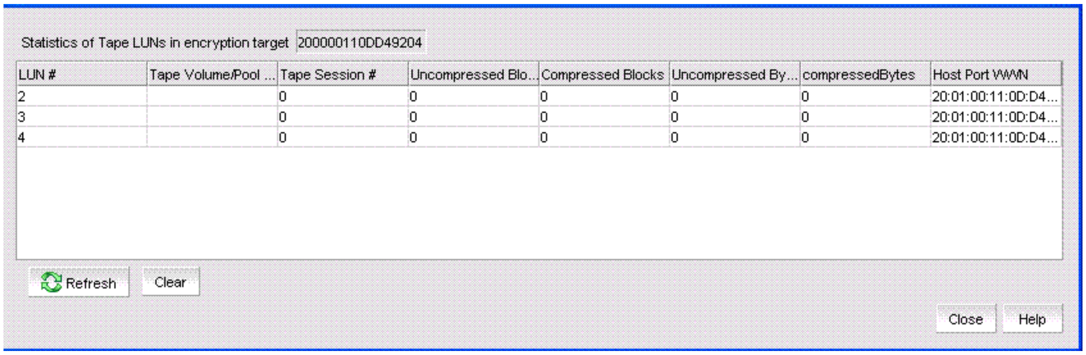
me	Target Node WWN	Target Node Name	Encryption Engine	Configuration Status	Target Type	# Encrypted / # Total LUNs	# Hosts	Fron
18451FC F28D	20:00:00:20:37:E8:47:31	[28] "SEAGATE ST318451FC F28D"	switch55 / Engine	Committed	Disk	0 / 1	3	0
	20:00:00:20:34:E8:47:32		switch55 / Engine	Committed	Tape	1 / 1	1	3

FIGURE 235 Encryption Targets dialog box

3. From the Encryption Targets table, select the container of type "Tape" for which to display or clear statistics.

4. Click **Statistics**.

   The Tape LUN Statistics dialog box displays (Figure 236). The dialog box lists statistics for all LUNs that are members of the selected tape container.



Statistics of Tape LUNs in encryption target 200000110DD49204

LUN #	Tape Volume/Pool ...	Tape Session #	Uncompressed Blo...	Compressed Blocks	Uncompressed By...	compressedBytes	Host Port WWN
2		0	0	0	0	0	20:01:00:11:0D:D4...
3		0	0	0	0	0	20:01:00:11:0D:D4...
4		0	0	0	0	0	20:01:00:11:0D:D4...

FIGURE 236 **Tape LUN Statistics dialog box**

5. To clear the tape LUN statistics for all member LUNs for the container, click **Clear**.
6. When prompted with a confirmation dialog box, click **Yes**.
7. To update the tape LUN statistics, click **Refresh**.

Viewing and clearing tape LUN statistics for specific tape LUNs

To view or clear statistics for tape LUNs in a container, follow these steps:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

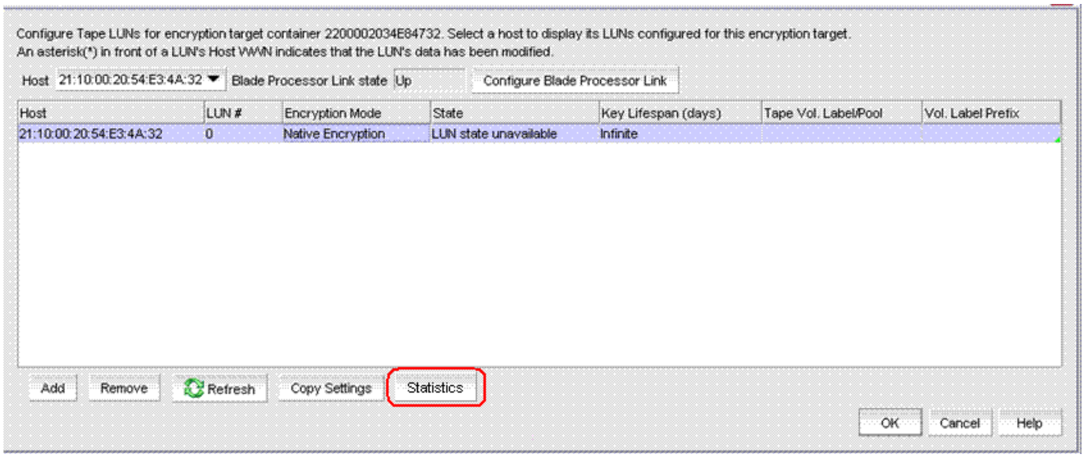
2. Select a group, switch, or engine from the **Encryption Center Devices** table that contains the storage device to be configured, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets**.

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   The **Encryption Targets** dialog box displays (Figure 217).

3. Select a tape target storage device, then click **LUNs**.

   The **Target Tape LUNs** dialog box displays (Figure 237).



Configure Tape LUNs for encryption target container 2200002034E84732. Select a host to display its LUNs configured for this encryption target.
An asterisk(*) in front of a LUN's Host WWN indicates that the LUN's data has been modified.

Host 21:10:00:20:54:E3:4A:32 Blade Processor Link state Up

Host	LUN #	Encryption Mode	State	Key Lifespan (days)	Tape Vol. Label/Pool	Vol. Label Prefix
21:10:00:20:54:E3:4A:32	0	Native Encryption	LUN state unavailable	Infinite		

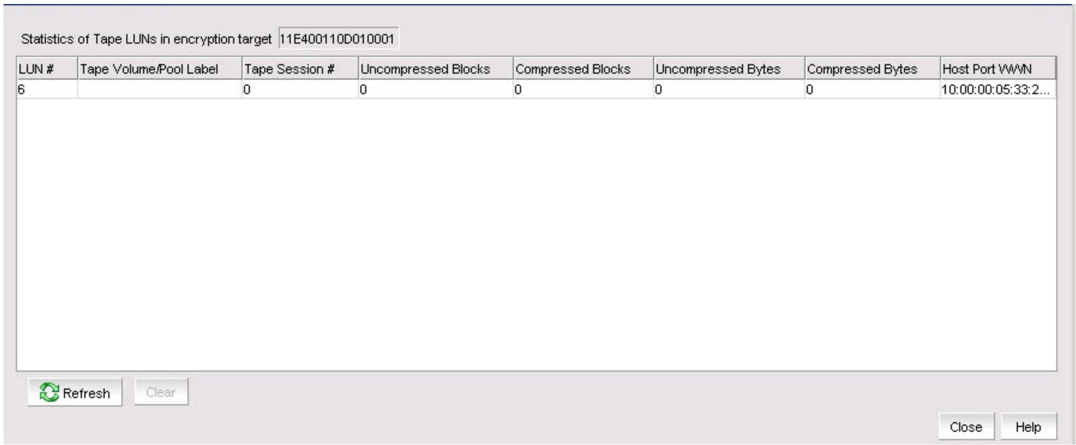
FIGURE 237 Target Tape LUNs dialog box

The dialog box lists configured tape LUNs.

4. Select the LUN or LUNs for which to display or clear statistics.

5. Click **Statistics.**

   The **Tape LUN Statistics** dialog box displays (Figure 238). The dialog box displays the statistic results based on the LUN or LUNs you selected.



Statistics of Tape LUNs in encryption target 11E400110D010001

LUN #	Tape Volume/Pool Label	Tape Session #	Uncompressed Blocks	Compressed Blocks	Uncompressed Bytes	Compressed Bytes	Host Port WWN
6		0	0	0	0	0	10:00:00:05:33:2...

FIGURE 238 Tape LUN Statistics dialog box

6. To clear the tape LUN statistics, click **Clear.**

7. When prompted with a confirmation dialog box, click **Yes.**

8. To update the tape LUN statistics, click **Refresh.**

Viewing and clearing statistics for tape LUNs in a container

To view or clear statistics for tape LUNs in a container, follow these steps:

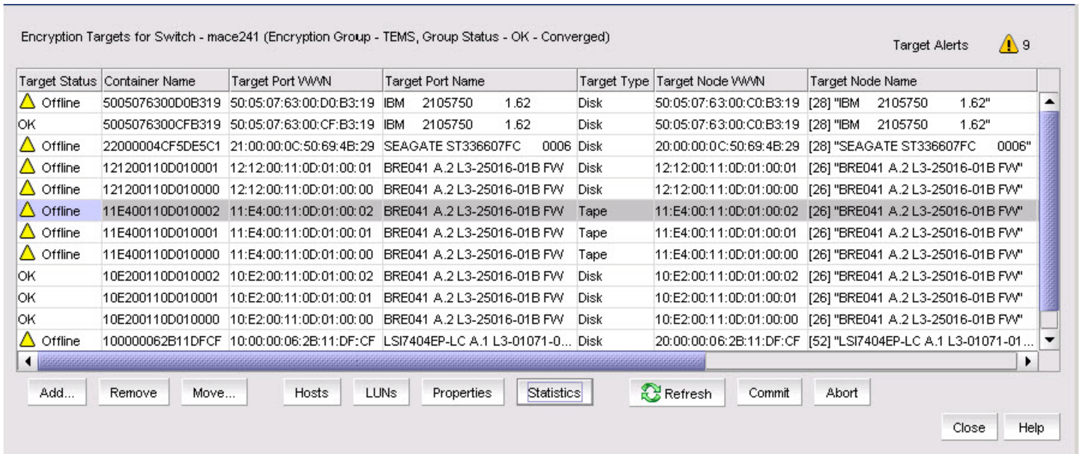
1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group, switch, or engine from the **Encryption Center Devices** table that contains the storage device to be configured, then select **Group/Switch/Engine** > **Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets.**

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   The **Encryption Targets** dialog box displays (Figure 239). The dialog box lists configured crypto target containers.



Encryption Targets for Switch - mace241 (Encryption Group - TEMS, Group Status - OK - Converged)

Target Alerts ⚠ 9

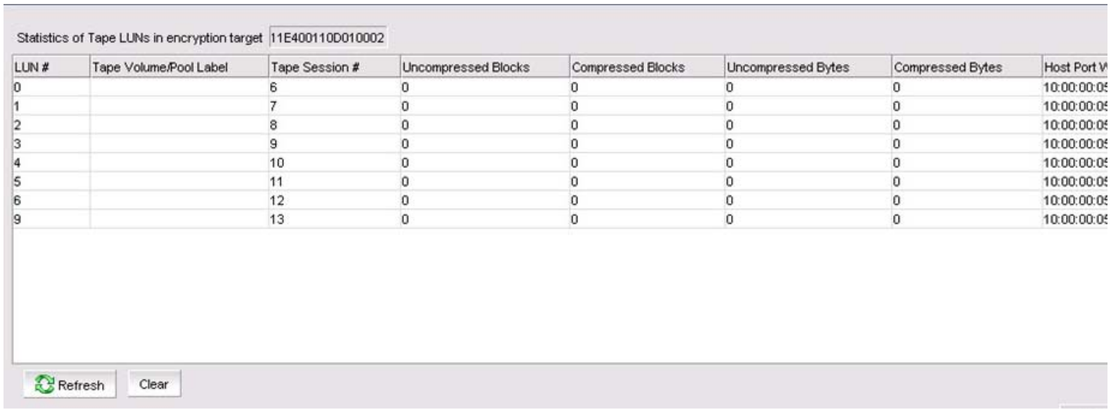
Target Status	Container Name	Target Port WWN	Target Port Name	Target Type	Target Node WWN	Target Node Name
⚠ Offline	5005076300D0B319	50:05:07:63:00:D0:B3:19	IBM 2105750 1.62	Disk	50:05:07:63:00:C0:B3:19	[28] "IBM 2105750 1.62"
OK	5005076300CFB319	50:05:07:63:00:CF:B3:19	IBM 2105750 1.62	Disk	50:05:07:63:00:C0:B3:19	[28] "IBM 2105750 1.62"
⚠ Offline	22000004CF5DE5C1	21:00:00:0C:50:69:4B:29	SEAGATE ST336607FC 0006	Disk	20:00:00:0C:50:69:4B:29	[28] "SEAGATE ST336607FC 0006"
⚠ Offline	121200110D010001	12:12:00:11:0D:01:00:01	BRE041 A.2 L3-25016-01B FW	Disk	12:12:00:11:0D:01:00:01	[26] "BRE041 A.2 L3-25016-01B FW"
⚠ Offline	121200110D010000	12:12:00:11:0D:01:00:00	BRE041 A.2 L3-25016-01B FW	Disk	12:12:00:11:0D:01:00:00	[26] "BRE041 A.2 L3-25016-01B FW"
⚠ Offline	11E400110D010002	11:E4:00:11:0D:01:00:02	BRE041 A.2 L3-25016-01B FW	Tape	11:E4:00:11:0D:01:00:02	[26] "BRE041 A.2 L3-25016-01B FW"
⚠ Offline	11E400110D010001	11:E4:00:11:0D:01:00:01	BRE041 A.2 L3-25016-01B FW	Tape	11:E4:00:11:0D:01:00:01	[26] "BRE041 A.2 L3-25016-01B FW"
⚠ Offline	11E400110D010000	11:E4:00:11:0D:01:00:00	BRE041 A.2 L3-25016-01B FW	Tape	11:E4:00:11:0D:01:00:00	[26] "BRE041 A.2 L3-25016-01B FW"
OK	10E200110D010002	10:E2:00:11:0D:01:00:02	BRE041 A.2 L3-25016-01B FW	Disk	10:E2:00:11:0D:01:00:02	[26] "BRE041 A.2 L3-25016-01B FW"
OK	10E200110D010001	10:E2:00:11:0D:01:00:01	BRE041 A.2 L3-25016-01B FW	Disk	10:E2:00:11:0D:01:00:01	[26] "BRE041 A.2 L3-25016-01B FW"
OK	10E200110D010000	10:E2:00:11:0D:01:00:00	BRE041 A.2 L3-25016-01B FW	Disk	10:E2:00:11:0D:01:00:00	[26] "BRE041 A.2 L3-25016-01B FW"
⚠ Offline	100000062B11DFCF	10:00:00:06:2B:11:DF:CF	LSI7404EP-LC A.1 L3-01071-0...	Disk	20:00:00:06:2B:11:DF:CF	[52] "LSI7404EP-LC A.1 L3-01071-01 ...

FIGURE 239 **Encryption Targets dialog box**

3. Select the container of type **Tape** for which to display or clear statistics.

4. Click **Statistics.**

   The Tape LUN Statistics dialog box displays (Figure 240). The dialog box lists the statistics for all LUNs that are members of the selected tape container.



Statistics of Tape LUNs in encryption target 11E400110D010002

LUN #	Tape Volume/Pool Label	Tape Session #	Uncompressed Blocks	Compressed Blocks	Uncompressed Bytes	Compressed Bytes	Host Port W
0		6	0	0	0	0	10:00:00:05
1		7	0	0	0	0	10:00:00:05
2		8	0	0	0	0	10:00:00:05
3		9	0	0	0	0	10:00:00:05
4		10	0	0	0	0	10:00:00:05
5		11	0	0	0	0	10:00:00:05
6		12	0	0	0	0	10:00:00:05
9		13	0	0	0	0	10:00:00:05

FIGURE 240 Tape LUN Statistics dialog box

5. To clear the tape LUN statistics for member LUNs in the container, click Clear.
6. When prompted with a confirmation dialog box, click Yes.
7. To update the tape LUN statistics, click Refresh.

Re-balancing the encryption engine

If you are currently using encryption and running Fabric OS 6.3.x or earlier, you are hosting tape and disk target containers on different encryption switches or blades. Beginning with Fabric OS 6.4, disk and tape target containers can be hosted on the same switch or blade. Hosting both disk and tape target containers on the same switch or blade might result in a drop in throughput, but it can reduce cost by reducing the number of switches or blades needed to support encrypted I/O in environments that use both disk and tape.

The throughput drop can be mitigated by re-balancing the tape and disk target containers across the encryption engine. This ensures that the tape and disk target containers are distributed within the encryption engine for maximum throughput.

All nodes within an encryption group must be upgraded to Fabric OS 6.4 or later to support hosting disk and tape target containers on the same encryption engine. If any node within an encryption group is running an earlier release, disk and tape containers must continue to be hosted on separate encryption engines.

During re-balancing operations, be aware of the following:

- You might notice a slight disruption in Disk I/O. In some cases, manual intervention may be needed.
- Backup jobs to tapes might need to be restarted after re-balancing is completed.

To determine if re-balancing is recommended for an encryption engine, check the encryption engine properties. Beginning with Fabric OS 6.4, a field is added that indicates whether or not re-balancing is recommended.

You might be prompted to re-balance during the following operations:

- When adding a new disk or tape target container.
- When removing an existing disk or tape target container.

- After failover to a backup encryption engine in an HA cluster.
- After a failed encryption engine in an HA cluster is recovered, and failback processing has occurred.

To re-balance an encryption engine, complete the following steps:

1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).
2. Select an engine, then select **Engine** > **Re-Balance** from the menu task bar, or right click an engine and select **Re-Balance**.

   A warning message displays, noting the potential disruption of disk and tape I/O, and that the operation may take several minutes.
3. Click **Yes** to begin re-balancing.

Master keys

When an opaque key vault is used, a master key is used to encrypt the data encryption keys. The master key status indicates whether a master key is used and whether it has been backed up. Encryption is not allowed until the master key has been backed up.

Only the active master key can be backed up, and multiple backups are recommended. You can back up or restore the master key to the key vault, to a file, or to a recovery card set. A recovery card set is set of smart cards. Each recovery card holds a portion of the master key. The cards must be gathered and read together from a card reader attached to a PC running the Management application to restore the master key.

NOTE
It is very important to back up the master key because if the master key is lost, none of the data encryption keys can be restored and none of the encrypted data can be decrypted.

For more information, see the following topics:

"Active master key" on page 537

"Alternate master key" on page 538

"Master key actions" on page 538

"Reasons master keys can be disabled" on page 538

Active master key

The active master key is used to encrypt newly created data encryption keys (DEKs) prior to sending them to a key vault to be stored. You can restore the active master key under the following conditions:

- The active master key has been lost, which happens if all encryption engines in the group have been zeroized or replaced with new hardware at the same time.
- You want multiple encryption groups to share the same active master key. Groups should share the same master key if the groups share the same key vault and if tapes (or disks) are going to be exchanged regularly between the groups.

Alternate master key

The alternate master key is used to decrypt data encryption keys that were not encrypted with the active master key. Restore the alternate master key for the following reasons:

- To read an old tape that was created when the group used a different active master key.
- To read a tape (or disk) from a different encryption group that uses a different active master key.

Master key actions

Master key actions are as follows:

- **Backup master key**, which is enabled any time a master key exists.

  You can back up the master key to a file, to a key vault, or to a smart card. You can back up the master key multiple times to any of these media in case you forget the passphrase you originally used to back up the master key, or if multiple administrators each needs a passphrase for recovery.
- **Restore master key**, which is enabled when no master key exists or the previous master key has been backed up.
- **Create new master key**, which is enabled when no master key exists or the previous master key has been backed up.

Reasons master keys can be disabled

Master key actions are disabled if unavailable. There are several ways a master key can be disabled:

- The user does not have Storage Encryption Security permissions. For more information, see "Encryption user privileges" on page 435.
- The group leader is not discovered or managed by the Management application.

Saving the master key to a file

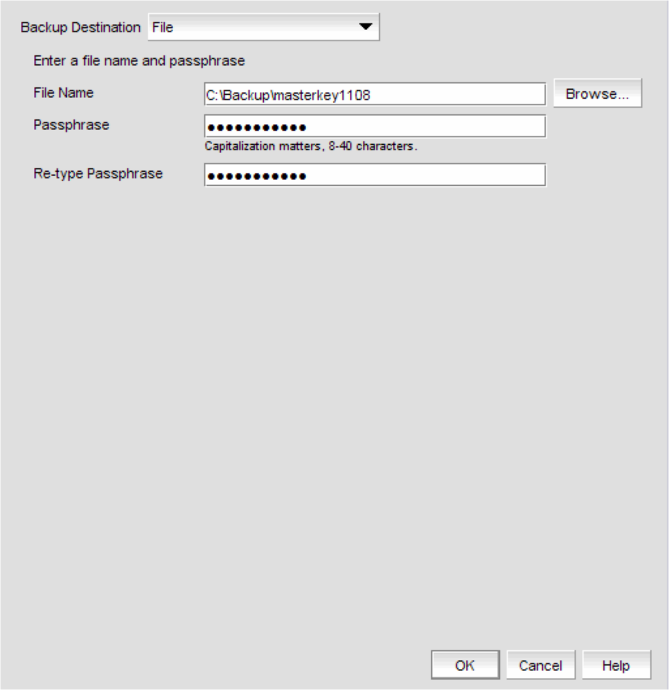
Use the following procedure to save the master key to a file.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).
2. Select a group from the **Encryption Center Devices** table, then select **Group > Properties** from the menu task bar.

   NOTE
   Master keys belong to the group and are managed from group properties.
3. Select the **Security** tab.
4. Select **Backup Master Key** as the **Master Key Action**.

   The **Master Key Backup** dialog box displays (Figure 241), but only if the master key has already been generated.



Backup Destination File

Enter a file name and passphrase

File Name C:\Backup\masterkey1108

Passphrase ●●●●●●●●●●●

Capitalization matters, 8-40 characters.

Re-type Passphrase ●●●●●●●●●●●

FIGURE 241 **Backup Destination (to file) dialog box**

5. Select **File** as the **Backup Destination.**
6. Enter a file name, or browse to the desired location.
7. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
8. Re-enter the passphrase for verification.
9. Click **OK.**

ATTENTION

Save the passphrase. This passphrase is required if you ever need to restore the master key from the file.

Saving a master key to a key vault

Use the following procedure to save the master key to a key vault.

1. Select **Configure** > **Encryption** from the menu task bar.

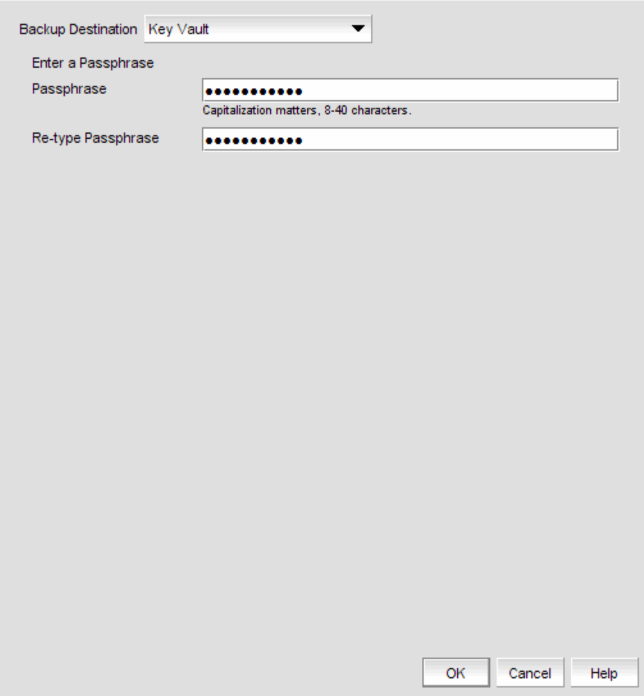
   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group from the **Encryption Center Devices** table, then select **Group** > **Properties** from the menu task bar.

   The **Encryption Properties** dialog box displays.

3. Select the **Security** tab.
4. Select **Backup Master Key** as the **Master Key Action.**

   The **Backup Master Key for Encryption Group** dialog box displays (Figure 242).



Backup Destination: Key Vault

Enter a Passphrase

Passphrase: ●●●●●●●●●●●

Capitalization matters, 8-40 characters.

Re-type Passphrase: ●●●●●●●●●●●

FIGURE 242 Backup Destination (to key vault) dialog box

5. Select **Key Vault** as the **Backup Destination**.
6. Enter the passphrase, which is required for restoring the master key. The passphrase can be between eight and 40 characters, and any character is allowed.
7. Re-type the passphrase for verification.
8. Click **OK**.

   A dialog box displays that shows the **Key ID**. The Key ID identifies the storage location in the key vault.
9. Store both the Key ID and the passphrase in a secure place. Both will be required to restore the master key in the future.
10. Click **OK**.

Saving a master key to a smart card set

A card reader must be attached to the SAN Management application PC to complete this procedure. Recovery cards can only be written once to back up a single master key. Each master key backup operation requires a new set of previously unused smart cards.

NOTE
Windows operating systems do not require smart card drivers to be installed separately; the driver is bundled with the operating system. However, you must install a smart card driver for Unix operating systems. For instructions, refer to the *Installation Guide*.

The key is divided between the cards in the card set. When the master key is backed up to a set of three cards, a minimum of two cards can be used together to restore the master key. When the master key is backed up to a set of five cards, a minimum of three cards can be used together to restore the master key. Backing up the master key to multiple recovery cards is the recommended and most secure option.

NOTE
When you write the key to the card set, be sure you write the full set without canceling. If you cancel, all the previously written cards become unusable, and you will need to discard them and create a new set.

1. Select **Configure** > **Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

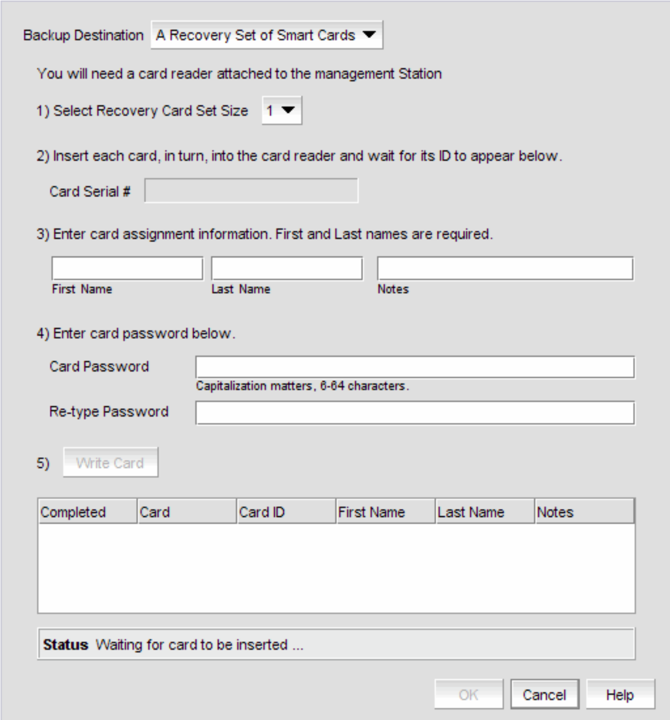
2. Select a group from the **Encryption Center Devices** table, then select **Group** >**Properties**, or right-click a group and select **Properties.**

   The **Encryption Center Properties** dialog box displays.

3. Select the **Security** tab.

4. Select **Backup Master Key** as the **Master Key Action**.

   The **Backup Master Key for Encryption Group** dialog box displays (Figure 243).



Backup Destination: A Recovery Set of Smart Cards

You will need a card reader attached to the management Station

1) Select Recovery Card Set Size: 1

2) Insert each card, in turn, into the card reader and wait for its ID to appear below.

3) Enter card assignment information. First and Last names are required.

4) Enter card password below.

Capitalization matters, 6-64 characters.

Completed	Card	Card ID	First Name	Last Name	Notes

Status Waiting for card to be inserted ...

FIGURE 243 Backup Destination (to smart cards) dialog box

5. Select **A Recovery Set of Smart Cards** as the **Backup Destination.**
6. Enter the recovery card set size.
7. Insert the first blank card and wait for the card serial number to appear.
8. Run the additional cards through the reader that are needed for the set. As you read each card, the card ID displays in the **Card Serial#** field. Be sure to wait for the ID to appear.
9. Enter the mandatory last name and first name of the person to whom the card is assigned.
10. Enter a Card **Password.**
11. Re-enter the password for verification.
12. Record and store the password in a secure location.
13. Click **Write Card.**

    The dialog box prompts you to insert the next card, up to the number of cards specified in step 6.
14. Repeat step 7 through step 13 for each card.
15. Continue until you have written to all cards in the set.
16. After the last card is written, click **OK** in the **Master Key Backup** dialog box to finish the operation.

Restoring a master key from a file

Use the following procedure to restore the master key from a file.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

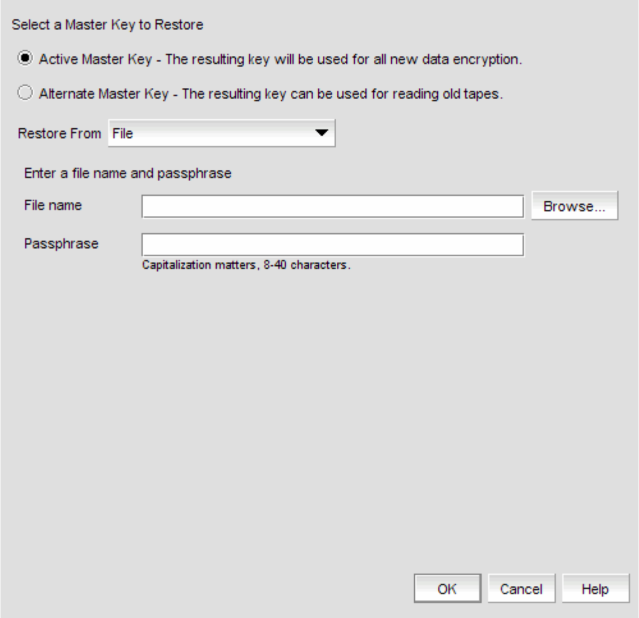
2. Select a group from the **Encryption Center Devices** table, then select **Group > Properties**, or right-click a group and select **Properties**.

   The **Encryption Center Properties** dialog box displays.

3. Select the **Security** tab.

4. Select **Restore Master Key** as the **Master Key Action**.

   The **Restore Master Key for Encryption Group** dialog box displays (Figure 244).



Select a Master Key to Restore

● Active Master Key - The resulting key will be used for all new data encryption.

○ Alternate Master Key - The resulting key can be used for reading old tapes.

Restore From: File

Enter a file name and passphrase

File name:

Passphrase:

Capitalization matters, 8-40 characters.

FIGURE 244 Select a Master Key to Restore (from file) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to "Active master key" on page 537 and "Alternate master key" on page 538 if you need more information on active and alternate master keys.

6. Select **File** as the **Restore From** location.

7. Enter a file name, or browse to the desired location.

8. Enter the passphrase. The passphrase that was used to back up the master key must be used to restore the master key.

9. Click **OK**.

Restoring a master key from a key vault

Use the following procedure to restore the master key from a key vault:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

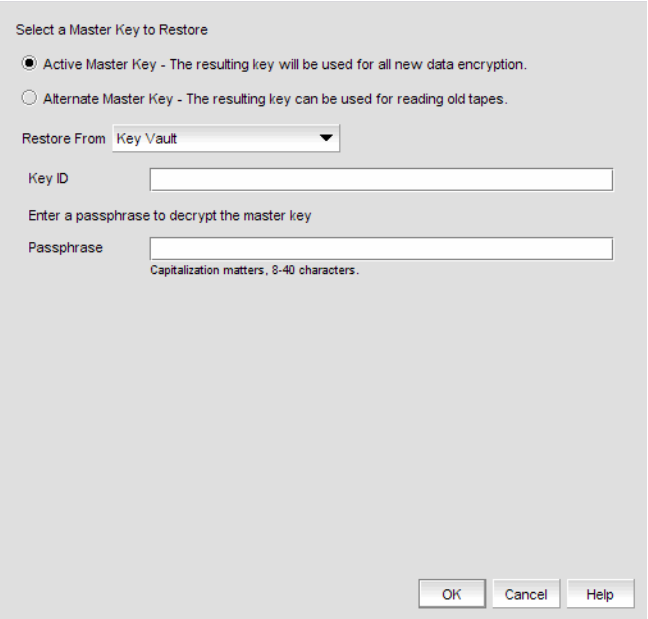
2. Select a group from the **Encryption Center Devices** table, then select **Group > Properties** from the menu task bar, or right-click a group and select **Properties.**

   The **Encryption Center Properties** dialog box displays.

3. Select the **Security** tab.

4. Select **Restore Master Key** as the **Master Key Action.**

   The **Restore Master Key for Encryption Group** dialog box displays (Figure 245).



Select a Master Key to Restore

● Active Master Key - The resulting key will be used for all new data encryption.

○ Alternate Master Key - The resulting key can be used for reading old tapes.

Restore From: Key Vault

Key ID:

Enter a passphrase to decrypt the master key

Passphrase:

Capitalization matters, 8-40 characters.

FIGURE 245 Select a Master Key to Restore (from key vault) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to "Active master key" on page 537 and "Alternate master key" on page 538 if you need more information on active and alternate master keys.

6. Select **Key Vault** as the **Restore From** location.

7. Enter the key ID of the master key that was backed up to the key vault.

8. Enter the passphrase. The passphrase that was used to back up the master key must be used to restore the master key.

9. Click **OK.**

Restoring a master key from a smart card set

A card reader must be attached to the SAN Management application PC to complete this procedure.

Use the following procedure to restore the master key from a set of smart cards.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

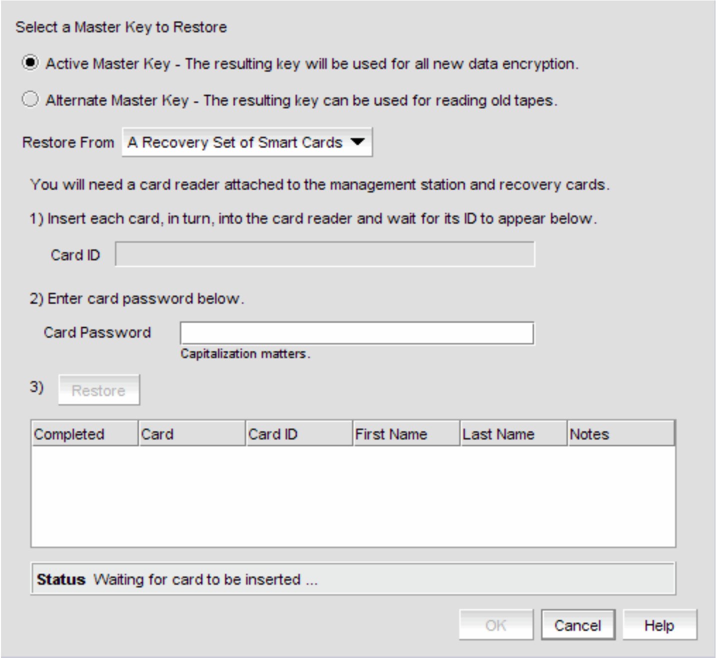
2. Select a group from the **Encryption Center Devices** table, then select **Group > Properties** from the menu task bar, or right-click a group and select **Properties.**

   The **Encryption Center Properties** dialog box displays.

3. Select the **Security** tab.

4. Select **Restore Master Key** as the **Master Key Action.**

   The **Restore Master Key for Encryption Group** dialog box displays (Figure 246).



Select a Master Key to Restore

● Active Master Key - The resulting key will be used for all new data encryption.

○ Alternate Master Key - The resulting key can be used for reading old tapes.

Restore From: A Recovery Set of Smart Cards

You will need a card reader attached to the management station and recovery cards.

1) Insert each card, in turn, into the card reader and wait for its ID to appear below.

Card ID

2) Enter card password below.

Card Password

Capitalization matters.

3) Restore

Completed	Card	Card ID	First Name	Last Name	Notes

Status Waiting for card to be inserted ...

FIGURE 246 Select a Master Key to Restore (from a recovery set of smart cards) dialog box

5. Choose the active or alternate master key for restoration, as appropriate. Refer to "Active master key" on page 537 and "Alternate master key" on page 538 if you need more information on active and alternate master keys.

6. Select **A Recovery Set of Smart Cards** as the **Restore From** location.

7. Insert the recovery card containing a share of the master key that was backed up earlier, and wait for the card serial number to appear.

8. Enter the password that was used to create the card. After five unsuccessful attempts to enter the correct password, the card becomes locked and unusable.

9. Click **Restore.**

   The dialog box prompts you to insert the next card, if needed.

10. Repeat step 7 through step 9 until all cards in the set have been read.
11. Click **OK.**

Creating a new master key

Although it is generally not necessary to create a new master key, you might be required to create one due to the following:

- The previous master key has been compromised.
- Corporate policy might require a new master key every year for security purposes.

When you create a new master key, the former active master key automatically becomes the alternate master key.

The new master key cannot be used (no new data encryption keys can be created, so no new encrypted LUNs can be configured), until you back up the new master key. After you have backed up the new master key, it is strongly recommended that all encrypted disk LUNs be re-keyed. Re-keying causes a new data encryption key to be created and encrypted using the new active master key, thereby removing any dependency on the old master key.

1. Select **Configure > Encryption** from the menu task bar.

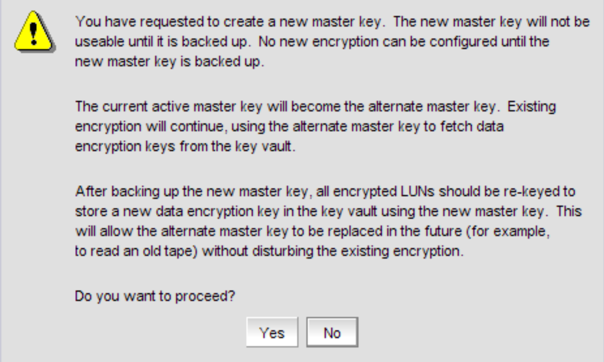
   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group from the **Encryption Center Devices** table, then select **Group > Properties** from the menu task bar, or right-click a group and select **Properties.**

   The **Encryption Center Properties** dialog box displays.

3. Select the **Security** tab.
4. Select **Create a New Master Key** from the list.

   The **Confirm Master Key Creation** dialog box displays (Figure 247).



You have requested to create a new master key. The new master key will not be useable until it is backed up. No new encryption can be configured until the new master key is backed up.

The current active master key will become the alternate master key. Existing encryption will continue, using the alternate master key to fetch data encryption keys from the key vault.

After backing up the new master key, all encrypted LUNs should be re-keyed to store a new data encryption key in the key vault using the new master key. This will allow the alternate master key to be replaced in the future (for example, to read an old tape) without disturbing the existing encryption.

Do you want to proceed?

FIGURE 247 Confirm master key creation dialog box

5. Read the information, then click **Yes** to proceed.

Viewing Master Key IDs

When the master key has been backed up multiple times, you can use this feature to view the associated key IDs.

To view master key IDs, follow these steps:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group from the **Encryption Center Devices** table, then select **Group > Properties** from the menu task bar, or right-click a group and select **Properties.**

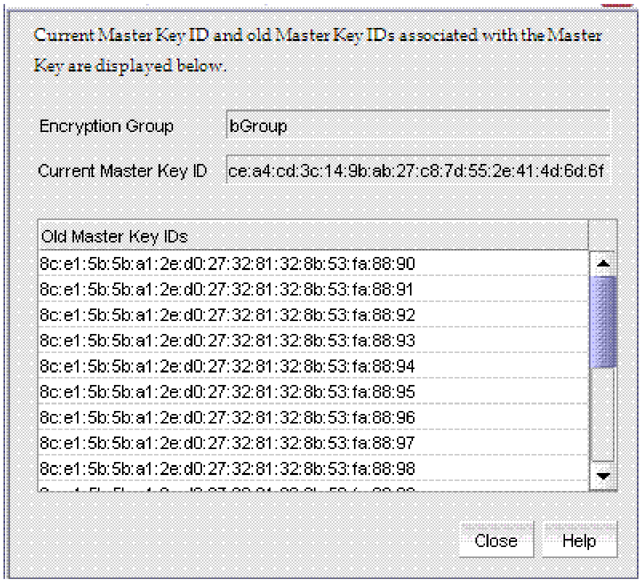
   NOTE
   You can also select a switch from the **Encryption Center Devices** table, then click the **Properties** icon.

   The **Properties** dialog box displays.

3. Select the **Security** tab.

4. From the **Master Key Action list,** select **Master Key IDs.**

   The **Master Key IDs** dialog box displays Figure 248).



Current Master Key ID and old Master Key IDs associated with the Master Key are displayed below.

Encryption Group: bGroup

Current Master Key ID: ce:a4:cd:3c:14:9b:ab:27:c8:7d:55:2e:41:4d:6d:6f

Old Master Key IDs
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:90
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:91
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:92
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:93
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:94
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:95
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:96
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:97
8c:e1:5b:5b:a1:2e:d0:27:32:81:32:8b:53:fa:88:98

FIGURE 248 Master Key IDs dialog box

Zeroizing an encryption engine

Zeroizing is the process of erasing all data encryption keys and other sensitive encryption information in an encryption engine. You can zeroize an encryption engine manually to protect encryption keys. No data is lost because the data encryption keys for the encryption targets are stored in the key vault.

Zeroizing has the following effects:

- All copies of data encryption keys kept in the encryption switch or blade are erased.
- Internal public and private key pairs that identify the encryption engine are erased and the encryption switch or blade is in the FAULTY state.
- All encryption operations on this engine are stopped and all virtual initiators (VI) and virtual targets (VT) are removed from the fabric's name service.
- The key vault link key (for NetApp LKM key vaults) or the master key (for other key vaults) is erased from the encryption engine.

  Once enabled, the encryption engine is able to restore the necessary data encryption keys from the key vault when the link key (for the NetApp Lifetime Key Management application) or the master key (for other key vaults) is restored.
- If the encryption engine was part of an HA cluster, targets fail over to the peer, which assumes the encryption of all storage targets. Data flow will continue to be encrypted.
- If there is no HA backup, host traffic to the target will fail as if the target has gone offline. The host will not have unencrypted access to the target. There will be no data flow at all because the encryption virtual targets will be offline.

NOTE
Zeroizing an engine affects the I/Os, but all target and LUN configuration remain intact. Encryption target configuration data is not deleted.

You can zeroize an encryption engine only if it is enabled (running), or disabled but ready to be enabled. If the encryption engine is not in one of these states, an error message results.

When using a NetApp LKM key vault, if all encryption engines in a switch are zeroized, the switch loses the link key required to communicate with the LKM vault. After the encryption engines are rebooted and re-enabled, you must use the CLI to create new link keys for the switch.

When using an opaque key vault, if all encryption engines in an encryption group are zeroized, the encryption group loses the master key required to read data encryption keys from the key vault. After the encryption engines are rebooted and re-enabled, you must restore the master key from a backup copy, or alternatively, you can generate a new master key and back it up. Restoring the master key from a backup copy or generating a new master key and backing it up indicates that all previously generated DEKs will not be decryptable unless the original master key used to encrypt them is restored.

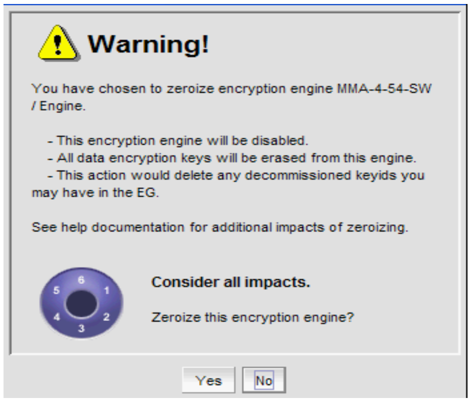
Use the **Restore Master key** wizard from the **Encryption Group Properties** dialog box to restore the master key from a backup copy.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select an encryption engine from the **Encryption Center Devices** table, then select **Engine > Zeroize** from the menu task bar, or right-click the encryption engine and select **Zeroize**.

   A confirmation dialog box describes consequences and actions required to recover.



Warning!

You have chosen to zeroize encryption engine MMA-4-54-SW / Engine.

- This encryption engine will be disabled.
- All data encryption keys will be erased from this engine.
- This action would delete any decommissioned keyids you may have in the EG.

See help documentation for additional impacts of zeroizing.

Consider all impacts.

Zeroize this encryption engine?

3. Click **Yes** to zeroize the encryption engine.

   - For an encryption blade, after the zeroize operation is successful, a message displays noting that the encryption blade will be powered off and powered on to make it operational again. Click **OK** to close the message. After the encryption blade is powered on, click **Refresh** in the **Encryption Center** dialog box to update the status of the encryption blade and perform any operations.
   - For an encryption switch, after the zeroization operation is successful, a message instructs you to reboot the encryption switch. Click **OK** to close the message. Reboot the encryption switch. After the encryption switch is rebooted, click **Refresh** in the **Encryption Center** dialog box to update the status of the encryption switch and perform any operations.

Using the Encryption Targets dialog box

The **Encryption Targets** dialog box enables you to send outbound data that you want to store as ciphertext to an encryption device. The encryption target acts as a virtual target when receiving data from a host, and as a virtual initiator when writing the encrypted data to storage.

To access the Encryption Targets dialog box, complete the following steps.

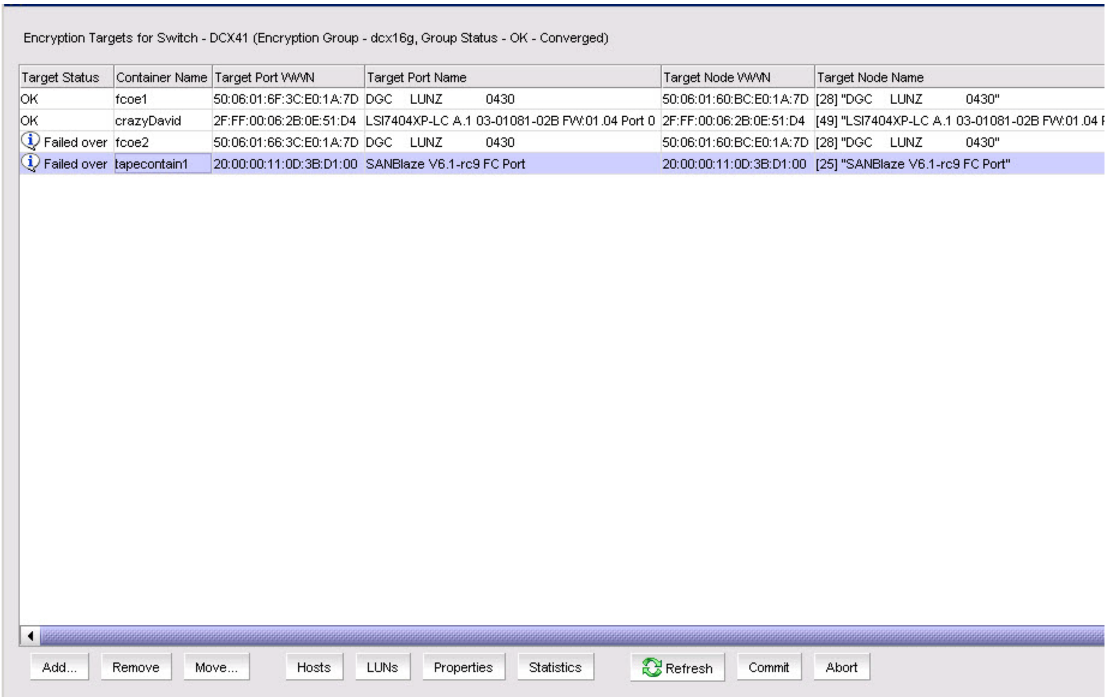
1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153). The dialog box shows the status of all encryption-related hardware and functions.

2. Select a group, switch, or engine from the **Encryption Center Devices** table, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets**.

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

The **Encryption Targets** dialog box displays (Figure 249). The dialog box lists the targets currently being encrypted by the selected group, switch, or encryption engine. If a group is selected, all configured targets in the group are displayed. If a switch is selected, all configured targets for the switch are displayed.



Encryption Targets for Switch - DCX41 (Encryption Group - dcx16g, Group Status - OK - Converged)

Target Status	Container Name	Target Port WWN	Target Port Name	Target Node WWN	Target Node Name
OK	fcoe1	50:06:01:6F:3C:E0:1A:7D	DGC LUNZ 0430	50:06:01:60:BC:E0:1A:7D	[28] "DGC LUNZ 0430"
OK	crazyDavid	2F:FF:00:06:2B:0E:51:D4	LSI7404XP-LC A.1 03-01081-02B FW:01.04 Port 0	2F:FF:00:06:2B:0E:51:D4	[49] "LSI7404XP-LC A.1 03-01081-02B FW:01.04
Failed over	fcoe2	50:06:01:66:3C:E0:1A:7D	DGC LUNZ 0430	50:06:01:60:BC:E0:1A:7D	[28] "DGC LUNZ 0430"
Failed over	tapecontain1	20:00:00:11:0D:3B:D1:00	SANBlaze V6.1-rc9 FC Port	20:00:00:11:0D:3B:D1:00	[25] "SANBlaze V6.1-rc9 FC Port"

FIGURE 249 Encryption Targets dialog box

The **Encryption Targets** dialog box enables you to launch a variety of wizards and other related dialog boxes.

Redirection zones

It is recommended that you configure the host and target in the same zone *before* you configure them for encryption. Doing so creates a redirection zone to redirect the host/target traffic through the encryption engine; however, a redirection zone can only be created if the host and target are in the same zone. If the host and target are not already configured in the same zone, you can configure them for encryption, but you will still need to configure them in the same zone, which will then enable you to create the redirection zone as a separate step.

NOTE
If the encryption group is busy when you click **Commit**, you are given the option to either force the commit, or abort the changes. Click **Commit** to re-create the redirection zone.

Disk device decommissioning

A disk device needs to be decommissioned when any of the following occurs:

- The storage lease expires for an array, and devices must be returned or exchanged.
- Storage is reprovisioned for movement between departments.
- An array or device is removed from service.

In all cases, all data on the disk media must be rendered inaccessible. Device decommissioning deletes all information that could be used to recover the data.

When a device decommission operation fails on the encryption group leader for any reason, the crypto configuration remains uncommitted until a user-initiated commit or a subsequent device decommission operation issued on the encryption group leader completes successfully. Device decommission operations should always be issued from a committed configuration. If not, the operation will fail with the error message **An outstanding transaction is pending in Switch/EG**. If this occurs, you can resolve the problems by committing the configuration from the encryption group leader.

Provided that the crypto configuration is not left uncommitted because of any crypto configuration changes or a failed device decommission operation issued on a encryption group leader node, this error message will not be seen for any device decommission operation issued serially on an encryption group member node. If more than one device decommission operation is tried in an encryption group from member nodes simultaneously, then this error message is transient and will go away after device decommission operation is complete. If the device decommissioning operation fails, retry the operation after some time has passed.

For more information, see "Decommissioning LUNs" on page 551.

Decommissioning LUNs

Use the following procedure to decommission a LUN.

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group, switch, or engine from the **Encryption Center Devices** table that contains the storage device to be configured, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets**.

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   The **Encryption Targets** dialog box displays.

3. Select a Target storage device from the list, then click **LUNs**.

   The **Encryption Target LUNs** dialog box displays.

4. Select the LUNs associated with the device, then click **Decommission**.

   A warning message displays.

5. Click **Yes** to proceed with decommissioning.

   If a re-key operation is currently in progress on a selected LUN, a message is displayed that gives you a choice of doing a **Forced Decommission**, or to **Cancel** and try later after the re-key operation is complete.

6. To check on the progress of the decommissioning operation, click **Refresh**. When decommissioning is complete, the LUNs are removed from the **Encryption Target LUNs** table.

Displaying and deleting decommissioned key IDs

When disk LUNs are decommissioned, the process includes the disabling of the key record in the key vault and indication that the key has been decommissioned. These decommissioned keys are still stored on the switch. You can display, copy, and delete them as an additional security measure.

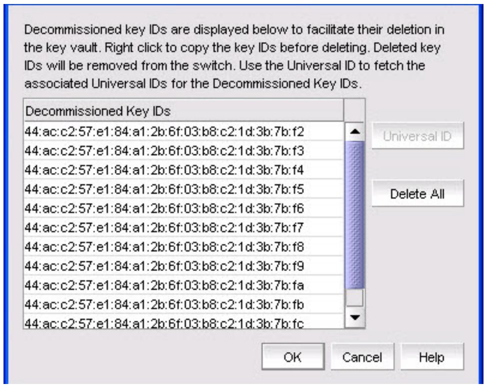
For RKM key vaults, you need to know the Universal ID (UUID) to delete keys from the key vault. To display vendor-specific UUIDs of decommissioned key IDs for RKM key vaults, complete the following steps:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a switch from the **Encryption Center Devices table**, then select **Switch > Decommissioned key IDs** from the menu task bar, or right-click a switch and select **Decommissioned key IDs.**

   The **Decommissioned Key IDs** dialog box displays (Figure 250).



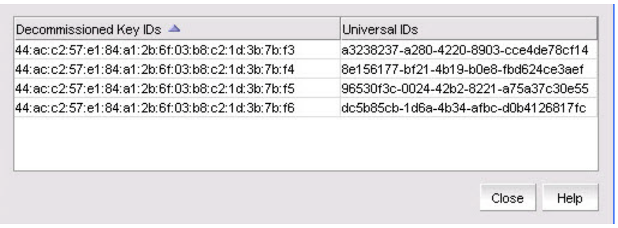
Decommissioned key IDs are displayed below to facilitate their deletion in the key vault. Right click to copy the key IDs before deleting. Deleted key IDs will be removed from the switch. Use the Universal ID to fetch the associated Universal IDs for the Decommissioned Key IDs.

Decommissioned Key IDs
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f2
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f3
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f4
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f5
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f6
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f7
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f8
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f9
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:fa
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:fb
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:fc

FIGURE 250 Decommissioned Key IDs dialog box

3. Click **Delete All** to delete the decommissioned keys from the switch. As a precaution, you might want to copy the keys to a secure location before deleting them from the switch. To export the keys, right-click and select **Export,** which will export the key IDs.

   NOTE
   For RKM key vaults, you need to know the Universal ID (UUID) associated with the decommissioned LUN key IDs to delete keys from the key vault. You can display vendor-specific UUIDs of decommissioned key IDs for RKM key vaults. Select the desired decommissioned key IDs from the Network Advisor Decommissioned Key IDs table, then click **Universal ID**. The Universal IDs dialog box displays (Figure 251).



Decommissioned Key IDs ▲	Universal IDs
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f3	a3238237-a280-4220-8903-cce4de78cf14
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f4	8e156177-bf21-4b19-b0e8-fbd624ce3aef
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f5	96530f3c-0024-42b2-8221-a75a37c30e55
44:ac:c2:57:e1:84:a1:2b:6f:03:b8:c2:1d:3b:7b:f6	dc5b85cb-1d6a-4b34-afbc-d0b4126817fc

FIGURE 251 Universal IDs dialog box

Re-keying all disk LUNs manually

The encryption management application allows you to perform a manual re-key operation on all encrypted primary disk LUNs and all non-replicated disk LUNs hosted on the encryption node that are in the read-write state.

Manual re-keying of all LUNs might take an extended period of time. The management application allows manual re-key of no more than 10 LUNs concurrently. If the node has more than 10 LUNs, additional LUN re-key operations will remain in the pending state until others have finished.

The following conditions must be satisfied for the manual re-key operation to run successfully:

- The node on which you perform the manual re-key operation must be a member of an encryption group, and that encryption group must have a key vault configured.
- The node must be running Fabric OS 7.0.0 or later.
- The encryption group must be in the converged state.
- The target container that hosts the LUN must be online.

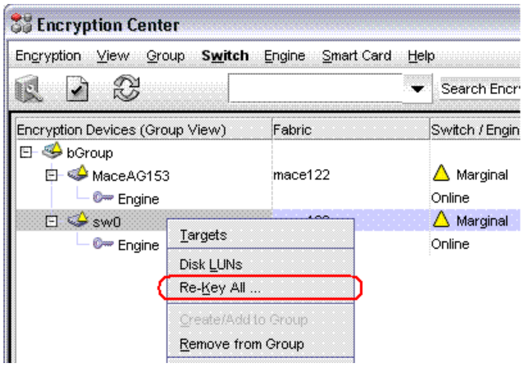
In addition to providing the ability to launch manual re-key operations, the management application also enables you to monitor their progress.

To re-key all disk LUNs on an encryption node, follow these steps:

1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select the switch on which to perform a manual re-key from the **Encryption Center Devices** table, then select **Switch > Re-Key All** from the menu task bar, or right-click the switch and select **Re-Key All** (Figure 252).



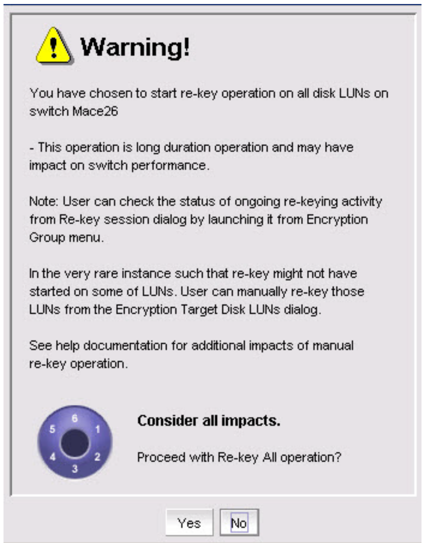
Encryption Devices (Group View)	Fabric	Switch / Engin
bGroup		
MaceAG153	mace122	Marginal
Engine		Online
sw0		Marginal
Engine		Online

FIGURE 252 Selecting the Re-Key All operation

If REPL support is enabled on the encryption group, a confirmation dialog box displays, asking whether to also re-key mirror LUNs.

3. Click **Yes** to includes mirror LUNs. Click **No** to exclude mirror LUNs.

   A critical warning message appears, requesting confirmation to proceed with the re-key operation (Figure 253).



Warning!

You have chosen to start re-key operation on all disk LUNs on switch Mace26

- This operation is long duration operation and may have impact on switch performance.

Note: User can check the status of ongoing re-keying activity from Re-key session dialog by launching it from Encryption Group menu.

In the very rare instance such that re-key might not have started on some of LUNs. User can manually re-key those LUNs from the Encryption Target Disk LUNs dialog.

See help documentation for additional impacts of manual re-key operation.

Consider all impacts.

Proceed with Re-key All operation?

FIGURE 253 Warning message - Re-key all

4. Click **Yes.**

   Re-keying operations begin on up to 10 LUNs. If more than 10 LUNs are configured on the switch, the remaining re-key operations are held in the pending state.

5. Open the **Encryption Target Disk LUNs** dialog box to see LUNs being re-keyed and LUNs pending.

   a. Select **Configure > Encryption** from the menu task bar.

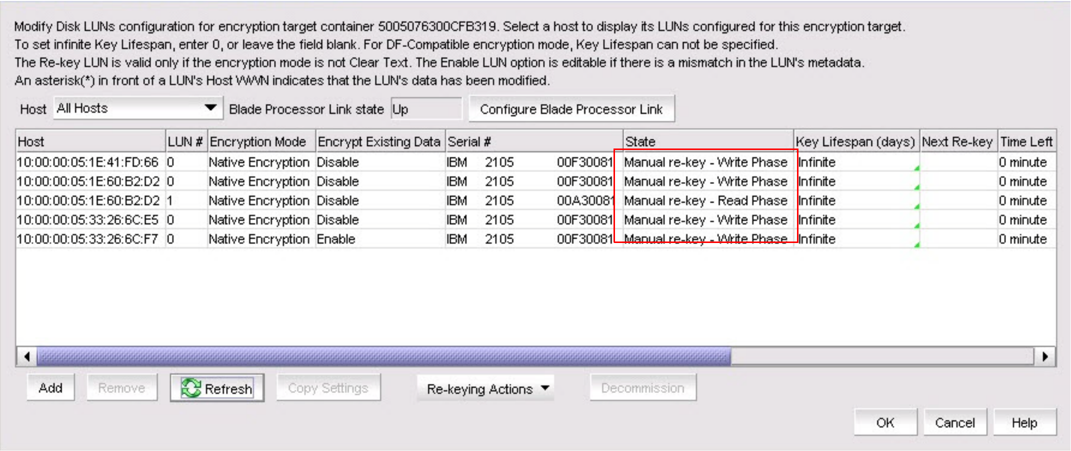
      The **Encryption Center** dialog box displays (Figure 153).

   b. Select the encryption switch from the **Encryption Center Devices** table, then select **Targets** from the menu task bar, or right-click the switch and select **Targets.**

      The **Encryption Targets** dialog box displays.

6. Select a disk LUN device from the table, then click **LUNs.**

   The **Encryption Targets Disk LUNs** dialog box displays, showing the status of the re-key operation (Figure 254).



Modify Disk LUNs configuration for encryption target container 5005076300CFB319. Select a host to display its LUNs configured for this encryption target.
To set infinite Key Lifespan, enter 0, or leave the field blank. For DF-Compatible encryption mode, Key Lifespan can not be specified.
The Re-key LUN is valid only if the encryption mode is not Clear Text. The Enable LUN option is editable if there is a mismatch in the LUN's metadata.
An asterisk(*) in front of a LUN's Host WWN indicates that the LUN's data has been modified.

Host: All Hosts
Blade Processor Link state: Up

Host	LUN #	Encryption Mode	Encrypt Existing Data	Serial #	State	Key Lifespan (days)	Next Re-key	Time Left
10:00:00:05:1E:41:FD:66	0	Native Encryption	Disable	IBM 2105 00F30081	Manual re-key - Write Phase	Infinite		0 minute
10:00:00:05:1E:60:B2:D2	0	Native Encryption	Disable	IBM 2105 00F30081	Manual re-key - Write Phase	Infinite		0 minute
10:00:00:05:1E:60:B2:D2	1	Native Encryption	Disable	IBM 2105 00A30081	Manual re-key - Read Phase	Infinite		0 minute
10:00:00:05:33:26:6C:E5	0	Native Encryption	Disable	IBM 2105 00F30081	Manual re-key - Write Phase	Infinite		0 minute
10:00:00:05:33:26:6C:F7	0	Native Encryption	Enable	IBM 2105 00F30081	Manual re-key - Write Phase	Infinite		0 minute

FIGURE 254 Pending manual re-key operations

Viewing the progress of manual re-key operations

To monitor the progress of manual re-key operations, follow these steps:

1. From the Encryption Center, right-click an encryption group.
2. Select **Re-Key Sessions** from the list.

   The **Re-Key Sessions Status** dialog box displays. The dialog box lists the status of each LUN that is being re-keyed.

3. Click **Refresh** periodically to update the display.

Viewing time left for auto re-key

You can view the time remaining until auto re-key is no longer active for a disk LUN. The information is expressed as the difference between the next re-key date and the current date and time, and is measured in days, hours, and minutes.

Although you cannot make changes directly to the table, you can modify the time left using CLI. For more information, see the administrator's guide supporting your key vault management system.

To view the time left for auto re-key, follow these steps:

1. Select **Configure > Encryption**.

   The **Encryption Center** dialog box displays (Figure 153).

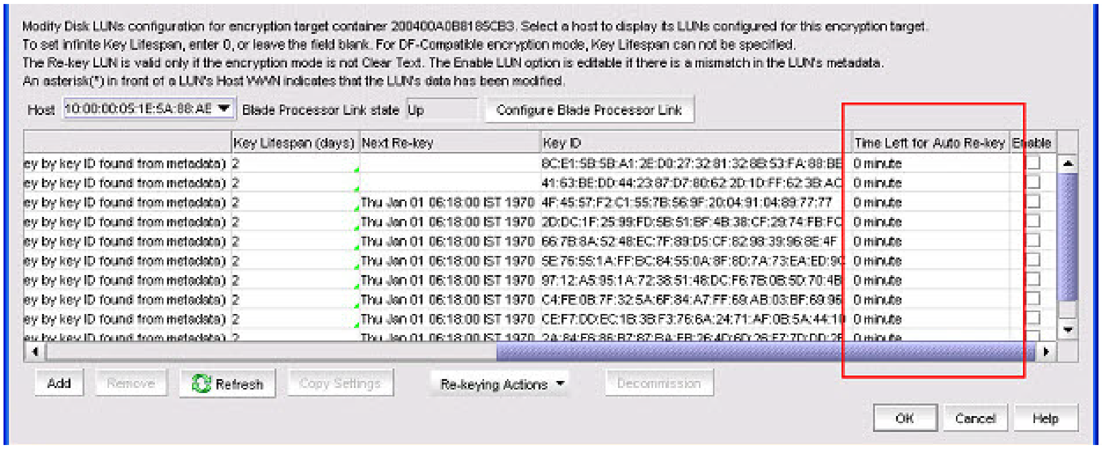
2. Select a group, switch, or engine from the **Encryption Center Devices** table for which to view the auto re-key information, then select **Group/Switch/Engine > Targets** from the menu task bar, or right-click a group, switch, or engine and select **Targets**.

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   The **Encryption Targets** dialog box displays.

3. Select a target disk device from the table, then click **LUNs.**

   The **Encryption Target Disk LUNs** dialog box displays. From this dialog box, you can view the time left for auto re-key information.



Modify Disk LUNs configuration for encryption target container 200400A0B8185CB3. Select a host to display its LUNs configured for this encryption target.
To set infinite Key Lifespan, enter 0, or leave the field blank. For DF-Compatible encryption mode, Key Lifespan can not be specified.
The Re-key LUN is valid only if the encryption mode is not Clear Text. The Enable LUN option is editable if there is a mismatch in the LUN's metadata.
An asterisk(*) in front of a LUN's Host WWN indicates that the LUN's data has been modified.

Host: 10:00:00:05:1E:5A:88:AE
Blade Processor Link state: Up

	Key Lifespan (days)	Next Re-key	Key ID	Time Left for Auto Re-key	Enable
ey by key ID found from metadata)	2		8C:E1:5B:5B:A1:2E:D0:27:32:81:32:8B:53:FA:88:BE	0 minute	☐
ey by key ID found from metadata)	2		41:63:BE:DD:44:23:87:D7:80:62:2D:1D:FF:62:3B:AC	0 minute	☐
ey by key ID found from metadata)	2	Thu Jan 01 06:18:00 IST 1970	4F:45:57:F2:C1:55:7B:56:9F:20:04:91:04:89:77:77	0 minute	☐
ey by key ID found from metadata)	2	Thu Jan 01 06:18:00 IST 1970	2D:DC:1F:25:99:FD:5B:51:BF:4B:38:CF:29:74:FB:FC	0 minute	☐
ey by key ID found from metadata)	2	Thu Jan 01 06:18:00 IST 1970	66:7B:8A:52:48:EC:7F:89:D5:CF:82:98:39:96:8E:4F	0 minute	☐
ey by key ID found from metadata)	2	Thu Jan 01 06:18:00 IST 1970	5E:76:55:1A:FF:BC:84:55:0A:8F:8D:7A:73:EA:ED:9C	0 minute	☐
ey by key ID found from metadata)	2	Thu Jan 01 06:18:00 IST 1970	97:12:A5:95:1A:72:38:51:46:DC:F6:7B:0B:5D:70:4B	0 minute	☐
ey by key ID found from metadata)	2	Thu Jan 01 06:18:00 IST 1970	C4:FE:0B:7F:32:5A:6F:84:A7:FF:69:AB:03:BF:69:96	0 minute	☐
ey by key ID found from metadata)	2	Thu Jan 01 06:18:00 IST 1970	CE:F7:DD:EC:1B:3B:F3:76:6A:24:71:AF:0B:5A:44:10	0 minute	☐
ey by key ID found from metadata)	2	Thu Jan 01 06:18:00 IST 1970	2A:84:F8:36:B7:87:BA:FB:26:4D:6D:26:F7:7D:DD:2E	0 minute	☐

FIGURE 255 Time left for auto re-key

Viewing and editing switch encryption properties

To view switch encryption properties, complete the following steps:

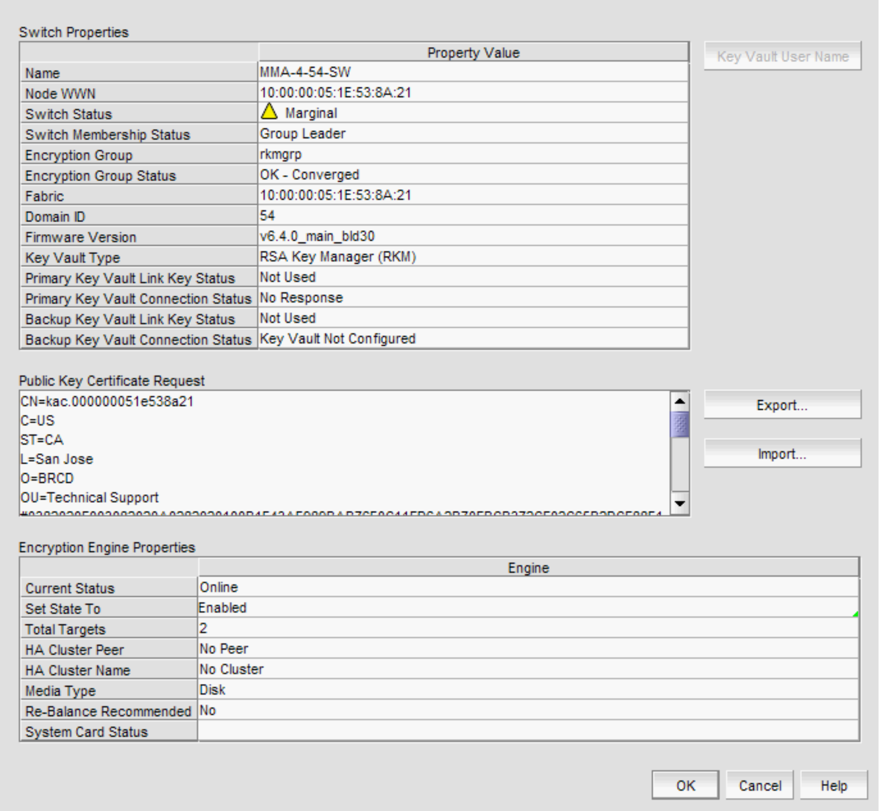
1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153). The dialog box shows the status of all encryption-related hardware and functions at a glance. It is the single launching point for all encryption-related configuration.

2. Select a switch or encryption engine from the **Encryption Center Devices** table, then select **Switch/Engine > Properties** from the menu task bar, or right-click a switch or encryption engine and select **Properties.**

   NOTE
   You can also select a group, switch, or engine from the **Encryption Center Devices** table, then click the **Targets** icon.

   The **Encryption Properties** dialog box displays (Figure 256). The dialog box contains the following information:



Switch Properties

	Property Value
Name	MMA-4-54-SW
Node WWN	10:00:00:05:1E:53:8A:21
Switch Status	⚠ Marginal
Switch Membership Status	Group Leader
Encryption Group	rkmgrp
Encryption Group Status	OK - Converged
Fabric	10:00:00:05:1E:53:8A:21
Domain ID	54
Firmware Version	v6.4.0_main_bld30
Key Vault Type	RSA Key Manager (RKM)
Primary Key Vault Link Key Status	Not Used
Primary Key Vault Connection Status	No Response
Backup Key Vault Link Key Status	Not Used
Backup Key Vault Connection Status	Key Vault Not Configured

Public Key Certificate Request

```
CN=kac.000000051e538a21
C=US
ST=CA
L=San Jose
O=BRCD
OU=Technical Support
```

Encryption Engine Properties

	Engine
Current Status	Online
Set State To	Enabled
Total Targets	2
HA Cluster Peer	No Peer
HA Cluster Name	No Cluster
Media Type	Disk
Re-Balance Recommended	No
System Card Status	

FIGURE 256 Encryption Properties dialog box

- Switch Properties table - the properties associated with the selected switch.
- Name - the name of the selected switch.
- Node WWN - the world wide name of the node.
- Switch Status - the health status of the switch. Possible values are Healthy, Marginal, Down, Unknown, Unmonitored, and Unreachable.
- Switch Membership Status - the alert or informational message description which details the health status of the switch. Possible values are Group Member, Leader-Member Comm, Error, Discovering, and Not a member.
- Encryption Group - the name of the encryption group to which the switch belongs.
- Encryption Group Status - Possible values are:
  - OK - Converged - the group leader can communicate with all members.
  - Degraded - the group leader cannot communicate with one or more members.
  - Unknown - the group leader is in an unmanaged fabric.

NOTE
When a group is in the **Degraded** state, the following operations are not allowed: key vault changes, master key operations, enable/disable encryption engines, Failback mode changes, HA Cluster creation or addition (removal is allowed), and any configuration changes for storage targets, hosts, and LUNs.

- Fabric - the name of the fabric to which the switch belongs.
- Domain ID - the domain ID of the selected switch.
- Firmware Version - the current encryption firmware on the switch.
- Primary Key Vault Link Key Status - the possible statuses are as follows:
  - Not Used – the key vault type is not LKM.
  - No Link Key – no access request has been sent to an LKM, or a previous request was not accepted.
  - Waiting for LKM approval – a request has been sent to LKM and is waiting for the LKM administrator's approval.
  - Waiting for local approval – a response was received from LKM.
  - Created, not validated – in interim state until first used.
  - Link Key valid, online – (LKM only) a shared link key exists and has been successfully used.
- Primary Key Vault Connection Status - whether the primary key vault link is connected. Possible values are Unknown, Key Vault Not Configured, No Response, Failed authentication, and Connected.
- Backup Key Vault Link Key Status - the possible statuses are as follows:
  - Not Used – the key vault type is not LKM.
  - No Link Key – no access request has been sent to an LKM, or a previous request was not accepted.
  - Waiting for LKM approval – a request has been sent to LKM and is waiting for the LKM administrator's approval.
  - Waiting for local approval – a response was received from LKM.
  - Created, not validated – in interim state until first used.
  - Link Key valid, online – (LKM only) a shared link key exists and has been successfully used.
- Backup Key Vault Connection Status - whether the backup key vault link is connected. Possible values are Unknown, Key Vault Not Configured, No Response, Failed authentication, and Connected.
- Key Vault User Name – (TEMS only) launches dialog box to identify key vault user information.
- Public Key Certificate Request text box - the switch's KAC certificate, which must be installed on the primary and backup key vaults.
- Export button – launches dialog box for saving Certificate Signing Request file.
- Import button – launches dialog box for identifying Signed Certificate file name.
- Encryption Engine Properties table - the properties for the encryption engine. There may be 0 to 4 slots, one for each encryption engine in the switch.
- Current Status - the status of the encryption engine. There are many possible values, but common values are Not Available (the engine is not initialized), Disabled, Operational, need master/link key, and Online.
- Set State To - enter a new value, enabled or disabled, and click OK to apply the change.
- Total Targets - the number of encrypted target devices.
- HA Cluster Peer - the name and location of the high-availability (HA) cluster peer (another encryption engine in the same group), if in an HA configuration.

- **HA Cluster Name** - the name of the HA cluster (for example, Cluster1), if in an HA configuration. HA Cluster names can have up to 31 characters. Letters, digits, and underscores are allowed.
- **Media Type** - the media type of the encryption engine. Possible values are Disk and Tape.
- **Re-Balance Recommended** - A value of **Yes** or **No** indicating whether or not LUN re-balancing is recommended for an encryption engine that is hosting both disk and tape LUNs.
- **System Card Status** - the current status of system card information for the encryption engine. (enabled or disabled).

Exporting the public key certificate signing request (CSR) from Properties

To export the CSR under Public Key Certificate Request, complete the following steps.

1. Click **Export**.

   A **Save** dialog box displays.

2. Browse to the location where you want to save the certificate.
3. Click **Save**.

   Alternatively, you may also copy the CSR and paste it to a file.

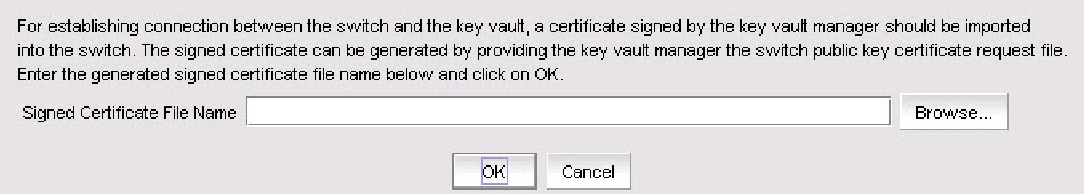
4. Submit the CSR to a certificate authority (CA) for signing. CA signing requirements and procedures differ per key manager appliance. Refer to "Supported encryption key manager appliances" on page 447 and review the following sections to find the procedure that applies.

Importing a signed public key certificate from Properties

To import a signed public key certificate, complete the following steps.

1. Click **Import**.

   The **Import Signed Certificate** dialog box displays (Figure 257).



For establishing connection between the switch and the key vault, a certificate signed by the key vault manager should be imported into the switch. The signed certificate can be generated by providing the key vault manager the switch public key certificate request file. Enter the generated signed certificate file name below and click on OK.

Signed Certificate File Name

FIGURE 257 Import Signed Certificate dialog box

2. Enter or browse to the file containing the signed certificate.
3. Click **OK**.

   The file is imported onto the switch.

Enabling the encryption engine state from Properties

To enable the encryption engine, complete the following steps:

1. Find the **Set State To** entry under **Encryption Engine Properties.**
2. Click the field and select **Enabled.**
3. Click **OK.**

Disabling the encryption engine state from Properties

To disable the encryption engine, complete the following steps.

1. Find the **Set State To** entry under **Encryption Engine Properties.**
2. Click the field and select **Disabled.**
3. Click **OK.**

Viewing and editing group properties

To view encryption group properties, complete the following steps.

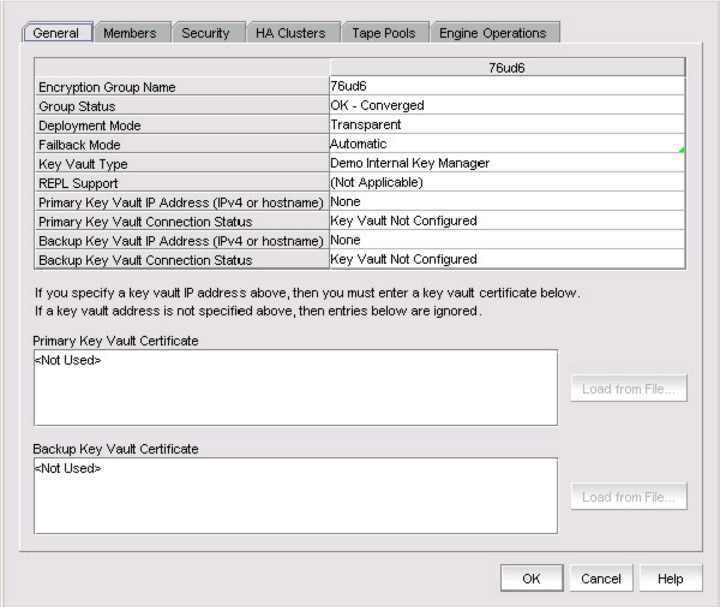
1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group from the **Encryption Center Devices** table, then select **Group > Properties** from the menu task bar, or right-click a group and select **Properties.**

   NOTE
   If groups are not visible in the **Encryption Center Devices** table, select **View > Groups** from the menu task bar.

The **Encryption Group Properties** dialog box displays (Figure 258).



	76ud6
Encryption Group Name	76ud6
Group Status	OK - Converged
Deployment Mode	Transparent
Failback Mode	Automatic
Key Vault Type	Demo Internal Key Manager
REPL Support	(Not Applicable)
Primary Key Vault IP Address (IPv4 or hostname)	None
Primary Key Vault Connection Status	Key Vault Not Configured
Backup Key Vault IP Address (IPv4 or hostname)	None
Backup Key Vault Connection Status	Key Vault Not Configured

If you specify a key vault IP address above, then you must enter a key vault certificate below.
If a key vault address is not specified above, then entries below are ignored.

Primary Key Vault Certificate
<Not Used>

Backup Key Vault Certificate
<Not Used>

FIGURE 258 Encryption Group Properties dialog box

The dialog box includes the following tabs:

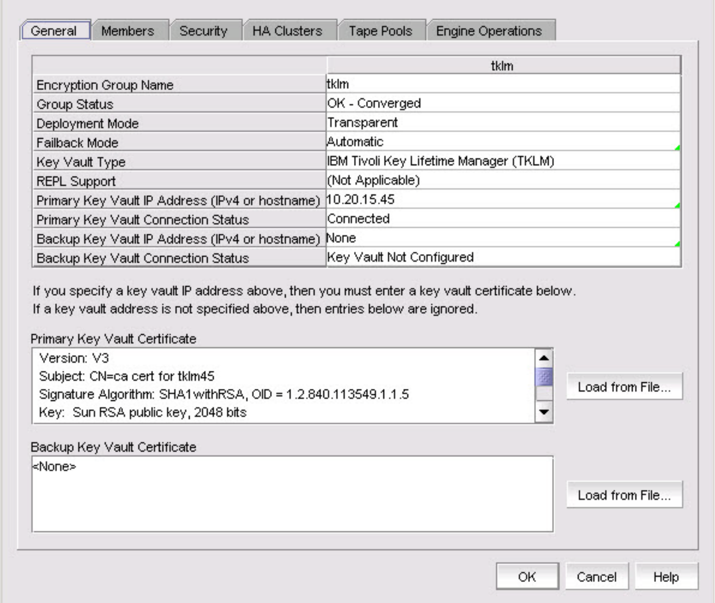
- "General tab" on page 562
- "Members tab" on page 563
- "Security tab" on page 566
- "HA Clusters tab" on page 567
- "Engine Operations tab" on page 572
- "Link Keys tab" on page 568
- "Tape Pools tab" on page 569

NOTE
The **Link Keys** tab appears only if the key vault type is NetApp LKM.

General tab

The **General** tab is viewed from the **Encryption Group Properties** dialog box. To access the **General** tab, select a group from the **Encryption Center Devices** table, then select **Group > Properties** from the menu task bar, or right-click a group and select **Properties**.

NOTE
You can also select a group from the **Encryption Center Devices** table, then click the **Properties** icon.



	tklm
Encryption Group Name	tklm
Group Status	OK - Converged
Deployment Mode	Transparent
Failback Mode	Automatic
Key Vault Type	IBM Tivoli Key Lifetime Manager (TKLM)
REPL Support	(Not Applicable)
Primary Key Vault IP Address (IPv4 or hostname)	10.20.15.45
Primary Key Vault Connection Status	Connected
Backup Key Vault IP Address (IPv4 or hostname)	None
Backup Key Vault Connection Status	Key Vault Not Configured

If you specify a key vault IP address above, then you must enter a key vault certificate below.
If a key vault address is not specified above, then entries below are ignored.

Primary Key Vault Certificate

```
Version: V3
Subject: CN=ca cert for tklm45
Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5
Key:  Sun RSA public key, 2048 bits
```

Backup Key Vault Certificate

```
<None>
```

FIGURE 259 **Encryption Group Properties dialog box - General tab**

The **General** tab displays the following properties:

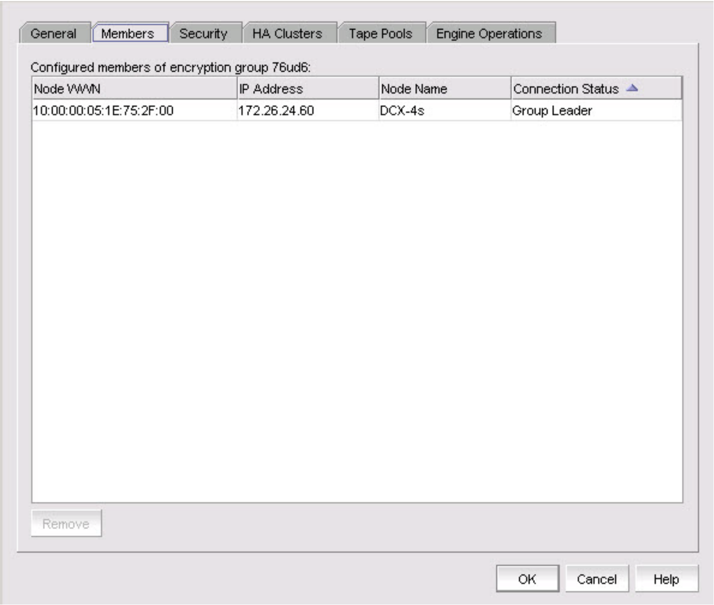
- **Encryption group name** - the name of the encryption group.
- **Group status** - the status of the encryption group, which can be **OK-Converged** or **Degraded.** Degraded means the group leader cannot contact all of the configured group members.
- **Deployment mode** - the group's deployment mode, which is transparent.
- **Failback mode** - The group's failback mode, which can be automatic or manual. The failback mode can be changed by clicking on the field and selecting the desired mode.
- **Key vault** - the vault type, either RSA Key Manager (RKM) NetApp Lifetime Key Manager (LKM), HP Secure Key Manager (SKM), Thales Encryption Manager for Storage (TEMS), or Tivoli Key Lifetime Manager (TKLM).
- **REPL Support** - whether or not remote replication LUNs support is enabled or disabled. You can change the current setting by clicking on the field and selecting the desired state.
- **Primary Key Vault IP address** - The IP address of the primary key vault, either IPv4 or host name.
- **Primary Key Vault Connection Status** - the status of the connection to the primary key vault. In an operating environment, the status should be Connected.
- **Backup key vault IP address** - the IP address of the backup key vault.

- **Backup Key Vault Connection Status** - the status of the connection to the backup key vault, if a backup is configured.
- **Primary key vault certificate** - the details of the primary vault certificate; for example, version and signature information.
- **Backup key vault certificate** - the details of the backup vault certificate; for example, version and signature information.

Members tab

The **Members** tab (Figure 260) is viewed from the **Encryption Group Properties** dialog box. To access the **Members** tab, select a group from the **Encryption Center Devices** table, then select **Group** > **Properties** from the menu task bar, or right-click a group and select **Properties.**

NOTE
You can also select a group from the **Encryption Center Devices** table, then click the **Properties** icon.



Configured members of encryption group 76ud6:

Node WWN	IP Address	Node Name	Connection Status ▲
10:00:00:05:1E:75:2F:00	172.26.24.60	DCX-4s	Group Leader

FIGURE 260 Encryption Group Properties dialog box - Members tab

The **Members** tab lists group switches, their role, and their connection status with the group leader. The tab displays the configured membership for the group (none of the table columns are editable). The list can be different from the members displayed in the **Encryption Center** dialog box if some configured members are unmanaged, missing, or in a different group.

Possible **Connection Status** values are as follows:

- **Group Leader** - this switch is the group leader so there is no connection status.
- **Trying to Contact** - the member is not responding to the group leader. This may occur if the member switch is not reachable by way of the management port, or if the member switch does not believe it is part of the encryption group.
- **Configuring** - the member switch has responded and the group leader is exchanging information. This is a transient condition that exists for a short time after a switch is added or restored to a group.

- OK - the member switch is responding to the group leader switch.
- Not Available - the group leader is not a managed switch, so connection statuses are not being collected from the group leader.

Members tab Remove button

You can click the **Remove** button to remove a selected switch or group from the encryption group table.

- You cannot remove the group leader unless it is the only switch in the group. If you remove the group leader, the Management application also removes the HA cluster, the target container, and the tape pool (if configured) that are associated with the switch.
- If you remove a switch from an encryption group, the Management application also removes the HA cluster and target container associated with the switch.

> **NOTE**
> If the encryption group is in a degraded state, the Management application does not remove the HA clusters or target containers associated with the switch. In this case, a pop-up error message displays.

- If you remove the last switch from a group, the Management application also deletes the group.

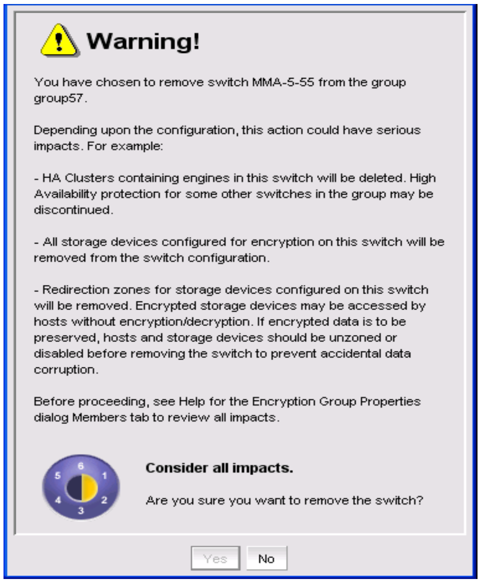
Consequences of removing an encryption switch

Table 35 explains the impact of removing switches.

TABLE 35 Switch removal impact

Switch configuration	Impact of removal
The switch is the only switch in the encryption group.	The encryption group is also removed.
The switch has configured encryption targets on encryption engines.	• The switch is configured to encrypt traffic to one or more encryption targets. • The target container configuration is removed. • The encrypted data remains on the encryption target but is not usable until the encryption target is manually configured on another encryption switch. ⚠ CAUTION **The encryption target data is visible in encrypted format to zoned hosts. It is strongly recommended that you remove the encryption targets from all zones before you disable encryption. Otherwise, hosts might corrupt the encrypted data by writing directly to the encryption target without encryption.**
The switch has encryption engines in HA Clusters.	The HA Clusters are removed. High availability is no longer provided to the other encryption engine in each HA Cluster.

A warning message displays when you attempt to remove a switch, requesting confirmation prior to removing the switch (Figure 261). Click **Yes** if you want to continue with removal of the switch.



Warning!

You have chosen to remove switch MMA-5-55 from the group group57.

Depending upon the configuration, this action could have serious impacts. For example:

- HA Clusters containing engines in this switch will be deleted. High Availability protection for some other switches in the group may be discontinued.

- All storage devices configured for encryption on this switch will be removed from the switch configuration.

- Redirection zones for storage devices configured on this switch will be removed. Encrypted storage devices may be accessed by hosts without encryption/decryption. If encrypted data is to be preserved, hosts and storage devices should be unzoned or disabled before removing the switch to prevent accidental data corruption.

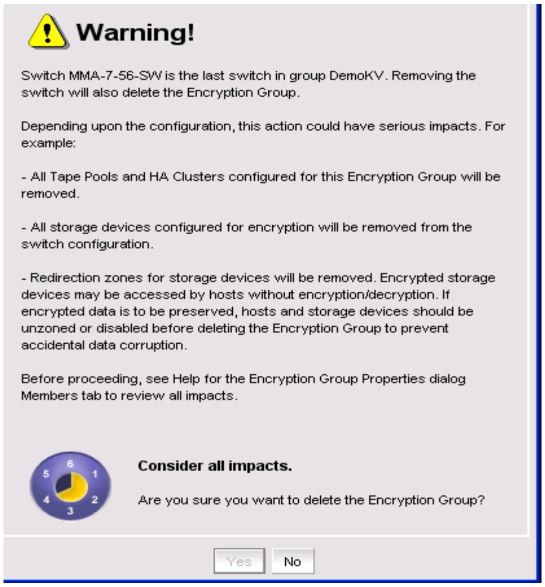
Before proceeding, see Help for the Encryption Group Properties dialog Members tab to review all impacts.

Consider all impacts.

Are you sure you want to remove the switch?

FIGURE 261 Removal of switch warning

A warning message displays when you attempt to remove an encryption group (Figure 262). Click **Yes** to continue.



Warning!

Switch MMA-7-56-SW is the last switch in group DemoKV. Removing the switch will also delete the Encryption Group.

Depending upon the configuration, this action could have serious impacts. For example:

- All Tape Pools and HA Clusters configured for this Encryption Group will be removed.

- All storage devices configured for encryption will be removed from the switch configuration.

- Redirection zones for storage devices will be removed. Encrypted storage devices may be accessed by hosts without encryption/decryption. If encrypted data is to be preserved, hosts and storage devices should be unzoned or disabled before deleting the Encryption Group to prevent accidental data corruption.

Before proceeding, see Help for the Encryption Group Properties dialog Members tab to review all impacts.

Consider all impacts.

Are you sure you want to delete the Encryption Group?

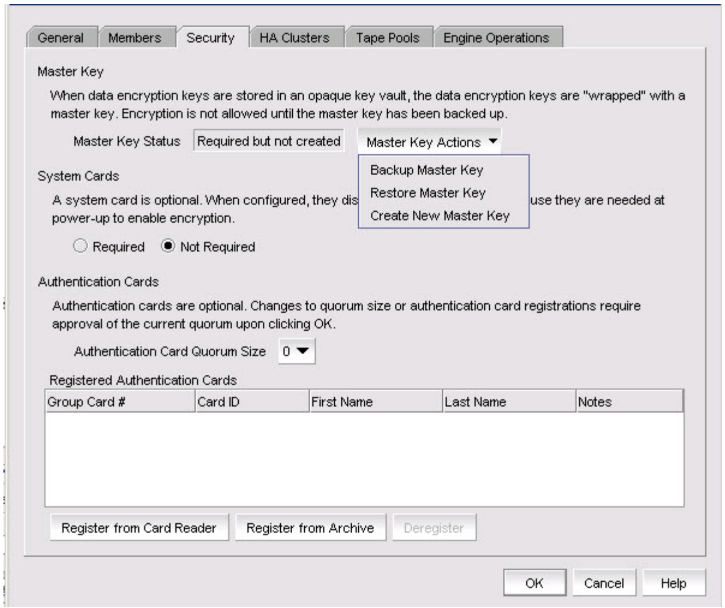
FIGURE 262 Removal of an encryption group warning

Security tab

The **Security** tab displays the status of the master key for the encryption group and whether smart cards are required. From here, you register smart cards for use.

The **Security** tab (Figure 263) is viewed from the **Encryption Group Properties** dialog box. To access the **Security** tab, select a group from the **Encryption Center Devices** table, then select **Group > Security** from the menu task bar, or right-click a group and select **Security.** The **Properties** dialog box displays with the **Security** tab selected.

NOTE
You can also select a group from the **Encryption Center Devices** table, then click the **Properties** icon.



Master Key

When data encryption keys are stored in an opaque key vault, the data encryption keys are "wrapped" with a master key. Encryption is not allowed until the master key has been backed up.

Master Key Status: Required but not created

System Cards

A system card is optional. When configured, they dis use they are needed at power-up to enable encryption.

○ Required ● Not Required

Authentication Cards

Authentication cards are optional. Changes to quorum size or authentication card registrations require approval of the current quorum upon clicking OK.

Authentication Card Quorum Size: 0

Registered Authentication Cards

Group Card #	Card ID	First Name	Last Name	Notes

FIGURE 263 Encryption Group Properties dialog box - Security tab

NOTE
You must enable encryption engines before you back up or restore master keys.

Master key actions are as follows:

- **Create a new master key**, which is enabled when no master key exists or the previous master key has been backed up.
- **Back up a master key**, which is enabled any time a master key exists.
- **Restore a master key**, which is enabled when either no master key exists or the previous master key has been backed up.
- **System Cards**, which identifies if the use of a system card is required for controlling activation of the encryption engine.

- **Authentication Cards**, which identifies if one or more authentication cards must be read by a card reader attached to a Management application PC to enable certain security-sensitive operations.

See “Master keys” on page 537 for complete information about managing master keys.

See “Smart card usage” on page 436 for information about system cards and authentication cards.

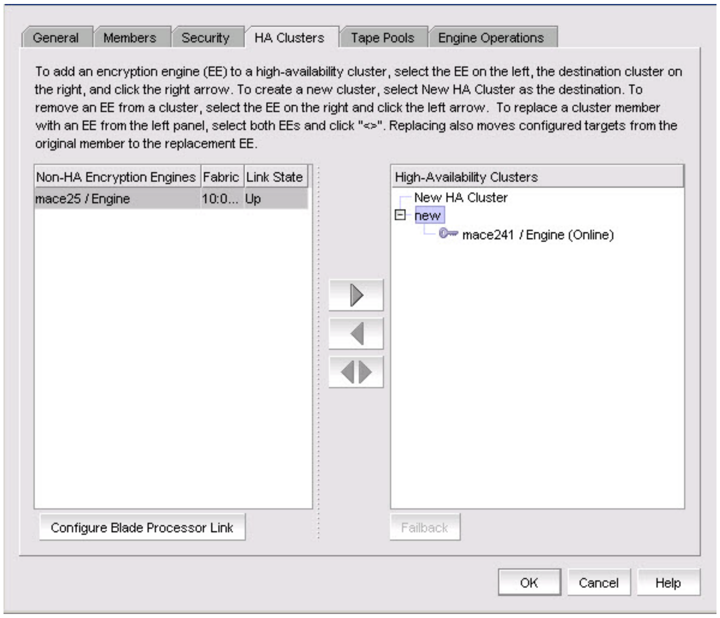
NOTE
Encryption is not allowed until the master key has been backed up.

HA Clusters tab

The **HA Clusters** tab allows you to create and delete HA clusters, add encryption engines to and remove encryption engines from HA clusters, and failback an engine.

The **HA Clusters** tab (Figure 264) is viewed from the **Encryption Group Properties** dialog box. To access the **HA Clusters** tab, select a group from the **Encryption Center Devices** table, then select **Group > HA Clusters** from the menu task bar, or right-click a group and select **HA Clusters.** The **Properties** dialog box displays with the **HA Clusters** tab selected.

NOTE
You can also select a group from the **Encryption Center Devices** table, then click the **Properties** icon.



To add an encryption engine (EE) to a high-availability cluster, select the EE on the left, the destination cluster on the right, and click the right arrow. To create a new cluster, select New HA Cluster as the destination. To remove an EE from a cluster, select the EE on the right and click the left arrow. To replace a cluster member with an EE from the left panel, select both EEs and click "<>". Replacing also moves configured targets from the original member to the replacement EE.

Non-HA Encryption Engines	Fabric	Link State
mace25 / Engine	10:0...	Up

High-Availability Clusters
- New HA Cluster
- new
  - mace241 / Engine (Online)

FIGURE 264 Encryption Group Properties dialog box - HA Clusters tab

HA clusters are groups of encryption engines that provide high availability features. If one of the engines in the group fails or becomes unreachable, the other cluster member takes over the encryption and decryption tasks of the failed encryption engine. An HA cluster consists of exactly two encryption engines. See “Creating high availability (HA) clusters” on page 511.
For more information, see also:

“Failback option” on page 513

"Invoking failback" on page 513

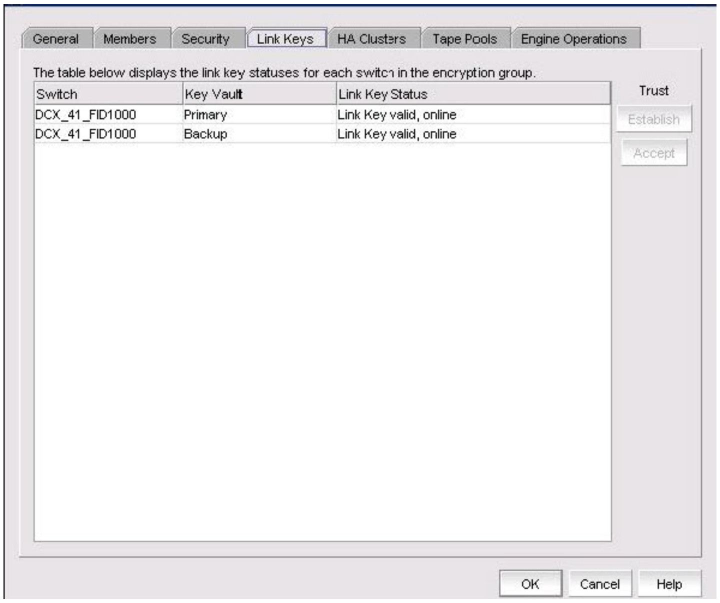
Link Keys tab

Connections between a switch and an NetApp LKM key vault require a shared link key. Link keys are used only with LKM key vaults. They are used to protect data encryption keys in transit to and from the key vault. There is a separate link key for each key vault for each switch. The link keys are configured for a switch but are stored in the encryption engines, and all the encryption engines in a group share the same link keys.

NOTE
The **Link Keys** tab appears only if the key vault type is NetApp LKM.

The **Link Keys** tab (Figure 265) is viewed from the **Encryption Group Properties** dialog box. To access the **Link Keys** tab, select an LKM group from the **Encryption Center Devices** table, then select **Group > Link Keys** from the menu task bar, or right-click an LKM group and select **Link Keys.** The **Properties** dialog box displays with the **Link Keys** tab selected.

NOTE
You can also select a group from the **Encryption Center Devices** table, then click the **Properties** icon.



The table below displays the link key statuses for each switch in the encryption group.

Switch	Key Vault	Link Key Status
DCX_41_FID1000	Primary	Link Key valid, online
DCX_41_FID1000	Backup	Link Key valid, online

FIGURE 265 Encryption Group Properties dialog box - Link Keys tab

The **Link Keys** tab displays a table that shows link key status for each switch in an encryption group.

You must create link keys under the following circumstances:

- When a new encryption group is created.
- When a new switch is added to an encryption group.
- When a new key vault is added to an encryption group.
- After all encryption engines in a switch have been zeroized.
- When all of the encryption blades have been removed from a director and one or more new encryption blades have been added.

Refer to “Establishing the trusted link” on page 453 for information on how the **Accept** and **Establish** buttons are used in establishing the trusted link between a switch and LKM.

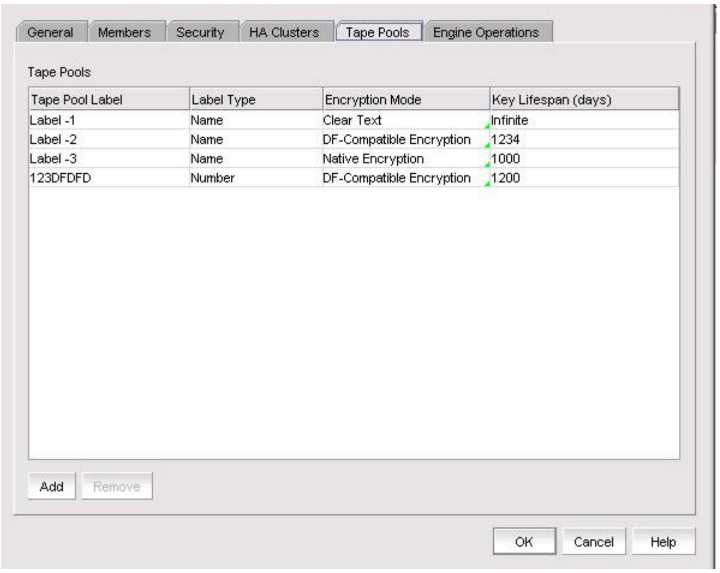
Tape Pools tab

Tape pools are managed from the **Tape Pools** tab. From the **Tape Pools** tab, you can add, modify, and remove tape pools.

- To add a tape pool, click **Add**, then complete the **Add Tape Pool** dialog box.
- To remove a tape pool, simply select one or more tape pools listed in the table, then click **Remove**.
- To modify a tape pool, you must remove the entry, then add a new tape pool.

The **Tape Pools** tab (Figure 266) is viewed from the **Encryption Group Properties** dialog box. To access the **Tape Pools** tab, select a group from the **Encryption Center Devices** table, then select **Group > Tape Pools** from the menu task bar, or right-click a group and select **Tape Pools**. The **Properties** dialog box displays with the **Tape Pools** tab selected.

NOTE
You can also select a group from the **Encryption Center Devices** table, then click the **Properties** icon.



Tape Pool Label	Label Type	Encryption Mode	Key Lifespan (days)
Label -1	Name	Clear Text	Infinite
Label -2	Name	DF-Compatible Encryption	1234
Label -3	Name	Native Encryption	1000
123DFDFD	Number	DF-Compatible Encryption	1200

FIGURE 266 Encryption Group Properties dialog box - Tape Pools tab

- To remove a tape pool, select one or more tape pools in the list, then click **Remove**.
- To modify a tape pool, you must remove the entry, then add a new tape pool. See “Adding tape pools” on page 570 for more information.
- To add a tape pool, see “Adding tape pools” on page 570.

For more information, see “Tape pools overview” on page 570.

Tape pools overview

Tape cartridges and volumes can be organized into a tape pool (a collection of tape media). The same data encryption keys are used for all cartridges and volumes in the pool. Tape pools are used by backup application programs to group all tape volumes used in a single backup or in a backup plan. The tape pool name or number used must be the same name or number used by the host backup application. If the same tape pool name or number is configured for an encryption group, tapes in that tape pool are encrypted according to the tape pool settings instead of the tape LUN settings.

Encryption switches and encryption blades support tape encryption at the tape pool level (for most backup applications) and at the LUN (tape drive) level. Since Tape Pool policies override the LUN (tape drive) policies, the LUN pool policies are used only if no tape pools exist or if the tape media/volume does not belong to any configured tape pools.

All encryption engines in the encryption group share the tape pool definitions. Tapes can be encrypted by an encryption engine where the container for the tape target LUN is hosted. The tape media is mounted on the tape target LUN.

Tape pool definitions are not needed to read a tape. Tape pool definitions are only used when writing to tape.

Adding tape pools

A tape pool can be identified by either a name or a number, but not both. Tape pool names and numbers must be unique within the encryption group. When a new encryption group is created, any existing tape pools in the switch are removed and must be added.

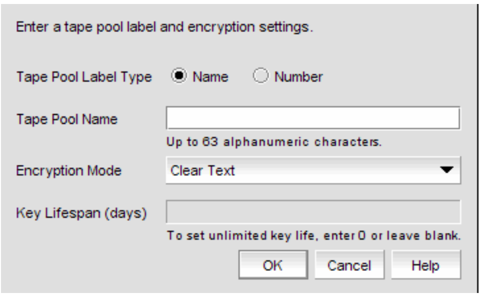
1. Select **Configure > Encryption** from the menu task bar.

   The **Encryption Center** dialog box displays (Figure 153).

2. Select a group from the **Encryption Center Devices** table, then select **Group > Tape Pools** from the menu task bar, or right-click a group and select **Tape Pools**.

   NOTE
   If groups are not visible in the **Encryption Center Devices** table, select **View > Groups** from the menu task bar.

   The **Add Tape Pool** dialog box displays (Figure 268). The **Name** tape pool label type is the default; however, you can change the tape pool label type to **Number** (Figure 268).


Enter a tape pool label and encryption settings.

Tape Pool Label Type ● Name ○ Number

Tape Pool Name

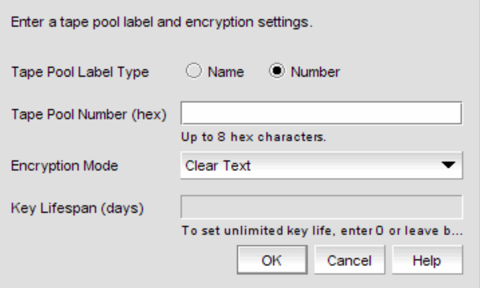
Up to 63 alphanumeric characters.

Encryption Mode: Clear Text

Key Lifespan (days)

To set unlimited key life, enter 0 or leave blank.

FIGURE 267 Add Tape Pool by name dialog box



Enter a tape pool label and encryption settings.

Tape Pool Label Type ○ Name ● Number

Tape Pool Number (hex)

Up to 8 hex characters.

Encryption Mode: Clear Text

Key Lifespan (days)

To set unlimited key life, enter 0 or leave b...

FIGURE 268 Add Tape Pool by number dialog box

3. Based on your selection, enter a name or number for the tape pool. If you selected **Number** as the **Tape Pool Label Type**, the name must match the tape pool label or tape ID/number that is configured on the tape backup/restore application.

4. Select the **Encryption Mode.**

   Choices include **Clear Text**, **DF-Compatible Encryption**, and **Native Encryption**.

   - **DF-Compatible Encryption** is valid only when LKM is the key vault.
   - The **Key Lifespan (days)** field is editable only if the tape pool is encrypted.
   - If **Clear Text** is selected as the encryption mode, the key lifespan is disabled.

   NOTE
   You cannot change the encryption mode after the tape pool I/O begins. DF-compatible encryption requires a DF-compatible encryption license to be present on the switch. If the license is not present, a warning message displays.

5. Enter the number of days to use a key before obtaining a new one, if you choose to enforce a key lifespan. The default is **Infinite** (a blank field or a value of `0`).

   NOTE
   The key lifespan interval represents the key expiry timeout period for tapes or tape pools. You can only enter the **Key Lifespan** field if the tape pool is encrypted. If **Clear Text** is selected as the encryption mode, the **Key Lifespan** field is disabled.

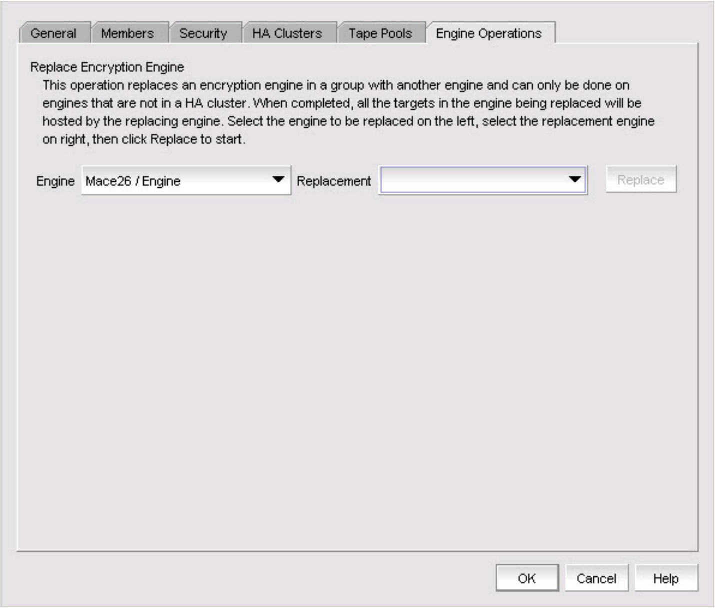
6. Click **OK.**

Engine Operations tab

The **Engine Operations** tab enables you to replace an encryption engine in a switch with another encryption engine in another switch within a DEK Cluster environment. A DEK Cluster is a set of encryption engines that encrypt the same target storage device. DEK Clusters do not display in the Management application, they are an internal implementation feature and have no user-configurable properties. Refer to "Replacing an encryption engine in an encryption group" on page 510.

The **Engine Operations** tab (Figure 264) is viewed from the **Encryption Group Properties** dialog box. To access the **Engine Operations** tab, select a group from the **Encryption Center Devices** table, then select **Group > Engine Operations** from the menu task bar, or right-click a group and select **Engine Operations.** The **Properties** dialog box displays with the **Engine Operations** tab selected.

NOTE
You can also select a group from the **Encryption Center Devices** table, then click the **Properties** icon.



Replace Encryption Engine

This operation replaces an encryption engine in a group with another engine and can only be done on engines that are not in a HA cluster. When completed, all the targets in the engine being replaced will be hosted by the replacing engine. Select the engine to be replaced on the left, select the replacement engine on right, then click Replace to start.

Engine Mace26 / Engine

Replacement

FIGURE 269 Encryption Group Properties Dialog Box - Engine Operations Tab

NOTE
You cannot replace an encryption engine if it is part of an HA Cluster. For information about HA Clusters, refer to "HA Clusters tab" on page 567.

Encryption-related acronyms in log messages

Fabric OS log messages related to encryption components and features may have acronyms embedded that require interpretation. Table 36 lists some of those acronyms.

TABLE 36 Encryption acronyms

Acronym	Name
EE	Encryption Engine
EG	Encryption Group
HAC	High Availability Cluster

Chapter

Zoning 20

In this chapter

Zoning overview

Zoning defines the communication paths in a fabric. A zone is 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.

Zoning is a fabric management service that can be used to create logical subsets of devices within a SAN and enable partitioning of resources for management and access control purposes. Zoning allows only members of a zone to communicate within that zone. All others attempting to access from outside the zone are rejected, hence zoning also provides a security function.

Zoning provides software zoning controlled at the Node World Wide Name (nWWN) level assisted by the name server of a switch. Depending on the vendor and interoperability mode, it also supports Domain/Port zoning. Domain/Port zoning is not supported when the fabric is in McDATA Open Mode (InteropMode 3).

Types of zones

Fabric OS has the following types of zones:

- Regular zones

  Enable you to partition your fabric into logical groups of devices that can access each other. These are “regular” or “normal” zones. Unless otherwise specified, all references to zones in this chapter refer to these regular zones.

- Frame redirection zones

  Re-route frames between an initiator and target through a Virtual Initiator and Virtual Target for special processing or functionality, such as for storage virtualization or encryption. See “Redirection zones” on page 550 for more information.

- LSAN zones

  Provide device connectivity between fabrics without merging the fabrics. See “LSAN zoning” on page 598 for more information.

- QoS zones

  Assign high or low priority to designated traffic flows. Quality of Service (QoS) zones are normal zones with additional QoS attributes that you select when you create the zone.
- Traffic Isolation zones (TI zones)

  Isolate inter-switch traffic to a specific, dedicated path through the fabric. See "Traffic isolation zoning" on page 603 for more information.

Online zoning

Online zoning allows you to do the following:

- View both defined and active zone information in the fabric.
- Create and modify zones and zone configurations in the software zone database.
- Activate a zone configuration in order to publish the zone information in the selected fabric.
- Deactivate the current active zone configuration.
- Configure zoning policies in the selected fabric.
- Generate zoning reports for the fabric.

NOTE
Online zoning is supported only in Brocade Native mode (InteropMode 0) and in a mixed Fabric OS and M-EOS McDATA Fabric Mode (InteropMode 2).

For pure EOS fabrics in McDATA Fabric Mode (InteropMode 2) or McDATA Open Mode (InteropMode 3) and for mixed Fabric OS and M-EOS fabrics in McDATA Open Mode, only offline zoning is available.

Offline zoning

NOTE
Offline zoning is available only for Enterprise and Professional Plus editions.

Offline zoning enables you to copy a fabric zone DB and edit it offline. The benefits to offline zoning include the following:

- You want to make changes to the zone database now, but apply them later.

  For example:

  - If you make incremental changes to zoning on an ongoing basis, but want to apply the changes to the fabric during scheduled downtime.
  - If you are expecting new servers to be delivered, but want to make changes to zoning now and apply the changes after the servers are delivered and ready to go online.
- You want to keep multiple copies of the zone database and switch between them.

  For example, if you want to allow specific servers access to tape drives for backup during specific time windows, you can have multiple zone databases (one or more for backup and one for normal operation) and switch between them easily.

- You want to analyze the impact of changes to storage access before applying the changes.

  For example, if you deploy a new server and want to ensure that the zoning changes result in only the new server gaining access to specific storage devices and nothing else. See "Comparing zone databases" on page 609.

Accessing zoning

Most of the zoning tasks are performed from the Zoning dialog box. You can access the Zoning dialog box from the main screen of the Management application using any of the following methods:

- Select **Configure > Zoning > Fabric**.
- Click the **Zoning** icon on the toolbar.
- Right-click a port, switch, switch group, or fabric in the device list and select **Zoning**.
- Right-click a port, switch, switch group, or fabric in the Connectivity Map and select **Zoning**.

Zoning naming conventions

The naming rules for zone names, zone aliases, and zone configuration names vary with the type of fabric.

The following conventions apply to Fibre Channel fabrics:

- Names must start with an alphabetic character and may contain alphanumeric characters and the underscore (_) character.

  For EOS fabrics, names can also include the dollar sign ($), carat (^), and hyphen (-) characters.

- Names are case sensitive in McDATA Open Mode. However, names are *not* case sensitive in Brocade Native Mode or McDATA Fabric Mode.
- Zone, alias, and configuration names cannot begin with "red_", "lsan_red_", or "d__efault__". Zone configuration names cannot begin with "r_e_d_i_r_c__fg". These prefixes are reserved.
- Names cannot begin with a numeric character or a special character.
- Recommended character limit: 64 characters.
- Duplicate names are not allowed between zones, zone aliases, and zone configurations within a zone database.

If you enter an invalid zone or zone configuration name, an error or warning message displays depending on the type of fabric you are trying to zone:

For FC fabrics, if an invalid name is entered for a zone or zone configuration, the application displays a warning message. If there is a naming violation according to the vendor, the switch returns the error message for the exact information along with the zone configuration activation failure message.

Administrator zoning privileges

NOTE
This section applies to the Enterprise and Professional Plus editions only.

You can set read-only or read/write access for the following zoning components:

- LSAN Zoning
- Zoning Activation (and deactivation)
- Zoning Offline
- Zoning Online
- Zoning Set Edit Limits

When read/write privileges are defined for all components, an administrator can perform all zoning-related operations provided by dialog boxes and shortcut menus. Table 37 summarizes the functions permitted for other privilege level settings.

TABLE 37 Privilege levels and accessible zoning functions

Privilege level per zoning components	Accessible functions
Read-only • Activation • LSAN • Offline • Online • Set Edit Limits	**Zone DB** tab • Zoning Policies • Find **Active Zone Configuration** tab • No accessible functions **Potential Members** list shortcut menu • Product Label • Port Label • Port Display • List Zone Members • List Un-Zone Members • Show Connected End Devices • Display All • Table **Zones** list shortcut menu • Port Label • Properties • Tree **Zone Configuration** list shortcut menu • Properties • Tree **Set Change Limits for Zoning Activation** dialog box • No accessible functions
Read/write • Activation • LSAN • Offline • Online • Set Edit Limits	All functions.

Note the following items about setting zoning privileges:

- If no privilege level is set for any of the components, zoning is disabled at the Management 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 Offline, Online, or LSAN Zoning, the **Zoning** dialog box cannot be opened. The Activation privilege cannot be added without setting at least one privilege above to either Read/Write or Read-Only. An information message displays when attempting to add the Zoning Activation only privilege.
- If a privilege level is set for the Offline, Online, or LSAN Zoning, or for all three, 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 configurations will not be possible.)

Zone database size

The supported maximum zone database size is 2 MB.

Virtual Fabric considerations: If Virtual Fabrics is enabled, the sum of the zone database sizes on all of the logical fabrics must not exceed the maximum size allowed for the chassis (1 MB).

Zoning configuration

At a minimum, zoning configuration entails creating zones and zone members. However, you can also create zone aliases, zone configurations, and zone databases. You can define multiple zone configurations, deactivating and activating individual configurations as your needs change. Zoning configuration can also involve enabling or disabling safe zoning mode and the default zone.

Configuring zoning for the SAN

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 database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box. If you click **Cancel** or the close button (X), no changes are saved.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all the discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
5. Create the zones.

   For specific instructions, refer to “Creating a new zone” on page 580.

6. Add members to each zone.

   For specific instructions, refer to "Adding members to a zone" on page 582 and "Creating a new member in an LSAN zone" on page 601.

7. Create a zone configuration.

   For specific instructions, refer to "Creating a zone configuration" on page 588.

8. Activate the zone configuration.

   For specific instructions, refer to "Activating a zone configuration" on page 590.

9. Set zoning policies for FC fabrics, if necessary.

   For specific instructions, refer to "Enabling or disabling the default zone for fabrics" on page 584 and "Enabling or disabling safe zoning mode for fabrics" on page 585.

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

    A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Creating a new zone

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **New Zone**.

   A new zone displays in the **Zones** list.

5. Type the name for the zone.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 577.

6. (Optional—Fabric OS only) Set the QoS for the zone by right-clicking the zone and selecting **QoS** > *Priority_Level* (High, Medium, or Low).

   NOTE
   QoS priority support is available for zones with WWN or Domain,Index (D,I) members.

   QoS zones using D,I notation cannot be created if any of the switches in the fabric are running Fabric OS versions earlier than 6.3.0.

   The zone name is automatically renamed to QoSX_*Zone_Name*, where X is the priority level (H—High, M—Medium, or L—Low) and *Zone_Name* is the name you entered for the zone.

7. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:

a. Select **Save to Switch** from the **Zone DB Operation** list.

b. Click **Yes** on the confirmation message.

The selected zone database is saved to the fabric without enabling a specific zone configuration.

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

A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

If the zone is empty, a warning message displays.

Viewing zone properties

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the zone you want to review in the **Zones** list and select **Properties**.

   The **Zone Properties** dialog box displays.

5. Review the zone properties.

   Depending on what type of zone you selected, the following information is included in the zone properties:

   - **Zone Name**—The name of the zone.
   - **Zone Configurations Containing This Zone**—The number of zone configurations to which this zone belongs.
   - **Total Zone Members**—The number of zone members in the selected zone.
   - **Number of Aliases**—The number of aliases in this zone.
   - **Zone Members Contained by Aliases**—The number of zone members in the selected alias.
   - **Configure Status** (TI Zone and Fabric OS only)—Whether or not the TI zone is enabled.
   - **Configure Failover** (TI Zone and Fabric OS only)—Whether or not the TI zone failover is enabled.
   - **Status** (not applicable for TI zones)—The status of the selected zone.

6. Click **OK** to close the **Zone Properties** 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 DB** tab.

Enterprise and Professional Plus versions: 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 583.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

   If you want to show all the discovered fabrics in your fabric group in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.

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 **Type** list.

   By default, the first time you launch the **Zoning** dialog box for a Zoning Scope, the **Potential Members** list displays valid members using the following rules:

   - If you select the **WWN** type, the valid members display by the Attached Ports.
   - If you select the **WWN-Fabric Assigned** type, the valid members display by the ports on which FA-PWWN is configured.
   - If you select the **Domain,Port Index** type, the valid members display by ALL Product Ports (both occupied and unoccupied). This option is available for FC fabrics only.
   - If you select the **Alias** type, the valid members display by the device Alias.

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 members 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. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:

   a. Select **Save to Switch** from the **Zone DB Operation** list.

   b. Click **Yes** on the confirmation message.

      The selected zone database is saved to the fabric without enabling a specific zone configuration.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

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 DB** 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 582.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

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. Click **New Member**.

   The **Add Zone Member** dialog box displays.

6. Select an option from the **Member Type** list.

   The fields in the dialog box vary based on the **Member Type** option you select.

7. Fill in the remaining fields in the dialog box.

   Click the **Help** button for additional information on each field.

8. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

   OR

   Click **Apply** to save your changes and keep the **Add 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.

9. For offline zone databases only, complete the following steps to save the zone configuration into the switch from the offline zone database:
   1. Select **Save to Switch** from the **Zone DB Operation** list.
   2. Click **Yes** on the confirmation message.

      The selected zone database is saved to the fabric without enabling a specific zone configuration.

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

    A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Customizing the zone member display

The following procedure applies to the zone display in the standard Zoning dialog box and also to the LSAN Zoning dialog box.

1. Select **Configure > Zoning > Fabric.**

   For LSAN zoning, select **Configure > Zoning > LSAN Zoning (Device sharing).**

   The **Zoning** or **LSAN Zoning** dialog box displays, based on the **Configure > Zoning** menu selection.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click the plus sign (+) by the appropriate zone in the **Zones** list to expand the listing and show the zone's members.
5. Right-click the name of any zone member and select **Member Display.**

   The **Zone Member Display** dialog box displays.

6. Select or clear the check boxes for the properties you want to display or hide.

   All of the options are selected by default. You cannot clear the **WWN / Domain,Port Index** check box. It is always selected.

7. Select a property and click the **Up** or **Down** buttons to rearrange the order in which the properties are displayed.
8. Click **OK.**

   The display is changed for all zone members in the **Zones** list.

Enabling or disabling the default zone for fabrics

1. Select **Configure > Zoning > Fabric.**

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zoning database you want from the **Zone DB** list.
5. Click **Zoning Policies.**

   The **Zoning Policies** dialog box displays.

   NOTE
   The format and content of this dialog box vary slightly depending on Interop Mode, the target selected in the **Zoning Scope** list, and whether safe zoning mode is enabled. If safe zoning mode is enabled, the **Default Zone** button is disabled. If you want to enable the default zone, you must disable the safe zoning mode.

6. Make sure the appropriate fabric is named on the **Zoning Policies** dialog box.
7. 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 DB** tab displays.
8. Click **OK** or **Apply** to save your changes.
   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Enabling or disabling safe zoning mode for fabrics

NOTE
Safe Zoning Mode is available only on devices running in McDATA Fabric Mode and, for pure EOS fabrics, in McDATA Open Mode.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Click **Zoning Policies**.

   The **Zoning Policies** dialog box displays.

   NOTE
   The format and content of this dialog box vary slightly depending on Interop Mode and the target selected in the **Zoning Scope** list.
5. Make sure the appropriate fabric is named on the **Zoning Policies** dialog box.
6. Perform one of the following actions based on the task you want to complete:
   - To enable Safe Zoning Mode, click **Enable**, and then click **OK**.
   - To disable Safe Zoning Mode, click **Disable**, and then click **OK**.
7. Click **OK** to apply your changes and close the **Zoning Policies** dialog box.
8. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Creating a zone alias

An alias is a logical group of port index numbers and WWNs. Specifying groups of ports or devices as an alias makes zone configuration easier, by enabling you to configure zones using an alias rather than inputting a long string of individual members. You can specify members of an alias using the following methods:

- Identifying members by switch domain and port index number pair (for example, 2, 20).
- Identifying members by device node and device port WWNs.

Zone aliases are supported only in Brocade Native mode (InteropMode 0) and in a mixed Fabric OS and M-EOS McDATA Fabric Mode (InteropMode 2).

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.
4. Select **Alias** from the **Type** list.
5. Click **New Alias**.

   The **New Alias** dialog box displays.

6. Type the desired name for the alias in the **Alias Name** field.
7. Select an option from the **Type** list to choose how to display the objects in the **Potential Members** list.
8. Show all discovered fabrics in the **Potential Members** list by right-clicking in the **Potential Members** list and selecting **Display All**.

   This right-click option is not available if you selected **WWN-Fabric Assigned** in the **Type** list.

9. Select one or more members that you want to add to the alias in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
10. Click the right arrow between the **Potential Members** list and **Selected Member(s)** list to add the selected members to the alias.
11. Click **OK** on the **New Alias** dialog box to save your changes.
12. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Editing a zone alias

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Select the alias you want to edit in the **Alias** list.
5. Click **Edit**.

   The **Edit Alias** dialog box displays.

6. Add members to the alias by completing the following steps.
   a. Select an option from the **Type** list to choose how to display the objects in the **Potential Members** list.
   b. Show all discovered fabrics in the **Potential Members** list by right-clicking in the **Potential Members** list and selecting **Expand All**.

      This right-click option is not available if you selected **WWN-Fabric Assigned**in the **Type** list.
   c. Select one or more members that you want to add to the alias in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
   d. Click the right arrow between the **Potential Members** list and **Selected Member(s)** list to add the selected members to the alias.
7. Remove members from the alias by completing the following steps.
   a. Select one or more members that you want to remove from the alias in the **Selected Member(s)** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)
   b. Click the left arrow between the **Potential Members** list and **Selected Member(s)** list to remove the selected members to the alias.
8. Click **OK** on the **Edit Alias** dialog box to save your changes.
9. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Removing an object from a zone alias

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Show all objects in the **Alias** list by right-clicking a object and selecting **Tree > Expand All**.
5. Select one or more objects that you want to remove from the alias in the **Alias** list. (Press **SHIFT** or **CTRL** and click each member to select more than one member.)

   You can select objects from different zone aliases.
6. Right-click one of the selected objects and select **Remove.**

   To selected objects are removed from the associated **Zone Alias**.
7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Exporting zone aliases

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.

4. Click **Export.**

   The **Export Alias** dialog box displays.

5. Browse to the location to which you want to export the zone alias data.

6. Enter a name for the export file in the **File Name** field.

7. Click **Export Alias**.

8. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Renaming a zone alias

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select **Alias** from the **Type** list.

4. Right-click the zone alias you want to rename and select **Rename.**

5. Edit the name and press **Enter.**

6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Creating a zone configuration

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click **New Configuration.**

   A new configuration displays in the **Zone Configurations** list.

5. Enter a name for the zone configuration.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 577.

6. 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.

7. Add zones to the zone configuration.

   For step-by-step instructions, refer to “Adding zones to a zone configuration” on page 589.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Viewing zone configuration properties

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Potential Members** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning library for the selected entity.

4. Right-click the zone configuration you want to review in the **Zone Configurations** list and select **Properties**.

   The **Zone Configuration Properties** dialog box displays.

5. Review the zone configuration properties.

   The following information is included in the zone properties:

   - **Zone Configuration Name**—The name of the selected zone configuration.
   - **Number of Zones**—The number of zones in the selected zone configuration.
   - **Total Zone Members**—The total number of zone members in the selected zone configuration.
   - **Number of Unique Zone Members**—The total number of zone members that are unique in the zone configuration.
   - **Status**—The status of the selected zone configuration (active or not active).

6. Click **OK** to close the **Zone Configuration Properties** dialog box.

Adding zones to a zone configuration

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations to which you want to add zones in the **Zone Configurations** list. (Press **SHIFT** or **CTRL** and click each zone configuration name to select more than one zone configuration.)

5. Select one or more zones to add to the zone configurations in the **Zones** list. (Press **SHIFT** or **CTRL** and click each zone name to select more than one zone.)
6. Click the right arrow between the **Zones** list and **Zone Configurations** list to add the zones to the zone configurations.
7. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Activating a zone configuration

For FC fabrics and router fabrics, when a zone configuration is active, its members can communicate with one another. Only one zone configuration can be active at any given time.

When you initiate activation of a zone configuration, a number of checks are performed on the zone configuration. These checks are performed before the **Activate Zone Configuration** dialog box is displayed, and look for the following problems:

- Zone and zone configuration name violations
- Zoning configuration violations
- Zone configuration change limit violations

For pure EOS fabrics, during zone configuration activation, the total number of zone members in each zone and in the zone configuration are checked against the limits imposed by the firmware and hardware product. If the limits are exceeded, a message is displayed informing you of the exceeded limits as well as the zone configuration failure information. Click **OK** to close the message box, and take appropriate action to meet the limits. For FC fabrics, this calculation is not done during activation, but a message is displayed whenever the size of the zone database exceeds the limits imposed by the switch.

When a zone configuration is activated, the entire zone database is sent to the fabric, except for McDATA Open Mode (Interop Mode 3) or a pure M-EOS fabric, when only the active configuration information is sent to the fabric.

NOTE
Only one server should be run at a time (actual servers performing discovery) or logon conflicts may occur. Also, activation speeds may differ depending on the hardware vendor and type of zoning used.

There are several conditions that could cause the **Activate** button to be unavailable. They include the following:

- If you do not have access privileges to activate zone configurations, the **Activate** button on the **Zone DB** tab will be unavailable. You will not be able to activate a zone configuration unless your access privileges are redefined.
- The fabric is not manageable.
- You do not have Read/Write or Activate privileges for the selected fabric and the selected zone database (for FC fabric only).
- The selected fabric is not supported by the Management application.

- The selected fabric is no longer discovered.
- In McDATA Open Mode (InteropMode 3), the seed switch is a Fabric OS switch and either no EOS switch is in the fabric or none of the EOS switches are manageable.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone configuration you want to activate in the **Zone Configurations** list.

5. Click **Activate**.

   The Management 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 configuration, 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 Configuration** dialog box, or click **No** to cancel the activation and consider your naming options.
   - For pure EOS 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 configuration 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 Configuration** dialog box, or click **No** to cancel the activation.

     You can then click **Cancel** to close the **Activate Zone Configuration** dialog box, reduce the number of zones or zone members on the **Zone DB** tab, and then return to this procedure to activate the zone configuration.

6. Review the information in the **Activate Zone Configuration** dialog box.

   a. Make sure the selected zone configuration is the one you want to activate.

   b. Select or clear the **Generate a report** check box as required.

   c. If you are activating a zone configuration from the offline zone database, select or clear the **Save only the selected zone configuration to the existing zone database in the fabric** check box.

      - If the check box is cleared (default), the entire offline zone database is saved to the switch and replaces the existing online zone database.
      - If the check box is selected, only the selected zone configuration and any TI zones in the offline zone database are saved to the switch and are added to the existing online zone database.

7. Click OK to activate the zone configuration.

   If you are activating a zone configuration from the offline zone database, a message might display informing you of name conflicts between items in the offline zone database and the existing online zone database. Click Yes to overwrite the items in the online zone database, or No to cancel the activation.

   A message box displays informing you that the zones and zone configurations you change will be saved in the zone database 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 configuration and its zones display green. When it fails, the message includes the reason for the failure.

8. Click OK to continue.

   The Activate Zone Configuration dialog box is closed and the Zone DB tab displays.

9. Click OK.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Deactivating a zone configuration

Use this procedure to deactivate the active zone configuration.

There are several conditions that could cause the Deactivate button to be unavailable. They include the following:

- There is no active zone configuration in the selected fabric.
- The fabric is not manageable.
- You do not have Read/Write or Activate privileges for the selected fabric and the selected zone database (for FC fabric only).
- The selected fabric is not supported by the Management application.
- The selected fabric is no longer discovered.

1. Select Configure > Zoning > Fabric.

   The Zoning dialog box displays.

2. Click the Active Zone Configuration tab.
3. Select an FC fabric from the Active Zone Configuration list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click Deactivate.
5. Click Yes on the confirmation message.

   If the deactivation succeeded, the zone configuration no longer displays in the Active Zone Configuration tab.
   If the deactivation failed, the zone configuration still displays in the Active Zone Configuration tab.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Creating an offline zone database

Offline zone databases are supported only in Enterprise and Professional Plus versions. Use this procedure to create a zone database and save it offline.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a zone database from the **Zone DB** list.
4. Select **Save As** from the **Zone DB Operation** list.

   The **Save Zone DB As** dialog box displays.

5. Enter a name for the database in the **Zone DB Name** field.
6. Click **OK**.
7. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

8. If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
9. Create the desired zones.

   For specific instructions, refer to "Creating a new zone" on page 580.

10. Add members to each zone.

    For specific instructions, refer to "Adding members to a zone" on page 582 and "Creating a new member in a zone" on page 583.

11. Create a zone configuration.

    For specific instructions, refer to "Creating a zone configuration" on page 588.

12. Activate the zone configuration.

    For specific instructions, refer to "Activating a zone configuration" on page 590.

13. Set zoning policies, if necessary.

    For specific instructions, refer to "Enabling or disabling the default zone for fabrics" on page 584 and "Enabling or disabling safe zoning mode for fabrics" on page 585.

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

    A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Refreshing a zone database

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select a zone database from the **Zone DB** list.
4. Select **Refresh** from the **Zone DB Operation** list.

   A message displays informing you that refresh will overwrite the selected database. Click **Yes** to continue.

5. Click **OK**.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Merging two zone databases

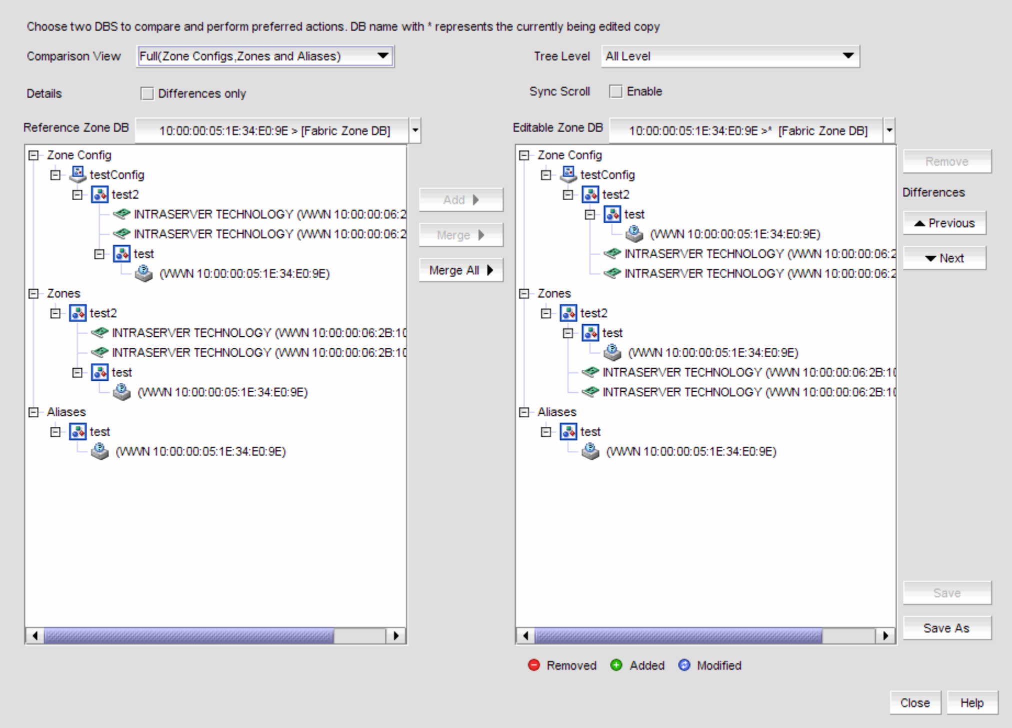
If a zone or zone configuration is merged, the resulting zone or zone configuration includes *all* members that were marked for addition or removal as well as all members not otherwise marked.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Select **Compare** from the **Zone DB Operation** list.

   The **Compare/Merge Zone DBs** dialog box displays, as shown in Figure 270.



Choose two DBS to compare and perform preferred actions. DB name with * represents the currently being edited copy

Comparison View: Full(Zone Configs,Zones and Aliases)

Tree Level: All Level

Details: □ Differences only

Sync Scroll: □ Enable

Reference Zone DB: 10:00:00:05:1E:34:E0:9E > [Fabric Zone DB]

Editable Zone DB: 10:00:00:05:1E:34:E0:9E >* [Fabric Zone DB]

Zone Config
testConfig
test2
INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2
INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2
test
(WWN 10:00:00:05:1E:34:E0:9E)
Zones
test2
INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2B:1
INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2B:1
test
(WWN 10:00:00:05:1E:34:E0:9E)
Aliases
test
(WWN 10:00:00:05:1E:34:E0:9E)
Add
Merge
Merge All
Zone Config
testConfig
test2
test
(WWN 10:00:00:05:1E:34:E0:9E)
INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2
INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2
Zones
test2
test
(WWN 10:00:00:05:1E:34:E0:9E)
INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2B:1
INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2B:1
Aliases
test
(WWN 10:00:00:05:1E:34:E0:9E)
Remove
Differences
Previous
Next
Save
Save As
Removed
Added
Modified
Close
Help

FIGURE 270 Compare/Merge Zone DBs dialog box

3. Select a database from the **Reference Zone DB** field.
4. Select a database from the **Editable Zone DB** field.

   The **Reference Zone DB** and **Editable Zone DB** areas display all available element types (zone configurations, zones, and aliases) for the two selected zone databases. In the **Editable zone DB** area, each element type and element display with an icon indicator (Table 38) to show the differences between the two databases.

5. Set the display for the database areas by selecting one of the following from the **Comparison View** list:
   - **Storage-to-Host Connectivity**—Displays only storage and host devices.
   - **Host-to-Storage Connectivity**—Displays only host and storage devices.
   - **Full (Zone Configurations, Zones, Aliases)**—Displays all zone configurations, zones, and aliases.
6. Set the level of detail for the database areas by selecting one of the following options from the **Tree Level** list.

   NOTE
   This list is only available when you set the **Comparison View** to **Full (Zone Configurations, Zones, Aliases)**.

   - **All Level**—Displays all zone configurations, zones, and aliases.
   - **Zone Configurations**—Displays only zone configurations.
   - **Zones**—Displays only zones.

7. Select the **Differences** check box to display only the differences between the selected databases.
8. Select the **Sync Scroll Enable** check box to synchronize scrolling between the selected databases.
9. Merge zone configurations by completing the followings steps.
    a. Select one or more zone configuration nodes from the **Reference Zone DB** area.
    b. Select an element in the **Editable Zone DB** area.
    c. Click **Merge**.
10. Merge zones by completing the followings steps.
    a. Select one or more zones from the **Reference Zone DB** area.
    b. Select one zone from the **Editable Zone DB** area.
    c. Click **Merge**.
11. Merge aliases by completing the followings steps.
    a. Select one or more aliases from the **Reference Zone DB** area.
    b. Select one alias from the **Editable Zone DB** area.
    c. Click **Merge**.
12. Merge all elements by clicking **Merge All**.
13. Add elements (aliases, zones, and zone configurations) to the editable database by completing the followings steps.
    a. Select one or more of the same elements in the **Reference Zone DB** area.
    b. Select the element type in the **Editable Zone DB** area.
    c. Click **Add**.
14. Remove elements from the editable zone database by selecting an available element (added) from the Editable Zone DB are and clicking **Remove**.

    Note that if a zone is removed from a zone configuration, it is removed *only* from that single zone configuration. However, if the zone is removed from the list of zones, it is removed from *all* zone configurations.
15. Click **Save As** to save the editable zone database in the offline repository (for Enterprise and Professional Plus editions only).

Saving a zone database to a switch

1. Select **Configure > Zoning > Fabric**.

    The **Zoning** dialog box displays.
2. Select a zone database from the **Zone DB** list.
3. Select **Save to Switch** from the **Zone DB Operation** list.

4. Click **Yes** on the confirmation message.

   The selected zone database is saved to the fabric without enabling a specific zone configuration.

5. Click **OK** to save your work and close the **Zoning** dialog box.

Exporting an offline zone database

NOTE
You cannot export an online zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select an offline zone database from the **Zone DB** list.
3. Select **Export** from the **Zone DB Operation** list.

   The **Export Zone DB** dialog box displays.

4. Browse to the location where you want to export the zone database file (.xml format).
5. Click **Export Zone DB**.
6. Click **OK** to save your work and close the **Zoning** dialog box.

Importing an offline zone database

NOTE
You cannot import an online zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select an offline zone database from the **Zone DB** list.
3. Select **Import** from the **Zone DB Operation** list.

   The **Import Zone DB** dialog box displays.

4. Browse to the zone database file (.xml format).
5. Click **Import Zone DB**.
6. Click **OK** to save your work and close the **Zoning** dialog box.

Rolling back changes to the offline zone database

Use this procedure to reverse changes made to an offline zone database.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Select the zone database you want to roll back from the **Zone DB** list.

   You must select an offline zone database that has a value in the **Last Saved to Fabric** column. You cannot roll back changes for zone databases that were never saved to the fabric.

3. Select **Roll Back** from the **Zone DB Operation** list.

   The selected zone database reverts back to what it was before the changes were applied.

4. Click **OK** to save your work and close the **Zoning** dialog box.

LSAN zoning

LSAN zoning is available only for backbone fabrics and any directly connected edge fabrics. A backbone fabric is a fabric that contains an FC router. All discovered backbone fabrics have the prefix LSAN_ in their fabric name, which is listed in the Zoning Scope list.

NOTE
LSAN zoning is supported only in Enterprise and Professional Plus editions.

Configuring LSAN zoning

The following procedure provides an overview of the steps you must perform to configure LSAN zoning.

Note that for any zoning-related procedure, changes to a zone database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box.

1. Select a backbone fabric from the Connectivity Map or Product List.

2. Select **Configure** > **Zoning** > **LSAN Zoning (Device Sharing)**.

   The **Zoning** dialog box displays.

3. Click the **Zone DB** tab if that tab is not automatically displayed.

4. If you want to show all edge fabrics in your backbone fabric in the **Potential Members** list, right-click a device and select **Table** > **Expand All**.

5. Create the LSAN zones.

   For specific instructions, refer to "Creating a new LSAN zone" on page 599.

6. Add members to each zone.

   For specific instructions, refer to "Adding members to the LSAN zone" on page 600.

   NOTE
   You cannot add an LSAN zone to a zone configuration.

7. Click **Activate.**

   The **Activate LSAN Zones** dialog box displays.

8. Review the information in this dialog box.

9. Click **OK** to activate the LSAN zones and close the dialog box.

   A message box displays informing you that the zones you change will be saved in the zone database 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 configuration and its zones display green. When it fails, the message includes the reason for the failure.

10. Click **OK** to continue.

    All LSAN zones are activated on the selected fabrics and saved to the Zone DB.

11. Click **OK** to close the dialog box.

Creating a new LSAN zone

1. Select a backbone fabric from the Connectivity Map or Product List.

2. Select **Configure > Zoning > LSAN Zoning (Device Sharing).**

   The **Zoning** dialog box displays.

3. Click the **Zone DB** tab if that tab is not automatically displayed.

4. Click **New Zone.**

   The prefix LSAN_ is automatically added in the text field.

5. Enter a name for the zone.

   For zone name requirements and limitations, refer to “Zoning naming conventions” on page 577.

6. 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.

7. Click **Activate.**

   The **Activate LSAN Zones** dialog box displays.

8. Review the information in this dialog box.

9. Click **OK** to activate the LSAN zones.

   A message box displays informing you that the zones you change will be saved in the zone database 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 configuration and its zones display green. When it fails, the message includes the reason for the failure.

10. Click **OK** to continue.

    All LSAN zones are activated on the selected fabrics and saved to the Zone DB.

11. Click **OK** to close the dialog box.

Adding members to the LSAN zone

Use this procedure to add a member to an LSAN zone when the member is listed in the **Potential Members** list of the **Zone DB** tab.

1. Select a backbone fabric from the Connectivity Map or Product List.
2. Select **Configure > Zoning > LSAN Zoning (Device Sharing)**.

   The **Zone DB** tab of the **Zoning** dialog box displays.

3. If you want to show all discovered fabrics in the **Potential Members** list, right-click anywhere in the table and select **Display All.**
4. Select one or more LSAN 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 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.
6. Select an option from the **Type** list.

   By default, the first time you launch the **LSAN Zoning** dialog box for a Zoning Scope, the **Potential Members** list displays valid members using the following rules:

   - If you select the **WWN** type, the valid members display by the Attached Ports.
   - If you select the **WWN-Fabric Assigned** type, the valid members display by the ports on which FA-PWWN is configured.

7. Click the right arrow between the **Potential Members** list and **Zones** list to add the selected members 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 **Activate.**

   The **Activate LSAN Zones** dialog box displays.

9. Review the information in this dialog box.

10. Click **OK** to activate the LSAN zones.

    A message box displays informing you that the zones you change will be saved in the zone database 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 configuration and its zones display green. When it fails, the message includes the reason for the failure.

11. Click **OK** to continue.

    All LSAN zones are activated on the selected fabrics and saved to the Zone DB.

12. Click **OK** to close the dialog box.

Creating a new member in an LSAN zone

Use this procedure to add a member to an LSAN zone when the member is not listed in the **Potential Members** list of the **Zone DB** 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 the LSAN zone" on page 600.

1. Select a backbone fabric from the Connectivity Map or Product List.
2. Select **Configure > Zoning > LSAN Zoning (Device Sharing)**.

   The **Zone DB** tab of the **Zoning** dialog box displays.

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 Zone Member** dialog box displays.

5. Add the new member by port WWN by completing the following steps.
   a. Select the **End Device Port WWN** option.
   b. Enter a port WWN in the **End Device Port WWN** field.
      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 enter an appropriate WWN.
   c. (*Optional*) Click the **Assign Name** check box and enter a name in the field.
      If a name was previously assigned, the name 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 name, or **No** to decline and close the message box.
6. Click **OK** to save your changes and close the **Add Zone Member** dialog box.

   OR

   Click **Apply** to save your changes and keep the **Add Zone Member** dialog box open so you can add more new members. Repeat steps 3 through 5 as many times as needed, and proceed to step 6 when you have finished adding members.

7. Click **Activate.**

   The **Activate LSAN Zones** dialog box displays.

8. Review the information in this dialog box.

9. Click **OK** to activate the LSAN zones.

   A message box displays informing you that the zones you change will be saved in the zone database 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 configuration and its zones display green. When it fails, the message includes the reason for the failure.

10. Click **OK** to continue.

    All LSAN zones are activated on the selected fabrics and saved to the Zone DB.

11. Click **OK** to close the dialog box.

Activating LSAN zones

1. Select a backbone fabric from the Connectivity Map or Product List.

2. Select **Configure > Zoning > LSAN Zoning (Device Sharing).**

   The **Zone DB** tab of the **Zoning** dialog box displays.

3. Click **Activate.**

   The **Activate LSAN Zones** dialog box displays.

4. Review the information in this dialog box.

5. Click **OK** to commit the LSAN zones and activate them in the selected fabrics.

   A message box displays informing you that the zones you change will be saved in the zone database 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 configuration and its zones display green. When it fails, the message includes the reason for the failure.

6. Click **OK** to close the dialog box.

   If you click OK without having activated the LSAN zones, a message displays informing you that your changes will be lost.

Traffic isolation zoning

A Traffic Isolation zone (TI zone) is a special zone that isolates inter-switch traffic to a specific, dedicated path through the fabric. A TI zone contains a list of E_Ports, followed by a list of N_Ports. When the TI zone is activated, the fabric attempts to isolate all inter-switch traffic between N_Ports to only those E_Ports that have been included in the zone. The fabric also attempts to exclude traffic not in the TI zone from using E_Ports within that TI zone.

Traffic isolation zoning is only supported with domain and port index number members.

A TI zone can have failover enabled or disabled.

Disable failover if you want to guarantee that TI zone traffic uses only the dedicated path, and that no other traffic can use the dedicated path.

Enable failover if you want traffic to have alternate routes if either the dedicated or non-dedicated paths cannot be used.

ATTENTION
If failover is disabled, use care when planning your TI zones so that non-TI zone devices are not isolated. If disabled failover is not used correctly, it can cause major fabric disruptions that are difficult to resolve.

Enhanced TI zones

In Fabric OS 6.4.0 or higher, ports can be in multiple TI zones. Zones with overlapping port members are called *enhanced TI zones* (ETIZ).

Enhanced TI zones are supported only on the following platforms:

- 24-port, 8 Gbps FC Switch
- 40-port, 8 Gbps FC Switch
- 80-port, 8 Gbps FC Switch
- 48-port, 16 Gbps FC Switch
- 8 Gbps 12-port Embedded Switch
- 8 Gbps 24-port Embedded Switch
- 8 Gbps 16-port Embedded Switch
- 8 Gbps 24-port Embedded Switch
- 8 Gbps Extension Switch
- 8 Gbps 8-FC port, 10 GbE 24-CEE port Switch
- 8 Gbps 40-port Switch
- 16 Gbps 192-port Backbone Chassis
- 16 Gbps 384-port Backbone Chassis
- 384-port Backbone Chassis
- 192-port Backbone Chassis
- 8 Gbps Encryption Switch

Enhanced TI zones are supported only if the following conditions are met:

- Every switch must be one of the supported platforms, as listed above.
- Every switch must be running Fabric OS v6.4.0 or later.

If the fabric contains a switch running an earlier version of Fabric OS, you cannot create an enhanced TI zone.

The failover mode must be the same for each enhanced TI zone to which a port belongs.

You cannot merge a downlevel switch into a fabric containing enhanced TI zones, and you cannot merge a switch with enhanced TI zones defined into a fabric containing switches that do not support ETIZ.

NOTE
FC router domains and EOS switches are excluded from the ETIZ platform restrictions. You can create enhanced TI zones with these switches in the fabric.

Configuring traffic isolation zoning

The following procedure provides an overview of the steps you must perform to configure traffic isolation zoning.

Note that for any zoning-related procedure, changes to a zone database are not saved until you click **OK** or **Apply** on the **Zoning** dialog box. If you click **Cancel** or the close button (X), no changes are saved.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select **Domain, Port Index** from the **Type** list.
5. If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
6. Create the traffic isolation zones.

   For specific instructions, refer to "Creating a traffic isolation zone" on page 605.

7. Add members to each zone.

   For specific instructions, refer to "Adding members to a traffic isolation zone" on page 605.

   NOTE
   You cannot add a traffic isolation zone to a zone configuration.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zones are activated when you activate a zone configuration in the same zone database.

Creating a traffic isolation zone

Traffic isolation zones are configurable only on a Fabric OS device. The seed switch must be running Fabric OS 6.1.1 or later.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select **Domain, Port Index** from the **Type** list.
5. Select **New TI Zone** from the **New Zone** list.
6. Enter a name for the zone.

   For zone name requirements and limitations, refer to "Zoning naming conventions" on page 577.

7. 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.

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

   A message displays informing you that any zones you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Adding members to a traffic isolation zone

NOTE
Traffic isolation zones are configurable only on a Fabric OS device.

Use this procedure to add a member to a zone when the member is listed in the **Potential Members** list of the **Zone DB** tab. Only ports can be added as members to a traffic isolation zone. You must add two or more N_Ports as well as all E_Ports on the path between the N_Ports.

NOTE
You cannot add a device as a member to a traffic isolation zone.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all discovered fabrics in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.

5. Select one or more traffic isolation 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.)
6. Select **Domain, Port Index** from the **Type** list.
7. Select two or more N_Ports (as well as all E_Ports on the path between the N_Ports) to add to the zone in the **Potential Members** list. (Press **SHIFT** or **CTRL** and click each port to select more than one port.)

   NOTE
   TI zones can be created in fabrics that contain logical switches; however, you can only select physical ports for TI zones.

   If you select a trunk port to add to the TI zone, all trunk ports in the trunk group are added to the TI zone automatically.
8. Click the right arrow between the **Potential Members** list and **Zones** list to add the selected ports 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.
9. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Enabling a traffic isolation zone

NOTE
Traffic isolation zones are configurable only on a Fabric OS device.

Use this procedure to enable a traffic isolation zone. When a zone configuration in the same zone database is activated, the enabled TI zones are also activated at that time. Traffic isolation zones are enabled by default when you create them.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.
2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Right-click the traffic isolation zone you want to enable in the **Zones** list and select **Configured Enabled**.
5. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zone is activated when you activate a zone configuration in the same zone database.

Disabling a traffic isolation zone

NOTE
Traffic isolation zones are configurable only on a Fabric OS device.

Traffic isolation zones are enabled by default when you create them. Use this procedure to disable a traffic isolation zone. To apply the settings and deactivate the zone, you must activate a zone configuration in the same zone database.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to disable in the **Zones** list and clear the **Configured Enabled** check box.
5. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas. The traffic isolation zone is not disabled until you activate a zone configuration in the same zone database.

Enabling failover on a traffic isolation zone

NOTE
Traffic isolation zones are configurable only on a Fabric OS device.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to enable failover on in the **Zones** list and select **Configured Failover.**
5. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Disabling failover on a traffic isolation zone

NOTE
Traffic isolation zones are configurable only on a Fabric OS device.

If failover is disabled, be aware of the following considerations:

- Ensure that there are non-dedicated paths through the fabric for all devices that are not in a TI zone.
- If you create a TI zone with just E_Ports, failover must be enabled. If failover is disabled, the specified ISLs will not be able to route any traffic.
- Ensure that there are multiple paths between switches. Disabling failover locks the specified route so that only TI zone traffic can use it.

ATTENTION
If failover is disabled, use care when planning your TI zones so that non-TI zone devices are not isolated. If disabled failover is not used correctly, it can cause major fabric disruptions that are difficult to resolve.

You cannot disable failover if the TI zone was created in the base fabric or in a fabric in which a logical switch is configured to use XISLs (the Base Fabric for Transport check box is selected).

1. Select Configure > Zoning > Fabric.

   The Zoning dialog box displays.

2. Click the Zone DB tab if that tab is not automatically displayed.
3. Select an FC fabric from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the traffic isolation zone you want to disable failover on in the Zones list and clear the Configured Failover check box.
5. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Zoning administration

This section provides instructions for performing administrative functions with zoning. You can rename, duplicate, delete, and perform other tasks on zone members, zones, and zone configurations.

Comparing zone databases

You can compare zone databases against one another to identify any and all differences between their membership prior to sending them to the switch. Once the two databases have been compared, icons display to show the differences between the two databases. These icons are illustrated and described in Table 38.

TABLE 38 Compare icon indicators

Icon	Description
⊕	Added—Displays when an element is added to the editable database.
⊙	Modified—Displays when an element is modified on the editable database.
⊖	Removed—Displays when an element is removed from the editable database.

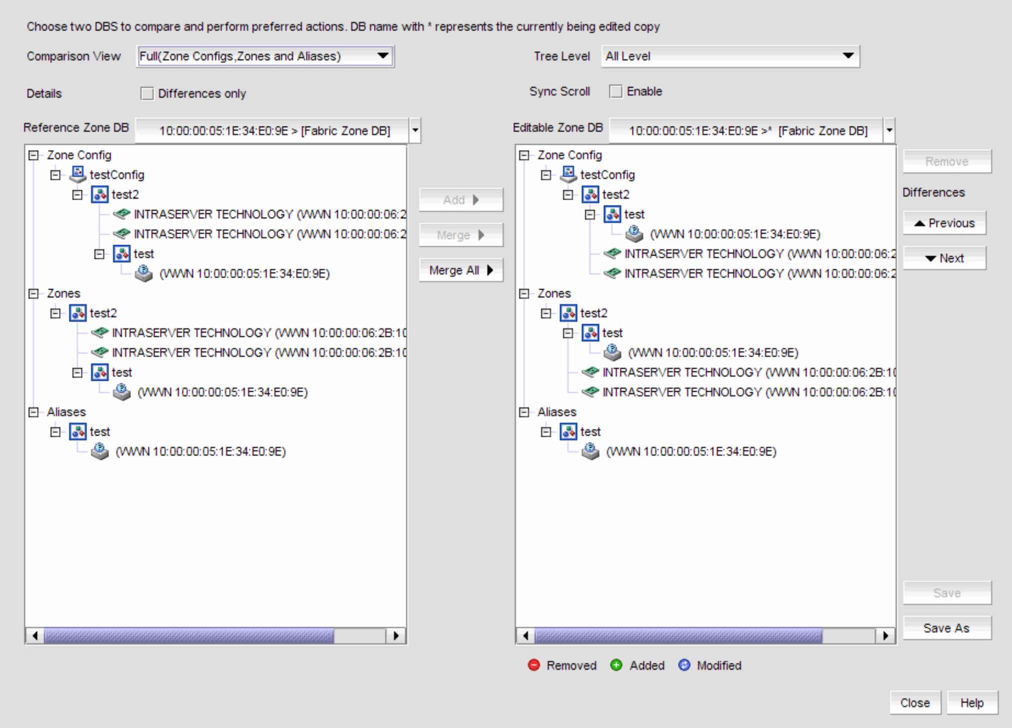
To compare two zone databases, complete the following steps.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Select **Compare** from the **Zone DB Operation** list.

   The **Compare/Merge Zone DBs** dialog box displays, as shown in Figure 271.



Choose two DBS to compare and perform preferred actions. DB name with * represents the currently being edited copy

Comparison View: Full(Zone Configs,Zones and Aliases)

Tree Level: All Level

Details: □ Differences only

Sync Scroll: □ Enable

Reference Zone DB: 10:00:00:05:1E:34:E0:9E > [Fabric Zone DB]

Editable Zone DB: 10:00:00:05:1E:34:E0:9E >* [Fabric Zone DB]

```
Zone Config
  testConfig
    test2
      INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2
      INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2
    test
      (WWN 10:00:00:05:1E:34:E0:9E)
Zones
  test2
    INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2B:1(
    INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2B:1(
  test
    (WWN 10:00:00:05:1E:34:E0:9E)
Aliases
  test
    (WWN 10:00:00:05:1E:34:E0:9E)
```

```
Zone Config
  testConfig
    test2
      test
        (WWN 10:00:00:05:1E:34:E0:9E)
      INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2
      INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2
Zones
  test2
    test
      (WWN 10:00:00:05:1E:34:E0:9E)
    INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2B:1(
    INTRASERVER TECHNOLOGY (WWN 10:00:00:06:2B:1(
Aliases
  test
    (WWN 10:00:00:05:1E:34:E0:9E)
```

FIGURE 271 Compare/Merge Zone DBs dialog box

3. Select a database from the **Reference Zone DB** field.
4. Select a database from the **Editable Zone DB** field.

   The **Reference Zone DB** and **Editable Zone DB** areas display all available element types (zone configurations, zones, and aliases) for the two selected zone databases. In the **Editable zone DB** area, each element type and element display with an icon indicator (Table 38) to show the differences between the two databases.

5. Set the display for the database areas by selecting one of the following from the **Comparison View** list:
   - **Storage-to-Host Connectivity**—Displays only storage and host devices.
   - **Host-to-Storage Connectivity**—Displays only host and storage devices.
   - **Full (Zone Configurations, Zones, Aliases)**—Displays all zone configurations, zones, and aliases.
6. Set the level of detail for the database areas by selecting one of the following options from the **Tree Level** list.

   NOTE
   This list is only available when you set the **Comparison View** to **Full (Zone Configurations, Zones, Aliases)**.

   - **All Level**—Displays all zone configurations, zones, and aliases.
   - **Zone Configurations**—Displays only zone configurations.
   - **Zones**—Displays only zones.

7. Select the **Differences** check box to display only the differences between the selected databases.
8. Select the **Sync Scroll Enable** check box to synchronize scrolling between the selected databases.
9. Click **Previous** or **Next** to navigate line-by-line in the **Editable Zone DB** area.
10. Click **Close**.

    To merge two zone databases, refer to “Merging two zone databases” on page 594.

Managing zone configuration comparison alerts

You can turn off the automatic zone configuration comparison function if you no longer want to see two of the alert messages that the comparison can produce. When a zone configuration is successfully activated, the comparison function can display an alert icon if either of two conditions exist.

The messages in question are “The active zone configuration does not exist in the zone database” and “The active zone configuration does not match <zone configuration> in the zone database.” To turn off the icons and the messages, complete the following steps.

1. After successfully activating a zone configuration, click the **Active Zone Configuration** tab.
2. Select the check box labeled **Turn off the comparison alerts between the active zone configuration and the zone database.**

   Any existing alert icons and messages are cleared and further comparisons are prevented.

   The check box selection defaults to the last setting per user.

Setting change limits on zoning activation

Use this procedure to set a limit on the number of changes a user can make to the zone database before activating a zone configuration. If the user exceeds the limit, zone configuration activation is not allowed. By default, all fabrics allow unlimited changes. Changes include adding, removing, or modifying zones, aliases, and zone configurations.

Using the following procedure you can do the following:

- Set a different limit for each fabric.
- Set limits on some fabrics while allowing other fabrics to have unlimited changes.
- Set a limit for fabrics that will be discovered later.

NOTE
You must have the Zoning Set Edit Limits privilege to perform this task.

1. Select **Configure > Zoning > Set Change Limits.**

   The **Set Change Limits for Zoning Activation** dialog box displays.
2. Click **Change Count** for the fabric on which you want to set limits.

   The field changes to an editable field.

3. Enter the maximum number of zone database changes that can be made for that fabric before a zone configuration is activated.

   To set a limit, enter a positive integer.

   To allow unlimited changes, enter 0.

4. Repeat step 2 and step 3 for each fabric on which you want to set limits.
5. To set a limit for new, undiscovered fabrics, enter a value in the **Default Change Count for New Fabrics** field.

   The default value is 0 (Unlimited).

6. Select the **Enforce change limits during zone activation** check box to enforce the change limits.

   If you want to set the limits now, but turn on enforcement of the limits at a later time, make sure the check box is clear.

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

Deleting a zone

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones in the **Zones** list that you want to delete, then right-click and select **Delete**.

   A message box displays asking you to confirm the deletion.

5. Click **Yes** to delete the selected zone.

   The message box closes and, if successful, the zone or zones are removed from the **Zones** list.

   NOTE
   If you delete something in error, click **Cancel** on the **Zoning** dialog box to exit without saving changes since the last operation (**Apply** or **Activate**). When you reopen the dialog box, the zone is restored.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Deleting a zone alias

1. Select **Configure > Zoning > Fabric.**

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Right-click the zone alias you want to delete and select **Delete.**
5. Click **Yes** on the confirmation message.

   To selected zone alias is deleted from the **Alias** list.

6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Deleting a zone configuration

1. Select **Configure > Zoning > Fabric.**

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations in the **Zone Configurations** list that you want to delete, then right-click and select **Delete.**

   A message box displays asking you to confirm the deletion.

5. Click **Yes** to delete the selected zone configuration.

   The message box closes and, when successful, the selected zone configurations are removed from the **Zone Configurations** list.

   NOTE
   If you select "**Do not show me this again.**" on the confirmation message box, the next time you delete a zone configuration, it will be deleted without requesting confirmation from you. If you delete something in error, click **Cancel** on the **Zoning** dialog box to exit without saving changes since the last operation (**Apply** or **Activate**). When you reopen the dialog box, the zone configuration is restored.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Deleting an offline zone database

For pure EOS fabrics in McDATA Fabric Mode (InteropMode 2) or McDATA Open Mode (InteropMode 3) and for mixed Fabric OS and M-EOS fabrics in McDATA Open Mode, you cannot delete the last available offline zone database, because only offline zoning is supported for these fabrics.

1. Select **Configure > Zoning > Fabric**.

   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 databases for the selected entity.

3. Select the offline zone database you want to delete in the **Zone DB** list.

   NOTE
   Only offline databases can be deleted.

4. Select **Delete** from the **Zone DB Operation** list.
5. Click **Yes** on the confirmation message.

   The message box closes and, when successful, the selected zone configurations are removed from the **Zone Configurations** list.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Clearing the fabric zone database

ATTENTION
Clearing the zone database removes all zoning configuration information, including all aliases, zones, and zone configurations, in the fabric.

Clearing the fabric zone database is disruptive to the fabric.

1. Select **Configure > Zoning > Fabric**.

   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 databases for the selected entity.

3. Select the Fabric Zone DB from the **Zone DB** list.
4. Select **Clear All** from the **Zone DB Operation** list.
5. Click **Yes** on the confirmation message.

   The message box closes and, when successful, the Fabric Zone DB is cleared of all zoning configurations.

6. Click **OK** to close the **Zoning** dialog box.

Removing all user names from a zone database

Use this procedure to remove all user names from the selected offline zone database.

1. Select **Configure > Zoning > Fabric**.

   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 databases for the selected entity.

3. Select a zone database that you have checked out (your user name is in the **Current User** column) in the **Zone DB** list.

4. Select **Undo CheckOut** from the **Zone DB Operation** list.

5. Click **Yes** in the confirmation message.

   This removes the user names of users currently logged in to the client from the **Current User** column for this zone database.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Duplicating a zone

When you duplicate a zone, you make a copy of it in the same zone database. 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>_copy_1*, *<zonelabel>_copy_2,* and *<zonelabel>_copy_3*.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zones in the **Zones** list that you want to duplicate, then right-click and select **Duplicate**.

   The duplicated zone or zones display in the **Zones** list.

5. (*Optional*) Type a new name for the zone.

   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 577.)

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Duplicating a zone alias

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select **Alias** from the **Type** list.
4. Right-click the zone alias you want to duplicate and select **Duplicate.**

   The duplicated zone alias displays in the **Alias** list (for example, <*Zone_Alias*>_Copy).

5. Edit the name.

   To edit the name, refer to "Renaming a zone alias" on page 588.

6. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

Duplicating a zone configuration

When you duplicate a zone configuration, you make a copy of it in the same zone database. The first time a zone configuration 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>_copy_1*, *<zonesetlabel>_copy_2,* and *<zonesetlabel>_copy_3*.

Note that these naming conventions apply both to duplicate and deep duplicate operations.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select one or more zone configurations in the **Zone Configurations** list that you want to duplicate, then right-click and select one of the following options:
   - **Duplicate** - To duplicate the zone configuration or configurations.
   - **Deep Duplicate** - To duplicate the zone configuration or configurations *and* all included zones.

   The duplicated zone configuration or sets display in the **Zone Configurations** list.

5. (*Optional*) Type a new name for the zone configuration.

   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 configuration name requirements and limitations, refer to "Zoning naming conventions" on page 577.)

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

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 DB** tab.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. If you want to show all fabrics discovered in the **Potential Members** list, right-click in the **Potential Members** list and select **Display All**.
5. Select the device or port you want to find in the **Potential Members** list.

   Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

6. 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 DB** tab.

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone member in the **Zones** list that you want to find in the **Potential Members** list.

   Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. 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 configuration

Use this procedure to locate all instances of a zone in the **Zone Configurations** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone you want to find in the **Zones** list.

   Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. Click **Find >** between the **Zones** list and the **Zone Configurations** list.
   - If the zone is found, all instances of the zone are highlighted in the **Zone Configurations** list.
   - If the zone is not found, a message displays informing you of this. Click **OK** to close the message box.

Finding a zone configuration member in the zones list

Use this procedure to locate a zone configuration member in the **Zones** list on the **Zone DB** tab.

1. Select **Configure > Zoning > Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.
3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Select the zone configuration member (i.e., the zone) in the **Zone Configurations** list that you want to find in the **Zones** list.

   Press **SHIFT** or **CTRL** and click each zone to select more than one zone.

5. Click Find < between the Zones list and the Zone Configurations 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.

Listing zone members

Use this procedure to identify the zone in the active zone configuration of the fabric to which an individual port belongs and the members of that zone.

If the seed switch is running Fabric OS 6.3.0 or later, the List Zone Members dialog box also displays any active TI zones to which the port belongs.

Note that the procedure is performed from the main view of the Management application.

1. On the product device list of the Management application, expand the list of products to show the ports.
2. Select a port and select Configure > Zoning > List Zone Members.

   The List Zone Members dialog box displays. If the port is a member of a zone, the fabric name, the port name, and WWN zone members display.
3. Click Close to exit the List Zone Members dialog box.

Listing un-zoned members

Use this procedure to identify the device ports in the current fabric that are not part of the active zone configuration.

You can use this procedure for standard zones as well as LSAN zones.

1. Select Configure > Zoning > Fabric.

   The Zoning dialog box displays.
2. Click the Zone DB tab if that tab is not automatically displayed.
3. Select an FC fabric from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.
4. Right-click within the Potential Members list panel and select List Un-Zone Members.

   The Un-Zone Members dialog box displays. The dialog box shows the fabric name and the connected device ports that are not part of the active zone configuration.
5. Click Close to exit the Un-Zone Members dialog box.

Removing a member from a zone

Use the following procedure to remove one or more members from a zone or zones. Note that the member is not deleted; it is only removed from the zone.

1. Select Configure > Zoning > Fabric.

   The Zoning dialog box displays.

2. Click the Zone DB tab if that tab is not automatically displayed.
3. Select an FC fabric from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click the plus sign (+) by the appropriate zone in the Zones list to expand the listing and show the zone's members.
5. Perform one of the following actions:
   - 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.
   - To remove multiple zone members, select the members to be removed from the zone, and click the left arrow between the Potential Members list and the Zones list.

   When successful, the zone member is removed from the Zones list.

6. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Removing a zone from a zone configuration

Use the following procedure to remove a zone from a zone configuration. Note that the zone is not deleted; it is only removed from the zone configuration.

1. Select Configure > Zoning > Fabric.

   The Zoning dialog box displays.

2. Click the Zone DB tab if that tab is not automatically displayed.
3. Select an FC fabric from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Click the plus sign (+) by the appropriate zone configuration in the Zone Configurations list to expand the listing and show the zone configuration members.

5. Perform one of the following actions:
   - Right-click the name of the zone you want to remove in the **Zone Configurations** list and select **Remove**.
   - To remove multiple zones, select the zones to be removed from the zone configuration, and click the left arrow between the **Zones** list and the **Zone Configurations** list.

   When successful, the zone is removed from the **Zone Configurations** list.
6. Click **OK** or **Apply** to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Removing an offline device

The Management application enables you to remove an offline device from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

   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 database for the selected entity.
3. Select **Offline Utility** from the **Zone DB Operation** list.

   The **Offline Device Management** dialog box displays.
4. Select the check box for the offline device you want to remove in the **Remove** column.

   Select the **Remove** check box to select all offline devices.
5. Click **OK** on the **Offline Device Management** dialog box.

   A warning message displays informing you that the selected zone members will be replaced from all zones and aliases in the selected zone DB.
6. Click **OK** on the message.
7. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Renaming a zone

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the name of the zone you want to change in the **Zones** list and select **Rename**.

5. Type the new name for the zone.

   For zone name requirements and limitations, refer to “Zoning naming conventions” on page 577.

6. Press **Enter** to save the new name.

   For FC fabrics, if an invalid name is entered for a zone or zone configuration, the application displays a warning message. If there is a naming violation according to the vendor, the switch returns the error message for the exact information along with the zone configuration activation failure message.

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

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Renaming a zone configuration

1. Select **Configure** > **Zoning** > **Fabric**.

   The **Zoning** dialog box displays.

2. Click the **Zone DB** tab if that tab is not automatically displayed.

3. Select an FC fabric from the **Zoning Scope** list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. Right-click the name of the zone configuration you want to change in the **Zone Configurations** list and select **Rename**.

5. Type the new name for the zone configuration.

   For zone configuration name requirements and limitations, refer to “Zoning naming conventions” on page 577.

6. 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.

7. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Replacing 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 > Fabric.

   The Zoning dialog box displays.

2. Click the Zone DB tab if that tab is not automatically displayed.
3. Select an FC fabric from the Zoning Scope list.

   This identifies the target entity for all subsequent zoning actions and displays the zoning database for the selected entity.

4. 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).

5. Select the option from the Type list that you want to use to identify the replacement zone member.
6. Enter the WWN, name, domain and port index numbers, or alias—whichever is appropriate for the method you chose in step 4.

   When you choose the WWN method, the Assign Name field is available; you may define a name for the replacement zone member. If a name was previously assigned to the potential member, a message displays informing you of this and asking whether you want to overwrite the existing name. Click Yes to continue and assign a new name, or No to decline and dismiss the message box.

7. 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.

8. Click OK or Apply to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Replacing an offline device by WWN

The Management application enables you to replace an offline device by WWN from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

   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 database for the selected entity.

3. Select **Offline Utility** from the **Zone DB Operation** list.

   The **Offline Device Management** dialog box displays.

4. Make sure the **Remove** column check box, for the offline device you want to replace, is clear.
5. Select **WWN** (default) in the corresponding **Replace Using** list.
6. Enter the WWN or select the name of the offline device in the corresponding **Replace Using** field.

   If the selected name has multiple device or device port WWNs assigned (names are set to non-unique in Management application), the **Device or Device Port WWN of Non-unique Name** dialog box displays. The WWN list includes all device and device port WWNs assigned to the selected name.

7. Click **OK** on the **Offline Device Management** dialog box.

   A warning message displays informing you that the selected zone members will be removed from all zones and aliases in the selected zone DB.

8. Click **OK** on the message.
9. Click **OK** or **Apply** on the **Zoning** dialog box to save your changes.

   A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Replacing an offline device by name

The Management application enables you to replace an offline device by name from all zones and zone aliases in the selected zone DB.

1. Select **Configure > Zoning > Fabric**.

   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 database for the selected entity.

3. Select **Offline Utility** from the **Zone DB Operation** list.

   The **Offline Device Management** dialog box displays.

4. Make sure the **Remove** column check box, for the offline device you want to replace, is clear.

5. Select Name (default is WWN) in the corresponding Replace Using list.
6. Select the name of the offline device in the corresponding Replace Using list.

   If the selected name has multiple device or device port WWNs assigned (names are set to non-unique in Management application), the Device or Device Port WWN of Non-unique Name dialog box displays. The WWN list includes all device and device port WWNs assigned to the selected name.
7. Select the WWN you want to use from the WWN list and click OK.
8. Click OK on the Offline Device Management dialog box.

   A warning message displays informing you that the selected zone members will be removed from all zones and aliases in the selected zone DB.
9. Click OK on the message.
10. Click OK or Apply on the Zoning dialog box to save your changes.

    A message displays informing you that any zones or zone configurations you have changed will be saved in the zone database, and warning you to make sure no other user is making changes to the same areas.

Chapter

Fibre Channel over IP 21

In this chapter

FCIP services licensing

Most of the FCIP extension services described in this chapter require the High Performance Extension over FCIP/FC license. FICON emulation features require additional licenses.

The following features and licensing apply to the 8 Gbps Extension platforms.

- FCIP Adaptive Rate Limiting requires the FTR_AE (Advanced Extension) license.
- FCIP trunking requires FTR_AE license.
- IBM z/OS Global Mirror emulation (formerly eXtended Remote Copy or XRC) requires the FTR_AFA (Advanced FICON Acceleration) license.

Use the licenseShow command to verify the needed licenses are present on the hardware used on both ends the FCIP tunnel. If required licenses are not installed, an error message will display while configuring the tunnel or circuit.

FCIP Concepts

Fibre Channel over IP (FCIP) is a tunneling protocol that enables you to connect Fibre Channel SANs over IP-based networks. Fabric OS extension switches and extension blades use FCIP to encapsulate Fibre Channel frames within IP frames that can be sent over an IP network to a partner Fabric OS extension switch or extension blade. When the IP packets are received, the Fibre Channel frames are reconstructed. FCIP uses a TCP transport that guarantees in-order delivery. The Fibre Channel fabric and all Fibre Channel targets and initiators are unaware of the presence of the IP network.

Because an FCIP tunnel uses an existing IP network, configuring and managing an FCIP tunnel requires knowledge of general IP networking concepts, and specific knowledge about the IP network that will be used for the tunnel. Because the IP network may be used to transport data over very long distances, and because the IP network is not designed exclusively for large data transfers, latency is an issue. Features such as data compression, trunking, FastWrite, Adaptive Rate Limiting (ARL), and Open Systems Tape Pipelining (OSTP) can reduce latency, and help manage tunnel bandwidth more effectively.

IP network considerations

Because FCIP uses TCP connections over an existing IP network, consult with the IP network administrator to be sure that the network hardware and software equipment operating in the data path can support those connections. Routers and firewalls that are in the data path need to be configured to pass layer 3 protocols 0800 (IP), 0806 (ARP), and 0001 (ICMP). Also, process layer ports for FTP (ports 20 and 21) Telnet (port 23), and SNMP (ports 161 and 162) should be configured on the management IP network to enable support personnel to access and transmit troubleshooting information.

FCIP platforms and supported features

The following Fabric OS platforms that support FCIP:

- The 8 Gbps extension switch.
- The 8 Gbps Extension blade (384-port Backbone Chassis, 192-port Backbone Chassis).
- The 4 Gbps Extension blade (384-port Backbone Chassis, 192-port Backbone Chassis, Director Chassis).

There are differences in platform capabilities. For example, the 4 Gbps Extension Blade cannot support FCIP trunking or Adaptive Rate Limiting. As another example, the 8 Gbps platforms cannot support third party WAN optimization hardware.

IPv6 addressing is not supported in conjunction with IPsec on all platforms in Fabric OS version v7.0, but will be supported in a later version.Table 39 summarizes FCIP capabilities per platform.

TABLE 39 FCIP capabilities

Capabilities	8 Gbps Extension Switch	8 Gbps Extension blade	4 Gbps Extension blade
FCIP trunking	Yes	Yes	No
Adaptive Rate Limiting	Yes	Yes	No
10 GbE ports	No	Yes	No
FC ports up to 8 Gbps	Yes	Yes	No
Compression	Yes	Yes	Yes
Open Systems Tape Pipelining (OSTP) • FCIP Fastwrite • Tape Acceleration	Yes	Yes	Yes
FICON extension	Yes	Yes	Yes
IPSec for tunnel traffic	Yes	Yes	Yes
Diffserv priorities	Yes	Yes	Yes
VLAN tagging	Yes	Yes	Yes
VEX_Ports	Yes	Yes	Yes
Support for third party WAN optimization hardware	No[1]	No[1]	No
IPv6 addresses for FCIP tunnels[2]	Yes	Yes	Yes
Support for jumbo frames	No[1] MTU of 1500 is maximum	No[1] MTU of 1500 is maximum	Yes

[1] Support is planned for a later release.

[2] IPv6 addressing is not supported in conjunction with IPsec in Fabric OS version v7.0, but will be supported in a later version.

The way FCIP tunnels and virtual ports map to the physical GbE ports depends on the switch or blade model. The 8 Gbps Extension Switch and 8 Gbps Extension Blade tunnels are not tied to a specific GbE port, and may be assigned to any virtual port within the allowed range. The 4 Gbps Extension Blade requires tunnels to be mapped to specific GbE ports and specific virtual ports. The mapping of GbE ports to tunnels and virtual port numbers is summarized in Table 40.

TABLE 40 GbE port mapping

Switch or Blade Model	GbE ports	Tunnels	Virtual ports (VE_Ports, VEX_Ports)
8 Gbps Extension Switch	GbE ports 0-5	0-8	16-23
8 Gbps Extension blade	GbE ports 0-9 10GbE ports 10, 11	0-20	12-21 used by GbE ports (0-9) and by XGE1 22-31 used by XGE0
4 Gbps Extension blade	ge0	0	16
		1	17
		2	18
		3	19
		4	20
		5	21
		6	22
		7	23
	ge1	0	24
		1	25
		2	26
		3	27
		4	28
		5	29
		6	30
		7	31

FCIP trunking

FCIP Trunking is a method for managing the use of WAN bandwidth and providing redundant paths over the WAN to protect against transmission loss. This feature is available only on the 8 Gbps extension switches and 8 Gbps extension Blades. Trunking is enabled by creating logical circuits within an FCIP tunnel. A tunnel may have multiple circuits. Each circuit is a connection between a pair of IP addresses that are associated with source and destination endpoints of an FCIP tunnel, as shown in Figure 272. Each circuit represents a portion of the available Ethernet bandwidth provided by the GbE ports that are connected to the WAN.

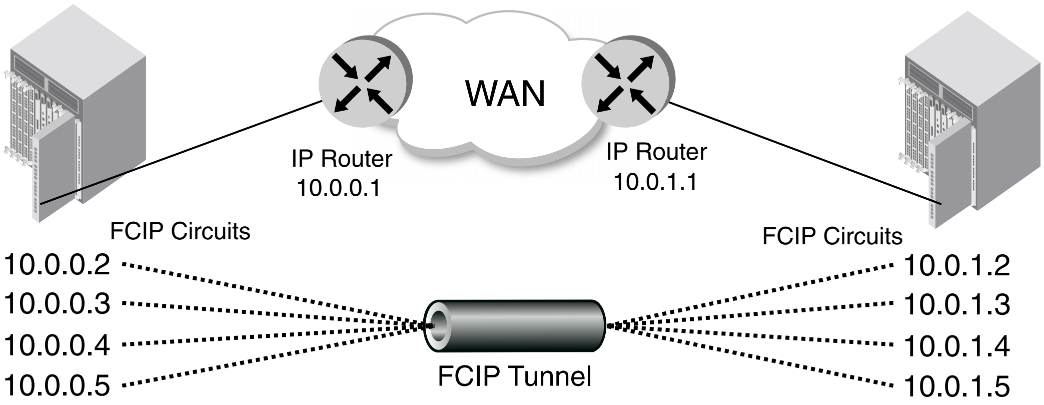


FIGURE 272 FCIP tunnel and FCIP circuits

Design for redundancy and fault tolerance

Multiple FCIP tunnels can be defined between pairs of 8 Gbps extension switches and 8 Gbps extension Blades, but doing so defeats the concept of a multiple circuit FCIP tunnel. Defining two tunnels between a pair of switches or blades rather than one tunnel with two circuits is not as redundant or fault tolerant as having one multiple circuit tunnel.

FCIP tunnel restrictions for FCP and FICON emulation features

Multiple FCIP tunnels are not supported between pairs of 8 Gbps extension Switches and 8 Gbps extension Blades when any of the FICON or FCP emulation features are enabled on the tunnel unless TI Zones or LS/LF configurations are used to provide deterministic flows between the switches. The emulation features require deterministic FC Frame routing between all initiators and devices over multiple tunnels. If there are non-controlled parallel (equal cost) tunnels between the same SID/DID pairs, emulation (Fast Write, Tape Pipelining, IBM z/OS Global Mirror (z Gm) or FICON Tape Pipelining) will fail when a command is routed via tunnel 1 and the responses are returned via tunnel 2. Therefore multiple equal cost tunnels are not supported between the switch pairs when emulation is enabled on any one or more tunnels without controlling the routing of SID/DID pairs to individual tunnels using TI Zones or LS/LF configurations.

FCIP Trunk configuration considerations

There are several points to consider when configuring an FCIP trunk:

- Each FCIP circuit is assigned a pair of IP addresses, one source IP address, and one destination IP address.
- The source IP address is used to determine which GbE interface to use. The GbE IP address must be on the same IP subnet as the source IP address. IP subnets cannot span across the GbE interfaces.
- The destination IP address is used to determine routing. If the destination IP address is also on the same subnet as the GbE interface, packets are routed over that subnet. If the destination IP address is on a different subnet, traffic must be routed to an IP gateway address.
- An FCIP circuit can have a maximum commit rate of 1,000,000 Kbps.
- In a scenario where a FCIP tunnel has multiple circuits of different metrics the data will flow over the lower metric circuits unless a failover condition occurs, as described in "FCIP circuit failover capabilities".
- The maximum bandwidth for a single circuit is 1 Gbps. However, a maximum of 10 Gbps per circuit is allowed between 10 GbE ports on 8 Gbps Extension Blades when both blades are running Fabric OS 7.0 or greater.

FCIP circuit failover capabilities

Each FCIP circuit is assigned a metric, which is used in managing failover for FC traffic. Typically, the metric will be either 0 or 1. If a circuit fails, FCIP Trunking tries first to retransmit any pending send traffic over another lowest metric circuit. In Figure 273, circuit 1 and circuit 2 are both lowest metric circuits. Circuit 1 has failed, and transmission fails over to circuit 2, which has the same metric. Traffic that was pending at the time of failure is retransmitted over circuit 2. In order delivery is ensured by the receiving 8 Gbps Extension Switch.

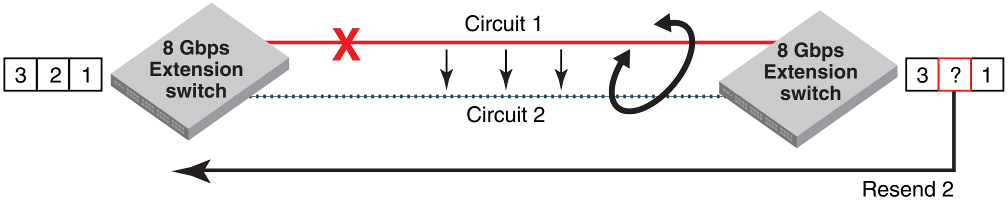


FIGURE 273 Link loss and retransmission over peer lowest metric circuit

In Figure 274, circuit 1 is assigned a metric of 0, and circuit 2 is assigned a metric of 1. In this case, circuit 2 is a standby that is not used unless there are no lowest metric circuits available. If all lowest metric circuits fail, then the pending send traffic is retransmitted over any available circuits with the higher metric,

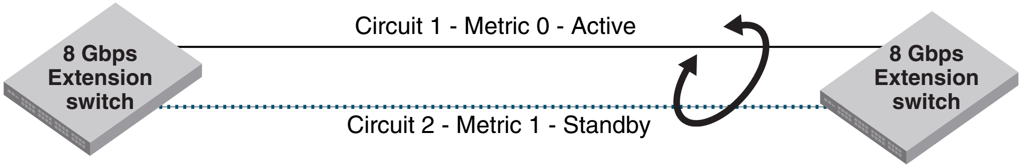


FIGURE 274 Failover to a higher metric standby circuit

Bandwidth calculation during failover

The bandwidth of higher metric circuits is not calculated as available bandwidth on an FCIP tunnel until all lowest metric circuits have failed. For example, assume the following:

- Circuits 0 and 1 are created with a metric of 0. Circuit 0 is created with a maximum transmission rate of 1 Gbps, and Circuit 1 is created with a maximum transmission rate of 500 Mbps. Together, Circuits 0 and 1 provide an available bandwidth of 1.5 Gbps.
- Circuits 2 and 3 are created with a metric of 1. Both are created with a maximum transmission rate of 1 Gbps, for a total of 2 Gbps. This bandwidth is held in reserve.
- If either circuit 0 or circuit 1 fails, traffic flows over the remaining circuit while the failed circuit is being recovered. The available bandwidth is still considered to be 1.5 Gbps.
- If both circuit 0 and circuit 1 fail, there is a failover to circuits 2 and 3, and the available bandwidth is updated as 2 Gbps.
- If a low metric circuit becomes available again, the high metric circuits go back to standby status, and the available bandwidth is updated again. For example, if circuit 0 is recovered, the available bandwidth is updated as 1 Gbps. If circuit 1 is also recovered, the available bandwidth is updated as 1.5 Gbps.

Adaptive Rate Limiting

Adaptive Rate Limiting (ARL) is performed on FCIP tunnel connections to change the rate in which the FCIP tunnel transmits data through the TCP connections. This feature is available only on the 8 Gbps extension switches and 8 Gbps Extension Blades. ARL uses information from the TCP connections to determine and adjust the rate limit for the FCIP tunnel dynamically. This allows FCIP connections to utilize the maximum available bandwidth while providing a minimum bandwidth guarantee.

ARL applies a minimum and maximum traffic rate, and allows the traffic demand and WAN connection quality to dynamically determine the rate. As traffic increases, the rate grows towards the maximum rate, and if traffic subsides, the rate reduces towards the minimum. If traffic is flowing error-free over the WAN, the rate grows towards the maximum rate. If TCP reports an increase in retransmissions, the rate reduces towards the minimum.

FSPF link cost calculation when ARL is used

Fabric Shortest Path First (FSPF) is a link state path selection protocol that directs traffic along the shortest path between the source and destination based upon the link cost. When ARL is used, The link cost is equal to the sum of maximum traffic rates of all established, currently active low metric circuits in the tunnel. The following formulas are used:

- If the bandwidth is greater than or equal to 2 Gbps, the link cost is 500.
- If the bandwidth is less than 2 Gbps, but greater than or equal to 1 Gbps, the link cost is 1000000 divided by the bandwidth.
- If the bandwidth is less than 1 Gbps, the link cost is 2000 minus the bandwidth

QoS SID/DID priorities over an FCIP trunk

QoS SID/DID traffic prioritization is a capability of Fabric OS Adaptive Networking licensed feature. This feature allows you to prioritize FC traffic flows between hosts and targets.

Four internal TCP connections provide internal circuits for managing QoS SID/DID priorities over an FCIP tunnel, as illustrated in Figure 275. The priorities are as follows:

- F class - F class is the highest priority, and is assigned bandwidth as needed at the expense of lower priorities, if necessary.
- QoS high - The QoS high priority gets at least 50% of the available bandwidth.
- QoS medium - The QoS medium priority gets at least 30% of the available bandwidth.
- QoS low - The QoS low priority gets at least 20% of the available bandwidth.

NOTE
The QoS high (50%), medium (30%), and low (20%) values are fixed for the 4 Gbps Extension Blade and cannot be configured. For 8 Gbps platforms, these are default values which you can change using procedures under “Configuring QoS Priorities” on page 635. These priorities are enforced only when there is congestion on the network. If there is no congestion, all traffic is handled at the same priority.

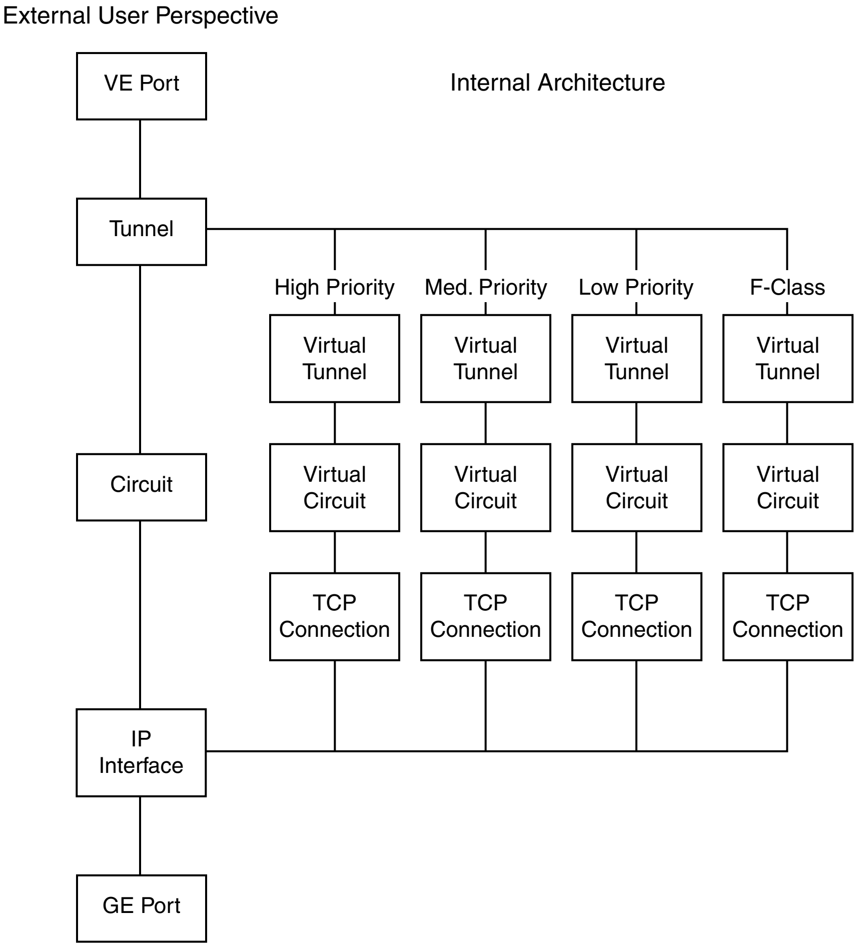


FIGURE 275 TCP connections for handling QoS SID/DID-based FC traffic prioritization

Configuring QoS Priorities

For 8 Gbps platforms only, you can change QoS priorities from the default settings using the following steps:

1. Select **Configure > FCIP Tunnels**.

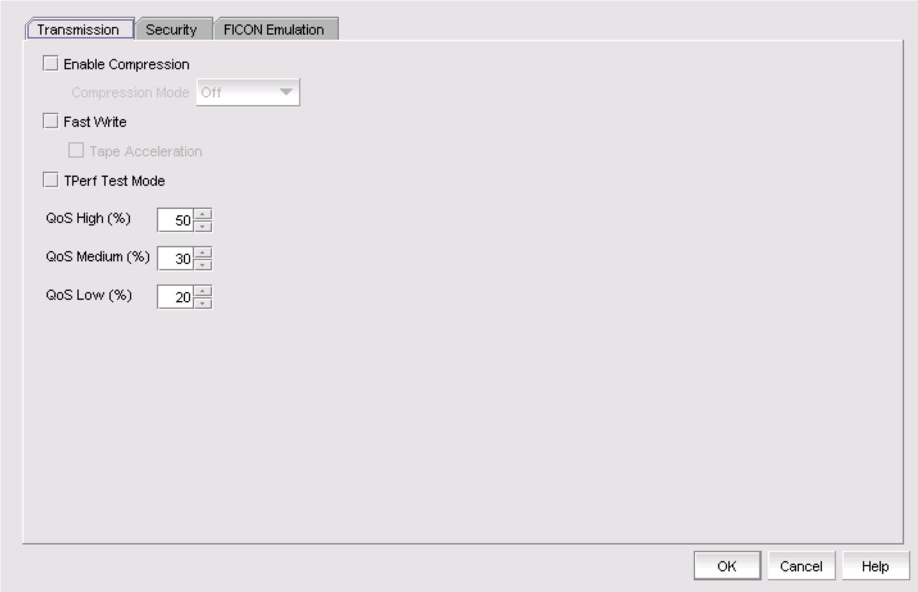
   The **FCIP Tunnels** dialog box is displayed. All discovered fabrics with extension switches are listed under devices, and all existing FCIP tunnels are displayed.

2. Select the switch you want to configure under **Products**.
3. Click the **Add** button, or right-click on the switch and select **Add Tunnel**.

   The **Add FCIP Tunnel** dialog box is displayed.

4. Click **Advanced Settings**.

The **Advanced Settings** dialog box is displayed. This dialog box has a **Transmission** tab, **Security** tab, and **FICON Emulation** tab. Configure QoS percentages on the **Transmission** tab (Figure 276).



☐ Enable Compression

Compression Mode: Off

☐ Fast Write

☐ Tape Acceleration

☐ TPerf Test Mode

QoS High (%): 50

QoS Medium (%): 30

QoS Low (%): 20

FIGURE 276 Advanced Settings Transmission Tab

5. Click the up or down arrows by QoS High, QoS Medium, and QoS Low to increment values by 1% and override the default values of 50% (high), 30% (medium), and 20% (low). The three values must equal 100%. A minimum of 10% is required for each level.

NOTE
Editing QoS values is a disruptive operation, so a warning message displays when you make changes.

IPsec and IKE implementation over FCIP

Internet Protocol security (IPsec) uses cryptographic security to ensure private, secure communications over Internet Protocol networks. IPsec supports network-level data integrity, data confidentiality, data origin authentication, and replay protection. It helps secure your SAN against network-based attacks from untrusted computers, attacks that can result in the denial-of-service of applications, services, or the network, data corruption, and data and user credential theft. IPsec does not require you to configure separate security for each application that uses TCP/IP.

When configuring for IPsec, however, you must ensure that the same policies are defined in the switches or blades at each end of the FCIP tunnel. IPsec works on FCIP tunnels with or without compression, FCIP Fastwrite, and tape acceleration. IPsec can only be created on tunnels using IPv4 addressing.

IPsec for the 4 Gbps platforms

IPsec uses some terms that you should be familiar with before beginning your configuration. These are standard terms, but are included here for your convenience.

Term	Definition
AES	Advanced Encryption Standard. FIPS 197 endorses the Rijndael encryption algorithm as the approved AES for use by US Government organizations and others to protect sensitive information. It replaces DES as the encryption standard.
AES-XCBC	Cipher Block Chaining. A key-dependent one-way hash function (MAC) used with AES in conjunction with the Cipher-Block-Chaining mode of operation, suitable for securing messages of varying lengths, such as IP datagrams.
AH	Authentication Header - like ESP, AH provides data integrity, data source authentication, and protection against replay attacks but does not provide confidentiality.
DES	Data Encryption Standard is the older encryption algorithm that uses a 56-bit key to encrypt blocks of 64-bit plain text. Because of the relatively shorter key length, it is not a secured algorithm and no longer approved for Federal use.
3DES	Triple DES is a more secure variant of DES. It uses three different 56-bit keys to encrypt blocks of 64-bit plain text. The algorithm is FIPS-approved for use by Federal agencies.
ESP	Encapsulating Security Payload is the IPsec protocol that provides confidentiality, data integrity and data source authentication of IP packets, and protection against replay attacks.
IKE	Internet Key Exchange is defined in RFC 2407, RFC 2408 and RFC 2409. IKEv2 is defined in RFC 4306. IKE uses a Diffie-Hellman key exchange to set up a shared session secret, from which cryptographic keys are derived and communicating parties are authenticated. The IKE protocol creates a security association (SA) for both parties.
MD5	Message Digest 5, like SHA-1, is a popular one-way hash function used for authentication and data integrity.
SHA	Secure Hash Algorithm, like MD5, is a popular one-way hash function used for authentication and data integrity.
MAC	Message Authentication Code is a key-dependent, one-way hash function used for generating and verifying authentication data.
HMAC	A stronger MAC because it is a keyed hash inside a keyed hash.
SA	Security Association is the collection of security parameters and authenticated keys that are negotiated between IPsec peers.

The following limitations apply to using IPsec:

- IPsec-specific statistics are not supported.
- To change the configuration of a secure tunnel, you must delete the tunnel and recreate it.
- There is no RAS message support for IPsec.
- IPsec can only be configured on IPv4 based tunnels.
- Secure Tunnels cannot be defined with VLAN Tagged connections.
- For the 4 Gbps Extension switch and Blade:
  - IPv6, NAT, and AH are not supported when IPsec is implemented.
  - You can only create a single secure tunnel on a port; you cannot create a nonsecure tunnel on the same port as a secure tunnel.
  - Jumbo frames are not supported.

IPSec for the 8 Gbps platforms

The 8 Gbps platforms use AES-GCM-ESP as a single, pre-defined mode of operation for protecting all TCP traffic over an FCIP tunnel. AES-GCM-ESP is described in RFC-4106. Key features are listed below:

- Encryption is provided by AES with 256 bit keys.
- The IKEv2 key exchange protocol is used by peer switches and blades for mutual authentication.
- IKEv2 uses UDP port 500 to communicate between the peer switches or blades.
- All IKE traffic is protected using AES-GCM-ESP encryption.
- Authentication requires the generation and configuration of 32 byte pre-shared secrets for each peer switch or blade.
- An SHA-512 hash message authentication code (HMAC) is used to check data integrity and detect third party tampering.
- PRF is used to strengthen security. The PRF algorithm generates output that appears to be random data, using the SHA-512 HMAC as the seed value.
- A 2048 bit Diffie-Hellman (DH) group is used for both IKEv2 and IPSec key generation.
- The SA lifetime limits the length of time a key is used. When the SA lifetime expires, a new key is generated, limiting the amount of time an attacker has to decipher a key. Depending on the length of time expired or the length of the data being transferred, parts of a message maybe protected by different keys generated as the SA lifetime expires. For the 8 Gbps Extension Switch and Blade, the SA lifetime is approximately eight hours, or two gigabytes of data, whichever occurs first.
- ESP is used as the transport mode. ESP uses a hash algorithm to calculate and verify an authentication value, and also encrypts the IP datagram.

QOS, DSCP, and VLANs

Quality of Service (QoS) refers to policies for handling differences in data traffic. These policies are based on data characteristics and delivery requirements. For example, ordinary data traffic is tolerant of delays and dropped packets, but voice and video data are not. QoS policies provide a framework for accommodating these differences in data as it passes through a network.

QoS for Fibre Channel traffic is provided through internal QoS priorities. Those priorities can be mapped to TCP/IP network priorities. There are two options for TCP/IP network-based QoS:

- Layer three DiffServ code Points (DSCP).
- VLAN tagging and Layer two class of service (L2CoS).

DSCP quality of service

Layer three class of service DiffServ Code Points (DSCP) refers to a specific implementation for establishing QoS policies as defined by RFC2475. DSCP uses six bits of the Type of Service (TOS) field in the IP header to establish up to 64 different values to associate with data traffic priority.

DSCP settings are useful only if IP routers are configured to enforce QoS policies uniformly within the network. IP routers use the DSCP value as an index into a Per Hop Behavior (PHB) table. Control connections and data connections may be configured with different DSCP values. Before configuring DSCP settings, determine if the IP network you are using implements PHB, and consult with your WAN administrator to determine the appropriate DSCP values.

VLANs and layer two quality of service

Devices in physical LANs are constrained by LAN boundaries. They are usually in close proximity to each other, and share the same broadcast and multicast domains. Physical LANs often contain devices and applications that have no logical relationship. Also, when logically related devices and applications reside in separate LAN domains, they must be routed from one domain to the other.

A VLAN is a virtual LAN network. A VLAN may reside within a single physical network, or it may span several physical networks. Related devices and applications that are separated by physical LAN boundaries can reside in the same VLAN. Also, a large physical network can be broken down into smaller VLANs. VLAN traffic is routed using 802.1Q-compliant tags within an Ethernet frame. The tag includes a unique VLAN ID, and Class of Service (CoS) priority bits. The CoS priority scheme (also called Layer two Class of Service or L2CoS), uses three Class of Service (CoS or 802.1P) priority bits, allowing eight priorities. Consult with your WAN administrator to determine usage.

When both DSCP and L2CoS are used

If an FCIP tunnel or circuit is VLAN tagged, both DSCP and L2CoS are relevant, unless the VLAN is end-to-end, with no intermediate hops in the IP network. The following table shows the default mapping of DSCP priorities to L2Cos priorities. This may be helpful when consulting with the WAN administrator. These values may be modified per FCIP tunnel.

TABLE 41 Default Mapping of DSCP priorities to L2Cos Priorities

DSCP priority/bits	L2CoS priority/bits	Assigned to:
46 / 101110	7 / 111	Class F
7 / 000111	1 / 001	Medium QoS
11 / 001011	3 / 011	Medium QoS
15 / 001111	3 / 011	Medium QoS
19 / 010011	3 / 011	Medium QoS
23 / 010111	3 / 011	Medium QoS
27 / 011011	0 / 000	Class 3 Multicast
31 / 011111	0 / 000	Broadcast/Multicast
35 / 100011	0 / 000	Low Qos
39 / 100111	0 / 000	Low Qos
43 / 101011	4 / 100	High QoS

TABLE 41 Default Mapping of DSCP priorities to L2Cos Priorities (Continued)

DSCP priority/bits	L2CoS priority/bits	Assigned to:
47 / 101111	4 / 100	High QoS
51 / 110011	4 / 100	High QoS
55 / 110111	4 / 100	High QoS
59 / 111011	4 / 100	High QoS
63 / 111111	0 / 000	-

Open systems tape pipelining

Open Systems Tape Pipelining (OSTP) can be used to enhance open systems SCSI tape write I/O performance. To implement OSTP over FCIP, you must enable the following two features:

- FCIP Fastwrite and Tape Acceleration.
- FC Fastwrite.

FCIP Fastwrite and Tape Acceleration

When the FCIP link is the slowest part of the network, consider using FCIP Fastwrite and Tape Read and Write Pipelining. FCIP Fastwrite and Tape Acceleration are two features that provide accelerated speeds for read and write I/O over FCIP tunnels in some configurations:

- FCIP Fastwrite accelerates the SCSI write I/Os over FCIP.
- Tape Acceleration accelerates SCSI read and write I/Os to sequential devices (such as tape drives) over FCIP, which reduces the number of round-trip times needed to complete the I/O over the IP network and speeds up the process. To use Tape Acceleration, you must also enable FCIP Fastwrite.

Both sides of an FCIP tunnel must have matching configurations for these features to work. FCIP Fastwrite and Tape Acceleration are enabled by turning them on during the tunnel configuration process. They are enabled on a per-FCIP tunnel basis.

Consider the constraints described in Table 42 when configuring tunnels to use OSTP.

TABLE 42 OSTP constraints

FCIP Fastwrite	Tape Acceleration
Each GbE port supports up to 2048 simultaneous accelerated exchanges, which means *a total of 2048 simultaneous exchanges combined* for Fastwrite and Tape Acceleration.	Each GbE port supports up to 2048 simultaneous accelerated exchanges, which means *a total of 2048 simultaneous exchanges combined* for Fastwrite and Tape Acceleration.
Does not natively support multiple equal-cost path configurations. Traffic isolation zoning can be used to support these configurations.	Does not natively support multiple equal-cost path configurations or multiple non-equal-cost path configurations. Traffic isolation zoning can be used to support these configurations.

TABLE 42 OSTP constraints

FCIP Fastwrite	Tape Acceleration
Class 3 traffic is accelerated with Fastwrite.	Class 3 traffic is accelerated between host and sequential device.
	With sequential devices (tape drives), there are 1024 initiator-tape (IT) pairs per GbE port, but 2048 initiator-tape-LUN (ITL) pairs per GbE port. The ITL pairs are shared among the IT pairs. For example: Two ITL pairs for each IT pair as long as the target has two LUNs. If a target has 32 LUNs, 32 ITL pairs for IT pairs. In this case, only 64 IT pairs are associated with ITL pairs. The rest of the IT pairs are not associated to any ITL pairs, so no Tape Acceleration is performed for those pairs. By default, only Fastwrite-based acceleration is performed on the unassociated pairs.
	Does not support multiple non-equal-cost path between host and sequential device

FICON emulation features

FICON emulation supports FICON traffic over IP WANs using FCIP as the underlying protocol. FICON emulation features support performance enhancements for specific applications. If you are using FCIP for distance extension in a FICON environment, evaluate the need for these features before you run the FCIP configuration wizard. FICON emulation may be configured by selecting **Advanced Settings** on the **Add Tunnel** or **Edit Tunnel** dialogs. The following features are available:

- IBM z/OS Global Mirror (z Gm) emulation.
- Tape write pipelining.
- Tape read pipelining.
- Teradata pipelining

IBM z/OS Global Mirror (z Gm) emulation

The IBM z/OS Global Mirror (z Gm) application, formerly known as eXtended Remote Copy (XRC), is a DASD application that implements disk mirroring, as supported by the disk hardware architecture and a host software component called System Data Mover (SDM). The primary volume and the secondary mirrored volume may be geographically distant across an IP WAN. The latency introduced by greater distance creates delays in anticipated responses to certain commands. The FICON pacing mechanism may interpret delays as an indication of a large data transfer that could monopolize a shared resource, and react by throttling the I/O. IBM z/OS Global Mirror (z Gm) emulation provides local responses to remote hosts, eliminating distance related delays. A FICON XRC Emulation License is required to enable IBM z/OS Global Mirror (z Gm) Emulation.

Tape write pipelining

FICON tape write pipelining improves performance for a variety of applications when writing to tape over extended distances. FICON tape write pipelining locally acknowledges write data records, enabling the host to generate more records while previous records are in transit across the IP WAN. If exception status is received from the device, the writing of data and emulation is terminated. The FICON Tape Emulation License is required to enable FICON Tape Write Pipelining.

Tape read pipelining

FICON tape read pipelining improves performance for certain applications when reading from FICON tape over extended distances. FICON tape read pipelining reads data from tape directly from the tape device. Reading of tape continues until a threshold is reached. The buffered data is forwarded to the host in response to requests from the host. When the host sends the status accept frame indicating that the data was delivered, the read processing on the device side credits the pipeline and requests more data from the tape. If exception status is received from the device, the reading of data and emulation is terminated. The FICON Tape Emulation License is required to enable FICON Tape Read Pipelining.

Teradata pipelining

Teradata emulation reduces latency on links to Teradata warehouse systems caused by WAN propagation delays and bandwidth restrictions. It accomplishes this by processing selected FICON commands for associated control, data, and status responses. FICON Teradata Emulation is supported between FICON Channels and FICON Teradata controllers. This feature is available only on 8 Gbps Extension Switch and Blade platforms operating with Fabric OS 6.4.1 and later.

Write pipelining

For write commands, control and status frames are generated for the host side of the WAN to pipeline write commands over the same or multiple exchanges.

Read pipelining

For read operations received by the device side of the WAN, a number of anticipatory read commands are generated and transferred to the device. The data and status associated with these commands are sent to the host side of the WAN and queued in anticipation of host-generated read commands.

FCIP configuration guidelines

FCIP configuration always involves two or more extension switches. The following should take place first before you configure a working FCIP connection from the Management application:

- The WAN link should be provisioned and tested for integrity.
- Cabling within the data center should be completed.
- Equipment should be physically installed and powered on.
- The Management application must have management port access to the extension switches.
- The Management application must be able to discover the fabrics the contain the extension switches.
- The extension switches should be physically connected to the IP network they will be using to pass data, and the connection should be active and working.
- Identify all the devices in the data path between the extension switches, including Ethernet switches, Ethernet routers, firewalls, and common carrier equipment. A network diagram is very helpful. Support engineers may ask you to provide a network diagram when troubleshooting problems.
- Routers and firewalls must be configured to pass ARP, ICMP, and IP layer 3 protocols.
- Persistently disable the VE_ports before you configure them. Ports on a new extension switch or extension blade are persistently disabled by default.
- Determine which features you are implementing, and gather the information needed to implement those features. Table 39 summarizes feature support per FCIP platform.

Virtual Port Types

Virtual ports may be defined as VE_Ports or VEX_Ports.

VE_Ports

VE_Ports (virtual E_Ports) are used to create interswitch links (ISLs) through an FCIP tunnel. If VE_Ports are used on both ends of an FCIP tunnel, the fabrics connected by the tunnel are merged.

VEX_Port

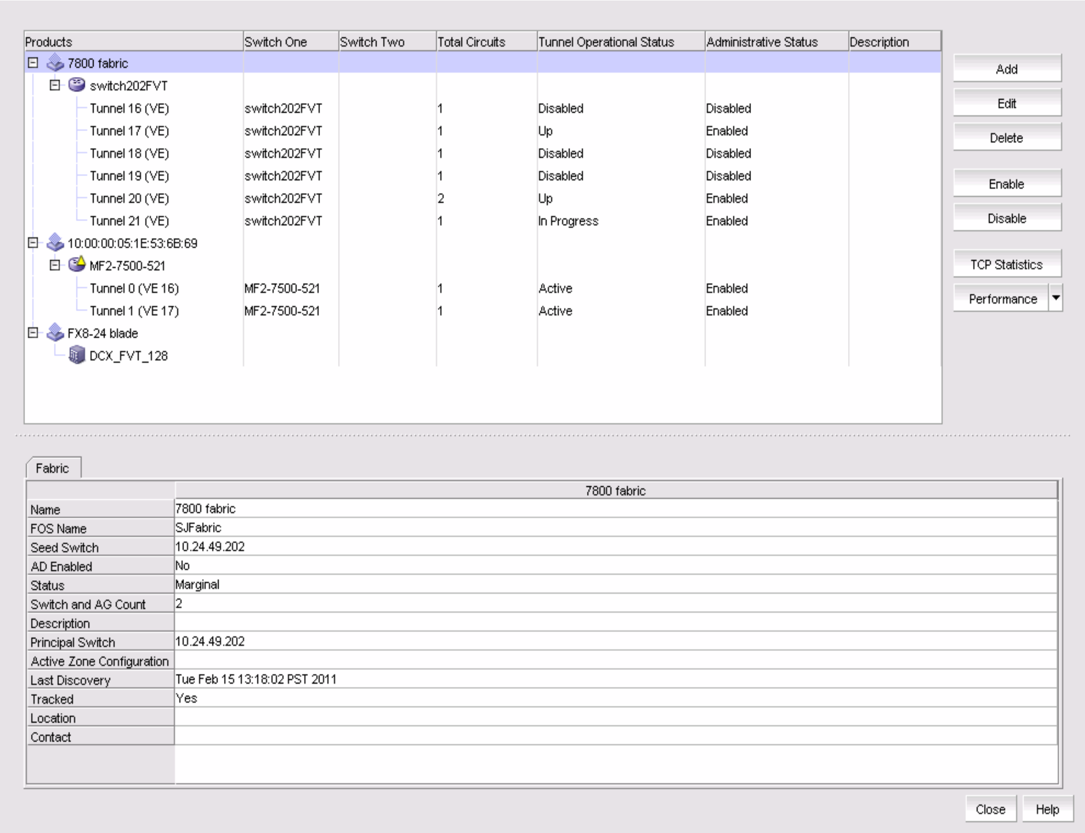
A VEX_Port enables FC-FC Routing Service functionality over an FCIP tunnel. VEX_Ports enable interfabric links (IFLs). If a VEX_Port is on one end of an FCIP tunnel, the fabrics connected by the tunnel are not merged. The other end of the tunnel must be defined as a VE_Port.

Configuring an FCIP tunnel

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

1. Select **Configure > FCIP Tunnels**.

   The **FCIP Tunnels** dialog box is displayed (Figure 277). All discovered fabrics with extension switches are listed under devices.



Products	Switch One	Switch Two	Total Circuits	Tunnel Operational Status	Administrative Status	Description
⊟ 7800 fabric						
⊟ switch202FVT						
Tunnel 16 (VE)	switch202FVT		1	Disabled	Disabled	
Tunnel 17 (VE)	switch202FVT		1	Up	Enabled	
Tunnel 18 (VE)	switch202FVT		1	Disabled	Disabled	
Tunnel 19 (VE)	switch202FVT		1	Disabled	Disabled	
Tunnel 20 (VE)	switch202FVT		2	Up	Enabled	
Tunnel 21 (VE)	switch202FVT		1	In Progress	Enabled	
⊟ 10:00:00:05:1E:53:6B:69						
⊟ MF2-7500-521						
Tunnel 0 (VE 16)	MF2-7500-521		1	Active	Enabled	
Tunnel 1 (VE 17)	MF2-7500-521		1	Active	Enabled	
⊟ FX8-24 blade						
DCX_FVT_128						

	7800 fabric
Name	7800 fabric
FOS Name	SJFabric
Seed Switch	10.24.49.202
AD Enabled	No
Status	Marginal
Switch and AG Count	2
Description	
Principal Switch	10.24.49.202
Active Zone Configuration	
Last Discovery	Tue Feb 15 13:18:02 PST 2011
Tracked	Yes
Location	
Contact	

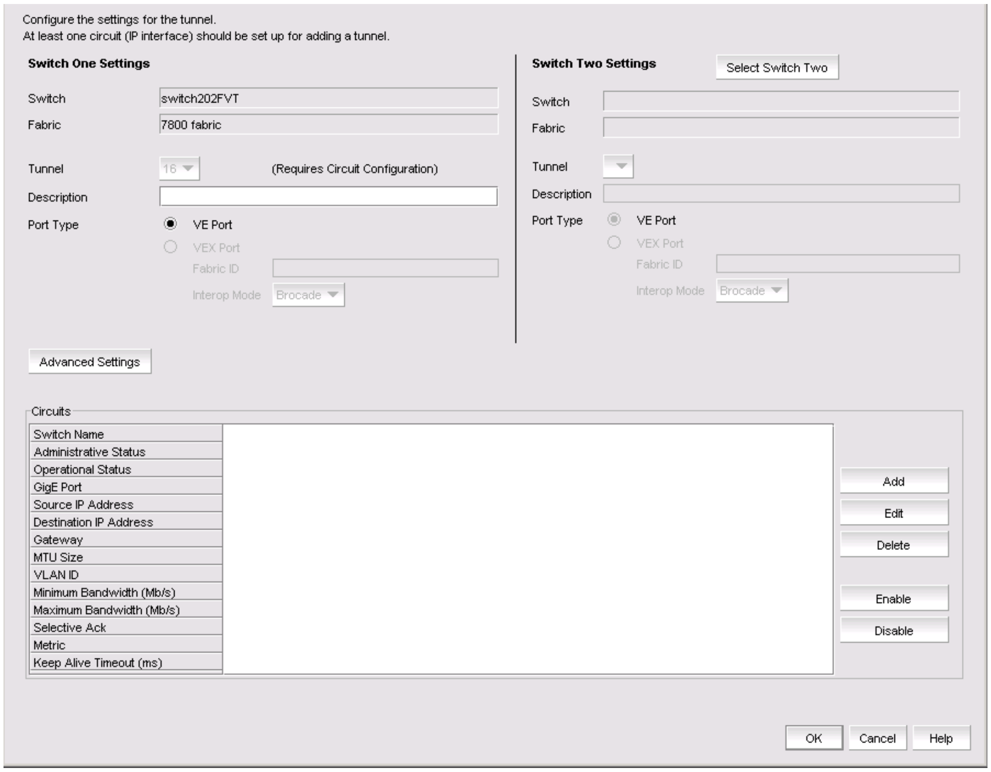
FIGURE 277 FCIP Tunnels dialog box (fabric selected from Product tree)

2. Select the switch you want to configure under the **Products** tree.

3. Click the **Add** button, or right-click on the switch and select **Add Tunnel**.

   The **Add FCIP Tunnel** dialog is displayed (Figure 278). The name of the switch you selected is displayed in the **Switch** field under **Switch One Settings**. This dialog allows you to configure settings for both switches on either end of the tunnel.

   A **Circuits** properties table displays at the bottom of the dialog box. For 8 Gbps platforms, this may contain columns for multiple circuits. Actual, as well as cached circuits display. You can configure circuits using the **Add**, **Edit**, **Delete**, **Enable**, and **Disable** circuits using the function buttons to the right of the table. For 4 Gbps platforms, the **Delete**, **Enable**, and **Disable** buttons do not display. In addition, the **Edit** operation is only supported for cached circuits.



Configure the settings for the tunnel.
At least one circuit (IP interface) should be set up for adding a tunnel.

Switch One Settings

Switch: switch202FVT
Fabric: 7800 fabric
Tunnel: 16 (Requires Circuit Configuration)
Description:
Port Type: ● VE Port ○ VEX Port
Fabric ID:
Interop Mode: Brocade

Switch Two Settings

Switch:
Fabric:
Tunnel:
Description:
Port Type: ● VE Port ○ VEX Port
Fabric ID:
Interop Mode: Brocade

FIGURE 278 Add FCIP Tunnel dialog box

4. Click **Select Switch Two** under **Switch Two Settings** to display discovered extension switches, and select the switch that you want to connect to switch one.

   The switch name and fabric are displayed in the **Switch** and **Fabric** fields.

5. Enter a description of the tunnel in the **Description** field.

NOTE
You cannot assign a **Tunnel ID** until after at least one circuit is configured. The **Add Circuit** dialog returns you to the **Add FCIP Tunnel** dialog to allow you to select the **Tunnel ID**.

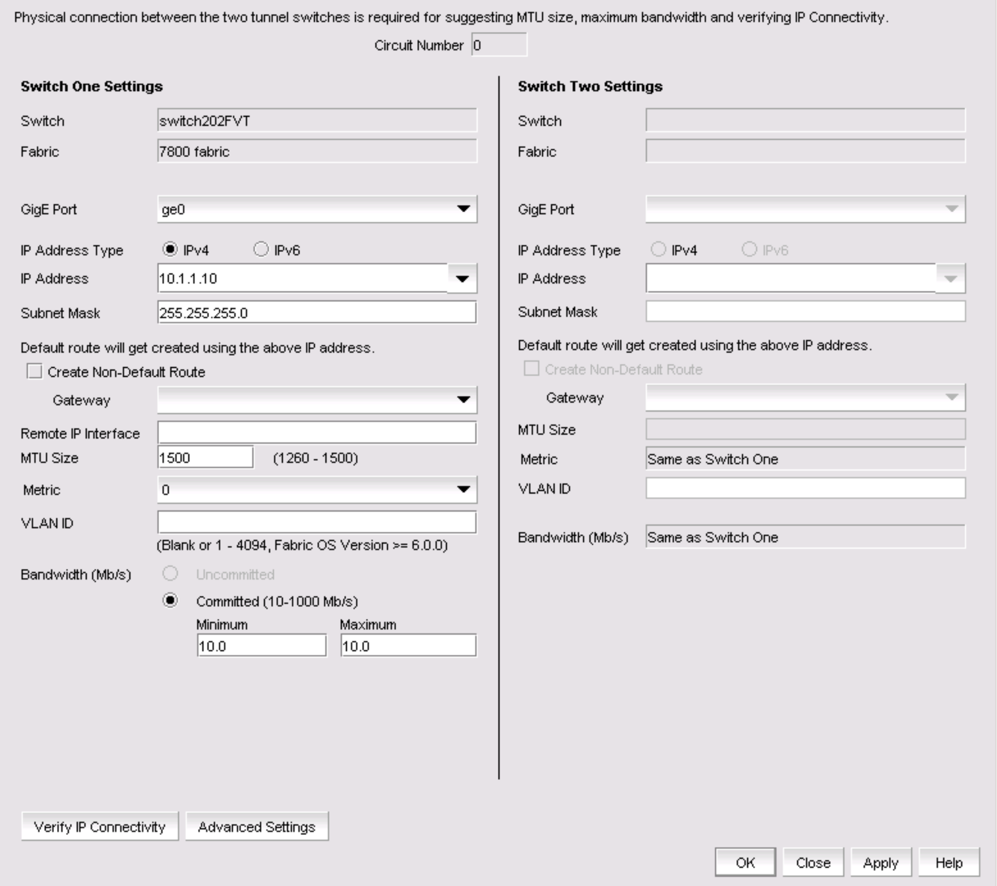
6. To add a circuit, click **Add** to the right of the **Circuits** properties table at the bottom of the dialog box.

   The **Add FCIP Circuit** dialog is displayed. Continue with “Adding an FCIP circuit”.

Adding an FCIP circuit

When adding a new FCIP tunnel, you can add an FCIP circuit by selecting the **Add** button to the right of the **Circuits** properties table on the **Add FCIP Tunnel** dialog box (Figure 278 on page 645). For 8 Gbps platforms, you can add multiple FCIP circuits to the tunnel with this button.

Add circuits to existing FCIP tunnels through the **Edit FCIP Tunnel** dialog box. To display this dialog box, right-click a tunnel on the **FCIP Tunnels** dialog box and select **Edit Tunnel** or select a tunnel and click the **Edit** button. For details, refer to “Editing FCIP tunnels” on page 660.



Physical connection between the two tunnel switches is required for suggesting MTU size, maximum bandwidth and verifying IP Connectivity.

Circuit Number: 0

Switch One Settings

Switch: switch202FVT
Fabric: 7800 fabric
GigE Port: ge0
IP Address Type: ● IPv4 ○ IPv6
IP Address: 10.1.1.10
Subnet Mask: 255.255.255.0
Default route will get created using the above IP address.
□ Create Non-Default Route
Gateway:
Remote IP Interface:
MTU Size: 1500 (1260 - 1500)
Metric: 0
VLAN ID:
(Blank or 1 - 4094, Fabric OS Version >= 6.0.0)
Bandwidth (Mb/s): ○ Uncommitted
● Committed (10-1000 Mb/s)
Minimum: 10.0 Maximum: 10.0

Switch Two Settings

Switch:
Fabric:
GigE Port:
IP Address Type: ○ IPv4 ○ IPv6
IP Address:
Subnet Mask:
Default route will get created using the above IP address.
□ Create Non-Default Route
Gateway:
MTU Size:
Metric: Same as Switch One
VLAN ID:
Bandwidth (Mb/s): Same as Switch One

FIGURE 279 Add FCIP Circuit dialog box

1. Select the **GiGE Port** used for the Ethernet connection on each switch. The choices available depend on the extension switch or blade model.
2. Select **Use as failover** to configure the 10 GbE port on an 8 Gbps Blade platform as a 10 Gbps lossless failover circuit.
3. Select the **IP Address Type**. The implementation is a dual IP layer operation implementation as described in RFC 4213. IPv6 addresses can exist with IPv4 addresses on the same interface, but the FCIP circuits must be configured as IPv6 to IPv6 and IPv4 to IPv4 connections. IPv6-to-IPv4 connections are not supported. Likewise, encapsulation of IPv4 in IPv6 and IPv6 in IPv4 is not supported.

4. Select the **IP Address** for each port. This implementation of IPv6 uses unicast addresses for the interfaces with FCIP circuits. The unicast address must follow the RFC 4291 IPv6 standard and use the IANA assigned IPv6 Global Unicast address space (2000::/3).

5. For IPv4 addresses, specify the **Subnet Mask**. For IPv6 addresses, specify the prefix length.

   The default is created from the IP address and Subnet Mask. If you want to create a route through a gateway router, click **Create Non-Default Rout**e, and select a **Gateway address**.

6. Enter the **MTU Size**.

   For SAN traffic, the largest possible MTU (Maximum Transmission Unit) size is generally the most efficient. Enter a value between 1260 and 2348 for the 4 Gbps platforms and between 1260 and 1500 for the 8 Gbps plaforms. MTU rates must match on both ends of the tunnel.

   If you have an active connection between switch one and switch two, click **Suggest** under **Switch One Settings**. To determine a suggested size, packets are sent across the FCIP tunnel, starting at the largest possible size packet that can be sent over IP. If a valid connection response is not received, a smaller packet is sent. This continues until a valid connection response is received, and that size becomes the suggested MTU. MTU settings must match at both ends of the tunnel, and the setting specified under **Switch One Settings** is automatically applied to switch two.

   NOTE
   Suggest button function requires and active IP connection. The button is not available for the **Add FCIP Circuit** and **Edit FCIP Circuit** dialog boxes for 8 Gbps Extension platforms.

7. If a VLAN ID is used to route frames between the switches over the physical connection, enter the **VLAN ID** under **Switch One Settings**. You must assign the VLAN ID to both switches. You can assign the same or different VLAN IDs to each switch.

   The VLAN ID is an integer value between 1 and 4094 which sets the VLAN tag value in the header assigning the traffic to that specific VLAN. Layer two class of service (L2CoS) values may be assigned to establish traffic priorities over a VLAN. This is done as an **Advanced Setting**.

8. The **Metric** option is used to identify a failover circuit. By assigning a non-zero metric (1), you identify the circuit as a failover circuit. By default, a circuit is assigned a metric of 0. If a circuit fails, FCIP trunking tries first to retransmit any pending send traffic over another circuit with a metric of 0. If no circuits with a metric of 0 are available, then the pending send traffic is retransmitted over any available circuit with a metric of 1.

   The default metric value for a crossport circuit configuration will be 1. If a failover circuit is created with a metric of 0, it will be used for load balancing and not for failover.

9. Select values for bandwidth settings. An uncommitted bandwidth is not allowed on an FCIP circuit. You must select **Committed bandwidth**. If you want to use ARL, set **Minimum** and **Maximum** bandwidth values. Bandwidth grows towards the maximum and reduces towards the minimum based on traffic conditions. If you do not want to use ARL, set **Minimum** and **Maximum** to the same value to set a single committed bandwidth. Refer to "Adaptive Rate Limiting" on page 633 for more information about ARL.

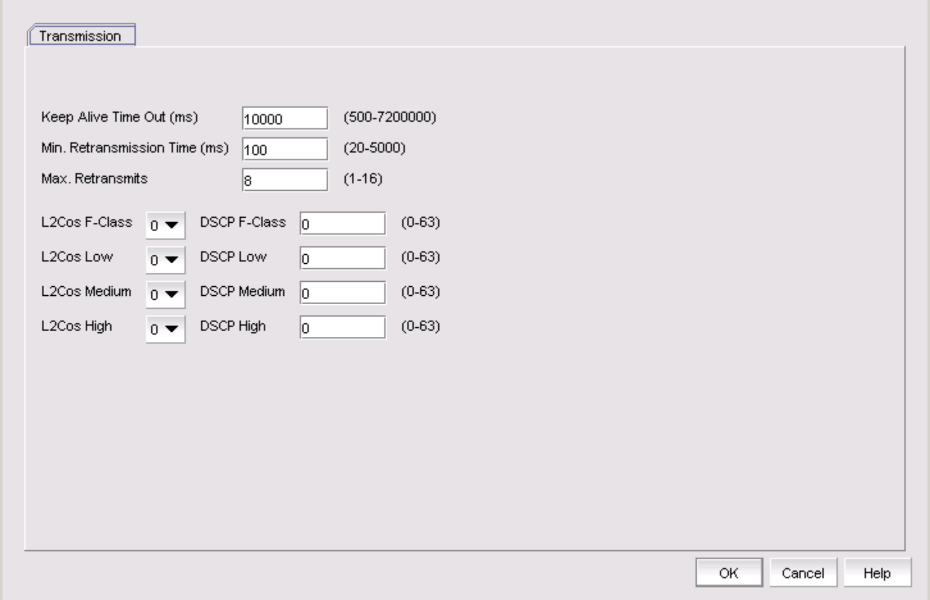
   NOTE
   The committed value range in the **Add FCIP Circuit** dialog box depends on the extension switch or blade platform.

10. If the physical connection exists, click **Verify IP Connectivity** to test the connection between switch one and switch two. The IP connectivity of the connection is tested with the ping utility.

11. Select **Advanced Settings** and continue if you want to do any of the following:

    - Set the keep alive timeout to a value other than the default of 10 seconds.
    - Set the minimum retransmission time to a value other than the default of 100 ms.
    - Set the maximum retransmits to a value other than the default.
    - Use TCP/IP DSCP or L2CoS to prioritize FC traffic.

    If you select **Advanced Settings**, the **Transmission tab** of the **FCIP Circuit Advanced Settings** dialog box displays (Figure 280).



Keep Alive Time Out (ms) 10000 (500-7200000)
Min. Retransmission Time (ms) 100 (20-5000)
Max. Retransmits 8 (1-16)

L2Cos F-Class 0 DSCP F-Class 0 (0-63)
L2Cos Low 0 DSCP Low 0 (0-63)
L2Cos Medium 0 DSCP Medium 0 (0-63)
L2Cos High 0 DSCP High 0 (0-63)

FIGURE 280 FCIP Circuit Advanced Settings

- Use the **Keep Alive Time Out (ms)** option to override the default value of 10000 ms. As shown, the range is from 500 to 7200000.
- Use the **Max. Retransmission Time (ms)** option to override the default value of 100 ms.
- Use the **Max. Retransmits** option to override the default value of 8. As shown, the range is 1 to 8.
- Select **L2CoS** and **DSCP** priorities. Refer to "QOS, DSCP, and VLANs" on page 638 for more information.
- Select **OK** to save the settings and close the dialog box.

12. Click **Apply** on the **Add FCIP Circuit** dialog box to add the circuit and leave the dialog box open to add additional circuits. Click **OK** to add the circuit and close the dialog box.

13. Click **OK** to close the **Add FCIP Tunnel** dialog box.

Circuit configuration failure

When a tunnel cannot be created because the process for adding a new circuit configuration fails, a **FCIP Tunnel/Circuit Configurations** dialog box displays. Using this dialog box, you can perform the following tasks:

- Roll back the current changes to the circuit configuration.
- Elect to not roll back current circuit configuration changes.
- Continue configuring additional circuits at this point.
- Stop configuring additional circuits.

Configuring FCIP tunnel advanced settings

Compression, FCIP fast write and tape pipelining, IPSec and IKE policies, and FICON emulation features are configured as advanced settings.

1. Click **Advanced Settings** on the **Add FCIP Tunnel** dialog box.

   The **Advanced Settings** dialog box is displayed. This dialog box has a **Transmission** tab, **Security** tab, and **FICON Emulation** tab.

2. Click **OK** to close **Advanced Settings** when you have configured the features that you want to implement.
3. Click **OK** to close the **Add FCIP Tunnel** dialog box.

Enabling and disabling compression

Data compression can improve performance on long distance connections. The procedure for enabling compression for the 4 Gbps Extension Switch and Blade is different than the procedure for enabling compression for the 8 Gbps Extension Switch and Extension Blade.

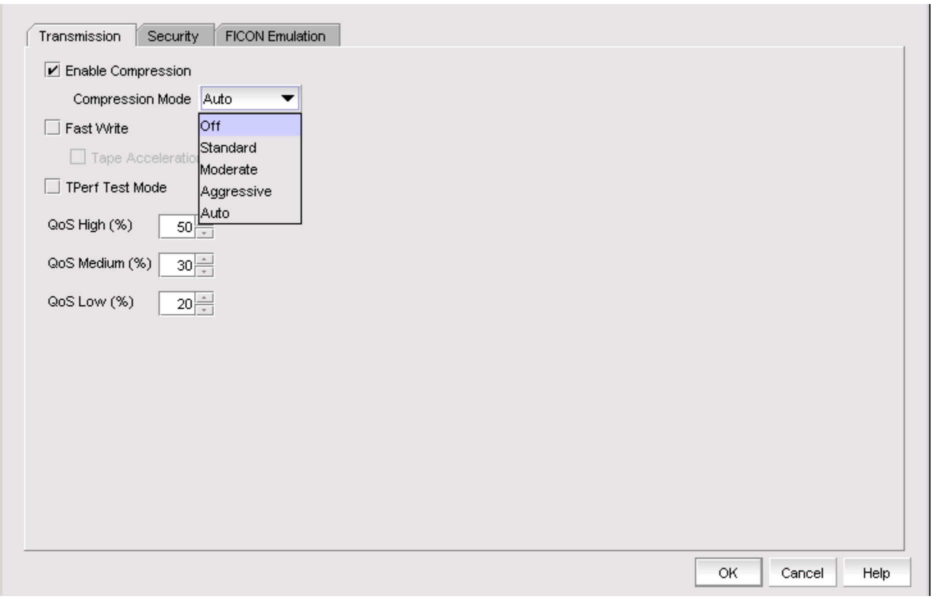
For 4 Gbps Extension Switch and Blade:

1. Select **Advanced Settings** on the **Add FCIP Tunnel** dialog box to display the **Advanced Settings** dialog box.
2. From the **Transmission** tab, select the **Enable Compression** check box to enable compression.
3. Click **OK** to commit your selection.

For the 8 Gbps Extension Switch and 8 Gbps Extension Blade:

1. Select Advanced Settings on the **Add FCIP Tunnel** dialog box to display the **Advanced Settings** dialog box.
2. From the **Transmission** tab, select the **Enable Compression** check box to enable compression.

   This enables the **Compression Mode** selector (Figure 281).



☑ Enable Compression

Compression Mode Auto

□ Fast Write

□ Tape Acceleratio

□ TPerf Test Mode

QoS High (%) 50

QoS Medium (%) 30

QoS Low (%) 20

FIGURE 281 Selecting a compression mode

3. Select the desired compression mode.

   A **Standard** option provides hardware compression and is available on all platforms. The 8 Gbps Extension Switch and the 8 Gbps Extension Blade provide three additional options for compression. The **Moderate** option enables a combination of hardware and software compression that provides more compression that hardware compression alone. This option supports up to 8 Gbps of FC traffic. the **Aggressive** option is a software only compression option that provides a more aggressive algorithm. This option supports up to 2.5 Gbps of FC traffic. The **Auto** option allows the system to set the best compression mode based on the tunnel's configured bandwidth and the bandwidth of all tunnels in the system.

4. Click **OK** to commit you selection.

To disable compression, click the **Enable Compression** to clear the check mark, and click **OK.**

Enabling Open Systems Tape Pipelining (OSTP)

Latency introduced by a long distance IP connection can negatively impact tape I/O performance. OSTP may be used to improve performance on SCSI write I/Os to sequential devices (such as tape drives). When OSTP is used, the extension blades or switches emulate write commands and responses locally to reduce delays caused by latency. Both sides of an FCIP tunnel must have matching configurations for these features to work. OSTP may be configured by selecting **Advanced Settings** on the **Add FCIP Tunnel** dialog. OSTP options are available on the **Transmission** tab.

To enable OSTP, do the following:

1. Select **Advanced Settings** on the **Add FCIP Tunnel** dialog box to display the **Advanced Settings** dialog box.

2. From the **Transmission** tab, select the **Fast Write** check box.

   This enables the **Tape Acceleration** check box.

3. Select the **Tape Acceleration** check box.
4. Click **OK**.

Enabling Tperf test mode

To enable Tperf test mode, do the following:

1. Select **Advanced Settings** on the **Add FCIP Tunnel** dialog box to display the **Advanced Settings** dialog box.
2. From the **Transmission** tab, select the **TPerf Test Mode** check box.
3. Select the **Tape Acceleration** check box.
4. Click **OK**.

Tperf test mode should not be enabled during normal operations. It is only used for testing and troubleshooting tunnels. Refer to the *Fabric OS FCIP Administrator's Guide* for information about Tperf.

Configuring QoS percentages

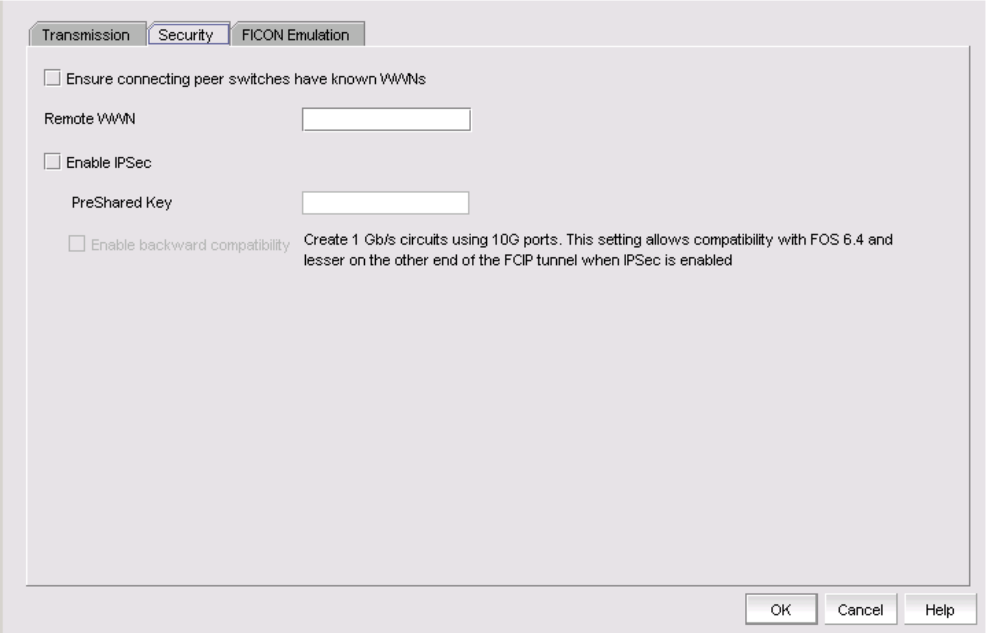
For 8 Gbps platforms, you can adjust QoS (Quality of Service) priority percentages from the preset default values of 50% (High), 30% (Medium), and 20% (low). Values for the three priority levels must equal 100%. A minimum of 10% is required for each level. You can adjust percentages in increments of 1%. To configure QoS percentages, do the following:

1. Select **Advanced Settings** on the **Add FCIP Tunnel** dialog box to display the **Advanced Settings** dialog box.
2. From the **Transmission** tab, click the up and down arrows by the **QoS (High)**, **QoS (Medium)**, and **QoS (Low)** percentage values to increase and decrease values.

Configuring IPSec and IKE policies

IPSec and IKE policies are configured from the **Security** tab. The screens and procedures are platform-dependent. Figure 282 on page 652 shows the screen for the 8 Gbps Extension Switch and 8 Gbps Extension Blade.

1. Select **Advanced Settings** on the **Add FCIP Tunnel** dialog box to display the **Advanced Settings** dialog box.
2. Select the **Security** tab.



□ Ensure connecting peer switches have known WWNs

Remote WWN

□ Enable IPSec

PreShared Key

□ Enable backward compatibility

Create 1 Gb/s circuits using 10G ports. This setting allows compatibility with FOS 6.4 and lesser on the other end of the FCIP tunnel when IPSec is enabled

FIGURE 282 Advanced Settings Security Tab for the 8 Gbps extension Switch and Blade

3. As an option, click **Ensure connecting peer switches have known WWNs**. This provides an added measure of security.
4. Enter the WWN for the remote switch.
5. Assign IKE and IPsec policies. For the 4 Gbps Extension Switch and Blade, you must choose from a drop-down list of policies. The 8 Gbps Extension Switch and Blade have predefined IKE and IPsec policies. These policies are enabled by selecting the **Enable IPSec** check box. Matching policies are applied to the remote switch. Note that the **Enable IPSec** check box is grayed while editing the tunnels because the IPsec settings cannot be edited for the secured tunnels.

NOTE
IPSec settings cannot be edited. If you want to change settings, you will need to delete the tunnel and then create a new tunnel with the new settings.

6. In the **PreShared Key** field, specify the key for IKE authentication. Use the following specifications, depending on your extension platform.
   - For the 4 Gbps Extension Switch and Blade and the 8 Gbps Extension Blade, the key value must be between 12 and 32 alphanumeric characters. The length depends on the chosen IKE policy.
   - For the 8Gbps Extension switch, the key value must be a minimum of 32 alphanumeric characters.

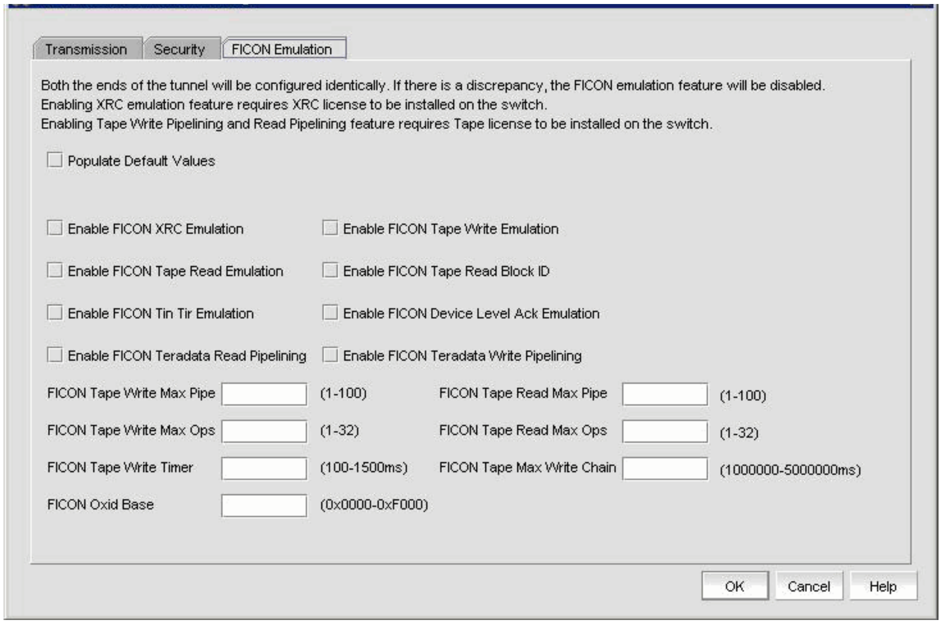
   These policies are used to make the connection more secure through authentication and encryption. When you select a policy for the local switch, a matching policy is automatically selected on the remote switch. If no matching policy is found, you must manually configure the policy on the remote switch.

7. You can activate the **Enable backward compatibility feature** on 8 Gbps platforms if IPSec is enabled. This allows multiple 1 Gbps circuits to be created using 10 Gbps ports even if the switch at one end of the tunnel is using Fabric OS 7.0 and the switch at the other end is using Fabric OS 7.0. Note that this feature can only be enabled when IPSec is enabled and when circuits are configured without any advanced 10 Gbps features, such as lossless failover, multi-gigabit circuits, or 10 Gbps Adaptive Rate Limiting (ARL).

Configuring FICON emulation

FICON emulation and acceleration features and operating parameters are configured from the **FICON Emulation** tab (Figure 283). Before you configure these features you must decide which features you want to implement, and you must look closely at the operational parameters to determine if values other than the default values are better for your installation.

1. Select **Advanced Settings** on the **Add FCIP Tunnel** dialog box to display the **Advanced Settings** dialog box.
2. Select the **FICON Emulation** tab.



Both the ends of the tunnel will be configured identically. If there is a discrepancy, the FICON emulation feature will be disabled.
Enabling XRC emulation feature requires XRC license to be installed on the switch.
Enabling Tape Write Pipelining and Read Pipelining feature requires Tape license to be installed on the switch.

☐ Populate Default Values

☐ Enable FICON XRC Emulation ☐ Enable FICON Tape Write Emulation
☐ Enable FICON Tape Read Emulation ☐ Enable FICON Tape Read Block ID
☐ Enable FICON Tin Tir Emulation ☐ Enable FICON Device Level Ack Emulation
☐ Enable FICON Teradata Read Pipelining ☐ Enable FICON Teradata Write Pipelining

FICON Tape Write Max Pipe		(1-100)	FICON Tape Read Max Pipe		(1-100)
FICON Tape Write Max Ops		(1-32)	FICON Tape Read Max Ops		(1-32)
FICON Tape Write Timer		(100-1500ms)	FICON Tape Max Write Chain		(1000000-5000000ms)
FICON Oxid Base		(0x0000-0xF000)			

FIGURE 283 Advanced Settings FICON Emulation Tab

3. Select the check boxes for the FICON emulation features you want to implement.

   The primary FICON emulation features are FICON XRC Emulation (IBM z/OS Global Mirror emulation), tape write pipelining, tape read pipelining, TIN/TUR emulation and device level ACK emulation provide support for the primary features. If you select any of the primary features, you must also select TIN/TUR emulation and device level ACK emulation.

   For 8 Gbps platforms operating with Fabric OS 6.4.1 and later, you can also enable FICON Teradata read pipelining and FICON Teradata write pipelining.

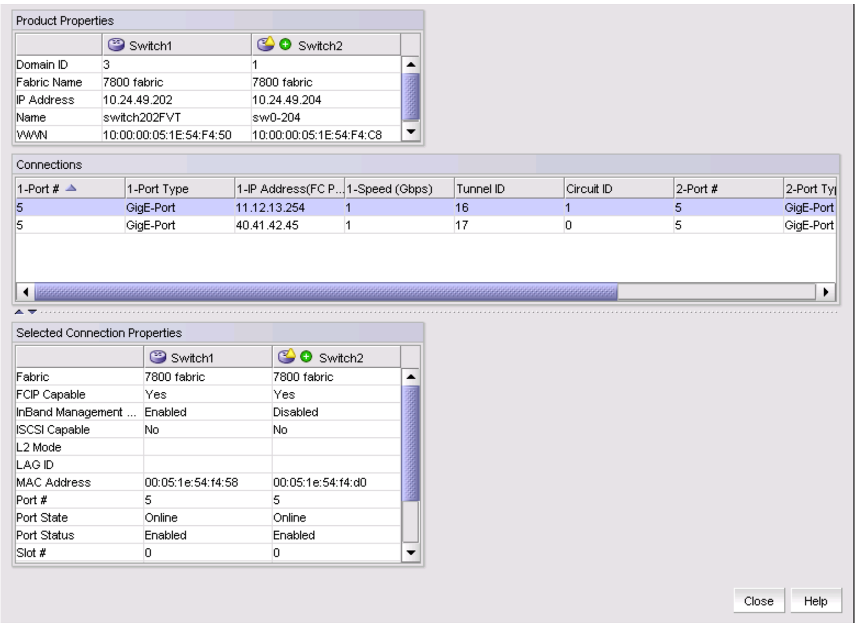
4. Select **Populate Default Values** at the top of the dialog box to set all operational parameters for FICON emulation to default values. This option is not be enabled if existing values are configured for the tunnel.

5. Select individual operational parameters for FICON emulation.

   - FICON Tape Write Max Pipe defines a maximum number of channel commands that may be outstanding at a given time during write pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The range is 1-100.
   - FICON Tape Read Max Pipe defines a maximum number of channel commands that may be outstanding at a given time during read pipelining. Too small of a value will result in poor performance. The value should be chosen carefully based upon the typical tape channel program that requires optimum performance. The range is 1-100.
   - FICON Tape Write Max Ops defines a maximum number of concurrent emulated tape write operations. The range is 1-32.
   - FICON Tape Read Max Ops defines a maximum number of concurrent emulated tape read operations. The range is 1-32.
   - FICON Tape Write Timer defines a time limit for pipelined write chains. This value is be specified in milliseconds (ms). If a pipelined write chain takes longer than this value to complete, the ending status for the next write chain will be withheld from the channel. This limits processing to what the network and device can support. Too small a value limits pipelining performance. Too large a value results in too much data being accepted for one device on a path. The range is 100-1500.
   - FICON Tape Max Write Chain defines the maximum amount of data that can be contained in a single CCW chain. If this value is exceeded, emulation is suspended. The range is 1,000,000 to 5,000,000 ms.
   - FICON Oxid Base defines the base value of an entry pool of 256 OXIDs supplied to emulation generated exchanges. It should fall outside the range used by FICON channels and devices to avoid conflicts. The range is 0x0000 to 0xF000.

Viewing FCIP connection properties

The FCIP connection properties show properties of the blades or switches on both sides of a connection. To view FCIP connection properties, right-click the connection between two extension blades or switches (Figure 284).



Product Properties

	Switch1	Switch2
Domain ID	3	1
Fabric Name	7800 fabric	7800 fabric
IP Address	10.24.49.202	10.24.49.204
Name	switch202FVT	sw0-204
WWN	10:00:00:05:1E:54:F4:50	10:00:00:05:1E:54:F4:C8

Connections

1-Port #	1-Port Type	1-IP Address(FC P...	1-Speed (Gbps)	Tunnel ID	Circuit ID	2-Port #	2-Port Ty
5	GigE-Port	11.12.13.254	1	16	1	5	GigE-Port
5	GigE-Port	40.41.42.45	1	17	0	5	GigE-Port

Selected Connection Properties

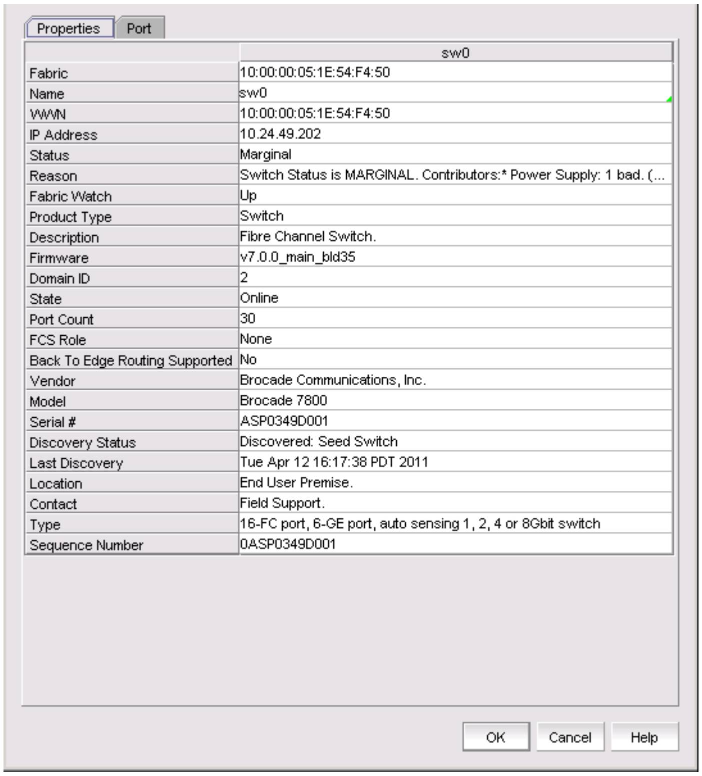
	Switch1	Switch2
Fabric	7800 fabric	7800 fabric
FCIP Capable	Yes	Yes
InBand Management ...	Enabled	Disabled
ISCSI Capable	No	No
L2 Mode		
LAG ID		
MAC Address	00:05:1e:54:f4:58	00:05:1e:54:f4:d0
Port #	5	5
Port State	Online	Online
Port Status	Enabled	Enabled
Slot #	0	0

FIGURE 284 FCIP connection properties

Viewing General FCIP properties

Use the following steps to view general FCIP properties for a switch or blade.

1. Right click an extension blade or switch from the Fabric Tree structure or on the Connectivity Map, and select **Properties**.
2. Select the **Properties** tab.

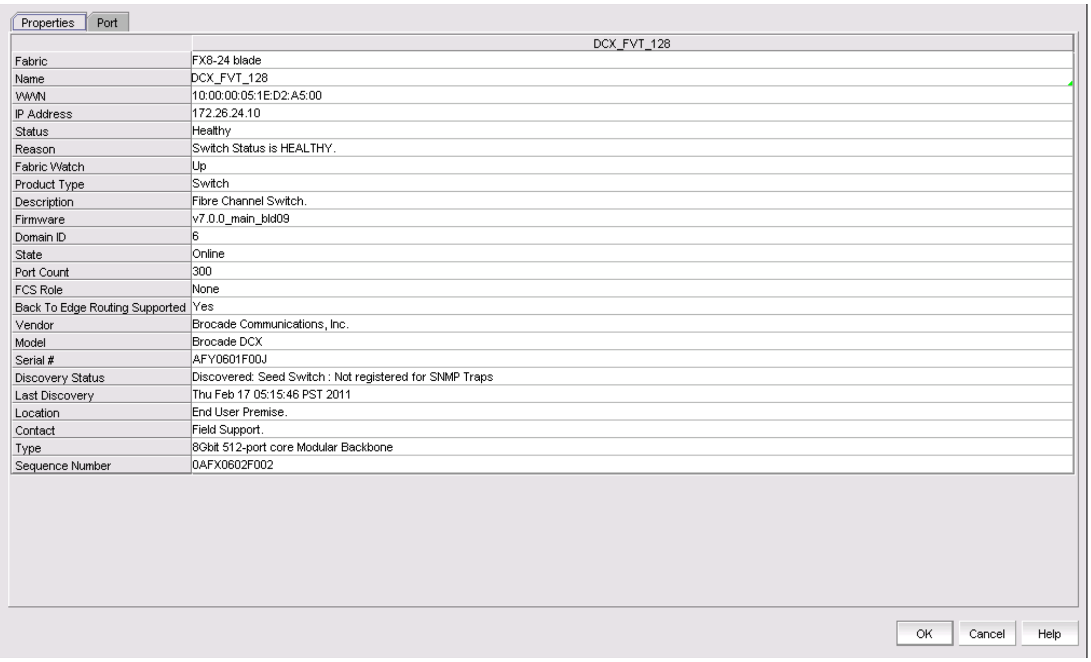


	sw0
Fabric	10:00:00:05:1E:54:F4:50
Name	sw0
WWN	10:00:00:05:1E:54:F4:50
IP Address	10.24.49.202
Status	Marginal
Reason	Switch Status is MARGINAL. Contributors:* Power Supply: 1 bad. (...
Fabric Watch	Up
Product Type	Switch
Description	Fibre Channel Switch.
Firmware	v7.0.0_main_bld35
Domain ID	2
State	Online
Port Count	30
FCS Role	None
Back To Edge Routing Supported	No
Vendor	Brocade Communications, Inc.
Model	Brocade 7800
Serial #	ASP0349D001
Discovery Status	Discovered: Seed Switch
Last Discovery	Tue Apr 12 16:17:38 PDT 2011
Location	End User Premise.
Contact	Field Support.
Type	16-FC port, 6-GE port, auto sensing 1, 2, 4 or 8Gbit switch
Sequence Number	0ASP0349D001

FIGURE 285 General FCIP properties tab (Extension switch or blade)

Use the following steps to view the properties of a chassis where an extension blade is installed.

1. Right click the chassis in the Switch group in Fabric Tree structure or on the Connectivity Map where the extension blade is installed, and select **Properties**.
2. Select the **Properties** tab.



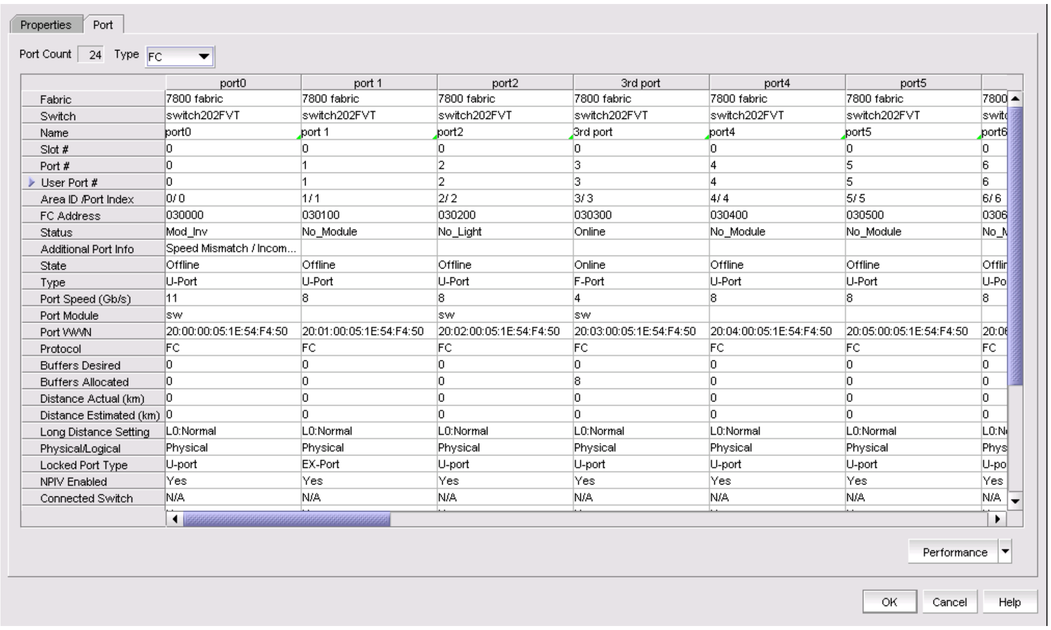
	DCX_FVT_128
Fabric	FX8-24 blade
Name	DCX_FVT_128
WWN	10:00:00:05:1E:D2:A5:00
IP Address	172.26.24.10
Status	Healthy
Reason	Switch Status is HEALTHY.
Fabric Watch	Up
Product Type	Switch
Description	Fibre Channel Switch.
Firmware	v7.0.0_main_bld09
Domain ID	6
State	Online
Port Count	300
FCS Role	None
Back To Edge Routing Supported	Yes
Vendor	Brocade Communications, Inc.
Model	Brocade DCX
Serial #	AFY0601F00J
Discovery Status	Discovered: Seed Switch : Not registered for SNMP Traps
Last Discovery	Thu Feb 17 05:15:46 PST 2011
Location	End User Premise.
Contact	Field Support.
Type	8Gbit 512-port core Modular Backbone
Sequence Number	0AFX0602F002

FIGURE 286 General FCIP properties tab (blade chassis)

Viewing FCIP FC port properties

Take the following steps to view FCIP FC port properties.

1. Right click an extension blade or switch from the Fabric Tree structure or on the Connectivity Map, and select **Properties**.
2. Select the **Port** tab.
3. Select the **FC** from the **Type** drop-down list (Figure 288).



Port Count 24 Type FC

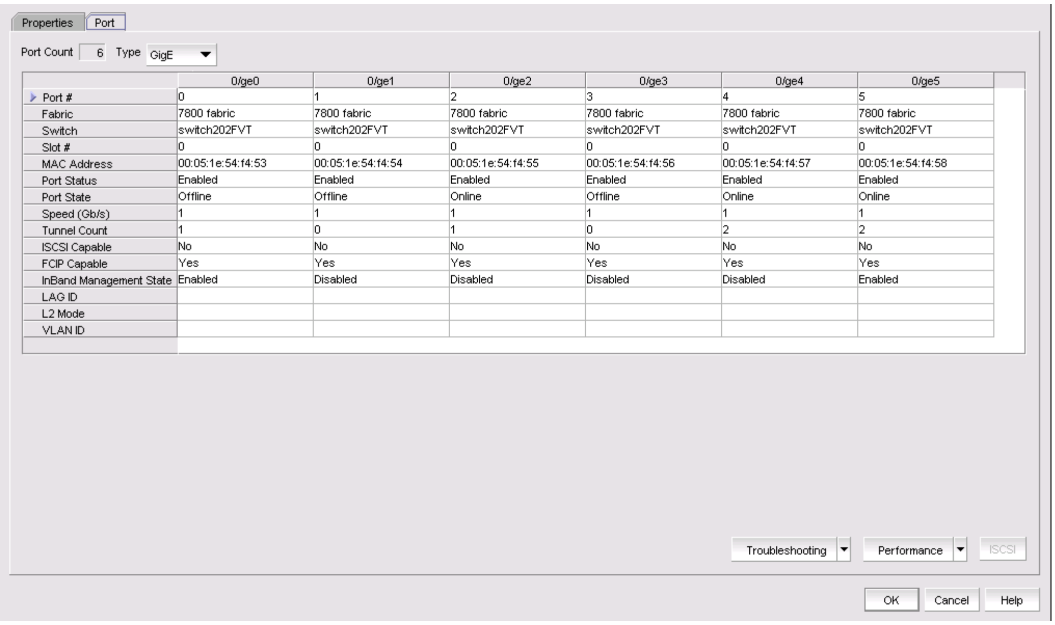
	port0	port 1	port2	3rd port	port4	port5	
Fabric	7800 fabric	7800 fabric	7800 fabric	7800 fabric	7800 fabric	7800 fabric	7800
Switch	switch202FVT	switch202FVT	switch202FVT	switch202FVT	switch202FVT	switch202FVT	switc
Name	port0	port 1	port2	3rd port	port4	port5	port6
Slot #	0	0	0	0	0	0	0
Port #	0	1	2	3	4	5	6
User Port #	0	1	2	3	4	5	6
Area ID /Port Index	0/ 0	1/ 1	2/ 2	3/ 3	4/ 4	5/ 5	6/ 6
FC Address	030000	030100	030200	030300	030400	030500	0306
Status	Mod_Inv	No_Module	No_Light	Online	No_Module	No_Module	No_N
Additional Port Info	Speed Mismatch / Incom...						
State	Offline	Offline	Offline	Online	Offline	Offline	Offlin
Type	U-Port	U-Port	U-Port	F-Port	U-Port	U-Port	U-Po
Port Speed (Gb/s)	11	8	8	4	8	8	8
Port Module	sw		sw	sw			
Port WWN	20:00:00:05:1E:54:F4:50	20:01:00:05:1E:54:F4:50	20:02:00:05:1E:54:F4:50	20:03:00:05:1E:54:F4:50	20:04:00:05:1E:54:F4:50	20:05:00:05:1E:54:F4:50	20:06
Protocol	FC	FC	FC	FC	FC	FC	FC
Buffers Desired	0	0	0	0	0	0	0
Buffers Allocated	0	0	0	8	0	0	0
Distance Actual (km)	0	0	0	0	0	0	0
Distance Estimated (km)	0	0	0	0	0	0	0
Long Distance Setting	L0:Normal	L0:Normal	L0:Normal	L0:Normal	L0:Normal	L0:Normal	L0:N
Physical/Logical	Physical	Physical	Physical	Physical	Physical	Physical	Phys
Locked Port Type	U-port	EX-Port	U-port	U-port	U-port	U-port	U-po
NPIV Enabled	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Connected Switch	N/A	N/A	N/A	N/A	N/A	N/A	N/A

FIGURE 287 FC ports properties

Viewing FCIP Ethernet port properties

Take the following steps to view Ethernet port properties.

1. Right click an extension blade or switch from the Fabric Tree structure or on the Connectivity Map, and select **Properties**.
2. Select the **Port** tab.
3. Select the **GigE** from the **Type** drop-down list (Figure 288).



Port Count 6 Type GigE

	0/ge0	0/ge1	0/ge2	0/ge3	0/ge4	0/ge5
Port #	0	1	2	3	4	5
Fabric	7800 fabric	7800 fabric	7800 fabric	7800 fabric	7800 fabric	7800 fabric
Switch	switch202FVT	switch202FVT	switch202FVT	switch202FVT	switch202FVT	switch202FVT
Slot #	0	0	0	0	0	0
MAC Address	00:05:1e:54:f4:53	00:05:1e:54:f4:54	00:05:1e:54:f4:55	00:05:1e:54:f4:56	00:05:1e:54:f4:57	00:05:1e:54:f4:58
Port Status	Enabled	Enabled	Enabled	Enabled	Enabled	Enabled
Port State	Offline	Offline	Online	Offline	Online	Online
Speed (Gb/s)	1	1	1	1	1	1
Tunnel Count	1	0	1	0	2	2
ISCSI Capable	No	No	No	No	No	No
FCIP Capable	Yes	Yes	Yes	Yes	Yes	Yes
InBand Management State	Enabled	Disabled	Disabled	Disabled	Disabled	Enabled
LAG ID						
L2 Mode						
VLAN ID						

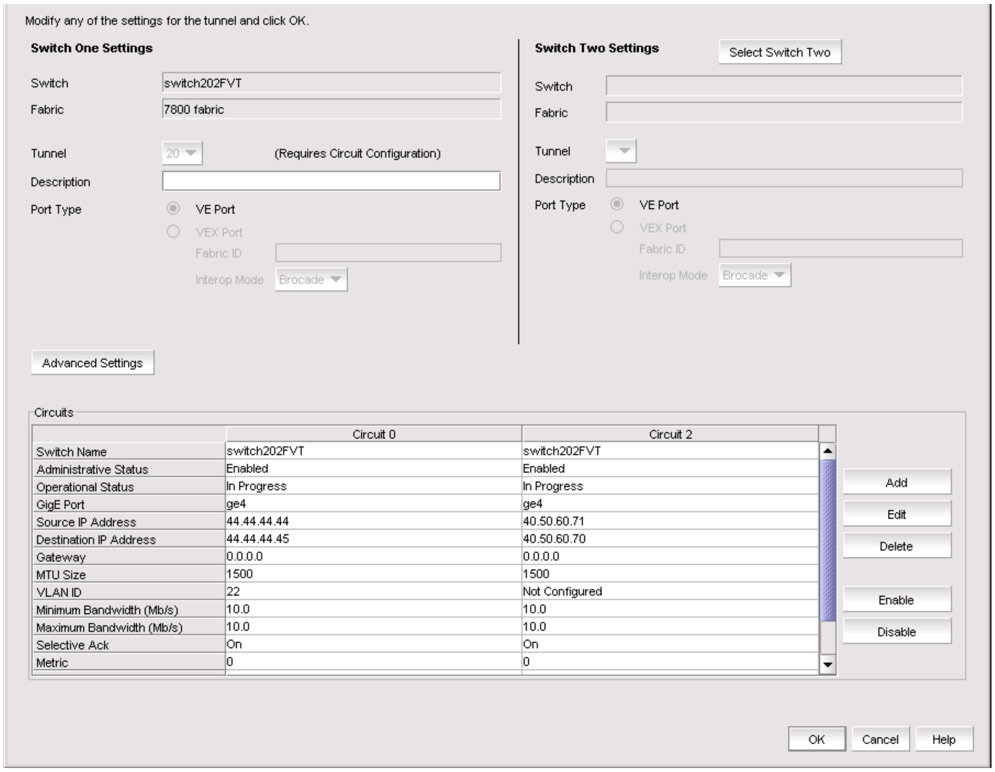
FIGURE 288 GigE ports properties

Editing FCIP tunnels

NOTE
You cannot edit an active tunnel; disable the tunnel before making changes.

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to edit.
2. Select **Edit**.

   The **Edit FCIP Tunnel** dialog box displays (Figure 289).



Modify any of the settings for the tunnel and click OK.

Switch One Settings

Switch: switch202FVT

Fabric: 7800 fabric

Tunnel: 20 (Requires Circuit Configuration)

Description:

Port Type: ● VE Port ○ VEX Port

Fabric ID:

Interop Mode: Brocade

Switch Two Settings

Switch:

Fabric:

Tunnel:

Description:

Port Type: ● VE Port ○ VEX Port

Fabric ID:

Interop Mode: Brocade

Circuits

	Circuit 0	Circuit 2
Switch Name	switch202FVT	switch202FVT
Administrative Status	Enabled	Enabled
Operational Status	In Progress	In Progress
GigE Port	ge4	ge4
Source IP Address	44.44.44.44	40.50.60.71
Destination IP Address	44.44.44.45	40.50.60.70
Gateway	0.0.0.0	0.0.0.0
MTU Size	1500	1500
VLAN ID	22	Not Configured
Minimum Bandwidth (Mb/s)	10.0	10.0
Maximum Bandwidth (Mb/s)	10.0	10.0
Selective Ack	On	On
Metric	0	0

FIGURE 289 Edit FCIP Tunnel dialog box

3. Fields and parameters are as described in "Configuring an FCIP tunnel". You can edit all editable fields and parameters.

Editing FCIP circuits

FCIP circuit settings may be edited from the **Edit FCIP Circuit** dialog box. The procedure for launching this dialog box for the 4 Gbps Extension Switch and Blade is different than the procedure for the 8 Gbps Extension Switch and the 8 Gbps Extension Blade. Also note the following differences for these platforms:

- The 4 Gbps Extension Switch and Blade have only one circuit per tunnel, and the circuit is edited as part of the tunnel. For 4 Gbps platforms, the **Delete**, **Enable**, and **Disable** buttons do not display. In addition, the **Edit** operation is only supported for cached circuits.
- The 8 Gbps Extension Switch and 8 Gbps Extension Blade may have multiple circuits per tunnel, and circuits may be selected individually.

For the 4 Gbps Extension Switch and Blade:

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to edit.
2. Select **Edit**.

   The **Edit FCIP Tunnel** dialog box displays.
3. Select **Edit** to the right of the **Circuits** properties table at the bottom of the dialog box.

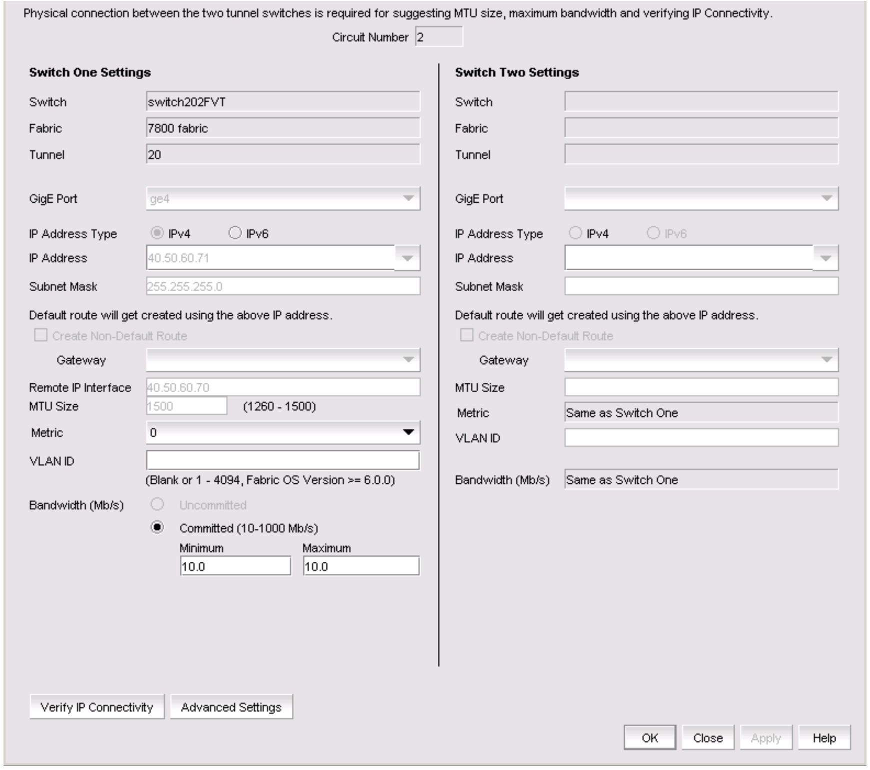
   The **Edit FCIP Circuit** dialog box displays.

For the 8 Gbps Extension Switch and the 8 Gbps Extension Blade:

1. Select **Edit**.

   The **Edit FCIP Tunnel** dialog box displays.
2. Select a circuit that you want to edit from the **Circuits** properties table at the bottom of the dialog box and select **Edit**.

   The **Edit FCIP Circuit** dialog box displays (Figure 290).


Physical connection between the two tunnel switches is required for suggesting MTU size, maximum bandwidth and verifying IP Connectivity.

Circuit Number 2

Switch One Settings

Switch: switch202FVT
Fabric: 7800 fabric
Tunnel: 20
GigE Port: ge4
IP Address Type: ● IPv4 ○ IPv6
IP Address: 40.50.60.71
Subnet Mask: 255.255.255.0
Default route will get created using the above IP address.
□ Create Non-Default Route
Gateway:
Remote IP Interface: 40.50.60.70
MTU Size: 1500 (1260 - 1500)
Metric: 0
VLAN ID:
(Blank or 1 - 4094, Fabric OS Version >= 6.0.0)
Bandwidth (Mb/s): ○ Uncommitted ● Committed (10-1000 Mb/s)
Minimum: 10.0
Maximum: 10.0

Switch Two Settings

Switch:
Fabric:
Tunnel:
GigE Port:
IP Address Type: ○ IPv4 ○ IPv6
IP Address:
Subnet Mask:
Default route will get created using the above IP address.
□ Create Non-Default Route
Gateway:
MTU Size:
Metric: Same as Switch One
VLAN ID:
Bandwidth (Mb/s): Same as Switch One

FIGURE 290 Edit FCIP Circuit dialog box

3. Fields and parameters are as described in "Adding an FCIP circuit". You can edit all editable fields and parameters.

Disabling FCIP tunnels

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to disable.
2. Select **Disable.**

   A confirmation dialog box displays showing the switches on both ends of the tunnel and tunnel number.
3. Click **Yes** to disable the tunnel.

Enabling FCIP tunnels

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to enable.
2. Select **Enable.**
3. Click **OK** to enable the tunnel.

Deleting FCIP tunnels

1. From the **FCIP Tunnels** dialog box, select the tunnel you want to delete.
2. Select the **Delete**.

   A confirmation dialog box displays, warning you of the consequences of deleting a tunnel.
3. Click **OK** to delete the tunnel.

Disabling FCIP circuits

1. From the **FCIP Tunnels** dialog box, select the tunnel that contains the circuit.
2. Select **Edit**.

   The **Edit FCIP Tunnel** dialog box displays.
3. Select the circuit that you want to disable from the **Circuit** properties table at the bottom of the dialog box.
4. Select **Disable**.
5. For tunnels with multiple circuits, select additional circuits from the table to disable and select **Disable** after each selection.
6. Click **OK** to disable the circuit(s).

Enabling FCIP circuits

1. From the **FCIP Tunnels** dialog box, select the tunnel that contains the circuit.
2. Select **Edit**.

   The **Edit FCIP Tunnel** dialog box displays.
3. Select the circuit that you want to disable from the **Circuit** properties table at the bottom of the dialog box.
4. Select **Enable**.
5. For tunnels with multiple circuits, select additional circuits from the table to enable and select **Enable** after each selection.
6. Click **OK** to enable the circuit(s).

Deleting FCIP Circuits

1. From the **FCIP Tunnels** dialog box, select the tunnel that contains the circuit.
2. Select **Edit**.

   The **Edit FCIP Tunnel** dialog box displays.
3. Select the circuit that you want to delete from the **Circuit** properties table at the bottom of the dialog box.
4. Select **Delete**.
5. For tunnels with multiple circuits, select additional circuits from the table to delete and select **Delete** after each selection.
6. Click **OK** to delete the circuit(s).

Displaying FCIP performance graphs

You can display performance graphs by clicking the **Performance** button on the FCIP Tunnels dialog box. You can also display performance graphs from Properties, as described in the following sections.

Displaying performance graphs for FC ports

1. Right-click a blade an extension blade or switch from the Fabric Tree structure or Connectivity Map, and select **Properties**.
2. Select the **Port** tab.
3. Select **FC** from the **Type** drop-down list.
4. Click **Performance > Real Time Graph**.

Displaying FCIP performance graphs for Ethernet ports

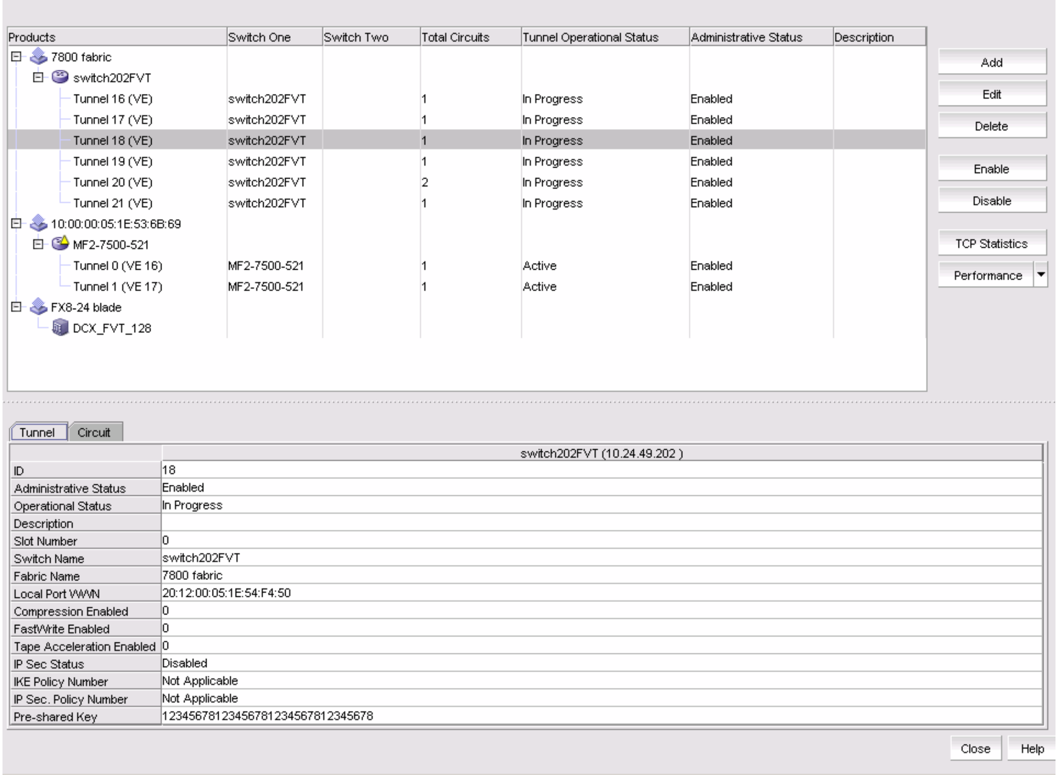
1. Right-click a blade an extension blade or switch from the Fabric Tree structure or Connectivity Map, and select **Properties**.
2. Select the **Port** tab.
3. Select **GigE** from the **Type** drop-down list.
4. Click **Performance > Real Time Graph**.

Displaying tunnel properties from the FCIP tunnels dialog box

Tunnel properties can be displayed from the **FCIP Tunnels** dialog box.

1. Select a tunnel from the **FCIP tunnels** dialog box.
2. Select the **Tunnel** tab.

   Tunnel properties are displayed.



Products	Switch One	Switch Two	Total Circuits	Tunnel Operational Status	Administrative Status	Description
⊟ 7800 fabric						
⊟ switch202FVT						
Tunnel 16 (VE)	switch202FVT		1	In Progress	Enabled	
Tunnel 17 (VE)	switch202FVT		1	In Progress	Enabled	
Tunnel 18 (VE)	switch202FVT		1	In Progress	Enabled	
Tunnel 19 (VE)	switch202FVT		1	In Progress	Enabled	
Tunnel 20 (VE)	switch202FVT		2	In Progress	Enabled	
Tunnel 21 (VE)	switch202FVT		1	In Progress	Enabled	
⊟ 10:00:00:05:1E:53:6B:69						
⊟ MF2-7500-521						
Tunnel 0 (VE 16)	MF2-7500-521		1	Active	Enabled	
Tunnel 1 (VE 17)	MF2-7500-521		1	Active	Enabled	
⊟ FX8-24 blade						
DCX_FVT_128						

	switch202FVT (10.24.49.202)
ID	18
Administrative Status	Enabled
Operational Status	In Progress
Description	
Slot Number	0
Switch Name	switch202FVT
Fabric Name	7800 fabric
Local Port WWN	20:12:00:05:1E:54:F4:50
Compression Enabled	0
FastWrite Enabled	0
Tape Acceleration Enabled	0
IP Sec Status	Disabled
IKE Policy Number	Not Applicable
IP Sec. Policy Number	Not Applicable
Pre-shared Key	12345678123456781234567812345678

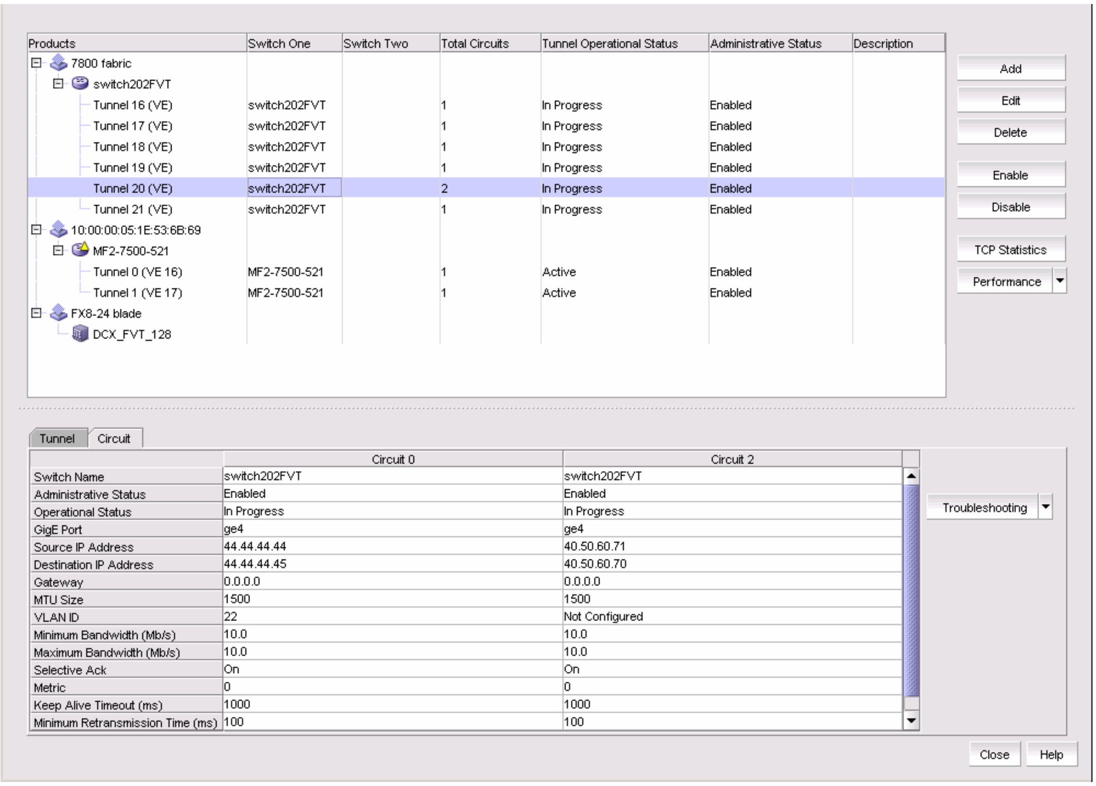
FIGURE 291 Tunnel properties on the FCIP Tunnels dialog box

Displaying FCIP circuit properties from the FCIP tunnels dialog box

Tunnel properties can be displayed from the **FCIP Tunnels** dialog box using the following procedure.

1. Select a tunnel from the **FCIP tunnels** dialog box.
2. Select the **Circuit** tab.

   Circuit properties are displayed (Figure 292).



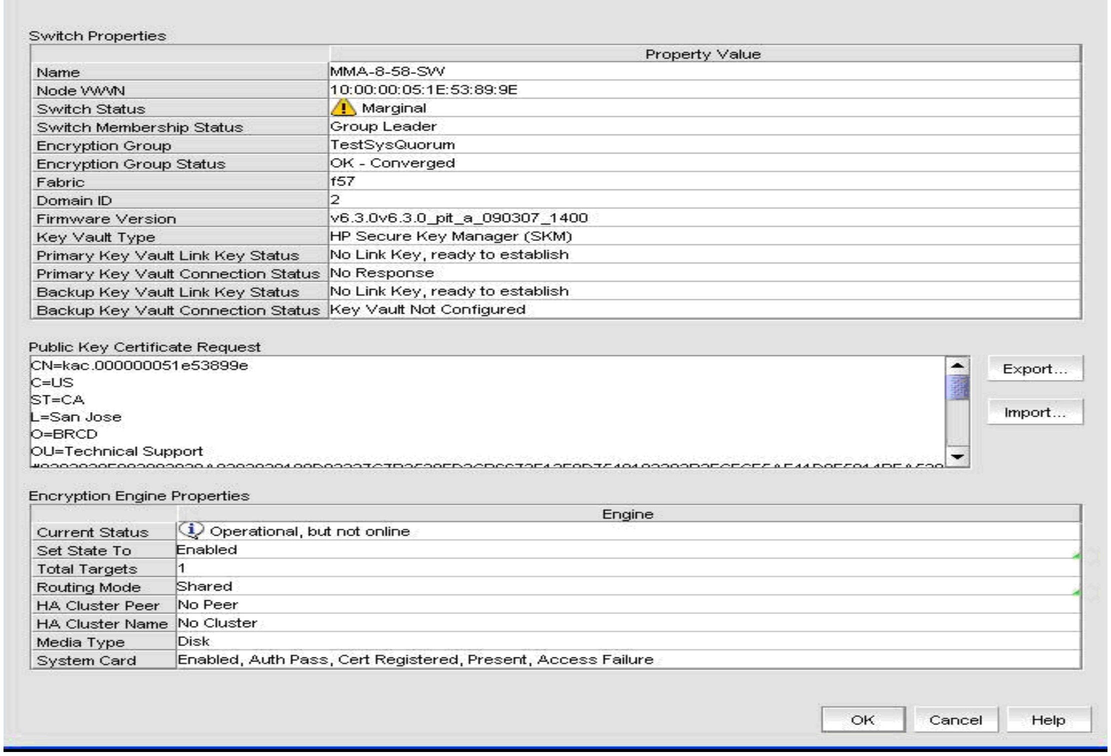
Products	Switch One	Switch Two	Total Circuits	Tunnel Operational Status	Administrative Status	Description
7800 fabric						
switch202FVT						
Tunnel 16 (VE)	switch202FVT		1	In Progress	Enabled	
Tunnel 17 (VE)	switch202FVT		1	In Progress	Enabled	
Tunnel 18 (VE)	switch202FVT		1	In Progress	Enabled	
Tunnel 19 (VE)	switch202FVT		1	In Progress	Enabled	
Tunnel 20 (VE)	switch202FVT		2	In Progress	Enabled	
Tunnel 21 (VE)	switch202FVT		1	In Progress	Enabled	
10:00:00:05:1E:53:6B:69						
MF2-7500-521						
Tunnel 0 (VE 16)	MF2-7500-521		1	Active	Enabled	
Tunnel 1 (VE 17)	MF2-7500-521		1	Active	Enabled	
FX8-24 blade						
DCX_FVT_128						

	Circuit 0	Circuit 2
Switch Name	switch202FVT	switch202FVT
Administrative Status	Enabled	Enabled
Operational Status	In Progress	In Progress
GigE Port	ge4	ge4
Source IP Address	44.44.44.44	40.50.60.71
Destination IP Address	44.44.44.45	40.50.60.70
Gateway	0.0.0.0	0.0.0.0
MTU Size	1500	1500
VLAN ID	22	Not Configured
Minimum Bandwidth (Mb/s)	10.0	10.0
Maximum Bandwidth (Mb/s)	10.0	10.0
Selective Ack	On	On
Metric	0	0
Keep Alive Timeout (ms)	1000	1000
Minimum Retransmission Time (ms)	100	100

FIGURE 292 Circuit properties on the FCIP Tunnels dialog box

Displaying switch properties from the FCIP Tunnels dialog box

Switch properties are displayed on the **FCIP Tunnels** dialog box when you select a switch (Figure 293).



Switch Properties

	Property Value
Name	MMA-8-58-SW
Node WWN	10:00:00:05:1E:53:89:9E
Switch Status	⚠ Marginal
Switch Membership Status	Group Leader
Encryption Group	TestSysQuorum
Encryption Group Status	OK - Converged
Fabric	f57
Domain ID	2
Firmware Version	v6.3.0v6.3.0_pit_a_090307_1400
Key Vault Type	HP Secure Key Manager (SKM)
Primary Key Vault Link Key Status	No Link Key, ready to establish
Primary Key Vault Connection Status	No Response
Backup Key Vault Link Key Status	No Link Key, ready to establish
Backup Key Vault Connection Status	Key Vault Not Configured

Public Key Certificate Request

```
CN=kac.000000051e53899e
C=US
ST=CA
L=San Jose
O=BRCD
OU=Technical Support
```

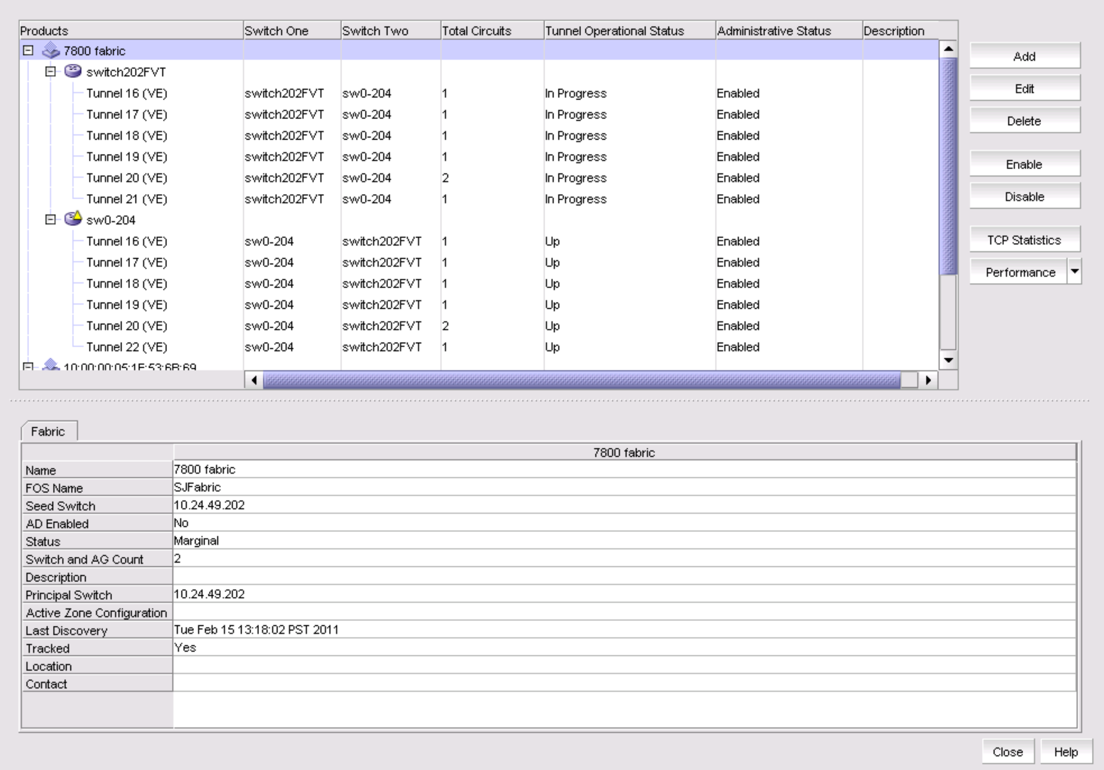
Encryption Engine Properties

	Engine
Current Status	ℹ Operational, but not online
Set State To	Enabled
Total Targets	1
Routing Mode	Shared
HA Cluster Peer	No Peer
HA Cluster Name	No Cluster
Media Type	Disk
System Card	Enabled, Auth Pass, Cert Registered, Present, Access Failure

FIGURE 293 Switch properties on the FCIP Tunnels dialog box

Displaying fabric properties from the FCIP Tunnels dialog box

Fabric properties are displayed on the **FCIP Tunnels** dialog box when you select a fabric. (Figure 294).



Products	Switch One	Switch Two	Total Circuits	Tunnel Operational Status	Administrative Status	Description
7800 fabric						
switch202FVT						
Tunnel 16 (VE)	switch202FVT	sw0-204	1	In Progress	Enabled	
Tunnel 17 (VE)	switch202FVT	sw0-204	1	In Progress	Enabled	
Tunnel 18 (VE)	switch202FVT	sw0-204	1	In Progress	Enabled	
Tunnel 19 (VE)	switch202FVT	sw0-204	1	In Progress	Enabled	
Tunnel 20 (VE)	switch202FVT	sw0-204	2	In Progress	Enabled	
Tunnel 21 (VE)	switch202FVT	sw0-204	1	In Progress	Enabled	
sw0-204						
Tunnel 16 (VE)	sw0-204	switch202FVT	1	Up	Enabled	
Tunnel 17 (VE)	sw0-204	switch202FVT	1	Up	Enabled	
Tunnel 18 (VE)	sw0-204	switch202FVT	1	Up	Enabled	
Tunnel 19 (VE)	sw0-204	switch202FVT	1	Up	Enabled	
Tunnel 20 (VE)	sw0-204	switch202FVT	2	Up	Enabled	
Tunnel 22 (VE)	sw0-204	switch202FVT	1	Up	Enabled	
10:00:00:05:1E:53:6B:69						

	7800 fabric
Name	7800 fabric
FOS Name	SJFabric
Seed Switch	10.24.49.202
AD Enabled	No
Status	Marginal
Switch and AG Count	2
Description	
Principal Switch	10.24.49.202
Active Zone Configuration	
Last Discovery	Tue Feb 15 13:18:02 PST 2011
Tracked	Yes
Location	
Contact	

FIGURE 294 Fabric properties on the FCIP Tunnels dialog box

Troubleshooting FCIP Ethernet connections

1. Right-click a blade an extension blade or switch from the Fabric Tree structure or Connectivity Map, and select **Properties**.
2. Select the **Port** tab.
3. Select **GigE** from the **Type** drop-down list.
4. Select an Ethernet port.
5. Click **Troubleshooting**.

   The following options are presented:

   - **IP Ping**—Tests connections between a local Ethernet port (ge0 or ge1) and a destination IP address.
   - **IP Traceroute**—Traces routes from a local Ethernet port (ge0 or ge1) to a destination IP address.

Chapter

Fabric Binding 22

In this chapter

Fabric binding overview

NOTE
In a pure Fabric OS environment, Fabric Binding is supported on Fabric OS 5.2 or later.

NOTE
In a mixed Fabric OS and M-EOS environment, Fabric Binding in Interop Mode 2 or 3 is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

NOTE
To enable or disable Fabric Binding in a mixed fabric, at least one Fabric OS device and one M-EOS device must be manageable.

NOTE
In a mixed Fabric OS and M-EOS environment, you cannot disable Fabric Binding if High Integrity Fabric is enabled. However, if High Integrity Fabric is disabled, you can disable Fabric Binding.

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.

For M-EOS devices, enabling Fabric Binding activates Fabric Binding and enables insistent domain ID. Disabling Fabric Binding on M-EOS devices deactivates Fabric Binding.

For Fabric OS devices, enabling Fabric Binding activates Switch Connection Control (SCC) policy and sets Fabric Wide Consistency Policy (FWCP) and insistent domain ID. Disabling Fabric Binding on Fabric OS devices deletes SCC policy and sets FWCP to absent.

NOTE
In a pure Fabric OS fabric, enabling insistent domain ID is mandatory.

Enabling fabric binding

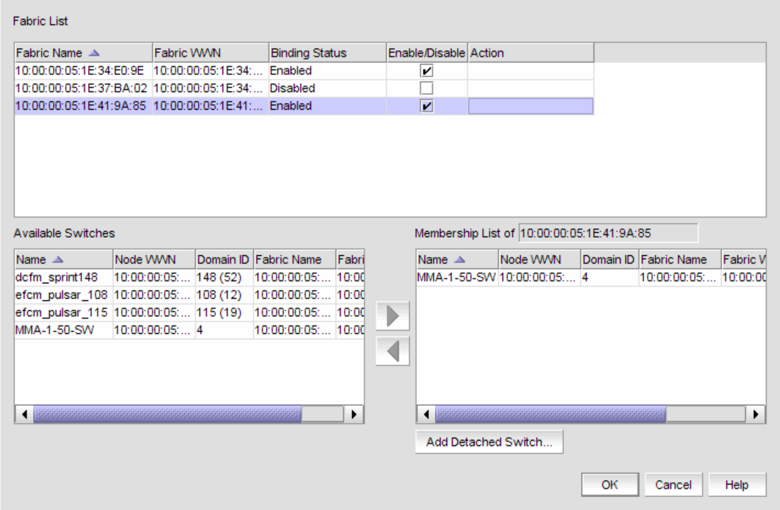
Fabric Binding is enabled through the **Fabric Binding** dialog box. After you have enabled Fabric Binding, use the **Fabric Membership List/Add Detached Switch** to add switches that you want to allow into the fabric.

NOTE

In a pure Fabric OS environment, Fabric Binding is only supported on Fabric OS 5.2 or later.
In a mixed Fabric OS and M-EOS environment, Fabric Binding is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

1. Select **Configure > Fabric Binding**.

   The **Fabric Binding** dialog box displays (Figure 295).



Fabric List

Fabric Name	Fabric WWN	Binding Status	Enable/Disable	Action
10:00:00:05:1E:34:E0:9E	10:00:00:05:1E:34:...	Enabled	☑	
10:00:00:05:1E:37:BA:02	10:00:00:05:1E:34:...	Disabled	☐	
10:00:00:05:1E:41:9A:85	10:00:00:05:1E:41:...	Enabled	☑	

Available Switches

Name	Node WWN	Domain ID	Fabric Name	Fabri
dcfm_sprint148	10:00:00:05:...	148 (52)	10:00:00:05:...	10:00
efcm_pulsar_108	10:00:00:05:...	108 (12)	10:00:00:05:...	10:00
efcm_pulsar_115	10:00:00:05:...	115 (19)	10:00:00:05:...	10:00
MMA-1-50-SW	10:00:00:05:...	4	10:00:00:05:...	10:00

Membership List of 10:00:00:05:1E:41:9A:85

Name	Node WWN	Domain ID	Fabric Name	Fabric V
MMA-1-50-SW	10:00:00:05:...	4	10:00:00:05:...	10:00:00

FIGURE 295 **Fabric Binding dialog box**

2. In the **Fabric List** table, click the **Enable/Disable** check box for fabrics for which you want to configure fabric binding.

   For instructions on adding and removing switches from the membership list, refer to “Adding switches to the fabric binding membership list” on page 671 and “Removing switches from fabric binding membership” on page 672.

3. Click **OK**.

Disabling fabric binding

Fabric Binding cannot be disabled while High Integrity Fabric is active if the switch is offline. This disables fabric binding and High Integrity Fabric 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
In a pure Fabric OS environment, Fabric Binding is only supported on Fabric OS 5.2 or later.
In a mixed Fabric OS and M-EOS environment, Fabric Binding is only supported on Fabric OS 6.0 or later and M-EOS manageable 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.
3. Click **OK**.

Adding switches to the fabric binding membership list

Once you have enabled Fabric Binding (refer to "Enabling fabric binding" on page 670), you can add switches to the fabric binding membership list.

NOTE
In a pure Fabric OS environment, Fabric Binding is only supported on Fabric OS 5.2 or later.
In a mixed Fabric OS and M-EOS environment, Fabric Binding is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

To add a switch to the fabric, complete the following steps.

1. Select **Configure** > **Fabric Binding**.

   The **Fabric Binding** dialog box (Figure 295) 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. Click **OK** on the **Fabric Binding** dialog box.

Adding detached devices to the fabric binding membership list

To add a switch that does not have a physical connection and is not discovered to the fabric, complete the following steps.

1. Select **Configure > Fabric Binding**.

   The **Fabric Binding** dialog box displays.

2. Click **Add Detached Switch**.

   The **Add Detached Switch** dialog box displays.

3. Enter the domain ID of the switch in the **Domain ID** field.
4. Enter the nodeworld wide name (WWN) of the switch in the **Node WWN** field.

   NOTE
   You can copy (Ctrl+C) and paste (Ctrl+V) the Node WWN into the **Node WWN** field. It does not matter if the copy source contains colons (11:22:33:44:55:66:77), only the numbers are pasted (11223344556677) in the **Node WWN** field.

5. Click **OK** on the **Add Detached Switch** dialog box.

   The added switch displays in the **Membership List of** *Fabric_Name* table on the **Fabric Binding** dialog box.

6. Click **OK** on the **Fabric Binding** dialog box.

Removing switches from fabric binding membership

Once you have enabled Fabric Binding (refer to "Enabling fabric binding" on page 670), you can remove switches that are not part of the fabric from the membership list.

NOTE
In a pure Fabric OS environment, Fabric Binding is only supported on Fabric OS 5.2 or later.
In a mixed Fabric OS and M-EOS environment, Fabric Binding is only supported on Fabric OS 6.0 or later and M-EOS manageable switches and fabrics.

1. Select **Configure > Fabric Binding**.

   The **Fabric Binding** dialog box (Figure 295) displays.

2. Select the switches you want to remove from the selected fabrics' Fabric Membership List (FML) in the **Membership List** table.

   NOTE
   The selected switch cannot be part of the fabric.

3. Click the left arrow to move the switches to the **Available Switches** table.
4. Click **OK**.

High integrity fabrics

The High Integrity Fabric (HIF) mode option automatically enables features and operating parameters that are necessary in multiswitch Enterprise Fabric environments. When HIF is enabled, each switch in the fabric automatically enforces a number of security-related features including Fabric Binding, Switch Binding, Insistent Domain IDs, and Domain Register for State Change Notifications (RSCNs).

For Pure Fabric OS fabrics, HIF activates the Switch Connection Control (SCC) policy, sets Insistent Domain ID, and sets the Fabric Wide Consistency Policy (FWCP) for SCC in strict mode.

For mixed Fabric OS and M-EOS fabrics:

- For Fabric OS switches, HIF activates the SCC policy, sets Insistent Domain ID, and sets the FWCP for SCC in tolerant mode.
- For M-EOS switches, HIF activates Enterprise Fabric Mode, Fabric Binding, Switch Binding, Insistent Domain ID, and RSCNs.

Activating HIF mode enables the following features:

- Fabric Binding (M-EOS only). Allows or prohibits switches from merging with a selected fabric.

  NOTE
  NOTE: Fabric Binding cannot be disabled while HIF is active even if the switch is offline.

- Switch Binding (M-EOS only). This feature, enabled through a device's Element Manager, allows or prohibits switches from connecting to switch E_Ports and devices from connecting to F_Ports.

  NOTE
  NOTE: Switch binding can be disabled while Enterprise Fabric Mode is active if the switch is offline.

- Switch Connection Control (Fabric OS only). This feature, enabled through a device's Element Manager, prevents unauthorized switches from joining a fabric.
- Fabric Wide Consistency Policy (Fabric OS only). This feature makes sure that switches in the fabric enforce the same policies.
- Domain RSCNs (M-EOS only). This feature, enabled through a device'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-devices.
- Insistent Domain ID (Fabric OS and M-EOS). This feature, enabled through a device's Element Manager, sets the domain ID as the active domain identification when the fabric initializes. When Insistent Domain ID is enabled, the switch isolates itself from the fabric if the preferred domain ID is not assigned as the switch's domain ID.

High integrity fabric requirements

The term high integrity fabric (HIF) refers to a set of strict, consistent, fabric-wide policies. There are several specific configuration requirements for high integrity fabrics:

- Insistent domain ID (IDID) must be enabled in the participating switches.
- Port-based routing must be used on the participating switches.
- A policy must be set that limits connectivity to only the switches within the same fabric. Fabric binding is a security method for restricting switches that may join a fabric. For Fabric OS switches, fabric binding is implemented by defining a switch connection control (SCC) policy that prevents unauthorized switches from joining a fabric.
- Switch binding is a more secure alternative to fabric binding. It is a security method for restricting devices that connect to a particular switch. Switch binding is available only on M-EOS switches and directors. Switch binding has two options: restrict all, and restrict switches only. Switch binding should only be implemented in FICON environments with the switch restriction only. The difference between switch binding and fabric binding is that with fabric binding a defined switch can join the fabric by connecting to any switch in the fabric while with switch binding the new switch can only join by connecting to a specific switch in the fabric.
- Dynamic Load Sharing (DLS) should be disabled. If DLS is not disabled, DLS automatically adjusts routes when a new ISL is added, and when an ISL is taken offline and brought online again. This process may result in dropped frames.

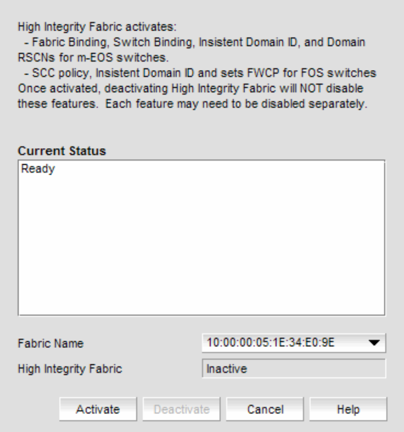
NOTE
Port binding is a security method for restricting devices that connect to particular switch ports. Port binding should never be used in FICON environments. The FICON channel cannot be added to the port binding list.

Activating high integrity fabrics

To activate a HIF, complete the following steps.

1. Select **Configure > High Integrity Fabric**.

   The **High Integrity Fabric** dialog box displays.



High Integrity Fabric activates:
  - Fabric Binding, Switch Binding, Insistent Domain ID, and Domain RSCNs for m-EOS switches.
  - SCC policy, Insistent Domain ID and sets FWCP for FOS switches
Once activated, deactivating High Integrity Fabric will NOT disable these features. Each feature may need to be disabled separately.

Current Status
Ready

Fabric Name: 10:00:00:05:1E:34:E0:9E
High Integrity Fabric: Inactive

FIGURE 296 High Integrity Fabric dialog box

2. Select the fabric on which you want to activate HIF from the **Fabric Name** list.

   The HIF status displays in the **High Integrity Fabric** field.

3. Click **Activate**.

   For Pure Fabric OS fabrics, HIF activates the Switch Connection Control (SCC) policy, sets Insistent Domain ID, and sets the Fabric Wide Consistency Policy (FWCP) for SCC in strict mode.

   For mixed Fabric OS and M-EOS fabrics:

   - For Fabric OS switches, HIF activates the SCC policy, sets Insistent Domain ID, and sets the FWCP for SCC in tolerant mode.
   - For M-EOS switches, HIF activates Enterprise Fabric Mode, Fabric Binding, Switch Binding, Insistent Domain ID, and RSCNs.

Deactivating high integrity fabrics

NOTE
Deactivating high integrity fabrics is not supported in a pure Fabric OS environment.

To deactivate a HIF, complete the following steps.

1. Select **Configure > High Integrity Fabric**.

   The **High Integrity Fabric** dialog box displays.

2. Select the fabric on which you want to deactivate HIF from the **Fabric Name** list.

   The HIF status displays in the **High Integrity Fabric** field.

3. Click **Deactivate**.

   Deactivating HIF on a fabric does not deactivate the features on the individual switches, you must disable them individually:

   - For Fabric OS switches, disable the SCC policy, Insistent Domain ID, and the Fabric Wide Consistency Policy for SCC in tolerant mode.
   - For M-EOS switches, disable Fabric Binding, Switch Binding, Insistent Domain ID, and RSCNs.

Chapter

Port Fencing 23

In this chapter

About port fencing

Port Fencing allows you to protect your SAN from repeated operational or security problems experienced by ports. Use Port Fencing to set threshold limits for the number of specific port events permitted during a given time period on the selected object.

Port Fencing objects include the SAN, Fabrics, Directors, Switches (physical), Virtual Switches, Ports, as well as Port Types (E_port, F_port, and FX_port). Use Port Fencing to directly assign a threshold to these objects. When a switch does not support Port Fencing, a “No Fencing Changes” message displays in the **Threshold** field in the **Ports** table.

If the port detects more events during the specified time period, the device firmware blocks the port, disabling transmit and receive traffic until you investigate, solve the problem, and manually unblock the port.

Physical fabrics, directors, switches, port types, and ports display when you have the privileges to manage that object and are indicated by the standard product icons.

NOTE
Port Fencing displays any existing thresholds discovered on manageable fabrics, directors, and switches running firmware versions M-EOS 9.X or Fabric OS 6.2 or later.

Port Fencing requirements

To configure port fencing, the following requirements must be met:

- All Fabric OS devices must have Fabric Watch and must be running firmware Fabric OS 6.2 or later.
- All M-EOS devices must be running firmware M-EOS 9.X or later.
- All M-EOS devices must be discovered directly using MPI.

Thresholds

You can create thresholds, which you can then assign to available objects in the tree. Port Fencing threshold types include the following:

- C3 Discard Frames (Fabric OS only)
- Invalid CRCs (Fabric OS only)
- Invalid Words (Fabric OS only)
- Link (M-EOS only)
- Link Reset (Fabric OS only)
- Protocol Errors (M-EOS and Fabric OS)
- Security (M-EOS)
- State Change (Fabric OS only)

NOTE
You can create up to 16 thresholds for M-EOS devices.

NOTE
Fabric OS devices are allowed only 2 defined thresholds (one default and one custom) foe each threshold type and only one of these thresholds can be active on the device.

During the dynamic operation of a Fabric, 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 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).

For default threshold values for Fabric OS devices, refer to Chapter 7 of the *Fabric Watch Administrator's Guide*.

C3 Discard Frames threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

NOTE
The C3 Discard Frames threshold cannot be applied to an E port.

Use this type of threshold to block a port when a C3 Discard Frames violation meets the Fabric OS switch threshold. This threshold is only supported on the following devices:

- 40-port, 8 Gbps FC Switch
- 80-port, 8 Gbps FC Switch
- 8 Gbps 12-port Embedded Switch
- 8 Gbps 24-port Embedded Switch

- 8 Gbps 16-port Embedded Switch
- 8 Gbps 24-port Embedded Switch
- 8 Gbps 8-FC port, 10 GbE 24-CEE port Switch
- 384-port Backbone Chassis
- 192-port Backbone Chassis
- 8 Gbps Encryption Switch
- Encryption Blade
- FC 8 GB 16-port Blade
- FC 8 GB 32-port Blade
- FC 8 GB 48-port Blade

Invalid CRCs threshold

NOTE
This threshold is only available for Fabric OS devices.

Use this type of threshold to block a port when an Invalid CRCs violation meets the Fabric OS switch threshold.

Invalid words threshold

NOTE
This threshold is only available for Fabric OS devices.

Use this type of threshold to block a port when an Invalid Words violation meets the Fabric OS switch threshold.

Link threshold

NOTE
This threshold is only available for M-EOS devices.

Use this type of threshold to block a port when a Link Level (Hot I/O) error meets the threshold. A Link Level (Hot I/O) occurs when an active loop port repeatedly receives a loop initialization primitive sequence error or an active non-loop port repeatedly receives a line repeater, offline sequence, or not operational sequence error.

Link Reset threshold

NOTE
This threshold is only available for Fabric OS devices.

Use this type of threshold to block a port when the link timeout errors meet the threshold.

Protocol error threshold

Use Protocol Error thresholds to block a port when one of the following protocol errors meet the threshold:

- ISL Bouncing–ISL has repeatedly become unavailable due to link down events.
- ISL Segmentation (M-EOS only)–ISL has repeatedly become segmented.
- ISL Protocol Mismatch–ISL has been repeatedly put into the Invalid Attachment state due to a protocol error.

State Change threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

Use this type of threshold to block a port when a state change violation type meets the Fabric OS switch threshold.

For 4 Gbps Router, Extension Switches and Blades only, when you apply this threshold on an E Port, the threshold is also applied to the VE Ports (internally by Fabric OS).

Security threshold

NOTE
This threshold is only available for M-EOS devices.

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.
- ISL Security–(Generic Security Error) the switch on the other side of the ISL has detected a specific security violation, but is only able to indicate 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 Management application allows you to create Invalid CRCs, Invalid words, Link, Link Reset, Protocol Error, Security, and Sync Loss thresholds.

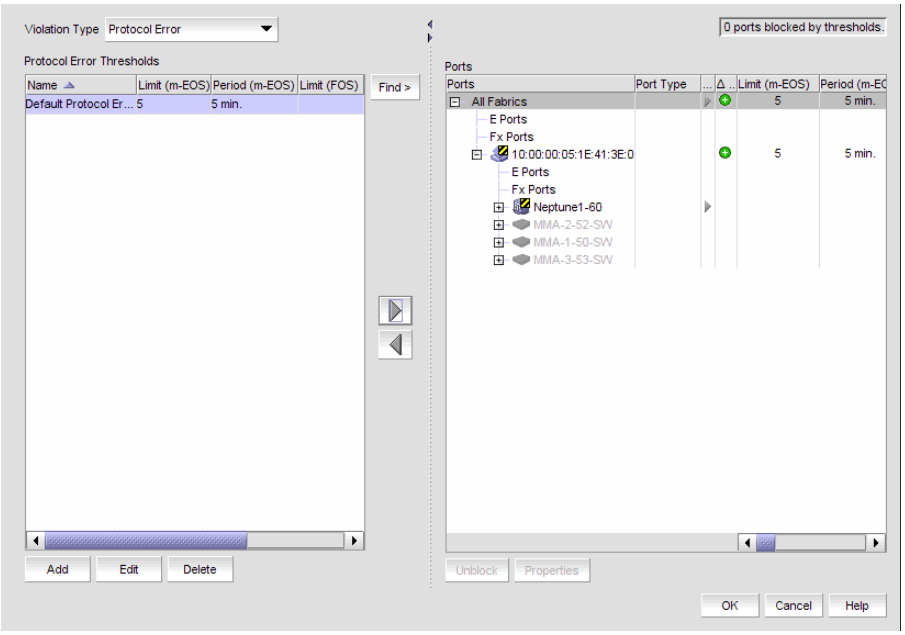
Adding a C3 Discard Frames threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

To add an C3 Discard Frames threshold, complete the following steps.

1. Select **Monitor** > **Fabric Watch** > **Port Fencing**.

   The **Port Fencing** dialog box displays (Figure 297).



Violation Type: Protocol Error

Protocol Error Thresholds

Name	Limit (m-EOS)	Period (m-EOS)	Limit (FOS)
Default Protocol Er...	5	5 min.	

0 ports blocked by thresholds.

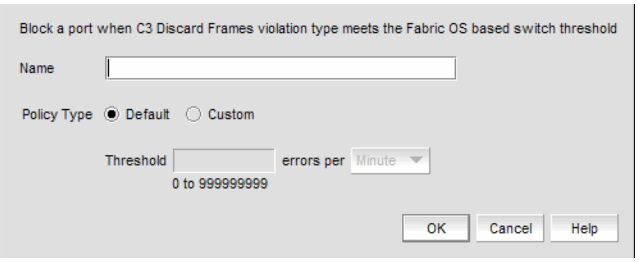
Ports

Ports	Port Type	...	Δ ..	Limit (m-EOS)	Period (m-EO
All Fabrics			●	5	5 min.
E Ports					
Fx Ports					
10:00:00:05:1E:41:3E:0			●	5	5 min.
E Ports					
Fx Ports					
Neptune1-60					
MMA-2-52-SW					
MMA-1-50-SW					
MMA-3-53-SW					

FIGURE 297 Port Fencing dialog box

2. Select **C3 Discard Frames (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

   The **Add C3 Discard Frames Threshold** dialog box displays.



Block a port when C3 Discard Frames violation type meets the Fabric OS based switch threshold

Name:

Policy Type ● Default ○ Custom

Threshold errors per Minute
0 to 999999999

FIGURE 298 Add C3 Discard Frames Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.
6. Enter the number of C3 discarded frames allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
   - None—the port is blocked as soon as the specified number of C3 discarded frames allowed is met.
   - Second—the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a second.
   - Minute—the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a minute.
   - Hour—the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a hour.
   - Day—the port is blocked as soon as the specified number of C3 discarded frames allowed is reached within a day.
8. Click **OK** to add the C3 discarded frames threshold to the table and close the **Add C3 Discard Frames Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.
9. Click **OK** on the **Port Fencing** dialog box.

Adding an Invalid CRCs threshold

NOTE
This threshold is only available for Fabric OS devices.

To add an Invalid CRCs threshold, complete the following steps.

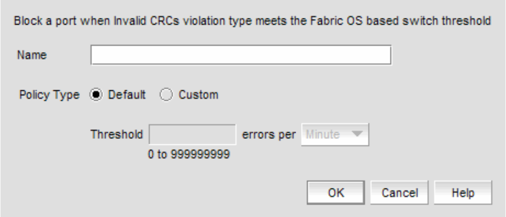
1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Invalid CRCs (Fabric OS only)** from the **Violation Type** list.

3. Click **Add**.

   The **Add Invalid CRCs Threshold** dialog box displays.



Block a port when Invalid CRCs violation type meets the Fabric OS based switch threshold

Name

Policy Type ● Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 299 Add Invalid CRCs Threshold dialog box

4. Enter a name for the threshold in the **Name** field.

5. Select one of the following options:

   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.

6. Enter the number of invalid CRCs allowed for the threshold in the **Threshold** errors field.

7. Select the time period for the threshold from the **errors per** list. The following choices are available:

   - None—the port is blocked as soon as the specified number of invalid CRCs allowed is met.
   - Second—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a second.
   - Minute—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a minute.
   - Hour—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a hour.
   - Day—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a day.

8. Click **OK** to add the Invalid CRCs threshold to the table and close the **Add Invalid CRCs Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.

9. Click **OK** on the **Port Fencing** dialog box.

Adding an Invalid Words threshold

NOTE
This threshold is only available for Fabric OS devices.

To add an Invalid Words threshold, complete the following steps.

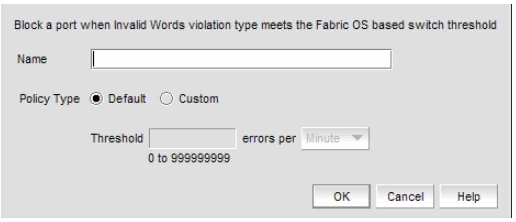
1. Select **Monitor** > **Fabric Watch** > **Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Invalid Words (Fabric OS only)** from the **Violation Type** list.

3. Click **Add**.

   The **Add Invalid Words Threshold** dialog box displays.



Block a port when Invalid Words violation type meets the Fabric OS based switch threshold

Name

Policy Type ● Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 300 Add Invalid Words Threshold dialog box

4. Enter a name for the threshold in the **Name** field.

5. Select one of the following options:
   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.

6. Enter the number of invalid words allowed for the threshold in the **Threshold** errors field.

7. Select the time period for the threshold from the **errors per** list. The following choices are available:
   - None—the port is blocked as soon as the specified number of invalid words allowed is met.
   - Second—the port is blocked as soon as the specified number of invalid words allowed is reached within a second.
   - Minute—the port is blocked as soon as the specified number of invalid words allowed is reached within a minute.
   - Hour—the port is blocked as soon as the specified number of invalid words allowed is reached within a hour.
   - Day—the port is blocked as soon as the specified number of invalid words allowed is reached within a day.

8. Click **OK** to add the Invalid Words threshold to the table and close the **Add Invalid Words Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 691.

9. Click **OK** on the **Port Fencing** dialog box.

Adding a Link threshold

NOTE
This threshold is only available for M-EOS devices.

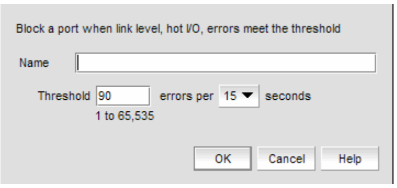
To add Link thresholds, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Link** from the **Violation Type** list.
3. Click **Add**.

   The **Add Link Threshold** dialog box displays (Figure 301).



Block a port when link level, hot I/O, errors meet the threshold

Name

Threshold 90 errors per 15 seconds

1 to 65,535

FIGURE 301 Add Link Threshold dialog box

4. Enter a name for the threshold in the **Name** field.
5. Select the number of link errors allowed for the threshold from the **Threshold** errors list.
6. Select the time period for the threshold (in minutes) from the **errors per** list.
7. Click **OK** to add the Link threshold to the table and close the **Add Link Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.

8. Click **OK** on the **Port Fencing** dialog box.

Adding a Link Reset threshold

NOTE
This threshold is only available for Fabric OS devices.

Use this threshold to block a port when a Link Reset violation meets the Fabric OS switch threshold.

To add a Link Reset threshold, complete the following steps.

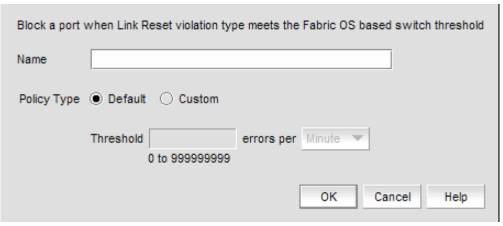
1. Select **Monitor** > **Fabric Watch** > **Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Link Reset (Fabric OS only)** from the **Violation Type** list.

3. Click **Add**.

   The **Add Link Reset Threshold** dialog box displays.



Block a port when Link Reset violation type meets the Fabric OS based switch threshold

Name

Policy Type ● Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 302 Add Link Reset Threshold dialog box

4. Enter a name for the threshold in the **Name** field.

5. Select one of the following options:

   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.

6. Enter the number of link resets allowed for the threshold in the **Threshold** errors field.

7. Select the time period for the threshold from the **errors per** list. The following choices are available:

   - None—the port is blocked as soon as the specified number of link resets allowed is met.
   - Second—the port is blocked as soon as the specified number of link resets allowed is reached within a second.
   - Minute—the port is blocked as soon as the specified number of link resets allowed is reached within a minute.
   - Hour—the port is blocked as soon as the specified number of link resets allowed is reached within a hour.
   - Day—the port is blocked as soon as the specified number of link resets allowed is reached within a day.

8. Click **OK** to add the Link Resets threshold to the table and close the **Add Link Reset Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 691.

9. Click **OK** on the **Port Fencing** dialog box.

Adding a Protocol Error threshold

To add a Protocol Error threshold, complete the following steps.

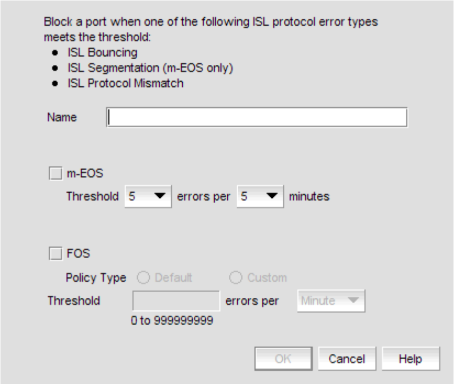
1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Protocol Error** from the **Violation Type** list.

3. Click **Add**.

   The **Add Protocol Error Threshold** dialog box displays.



Block a port when one of the following ISL protocol error types meets the threshold:

- ISL Bouncing
- ISL Segmentation (m-EOS only)
- ISL Protocol Mismatch

Name

□ m-EOS

Threshold 5 errors per 5 minutes

□ FOS

Policy Type ○ Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 303 **Add Protocol Error Threshold dialog box**

4. Enter a name for the threshold in the **Name** field.

5. (M-EOS devices only) Select the **M-EOS** check box.

   a. Select the number of protocol errors allowed for the threshold from the **Threshold** errors list.

   b. Select the time period for the threshold (in minutes) from the **errors per** list.

6. (Fabric OS devices only) Select the **Fabric OS** check box.

   a. Select one of the following options:

      - Default—Uses device defaults. Go to step 7.
      - Custom—Uses your selections. Continue with step b.

   b. Enter the number of protocol errors allowed for the threshold from the **Threshold** errors field.

c. Select the time period for the threshold from the **errors per** list. The following choices are available:

- None—the port is blocked as soon as the specified number of protocol errors allowed is met.
- Second—the port is blocked as soon as the specified number of protocol errors allowed is reached within a second.
- Minute—the port is blocked as soon as the specified number of protocol errors allowed is reached within a minute.
- Hour—the port is blocked as soon as the specified number of protocol errors allowed is reached within a hour.
- Day—the port is blocked as soon as the specified number of protocol errors allowed is reached within a day.

7. Click **OK** to add the protocol errors threshold to the table and close the **Add Protocol Error Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.

8. Click **OK** on the **Port Fencing** dialog box.

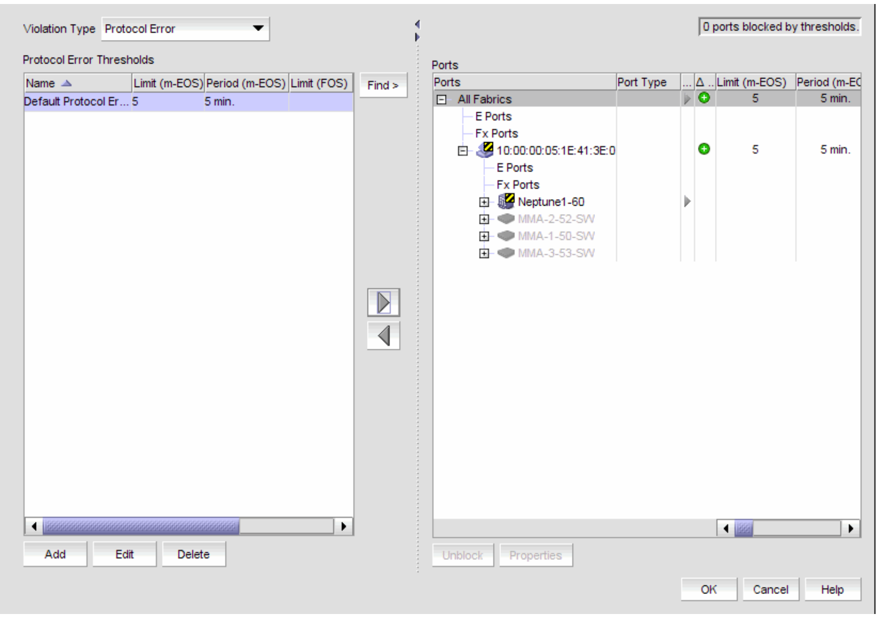
Adding a State Change threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

To add an State Change threshold, complete the following steps.

1. Select **Monitor** > **Fabric Watch** > **Port Fencing.**

   The **Port Fencing** dialog box displays (Figure 304).



Violation Type: Protocol Error

0 ports blocked by thresholds.

Protocol Error Thresholds

Name	Limit (m-EOS)	Period (m-EOS)	Limit (FOS)
Default Protocol Er...	5	5 min.	

Ports

Ports	Port Type	...	Δ ..	Limit (m-EOS)	Period (m-EC
All Fabrics			⊕	5	5 min.
E Ports					
Fx Ports					
10:00:00:05:1E:41:3E:0			⊕	5	5 min.
E Ports					
Fx Ports					
Neptune1-60					
MMA-2-52-SW					
MMA-1-50-SW					
MMA-3-53-SW					

FIGURE 304 Port Fencing dialog box

2. Select **State Change (Fabric OS only)** from the **Violation Type** list.
3. Click **Add**.

   The **Add State Change Threshold** dialog box displays.
4. Enter a name for the threshold in the **Name** field.
5. Select one of the following options:
   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.
6. Enter the number of state changes allowed for the threshold in the **Threshold** errors field.
7. Select the time period for the threshold from the **errors per** list. The following choices are available:
   - None—the port is blocked as soon as the specified number of state changes allowed is met.
   - Second—the port is blocked as soon as the specified number of state changes allowed is reached within a second.
   - Minute—the port is blocked as soon as the specified number of state changes allowed is reached within a minute.
   - Hour—the port is blocked as soon as the specified number of state changes allowed is reached within a hour.
   - Day—the port is blocked as soon as the specified number of state changes allowed is reached within a day.
8. Click **OK** to add the state changes threshold to the table and close the **Add State Change Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.
9. Click **OK** on the **Port Fencing** dialog box.

Adding a Security threshold

NOTE
This threshold is only available for M-EOS devices.

To add a Security threshold, complete the following steps.

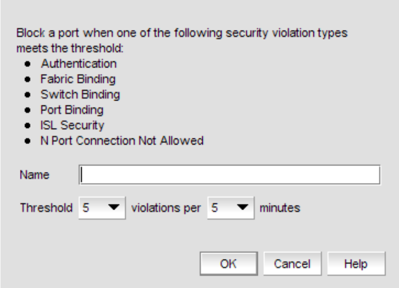
1. Select **Monitor** > **Fabric Watch** > **Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Security** from the **Violation Type** list.

3. Click **Add**.

   The **Add Security Threshold** dialog box displays (Figure 305).



Block a port when one of the following security violation types meets the threshold:

- Authentication
- Fabric Binding
- Switch Binding
- Port Binding
- ISL Security
- N Port Connection Not Allowed

Name

Threshold 5 violations per 5 minutes

FIGURE 305 Add Security Threshold dialog box

4. 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 list.

6. Select the time limit for the threshold from the **violations per** list.

7. Click **OK** to add the security threshold to the table and close the **Add Security Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.

8. Click **OK** on the **Port Fencing** dialog box.

Assigning thresholds

You can assign thresholds to any active object in the **Ports** table. You can only assign one threshold to an object at a time. 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. Select **Monitor** > **Fabric Watch** > **Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select the threshold you want to assign from the **Thresholds** table.
4. Select the objects (All Fabrics, Fabric, Director, Switch, Port Type, and/or Port) to which you want to assign the threshold from the **Ports** table.
5. Click the right arrow.

   A directly assigned icon (▸) displays 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 subordinate object below it in the tree (if not affected by lower level direct assignments).

   An added icon (⊕) appears next to every object in the tree to which the new threshold is applied.

6. Click **OK** on the **Port Fencing** dialog box.

Unblocking a port

The Management application allows you to unblock a port (only if it was blocked by Port Fencing) once the problem that triggered the threshold is fixed. When a port is blocked an Attention icon (⚠) displays next to the port node.

To unblock a port, complete the following steps.

1. Select Monitor > Fabric Watch > Port Fencing.

   The Port Fencing dialog box displays.

2. Right-click anywhere in the Ports table and select Expand.
3. Select a blocked port from the Ports table.
4. Click Unblock.
5. Click OK on the message.

   If you did not solve the root problem, the threshold will trigger again.

6. Click OK on the Port Fencing dialog box.

Avoiding port fencing inheritance

When you directly assign a threshold to an object, the threshold is inherited by all subordinate objects in the tree (unless they already have directly assigned thresholds). You cannot remove an inherited threshold from a subordinate object. However, the Management application allows you to effectively avoid inheritance for individual subordinate objects while maintaining inheritance for other subordinate objects. To avoid 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 Monitor > Fabric Watch > Port Fencing.

   The Port Fencing dialog box displays.

2. Select a threshold type from the Violation Type list.
3. Click Add.

   The Add *Type* Threshold dialog box displays.

4. Type a name for the new threshold (for example, AvoidProtocolError) in the Name field.
5. Select or enter the maximum number of errors or violations allowed in the Threshold errors/violations field.
6. Select the minimum time period available from the Threshold minutes/seconds list.
7. Click OK on the Add *Type* Threshold dialog box.
8. Click OK on the Port Fencing dialog box.

Editing thresholds

The Management application allows you to edit the name, number of events needed, and time period of ISL Protocol, Link, and Security thresholds.

Editing a C3 Discard Frames threshold

NOTE
This threshold is only available for Fabric OS devices.

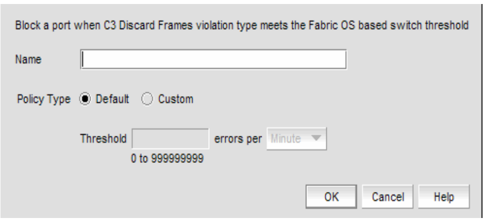
To edit a C3 Discard Frames threshold, complete the following steps.

1. Select Monitor > Fabric Watch > Port Fencing.

   The Port Fencing dialog box displays.

2. Select C3 Discard Frames (Fabric OS only) from the Violation Type list.
3. Select the threshold you want to change and click Edit.

   The Edit C3 Discard Frames dialog box displays.



Block a port when C3 Discard Frames violation type meets the Fabric OS based switch threshold

Name

Policy Type ● Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 306 Edit C3 Discard Frames Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.
6. Change the number of discarded frames allowed for the threshold in the **Threshold** field, if necessary.
7. Change the time period for the threshold from the **errors per** list, if necessary.
8. Click **OK** on the **Edit C3 Discard Frames Threshold** dialog box.

   If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 691.
9. Click **OK** on the **Port Fencing** dialog box.

Editing an Invalid CRCs threshold

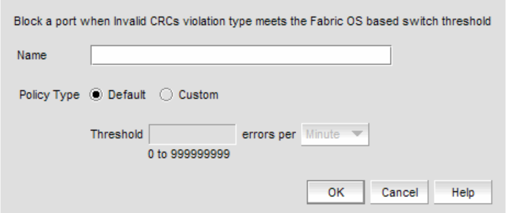
NOTE
This threshold is only available for Fabric OS devices.

To edit an Invalid CRCs threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing.**

   The **Port Fencing** dialog box displays.
2. Select **Invalid CRCs (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit.**

   The **Edit Invalid CRCs Threshold** dialog box displays.



Block a port when Invalid CRCs violation type meets the Fabric OS based switch threshold

Name

Policy Type ● Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 307 Edit Invalid CRCs Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.
6. Change the number of port events allowed for the threshold in the **Threshold** field, if necessary.
7. Change the time period for the threshold from the **errors per** list, if necessary.
8. Click **OK** on the **Edit Invalid CRCs Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.
9. Click **OK** on the **Port Fencing** dialog box.

Editing an Invalid Words threshold

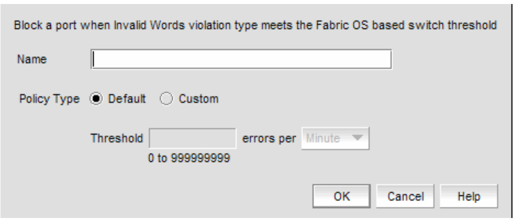
NOTE
This threshold is only available for Fabric OS devices.

To edit an Invalid Words threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing.**

   The **Port Fencing** dialog box displays.
2. Select **Invalid Words (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit.**

   The **Edit Invalid Words Threshold** dialog box displays.



Block a port when Invalid Words violation type meets the Fabric OS based switch threshold

Name

Policy Type ● Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 308 Edit Invalid Words Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.
6. Change the number of port events allowed for the threshold in the **Threshold** field, if necessary.
7. Change the time period for the threshold from the **errors per** list, if necessary.

8. Click **OK** on the **Edit Invalid Words Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.

9. Click **OK** on the **Port Fencing** dialog box.

Editing a Link threshold

NOTE
This threshold is only available for M-EOS devices.

To edit a Link threshold, complete the following steps.

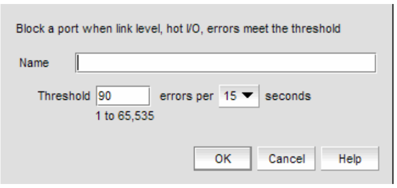
1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Link** from the **Violation Type** list.

3. Click **Edit**.

   The **Edit Link Threshold** dialog box displays.



Block a port when link level, hot I/O, errors meet the threshold

Name

Threshold 90 errors per 15 seconds

1 to 65,535

FIGURE 309 Edit Link Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.

5. Change the number of link events allowed for the threshold from the **Threshold** errors list.

6. Select the time period for the threshold (in minutes) from the **errors per** list.

7. Click **OK** on the **Edit Link Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.

8. Click **OK** on the **Port Fencing** dialog box.

Editing a Link Reset threshold

NOTE
This threshold is only available for Fabric OS devices.

To edit a Link Reset threshold, complete the following steps.

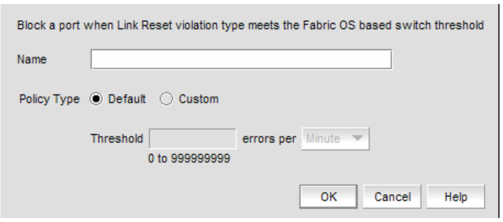
1. Select **Monitor** > **Fabric Watch** > **Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Link Reset (Fabric OS only)** from the **Violation Type** list.

3. Select the threshold you want to change and click **Edit**.

   The **Edit Link Reset Threshold** dialog box displays.



Block a port when Link Reset violation type meets the Fabric OS based switch threshold

Name

Policy Type ● Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 310 Edit Link Reset Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.

5. Select one of the following options:

   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.

6. Change the number of port events allowed for the threshold in the **Threshold** field, if necessary.

7. Change the time period for the threshold from the **errors per** list, if necessary.

8. Click **OK** on the **Edit Link Reset Threshold** dialog box.

   If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 691.

9. Click **OK** on the **Port Fencing** dialog box.

Editing a Protocol Error threshold

To edit a Protocol Error threshold, complete the following steps.

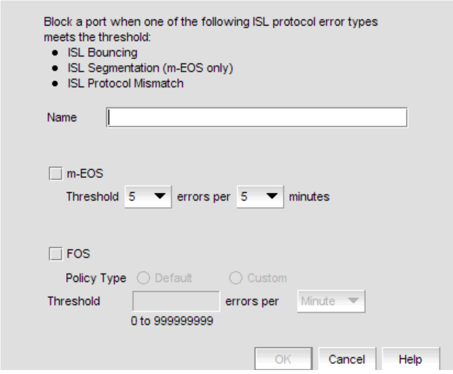
1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Protocol Error** from the **Violation Type** list.

3. Select the threshold you want to change and click **Edit**.

   The **Edit Protocol Error Threshold** dialog box displays.



Block a port when one of the following ISL protocol error types meets the threshold:

- ISL Bouncing
- ISL Segmentation (m-EOS only)
- ISL Protocol Mismatch

Name

□ m-EOS

Threshold 5 errors per 5 minutes

□ FOS

Policy Type ○ Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 311 Edit Protocol Error Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.

5. (M-EOS devices only) Change the **M-EOS** Protocol Error thresholds by completing the following steps.

   a. Change the number of protocol errors allowed for the threshold from the **Threshold** errors list, if necessary.

   b. Change the time period for the threshold (in minutes) from the **errors per** list, if necessary.

6. (Fabric OS devices only) Change the **Fabric OS** Protocol Error thresholds by completing the following steps.

   a. Select one of the following options:

      - Default—Uses device defaults. Go to step 7.
      - Custom—Uses your selections. Continue with step b.

   b. Change the number of protocol errors allowed for the threshold from the **Threshold** errors list, if necessary.

   c. Change the time period for the threshold from the **errors per** list, if necessary.

7. Click **OK** on the **Edit Protocol Error Threshold** dialog box.

   If the threshold has already been assigned to ports, an "Are you sure you want to make the requested changes to this threshold on "X" ports?" message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to "Assigning thresholds" on page 691.

8. Click **OK** on the **Port Fencing** dialog box.

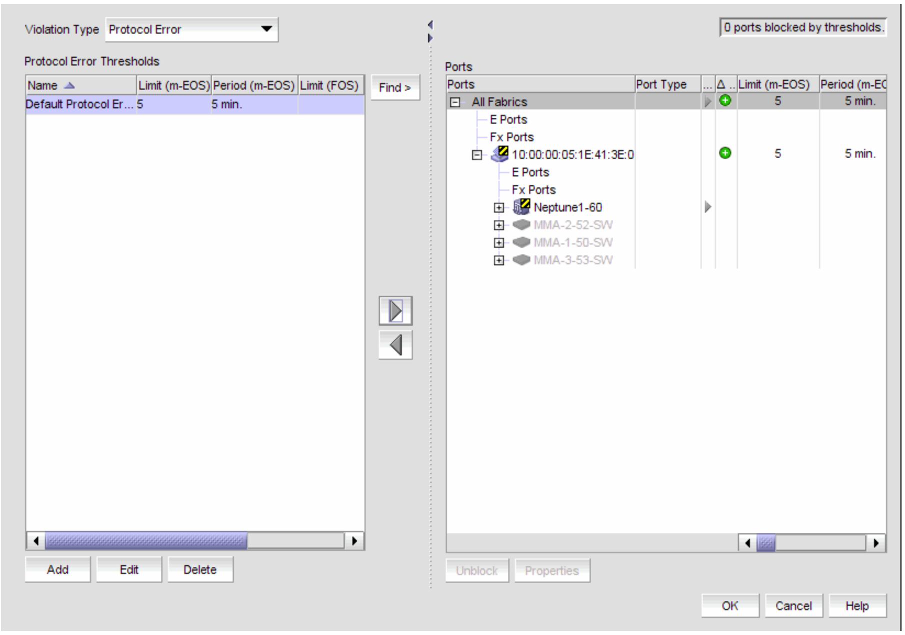
Editing a State Change threshold

NOTE
This threshold is only available for Fabric OS devices running 6.3 or later.

To edit an State Change threshold, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays (Figure 312).



Violation Type: Protocol Error

Protocol Error Thresholds

Name	Limit (m-EOS)	Period (m-EOS)	Limit (FOS)
Default Protocol Er...	5	5 min.	

0 ports blocked by thresholds.

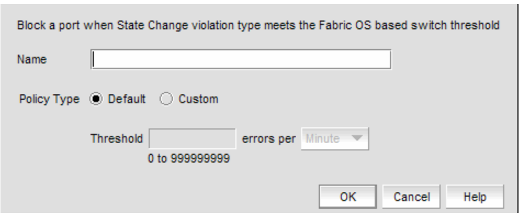
Ports

Ports	Port Type	...	Δ ..	Limit (m-EOS)	Period (m-EC
All Fabrics			●	5	5 min.
E Ports					
Fx Ports					
10:00:00:05:1E:41:3E:0			●	5	5 min.
E Ports					
Fx Ports					
Neptune1-60					
MMA-2-52-SW					
MMA-1-50-SW					
MMA-3-53-SW					

FIGURE 312 Port Fencing dialog box

2. Select **State Change (Fabric OS only)** from the **Violation Type** list.
3. Select the threshold you want to change and click **Edit**.

   The **Edit State Change Threshold** dialog box displays.



Block a port when State Change violation type meets the Fabric OS based switch threshold

Name

Policy Type ● Default ○ Custom

Threshold errors per Minute

0 to 999999999

FIGURE 313 Edit State Change Threshold dialog box

4. Change the name for the threshold in the **Name** field, if necessary.
5. Select one of the following options:
   - Default—Uses device defaults. Go to step 8.
   - Custom—Uses your selections. Continue with step 6.

6. Edit the number of state changes allowed for the threshold in the **Threshold** errors field, if necessary.

7. Change the time period for the threshold from the **errors per** list, if necessary. The following choices are available:

   - None—the port is blocked as soon as the specified number of invalid CRCs allowed is met.
   - Second—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a second.
   - Minute—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a minute.
   - Hour—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a hour.
   - Day—the port is blocked as soon as the specified number of invalid CRCs allowed is reached within a day.

8. Click **OK** to add the state change threshold to the table and close the **Edit State Change Threshold** dialog box.

   To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 691.

9. Click **OK** on the **Port Fencing** dialog box.

Editing a Security threshold

NOTE
This threshold is only available for M-EOS devices.

To edit a Security threshold, complete the following steps.

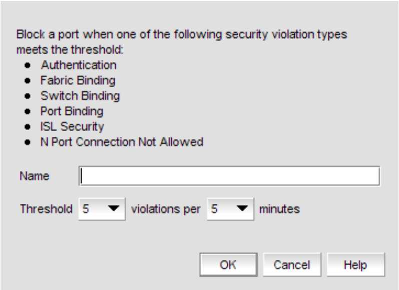
1. Select **Monitor** > **Fabric Watch** > **Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select **Security** from the **Violation Type** list.

3. Select the threshold you want to change and click **Edit**.

   The **Edit Security Threshold** dialog box displays.



Block a port when one of the following security violation types meets the threshold:

- Authentication
- Fabric Binding
- Switch Binding
- Port Binding
- ISL Security
- N Port Connection Not Allowed

Name

Threshold 5 violations per 5 minutes

FIGURE 314 Edit Security Threshold dialog box

4. 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 list, if necessary.
6. Change the time period for the threshold from the **violations per** list, if necessary.
7. Click **OK** on the **Edit Security Threshold** dialog box.

   If the threshold has already been assigned to ports, an “Are you sure you want to make the requested changes to this threshold on “X” ports?” message displays. Click **OK** to close.

   To assign this threshold to fabrics, switches, or switch ports, refer to “Assigning thresholds” on page 691.
8. Click **OK** on the **Port Fencing** dialog box.

Finding assigned thresholds

The Management application allows you to find all ports with a specific threshold applied.

NOTE
This search is performed on the threshold name. Since Fabric OS devices do not retain the threshold name, the ability to search for a threshold on a Fabric OS device is not available in most cases.

To find assigned thresholds, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing.**

   The **Port Fencing** dialog box displays.
2. Select a threshold type from the **Violation Type** list.
3. Select a threshold from the **Threshold** table.
4. Click **Find.**
5. Every port which uses the selected threshold is highlighted in the **Ports** table.
6. Click **OK** on the **Port Fencing** dialog box.

Viewing thresholds

1. Select **Monitor > Fabric Watch > Port Fencing.**

   The **Port Fencing** dialog box displays.
2. Select a threshold type from the **Violation Type** list.
3. Review the **Thresholds** and **Ports** tables.
4. Repeat step 2 and step 3, as necessary.
5. Click **OK** on the **Port Fencing** dialog box.

Viewing all thresholds on a specific device

To view all thresholds assigned to a specific switch, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Right-click anywhere in the **Ports** table and select **Expand**.
3. Right-click the device for which you want to view threshold information and select **Switch Thresholds.**

   The **Switch Thresholds** dialog box displays with a list of all thresholds assigned to the selected switch.

4. Review the **Thresholds** table.
5. Click **Close** on the **Switch Thresholds** dialog box.
6. Click **OK** on 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 Management application 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.

Removing thresholds from individual objects

To remove thresholds from the All Fabrics object, an individual Fabric, Chassis group, Switch, or Switch Port, complete the following steps.

1. Select **Monitor > Fabric Watch > Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select the object with the threshold you want to remove in the **Ports** table.

4. Click the left arrow.

NOTE
If the selected object inherits a threshold assignment from an object higher in the tree, you cannot remove the threshold. However, you may assign a different threshold directly to the selected subordinate objects or change the assignment on the higher object.

A removed icon (⊖) displays next to every instance where the threshold was removed from a selected object and it does not inherits a threshold from higher in the tree.

If an inherited threshold replaces the removed threshold, an added icon (⊕) displays next to every instance where the threshold was replaced.

A directly assigned icon (▶) displays next to each object with an assigned threshold which does not inherit a threshold from higher in the tree.

NOTE
If you remove a threshold from All Fabrics, it removes the threshold from individual Fabrics, switches, and switch ports in all Fabrics except for a Chassis group. You must remove repeat the procedure for the Chassis group.

5. Click **OK** on the **Port Fencing** dialog box.

Removing thresholds from the thresholds table

To remove thresholds from all Fabrics, Switches, and Switch Ports as well as the **Threshold** table, complete the following steps.

1. Select **Monitor** > **Fabric Watch** > **Port Fencing**.

   The **Port Fencing** dialog box displays.

2. Select a threshold type from the **Violation Type** list.
3. Select the threshold you want to remove in the **Thresholds** table.
4. Click **Delete**.

   A removed icon (⊖) displays next to the selected threshold in the **Thresholds** table when you click **Delete**.

5. Click **OK** on the **Port Fencing** dialog box.

Chapter

VLAN Management 24

In this chapter

VLAN Manager

VLAN Manager allows you to manage Virtual Local Area Networks (VLANs) on Brocade products. You can use VLAN Manager to configure port VLANs. By default, interfaces on a Brocade device that are not assigned to a VLAN are members of the default port VLAN; therefore, all device interfaces assigned to the default VLAN constitute a single Layer 2 broadcast domain.

When you assign an interface to a port VLAN, that interface is automatically removed from VLAN 1. Interfaces assigned to port VLANs can be defined as untagged, tagged, and converged ports. An untagged port can be a member of only one VLAN, while a tagged port can be a member of more than one VLAN. Interfaces defined as converged allow tagged and untagged traffic to pass through an interface at the same time.

Default VLAN

When you enable port-based VLANs, all ports in the system are added to the default VLAN. By default, the default VLAN ID is 1. The default VLAN is configurable. If you want to use the VLAN ID "VLAN 1" as a configurable VLAN, you can assign a different VLAN ID to the default VLAN.

You must specify a valid VLAN ID that is not already in use. For example, if you have already defined VLAN 10, do not try to use "10" as the new VLAN ID for the default VLAN. Valid VLAN IDs are 1 through 4095.

NOTE
Default VLANs are not configurable on Data Center Bridging (DCB) products.

Super Aggregated VLAN

A super aggregated VLAN allows multiple VLANs to be placed within another VLAN. This feature allows you to construct Layer 2 paths and channels. It is useful for Virtual Private Network (VPN) applications in which you need to provide a private, dedicated, Ethernet connection for an individual client who can transparently reach its subnet across multiple networks.

Configuration requirements for VLAN Manager

Before you can manage VLANs with VLAN Manager, you must complete the following tasks:

- Make sure that the discovery process has been run. Discovery captures configuration information from Brocade products and places that information in the Management application database. Refer to Chapter 4, “Discovery” for details on running discovery.
- Make sure the VLAN Manager privilege is in your Management application user role or account if you need to use VLAN Manager.
- If you want to view VLAN connectivity in the Layer 2 topology, make sure Foundry Discovery Protocol (FDP) or Link Layer Discovery Protocol (LLDP) is enabled on the products on the network.

Displaying a list of VLANs

To view the list of VLANs that were discovered on the network, select **Configure > VLANs** from either the SAN or the IP tab.

The **VLAN View** tab of the **VLAN Manager** dialog box displays.

The VLAN Manager tool bar contains the following buttons:

- Add—Launches the Add VLAN dialog box
- **Edit**—Launches the Edit VLAN dialog box
- **Delete**—Deletes a VLAN.
- **STP**—Allows you to configure STP, RSTP, or MSTP information for a product, port, or VLAN.
- **ACL**—Launches the ACL Configuration dialog box, where you can assign access control lists to a VLAN.
- **802.1ag CFM**—If the Management application manages at least one of service provider products (NetIron XMR, MLX, CES, or CER), this button launches the 802.1ag CFM configuration dialog box.
- **Virtual Port IP**—Launches the IP Address dialog box which allows you to add an IP address to a switch virtual interfaces (SVI) on DCB products (also known as a virtual routing interface on IOS products).

VLAN Manager tabs

VLAN Manager has two views:

- VLAN View

  Displays distinct Layer 2 broadcast domains by VLAN ID. If FDP or LLDP is not enabled on a device, each VLAN from each device is displayed in separate folders by VLAN ID. If FDP or LLDP is enabled on the products, a VLAN folder shows device connectivity on the Layer 2 broadcast domains.

  If there are super-aggregated VLANs that have been configured on the network, VLANs are grouped by their super-aggregated VLAN memberships.

- Product View

  Displays the VLANs configured on a product. The information is grouped by products. Select a product to view the VLANs that are on that product.

Displaying VLANs in the VLAN View

The **VLAN View** tab displays all the VLANs discovered on the network and lists them by VLAN IDs.

To view the VLANs in the **VLAN View** tab, complete the following steps.

1. Click the **VLAN View** tab in the **VLAN Manager** dialog box to display all the port VLANs.
2. Expand the folder under the **VLAN View** tab, then double-click a super-aggregated VLAN to display its port VLANs.

   VLANs are listed by their topologically distinct broadcast domains. A VLAN that is listed several times means that the products on which the VLAN has been configured cannot communicate with each other. Either they are not physically connected or FDP or LLDP is not enabled on these products. If FDP or LLDP is enabled, then each VLAN lists the products in that broadcast domain.
3. Select a VLAN to expand the list of products listed under that VLAN. Use the Search tool to find VLANs, products, or ports quickly.

   A VLAN may be listed several times. For example, the first three VLAN1s have only one product. Each product in each VLAN is in its own broadcast domain and either does not have connectivity with other products or FDP or LLDP is not enabled on that product.

   The fourth VLAN1 has several products listed under it. All those products are in the same Layer 2 broadcast domain.

   While a port VLAN is selected, the **Add** and **Delete** buttons become available. At this point, you can create or modify port VLANs, delete a port VLAN, and configure STP or RSTP definitions.
4. Click a product under a port VLAN to select it. The interfaces on that product that belong to the VLAN are listed in the interface list.

   The list shows the following information:

   - Port—The interface number. This can be a port number represented as a unit, slot number or port number, or a virtual routing interface ID.
   - Port Type—A description of the type of interface on the product, for example, ETHERNET_INTERFACE or VIRTUAL_INTERFACE.
   - Port Name—The name of the interface, if one was configured.
   - Port Mode—Indicates the tag mode of the interface. Tagged represents the port is in dual mode but is in the tagged state for that particular VLAN. Untagged represents the port is untagged for that particular VLAN. The third port mode is Converged.
   - STP—Indicates If STP is enabled or disabled.
   - Path Cost—The STP cost of using the port to reach the root bridge.
   - Port Priority—The preference that STP gives this port relative to other ports for forwarding traffic out of the spanning tree.
   - Classifiers—The VLAN Classifier group IDs associated with Access/Converged ports and LAGS (for DCB products only). This column is empty for trunk ports and for ports from IOS products.

Displaying VLANs by products

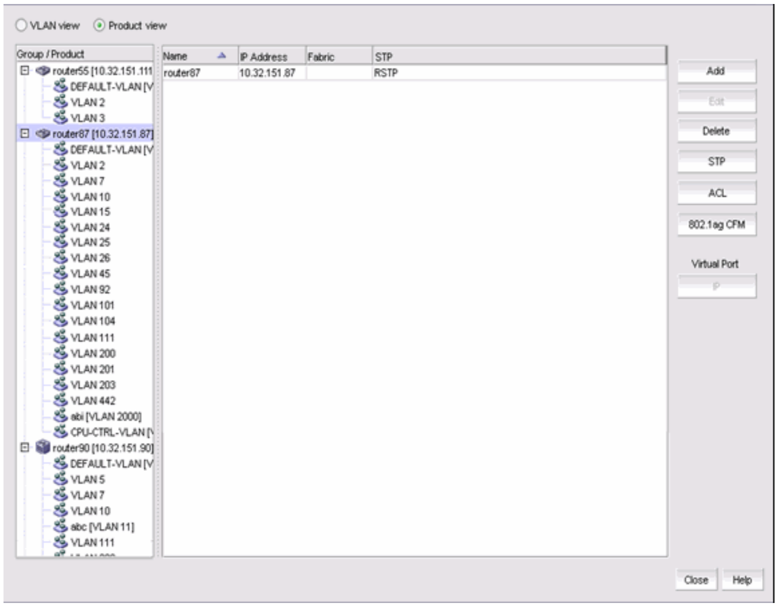
The **Product View** tab of the **VLAN Manager** dialog box presents the products that have been discovered on the network and the VLANs that have been assigned to them.

NOTE
Only products assigned to Management application areas of responsibility (AORs) are listed under the VLANs in the **Product View** tab.

To view VLANs, complete the following steps.

1. Click the **Product View** tab in the **VLAN Manager** dialog box.

   The **VLAN Manager - Product View** dialog box displays.



○ VLAN view ● Product view

Group / Product
- router55 [10.32.151.111
  - DEFAULT-VLAN [V
  - VLAN 2
  - VLAN 3
- router87 [10.32.151.87]
  - DEFAULT-VLAN [V
  - VLAN 2
  - VLAN 7
  - VLAN 10
  - VLAN 15
  - VLAN 24
  - VLAN 25
  - VLAN 26
  - VLAN 45
  - VLAN 92
  - VLAN 101
  - VLAN 104
  - VLAN 111
  - VLAN 200
  - VLAN 201
  - VLAN 203
  - VLAN 442
  - abi [VLAN 2000]
  - CPU-CTRL-VLAN [\
- router90 [10.32.151.90]
  - DEFAULT-VLAN [V
  - VLAN 5
  - VLAN 7
  - VLAN 10
  - abc [VLAN 11]
  - VLAN 111

Name	IP Address	Fabric	STP
router87	10.32.151.87		RSTP

FIGURE 315 Product View tab of the VLAN Manager dialog box

   The highest level of the VLAN list displays Products.

2. Expand a product to display the port VLANs that have been configured on that product.
3. Click a VLAN in the list to display the interfaces on that product that belong to the VLAN.

Port VLANs

VLAN Manager facilitates the creation, modification, and deletion of port VLANs on products that are known to the Management application. It also aids in the bulk deployment of these VLANs. For example, VLAN 3 may be configured on four products. If the VLAN definition for VLAN 3 is modified, the new definition can be deployed to all four products at one time.

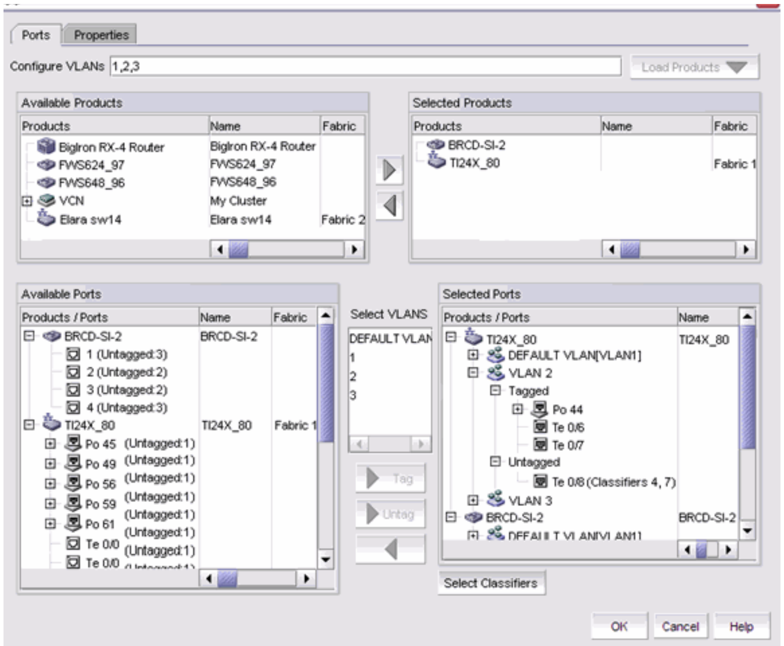
The Configure Port VLAN function in VLAN Manager allows you to define a port VLAN definition that adds a new VLAN to a product or modify an existing port VLANs on a product. The port VLANs can be designated as tagged, untagged, or dual-mode.

Adding or modifying Port VLANs

To create or modify port VLANs, complete the following steps.

1. On the VLAN Manager dialog box, click the **VLAN View** or **Product View** tab to enable the **Add** button.
2. Click **Add** to add port VLANs or click **Edit** to modify port VLANs.

   The **Edit VLAN** dialog box, Ports tab, shown in Figure 316, displays. It is identical to the **Add VLAN** dialog box, but the VLANs associated with the selected product are pre-populated on the Configure VLANs field.



Configure VLANs: 1,2,3

FIGURE 316 Edit VLAN dialog box, Ports tab

3. Enter a VLAN ID in the **Configure VLANs** field.

   You can enter more than one ID, separating individual IDs with a comma (for example, 10, 45, 79, 30). You can also enter ranges of VLAN IDs (for example, 41-51).

4. Click the **Load Products** button. Products that already have the entered VLAN IDs configured on them are automatically moved to the **Selected Products** panel. The **Load Products** button is disabled by default.
5. Under the **Available Products** list, select one or more products to which the VLAN will be assigned. You can also use the Search tool to find ports.
6. Click the right arrow button to move your selection to the **Selected Products** list.
7. Expand the folder for a selected product in the **Available Ports** list to display all the interfaces or trunk groups on the product that can be added to the VLAN.

   The **Selected Ports** list displays the list of configured VLANs. Initially these VLANs contain no ports. If no ports or trunk groups are selected, an empty VLAN is created on the products (DCB products only). If no ports are selected for IOS products, an error message displays.

8. In the **Available Ports** list, select the interfaces that you want to assign to a VLAN.

   If you place your pointer over an interface in the **Available Ports** list, a tool tip appears, showing the VLAN assignment of the interface. You can also use the Search tool bar to search for ports under the **Available Ports** list, then assign the ports found to the VLAN.

9. In the **Select VLANs** list, select the VLAN you want to assign to the selected interfaces. The list includes the Default VLAN (VLAN1) and the VLAN or VLANs you are currently creating. You can assign one or more VLANs to the selected ports.

   In the **Selected Ports** list, each VLAN node is shown as Tagged, Untagged, or Converged. If a port is already tagged in one VLAN, it can be marked as Tagged in other VLANs. The port can also be marked as Untagged in other VLANs, which changes its mode to Dual mode.

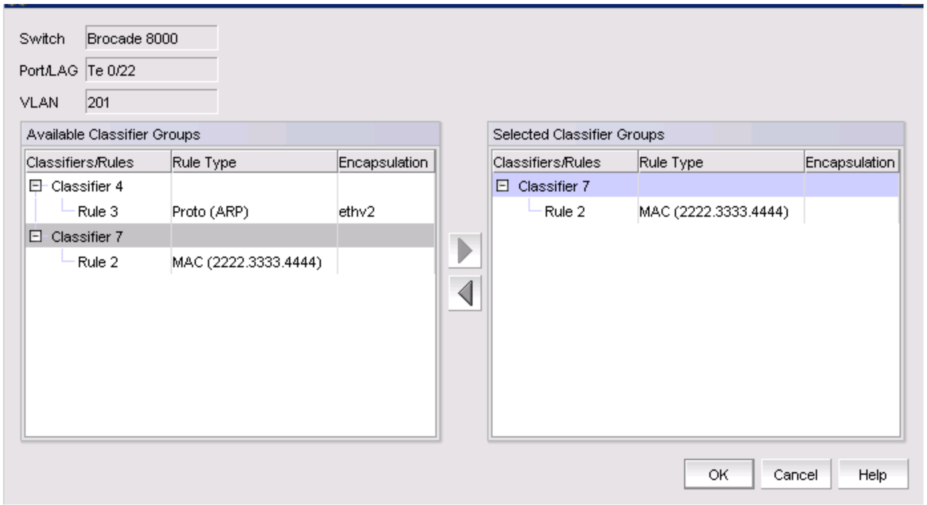
10. Complete one of the following tasks.

    - If you want to assign the interface to the VLAN as an untagged port, click **Untag**.
    - If you want to assign the interface to the VLAN as a tagged port, click **Tag**.
    - If you want to make the VLAN on the interface dual-mode, assign that interface as Tagged and select the same interface and assign as Untagged to another VLAN. Dual mode ports can be added to any VLAN except for the default (VLAN 1).

    NOTE
    Check the release notes for your product to determine the VLAN support available on that product.

    The **Select Classifiers** button is disabled by default. To enable the button, select a single row in the **Selected Ports** list.

11. Click the **Select Classifiers** button to launch the **Select Classifier Groups** dialog box, shown in Figure 317, where you can assign classifiers and rules for supported DCB platform-based VLANs.



Switch: Brocade 8000

Port/LAG: Te 0/22

VLAN: 201

Available Classifier Groups

Classifiers/Rules	Rule Type	Encapsulation
⊟ Classifier 4		
Rule 3	Proto (ARP)	ethv2
⊟ Classifier 7		
Rule 2	MAC (2222.3333.4444)	

Selected Classifier Groups

Classifiers/Rules	Rule Type	Encapsulation
⊟ Classifier 7		
Rule 2	MAC (2222.3333.4444)	

FIGURE 317 Select Classifier Groups dialog box

Adding or modifying dual-mode ports

You can configure an interface in a VLAN as a dual-mode port by assigning it as a tagged port to one VLAN and as an untagged port to another VLAN. You can add a dual-mode port to any VLAN except the default VLAN, VLAN 1.

To add a dual-mode port to a VLAN, perform the following steps.

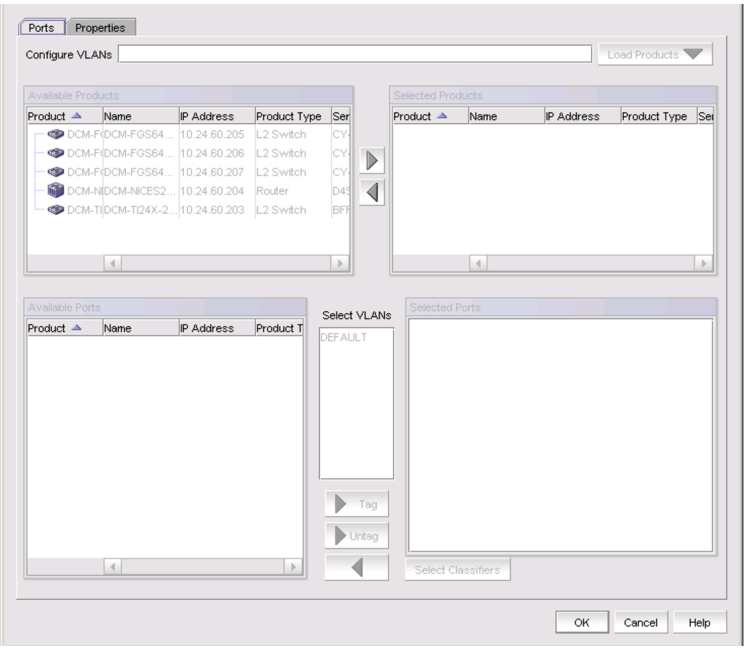
1. Read the steps in the section "Adding or modifying Port VLANs" on page 707 to familiarize yourself with adding tagged and untagged ports to a VLAN.
2. From the **Available Ports** list on the **Port VLAN Configuration** dialog box, select the interface that will be added as a dual-mode port.
3. Select a VLAN from the **Select VLANs** list.
4. Click the **Untag >>** button to assign the port as an untagged port into the selected VLAN. The Selected Ports list shows the interface listed under the VLAN to which it was assigned.
5. Select the same interface from the **Available Ports** list.
6. Select another VLAN from the **Select VLANs** list.
7. Click the **Tag >>** button to assign it as a tagged port to the second VLAN. The **Selected Ports** list shows the port as untagged under one VLAN and tagged under another VLAN.

Adding VLAN Properties

The **Add VLAN** dialog box has two tabs: **VLAN View** and **Product View**. The VLAN properties vary for IOS and DCB products. When an IOS VLAN is selected, the Name, QoS, and Router Interface fields display. When a DCB VLAN or product is selected and moved to the Products/VLAN list, the Name and Admin Status fields and the FCoE check box display. All the fields displayed for DCB products are read-only.

1. On the **Add VLAN** dialog box, click the Properties tab.

   The **Add VLAN** dialog box in VLAN View displays, as shown in Figure 318.



Configure VLANs

Available Products

Product	Name	IP Address	Product Type	Ser
DCM-F(	DCM-FGS64...	10.24.60.205	L2 Switch	CY(
DCM-F(	DCM-FGS64...	10.24.60.206	L2 Switch	CY(
DCM-F(	DCM-FGS64...	10.24.60.207	L2 Switch	CY(
DCM-NI	DCM-NICES2...	10.24.60.204	Router	D4S
DCM-TI	DCM-TI24X-2...	10.24.60.203	L2 Switch	BFF

FIGURE 318 Add VLAN dialog box - VLAN Properties pane - Product View

2. Click the **VLAN View** option to view the products to which the VLANs are to be deployed, or click the **Product View** option to display the VLANs that are to be deployed to that product.
3. Select and expand a product entry to display the VLANs that are to be deployed to that product.
4. Select and expand a VLAN entry to display the products to which it will be deployed.
5. Enter the following information for IOS products:
   - **Name**—Displays the name of the VLAN (not editable).
   - **QoS**—Select a QoS level from the list.
     - Select Low (None or 0) through High (7) for NetIron CES products. Select None for NetIron CER and NetIron CES products if the product does not have VLAN priority configured (None applies only to NetIron CER and NetIron CES products).
     - Select Low (0) through High (7) for all other Brocade IP products.

- Router Interface

  If you want to add a virtual routing interface to the VLAN, enter the virtual routing interface number in this parameter. You can add an IP address to the virtual routing interface once the VLAN is deployed. From the **Product View** tab, you can configure one virtual routing interface per VLAN, for each product. From the **VLAN View** tab, you can edit virtual routing interfaces on multiple products for a specific VLAN.

  NOTE
  The **Router Interface** field is editable for products that support routing and have router image of the firmware installed.

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

Modifying port VLAN properties

Complete the following steps to modify port VLANs using the **VLAN View** tab or the **Product View** tab on the **Edit VLAN** dialog box.

1. On the VLAN Manager dialog box, click the **VLAN View** or **Product View** tab.
2. If in the VLAN view, select and expand a VLAN entry or if in the Product view, select and expand a product and click the **Edit** button.

   The **Edit VLAN** dialog box, **Ports** tab displays.
3. Modify the following information for IOS products:
   - **Name**—Displays the name of the VLAN (not editable).
   - **QoS**—Select a QoS level from the list.
     - Select either Normal or High as the QoS level for Brocade IP stackable products.
     - Select Low (None or 0) through High (7) for NetIron CES products. Select None for NetIron CER and NetIron CES products if the product does not have VLAN priority configured (None applies only to NetIron CER and NetIron CES products).
     - Select Low (0) through High (7) for all other Brocade IP products.
   - Router Interface

     If you want to add a virtual routing interface to the VLAN, enter the virtual routing interface number in this parameter. You can add an IP address to the virtual routing interface once the VLAN is deployed. From the **Product View** tab, you can configure one virtual routing interface per VLAN, for each product. From the **VLAN View** tab, you can edit virtual routing interfaces on multiple products for a specific VLAN.

     NOTE
     The **Router Interface** field is editable for products that support routing and have router image of the firmware installed.
4. Click **OK** to save the changes.

Deleting port VLANs from products

Deleting a port VLAN removes all the interfaces on a product from that VLAN. A port VLAN can be deleted in both the VLAN and Product views.

Deleting a port VLAN in the VLAN view

1. On the **VLAN Manager** dialog box, select the **VLAN** view.
2. Select the VLAN to be deleted. You can select multiple VLANs by holding down the **Ctrl** key and clicking the VLAN nodes.
3. Click **Delete** to launch the **Deploy VLANs** dialog box.
4. Deploy the VLAN configuration to the product by completing deployment steps in the section "Deploying VLAN configurations" on page 713.

Once the VLAN is deployed, it is deleted from the product.

Deleting a port VLAN in the Product view

1. On the **VLAN Manager** dialog box, select the **Product** view.
2. Expand the product on which you want the VLAN to be deleted.
3. Select the VLAN under the product. You can select multiple VLANs by holding down the **Ctrl** key and clicking the VLAN nodes.
4. Click **Delete** to launch the **Deploy VLANs** dialog box.
5. Deploy the VLAN configuration to the product by completing deployment steps in the section "Deploying VLAN configurations" on page 713.

Once the VLAN is deployed, it is deleted from the product.

Assigning DCB ports to a VLAN

In Data Center Bridging (DCB) switches, the L2 mode of the port determines whether a port can be in an untagged, tagged, or dual mode. Table 43 shows the L2 mode and tagged mode compatibility on the DCB interface.

TABLE 43 L2 mode and tagged mode compatibility on a DCB interface

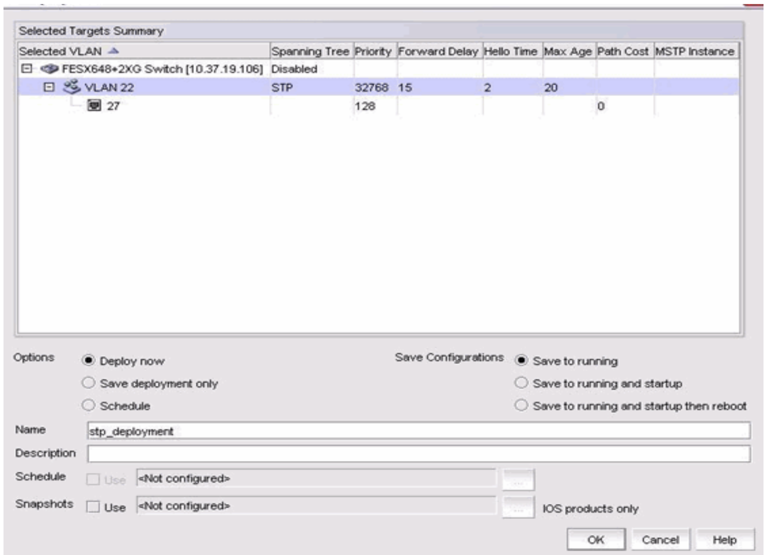
L2 mode	Tagged mode
Access, Converged	Untagged
Trunk, Converged	Tagged
Converged	Dual

NOTE
To make L2 interface mode changes, you must have the DCB Management privilege.

You can change the L2 interface mode of a port using the Add LAG dialog box. See "Adding a LAG" on page 350 for instructions.

Deploying VLAN configurations

The **Deploy VLAN**s dialog box allows you to deploy a VLAN configuration to target products.



Selected Targets Summary

Selected VLAN	Spanning Tree	Priority	Forward Delay	Hello Time	Max Age	Path Cost	MSTP Instance
⊟ FESX648+2XG Switch [10.37.19.106]	Disabled						
⊟ VLAN 22	STP	32768	15	2	20		
27		128				0	

Options ● Deploy now ○ Save deployment only ○ Schedule

Save Configurations ● Save to running ○ Save to running and startup ○ Save to running and startup then reboot

Name: stp_deployment

Description:

Schedule □ Use <Not configured>

Snapshots □ Use <Not configured> IOS products only

FIGURE 319 STP/RSTP Configuration dialog box - Deployment Properties pane

1. Select a deployment option:
   - Click the **Deploy now** option if you want to deploy the VLAN definition.
   - Click the **Save deployment only** option if you want to save the VLAN definition without scheduling its deployment.
   - Click the **Schedule** option if you want to schedule the deployment of the VLAN definition.
2. Select a **Save Configuration** option:
   - Click the **Save to running** option to save the configuration while the system is running.
   - Click the **Save to running and startup** option to save the save the configuration both while the system is running and when the system starts up.
   - Click the **Save to running and startup then reboot** option to save the configuration both while the system is running and when the system starts up, and then automatically reboots.
3. Click the **Schedule** check box, which is available if you selected **Schedule** as a deployment option, to select a frequency.
4. Enter a name in the **Name** field that will be used to identify the configured VLAN.
5. Enter a description in the **Description** field that will be used to identify the configured VLAN.
6. Click the **Snapshots** check box if you want the Management application to run and save a report after this configuration is deployed to the device. You can run snapshots before and after deployments only for IOS products. Snapshots are not supported for DCB products.
7. Click **OK** to deploy the configuration on the selected port VLAN.
8. Click **OK**.

   The **Deployment Status** dialog box launches.

9. Click **Start** on the **Deployment Status** dialog box to save the changes to the selected products.
10. Click **Close** to close the **Deployment Status** dialog box.

Spanning Tree Protocol Configuration

Spanning Tree Protocol (STP) is a Layer 2 protocol that ensures a loop-free topology for any bridged local area network (LAN). STP allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails. STP creates a spanning tree within a mesh network of connected Layer 2 bridges and disables those links that are not part of the tree, leaving a single active path between any two network nodes.

The Management application supports the following types of STP:

- STP—The Spanning tree protocol (IEEE 802.1d) is a link layer network protocol that ensures a loop-free topology for any bridged LAN.
- RSTP—Rapid Spanning Tree Protocol (IEEE 802.1w internet standard) is a refinement of STP, which provides for faster spanning tree convergence after a topology change.
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s internet standard) allows several VLANs to be mapped to a reduced number of spanning-tree instances. This is possible since most networks do not need more than a few logical topologies. Each instance handles multiple VLANs that have the same Layer 2 topology.

  MSTP allows formation of MST regions that can run multiple MST instances (MSTI). Multiple regions and other STP bridges are interconnected using one single Common Spanning Tree (CST).

STP or RSTP configuration on a port VLAN

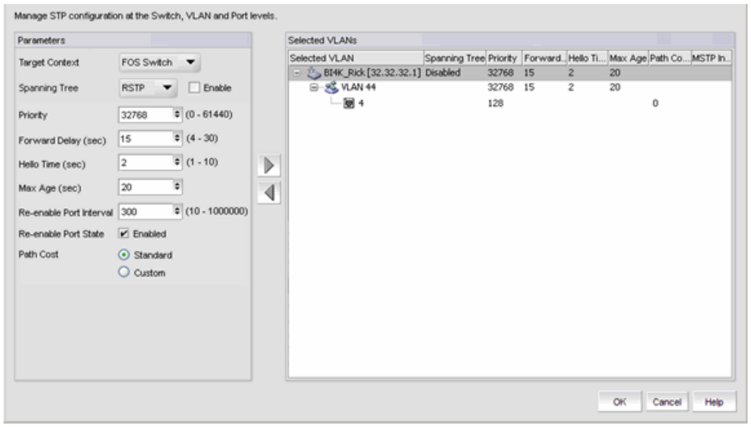
You can configure STP and RSTP attributes from the **VLAN View** tab or the **Product View** tab.

1. Perform one of the following tasks to select the VLAN on which STP or RSTP will be configured:
   - On the **VLAN View** tab, expand the list of VLANs and select one or multiple VLANs on which STP, RSTP, or MSTP will be configured.
   - On the **Product View** tab, expand the product, product group, or IP subnet folder that contains the products on which the VLAN you want is configured. Then expand the entry to display its VLAN and select the VLAN where STP or RSTP will be configured. You can select more than one VLAN from this tab

   For either view, you can use the Search tool to look for the VLAN on which STP or RSTP will be configured.

   Either of these methods enables the **STP** button on the **VLAN Manager** dialog box.
2. Click the **STP** button on the **VLAN Manager** dialog box to display the **STP Configuration** dialog box.

   The products on which the VLAN is configured appear on the dialog box, shown in Figure 322.



Manage STP configuration at the Switch, VLAN and Port levels.

Parameters

Target Context: FOS Switch

Spanning Tree: RSTP □ Enable

Priority: 32768 (0 - 61440)

Forward Delay (sec): 15 (4 - 30)

Hello Time (sec): 2 (1 - 10)

Max Age (sec): 20

Re-enable Port Interval: 300 (10 - 1000000)

Re-enable Port State: ☑ Enabled

Path Cost: ● Standard ○ Custom

Selected VLANs

Selected VLAN	Spanning Tree	Priority	Forward...	Hello Ti...	Max Age	Path Co...	MSTP In...
BI4K_Rick [32.32.32.1]	Disabled	32768	15	2	20		
VLAN 44		32768	15	2	20		
4		128				0	

FIGURE 320 STP/RSTP Configuration dialog box

3. Select the target switch, VLAN, or port from the **Target Context** list.

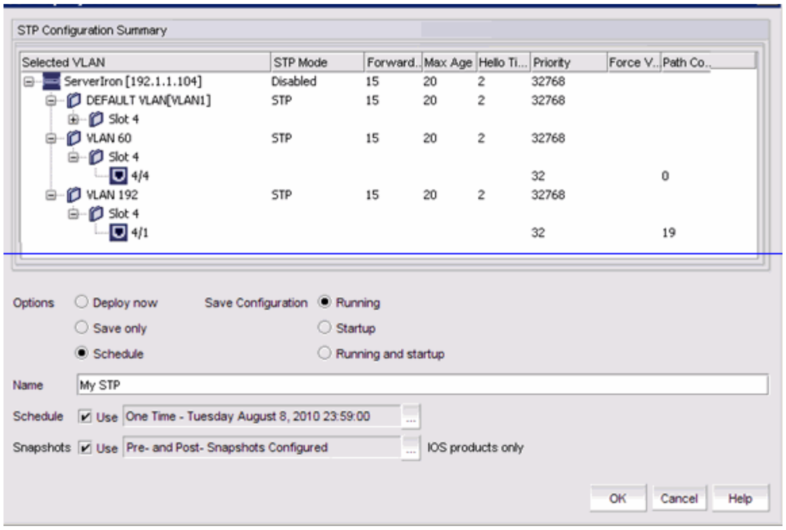
4. Specify the following information:

   - Select STP or RSTP from the **Spanning Tree** list.
   - Select the **Enable** check box if you want to enable the protocol you selected.
   - Enter a value in the **Priority** field to identify the root bridge in a spanning tree (instance of STP). The bridge with the lowest value has the highest priority and is the root. A higher numerical value means a lower priority; thus, the highest priority is 0. The values range from 0 through 65535. The default is 32768.
   - Enter the number of seconds a bridge waits (the listen and learn period) before it begins to forward data packets in the **Forward Delay** field. The values range from 4 through 30 seconds. The default is 15 seconds.
   - Enter the number of seconds a root bridge waits before it sends the next BPDU in the **Hello Time** field. The values range from 1 through 10 seconds. The default is 2 seconds.
   - Enter the number of seconds a bridge waits for a hello packet from the root bridge before initiating a topology change in the **Maximum Age** field. The values range from 6 through 40 seconds. The default is 20 seconds.
   - The **Force Version** list is available only if you selected RSTP. This parameter forces the bridge to send BPDUs in a specific format. You can enter one of the following values:
     - 0: The bridge has been forced to operate in an STP compatibility mode.
     - 2: The bridge has been forced to operate in an 802.1W mode. (This is the default.)
   - Enter a cost in the **Path Cost** field, which is the cost of using the port to reach the root bridge. When selecting among multiple links to the root bridge, STP chooses the link with the lowest path cost and blocks the other paths. Each port type has its own default STP path cost.
   - Enter the preference in the **Port Priority** field that STP gives to this port relative to other ports for forwarding traffic out of the spanning tree. A higher numerical value means a lower priority; thus, the highest priority is 0. The values range from 0 through 240. The default is 128.
   - Click the right arrow button to move the selected product to the Selected VLANs list.

5. Click **OK** to launch the Deploy STP dialog box.

Deploying STP configuration on a port VLAN

The Deploy VLAN dialog box allows you to deploy an STP configuration to target products. The Selected Targets Summary list



STP Configuration Summary

Selected VLAN	STP Mode	Forward..	Max Age	Hello Ti...	Priority	Force V..	Path Co..
ServerIron [192.1.1.104]	Disabled	15	20	2	32768		
DEFAULT VLAN[VLAN1]	STP	15	20	2	32768		
Slot 4							
VLAN 60	STP	15	20	2	32768		
Slot 4							
4/4					32		0
VLAN 192	STP	15	20	2	32768		
Slot 4							
4/1					32		19

Options ○ Deploy now ○ Save only ● Schedule

Save Configuration ● Running ○ Startup ○ Running and startup

Name: My STP

Schedule ☑ Use One Time - Tuesday August 8, 2010 23:59:00

Snapshots ☑ Use Pre- and Post- Snapshots Configured IOS products only

FIGURE 321 STP/RSTP Configuration dialog box - Deployment Properties pane

6. Select a deployment option:
   - Click the **Deploy now** option if you want to deploy the VLAN definition.
   - Click the **Save only** option if you want to save the VLAN definition without scheduling its deployment.
   - Click the **Schedule** option if you want to schedule the deployment of the VLAN definition.
7. Select a **Save Configuration** option:
   - Click the **Running** option to save the configuration while the system is running.
   - Click the **Startup** option to save the configuration when the system starts up.
   - Click the **Running and startup** option to save the configuration both while the system is running and when the system starts up.
8. Click the **Schedules** check box, which is available if you selected **Schedule** as a deployment option, to select a frequency.
9. Enter a name in the **Name** field that will be used to identify the configured VLAN.
10. Click the **Snapshots** check box if you want the Management application to run and save a report after this configuration is deployed to the device.
11. Click **OK** to deploy the STP configuration on the selected port VLAN.

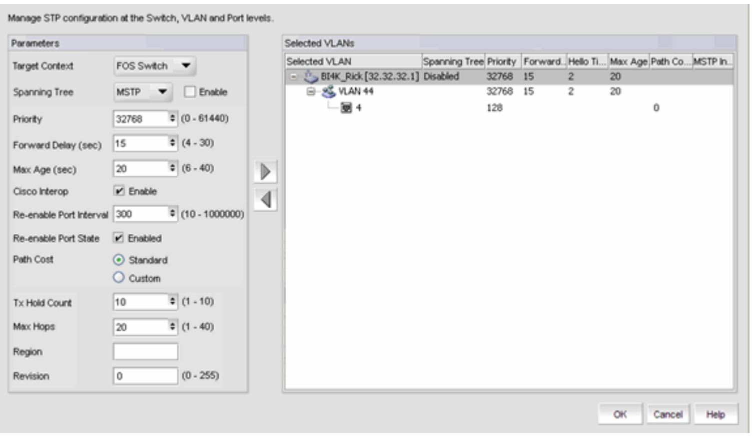
Configuring MSTP on a port VLAN

You can configure MSTP attributes from the **VLAN View** tab or the **Product View** tab.

1. Perform one of the following tasks to select the VLAN on which MSTP will be configured:
   - On the **VLAN View** tab, expand the list of VLANs and select one or multiple VLANs on which MSTP will be configured.
   - On the **Product View** tab, expand the product, product group, or IP subnet folder that contains the products on which the VLAN you want is configured. Then expand the entry to display its VLAN and select the VLAN where MSTP will be configured. You can select more than one VLAN from this tab

   Either of these methods enables the **STP** button on the **VLAN Manager** dialog box.
2. Click the **STP** button on the **VLAN Manager** dialog box to display the **STP Configuration** dialog box.
3. Select **MSTP** from the Spanning Tree list.

   The products on which the VLAN is configured appear on the dialog box, shown in Figure 322.



Manage STP configuration at the Switch, VLAN and Port levels.

Parameters

Target Context: FOS Switch

Spanning Tree: MSTP □ Enable

Priority: 32768 (0 - 61440)

Forward Delay (sec): 15 (4 - 30)

Max Age (sec): 20 (6 - 40)

Cisco Interop: ☑ Enable

Re-enable Port Interval: 300 (10 - 1000000)

Re-enable Port State: ☑ Enabled

Path Cost: ● Standard ○ Custom

Tx Hold Count: 10 (1 - 10)

Max Hops: 20 (1 - 40)

Region:

Revision: 0 (0 - 255)

Selected VLANs

Selected VLAN	Spanning Tree	Priority	Forward...	Hello Ti...	Max Age	Path Co...	MSTP In...
BI4K_Rick [32.32.32.1]	Disabled	32768	15	2	20		
VLAN 44		32768	15	2	20		
4		128				0	

FIGURE 322 **MSTP Configuration dialog box**

4. Select the target switch, VLAN, or port from the **Target Context** list.
5. Specify the following information:
   - Select the **Enable** check box if you want to enable the protocol you selected.
   - Enter a value in the **Priority** field to identify the root bridge in a spanning tree (instance of STP). The bridge with the lowest value has the highest priority and is the root. A higher numerical value means a lower priority; thus, the highest priority is 0. The values range from 0 through 61440. The default is 32768.
   - Enter the number of seconds a bridge waits (the listen and learn period) before it begins to forward data packets in the **Forward Delay** field. The values range from 4 through 30 seconds. The default is 15 seconds.
   - Enter the number of seconds a bridge waits for a hello packet from the root bridge before initiating a topology change in the **Maximum Age** field. The values range from 6 through 40 seconds. The default is 20 seconds.
   - Click the **Cisco Interop Enable** check box to enable Cisco interoperability.

- Enter the interval after which the port will be enabled in the **Re-enable Port Interval** text box. The value range is 10 through 1000000 and the default is 300.
- Click the **Re-enable Port State** check box to enable the time out mechanism for the port.
- Select the **Path Cost** behavior option (Standard or Custom).
- Select the transmit hold count for the bridge from the **Tx Hold Count** list. The value range is 1 through 10.
- Specify the number of hops in a region before the Bridge Protocol Data Units (BPDU) are discarded and the information held for a port is aged in the **Max Hops** text box. The hop count determines when to trigger a reconfiguration. The value range is 1 through 40 and the default is 20.
- Enter the Multiple Spanning Tree (MST) region into the **Region** text box.
- Enter the revision number for the configuration in the **Revision** text box. The value range is 0 through 255 and the default is 0.

6. Click **OK** to launch the Deploy STP dialog box.

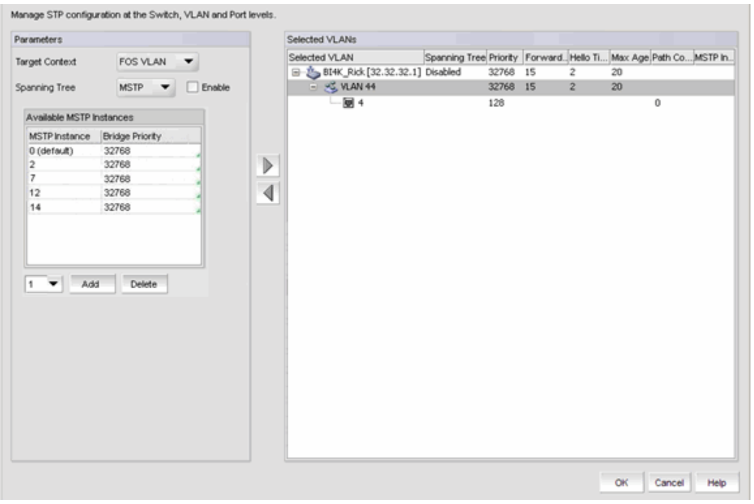
Assigning an MSTP instance to a VLAN

For Brocade 8000 switches, you can configure 1-15 MSTP instances; for the Brocade converged 10 GbE switch module for the IBM BladeCenter, you can configure 1-31 MSTP instances.

1. Click the **STP** button on the **VLAN Manager** dialog box to display the **STP/RSTP Configuration** dialog box, shown in Figure 322.
2. Select a VLAN node under a FOS node in the **Selected VLAN** list, and click the left arrow button.

   The target is automatically set to **FOS VLAN** in the **Target Context** list
3. Select **MSTP** from the Spanning Tree list.

   The **VLAN - STP Configuration** dialog box displays the **Available MSTP Instances** list, as shown in Figure 323.



Manage STP configuration at the Switch, VLAN and Port levels.

Parameters

Target Context: FOS VLAN

Spanning Tree: MSTP □ Enable

Available MSTP Instances

MSTP Instance	Bridge Priority
0 (default)	32768
2	32768
7	32768
12	32768
14	32768

1 Add Delete

Selected VLANs

Selected VLAN	Spanning Tree	Priority	Forward...	Hello Ti...	Max Age	Path Co...	MSTP In...
BI4K_Rick [32.32.32.1]	Disabled	32768	15	2	20		
VLAN 44		32768	15	2	20		
4		128				0	

FIGURE 323 STP Configuration dialog box - Assign MSTP Instance to FOS

4. Select one instance from the **Available MSTP Instances** list and, using the right arrow button, assign it to a VLAN in the **Selected VLAN** list.

Adding an MSTP instance

1. Click the **STP** button on the **VLAN Manager** dialog box to display the **STP/RSTP Configuration** dialog box, shown in Figure 322.
2. Select a VLAN node under a FOS node in the **Selected VLAN** list, and click the left arrow button.

   The target is automatically set to **FOS VLAN** in the **Target Context** list
3. Select **MSTP** from the Spanning Tree list.

   The **VLAN - STP Configuration** dialog box displays the **Available MSTP Instances** list, as shown in Figure 323.
4. Select an MSTP instance from the drop down list under the **Available MSTP Instances** list, or enter the MSTP instance number.
5. Click the **Add** button.

   A new row is added to the **Available MSTP Instances** list. You can change the bridge priority, which is set, by default, to 32768.

Deleting an MSTP instance

1. Select **MSTP** from the Spanning Tree list.

   The **VLAN - STP Configuration** dialog box displays the **Available MSTP Instances** list, as shown in Figure 323.
2. Select an MSTP instance from the **Available MSTP Instances** list, or enter the MSTP instance number.
3. Click the **Delete** button.
4. Click the right arrow button to move the MSTP instance to the **Selected VLAN** list.
5. Click **OK**.

VLAN Routing

VLAN restricts the broadcast domain to only its interface members. If nodes connected to two different VLANs want to communicate, they require an external router to route between the VLANs. Optionally, Brocade DCB products offer the ability to create Switch Virtual Interface (SVI) to route between VLANs.

An SVI is a VLAN of switch ports represented by one interface to a routing or bridging system. There is no physical interface for the VLAN and the SVI provides the Layer 3 processing for packets from all switch ports associated with the VLAN. There is one-to-one mapping between a VLAN and SVI; therefore, only a single SVI can be mapped to a VLAN. The VLAN is mapped to a network address using the SVI. All the nodes in the VLAN will belong to the subnet of the SVI.

NOTE
In IOS terms, an SVI is also called a Virtual Routing Interface (VRI). The SVI in DCB products and VRI in IOS products mean the same.

Managing IP addresses on a switch virtual interface

Switch virtual interfaces (SVIs) can be added to port VLANs when you create or modify VLAN definitions. SVIs can only be created in Layer 3 products.

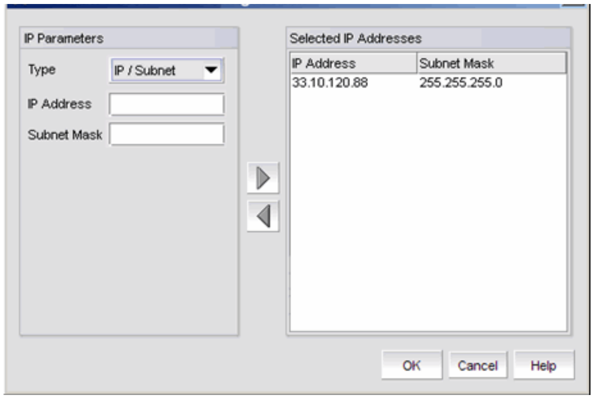
Once VLAN definitions are deployed to products, you can add an IP address to the SVI by completing the following steps.

1. On the **VLAN Manager** dialog box, complete one of the following tasks:
   - Click the **VLAN View** tab and expand the VLAN node. Select the product that contains the switch virtual interface that you want to define. The list of interfaces appears in the interface list. Click the SVI in the list of interfaces to select it.
   - On the **Product View** tab, expand the product or group folders. Expand the products under the folder and select the VLAN that contains a switch virtual interface. The list of interfaces appears in the interface list. Click the SVI in the list of interfaces to select it.

NOTE
For DCB products, you must select the port VLAN itself to enable the IP button.

2. Click the **IP** button on the tool bar.

   The **Virtual Port - IP Configuration** dialog box displays, as shown in Figure 324. If IP addresses have been configured for the switch virtual interface, they are listed in the **Selected IP Addresses** list in the dialog box.



Type: IP / Subnet

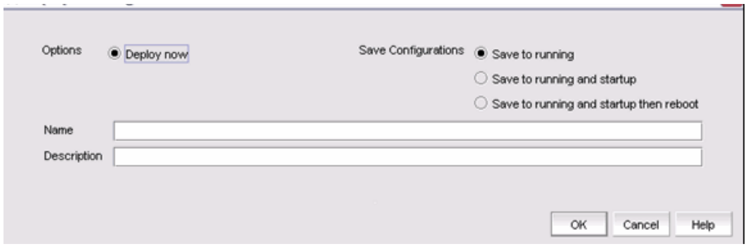
IP Address	Subnet Mask
33.10.120.88	255.255.255.0

FIGURE 324 Virtual Port - IP Configuration dialog box

3. Complete one of the following steps:
   - To add a new IP address to the switch virtual interface, enter the IP address in the **IP Address** field and click the right arrow button to move it to the **Selected IP Addresses** list.
   - To modify an IP address of a switch virtual interface, select the IP address from the list and click the left arrow button to move the IP address back to the **IP Parameters** list. Since this list is for a single IP address, multiple IP addresses cannot be edited.
   - To delete an IP address, select the IP address from the list and click the left arrow button.

4. Enter the following information:
   - **Primary** or **Secondary** options (DCB products only)—Indicates whether the IP address is the primary or secondary IP address of the VLAN.
   - Type—Select the type of IP address you want to assign to the VLAN. Choose CIDR or IP/Subnet.
   - Enter the IP address in the fields provided:
     - If you chose the CIDR Subnet format, enter a subnet address in the subnet_address/subnet_mask_bits format (for example, 192.168.2.10/24).
     - If you chose the Subnet format, enter a subnet address in the subnet_address/subnet_mask format (for example, 192.168.2.10/255.255.255.0).
5. Click the right arrow button to add the IP address to the list. If additional IP addresses are needed, continue adding them to the switch virtual interface. You can assign a maximum of 255 IP addresses on DCB products and a maximum of 24 IP addresses on IOS products
6. Click **OK** to begin the deployment of the address to the product.

The **Deploy IP Configuration** dialog box displays.



Options ● Deploy now

Save Configurations ● Save to running
○ Save to running and startup
○ Save to running and startup then reboot

Name

Description

FIGURE 325 Deploy IP Configuration dialog box

7. Select a **Save Configurations** option:
   - Click the **Save to running** option to save the configuration while the system is running.
   - Click the **Save to running and startup** option to save the save the configuration both while the system is running and when the system starts up.
   - Click the **Save to running and startup then reboot** option to save the configuration both while the system is running and when the system starts up, and then the system automatically reboots.
8. Enter a name in the **Name** field that will be used to identify the configured VLAN.
9. Enter a description in the **Description** field that will be used to identify the configured VLAN.
10. Click **OK** to deploy the IP address.

Chapter

Deployment Manager 25

In this chapter

Introduction to the Deployment Manager

The Deployment Manager allows you to view, edit, duplicate, deploy, and generate reports for the following types of deployment configurations:

- DCB
- VLAN
- STP
- Security configurations

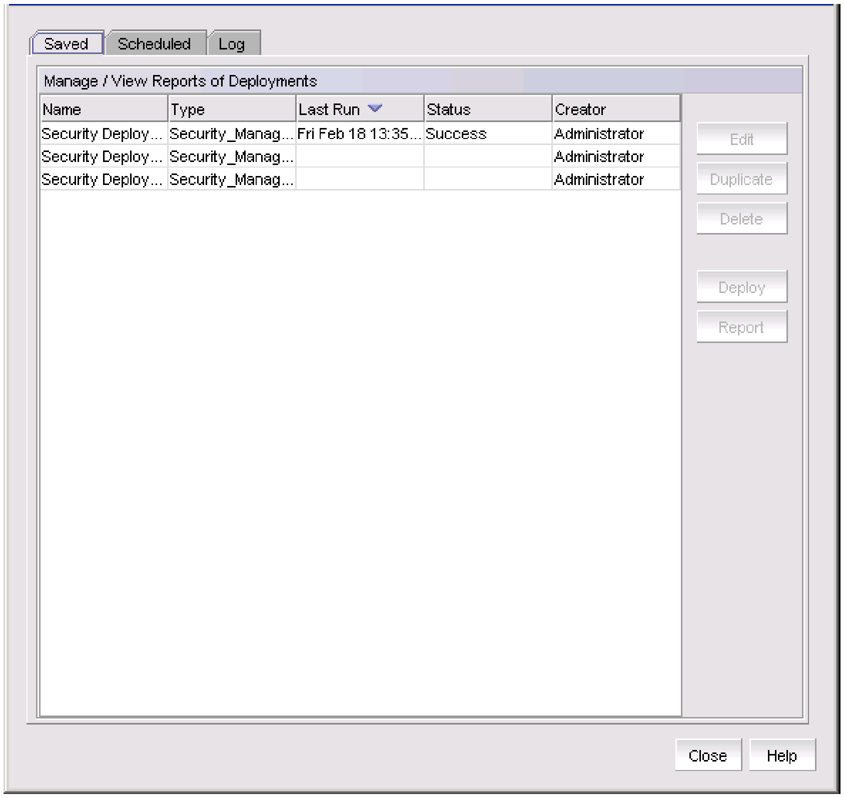
The deployment configurations must have been previously created and saved. You cannot create configurations using the Deployment Manager. Refer to the following sections for information about creating these types of configurations:

- “Fibre Channel over Ethernet” on page 339
- “VLAN Management” on page 703
- “Security Management” on page 393

Editing a deployment configuration

1. Select **Configure > Deployment.**

   The Deployment dialog box displays, as shown in Figure 326.



Manage / View Reports of Deployments

Name	Type	Last Run	Status	Creator
Security Deploy...	Security_Manag...	Fri Feb 18 13:35...	Success	Administrator
Security Deploy...	Security_Manag...			Administrator
Security Deploy...	Security_Manag...			Administrator

FIGURE 326 Deployment dialog box

2. Select a deployment configuration in the **Saved** or **Scheduled** tab.
3. Click **Edit.**

   A dialog box specific to the type of deployment displays. This is the same dialog box that was used when the deployment was created.
4. Update the dialog box with the information you want to change.

Duplicating a deployment configuration

1. Select **Configure > Deployment**.

   The Deployment dialog box displays.

2. Select a deployment configuration in the **Saved** or **Scheduled** tab.

   NOTE
   VLAN configurations cannot be duplicated.

3. Click **Duplicate**.

   A dialog box specific to the type of deployment displays. This is the same dialog box that was used when the original deployment was created.

4. Update the dialog box with any information you want to change.

   A copy of the deployment configuration is created with the name "*originalName* **copy***n*". For example, if the original name is "test", the new name is "test copy1". If you duplicate "test" again, the name of the second duplicate is "test copy2".

Deleting a deployment configuration

1. Select **Configure > Deployment**.

   The Deployment dialog box displays.

2. Select a deployment configuration in the **Saved** or **Scheduled** tab.
3. Click **Delete**.
4. Click **Yes** in the confirmation dialog.

   The deployment configuration is deleted and removed from the deployment dialog box.

   If the deployment configurations is already in progress, it is not deleted.

Deploying a configuration

1. Select **Configure > Deployment**.

   The Deployment dialog box displays.

2. Select a deployment configuration in the **Saved** or **Scheduled** tab.
3. Click **Deploy**.

   The Deployment Status dialog box displays.

4. Click **Start**.

   The selected configuration is deployed.

   You cannot deploy configurations that are already in progress.

Viewing deployment logs

1. Select **Configure > Deployment**.

   The Deployment dialog box displays.

2. Click the **Log** tab.

   A list of deployment configurations that are executed and the status of each displays.

Generating a deployment report

1. Select **Configure > Deployment.**

   The Deployment dialog box displays.

2. Select a deployment in the **Saved**, **Scheduled**, or **Log** tab.
3. Click **Report.**

   An HTML report displays. You can click the Configuration Name or Deployment Time to see additional details.

Generating a deployment configuration snapshot report

1. Select **Configure > Deployment.**

   The Deployment dialog box displays.

2. Select a deployment in the **Saved** or **Scheduled** tab.
3. Click **Deploy.**

   The Deployment Status dialog box displays.

4. Click **Snapshot Report.**

   The **Configuration Snapshot Report** dialog box displays.

5. (*Optional*) If the configuration snapshot list is too long, you can filter the list.
   a. Select the start date and end date of the configuration snapshots you wish to view.
   b. Click **Find.**

      The Management application displays the list of snapshots that match the start date and end date you specified.

6. Select a product from the **Device Configuration** column to display the configuration snapshots that are available for that product.
7. Click **View** to display information for that deployment.

   The **View Pre/Post Configuration Snapshot** dialog box displays details of the selected configuration.

Chapter

Troubleshooting 26

In this chapter

FC troubleshooting

NOTE
FC troubleshooting is only available for Fabric OS and M-EOS devices.

You can perform the following operations using FC troubleshooting:

- Trace Route (Path Information and FC Ping) – Use to obtain the detailed routing information for any two selected device ports. The devices can exist in the same fabric or in two different fabrics shared through FC Routers.
- Device Connectivity Troubleshooting – Use to identify any problems that might be preventing communication between the two selected device ports. The device ports can be selected from the same fabric or from two different fabrics.
- Fabric Device Sharing Diagnosis (pure Fabric OS fabrics only) – Use to confirm that any two or more selected fabrics are capable of sharing devices between them.
- Diagnostic Port Testing (Fabric OS 16 Gbps-capable ports only) – Use to run the following diagnostic port test on the 16 Gbps-capable ports: electrical, optical, measure link distance, and link traffic.

Tracing FC routes

The Management application enables you to select a source port and a destination port and displays the detailed routing information from the source port or area on the local switch to the destination port or area on another switch.

NOTE
Trace route cannot be performed on offline devices.

NOTE
Trace route cannot be performed in a mixed (Fabric OS and M-EOS) fabric.

Fabric OS trace route requirements

- Fabric OS trace route is only supported in a pure-Fabric OS fabric.
- All Fabric OS switches in the fabric must be running Fabric OS 5.2 or later.

M-EOS trace route requirements

NOTE
M-EOS trace route fails if any device loses manageability during the operation.

- M-EOS trace route is only supported in a pure-M-EOS fabric.
- All M-EOS switches in the fabric must be running M-EOS 9.8 or later.
- All M-EOS switches must be managable in the M-EOS fabric.
- M-EOS trace route is not supported in a Meta SAN across Backbone fabrics. However, M-EOS trace route is supported within an edge fabric in a Meta SAN.
- M-EOS trace route only supports device-to-device trace route.

To trace routes, complete the following steps.

1. Select **Configure > FC Troubleshooting > FC Trace Route.**

   The **Trace Route** dialog box displays.

2. Choose from one of the following options:

   - Select a fabric from the **Fabric** list.
   - Select a router from the **Routing** list. Requires Fabric OS 6.2 or later.

3. Select the source and destination ports by choosing one of the following:

   The source and destination ports must be on the same fabric; however, they cannot be connected to the same switch.

   - To enter the ports, select the **Enter port FC Address** option.
     a. Enter the source port FC address in the **Source** field.
     b. Enter the destination port FC address in the **Destination** field.
   - To select the ports, select the **Select two device ports** option.
     a. Right-click a fabric in the **Available Device Ports** table and select **Expand All.**
     b. Select the ports (two) for which you want to display the detailed routing information from the **Available Device Ports** table.

4. Click the right arrow button.
5. Click **OK**.

   The **Trace Route Summary** dialog box displays. This dialog box includes the following information:

   - **Trace Route Summary.** This table shows a brief summary of the trace including the following:
     - Port WWN
     - Port name
     - FC address
     - Switch name
     - (Fabric OS only) Whether ping was successful (Fabric OS only)
     - (Fabric OS only) Round trip time (minimum, maximum, and average)
     - (Fabric OS only) Whether the device ports are in active zones.
   - **Forward Route.** This tab shows the path taken by data packets from the port belonging to the switch on which the trace route has been invoked (source port) to the port on the other switch (destination port).
   - (Fabric OS only) **Reverse Route.** This tab shows the path from the destination port to the source port.

     NOTE
     This reverse route may sometimes be different from the forward route.

   - (Fabric OS only) **FC Ping.** This tab shows the minimum, maximum and average round trip times between the selected device port WWNs and the domain controller. It details whether the selected device port WWNs are zoned or not. It also shows the number of frames sent to the device port, frames rejected, frames timed-out and frames received by the device port.
6. Click **Close** on the **Trace Route Summary** dialog box.
7. Click **Cancel** on the **Trace Route** dialog box.

Troubleshooting device connectivity

To troubleshoot device connectivity, complete the following steps.

1. Select **Configure > FC Troubleshooting > Device Connectivity.**

   The **Device Connectivity Troubleshooting** dialog box displays.
2. Select the source and destination ports on which you want to troubleshoot device connectivity using one of the following options:

   - Enter the source and destination ports directly by selecting the **Enter port FC Address** option and completing the following steps.

     a. Enter the source port in the **Source** field.

     b. Enter the destination port in the **Destination** field.

     c. Click **Search and Add.**

- Select the source and destination ports from a list by selecting the **Select two device ports** option and completing the following steps.
   a. Right-click a fabric in the **Available Device Ports** table and select **Expand All**.
   b. Select the ports (source and destination) for which you want to confirm device sharing from the **Available Device Ports** table.
   To add a detached device to troubleshoot device connectivity, refer to "Adding a detached device" on page 730.
   c. Click the right arrow button.

3. Click **OK**.

   The following diagnostic tests are performed:

   - Device Status
   - Switch port health status
   - Zone configuration in the fabric
   - LSAN zone configuration in edge fabrics
   - Edge fabric - FC router physical connection status.
   - Active ACL DCC policy check (Fabric OS only)

   The **Device Connectivity Troubleshooting Results** dialog box displays.

   If no problems are found, the diagnostic test is marked with a check mark. If problems are found, an alert icon appears next to the test, with a brief statement detailing the error as well as a suggested resolution.

4. Click **Re-run Diagnosis** to run the device connectivity on the same ports.
5. Click **Trace Route** to trace the route between the two selected ports.
6. Click **Close** on the **Device Connectivity Troubleshooting Results** dialog box.

Adding a detached device

To add a detached device to the **Selected Device Ports** table, complete the following steps.

1. Select **Configure > FC Troubleshooting > Device Connectivity**.

   The **Device Connectivity Troubleshooting** dialog box displays.

2. Click **Add Detached**.
3. Enter the port WWN of the detached device port in the **Port WWN** field.
4. Click **OK**.

Confirming Fabric Device Sharing

NOTE
Fabric device sharing is only available with Trial or Licensed version.

NOTE
Fabric device sharing is only available on pure Fabric OS fabrics.

To confirm fabric device sharing, complete the following steps.

1. Select **Configure > FC Troubleshooting > Fabric Device Sharing**.

   The **Fabric Device Sharing Diagnosis** dialog box displays.

2. Select the fabrics (two or more) for which you want to confirm device sharing from the **Available Fabrics** table.
3. Click the right arrow button.
4. Click **OK**.

   The following checks are performed on the selected fabrics:

   - Are the selected fabrics configured with an FC Router?
   - Are the selected fabrics connected to the same backbone fabric?
   - Is sharing of devices between backbone and edge fabric supported?

   The **Fabric Device Sharing Diagnosis Results** dialog box displays with the details of the fabrics selected for diagnosis, the details of the tests performed, the results of the test, as well as short description of the test results.

5. Click **Close** on the **Fabric Device Sharing Diagnosis Results** dialog box.
6. Click **Cancel** on the **Fabric Device Sharing Diagnosis** dialog box.

Troubleshooting port diagnostics

This dialog box allows you to run a diagnostic port test on the selected ports.

NOTE
You can only run this test on devices with 16 Gbps capable E ports running Fabric OS 7.0 or later.

NOTE
Both the source and destination ports must be managed by the Management application.

To run a diagnostic port test, complete the following steps.

1. Select **Configure > FC Troubleshooting > Diagnostic Port Test**.

   The **Diagnostic Port Test** dialog box displays.

2. Select the ports for which you want to run a diagnostic port test from the **Available Ports** table.

   You can only run 10 diagnostic port tests at a time. If you select more than 10 ports, the Management application runs the first 10 diagnostic port tests and queues the rest. When the first test is completed, the next test in the queue begins and so on until all tests are completed.

3. Click the right arrow button.

4. Click **Start**.

   The Management application performs the following operations to enable diagnostic mode on the selected ports:

   1. Disable the source port.
   2. Disable the destination port.
   3. Enable the diagnostic mode on source E port.
   4. Enable the diagnostic mode on destination E port.
   5. Enable the source port.
   6. Enable the destination port.

   The following tests are performed on the selected ports:

   - Electrical
   - Optical
   - Measure link distance
   - Link traffic

   If any of the tests fail, the Management application does not rollback to already executed operations.

   When the test successfully completes, the Management application performs the following operations to change the port type back to E port:

   1. Disable the source port.
   2. Disable the destination port.
   3. Disable the diagnostic mode on source D port.
   4. Disable the diagnostic mode on destination D port.
   5. Enable the source port.
   6. Enable the destination port.

   The **Progress** column shows whether the test is not started, in progress, or completed.

   The **Status** column shows the overall status (Success or Failed) of the test.

5. Select a port row in the Selected Ports table to display the detailed status in the **Status Details of the Selected Row** table.

   The **Status Details of the Selected Row** table displays with the details of the port selected for diagnosis, the details of the tests performed, the results of the test, as well as short description of the test results. The following table details the messages that display depending on the success or failure of the operations and tests.

TABLE 44 Status Detail messages

Operation/Test	Possible message
Disable the source or destination port	Disabled the port *slot_number/port_number* of the switch *switch_IP_address*.
	Failed to disable the port *slot_number/port_number* of the switch *switch_IP_address*. Reason: *CAL_error_message*

TABLE 44 Status Detail messages

Operation/Test	Possible message
Enable the diagnostic mode on source or destination E ports	Enabled diagnostic mode on port *slot_number/port_number* of the switch *switch_IP_address.*
	Failed to enable diagnostic mode on port *slot_number/port_number* of the switch *switch_IP_address*. Reason: *CAL_error_message*
Enable the source or destination port	Enabled the port *slot_number/port_number* of the switch *switch_IP_address*.
	Failed to enable the port *slot_number/port_number* of the switch *switch_IP_address*. Reason: *CAL_error_message*
Disable the diagnostic mode on source or destination D ports	Disabled diagnostic mode on port *slot_number/port_number* of the switch *switch_IP_address*.
	Failed to disable diagnostic mode on port *slot_number/port_number* of the switch *switch_IP_address*. Reason: *CAL_error_message*
Lost connectivity to switch while test is in progress	Connection failed to the switch during the operation.
Diagnostic port test timed out The Management application waits 30 minutes to complete the test. If not completed, the test times out.	Diagnostic port test time-out. You may need to change the port configuration before retrying.
Electrical Loopback Test	Successfully completed Electrical Loopback Test on port *slot_number/port_number* of the switch *switch_IP_address*.
	Electrical Loopback Test failed on port *slot_number/port_number* of the switch *switch_IP_address.*
	Electrical Loopback Test skipped on port *slot_number/port_number* of the switch *switch_IP_address*. Reason: *CAL_error_message*
Optical Loopback Test	Successfully completed Optical Loopback Test.
	Optical Loopback Test failed
	Optical Loopback Test skipped. Reason: *CAL_error_message*
Link Traffic Test	Successfully completed Link Traffic Test.
	Link Traffic Test failed.
Distance between ports	Approximate distance between the ports is *numerical_value* meters.

6. Click **Close** on the **Diagnostic Port Test** dialog box.

FCIP troubleshooting

NOTE
FCIP troubleshooting is only available for Fabric OS devices.

You can perform the following operations using FCIP troubleshooting:

- **Ping.** Use to confirm that the configured FCIP tunnels are working correctly.
- **Trace Route.** Use to view the route information from a source port on the local device to a destination port on another device and determine where connectivity is broken.
- **Performance.** Select to view FCIP tunnel performance between two devices.

Configuring IP ping

NOTE
IP Ping only supported on Fabric OS devices running Fabric OS 5.2 or later.

NOTE
IP Perf is not supported on the Fabric OS 8 Gbps Extension Switch or Blade.

You can also verify IP connectivity when configuring an FCIP circuit. For more information, refer to "Adding an FCIP circuit".

To configure IP ping, complete the following steps.

1. Select **Configure > FCIP Troubleshooting > Ping.**

   The **IP Ping** dialog box displays.
2. Select a switch from the **Available Switches** table.
3. Select a port from the **GigE Port** list.
4. Select an IP address switch from the **IP Interface** list.
5. Enter the remote IP address in the **Remote IP Address** field.
6. Click **OK.**

   Ping sends four Internet Control Message Protocol (ICMP) Ping packets to the destination address and records the time until a response.

   The **IP Ping Result** dialog box displays with two tables.

   The top table (**FCIP IP Ping Response Details**) contains the following statistics:

TABLE 45 FCIP IP Ping Response Details

Field or Component	Description
Status	Always displays 'Completed'. If there is a failure, an error message displays instead of the **IP Ping Result** dialog box.
Packets Sent	Always displays '4. This is not configurable.
Packets Received	The number of received responses.
Packets Lost	Equal to the number of packets sent minus the number of packets received.

TABLE 45 FCIP IP Ping Response Details

Field or Component	Description
Packet Lost percentage	The number of packets lost expressed as a percentage of the packets sent. This will be 0%, 25%, 50%, 75% or 100% for 0, 1, 2, 3, or all 4 packets lost.
Minimum Round Trip Time	The shortest time, in milliseconds, of any response. If no response, the round trip times is 0.
Maximum Round Trip Time	The longest time, in milliseconds, of any response. If no response, the round trip times is 0.
Average Round Trip Time	The average time, in milliseconds, of all responses. If no response, the round trip times is 0.

The bottom table (**IP Ping Details**) provides details for each ping attempt.

TABLE 46 IP Ping Details

Field or Component	Description
Reply From	The IP address of the device that sent the reply. For a normal response, this is the destination IP address. Some error responses (such as "destination unreachable") may come from an intermediate router.
Status	Displays either Success or an error message (such as request timed out or destination unreachable) from the switch.
Number of bytes	The number of bytes in the data portion of the response. Should be 64, matching the 64 bytes of data sent in the transmitted packet.
Round Trip Time (ms)	The time in milliseconds between sending the packet and receiving the response. This provides a rough indication of network congestion or latency. It is normal for the first packet to experience a higher round trip time than later packets, if the intermediate routers need to do ARP requests to locate the next hop.
Time To Live (hops)	The number of hops remaining in the received response. The time to live is decremented by each router that forwards the packet. The packet is dropped if the time to live reaches zero.

7. Click **Close** on the **IP Ping Result** dialog box.
8. Click **Cancel** on the **IP Ping** dialog box.

Tracing IP routes

The Management application enables you to select an source and a target and displays the detailed routing information from the source port or area on the local switch to the destination port or area on another switch.

Trace route cannot be performed on the offline devices or virtual devices.

NOTE
Trace route is only supported on Fabric OS devices running Fabric OS 5.2 or later.

To trace routes, complete the following steps.

1. Select Configure > FCIP Troubleshooting > Trace Route.

   The IP Traceroute dialog box displays.

2. Select a switch from the Available Switches table.
3. Select a port from the GigE Port list.
4. Select an IP address switch from the IP Interface list.
5. Enter the remote IP address in the Remote IP Address field.
6. Click OK.

   The IP Traceroute Result dialog box displays.

   Traceroute sends three ICMP Ping packets to the destination address with a time to live (TTL) of one hop, and expects a ‘TTL Expired’ error back from the first router to obtain the IP address of the first hop. Traceroute then repeats the operation with a TTL of two hops to get the IP address of the second hop. This process repeats for up to ten hops, or until a successful PING response is received.

   The IP Trace Details table displays the results of each attempt.

TABLE 47 IP Trace Details

Field or Component	Description
Hop Number	The TTL inserted in the transmitted probe packet.
IP Address 1	The IP address of the system that responded to the first of the three probes, or 0.0.0.0 if there was no response.
IP Address 2	The IP address of the system that responded to the second of the three probes, or 0.0.0.0 if there was no response.
IP Address 3	The IP address of the system that responded to the third of the three probes, or 0.0.0.0 if there was no response.
RTT 1	The time in milliseconds for the first of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path.
RTT 2	the time in milliseconds for the second of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path.
RTT 3	the time in milliseconds for the third of the three responses to be received, or blank if there was no response. This value helps identify a congested or slow link in the path.

7. Click **Close** on the **IP Traceroute Result** dialog box.
8. Click **Cancel** on the **IP Traceroute** dialog box.

Viewing FCIP tunnel performance

NOTE
IP Performance is only supported on the 4 Gbps Router, Extension Switch and Encryption Blade running Fabric OS 5.2 or later.

NOTE
If you run IP Performance over a link also being used for production traffic, it will impact the production traffic performance.

To view FCIP tunnel performance, complete the following steps.

1. Select **Configure > FCIP Troubleshooting > Performance**.

   The **IP Performance** dialog box displays.
2. Select a switch from the **Available Switches** table.
3. Select a port from the **GigE Port** list.
4. Select an IP address switch from the **IP Interface** list.
5. Enter the remote IP address in the **Remote IP Address** field.
6. Click **OK**.

   The **IP Performance Result** dialog box displays.

   IP Performance sends dummy data as fast as possible to the remote IP address and measures how much data can be sent over a given interval. IP Performance attempts to saturate the network link to see how much bandwidth is available. It will display the media link bandwidth only if no other traffic is flowing. The remote IP address must belong to a managed switch so that IP Performance can set up the receiving end on the remote switch.

   For more information about IP Performance, refer to Chapter 20 in the *Fabric OS Administrator's Guide*.

   During the IP Performance test, data is sent continuously and statistics are sampled every 30 seconds. At the end of the period, the IP Performance results dialog box displays. The IP Performance results dialog contains a table with one row for each 30-second sample of the test. Columns in the perf results dialog are:

Field/Component	Description
Available Bandwidth	The average bytes per second sent during the sample interval. This is a count of FC payload bytes; for example, the throughput seen by an FC application. It is slightly lower than the actual bytes-per-second on the wire since it does not include headers and acknowledgements.
Weighted Bandwidth	The weighted bandwidth represents what the FCIP tunnel / FC application sees for throughput rather than the Ethernet on-the-wire bytes.
Loss Percent	An estimate of the percentage of data packets lost during the sampling interval, based on TCP re-transmits.

Field/Component	Description
DELAY	The average round trip time to send a packet of data and receive the acknowledgement.
PMTU (Path Maximum Transmission Unit)	The largest packet size that can be transmitted over the end-to- end path without fragmentation. This value is measured in bytes and includes the IP header and payload. IP Performance tries the configured Fabric OS Jumbo MTU value (anything over 15000, then 1500, then 1260. The value displayed in the table is the largest value that worked.

7. Click **Close** on the **IP Performance Result** dialog box.
8. Click **Cancel** on the **IP Performance** dialog box.

Application Configuration Wizard troubleshooting

The following section states a possible issue and the recommended solution for Management application Configuration Wizard errors.

Problem	Resolution
Unable to launch the Management application Configuration Wizard on a Windows Vista, Windows 7,or Windows 2008 R2 system	The Windows Vista, Windows 7,or Windows 2008 R2 system enables the User Access Control (UAC) option by default. When the UAC option is enabled, the Configuration Wizard cannot launch. If the Configuration Wizard does not launch, use one of the following options to disable the UAC option: The following are the various ways we can disable UAC in vista: **Disable using msconfig by completing the following steps.** 1 Select **Start > Run**. 2 Type msconfig on the **Run** dialog box and click **OK**. 3 Click the **Tools** tab on the **System Configuration Utility.** 4 Scroll down to and select the **Disable UAC** tool name. 5 Click **Launch.** A command window displays and runs the disable UAC command. When the command is complete, close the window. 6 Close the **System Configuration Utility.** 7 Restart the computer to apply changes. NOTE: You can re-enable UAC using the above procedure and selecting the **Enable UAC** tool name in step 4. **Disable using regedit by completing the following steps.** NOTE: Before making changes to the registry, make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes. 1 Select **Start > Run**. 2 Type regedit on the **Run** dialog box and click **OK.** 3 Navigate to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System 4 Right-click the **EnableLUA** value and select Modify. 5 Change the **Value data** field to 0 on the **Edit DWORD Value** dialog box and click **OK.** 6 Close the **Registry Editor.** 7 Restart the computer to apply changes. NOTE: You can re-enable UAC using the above procedure and changing the **Value data** field to 1 in step 5.

Browser troubleshooting

The following section states a possible issue and the recommended solution for browser errors.

Problem	Resolution
The **Cancel** button does not work on the **Report via E-mail** dialog box when you use the Mozilla Firefox browser.	Mozilla Firefox Browser does not support window close script. Click the browser Close button to cancel. **NOTE:** The **Cancel** button still displays on all **Report via E-mail** dialog boxes.

Client browser troubleshooting

The following section states a possible issue and the recommended solution for client browser errors.

Problem	Resolution
Downloading Client from a Internet Explorer Browser over HTTPS	If the JNLP file does not launch automatically, use one of the following options: • Complete the following steps. 1 Save the JNLP file to the local host. 2 Launch the JNLP file manually. • In Internet Explorer 7, complete the following steps. 1 Select **Tools > Internet Options**. 2 Click the **Advanced** tab. 3 Clear the **Do not save encrypted pages to disk** check box. If the browser warns you about the security certificate, use the fully qualified hostname to launch the web page.

Fabric tracking troubleshooting

The following section states a possible issue and the recommended solution for fabric tracking errors.

Problem	Resolution
If a switch is replaced by another switch having the same IP address but a different node WWN while fabric tracking is on, the Management application does not update the Product List, Connectivity Map or switch properties with the new node WWN.	Choose from one of the following options: • Turn fabric tracking off while the switch is replaced. This causes the old switch to be removed and the new switch added. • After the switch is replaced, remove and re-add the fabric in the **Discover Setup** dialog box.

FICON troubleshooting

The following section states a possible issue and the possible cause for FICON errors.

Problem	Causes
FICON not supported on switch error.	FICON Unsupported Configurations: • FICON is not supported on base switches. • FICON is not supported on a logical switch which has an XISL configured. • FICON is not supported if the PID format is 2. • FICON is not supported if 10 bit address is enabled on 384-port Backbone Chassis for non-default switch. • FICON is not supported if any port address is greater than the maximum port number of the switch. • 48-port blades are not allowed in the Director Chassis for FICON. • FICON is not supported on 48-port blades in the 384-port Backbone Chassis when Virtual Fabrics is disabled. However, when Virtual Fabrics is enabled in the Backbone Chassis, FICON is supported on the 48-port blade as long as the 48-port blade is part of a logical switch. If the 48-port blade is part of the default switch on the Backbone Chassis, FICON is not supported. • FICON is not supported on Admin Domain-enabled fabrics. • FICON is not supported on 64-port blades.

Firmware download troubleshooting

The following section states a possible issue and the recommended solution for firmware download errors.

Problem	Resolution
If you configured an internal FTP server and the Management application server is running IPv6, firmware download is not supported.	Choose from one of the following options: • If the Management application is running IPv6 only, configure an external FTP server. • If the Management application is running IPv4 and IPv6, configure IPv4 to be the preferred address.

Launch Client troubleshooting

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

Problem	Resolution
Remote client does not upgrade from versions prior to 11.0.	The remote client does not automatically upgrade when you select the remote client shortcut of client versions earlier than 11.0. To clear the old client and launch the new remote client version, complete the following steps. 1 Clear the previous version from the Java cache,. a Select **Start > Settings > Control Panel > Java**. The **Java Control Panel** dialog box displays. b Click **View** on the **General** tab. The **Java Cache Viewer** dialog box displays. c Right-click the application and select **Delete.** d Click **Close** on the **Java Cache Viewer** dialog box. e Click **OK** on the **Java Control Panel** dialog box. 2 Launch the remote client. a Open a web browser and enter the IP address of the Management application server in the **Address** bar. If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address:Port_Number*. The Management application web start screen displays. b Click the Management application web start link. The **Log In** dialog box displays. c Enter your user name and password. The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change. d Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in. e Click **Login**. f Click **OK** on the **Login Banner** dialog box. The Management application displays.

Problem	Resolution
Unable to log into the Client (the application does not launch when you use a valid user name and password and exceptions are thrown in the client side).	Use one the following procedures to configure the IP address in the host file. **Windows operating systems** 1 Log in using the 'Administrator' privilege. 2 Select **Start > Run**. 3 Type drivers in the **Open** field and press **Enter**. 4 Go to the ‘etc’ folder and open the ‘hosts’ file using a text editor. 5 Add the IP address and host name of the client in the following format: *IP_Address Host_Name*. For example, 127.0.0.1 localhost 6 Save and exit the file. **Unix operating systems** 1 Log in using the 'root' privilege. 2 Open the ‘/etc/hosts’ file using a text editor. 3 Add the IP address and host name of the client in the following format: *IP_Address Host_Name*. For example, 127.0.0.1 localhost 4 Save and exit the file.
Unable to launch the remote client (the SSL setting, web server port number, or server starting point number changed during the server upgrade).	To remove the old link and launch the correct remote client version, complete the following steps. 1 Clear the previous version from the Java cache,. a Select **Start > Settings > Control Panel > Java**. The **Java Control Panel** dialog box displays. b Click **View** on the **General** tab. The **Java Cache Viewer** dialog box displays. c Right-click the application and select **Delete**. d Click **Close** on the **Java Cache Viewer** dialog box. e Click **OK** on the **Java Control Panel** dialog box. 2 Log into the remote client from the browser. a Open a web browser and enter the IP address of the Management application server in the **Address** bar. If the web server port number does not use the default (443 if is SSL Enabled; otherwise, the default is 80), you must enter the web server port number in addition to the IP address. For example, *IP_Address*:*Web_Server_Port_Number*. The Management application web start screen displays. b Click the Management application web start link. The **Log In** dialog box displays. c Enter your user name and password. The defaults are Administrator and password, respectively. If you migrated from a previous release, your username and password do not change. d Select or clear the **Save password** check box to choose whether you want the application to remember your password the next time you log in. e Click **Login**. f Click **OK** on the **Login Banner** dialog box. The Management application displays.

Names troubleshooting

The following section states a possible issue and the recommended solution for names errors.

Problem	Resolution
Duplicate name error.	If you configured the Management application to only allow unique names and you try to use a name that already exists in the fabric. You can enter a different name for the device or search for the duplicate name using one of the following procedures: • "Searching for a device by name" on page 109 in the **Configure Names** dialog box • "Searching for a device by WWN" on page 110 in the **Configure Names** dialog box • "Searching for a device" on page 197

Patch troubleshooting

The following section states a possible issue and the recommended solution for patch errors.

Problem	Resolution
Unable to launch the SMC on a Windows Vista,Windows 7,or Windows 2008 R2 system	The Windows Vista,Windows 7,or Windows 2008 R2 system enables the User Access Control (UAC) option by default. When the UAC option is enabled, the SMC cannot launch. If the SMC does not launch, use one of the following options to disable the UAC option: The following are the various ways we can disable UAC in vista: **Disable using msconfig by completing the following steps.** 1 Select **Start** > **Run**. 2 Type msconfig on the **Run** dialog box and click **OK**. 3 Click the **Tools** tab on the **System Configuration Utility**. 4 Scroll down to and select the **Disable UAC** tool name. 5 Click **Launch**. A command window displays and runs the disable UAC command. When the command is complete, close the window. 6 Close the **System Configuration Utility**. 7 Restart the computer to apply changes. NOTE: You can re-enable UAC using the above procedure and selecting the **Enable UAC** tool name in step 4. **Disable using regedit by completing the following steps.** NOTE: Before making changes to the registry, make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes. 1 Select **Start** > **Run**. 2 Type regedit on the **Run** dialog box and click **OK**. 3 Navigate to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System 4 Right-click the **EnableLUA** value and select Modify. 5 Change the **Value data** field to 0 on the **Edit DWORD Value** dialog box and click **OK**. 6 Close the **Registry Editor**. 7 Restart the computer to apply changes. NOTE: You can re-enable UAC using the above procedure and changing the **Value data** field to 1 in step 5.

Performance troubleshooting

The following section states a possible issue and the recommended solution for Performance errors.

Problem	Resolution

An error message with the following text displays:
Real Time statistics collection has failed. Please see master log for details.
	Make sure that the following prerequisites for Performance Monitoring Data collection are met.
	1 To collect performance statistics for any protocol type (FC/FCIP/FCOE/GE), the snmp access control list must have an empty list or the Management server IP must be included in the access control list.
	For example, data collection occurs in the following cases.
	Case 1: Default access control list is empty
	`FCRRouter:admin> snmpconfig --show accesscontrol`
	`SNMP access list configuration:`
	`Entry 0:  No access host configured yet`
	`Entry 1:  No access host configured yet`
	`Entry 2:  No access host configured yet`
	`Entry 3:  No access host configured yet`
	`Entry 4:  No access host configured yet`
	`Entry 5:  No access host configured yet`
	
	Case 2: Management Server IP included in access control list
	`FCRRouter:admin> snmpconfig --show accesscontrol`
	`SNMP access list configuration:`
	`Entry 0:  Access host subnet area 172.26.1.86 (rw)`
	`Entry 1:  No access host configured yet`
	`Entry 2:  No access host configured yet`
	`Entry 3:  No access host configured yet`
	`Entry 4:  No access host configured yet`
	`Entry 5:  No access host configured yet`
	Verification and Troubleshooting.
	To add the server IP address to the access control list, use the following command from the switch CLI:
	`FCRRouter:admin> snmpconfig --set accesscontrol`
	To set the default access control, use the following command from the switch CLI:
	`FCRRouter:admin> snmpconfig --default accesscontrol`

Problem	Resolution

An error message with the following text displays:
Real Time statistics collection has failed. Please see master log for details.
	2 To collect data, the SNMP credentials in the Management application and switch must match.
	SNMP v1 or v3: The community strings entered in the **Address Properties** dialog box - **SNMP** tab must match the one entered in the switch.
	If you enter ‘test’ as the SNMP v1 community string in the Management application, then the community string in the switch must be ‘test’ as well.
	To view the switch SNMP value, use one of the following commands from the switch CLI:
	`HCLSwitch:admin> snmpconfig --show snmpv1`
	`HCLSwitch:admin> snmpconfig --show snmpv3`
	To set the switch SNMP value, use one of the following commands from the switch CLI:
	`HCLSwitch:admin> snmpconfig --set snmpv1`
	`HCLSwitch:admin> snmpconfig --set snmpv3`
	Example
	`HCLSwitch:admin> snmpconfig --set snmpv1`
	`SNMP community and trap recipient configuration:`
	`Community (rw): [test]`
	`Trap Recipient's IP address : [172.26.1.183]`
	`Trap recipient Severity level : (0..5) [4]`
	`Trap recipient Port : (0..65535) [162]`
	`Community (rw): [OrigEquipMfr]`
	`Trap Recipient's IP address : [172.26.24.26]`
	`Trap recipient Severity level : (0..5) [4]`
	`Trap recipient Port : (0..65535) [162]`
	`Community (rw): [custom]`
	`Trap Recipient's IP address : [172.26.1.158]`
	`Trap recipient Severity level : (0..5) [4]`
	`Trap recipient Port : (0..65535) [162]`
	`Community (ro): [custom]`
	`Trap Recipient's IP address : [0.0.0.0]`
	`Community (ro): [common]`
	`Trap Recipient's IP address : [0.0.0.0]`
	`Community (ro): [FibreChannel]`
	`Trap Recipient's IP address : [172.26.1.145]`
	`Trap recipient Severity level : (0..5) [4]`
	`Trap recipient Port : (0..65535) [162]`

<table>
<tr><th>Problem</th><th>Resolution</th></tr>
<tr><td>An error message with the following text displays:
Real Time statistics collection has failed. Please see master log for details.</td><td>3 To collect GigE port and FCIP statistics, you must enable the FCIP-MIB capability.
Verification and Troubleshooting
To verify that FCIP-MIB capability is enabled, use the following command from the switch CLI:
<pre>
FCRRouter:admin> snmpconfig --show mibcapability
    FCIP-MIB: YES
</pre>
To enabling FCIP-MIB capability, use the following command from the switch CLI:
<pre>
FCRRouter:admin> snmpconfig --set mibcapability
FA-MIB (yes, y, no, n): [yes]
FICON-MIB (yes, y, no, n): [yes]
HA-MIB (yes, y, no, n): [yes]
FCIP-MIB (yes, y, no, n): [yes]
ISCSI-MIB (yes, y, no, n): [yes]
</pre>
4 To collect FCIP or GE statistics, you must configure SNMPv3 credentials in the Address Properties dialog box - SNMP tab.
Verify that the SNMPv3 credentials are valid. When you discover a switch using ‘admin’ as the v3 credentials, a new user (for example, User 6) is created with the SNMP user name ‘admin’. To verify the SNMP user credentials, use the following command from the switch CLI:
<pre>
sw1:FID128:admin> snmpconfig --show snmpv3

SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 2 (rw): snmpadmin2
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 3 (rw): snmpadmin3
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 4 (ro): snmpuser1
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 5 (ro): snmpuser2
        Auth Protocol: noAuth
        Priv Protocol: noPriv
User 6 (ro): admin
        Auth Protocol: noAuth
        Priv Protocol: noPriv
</pre></td></tr>
</table>

Problem	Resolution

An error message with the following text displays:
Real Time statistics collection has failed.
Please see master log for details.
	5 To collect data on Virtual Fabric-enabled switches, the Fabric OS user must have access to all Virtual Fabrics. The SNMPv3 user name must be the same as the Fabric OS user name. If the SNMPv3 and Fabric OS user names do not match, data is not collected for the virtual switches with the non-default VF ID. By default, the user 'admin' has access to all Virtual Fabrics.
	To verify the Fabric OS user (verify Role-LF List), use the following command from the switch CLI:
	`sw1:FID128:admin> userconfig --show`
	`Account name: admin`
	`Description: Administrator`
	`Enabled: Yes`
	`Password Last Change Date: Unknown`
	`Password Expiration Date: Not Applicable`
	`Locked: No`
	`Home LF Role: admin`
	`Role-LF List: admin: 1-128`
	`Chassis Role: admin`
	`Home LF: 128`
	6 To collect real time data, I/O must be running in the switch. To view the statistics in the switch, use one of the following command:
	FC Ports command from the switch CLI:
	`portperfshow <interval>`
	Example `Sprint-65:root> portperfshow 5`
	FCIP tunnels: command:
	`portshow fciptunnel <Ge port number> <tunnel no> -perf`
	Example `Sprint-65:root> portshow fciptunnel ge0 1 -perf`

An error message with the following text displays:
Real Time statistics collection has failed.
Please see master log for details.
	7 To collect performance statistics from a switch, the SNMP security level must be set correctly in the switch. For example, a secLevel of '3' means "No access" which stops the management application from collecting performance statistics from the switch.
	To show the security level respectively, use the following command from the switch CLI:
	`snmpconfig --show secLevel`
	Example
	`snmpconfig --show secLevel`
	`GET security level = 0, SET level = 0`
	`SNMP GET Security Level: No security`
	`SNMP SET Security Level: No security`
	To set the security level respectively, use the following command from the switch CLI:
	`snmpconfig --set secLevel`
	Example
	`snmpconfig --set secLevel 0`
	`Select SNMP GET Security Level`
	`(0 = No security, 1 = Authentication only, 2 = Authentication and Privacy, 3 = No Access): (0..3) [0]`

Port Fencing troubleshooting

The following section states a possible issue and the recommended solution for Port Fencing errors.

Problem	Resolution
In a pure M-EOS fabric, fabric level policy information (for example, Port Fencing Link threshold) is stored in database based on the principle switch WWN. Therefore, if you add a switch to the fabric and the new switch becomes the Principle switch, the Management application cannot obtain the policy information and the threshold is not applied.	Re-assign the threshold to the fabric. For step-by-step instructions, refer to "Assigning thresholds" on page 691.
If you segment a switch from a fabric then rediscover the switch without accepting changes, the **Port Fencing** dialog box displays the switch twice and the port count is doubled.	Right-click on the fabric that the segmented switch (with red minus icon) is part of and select **Accept Changes**.

Server Management Console troubleshooting

The following section states a possible issue and the recommended solution for server management console errors.

Problem	Resolution
Unable to launch the SMC on a Windows Vista,Windows 7 , or Windows 2008 R2 system	The Windows Vista,Windows 7,or Windows 2008 R2 system enables the User Access Control (UAC) option by default. When the UAC option is enabled, the SMC cannot launch. If the SMC does not launch, use one of the following options to disable the UAC option: The following are the various ways we can disable UAC in vista: **Disable using msconfig by completing the following steps.** 1 Select **Start** > **Run**. 2 Type msconfig on the **Run** dialog box and click **OK**. 3 Click the **Tools** tab on the **System Configuration Utility**. 4 Scroll down to and select the **Disable UAC** tool name. 5 Click **Launch**. A command window displays and runs the disable UAC command. When the command is complete, close the window. 6 Close the **System Configuration Utility**. 7 Restart the computer to apply changes. **NOTE:** You can re-enable UAC using the above procedure and selecting the **Enable UAC** tool name in step 4. **Disable using regedit by completing the following steps.** **NOTE:** Before making changes to the registry, make sure you have a valid backup. In cases where you're supposed to delete or modify keys or values from the registry it is possible to first export that key or value(s) to a .REG file before performing the changes. 1 Select **Start** > **Run**. 2 Type regedit on the **Run** dialog box and click **OK**. 3 Navigate to the following registry key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System 4 Right-click the **EnableLUA** value and select Modify. 5 Change the **Value data** field to 0 on the **Edit DWORD Value** dialog box and click **OK**. 6 Close the **Registry Editor**. 7 Restart the computer to apply changes. **NOTE:** You can re-enable UAC using the above procedure and changing the **Value data** field to 1 in step 5.

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

Supportsave troubleshooting

The following section states a possible issue and the recommended solution for supportsave errors.

Problem	Resolution
Cannot capture support save information.	Capture support show by running the batch file from the *Install_Home*/bin/supportshow.bat from Windows and UNIX systems. 1 *Open Install_Home*\bin\supportsave.bat. 2 Edit file `supportsave dbuser dbpasswd [tareget-dir] [pause-option]`.

View All list troubleshooting

The following section states a possible issue and the recommended solution for **View All** list errors.

Problem	Resolution
View All list does not display.	The **View All** list does not display until you discover a fabric. To discover a fabric, refer to “Discovering fabrics” on page 53.
View All list does not display and there are discovered fabrics. **Example** If you create a new view ’V1’ that has one fabric ‘F1’ and you display the new view in the SAN tab (select **V1** from the **View All** list). Then you delete the fabric F1 from Discovery, the **View All** list no longer displays and the following messages displays: View loaded, no devices present in the current view. Refer to the Troubleshooting Guide in Help (F1) for assistance.	To select another view, select **View** > **Manage View** > **Display View** > *View_Name*.

Zoning troubleshooting

The following section states some possible issues and recommended solutions for zoning errors.

Problem	Resolution
Cannot perform zoning on a new switch.	You must use telnet (or the **Product Type and Access** tab in the **Add Properties** dialog box) to change the default password on the new switch before you can use the Management application to perform zoning.
When configuring a large zone configuration a switch displays offline during discovery.	If a large zone configuration is configured in a fabric, switches may temporarily display as being offline during discovery. Wait for the next discovery cycle and click the **Refresh** button on the toolbar.
When activating a large zone configuration on a two-switch fabric on UNIX platforms, an error message displays stating “Failed to perform the requested zoning action: Failed to zone due to exception.”	Although the error message states that the requested zoning action failed, the zone configuration will be correctly activated. Wait for the next zoning polling to occur. This issue only occurs on UNIX systems.
Zoning activation message displays for a long time, but zone configuration is not activated.	Telnet zoning can take a long time. To improve speed, open the **Discover Setup** dialog box (**Discover** > **Setup**) and add the IP address for the device to the **Selected Individual Addresses** list.
Out of memory error caused by running a zoning report for a large zone configuration (1 MB) in a medium-sized SAN due to a third party tool.	You must increase the client memory allocation by completing “Configuring memory allocation settings” on page 123.

Chapter

Performance Data

27

In this chapter

SAN performance overview

Performance monitoring provides details about the quantity of traffic and errors a specific port or device generates on the fabric over a specific time frame. You can also use performance to indicate the devices that create the most traffic and to identify the ports that are most congested.

Performance allows you to monitor your SAN using the following methods (requires a Licensed version):

- Display the connections which are using the most bandwidth on the selected device or one of the F_ports on the device with a feature called Top Talkers.
- Gather and display real-time performance data (FC ports, ISL ports, Device ports, GE ports, FCIP tunnels, Managed HBA ports, Managed CNA ports, E port trunks, and 10 GE ports).
- Persist and display historical performance data (FC ports, ISL ports, Device ports, FCIP tunnels, and 10 GE ports) for selected fabrics or the entire SAN.
- Support End-to-End monitors for real-time and historical performance data.
- Enforce user-defined performance thresholds and notification when thresholds are exceeded.

NOTE
When the server is busy and you request performance statistics, an "insufficent resources" message displays. Wait a while before you request the performance statistics again.

- Display percentage utilization for FC and FCIP links.

- Provide aging scheme.

  The granularity varies depending on the configuration on the **Server Management Console**, **Performance Data Aging** tab.

  Option 1—2 years data with the following samples

  - 5 minutes granularity for last 1 day (288 samples)
  - 30 minutes granularity for last 3 days (144 samples)
  - 2 hour granularity for last 7 days (84 samples)
  - 1 day granularity for last 2 years (730 samples)

  Option 2—2 years data with the following samples

  - 5 minutes granularity for last 8 days (2304 samples)
  - 1 day granularity for last 2 years (730 samples)

  For more information, refer to "Defining the performance data aging interval" on page 235.

- Provide enhanced performance reports.

SAN Performance measures

Performance measures enable you to select one or more measures to define the graph or report. The measures available to you depend on the object type from which you want to gather performance data.

NOTE
Devices with 10GE ports must be running Fabric OS 6.4.1ltd or later to obtain the correct TE port statistics (TX/RX).

NOTE
Devices with 10GE ports must have the rmon MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference*.

- Tx % Utilization — available for FC, GE, Managed HBA ports, Managed CNA ports, E port trunks, 10GE ports, and FCIP tunnels.
- Rx % Utilization — available for FC, GE, Managed HBA ports, Managed CNA ports, 10GE ports, E port trunks, and FCIP tunnels.
- Tx MB/Sec — available for FC, GE, Managed HBA ports, Managed CNA ports, 10GE ports, E port trunks, FCIP tunnels, and End-to-End monitors.
- Rx MB/Sec — available for FC, GE, Managed HBA ports, Managed CNA ports, 10GE ports, E port trunks, FCIP tunnels, and End-to-End monitors.
- CRC Errors — available for FC, Managed HBA ports, Managed CNA ports, 10GE ports and End-to-End monitors.
- Signal Losses — available for Managed HBA ports, Managed CNA ports, and FC ports.
- Sync Losses — available for Managed HBA ports, Managed CNA ports, and FC ports.
- Link Failures — available for Managed HBA ports, Managed CNA ports, and FC ports.
- Sequence Errors — available for FC ports.
- Invalid Transmissions — available for FC ports.

- Rx Link Resets — available for FC ports.
- Tx Link Resets — available for FC ports.
- C3 Discard— available for FC ports.
- Dropped Packets — available for FCIP tunnels only.
- Compression Ratio — available for FCIP tunnels only.
- Latency — available for FCIP tunnels only.
- Link Retransmits — available for FCIP tunnels only.
- Timeout Retransmits — available for FCIP tunnels only.
- Fast Retransmits — available for FCIP tunnels only.
- Duplicate Ack Received — available for FCIP tunnels only.
- Window Size RTT — available for FCIP tunnels only.
- TCP Out of Order Segments — available for FCIP tunnels only.
- Slow Start Status — available for FCIP tunnels only.
- Frames Received — available for 10GE ports only.
- Overflow Errors — available for 10GE ports only.
- Runtime Errors — available for 10GE ports only.
- Receive EOF — available for 10GE ports only.
- Too Long Errors — available for 10GE ports only.
- Underflow Errors — available for 10GE ports only.
- Alignment Errors — available for 10GE ports only.
- NOS Count — available for Managed HBA ports and Managed CNA ports.
- Error Frames — available for Managed HBA ports and Managed CNA ports.
- Under Sized Frames — available for Managed HBA ports and Managed CNA ports.
- Over Sized Frames — available for Managed HBA ports and Managed CNA ports.
- Primitive Sequence Protocol Errors — available for Managed HBA ports and Managed CNA ports.
- Dropped Frames — available for Managed HBA ports and Managed CNA ports.
- Bad EOF Frames — available for Managed HBA ports and Managed CNA ports.
- Invalid Ordered Sets — available for Managed HBA ports and Managed CNA ports.
- Non Frame Coding Error — available for Managed HBA ports and Managed CNA ports.

SAN Performance management requirements

To collect performance data, make sure the following requirements have been met:

- Make sure the snmp access control list for the device is empty or the Management application server IP is in the access control list.

  Example of default access control list

  ```
  FCRRouter:admin> snmpconfig --show accesscontrol
  SNMP access list configuration:
  Entry 0:  No access host configured yet
  Entry 1:  No access host configured yet
  Entry 2:  No access host configured yet
  Entry 3:  No access host configured yet
  Entry 4:  No access host configured yet
  Entry 5:  No access host configured yet
  ```

  Example of Management application Server IP included in access control list

  ```
  FCRRouter:admin> snmpconfig --show accesscontrol
  SNMP access list configuration:
  Entry 0:  Access host subnet area 172.26.1.86 (rw)
  Entry 1:  No access host configured yet
  Entry 2:  No access host configured yet
  Entry 3:  No access host configured yet
  Entry 4:  No access host configured yet
  Entry 5:  No access host configured yet
  ```

  To add the Management application server IP address to the access control list, use the `snmpconfig --add accesscontrol` command:

  To set the default access control, use the `snmpconfig --default accesscontrol` command:

- Make sure that the SNMP credentials in the Management application match the SNMP credentials on the device.
  - To check the SNMP v1 credentials on the device, use the `snmpconfig --show snmpv1` command.

    Example of SNMP v1

    ```
    HCLSwitch:admin> snmpconfig --show snmpv1
    SNMPv1 community and trap recipient configuration:
    Community 1: Secret C0de (rw)
    Trap recipient: 10.103.4.63
    Trap port: 162
    Trap recipient Severity level: 4
    Community 2: OrigEquipMfr (rw)
    Trap recipient: 10.191.12.240
    Trap port: 162
    Trap recipient Severity level: 4
    Community 3: private (rw)
    Trap recipient: 10.103.5.105
    Trap port: 162
    Trap recipient Severity level: 4
    Community 4: public (ro)
    Trap recipient: 192.168.102.41
    Trap port: 162
    Trap recipient Severity level: 4
    Community 5: common (ro)
    Trap recipient: 10.32.150.116
    ```

```
Trap port: 162
Trap recipient Severity level: 4
Community 6: FibreChannel (ro)
Trap recipient: 1001:0:0:0:0:0:0:172
Trap port: 162
Trap recipient Severity level: 4
```

- To set the SNMP v1 credentials on the device, use the `snmpconfig --set snmpv1` command.

  Example of setting SNMP v1

```
HCLSwitch:admin> snmpconfig --set snmpv1
SNMP community and trap recipient configuration:
Community (rw): [test]
Trap Recipient's IP address : [172.26.1.183]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [OrigEquipMfr]
Trap Recipient's IP address : [172.26.24.26]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (rw): [custom]
Trap Recipient's IP address : [172.26.1.158]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Community (ro): [custom]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [common]
Trap Recipient's IP address : [0.0.0.0]
Community (ro): [FibreChannel]
Trap Recipient's IP address : [172.26.1.145]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
```

- To check the SNMP v3 credentials on the device, use the `snmpconfig --show snmpv3` command.

  Example of SNMP v3

```
sw1:FID128:admin> snmpconfig --show snmpv3
SNMPv3 USM configuration:
User 1 (rw): snmpadmin1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 2 (rw): snmpadmin2
Auth Protocol: noAuth
Priv Protocol: noPriv
User 3 (rw): snmpadmin3
Auth Protocol: noAuth
Priv Protocol: noPriv
User 4 (ro): snmpuser1
Auth Protocol: noAuth
Priv Protocol: noPriv
User 5 (ro): snmpuser2
Auth Protocol: noAuth
Priv Protocol: noPriv
User 6 (ro): admin
Auth Protocol: noAuth
```

```
Priv Protocol: noPriv
```

- To set the SNMP v3 credentials on the device, use the `snmpconfig --set snmpv3` command.

```
FM_4100_21:admin> snmpconfig --set snmpv3
SNMPv3 user configuration(SNMP users not configured in Fabric OS user
database will have physical AD and admin role as the default):
User (rw): [snmpadmin1] admin
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3] 1
New Auth Passwd:
Verify Auth Passwd:
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(1..6) [2] 1
New Priv Passwd:
Verify Priv Passwd:
User (rw): [snmpadmin2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (rw): [snmpadmin3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser1]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser2]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
User (ro): [snmpuser3]
Auth Protocol [MD5(1)/SHA(2)/noAuth(3)]: (1..3) [3]
Priv Protocol [DES(1)/noPriv(2)/3DES(3)/AES128(4)/AES192(5)/AES256(6)]):
(2..2) [2]
SNMPv3 trap recipient configuration:
Trap Recipient's IP address : [192.168.71.32]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [1.1.1.1]
UserIndex: (1..6) [2]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [10.64.209.171]
UserIndex: (1..6) [1]
Trap recipient Severity level : (0..5) [4]
Trap recipient Port : (0..65535) [162]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
Trap Recipient's IP address : [0.0.0.0]
```

- To check SNMP credentials in the Management application, complete the following steps.

  1. Select **Discover > Fabrics.**
     The **Discover Fabrics** dialog box displays.

  2. Select an IP address from the **Available Addresses** table.

  3. Click **Edit.**
     The **AddFabric Discovery** dialog box displays.

4. Click the **Manual** option to view SNMP credentials.
5. Click the **SNMP** tab.
6. Select the **v1** or **v3** from the **SNMP Version** list.
7. Make sure SNMP credentials match those on the device.
8. Click **OK** on the **AddFabric Discovery** dialog box.
9. Click **Close** on the **Discover Fabrics** dialog box.

- To set SNMP credentials in the Management application, refer to "Configuring SNMP credentials" on page 58.

- Make sure that the SNMP security level is set to the appropriate level for the switch.
  - To check the SNMP security level, use the snmpconfig --show secLevel command.

    Example of checking SNMP security level

    ```
    snmpconfig --show secLevel
    GET security level = 0, SET level = 0
    SNMP GET Security Level: No security
    SNMP SET Security Level: No security
    ```

  - To set the SNMP security level, use the snmpconfig --set secLevel command.

    Example of checking SNMP security level

```
snmpconfig --set secLevel 0
    Select SNMP GET Security Level
    (0 = No security, 1 = Authentication only, 2 = Authentication and Privacy,
    3 = No Access): (0..3) [0]
```

- To collect performance for GigE ports and FCIP statistics, make sure that SNMP v3 credentials match (see above) and that FCIP-MIB capability is enabled.
  - To check FCIP-MIB capability, use the `snmpconfig --show mibcapability` command.

    Example of showing FCIP-MIB

    ```
    FCRRouter:admin> snmpconfig --show mibcapability
    FCIP-MIB: YES
    ```

  - To enable FCIP-MIB capability, use the `snmpconfig --set mibcapability` command.

    Example of enabling FCIP-MIB

    ```
    FCRRouter:admin> snmpconfig --set mibcapability
    FA-MIB (yes, y, no, n): [yes]
    FICON-MIB (yes, y, no, n): [yes]
    HA-MIB (yes, y, no, n): [yes]
    FCIP-MIB (yes, y, no, n): [yes]
    ISCSI-MIB (yes, y, no, n): [yes]
    ```

- To collect performance on a Virtual Fabric enabled device, use the `userconfig --show` command to make sure the Fabric OS user has access to all the Virtual Fabrics. Make sure that the SNMPv3 user name is same as the Fabric OS user name. Otherwise, the data is not collected for virtual switches with a non-default VF ID. By default the `admin` user has access to all Virtual Fabrics.

  Example of Fabric OS user verification

  ```
  sw1:FID128:admin> userconfig --show
  Account name: admin
  Description: Administrator
  Enabled: Yes
  Password Last Change Date: Unknown
  Password Expiration Date: Not Applicable
  Locked: No
  Home LF Role: admin
  Role-LF List: admin: 1-128
  Chassis Role: admin
  Home LF: 128
  ```

  - Make sure I/O is running on the switch to obtain real statistics. To view switch statistics, use the `portperfshow [slot/]port -[slot/]port | -tx | -rx | -tx -rx | -t <`*`interval`*`>` (FC Ports) or `portshow fciptunnel <Ge port number> <tunnel no> -perf` (FCIP tunnels) command.

  Example for FC ports

  ```
  Sprint-65:root> portperfshow 5
  ```

  Example for FCIP tunnels

  ```
  Sprint-65:root> portshow fciptunnel ge0 1 -perf
  ```

SAN real-time performance data

Real-time performance enables you to collect data from managed devices in your SAN. Real-time performance is only supported on the following managed objects: FC (E_ and F_ports), GE_ports, E port trunks, 10GE_ports, Managed HBA Ports, Managed CNA Ports, and FCIP tunnels. You can use real-time performance to configure the following options:

- Select the polling rate from 10 seconds up to 1 minute.
- Select up to 32 ports total from a maximum of 10 devices for graphing performance.

  For E port trunks, you can select up to 8 trunks (the trunk member (port) count must be below 32) from a maximum of 10 devices for graphing performance.

  NOTE
  Virtual Fabric logical ISL ports are not included in performance collection.

- Choose to display the same Y-axis range for both the Tx MB/Sec and Rx MB/Sec measure types for easier comparison of graphs.

Generating a real-time performance graph

You can monitor a device's performance through a performance graph that displays transmit and receive data. The graphs can be sorted by the column headers. You can create multiple real-time performance graph instances.

NOTE
To make sure that statistic collection for a switch does not fail, you must configure SNMP credentials for the switch. For step-by-step instructions, refer to "Configuring SNMP credentials" on page 58.

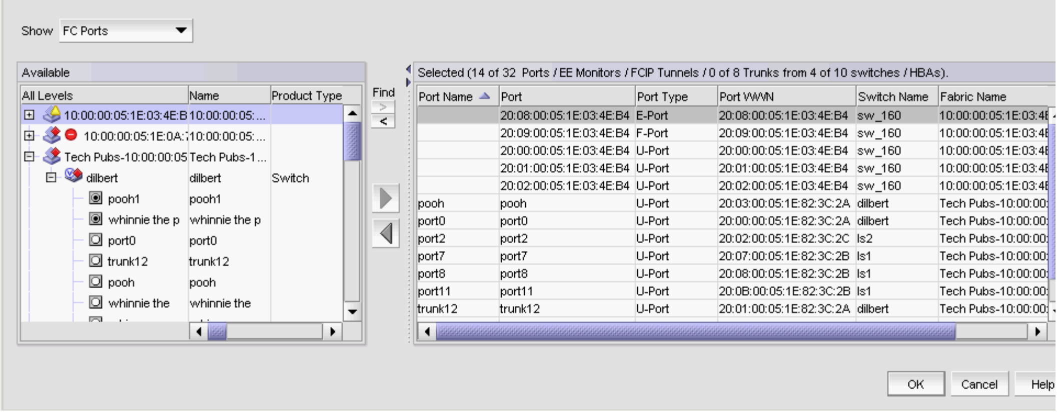
To generate a real-time performance graph for a device, complete the following steps.

1. Select the fabric, device, or port for which you want to generate a performance graph.
2. Choose one of the following options:
   - Select **Monitor** > **Performance** > **Real-Time Graph**.

     OR
   - Right-click the device or fabric and select **Performance** > **Real-Time Graph**.

   If you selected a port, the **Real Time Performance Graphs** dialog box for the selected port displays. To filter real-time performance data from the **Real Time Performance Graphs** dialog box, refer to "Filtering real-time performance data" on page 762.

   If you selected a fabric or device, the **Realtime Port Selector** dialog box displays. Continue with step 3.



All Levels	Name	Product Type
10:00:00:05:1E:03:4E:B	10:00:00:05:...	
10:00:00:05:1E:0A:7	10:00:00:05:...	
Tech Pubs-10:00:00:05	Tech Pubs-1...	
dilbert	dilbert	Switch
pooh1	pooh1	
whinnie the p	whinnie the p	
port0	port0	
trunk12	trunk12	
pooh	pooh	
whinnie the	whinnie the	

Selected (14 of 32 Ports / EE Monitors / FCIP Tunnels / 0 of 8 Trunks from 4 of 10 switches / HBAs).

Port Name	Port	Port Type	Port WWN	Switch Name	Fabric Name
	20:08:00:05:1E:03:4E:B4	E-Port	20:08:00:05:1E:03:4E:B4	sw_160	10:00:00:05:1E:03:4E
	20:09:00:05:1E:03:4E:B4	F-Port	20:09:00:05:1E:03:4E:B4	sw_160	10:00:00:05:1E:03:4E
	20:00:00:05:1E:03:4E:B4	U-Port	20:00:00:05:1E:03:4E:B4	sw_160	10:00:00:05:1E:03:4E
	20:01:00:05:1E:03:4E:B4	U-Port	20:01:00:05:1E:03:4E:B4	sw_160	10:00:00:05:1E:03:4E
	20:02:00:05:1E:03:4E:B4	U-Port	20:02:00:05:1E:03:4E:B4	sw_160	10:00:00:05:1E:03:4E
pooh	pooh	U-Port	20:03:00:05:1E:82:3C:2A	dilbert	Tech Pubs-10:00:00:
port0	port0	U-Port	20:00:00:05:1E:82:3C:2A	dilbert	Tech Pubs-10:00:00:
port2	port2	U-Port	20:02:00:05:1E:82:3C:2C	ls2	Tech Pubs-10:00:00:
port7	port7	U-Port	20:07:00:05:1E:82:3C:2B	ls1	Tech Pubs-10:00:00:
port8	port8	U-Port	20:08:00:05:1E:82:3C:2B	ls1	Tech Pubs-10:00:00:
port11	port11	U-Port	20:0B:00:05:1E:82:3C:2B	ls1	Tech Pubs-10:00:00:
trunk12	trunk12	U-Port	20:01:00:05:1E:82:3C:2A	dilbert	Tech Pubs-10:00:00:

FIGURE 327 Realtime Port Selector dialog box

3. Select the object type (FC Ports, ISL Ports, Device Ports, EE Monitors, GE Ports, FCIP Tunnels, Managed HBA Ports, Managed CNA Ports, E Port Trunks, or 10GE Ports) by which you want to graph performance from the **Show** list.

   NOTE
   Devices with 10GE ports must be running Fabric OS 6.4.1ltd or later to obtain the correct TE port statistics (TX/RX).

   NOTE
   Devices with 10GE ports must have the rmon MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference*.

4. Right-click anywhere in the **Available** table and select **Expand All**.
5. Select the ports or trunks you want to include in the performance graph in the **Available** table.

   Press **Ctrl** or **Shift** and then click to select more than one port.
6. Click the right arrow to move the selected ports to the **Selected** table.
7. Click **OK**.

   The **Real Time Performance Graphs** dialog box displays.

Filtering real-time performance data

To filter real-time performance data from the **Real Time Performance Graphs** dialog box, complete the following steps.

1. Open the **Real Time Performance Graphs** dialog box.

   For step-by-step instructions, refer to "Generating a real-time performance graph" on page 761. The **Real Time Performance Graphs** dialog box displays.
2. Click **Select** to change the object type.
3. Select the object type (FC Ports, ISL Ports, Device Ports, EE Monitors, GE Ports, FCIP Tunnels, Managed HBA Ports, Managed CNA Ports, E Port Trunks, or 10GE Ports) by which you want to graph performance from the **Show** list.

   NOTE
   Devices with 10GE ports must be running Fabric OS 6.4.1ltd or later to obtain the correct TE port statistics (TX/RX).

   NOTE
   Devices with 10GE ports must have the rmon MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference*.
4. Right-click anywhere in the **Available** table and select **Expand All**.
5. Select the ports or trunks you want to include in the performance graph in the **Available** table.

   Press **Ctrl** or **Shift** and then click to select more than one port.
6. Click the right arrow to move the selected ports to the **Selected** table.
7. Click **OK**.

   The **Real Time Performance Graphs** dialog box displays.
8. Select the measure by which you want to gather performance data from the **Measures** list.

   To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.
9. (Optional) Enter a value (percentage) in the **Reference Line** field to set a reference for the transmit and receive utilization.

   Note that this field is only available when you select **Tx % Utilization** or **Rx % Utilization** from the **Measures** list.
10. Select the granularity at which you want to gather performance data from the **Granularity** list.

11. Select the **Interpolate** check box to use interpolation to fill existing gaps, if necessary.
12. (Optional) Click **Other Options** and select the **Use Same Y-axis** check box to make the Y-axis range the same for object.

    The **Use Same Y-axis** check box is only available when you select **Rx MB/sec** and **Tx MB/sec** from the **Measures** list. You do not have to apply this change, the performance graph automatically updates.
13. Move the **Row Height** slider to the left to make the row height smaller or to the right to make it bigger.
14. Select the **Display tabular data only** check box to only show text with no graphs or icons.

    The **Source** and **Destination** icons and the **Graph** column do not display
15. Click **Apply.**

    The selected graph automatically displays in the **Real Time Performance Graphs** dialog box.
16. Click the close button (X) to close the **Real Time Performance Graphs** dialog box.

Exporting real-time performance data

To export real-time performance data, complete the following steps.

1. Generate a performance graph.

   To generate a performance graph, refer to “Generating a real-time performance graph” on page 761.
2. Right-click anywhere in the graph table and select **Export Table.**

   The **Save table to a tab delimited file** dialog box displays.
3. Browse to the file location where you want to save the performance data.
4. Enter a name for the file and click **Save.**

Clearing port counters

To reset all port statistic counters to zero on a selected device, complete the following steps.

1. Right-click a device on the Connectivity Map or Product List and select **Performance > Clear Counters.**
2. Click **Yes** on the message.

   A **Port Stats Counter Reset** message displays. If any of the counters do not clear, the message displays a list of the associated ports.
3. Click **Ok** on the **Port Stats Counter Reset** message.

SAN Historical performance data

Performance should be enabled constantly to receive the necessary historical data required for a meaningful report. The following options and features are available for obtaining historical performance data:

- Collect historical performance data from the entire SAN or from a selected .

  NOTE
  Virtual Fabric logical ISL ports are not included in performance collection.

- Persist data on every polling cycle (5 minutes).

  Store up to records (maximum) for each port. Most ports require 600 KB disk space; however, the 256-Port Director requires 7GB disk space.The maximum number of records varies depending on the configuration on the **Server Management Console**, **Performance Data Aging** tab.

  Option 1—1,246 records

  Option 2—3,034 records

  For more information, refer to "Defining the performance data aging interval" on page 235.

- Use the RRD (Round Robin Database) style aging scheme.
- Enable granularity.

  The granularity varies depending on the configuration on the **Server Management Console**, **Performance Data Aging** tab.

  Option 1—2 years data with the following samples

  - 5 minutes granularity for last 1 day (288 samples)
  - 30 minutes granularity for last 3 days (144 samples)
  - 2 hour granularity for last 7 days (84 samples)
  - 1 day granularity for last 2 years (730 samples)

  Option 2—2 years data with the following samples

  - 5 minutes granularity for last 8 days (2304 samples)
  - 1 day granularity for last 2 years (730 samples)

  For more information, refer to "Defining the performance data aging interval" on page 235.

- Support interpolation for up to 6 data points.
- Generate reports. For instructions on generating reports, refer to "Generating SAN performance reports" on page 905.

Enabling historical performance collection SAN wide

To enable historical performance collection, select **Monitor** > **Performance** > **Historical Data Collection** > **Enable SAN Wide.**

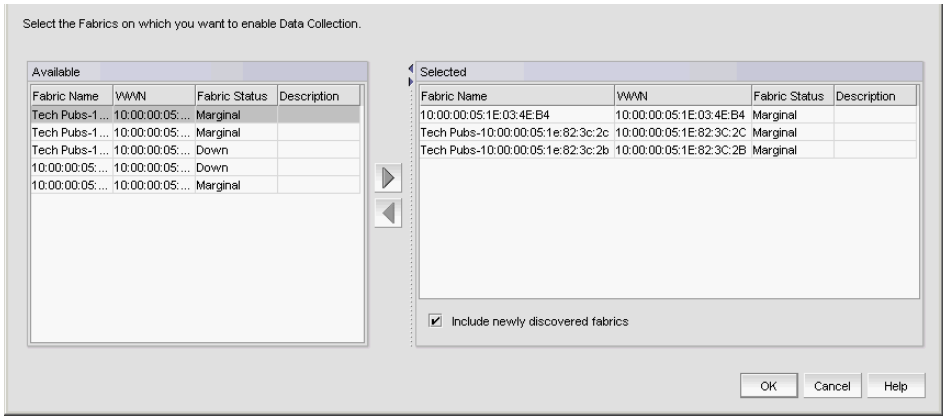
Historical performance data collection is enabled for all fabrics in the SAN.

Enabling historical performance collection for selected fabrics

To enable historical performance collection for selected fabrics, complete the following steps.

1. Select **Monitor > Performance > Historical Data Collection > Enable Selected**.

   The **Historical Data Collection** dialog box displays.



Select the Fabrics on which you want to enable Data Collection.

Available

Fabric Name	WWN	Fabric Status	Description
Tech Pubs-1...	10:00:00:05:...	Marginal	
Tech Pubs-1...	10:00:00:05:...	Marginal	
Tech Pubs-1...	10:00:00:05:...	Down	
10:00:00:05:...	10:00:00:05:...	Down	
10:00:00:05:...	10:00:00:05:...	Marginal	

Selected

Fabric Name	WWN	Fabric Status	Description
10:00:00:05:1E:03:4E:B4	10:00:00:05:1E:03:4E:B4	Marginal	
Tech Pubs-10:00:00:05:1e:82:3c:2c	10:00:00:05:1E:82:3C:2C	Marginal	
Tech Pubs-10:00:00:05:1e:82:3c:2b	10:00:00:05:1E:82:3C:2B	Marginal	

☑ Include newly discovered fabrics

FIGURE 328 Historical Data Collection dialog box

2. Select the fabrics for which you want to collect historical performance data in the **Available** table.

NOTE
Devices with 10GE ports must be running Fabric OS 6.4.1ltd or later to obtain the correct TE port statistics (TX/RX).

NOTE
Devices with 10GE ports must have the rmon MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference*.

3. Click the right arrow to move the selected fabrics to the **Selected** table.
4. Select the **Include newly discovered fabrics** check box to automatically add all newly discovered fabrics to the **Selected** table.
5. Click **OK**.

   Historical performance data collection is enabled for all selected fabrics.

Disabling historical performance collection

To disable historical performance collection on all fabrics, select **Monitor > Performance > Historical Data Collection > Disable All.**

Historical performance data collection is disabled for all fabrics in the SAN.

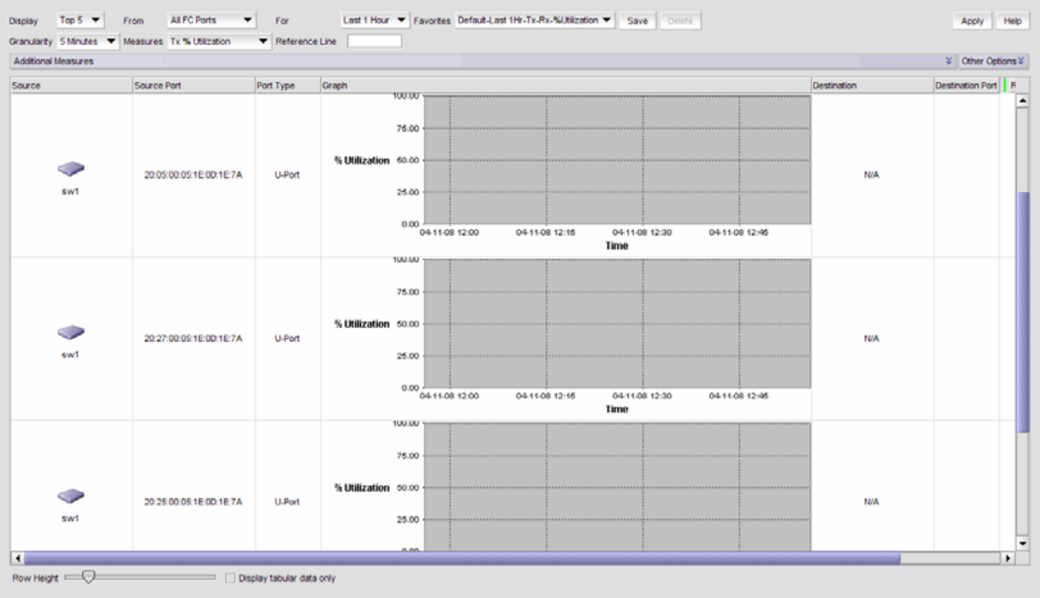
Generating a historical performance graph

To generate a historical performance graph for a device, complete the following steps.

1. Select the device for which you want to generate a performance graph.
2. Choose one of the following options:
   - Select **Monitor > Performance > Historical Graph.**

     OR
   - Right-click the device or fabric and select **Performance > Historical Graph.**

   The **Historical Performance Graph** dialog box displays.



Display: Top 5 From: All FC Ports For: Last 1 Hour Favorites: Default-Last 1Hr-Tx-Rx-%Utilization

Granularity: 5 Minutes Measures: Tx % Utilization Reference Line:

Additional Measures

Source	Source Port	Port Type	Graph	Destination	Destination Port	R
sw1	20:05:00:05:1E:0D:1E:7A	U-Port		N/A		
sw1	20:27:00:05:1E:0D:1E:7A	U-Port		N/A		
sw1	20:25:00:05:1E:0D:1E:7A	U-Port		N/A		

FIGURE 329 Historical Performance Graphs dialog box

3. Select a default or custom-saved (port and time) from the **Favorites** list or filter the historical data by completing the following steps.
   a. Select the number of results to display from the **Display** list.
   b. Select the ports from which you want to gather performance data from the **From** list.

   NOTE
   Devices with 10GE ports must be running Fabric OS 6.4.1ltd or later to obtain the correct TE port statistics (TX/RX).

   NOTE
   Devices with 10GE ports must have the rmon MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference.*

   If you select **Custom**, refer to “Filtering data by ports” on page 768.

c. Select the historical period for which you want to gather performance data from the **For** list.

   If you select **Custom**, refer to “Filtering data by time” on page 769.

d. Select the granularity at which you want to gather performance data from the **Granularity** list.

   The granularity varies depending on the configuration on the **Server Management Console**, **Performance Data Aging** tab.

   Option 1—2 years data with the following samples

   - 5 minutes granularity for last 1 day (288 samples)
   - 30 minutes granularity for last 3 days (144 samples)
   - 2 hour granularity for last 7 days (84 samples)
   - 1 day granularity for last 2 years (730 samples)

   Option 2—2 years data with the following samples

   - 5 minutes granularity for last 8 days (2304 samples)
   - 1 day granularity for last 2 years (730 samples)

   For more information, refer to “Defining the performance data aging interval” on page 235.

e. Select the measure by which you want to gather performance data from the **Measures** list.

   To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.

f. Move the **Row Height** slider to the left to make the row height smaller or to the right to make it bigger.

g. Select the **Display tabular data only** check box to only show text with no graphs or icons.

   The **Source** and **Destination** icons and the **Graph** column do not display

h. Click **Apply.**

   The selected graph automatically displays in the **Historical Performance Graph** dialog box.

   To save a filtered graph, refer to “Saving a historical performance graph configuration” on page 769.

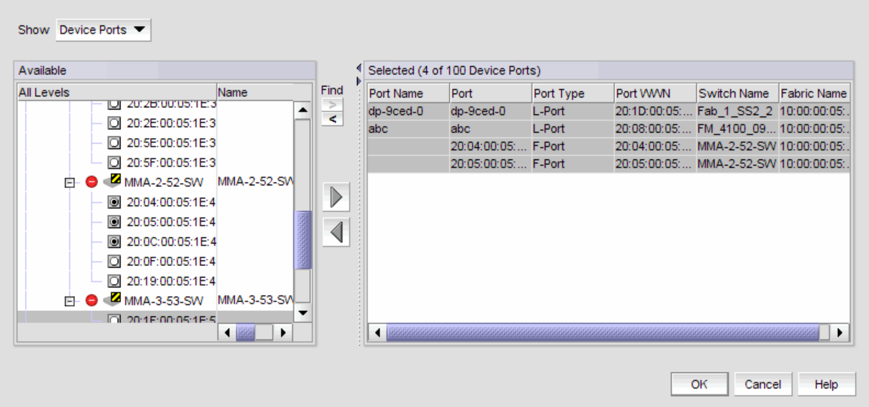
   To delete user-defined graph, refer to “Deleting a historical performance graph” on page 770.

4. Click the close button (X) to close the **HIstorical Performance Graph** dialog box.

Filtering data by ports

To filter data for a historical performance graph by ports, complete the following steps.

1. Select the type of ports from the **Show** list.



Show: Device Ports

Available

All Levels	Name
20:2B:00:05:1E:3	
20:2E:00:05:1E:3	
20:5E:00:05:1E:3	
20:5F:00:05:1E:3	
MMA-2-52-SW	MMA-2-52-SW
20:04:00:05:1E:4	
20:05:00:05:1E:4	
20:0C:00:05:1E:4	
20:0F:00:05:1E:4	
20:19:00:05:1E:4	
MMA-3-53-SW	MMA-3-53-SW
20:1F:00:05:1E:5	

Selected (4 of 100 Device Ports)

Port Name	Port	Port Type	Port WWN	Switch Name	Fabric Name
dp-9ced-0	dp-9ced-0	L-Port	20:1D:00:05:...	Fab_1_SS2_2	10:00:00:05:..
abc	abc	L-Port	20:08:00:05:...	FM_4100_09...	10:00:00:05:..
	20:04:00:05:...	F-Port	20:04:00:05:...	MMA-2-52-SW	10:00:00:05:..
	20:05:00:05:...	F-Port	20:05:00:05:...	MMA-2-52-SW	10:00:00:05:..

FIGURE 330 Custom Port Selector dialog box

2. Right-click a device in the **Available** table and select **Expand All**.
3. Select the ports (press **Ctrl** or **Shift** and then click to select multiple ports) from which you want to gather performance data from the **Available** table and click the right arrow button.

NOTE
Devices with 10GE ports must be running Fabric OS 6.4.1ltd or later to obtain the correct TE port statistics (TX/RX).

NOTE
Devices with 10GE ports must have the rmon MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference*.

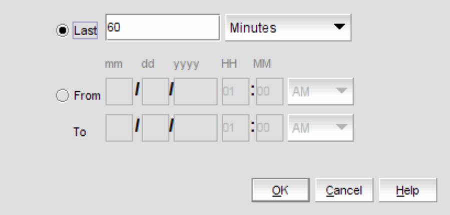
The selected ports move to the **Select Ports** table.

4. Click **OK**.

Filtering data by time

To filter data for a historical performance graph by time, complete the following steps.

1. Select the **Last** option and enter the number of minutes, hours, or days.
   OR
   Select the **From** option and enter the date and time.



● Last 60 Minutes

○ From mm/dd/yyyy HH:MM 01:00 AM

To mm/dd/yyyy HH:MM 01:00 AM

FIGURE 331 Custom Port Selector dialog box

2. Click **OK**.

Saving a historical performance graph configuration

To save a historical performance graph configuration, complete the following steps.

1. Select the device for which you want to generate a performance graph.
2. Choose one of the following options:
   - Select **Monitor > Performance > Historical Graph**.
     OR
   - Right-click the device or fabric and select **Performance > Historical Graph**.

   The **Historical Performance Graph** dialog box displays.
3. Filter the historical data by completing the following steps.
4. Select the number of results to display from the **Display** list.
5. Select the ports from which you want to gather performance data from the **From** list.

NOTE
Devices with 10GE ports must be running Fabric OS 6.4.1ltd or later to obtain the correct TE port statistics (TX/RX).

NOTE
Devices with 10GE ports must have the rmon MIB enabled on the switch. For more information about the **rmon collection** command, refer to the *Fabric OS Converged Enhanced Ethernet Command Reference*.

6. Select the historical period for which you want to gather performance data from the **For** list.
7. Select the granularity at which you want to gather performance data from the **Granularity** list.
8. Select the measure by which you want to gather performance data from the **Measures** list.

   To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.

9. Enter a reference line value percentage for Tx% or Rx % Utilization.

   This field is only enabled when Tx% or Rx % Utilization is selected from the **Measures** list.

10. Move the **Row Height** slider to the left to make the row height smaller or to the right to make it bigger.

11. Select the **Display tabular data only** check box to only show text with no graphs or icons.

    The **Source** and **Destination** icons and the **Graph** column do not display

12. Save this configuration by selecting **Save**.

    The **Save Favorites** dialog box displays. This enables you to save the selected configuration so that you can use it to generate the same type of report at a later date.

13. Enter a name for the configuration in the **Favorites Name** field.

14. Click **OK**.

15. Click **Apply**.

    The selected graph automatically displays in the **Historical Performance Graph** dialog box.

16. Click the close button (X) to close the **HIstorical Performance Graph** dialog box.

Exporting historical performance data

To export historical performance data, complete the following steps.

1. Generate a performance graph.

   To generate a performance graph, refer to "Generating a historical performance graph" on page 766.

2. Right-click anywhere in the graph table and select **Export Table**.

   The **Save table to a tab delimited file** dialog box displays.

3. Browse to the file location where you want to save the performance data.

4. Enter a name for the file and click **Save**.

Deleting a historical performance graph

To delete a user-defined historical performance graph configuration, complete the following steps.

1. Select the device for which you want to generate a performance graph.

2. Choose one of the following options:

   - Select **Monitor > Performance > Historical Graph**.

     OR

   - Right-click the device or fabric and select **Performance > Historical Graph**.

   The **Historical Performance Graph** dialog box displays.

3. Select the configuration you want to delete from the **Favorites** list.

   You can only delete a user-defined historical performance graph. You cannot delete a default favorite historical performance graph.

4. Click **Delete**.
5. Click **Yes** on the confirmation message.
6. Click the close button (X) to close the **Historical Performance Graph** dialog box.

SAN end-to-end monitoring

NOTE
End-to-end monitoring requires a Fabric OS device.

NOTE
End-to-end monitoring on an Access Gateway device requires Fabric OS 7.0 or later with an Advanced Performance Monitor license.

Performance enables you to provision end-to-end monitors of selected target and initiator pairs. These monitors are persisted in the database and are enabled on one of the F_ports on the connected device (the Management application server determines the port). You can use these monitors to view both real-time and historical performance data.

NOTE
A Top Talker and an end-to-end monitor cannot be configured on the same fabric. You must delete the Top Talker monitor before you configure the end-to-end monitor.

Configuring an end-to-end monitor pair

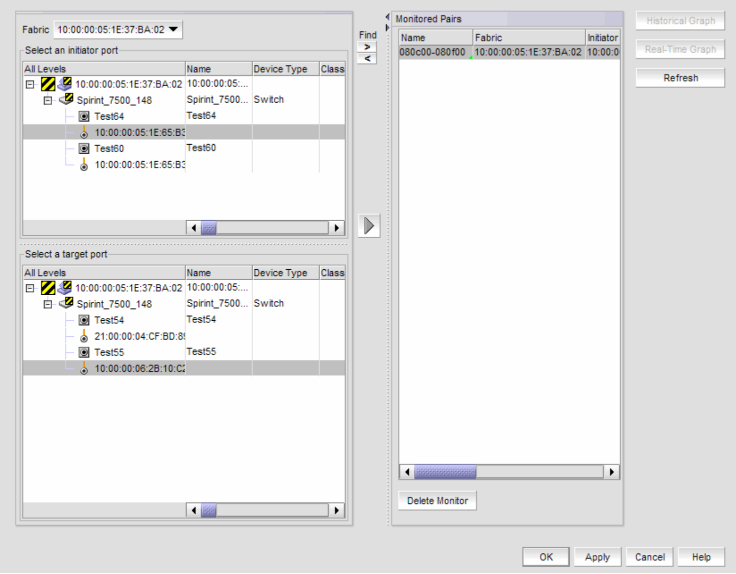
NOTE
End-to-end monitoring on an Access Gateway device requires Fabric OS 7.0 or later with an Advanced Performance Monitor license.

NOTE
Either the initiator device or the target device must have a Advanced Performance Monitor license configured to create an end-to-end monitor.

To configure an end-to-end monitor pair, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors**.

   The **Set End-to-End Monitors** dialog box displays.


Fabric 10:00:00:05:1E:37:BA:02

Select an initiator port

All Levels	Name	Device Type	Class
10:00:00:05:1E:37:BA:02	10:00:00:05:...		
Spirint_7500_148	Spirint_7500...	Switch	
Test64	Test64		
10:00:00:05:1E:65:B3			
Test60	Test60		
10:00:00:05:1E:65:B3			

Select a target port

All Levels	Name	Device Type	Class
10:00:00:05:1E:37:BA:02	10:00:00:05:...		
Spirint_7500_148	Spirint_7500...	Switch	
Test54	Test54		
21:00:00:04:CF:BD:8			
Test55	Test55		
10:00:00:06:2B:10:C2			

Monitored Pairs

Name	Fabric	Initiator
080c00-080f00	10:00:00:05:1E:37:BA:02	10:00:0

FIGURE 332 Set End-to-End Monitors dialog box

2. Select the fabric for which you want to configure end-to-end monitoring from the **Fabric** list.
3. Select an initiator port from the **Select an initiator port** table.
4. Select a target port from the **Select a target port** table.
5. Click the right arrow to move the selected initiator and target ports to the **Monitored Pairs** table.

   The system automatically determines the initiator SID and the target DID identifiers for the pair and displays them in the **Monitored Pairs** table.
6. Click **Apply**.

   Once the end-to-end monitored pair is applied to the device, the **Status** column in the **Monitored Pairs** table displays 'Enabled'. If the end-to-end monitored pair fails, the **Status** column in the **Monitored Pairs** table displays 'Failted:Reason'.

NOTE

If the initiator or target port is part of a logical switch and you move it to another logical switch, the end-to-end monitor fails.

Once you have created the end-to-end monitored pair, you can view both real-time and historical performance data. For step-by-step instructions refer to "Displaying end-to-end monitor pairs in a real-time graph" on page 773 or "Displaying end-to-end monitor pairs in a historical graph" on page 773.

Displaying end-to-end monitor pairs in a real-time graph

To display an end-to-end monitor pair in a graph, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors.**

   The **Set End-to-End Monitor** dialog box displays.

2. Select one or more end-to-end monitor pairs you want to view from the **Monitored Pairs** table.

   You can select up to 32 monitored pairs.

3. Click **Real-Time Graph.**

   The **Real Time Performance Graphs** dialog box displays.

Displaying end-to-end monitor pairs in a historical graph

To display monitored pairs in a historical graph, data collection must be enabled for the selected fabric or enabled SAN wide.

To display an end-to-end monitor pair in a graph, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors.**

   The **Set End-to-End Monitor** dialog box displays.

2. Select one or more end-to-end monitor pairs you want to view from the **Monitored Pairs** table.

   You can select up to 100 monitored pairs.

3. Click **Historical Graph.**

   The **Historical Performance Graph** dialog box displays.

Refreshing end-to-end monitor pairs

The Management application enables you to rewrite the end-to-end monitors (deleted through CLI or an Element Manager) back to a device.

To refresh all end-to-end monitor pairs, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors.**

   The **Set End-to-End Monitor** dialog box displays.

2. Click **Refresh.**

   All end-to-end monitor pairs are rewritten back to any devices where the end-to-end monitor pairs were deleted through CLI or an Element Manager.

3. Click **OK.**

Deleting an end-to-end monitor pair

To delete an end-to-end monitor pair, complete the following steps.

1. Select **Monitor > Performance > End-to-End Monitors.**

   The **Set End-to-End Monitor** dialog box displays.

2. Select the end-to-end monitor pair you want to delete from the **Monitored Pairs** table.
3. Click **Delete Monitor**.
4. Click **OK**.

SAN Top Talker monitoring

NOTE
Top Talkers requires the Advance Performance Monitoring (APM) license on the device.

NOTE
Top Talkers requires Fabric OS version 6.2 or later.

NOTE
On the 8 Gbps 8-FC port, 10 GbE 24-CEE port Switch, Top Talkers is only supported on the 8 Gbps FC Ports.

Advanced Performance Monitoring enables you to create Top Talker monitors on selected devices. Use Top Talkers to display the connections which are using the most bandwidth on the selected device or port. Top Talkers can be enabled on the device or one of the F_ports on the device. You can only use Top Talkers to view real-time performance data. Data is only collected while the **Top Talkers** dialog box is open; it is not persisted in the database.

You can have multiple Top Talker monitors configured at the same time. You can monitor up to 10 switches for Fabric mode Top Talkers and 32 ports and 10 switches for F_Port Top Talkers; however, you can only monitor one device or port for each Top Talker you configure.

NOTE
If the Fabric OS device is configured for Fibre Channel routing (FCR), you can only configure a Top Talker monitor on the following devices:
- 16 Gbps Backbone Chassis with a FC 16 Gbps 32-port or 48-port blade
- 16 Gbps 48-port switch

Configuring a fabric mode Top Talker monitor

NOTE
A fabric mode Top Talker and an end-to-end monitor cannot be configured on the same fabric. You must delete the end-to-end monitor before you configure the fabric mode Top Talker.

NOTE
A fabric mode Top Talker and an F_port mode Top Talker cannot be configured on the same fabric. You must delete the F_port mode Top Talker before you configure the fabric mode Top Talker.

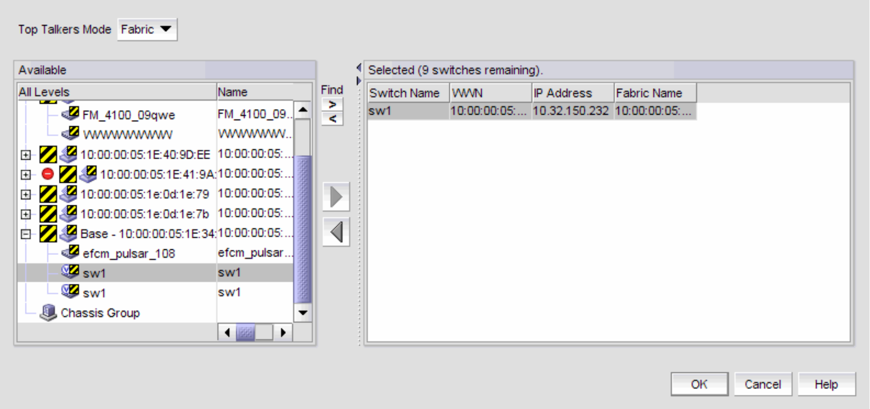
To configure a fabric mode Top Talker monitor, complete the following steps.

1. Select the device or fabric on which you want to monitor Top Talker data.

   NOTE
   On the 8 Gbps 8-FC port, 10 GbE 24-CEE port Switch, Top Talkers is only supported on the 8 Gbps FC Ports.

2. Select **Monitor** > **Performance** > **Top Talkers.**

   The **Top talker Selector** dialog box displays.



Top Talkers Mode: Fabric

Available

All Levels	Name
FM_4100_09qwe	FM_4100_09...
WWWWWWWWW	WWWWWW...
10:00:00:05:1E:40:9D:EE	10:00:00:05:...
10:00:00:05:1E:41:9A:	10:00:00:05:...
10:00:00:05:1e:0d:1e:79	10:00:00:05:...
10:00:00:05:1e:0d:1e:7b	10:00:00:05:...
Base - 10:00:00:05:1E:34:	10:00:00:05:...
efcm_pulsar_108	efcm_pulsar...
sw1	sw1
sw1	sw1
Chassis Group	

Selected (9 switches remaining).

Switch Name	WWN	IP Address	Fabric Name
sw1	10:00:00:05:...	10.32.150.232	10:00:00:05:...

FIGURE 333 Top talker Selector dialog box

3. Select **Fabric** to select a switch to monitor in the **Top Talker Mode** list.

   You can only select one device on which to enable Top Talker.

4. Click **OK** on the **Top talker Selector** dialog box.

   Top Talker is enabled on the selected device. The **Top Talkers - Fabric Mode for** *Device_Name* dialog box displays.

   The **Top Talkers - Fabric Mode for** *Device_Name* dialog box displays.

5. Select the number of Top Talkers (1 through 20) to display from the **Display** list.

6. Select how often you want the Top Talker to refresh (10, 20, 30, 40, or 50 seconds, or 1 minute) from the **Refresh Interval** list.

7. Click **Apply**.

   The top 20 conversations display in the **Current Top Talkers** table. The **Top Talkers Summary** table displays all Top Talkers that occurred since the **Top Talkers** dialog box was opened (displays a maximum of 360). When the maximum is reached, the oldest Top Talker drops as a new one occurs.

   The fabric mode Top Talker provides the following details:

   - Tx+Rx Ave (MB/sec)
   - Occurrences
   - Source
   - Source Switch/Port
   - Destination
   - Destination Switch/Port
   - Last Occurred
   - SID
   - Source Port
   - DID
   - Destination Port

8. Click **Destination** to launch the Port Properties dialog box for the Destination port.
9. Click **Source** to to launch the Port Properties dialog box for the Source port.
10. Click the minimize button to hide this dialog box when it is not needed.

Configuring an F_port mode Top Talker monitor

NOTE
An F_port mode Top Talker and an end-to-end monitor cannot be configured on the same F_port. You must delete the end-to-end monitor before you configure the F_port mode Top Talker.

NOTE
An F_port mode Top Talker and a fabric mode Top Talker cannot be configured on the same fabric. You must delete the fabric mode Top Talker before you configure the F_port mode Top Talker.

To configure an F_port mode Top Talker monitor, complete the following steps.

1. Select the port on which you want to monitor Top Talker data.
2. Select **Monitor > Performance > Top Talkers**.

   The **Top Talkers - F Port Mode for** *F_Port* dialog box displays.
3. Click **Select**.

   The **Top talker Selector** dialog box displays.
4. Select **F Port** to select the F_port to monitor in the **Top Talker Mode** list.

   You can only select one F_port on which to enable the Top Talker monitor.
5. Click **OK** on the **Top Talker Selector** dialog box.

   Top Talker is enabled on the selected port.
6. Select the number of Top Talkers (1 through 20) to display from the **Display** list.
7. Select how often you want the Top Talker to refresh (10, 20, 30, 40, or 50 seconds, or 1 minute) from the **Refresh Interval** list.

8. Select whether you want to monitor the receive (Rx) flow or the transmit (Tx) flow for the port from the **Flow** list.
9. Click **Apply**.

   The top 20 conversations display in the **Current Top Talkers** table. The **Top Talkers Summary** table displays all Top Talkers that occurred since the **Top Talkers** dialog box was opened (displays a maximum of 360). When the maximum is reached, the oldest Top Talker drops as a new one occurs.
   The F_port mode Top Talker provides the following details:

   - Rx Ave (MB/sec) or Tx Ave (MB/sec)
   - Occurrences
   - Source
   - Source Switch/Port
   - Destination
   - Destination Switch/Port
   - % Utilization
   - Last Occurred
   - SID
   - Source Port
   - DID
   - Destination Port
   - Port Speed

10. Click the minimize button to hide this dialog box when it is not needed.

Deleting a Top Talker monitor

To delete a Top Talker monitor, complete the following steps.

1. Select the dialog box of the Top Talker monitor you want to delete.
2. Click **Close**.
3. Click **Yes** on the ‘do you want to delete this monitor’ message.

Pausing a Top Talker monitor

To pause a Top Talker monitor, complete the following steps.

1. Select the dialog box of the Top Talker monitor you want to pause.
2. Click **Pause**.

Restarting a Top Talker monitor

To restart a Top Talker monitor, complete the following steps.

1. Select the dialog box of the Top Talker monitor you want to restart.
2. Click **Continue**.

Bottleneck detection

A *bottleneck* is a port in the fabric where frames cannot get through as fast as they should. In other words, a bottleneck is a port where the offered load is greater than the achieved egress throughput. Bottlenecks can cause undesirable degradation in throughput on various links. When a bottleneck occurs at one place, other points in the fabric can experience bottlenecks as the traffic backs up.

The bottleneck detection feature detects two types of bottlenecks:

- Latency bottleneck
- Congestion bottleneck

A *latency bottleneck* is a port where the offered load exceeds the rate at which the other end of the link can continuously accept traffic, but does not exceed the physical capacity of the link. This condition can be caused by a device attached to the fabric that is slow to process received frames and send back credit returns. A latency bottleneck due to such a device can spread through the fabric and can slow down unrelated flows that share links with the slow flow.

A *congestion bottleneck* is a port that is unable to transmit frames at the offered rate because the offered rate is greater than the physical data rate of the line. For example, this condition can be caused by trying to transfer data at 8 Gbps over a 4 Gbps ISL.

You can set alert thresholds for the severity and duration of the bottleneck.

If a bottleneck is reported, you can then investigate and optimize the resource allocation for the fabric. Using the zone setup and Top Talkers, you can also determine which flows are destined to any affected F_Ports.

You configure bottleneck detection on a per-fabric or per-switch basis, with per-port exclusions.

NOTE
Bottleneck detection is disabled by default. Best practice is to enable bottleneck detection on all switches in the fabric, and leave it on to continuously gather statistics.

Supported configurations for bottleneck detection

Note the following configuration rules for bottleneck detection:

- The switch must be running Fabric OS 6.4.0 or later.
- Bottleneck detection is supported on Fibre Channel ports and FCoE F_Ports.
- Bottleneck detection is supported on the following port types:
  - E_Ports
  - EX_Ports
  - F_Ports
  - FL_Ports
- F_Port and E_Port trunks are supported.
- Long distance E_Ports are supported.
- FCoE F_Ports are supported.

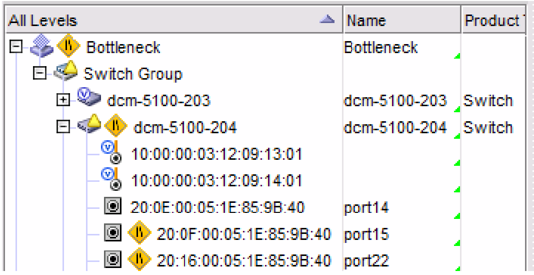
- Bottleneck detection is supported on 4 Gbps, 8 Gbps, and 16 Gbps platforms.
- Bottleneck detection is supported in Access Gateway mode.
- Bottleneck detection is supported whether Virtual Fabrics is enabled or disabled. In VF mode, bottleneck detection is supported on all fabrics, including the base fabric.

How bottlenecks are reported

Bottlenecks are reported through alerts in the Master Log. A bottleneck cleared alert is sent when the bottleneck is cleared.

NOTE
A bottleneck cleared alert is sent if you disable bottleneck detection on a bottlenecked port, even though the port is still bottlenecked.

Bottlenecks can be highlighted in the Connectivity Map and Product List. Select **Monitor > Performance > View Bottlenecks**. If a port is experiencing a bottleneck, a bottleneck icon is displayed in the Connectivity Map for the switch and fabric, and in the Product List for the port, switch, and fabric, as shown in Figure 334. In the figure, port15 and port22 are bottlenecked.



All Levels	Name	Product
Bottleneck	Bottleneck	
Switch Group		
dcm-5100-203	dcm-5100-203	Switch
dcm-5100-204	dcm-5100-204	Switch
10:00:00:03:12:09:13:01		
10:00:00:03:12:09:14:01		
20:0E:00:05:1E:85:9B:40	port14	
20:0F:00:05:1E:85:9B:40	port15	
20:16:00:05:1E:85:9B:40	port22	

FIGURE 334 Bottleneck port indications

Limitations of bottleneck detection

Using this feature for latency bottleneck detection is not recommended for link utilizations above 85%.

The bottleneck detection feature detects latency bottlenecks only at the point of egress, not ingress. For example, for E_Ports, only the traffic egressing the port is monitored. For FCoE ports, bottleneck detection monitors traffic going from the FC side to the CEE side, and does not monitor traffic going in the reverse direction.

Enabling bottleneck detection

Bottleneck detection is enabled on a switch or fabric basis.

- If you enable bottleneck detection on a fabric, the feature is applied to all eligible switches in the fabric and all eligible ports on the switches.
- If you enable bottleneck detection on a switch, the feature is applied to all eligible ports on that switch.

If ineligible ports later become eligible or, in the case of a logical switch, if ports are moved to the logical switch, bottleneck detection is automatically applied to those ports.

If you add additional switches, including logical switches, to the fabric, bottleneck detection is not automatically applied, so be sure to enable bottleneck detection on those switches as well.

NOTE
It is recommended that you enable bottleneck detection on every switch in the fabric.

Enabling bottleneck detection enables both latency and congestion detection.

When you enable bottleneck detection, you also determine whether alerts are to be sent when the bottleneck conditions at a port exceed a specified threshold. These alert parameters apply to all ports in the switch, unless you override them later.

1. Select Monitor > Performance > Bottlenecks.

   The Bottlenecks dialog box displays.

2. Select Enable if it is not already selected.
3. (*Optional*) Select the Alerts check box to enable alerts.
4. (*Optional*) Enter values for the alert settings, or use the default values.

   NOTE
   Best practice is to enable alerts and use the default values:
   Congestion80%
   Latency10%
   Window300 seconds
   Quiet Time300 seconds
   If you change the Window value, you should use a setting that is 300 seconds or higher.

5. Select one or more fabrics, switches, or ports from the Products/Ports list.

   You can select fabrics or switches or ports, but you cannot select a mix of fabrics, switches, and ports.

6. Click the right arrow to apply the settings in the Bottleneck Detection pane to the selected elements in the Products/Ports list.

   If you selected one or more ports, and bottleneck detection is disabled on the switch, you are prompted to enable bottleneck detection on the entire switch. You cannot enable a single port unless you had specifically disabled it previously.

7. Click OK or Apply to save your changes.

Configuring bottleneck alert parameters

After you enable bottleneck detection, you can change the alert parameters on all eligible ports, switches, and fabrics.

The alert parameters include whether alerts are sent and the threshold, time, and quiet time options.

NOTE

Best practice is to enable alerts and use the default values:

Congestion	80%
Latency	10%
Window	300 seconds
Quiet Time	300 seconds

If you change the Window value, you should use a setting that is 300 seconds or higher.

If you change the alert parameters for a port, you can later cancel these settings and inherit the settings from the switch. See "Inheriting alert parameters from a switch" on page 782 for instructions.

1. Select **Monitor** > **Performance** > **Bottlenecks.**

   The **Bottlenecks** dialog box displays.

2. Select **Enable** if it is not already selected.
3. Select the **Alerts** check box to enable alerts. Clear this check box to disable alerts.
4. If you enabled alerts, enter values for the alert settings, or use the default values.
5. Select one or more fabrics, switches, or ports from the Products/Ports list.

   You can select fabrics or switches or ports, but you cannot select a mix of fabrics, switches, and ports.

6. Click the right arrow to apply the settings in the Bottleneck Detection pane to the selected elements in the Products/Ports list.

   If you selected one or more ports, a right arrow displays in the Direct Assigned column for these ports, indicating that the alert parameters for the ports override the alert parameters for the switch.

   If you selected switches or fabrics, the alert parameters are changed for all of the eligible ports in those switches and fabrics except for the ports that had been directly assigned alert parameters previously.

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

Inheriting alert parameters from a switch

When you enable bottleneck detection on a switch, all eligible ports on that switch inherit the same bottleneck parameters as the switch. You can then change the parameters for specific ports or exclude specific ports from bottleneck detection.

Use the following procedure if you want to restore the switch bottleneck parameters to a port that has direct assigned settings.

1. Select Monitor > Performance > Bottlenecks.

   The Bottlenecks dialog box displays.

2. Select a port that has directly assigned bottleneck settings, which is indicated by a right arrow in the Direct Assigned column.
3. Click Inherit From Switch.
4. Select the Alerts check box to enable alerts. Clear this check box to disable alerts.

   The bottleneck parameters that are specified for the switch are applied to the port.

5. Click OK or Apply to save your changes.

Copying alert parameters from one switch or port to another

1. Select Monitor > Performance > Bottlenecks.

   The Bottlenecks dialog box displays.

2. Select the switch or port from which you want to copy the bottleneck parameters.
3. Click the left arrow.

   The parameters display in the Bottleneck Detection pane.

4. Select one or more switches, ports, or fabrics to which you want to copy the bottleneck parameters.

   You can select fabrics or switches or ports, but you cannot select a mix of fabrics, switches, and ports.

5. Click the right arrow.

   The bottleneck parameters are applied to the selected items.

6. Click OK or Apply to save your changes.

Displaying bottleneck statistics

You can display a graph of bottleneck statistics for up to 32 ports at one time.

You can display a graph showing the history of bottleneck conditions, for up to the last 150 minutes.

1. Select **Monitor > Performance > Bottleneck Graph**.

   The **Bottleneck Graph Port Selector** dialog box displays with bottlenecked ports shown in the Available list.

2. (*Optional*) Select **All Ports** from the Show list to display all ports in the Available list.

3. Select one or more ports for which you want to display bottleneck statistics and click the right arrow to move them to the Selected list.

   You can select up to 32 ports.

4. Click **OK**.

   The **Bottleneck Graph** dialog box displays, showing bottleneck statistics for the selected ports. This dialog box has several options for displaying the data:

   - Change the display interval and the display range.

     The display range cannot exceed the 30 times the display interval. Note that the display interval is in seconds and the display range is in minutes. So if the display interval is 10 (seconds), the display range cannot be greater than (5 minutes). (10 seconds X 30 = 300 seconds = 5 minutes)

   - Click **Refresh** to update the displayed data with fresh data.

     If you change the display interval or display range, you must click **Refresh** for the changes to take effect.

   - Display realtime and historical performance graphs.
   - Select a bottlenecked F_ or FL_Port and click **Show Affected Hosts** to see the hosts that might be affected by the bottleneck.

Displaying hosts that could be affected by an F_ or FL_Port bottleneck

The following procedure displays hosts that could be affected because of a bottlenecked F_ or FL_Port. These hosts are determined based on zoning information and are not based on actual traffic flow.

Affected hosts cannot be determined for bottlenecked E_Ports.

1. Select **Monitor > Performance > Bottlenecks.**

   The Bottlenecks dialog box displays.

2. In the Current Settings list, select a bottlenecked port (a port with “Bottlenecked” in the Bottleneck Status column).

3. Click **Show Affected Hosts**.

   The Bottleneck Affected Hosts dialog box displays.

4. Select a port in the Bottleneck Ports list to display the affected hosts in Hosts Affected by Bottlenecks list.

Disabling bottleneck detection

Use this procedure to exclude specific ports from bottleneck detection or to disable bottleneck detection on entire switches or fabrics.

It is not recommended to disable bottleneck detection on a port except under special circumstances. For example, if a long-distance port is known to be a bottleneck because of credit insufficiency, you could disable bottleneck detection on that port.

1. Select **Monitor > Performance > Bottlenecks**.

   The **Bottlenecks** dialog box displays.

2. Select **Disable**.

3. Select one or more fabrics, switches, or ports from the Products/Ports list.

   You can select fabrics or switches or ports, but you cannot select a mix of fabrics, switches, and ports.

4. Click the right arrow to apply the settings in the Bottleneck Detection pane to the selected elements in the Products/Ports list.

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

Thresholds and event notification

Performance allows you to apply thresholds and event notification to real-time performance data. A performance monitor process (thread) monitors the performance data against the threshold setting for each port and issues an appropriate alert to notify you when the threshold is exceeded. For information about configuring event notification, refer to *Event Notification*.

NOTE
It is not necessary to configure event notification to receive events in the master log. If the threshold is exceeded for a threshold, an event is automatically generated and displayed in the master log.

Creating a threshold policy

NOTE
If you set the threshold for a particular critical event to 100%, by the time you are notified, it may be too late to prevent a failure. However, when you set the threshold to 85%, for example, you may be able to prevent the failure from occurring.

Example

The values at 1 second, 3 seconds, and 5 seconds generate events because they exceed boundaries. The value at 2 seconds does not generate an event because, although it crosses the boundary, it remains in the buffer zone. The value at 6 seconds generates an event because it crosses the lower boundary and returns to a value beyond the buffer zone.

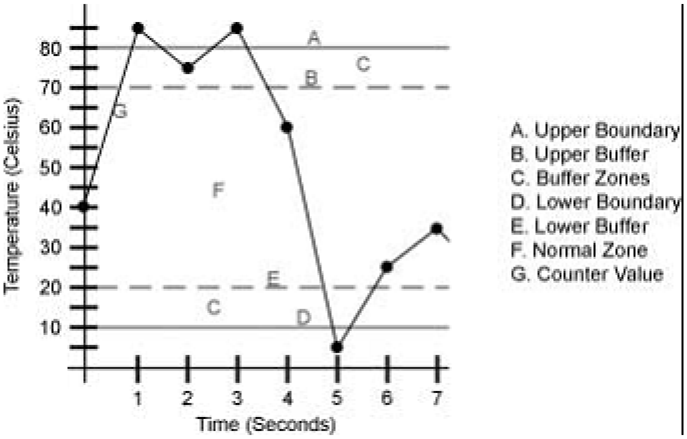
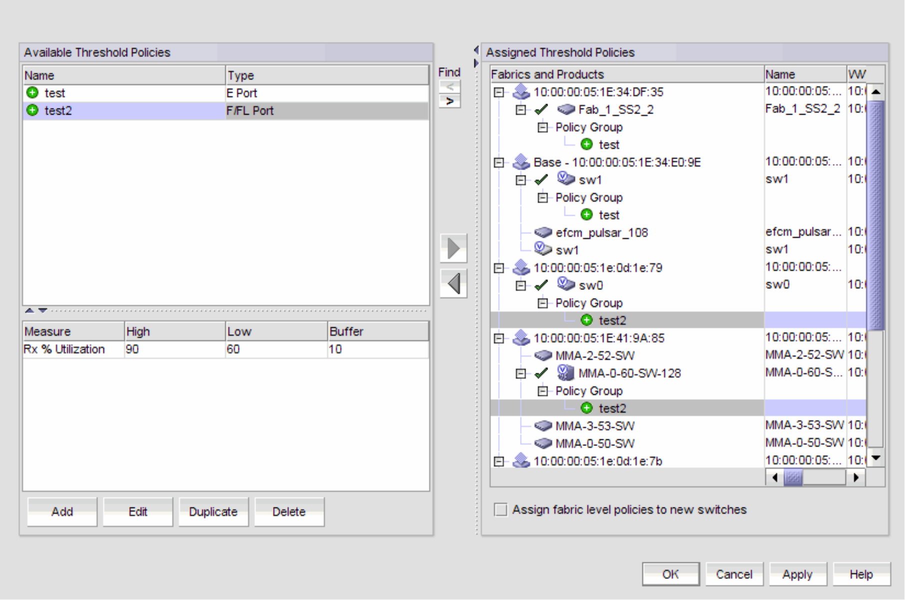


FIGURE 335 Threshold example

To create a threshold policy, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds**.

   The **Set Threshold Policies** dialog box displays.



Available Threshold Policies

Name	Type
test	E Port
test2	F/FL Port

Measure	High	Low	Buffer
Rx % Utilization	90	60	10

Assigned Threshold Policies

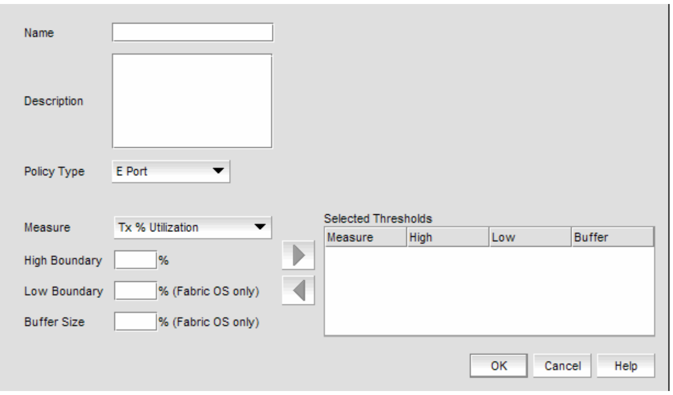
Fabrics and Products	Name	WW
10:00:00:05:1E:34:DF:35	10:00:00:05:...	10:
✓ Fab_1_SS2_2	Fab_1_SS2_2	10:
Policy Group		
test		
Base - 10:00:00:05:1E:34:E0:9E	10:00:00:05:...	10:
✓ sw1	sw1	10:
Policy Group		
test		
efcm_pulsar_108	efcm_pulsar...	10:
sw1	sw1	10:
10:00:00:05:1e:0d:1e:79	10:00:00:05:...	
✓ sw0	sw0	10:
Policy Group		
test2		
10:00:00:05:1E:41:9A:85	10:00:00:05:...	10:
MMA-2-52-SW	MMA-2-52-SW	10:
✓ MMA-0-60-SW-128	MMA-0-60-S...	10:
Policy Group		
test2		
MMA-3-53-SW	MMA-3-53-SW	10:
MMA-0-50-SW	MMA-0-50-SW	10:
10:00:00:05:1e:0d:1e:7b	10:00:00:05:...	10:

□ Assign fabric level policies to new switches

FIGURE 336 Set Threshold Policies dialog box

2. Click **Add**.

   The **New Threshold Policy** dialog box displays.



Name

Description

Policy Type: E Port

Measure: Tx % Utilization

High Boundary %

Low Boundary % (Fabric OS only)

Buffer Size % (Fabric OS only)

Selected Thresholds

Measure	High	Low	Buffer

FIGURE 337 New Threshold Policy dialog box

3. Enter a name for the policy (100 characters maximum) in the **Name** field.

4. Select a policy type from the **Policy Type** list.

   You can only define policies for E and F/FL ports.

5. Select a measure from the **Measure** list.

   You can only define policies for the Tx and Rx % Utilization measures. You cannot add the same measure more than once. If you try to add another threshold with the same measure, the new values overwrite the older threshold values in the **Selected Thresholds** table.

6. Enter a percentage for the high boundary in the **High Boundary** field.

   When the counter value exceeds high boundary, an event is raised.

7. (Fabric OS only) Enter a percentage for the low boundary in the **Low Boundary** field.

   When the counter value goes below the low boundary an event is raised.

8. (Fabric OS only) Enter a percentage for the buffer in the **Buffer Size** field.

   Counters may fluctuate around the upper or lower boundary of a range threshold, and as a result cause numerous events in a short period of time. To reduce the number of events, configure a buffer (a range of values just below the upper boundary and just above the lower boundary) in which a counter does not register an event if it returns to a "normal" value. An event only registers if the counter returns to a "normal" value beyond the buffer.

9. Click the right arrow button to move the threshold to the **Selected Thresholds** table.

   If an error is detected, a message displays informing you to enter a valid value. Click **OK** to close this message. Fix any errors and repeat step 9.

10. Repeat steps 5 through 9 for each measure that you want to add to the policy.

11. Click **OK** on the **New Threshold Policy** dialog box.

    The threshold policy displays in the **Available Threshold Policies** table with an added icon (⊕). To assign a threshold policy to a fabric or device, refer to "Assigning a threshold policy" on page 790.

12. Click **OK** on the **Set Threshold Policies** dialog box.

    The **Confirm Threshold Changes** dialog box displays.

13. Make the threshold changes by selecting one of the following options:

    - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
    - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.

14. Click **OK** on the **Confirm Threshold Changes** dialog box.

Editing a threshold policy

To edit a threshold policy, complete the following steps.

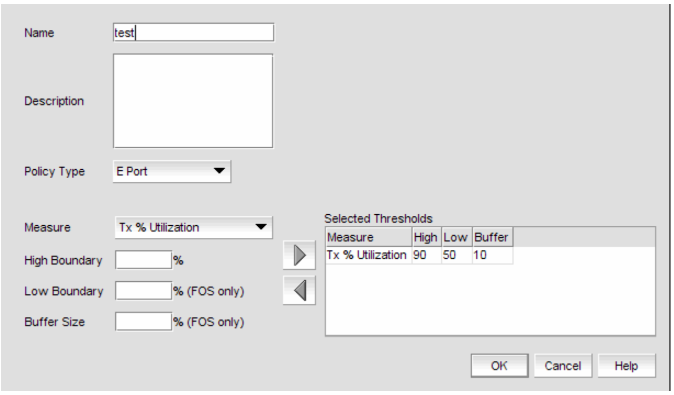
1. Select **Monitor > Performance > Configure Thresholds**.

   The **Set Threshold Policies** dialog box displays.

2. Select the threshold policy you want to edit in the **Available Threshold Policies** table.

3. Click **Edit**.

   The **Edit Threshold Policy** dialog box displays.



Name: test

Description:

Policy Type: E Port

Measure: Tx % Utilization

High Boundary: %

Low Boundary: % (FOS only)

Buffer Size: % (FOS only)

Selected Thresholds

Measure	High	Low	Buffer
Tx % Utilization	90	50	10

FIGURE 338 Edit Threshold Policy dialog box

4. Change the policy type from the **Policy Type** list.

5. Select a measure from the **Measure** list.

   You cannot add the same measure more than once. If you try to add another threshold with the same measure, the new values overwrite the older threshold values in the **Selected Thresholds** table.

6. Enter a percentage for the high boundary in the **High Boundary** field.

7. (Fabric OS only) Enter a percentage for the low boundary in the **Low Boundary** field.

8. (Fabric OS only) Enter a percentage for the buffer in the **Buffer Size** field.

9. Click the right arrow button to move the threshold to the **Selected Thresholds** table.

   If an error is detected, a message displays informing you to enter a valid value. Click **OK** to close this message. Fix any errors and repeat step 9.

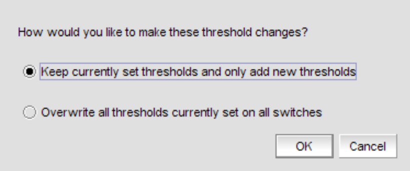
10. Repeat steps 5 through 9 for each measure that you want to add to the policy.

11. Click **OK** on the **Edit Threshold Policy** dialog box.

    The threshold policy displays in the **Available Threshold Policies** table with a modified icon (◉). To assign a threshold policy to a fabric or device, refer to “Assigning a threshold policy” on page 790.

12. Click **OK** on the **Set Threshold Policies** dialog box.

    The **Confirm Threshold Changes** dialog box displays.



How would you like to make these threshold changes?

● Keep currently set thresholds and only add new thresholds

○ Overwrite all thresholds currently set on all switches

FIGURE 339 Confirm Threshold Changes dialog box

13. Make the threshold changes by selecting one of the following options:

    - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
    - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.

14. Click **OK** on the **Confirm Threshold Changes** dialog box.

Duplicating a threshold policy

To duplicate a threshold policy, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds.**

   The **Set Threshold Policies** dialog box displays.

2. Select the threshold policy you want to copy in the **Available Threshold Policies** table.

3. Click **Duplicate.**

   The threshold policy displays in the **Available Threshold Policies** table with an added icon (⊕) using the following naming format copy of *Threshold_Name*. To edit the threshold, refer to "Editing a threshold policy" on page 788. To assign a threshold policy to a fabric or device, refer to "Assigning a threshold policy" on page 790.

4. Click **OK** on the **Set Threshold Policies** dialog box.

   The **Confirm Threshold Changes** dialog box displays.

5. Make the threshold changes by selecting one of the following options:

   - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
   - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.

6. Click **OK** on the **Confirm Threshold Changes** dialog box.

Assigning a threshold policy

To assign a threshold policy to a fabric or device, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds**.

   The **Set Threshold Policies** dialog box displays.

2. Select one or more threshold policies you want to assign to a fabric or device in the **Available Threshold Policies** table.

   Press **Ctrl** or **Shift** and then click to select multiple policies.

3. Select one or more fabrics or devices to which you want to assign the policy in the **Available Threshold Policies** table.

   If you choose to assign the policy to a fabric and a M-EOS logical switch is present in the fabric, the policy is not assigned to the M-EOS logical switch. You must directly assign a policy to a M-EOS physical chassis.

   When you directly assign a policy to a M-EOS physical chassis, the policy is assigned to all logical switches in the physical chassis.

   Press **Ctrl** or **Shift** and then click to select multiple fabrics or devices.

4. Click the right arrow button to apply the selected policies to the selected fabrics and devices.

   If any of the selected devices do not have a Fabric Watch license, the threshold policies are not set on the device and a message displays listing the affected devices. You will need to upgrade the Fabric Watch license and then assign threshold policies to these devices. Click **OK** to close the message.

5. Click **OK** on the **Set Threshold Policies** dialog box.

   The **Confirm Threshold Changes** dialog box displays.

6. Make the threshold changes by selecting one of the following options:

   - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
   - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.

7. Click **OK** on the **Confirm Threshold Changes** dialog box.

Deleting a threshold policy

To delete a threshold policy, complete the following steps.

1. Select **Monitor > Performance > Configure Thresholds.**

   The **Set Threshold Policies** dialog box displays.

2. Select the threshold policy you want to delete in the **Available Threshold Policies** table.

   When you delete a policy from the M-EOS physical chassis, the policy is deleted from all logical switches in the physical chassis.

3. Click **Delete.**

   The threshold policy displays in the **Available Threshold Policies** table with a removed icon (⊖).

4. Click **Yes** on the confirmation message.
5. Click **OK** on the **Set Threshold Policies** dialog box.

   The **Confirm Threshold Changes** dialog box displays.
6. Make the threshold changes by selecting one of the following options:
   - To only add new thresholds, select the **Keep currently set thresholds and only add new thresholds** check box.
   - To overwrite all existing thresholds on all fabrics and devices, select the **Overwrite all thresholds currently set on all switches** check box.
7. Click **OK** on the **Confirm Threshold Changes** dialog box.

SAN Connection utilization

NOTE
Connection utilization is only supported on the following managed objects: E_ports, F_ports, N_ports, 10 GE_ports and FCIP tunnels.

Performance connection utilization for device ports provides the following features:

- Turns the utilization display on and off from the menu and tool bar.
- Displays moving dotted colored lines that originate from a port.
- Displays two lines in the topology (when turned on); one represents percentage utilization for transmit and the other percentage utilization for receive. The movement of the line determines if it is a transmit or a receive.
  - Receive (Rx)—line moves into a port.
  - Transmit (Tx)—line moves out of a port.
- Displays different colors to represent the percentage utilization range (Figure 340).

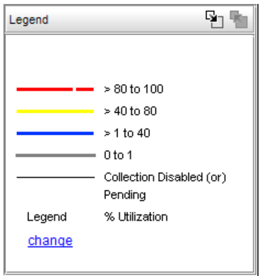


FIGURE 340 Utilization Legend

The colors and their meanings are outlined in the following table.

Line Color	Utilization Defaults
Red line	80% to 100% utilization
Yellow line	40% to 80% utilization
Blue line	1% to 40% utilization
Gray line	0% to 1% utilization
Black line	Utilization disabled

Enabling connection utilization

NOTE
Fabrics where performance data collection is not enabled display connections as thin black lines.

To display the connection utilization, complete the following steps.

1. Choose from one of the following options:
   - Select **Monitor** > **Performance** > **View Utilization**
   - Press CTRL + U.
   - Click the Utilization icon ( ).

   If you have already enabled historical data collection, the Utilization Legend displays in the main interface window.

   If you have not already enabled historical data collection, a message appears informing you that you must enable historical data collection before you can view utilization.

2. Choose one of the following options:
   - Select **Enable SAN Wide** to enable data collection for the entire SAN.
   - Select **Enable Selected Fabrics** to enable data collection for specific fabrics.

     The Historical Data Collection dialog box displays. To select the fabrics on which you want to enable data collection, refer to “Enabling historical performance collection for selected fabrics” on page 765.

     If you click **Close** on the Historical Data Collection message, Historical Data Collection is not enabled; however, the Utilization Legend still displays in the main window.

   There is a 5 minute delay to start displaying values.

Disabling connection utilization

NOTE
Fabrics where performance data collection is not enabled display connections as thin black lines.

To turn off the connection utilization, choose one of the following options:

- Select **Monitor** > **Performance** > **View Utilization** (or CTRL + U).
- Press CTRL + U.
- Click the Utilization icon ( ).

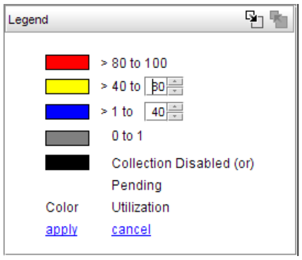
  The Utilization Legend is removed from the main interface window.

Changing connection utilization

You can change the utilization percentages.

To change the utilization percentages, complete the following steps.

1. Click the **change** link in the utilization legend.



Legend

🟥 > 80 to 100
🟨 > 40 to 80
🟦 > 1 to 40
▨ 0 to 1
⬛ Collection Disabled (or) Pending

Color Utilization
apply cancel

FIGURE 341 Utilization Legend in edit mode

2. Enter or select the end percentage you want for the blue line.

   When you make a change to the end percentage of a utilization line, you also change the start percentage for the utilization line immediately above the one you changed when you click **apply**. For example, if you change the blue line end percentage to 60 the yellow line start percentage changes to 60 when you click **apply**.

3. Enter or select the end percentage you want for the yellow line.
4. Click the **apply** link.

   The new values appear in the utilization legend.

Chapter

Frame Monitor 28

In this chapter

Frame Monitor

NOTE
Frame Monitoring is supported in Professional Plus and Enterprise Editions only.

Frame monitors count the number of frames transmitted through a port that match specific values in the first 64 bytes of the frame. Since the entire Fibre Channel frame header and many upper protocol (for example, SCSI) headers fall within the first 64 bytes of a frame, frame monitors can detect different types of traffic transmitted through a port. Each frame monitor keeps a timestamp of its last refresh. It also keeps a generation count, which is incremented each time the monitor is cleared.

Frame monitors generate alerts whenever the frame count for a certain frame type crosses the threshold configured for that frame type. You can configure high thresholds for every frame type, specify actions to be taken when the threshold is exceeded, and configure how often the data are sampled.

Virtual Fabrics considerations: You can assign frame monitors to ports in a logical switch. If a port is moved from one logical switch to another, however, all monitors that were assigned to the port are cleared in the new logical switch.

Trunking considerations: For trunked ports, the frame monitor is configured on the trunk master.

Frame types

The frame type can be a standard type (for example, a SCSI read command filter that counts the number of SCSI read commands that have been transmitted by the port) or a user-defined frame type customized for your particular use.

Pre-defined frame types

Pre-defined frame types include the following:

- ABTS (Abort Sequence Basic Link Service command)
- BA_ACC (Abort Accept)
- IP
- SCSI
- SCSI Read
- SCSI Write
- SCSI RW
- SCSI-2 Reserve
- SCSI-3 Reserve

Custom frame types

In addition to the standard frame types, you can create custom frame types to gather statistics that fit your needs. To define a custom frame type, you must specify a series of *offsets*, *bitmasks*, and *values*. For all transmitted frames, the switch performs these tasks:

- Locates the byte found in the frame at the specified *offset.*
- Applies the *bitmask* to the byte found in the frame.
- Compares the new value with the given *value*.
- Increments the filter counter if a match is found.

You can specify up to four values to compare against each offset. If more than one offset is required to properly define a filter, the bytes found at each offset must match one of the given values for the filter to increment its counter. If one or more of the given offsets does not match any of the given values, the counter does not increment. The value of the offset must be between 0 and 63, in decimal format. Byte 0 indicates the first byte of the Start of Frame (SOF), byte 4 is the first byte of the frame header, and byte 28 is the first byte of the payload. Thus only the SOF, frame header, and first 36 bytes of payload can be selected as part of a filter definition. Offset 0 is a special case, which can be used to monitor the first 4 bytes of the frame (SOF). When the offset is set to 0, the values 0–7 that are checked against that offset are predefined as shown in Table 48.

TABLE 48 Predefined values at offset 0

Value	SOF	Value	SOF
0	SOFf	4	SOFi2
1	SOFc1	5	SOFn2
2	SOFi1	6	SOFi3
3	SOFn1	7	SOFn3

Frame Monitoring requirements

To configure Frame Monitoring, the following requirements must be met:

- The switch must be running Fabric OS 7.0.0 or later.
- Frame Monitoring requires the Advanced Performance Monitoring license and the Fabric Watch license.

NOTE
The Advanced Performance Monitoring license is required to configure frame monitors. The monitoring functionality requires the Fabric Watch license.

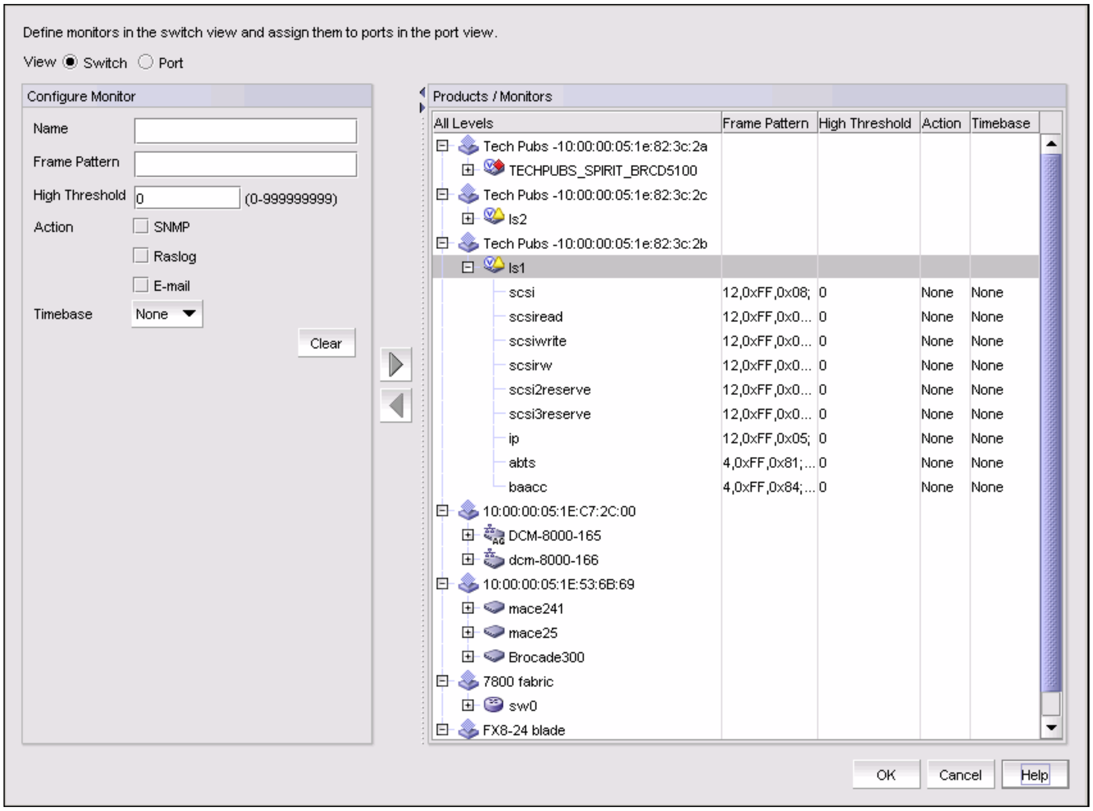
The maximum number of frame monitors and offsets per port is platform-specific. Refer to the *Fabric OS Administrator's Guide* for more information.

Creating a custom frame monitor

Pre-defined frame monitors are already installed on switches that support Frame Monitoring. Use this procedure if you want to create a custom frame monitor.

1. Select **Monitor > Fabric Watch > Frame Monitor.**

   The Frame Monitor dialog box displays (Figure 342).



Define monitors in the switch view and assign them to ports in the port view.

View ● Switch ○ Port

Configure Monitor

Name

Frame Pattern

High Threshold 0 (0-999999999)

Action ☐ SNMP ☐ Raslog ☐ E-mail

Timebase None

Products / Monitors

All Levels	Frame Pattern	High Threshold	Action	Timebase
Tech Pubs -10:00:00:05:1e:82:3c:2a				
TECHPUBS_SPIRIT_BRCD5100				
Tech Pubs -10:00:00:05:1e:82:3c:2c				
ls2				
Tech Pubs -10:00:00:05:1e:82:3c:2b				
ls1				
scsi	12,0xFF,0x08;	0	None	None
scsiread	12,0xFF,0x0...	0	None	None
scsiwrite	12,0xFF,0x0...	0	None	None
scsirw	12,0xFF,0x0...	0	None	None
scsi2reserve	12,0xFF,0x0...	0	None	None
scsi3reserve	12,0xFF,0x0...	0	None	None
ip	12,0xFF,0x05;	0	None	None
abts	4,0xFF,0x81;...	0	None	None
baacc	4,0xFF,0x84;...	0	None	None
10:00:00:05:1E:C7:2C:00				
DCM-8000-165				
dcm-8000-166				
10:00:00:05:1E:53:6B:69				
mace241				
mace25				
Brocade300				
7800 fabric				
sw0				
FX8-24 blade				

FIGURE 342 **Frame Monitor dialog box**

2. Select the **Switch** option.

   The Products / Monitors list displays the switches that support Frame Monitoring.

3. Enter the monitor data in the Configure Monitor area.

4. Select one or more switches in the Products / Monitors list, and click the right arrow button to assign the frame monitor to those switches.

5. Select the **Port** option.

6. Expand the switch in the Products / Ports list.

   The Monitors list displays all of the frame monitors defined for that switch.

7. Select one or more ports.

   You must select only ports belonging to the same switch.

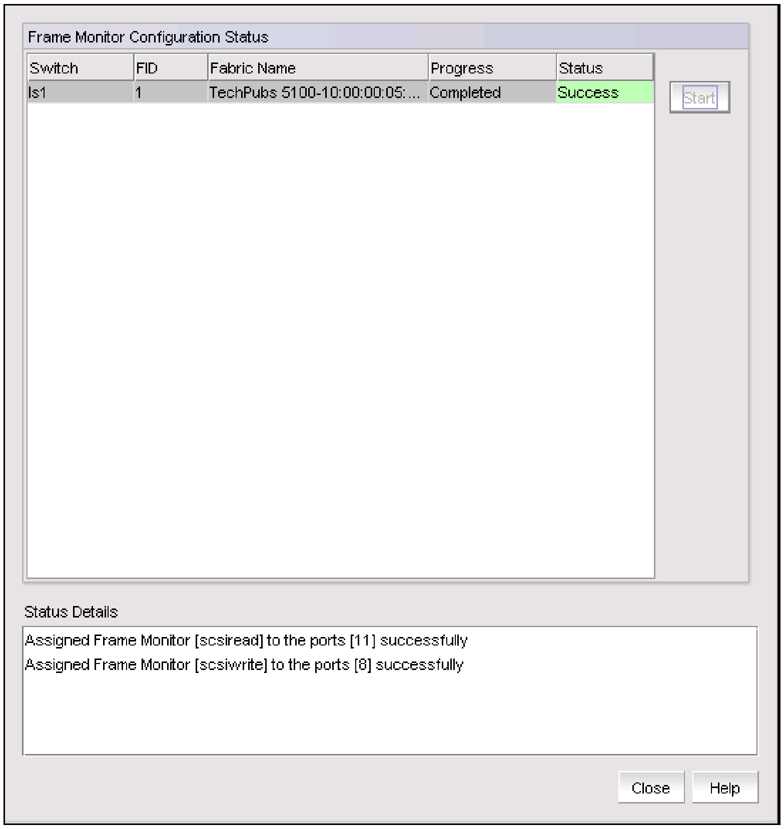
8. Select one or more frame monitors in the Monitors list.

9. Click the right arrow button to move the frame monitor to the selected ports.

   The Monitor Details list displays the monitors that are assigned to a selected port. If no monitors are assigned, or if more than one port is selected, the Monitor Details list does not display.

10. Click **OK**.

    The Frame Monitor Configuration Status dialog box displays (Figure 343).



Frame Monitor Configuration Status

Switch	FID	Fabric Name	Progress	Status
ls1	1	TechPubs 5100-10:00:00:05:...	Completed	Success

Status Details

Assigned Frame Monitor [scsiread] to the ports [11] successfully

Assigned Frame Monitor [scsiwrite] to the ports [8] successfully

FIGURE 343 Frame Monitor Configuration Status dialog box

11. Click **Start**.

    The frame monitor configuration is applied to the switches.

12. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Editing a frame monitor

1. Select **Monitor** > **Fabric Watch** > **Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Switch** option.
3. Expand the Products / Monitors list to display the frame monitors for each switch.
4. Select a frame monitor and click the left arrow button.

   The frame monitor is removed from the switch and the Configure Monitor area is populated with the values for that frame monitor.

5. Make changes to the monitor data in the Configure Monitor area.
6. Select one or more switches in the Products / Monitors list, and click the right arrow button to assign the frame monitor to those switches.

   If the frame monitor already exists on the switches, the frame monitor is modified. If the frame monitor does not exist on the switch, it is added.

7. Click **OK**.

   The Frame Monitor Configuration Status dialog box displays.

8. Click **Start**.

   The frame monitor configuration is applied to the switches and ports.

9. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Assigning a frame monitor to a port

1. Select **Monitor** > **Fabric Watch** > **Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Port** option.
3. Expand the switch in the Products / Ports list.

   The Monitors list displays all of the frame monitors defined for that switch.

4. Select one or more ports.

   You must select only ports belonging to the same switch.

5. Select one or more frame monitors in the Monitors list.

6. Click the right arrow button to move the frame monitor to the selected ports.

   The Monitor Details list displays the monitors that are assigned to a selected port. If no monitors are assigned, or if more than one port is selected, the Monitor Details list does not display.

7. Click **OK**.

   The Frame Monitor Configuration Status dialog box displays.

8. Click **Start**.

   The frame monitor configuration is applied to the ports.

9. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Finding frame monitor assignments

Using the following procedure, you can select a frame monitor on a switch and see the ports to which it is assigned.

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Port** option.
3. Select a switch in the Products / Ports list.

   The Monitors list displays all of the frame monitors defined for that switch.

4. Select a frame monitor in the Monitors list.
5. Click the **Find** arrow.

   The ports to which the frame monitor is assigned are highlighted.

Removing a frame monitor from a port

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Port** option.
3. Expand the switch in the Products / Ports list.

   The Monitors list displays all of the frame monitors defined for that switch.

4. Select the port from which you want to remove the frame monitor.

   The Monitor Details list displays all of the frame monitors assigned to that port.

5. Select one or more frame monitors in the Monitor Details list.
6. Click **Remove**.
7. Click **OK**.

   The Frame Monitor Configuration Status dialog box displays.

8. Click **Start**.

   The frame monitor configuration is applied to the ports.

9. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Removing a frame monitor from a switch

When you remove a frame monitor from a switch, the frame monitor is automatically removed from all assigned ports in the switch.

You can remove only custom frame types; you cannot remove the pre-defined frame types.

1. Select **Monitor > Fabric Watch > Frame Monitor**.

   The Frame Monitor dialog box displays.

2. Select the **Switch** option.

   The Products / Monitors list displays the switches that support Frame Monitoring.

3. Expand the Products / Monitors list to display the frame monitors for each switch.

4. Select a frame monitor and click the left arrow button.

   The frame monitor is removed from the switch and the Configure Monitor area is populated with the values for that frame monitor.

5. Click **OK**.

   The Frame Monitor Configuration Status dialog box displays.

6. Click **Start**.

   The frame monitor configuration is applied to the switches and ports.

7. Click **Close** after configuration is complete (indicated by “Completed” in the Progress column).

Chapter

Policy Monitor 29

In this chapter

Policy Monitor overview

Use this feature is to provide best practice guidelines for network setup at the fabric, switch, port and device level as well as software configurations at the Fabric OS, Network OS and the Management application level.

Configuring policy monitors enables you to perform the following:

- Provide selectable and configurable built-in rules to check for best practices
- Schedule policies to run periodically
- Run a policy manually (on demand)
- Generate a report that will detail any issues found by the policy

The following sections provide more detailed information on the policy monitor type and rules.

Fabric policy monitors

Enables you to set the following policy monitors on fabrics.

- **Check zoning status**—Enables you to determine if zoning is enabled or disabled on the fabric.

  Zoning plays a key role in the management of device communication. When you enforce zoning, devices not in the same zone cannot communicate. Zoning provides protection from disruption in the fabric (putting bounds on the scope of RSCNs). The best practice is always enabling zoning.

  Rule Violation Fix—If the report shows a violation, the SAN Administrator can use the **Zoning** dialog box (**Configure > Zoning > Fabric**) to fix the violation. Refer to **Zoning.**

  For example, if you use the policy monitor to make sure that the zoning status is enabled, you can fix the violation through the **Zoning** dialog box by locating the target fabric, defining a zone configuration, and activating the zone configuration.

- **Check that all zones belong to at least one zone config**—Enables you to determine if there are any orphaned zones in the fabric zone database.

  Too many orphaned zones can fill up zone database and complicate other ongoing administrative tasks.

  Rule Violation Fix—If the report shows a violation, the SAN Administrator can use the **Zoning** dialog box (**Configure > Zoning > Fabric**) to fix the violation. Refer to **Zoning.**

  For example, the SAN Administrator can fix the violation through the **Zoning** dialog box using one of the following methods

  - Defining new zone configuration and moving the orphaned zones to the new zone configuration.
  - Moving the orphaned zones to existing zone configuration.
  - Cleaning up unused orphaned zones.

- **Check the number of initiator ports zoned to each storage port**—Enables you to determine the total number of initiator ports zoned to each storage port.

  When too many initiators share the same connection (share the bandwidth of the storage port), congestion can occur.

  Rule Violation Fix—If the report shows a violation, the SAN Administrator must make sure the initiator port limit is under the recommended number.

SAN Switch policy monitors

Enables you to set the following policy monitors on SAN switches.

- **Check if the product is configured to send events to this server**—Enables you to determine if the Management application server is registered as an SNMP recipient and Syslog recipient.

  If the Management application server fails to register as a listener for SNMP, Syslog, and other events, the Management application server cannot notify you of changes to the fabric or device. If a fabric or switch fails, the Management application cannot provide notification, log, or support data. Therefore, you may not realize that there is an inconsistency between the physical device status and device status in the Management application for some time.

  Rule Violation Fix—If the report shows a SNMP not registered as recipient violation, the SAN Administrator can register the Managemet server as a SNMP recipient through the **SNMP Trap Recipients** dialog box (**Monitor > SNMP Setup > Product Trap Recipients**). Refer to **Fault Management.**

  If the report shows a Syslog not registered as recipient violation, the SAN Administrator can register the Managemet server as a Syslog recipient through the **Syslog Recipients** dialog box (**Monitor > Syslog Configuration > Product Syslog Recipients**). Refer to **Fault Management.**

- **Check for redundant connections to neighboring switches**—Enables you to determine if there are at least the minimum number of configured inter-switch links (ISL) between each switch pair.

  The resiliency and/or redundancy of the fabric is an important aspect of the SAN topology. To remove any single point of failure, SAN fabrics have resiliency built into the Fabric OS.

  For example, when a link between two switches fails, routing is recalculated and traffic is assigned to a new route. Therefore, to provide redundancy and enable resiliency, using ISLs, the best practice is to make sure that there are at least two ISLs between each switch pair.

  The redundant link refers to both the physical connection and logical ISL. No matter how many physical connections exist between the two base switches, there is only one logical ISL between two logical switches. A logical ISL counts as one connection between the source and destination switches; therefore, when a logical ISL is present, the connection count may be inaccurate. To pass this monitor, the total number of logical ISL and physical connections must be greater than the minimum connection.

  For FCIP tunnels, one tunnel counts as one connection. This rule does not check circuits within the FCIP tunnel. The total number of trunk ISLs, single ISLs and number of tunnels is used to compare with the minimum number setting to decide if the redundant ISL check is success or fail.

  Rule Violation Fix—If the report shows a violation, the SAN Administrator can add redundant ISLs between the source and target switch.

- **Check if the product is configured to send Upload Failure Data Capture to an FTP server**—Enables you to determine if Upload Failure Data Capture is enabled on the selected switches, that the configured FTP Server is accessible, and that you have write permission to the directory.

  Upload Failure Data Capture enables you to collect switch data periodically. This assists you to troubleshoot switch failure.

  Rule Violation Fix—If the report shows a violation, the SAN Administrator can change the Upload Failure Data Capture configuration through the **Upload Failure Data Capture** dialog box (**Monitor > Technical Support > Upload Failure Data Capture**). Refer to“Enabling upload failure data capture” on page 897.

Host policy monitors

Enables you to set the following policy monitor on Host devices.

Check for redundant connections to attached fabrics—Enables you to determine if there are at least the minimum number of configured physical connections between the host and the attached fabric.

To prevent a single point of failure, the host should have a redundant connection to the attached fabric. Available hosts include both automatic hosts and manual hosts.

Depending on how you discover the hosts, there are recommended configurations you should complete to avoid inaccuracy.

- Fabric discovery (refer to“Host port mapping overview” on page 299)

  Make sure there are Brocade HBAs on the host.

  Make sure to configure the host port mapping.
- Host adaptor discovery (refer to“Host discovery” on page 70)

  Make sure there are Brocade HBAs on the host.
- VM Manager discovery (refer to“VM Manager Discovery” on page 78)

  Make sure there are Brocade HBAs on the host.

  Make sure you discover the associated fabrics.

Rule Violation Fix—If the report shows a violation, the SAN Administrator can add a redundant host connection to the attached fabrics. Note that if a host is attached to multiple fabrics, and only some of the fabrics violate the policy, the report only lists the fabrics that failed.

Management policy monitor

Enables you to set a policy monitor on the Management application.

Check to see if the server backup is enabled and working—Enables you to determine if back up is enabled for the Management application server and if the backup output directory is accessible and writable.

Server backup automatically backs up the Management application database on a user-defined schedule.

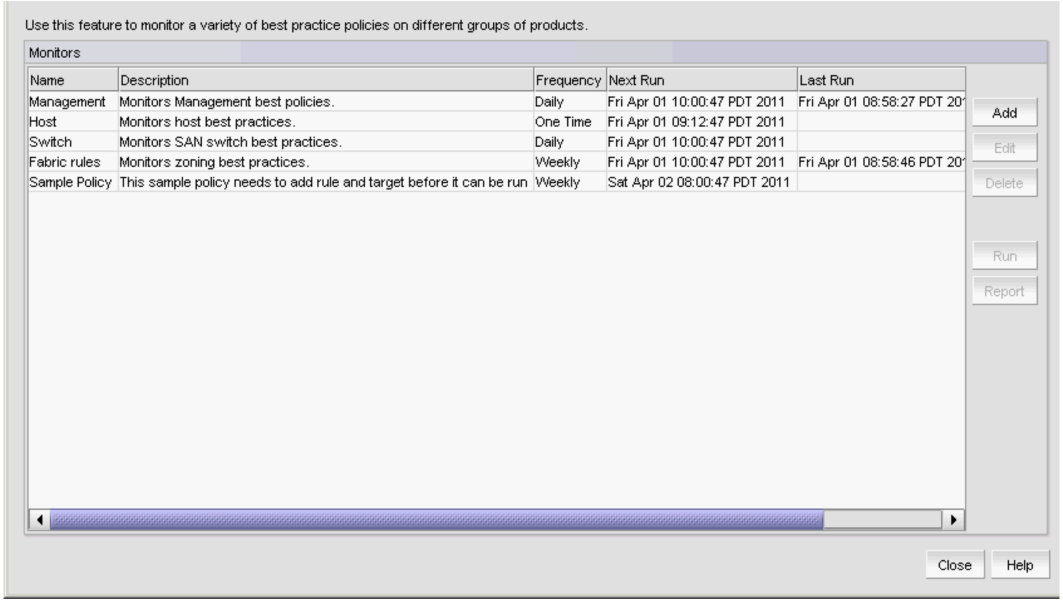
Rule Violation Fix—If the report shows a violation, the SAN Administrator can edit the backup configuration through the **Options** dialog box, **Server Backup** pane (**Server** > **Options**). Refer to "Management server backup" on page 86.

Viewing existing policy monitors

To view existing policy monitors, complete the following steps.

1. Select **Monitor** > **Policy Monitor.**

   The **Policy Monitor** dialog box displays.



Use this feature to monitor a variety of best practice policies on different groups of products.

Monitors

Name	Description	Frequency	Next Run	Last Run
Management	Monitors Management best policies.	Daily	Fri Apr 01 10:00:47 PDT 2011	Fri Apr 01 08:58:27 PDT 20
Host	Monitors host best practices.	One Time	Fri Apr 01 09:12:47 PDT 2011	
Switch	Monitors SAN switch best practices.	Daily	Fri Apr 01 10:00:47 PDT 2011	
Fabric rules	Monitors zoning best practices.	Weekly	Fri Apr 01 10:00:47 PDT 2011	Fri Apr 01 08:58:46 PDT 20
Sample Policy	This sample policy needs to add rule and target before it can be run	Weekly	Sat Apr 02 08:00:47 PDT 2011	

FIGURE 344 **Policy Monitor dialog box**

2. Review the policy monitor details:

   - **Name**—The user-defined name of the policy.
   - **Description**—A description of the policy.
   - **Frequency**—The frequency (one time, hourly, daily, weekly, or monthly) at which the policy is scheduled.

- **Next Run**—The time the policy will run again.
- **Last Run**—The time the policy ran last.
- **Result**—The result of last Policy Monitor run. There are three possible results: Success, Partially Failed, Failed, and Not Applicable.

3. Click **Close** on the **Policy Monitor** dialog box.

Adding a policy monitor

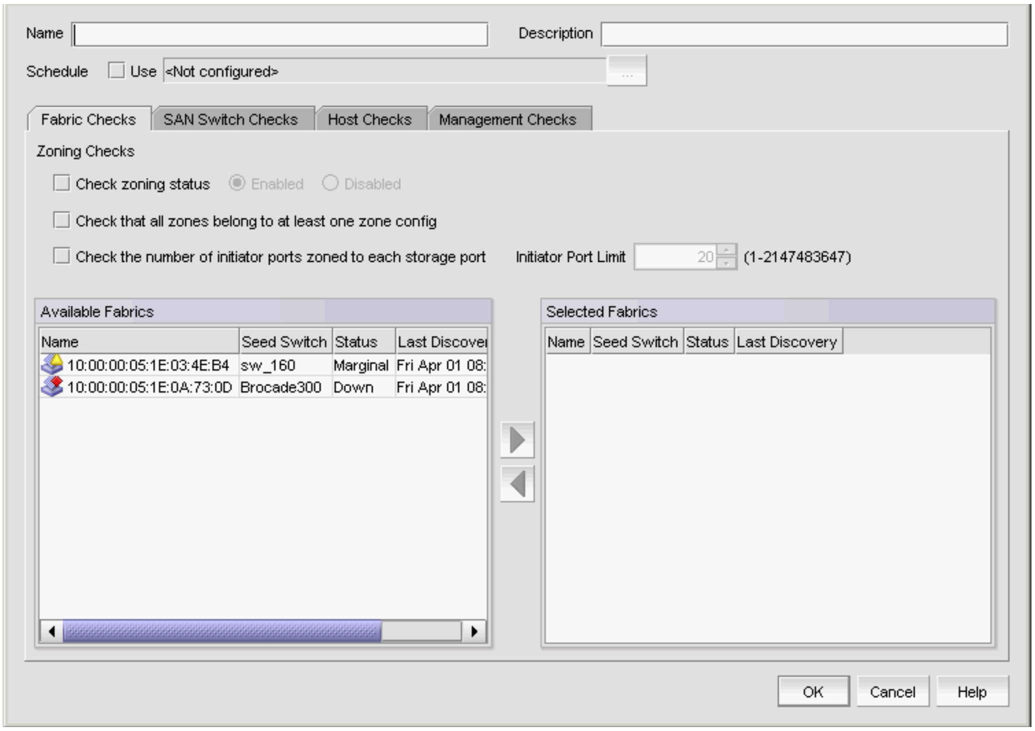
To view existing policy monitors, complete the following steps.

1. Select **Monitor > Policy Monitor.**

   The **Policy Monitor** dialog box displays.

2. Click **Add** .

   The **Add Monitor** dialog box displays.



Name

Description

Schedule □ Use <Not configured>

Zoning Checks

□ Check zoning status ● Enabled ○ Disabled

□ Check that all zones belong to at least one zone config

□ Check the number of initiator ports zoned to each storage port Initiator Port Limit 20 (1-2147483647)

Available Fabrics

Name	Seed Switch	Status	Last Discover
10:00:00:05:1E:03:4E:B4	sw_160	Marginal	Fri Apr 01 08:
10:00:00:05:1E:0A:73:0D	Brocade300	Down	Fri Apr 01 08:

Selected Fabrics

Name	Seed Switch	Status	Last Discovery

FIGURE 345 Add Policy Monitor dialog box, Fabric Checks tab

3. Enter a user-defined name for the policy in the **Name** field.

   The name does not have to be unique. It cannot be over 64 characters or empty. It cannot include asterisks.

4. Enter a description of the policy in the **Description** field.

   The description cannot be over 128 characters. It cannot include asterisks.

5. Click the **Schedule Use** check box.

6. Choose one of the following options:
   - To use the default frequency (one time, runs at current system time plus fifteen minutes), go to step 7.
   - To configure the frequency, click the ellipsis button and choose one of the following options to configure the frequency at which deployment runs for the policy monitor:
     - To configure deployment to run only once, refer to "Configuring a one-time policy monitor schedule" on page 819.
     - To configure hourly deployment, refer to "Configuring an hourly policy monitor schedule" on page 820.
     - To configure daily deployment, refer to "Configuring a daily policy monitor schedule" on page 820.
     - To configure weekly deployment, refer to "Configuring a weekly policy monitor schedule" on page 820.
     - To configure monthly deployment, refer to "Configuring a monthly policy monitor schedule" on page 821.
7. To set policy monitors for fabrics, select the **Fabric Checks** tab and complete the following steps.
   a. Select the **Check zoning status** check box to determine if zoning is enabled or disabled on the fabric.
      - Select the **Enabled** option to determine if zoning is enabled.
      - Select the **Disabled** option to determine if zoning is disabled.

   b. Select the **Check that all zones belong to at least one zone config** check box to determine if there are orphaned zones in the fabric zone database.

   c. Select the **Check the number of initiator ports zoned to each storage port** check box to determine the total number of initiator ports zoned to each storage port.

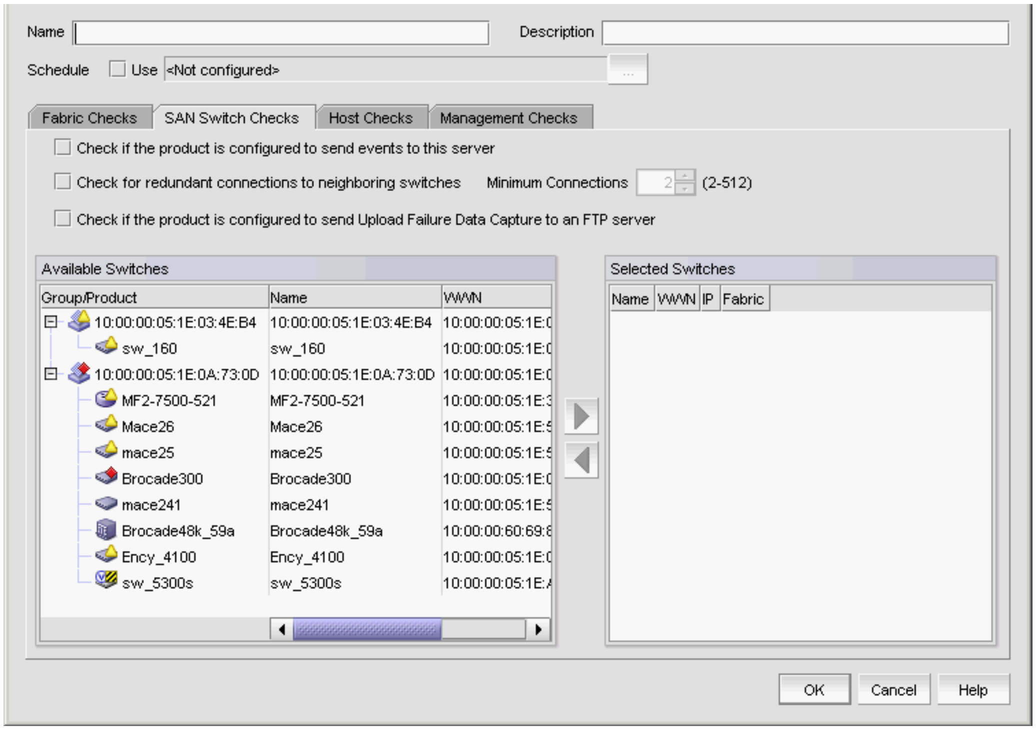
   d. Enter the initiator port limit in the **Initiator Port Limit** field.

      The default recommended is 20.

   e. Select the fabrics to which you want to apply this policy in the **Available Fabrics** table and click the right arrow button.

      The selected fabrics display in the **Selected Fabrics** table.

8. To set policy monitors for switches, select the **SAN Switch Checks** tab and complete the following steps.



Name
Description
Schedule □ Use <Not configured> ...

□ Check if the product is configured to send events to this server

□ Check for redundant connections to neighboring switches Minimum Connections 2 (2-512)

□ Check if the product is configured to send Upload Failure Data Capture to an FTP server

Available Switches

Group/Product	Name	WWN
⊟ 10:00:00:05:1E:03:4E:B4	10:00:00:05:1E:03:4E:B4	10:00:00:05:1E:0
sw_160	sw_160	10:00:00:05:1E:0
⊟ 10:00:00:05:1E:0A:73:0D	10:00:00:05:1E:0A:73:0D	10:00:00:05:1E:0
MF2-7500-521	MF2-7500-521	10:00:00:05:1E:3
Mace26	Mace26	10:00:00:05:1E:5
mace25	mace25	10:00:00:05:1E:5
Brocade300	Brocade300	10:00:00:05:1E:0
mace241	mace241	10:00:00:05:1E:5
Brocade48k_59a	Brocade48k_59a	10:00:00:60:69:8
Ency_4100	Ency_4100	10:00:00:05:1E:0
sw_5300s	sw_5300s	10:00:00:05:1E:A

Selected Switches

Name	WWN	IP	Fabric

FIGURE 346 **Add Policy Monitor dialog box, SAN Switch Checks tab**

a. Select the **Check if the product is configured to send events to this server** check box to determine if the Management application server is registered as an SNMP recipient and Syslog recipient.

b. Select the **Check for redundant connections to neighboring switches** check box to determine if there are at least the minimum number of configured ISLs between each switch pair.

   The default is 2.

c. Enter the minimum number of connections allowed between a switch pair in the **Minimum Connections** field.

   The default recommended is 2.

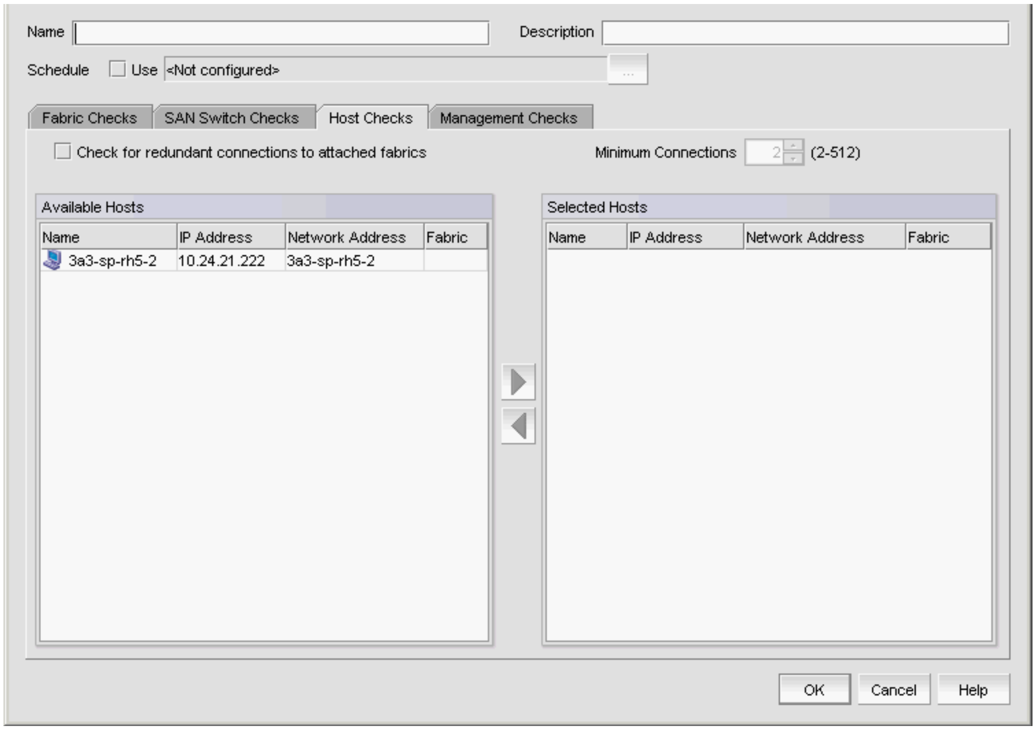
d. Select the **Check if the product is configured to send Upload Failure Data Capture to an FTP server** check box to determine the following configurations:

   - Upload Failure Data Capture is enabled on the selected switches
   - Configured FTP Server is accessible
   - You have write permission to the directory.

e. Select the switches to which you want to apply this policy in the **Available Switches** table and click the right arrow button.

   The selected switches display in the **Selected Switches** table.

9. To set policy monitors for hosts, select the **Host Checks** tab and complete the following steps.



Name

Description

Schedule □ Use <Not configured> ...

□ Check for redundant connections to attached fabrics

Minimum Connections 2 (2-512)

Available Hosts

Name	IP Address	Network Address	Fabric
3a3-sp-rh5-2	10.24.21.222	3a3-sp-rh5-2	

Selected Hosts

Name	IP Address	Network Address	Fabric

FIGURE 347 Add Policy Monitor dialog box, Hosts Checks tab

a. Select the **Check for redundant connections to attached fabrics** check box to determine if there are at least the minimum number of configured physical connections between the host and the attached fabric.

   The default is 2.

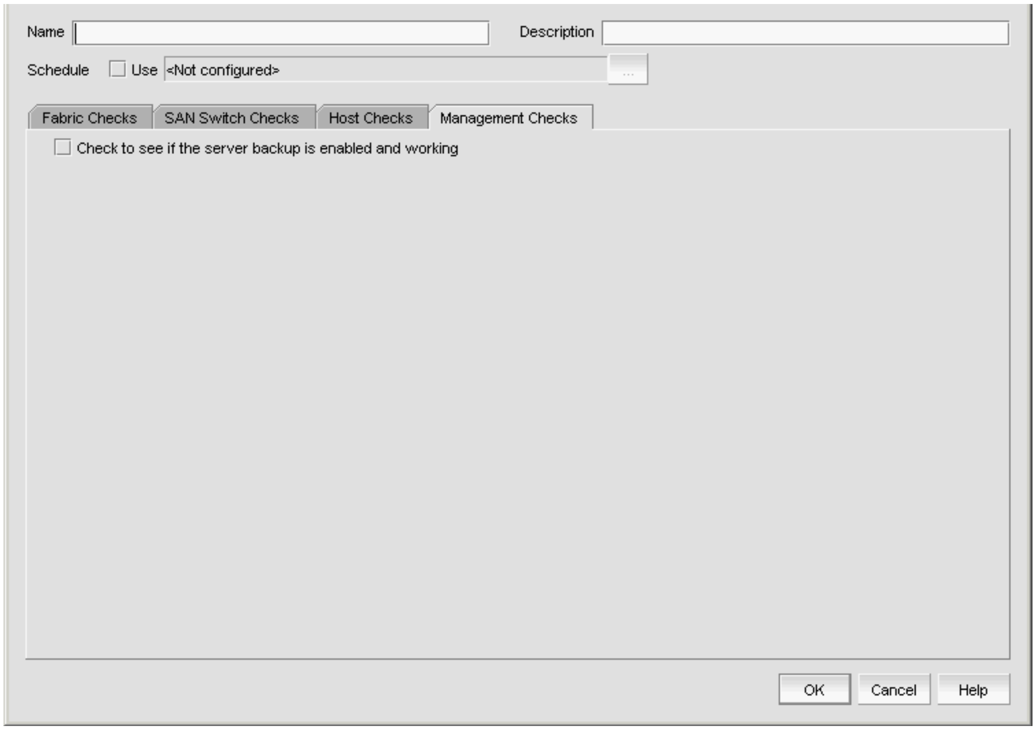
b. Enter the minimum number of connections between the host and the attached fabric in the **Minimum Connections** field.

   The default recommended is 2.

c. Select the hosts to which you want to apply this policy in the **Available Hosts** table and click the right arrow button.

   The selected hosts display in the **Selected Hosts** table.

10. To set policy monitors for the Management application, complete the following steps.



Name

Description

Schedule □ Use <Not configured>

□ Check to see if the server backup is enabled and working

FIGURE 348 Add Policy Monitor dialog box, Management Checks tab

a. Select the **Management Checks** tab.

b. Select the **Check to see if the server backup is enabled and working** check box to determine the following configurations:

- Back up enabled for the Management application server.
- Backup output directory is accessible and writable.

This policy only applies to scheduled backup, not manual (on demand) backup.

11. Click **OK** on the **Add Monitor** dialog box.

The new policy monitor displays in the **Monitors** table.

12. Click **Close** on the **Policy Monitor** dialog box.

Editing a policy monitor

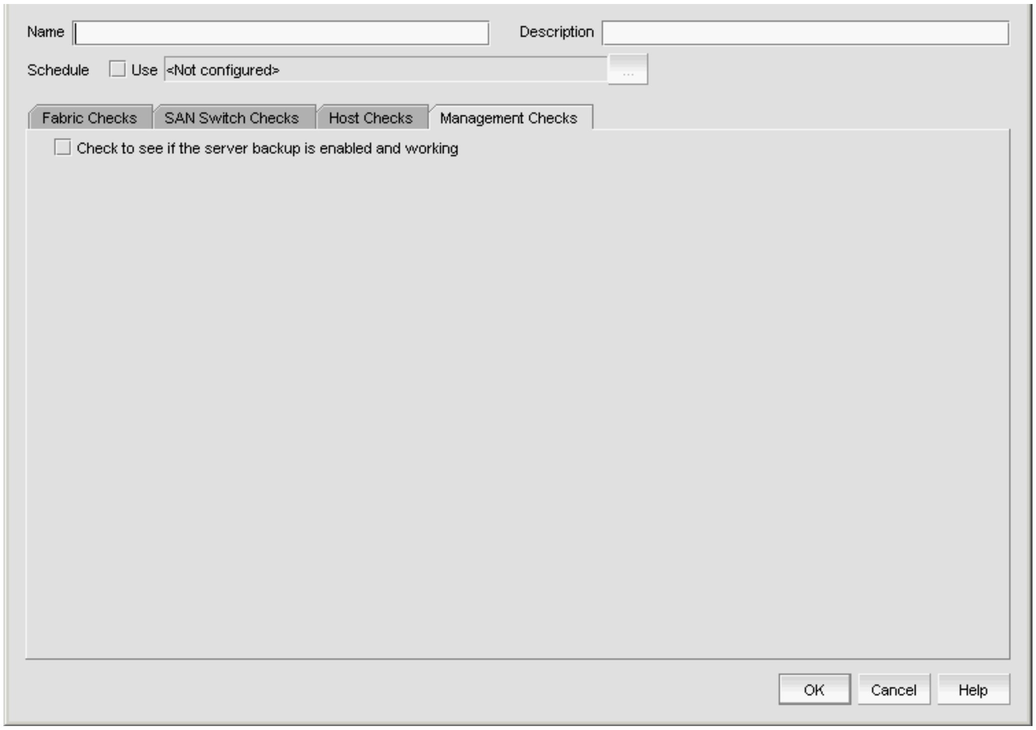
To edit an existing policy monitor, complete the following steps.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Select the policy you want to edit in the **Monitors** table and click **Edit**.

   The **Edit Policy Monitor** dialog box displays.



Name

Description

Schedule □ Use <Not configured>

□ Check to see if the server backup is enabled and working

FIGURE 349 Add Policy Monitor dialog box, Management Checks tab

3. Change the user-defined name for the policy in the **Name** field.

   The name does not have to be unique. It cannot be over 64 characters or empty. It cannot include asterisks.

4. Change the description of the policy in the **Description** field.

   The description cannot be over 128 characters. It cannot include asterisks.

5. Click the **Schedule Use** check box.

6. Choose one of the following options:
   - To use the default frequency (one time, runs at current system time plus fifteen minutes), go to step 7.
   - To configure the frequency, click the ellipsis button and choose one of the following options to configure the frequency at which deployment runs for the policy monitor:
     - To configure deployment to run only once, refer to "Configuring a one-time policy monitor schedule" on page 819.
     - To configure hourly deployment, refer to "Configuring an hourly policy monitor schedule" on page 820.
     - To configure daily deployment, refer to "Configuring a daily policy monitor schedule" on page 820.
     - To configure weekly deployment, refer to "Configuring a weekly policy monitor schedule" on page 820.
     - To configure monthly deployment, refer to "Configuring a monthly policy monitor schedule" on page 821.
7. To set policy monitors for fabrics, select the **Fabric Checks** tab and complete the following steps.

   a. Select the **Check zoning status** check box to determine if zoning is enabled or disabled on the fabric.

      - Select the **Enabled** option to determine if zoning is enabled.
      - Select the **Disabled** option to determine if zoning is disabled.

   b. Select the **Check that all zones belong to at least one zone config** check box to determine if there are orphaned zones in the fabric zone database.

   c. Select the **Check the number of initiator ports zoned to each storage port** check box to determine the total number of initiator ports zoned to each storage port.

   d. Enter the initiator port limit in the **Initiator Port Limit** field.

      The default recommended is 20.

   e. To add fabrics, select the fabrics to which you want to apply this policy in the **Available Fabrics** table and click the right arrow button.

      The selected fabrics display in the **Selected Fabrics** table.

   f. To remove fabrics, select the fabrics to which you do not want to apply this policy in the **Selected Fabrics** table and click the left arrow button.

      The removed fabrics display in the **Available Fabrics** table.
8. To set policy monitors for switches, select the **SAN Switch Checks** tab and complete the following steps.

   a. Select the **Check if the product is configured to send events to this server** check box to determine if the Management application server is registered as an SNMP and Syslog recipient.

   b. Select the **Check for redundant connections to neighboring switches** check box to determine if there are at least the minimum number of configured ISLs between each switch pair.

c. Enter the minimum number of connections allowed between a switch pair in the **Minimum Connections** field.

   The default recommended is 2.

d. Select the **Check if the product is configured to send Upload Failure Data Capture to an FTP server** check box to determine the following configurations:

   - Upload Failure Data Capture is enabled on the selected switches
   - Configured FTP Server is accessible
   - You have write permission to the directory.

e. To add switches, select the switches to which you want to apply this policy in the **Available Switches** table and click the right arrow button.

   The selected switches display in the **Selected Switches** table.

f. To remove switches, select the switches to which you do not want to apply this policy in the **Selected Switches** table and click the left arrow button.

   The removed switches display in the **Available Switches** table.

9. To set policy monitors for hosts, select the **Host Checks** tab and complete the following steps.

   a. Select the **Check for redundant connections to attached fabrics** check box to determine if there are at least the minimum number of configured physical connections between the host and the attached fabric.

   b. Enter the minimum number of connections between the host and the attached fabric in the **Minimum Connections** field.

      The default recommended is 2.

   c. To add hosts, select the hosts to which you want to apply this policy in the **Available Hosts** table and click the right arrow button.

      The selected hosts display in the **Selected Hosts** table.

   d. To remove hosts, select the hosts to which you do not want to apply this policy in the **Selected Hosts** table and click the left arrow button.

      The selected hosts display in the **Available Hosts** table.

10. To set policy monitors for the Management application, complete the following steps.

    a. Select the **Management Checks** tab.

    b. Select the **Check to see if the server backup is enabled and working** check box to determine the following configurations:

       - Back up enabled for the Management application server.
       - Backup output directory is accessible and writable.

       This policy only applies to scheduled backup, not manual (on demand) backup.

11. Click **OK** on the **Edit Monitor** dialog box.

    The updated policy monitor displays in the **Monitors** table.

12. Click **Close** on the **Policy Monitor** dialog box.

Deleting a policy monitor

To delete an existing policy monitor, complete the following steps.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Select the policy you want to delete in the **Monitors** table.
3. Click **Delete**.
4. Click **Yes** on the confirmation message.
5. Click **Close** on the **Policy Monitor** dialog box.

Running a policy monitor

Before you run a policy monitor, make sure your policy monitors are valid. Valid policy monitors must have at least one policy selected with one or more targets. Management checks do not require a target.

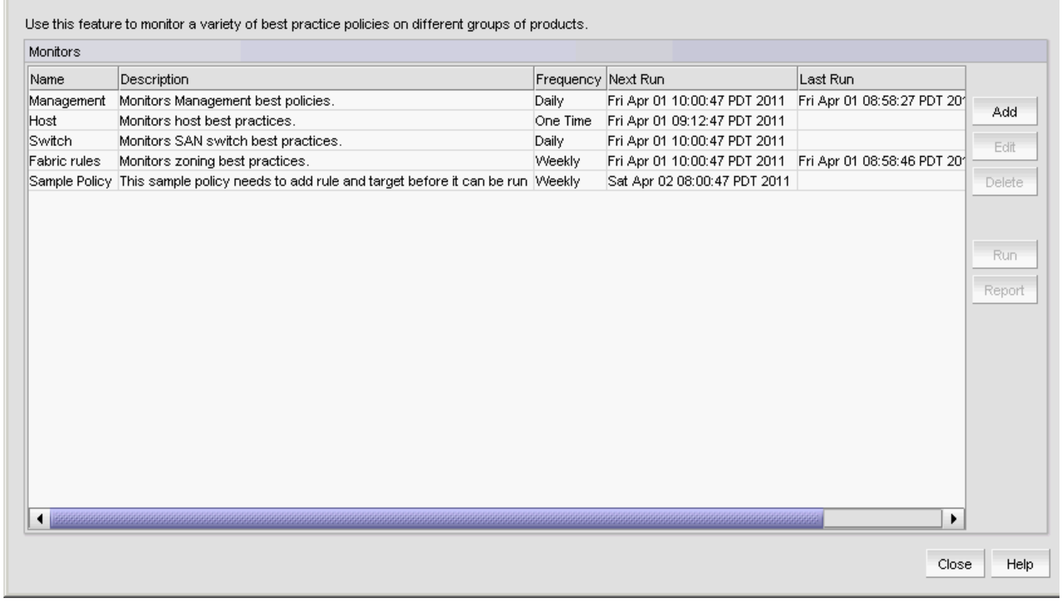
To run an existing policy monitor, complete the following steps.

1. Select **Monitor > Policy Monitor**.

   The **Policy Monitor** dialog box displays.

2. Select the policy you want to run in the **Monitors** table.
3. Click **Run**.

   When the policy monitor check is complete, the *Policy_Name* - **Policy Monitor Report** displays in a web browser.



Use this feature to monitor a variety of best practice policies on different groups of products.

Monitors

Name	Description	Frequency	Next Run	Last Run
Management	Monitors Management best policies.	Daily	Fri Apr 01 10:00:47 PDT 2011	Fri Apr 01 08:58:27 PDT 20
Host	Monitors host best practices.	One Time	Fri Apr 01 09:12:47 PDT 2011	
Switch	Monitors SAN switch best practices.	Daily	Fri Apr 01 10:00:47 PDT 2011	
Fabric rules	Monitors zoning best practices.	Weekly	Fri Apr 01 10:00:47 PDT 2011	Fri Apr 01 08:58:46 PDT 20
Sample Policy	This sample policy needs to add rule and target before it can be run	Weekly	Sat Apr 02 08:00:47 PDT 2011	

FIGURE 350 Policy Monitor Report

4. Review the report details.
    - Fabric Checks—Displays the Fabric Name and Status of the policy check for the following options:
        - Fabric - Check zoning is Enabled
        - Fabric - Check that all zones belong to at least one zone config
        - Fabric - Check the number of initiator ports zoned to each storage port is less than *Configured_Value*
    - SAN Switch Checks—Displays the switch name and switch IP address and Status of the policy check for the following options:
        - SAN Switch - Check if the product is configured to send events to this server
        - SAN Switch - Check if the product is configured to send Upload Failure Data Capture to an FTP server
        - SAN Switch - Check for at least *Configured_Minimum_Value* connections to neighboring switches
    - Host Check—Displays the Host name and Status of the policy check for the following option:
        - Host - Check for at least *Configured_Minimum_Value* connections to attached fabrics
    - Management Check—Displays the Status of the policy check for the following option:
        - Management - Check to see if the server backup is enabled and working

    To export a report, refer to “Exporting SAN reports” on page 903.

5. Click the close button (X) on the *Policy_Name* - **Policy Monitor Report** browser window.
6. Click **Close** on the **Policy Monitor** dialog box.

Viewing a policy monitor report

To view an existing (must have been run at least once) policy monitor report, complete the following steps.

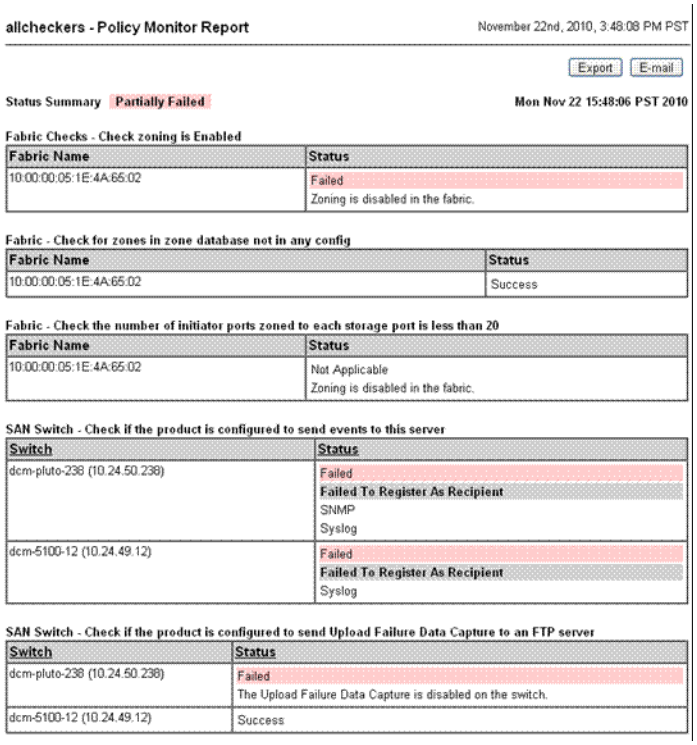
1. Select **Monitor > Policy Monitor.**

   The **Policy Monitor** dialog box displays.

2. Select the policy for which you want to view a report in the **Monitors** table.

3. Click **Report.**

   The *Policy_Name* - **Policy Monitor Report** displays in a web browser.



allcheckers - Policy Monitor Report November 22nd, 2010, 3:48:08 PM PST

Status Summary **Partially Failed** **Mon Nov 22 15:48:06 PST 2010**

Fabric Checks - Check zoning is Enabled

Fabric Name	Status
10:00:00:05:1E:4A:65:02	Failed Zoning is disabled in the fabric.

Fabric - Check for zones in zone database not in any config

Fabric Name	Status
10:00:00:05:1E:4A:65:02	Success

Fabric - Check the number of initiator ports zoned to each storage port is less than 20

Fabric Name	Status
10:00:00:05:1E:4A:65:02	Not Applicable Zoning is disabled in the fabric.

SAN Switch - Check if the product is configured to send events to this server

Switch	Status
dcm-pluto-238 (10.24.50.238)	Failed **Failed To Register As Recipient** SNMP Syslog
dcm-5100-12 (10.24.49.12)	Failed **Failed To Register As Recipient** Syslog

SAN Switch - Check if the product is configured to send Upload Failure Data Capture to an FTP server

Switch	Status
dcm-pluto-238 (10.24.50.238)	Failed The Upload Failure Data Capture is disabled on the switch.
dcm-5100-12 (10.24.49.12)	Success

FIGURE 351 ***Policy_Name*** **- Policy Monitor Report**

4. Review the report details.

   When a policy status fails or partially fails, the status is highlighted in pink.

   - Fabric Checks—Displays the Fabric Name and Status of the policy check for the following options:
     - Fabric - Check zoning is Enabled/Disabled (depends on your setting)
     - Fabric - Check that all zones belong to at least one zone config
     - Fabric - Check the number of initiator ports zoned to each storage port is less than *Configured_Value*

- SAN Switch Checks—Displays the switch name and switch IP address and Status of the policy check for the following options:
  - SAN Switch - Check if the product is configured to send events to this server
  - SAN Switch - Check if the product is configured to send Upload Failure Data Capture to an FTP server
  - SAN Switch - Check for at least *Configured_Minimum_Value* connections to neighboring switches
- Host Check—Displays the Host name and Status of the policy check for the following option:
  - Host - Check for at least *Configured_Minimum_Value* connections to attached fabrics
- Management Check—Displays the Status of the policy check for the following option:
  - Management - Check to see if the server backup is enabled and working

To export a report, refer to "Exporting SAN reports" on page 903.

5. Clickthe closebutton (X) on the *Policy_Name* - **Policy Monitor Report** browser window.
6. Click **Close** on the **Policy Monitor** dialog box.

Policy monitor scheduling

You can schedule a policy monitor to run automatically.

Configuring a one-time policy monitor schedule

To configure a one-time schedule, complete the following steps.

1. Select **One Time** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click the **Date** list to select a date from the calendar.
4. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to one of the following procedures:

   - To add policy monitor, refer to step 7 of "Adding a policy monitor" on page 808.
   - To edit policy monitor, refer to step 7 of "Editing a policy monitor" on page 813.

Configuring an hourly policy monitor schedule

To configure an hourly schedule, complete the following steps.

1. Select **Hourly** from the **Frequency** list.
2. Select the minute past the hour you want deployment to run from the **Minutes past the hour** list.

   Where the minute value is from 00 through 59.
3. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to one of the following procedures:

   - To add policy monitor, refer to step 7 of “Adding a policy monitor” on page 808.
   - To edit policy monitor, refer to step 7 of “Editing a policy monitor” on page 813.

Configuring a daily policy monitor schedule

To configure a daily deployment schedule, complete the following steps.

1. Select **Daily** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to one of the following procedures:

   - To add policy monitor, refer to step 7 of “Adding a policy monitor” on page 808.
   - To edit policy monitor, refer to step 7 of “Editing a policy monitor” on page 813.

Configuring a weekly policy monitor schedule

To configure a weekly schedule, complete the following steps.

1. Select **Weekly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Select the day you want deployment to run from the **Day of the Week** list.
4. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to one of the following procedures:

   - To add policy monitor, refer to step 7 of “Adding a policy monitor” on page 808.
   - To edit policy monitor, refer to step 7 of “Editing a policy monitor” on page 813.

Configuring a monthly policy monitor schedule

To configure a monthly schedule, complete the following steps.

1. Select **Monthly** from the **Frequency** list.
2. Select the time of day you want deployment to run from the **Time (hh:mm)** lists.

   Where the hour value is from 1 through 12, the minute value is from 00 through 59, and the day or night value is AM or PM.
3. Select the day you want deployment to run from the **Day of the Month** list (1 through 31).
4. Click **OK** on the **Schedule Properties** dialog box.

   To finish configuring the policy monitor, return to one of the following procedures:

   - To add policy monitor, refer to step 7 of "Adding a policy monitor" on page 808.
   - To edit policy monitor, refer to step 7 of "Editing a policy monitor" on page 813.

Chapter

Fault Management 30

In this chapter

Fault management overview

Fault management enables you to monitor your managed SAN and IP networks using the following methods:

- Listen, forward, and process SNMP traps for SAN and IP devices, which eliminates the need to poll devices for events.
- Receive and forward Syslog messages from Fabric OS switches, IP devices, and Brocade adapters—HBAs and CNAs are managed using the host connectivity manager (HCM) Agent.
- Manage pseudo events.
- Configure the following event actions:
  - Logging policy
  - E-mail alerts
  - Scripts
  - Broadcast to clients
  - Special events handling
  - Run Support Save (SAN only)
  - Deploy CLI configurations (IP only)
- Monitor audit logs and event logs for specified conditions
- Support application events.

Event notification

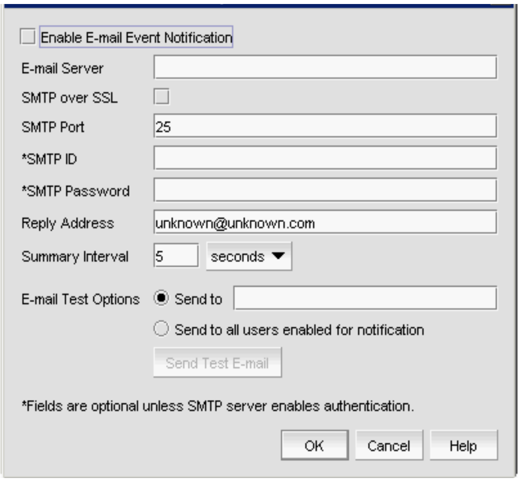
The Management application records the SAN and IP events in the Master Log. You can configure the application to send event notifications to e-mail addresses at certain time intervals. This is a convenient way to keep track of events that occur on the SAN and IP networks. You can also configure products to "call home" for certain events, notifying the service center of product problems. For instructions about configuring call home for events, refer to "Call Home" on page 161.

Configuring e-mail notification

To send notification of events to users, complete the following steps.

1. Select **Monitor** > **Event Notification** > **E-mail**.

   The **E-mail Event Notification Setup** dialog box displays (Figure 352).



☐ Enable E-mail Event Notification

E-mail Server

SMTP over SSL ☐

SMTP Port 25

*SMTP ID

*SMTP Password

Reply Address unknown@unknown.com

Summary Interval 5 seconds

E-mail Test Options ● Send to

○ Send to all users enabled for notification

*Fields are optional unless SMTP server enables authentication.

FIGURE 352 E-mail Notification Setup dialog box

2. Select the **Enable E-mail Event Notification** check box.
3. Enter the IP address or the name of the SMTP mail server that the Server can use to send the e-mail in the **E-mail Server** field.
4. Select the **SMTP over SSL** check box to enable secure communication.
5. Enter the authentication ID of the SMTP mail server in the **SMTP ID** field.

   NOTE
   This field is optional unless the SMTP server enables authentication.

6. Enter the authentication password of the SMTP mail server in the **SMTP Password** field.

   NOTE
   This field is optional unless the SMTP server enables authentication.

7. Enter the sender's e-mail address in the **Reply Address** field.

8. Enter the length of time the application should wait between notifications in the **Summary Interval** field and list.

   Notifications are combined into a single e-mail and sent at each interval setting. An interval setting of zero causes notifications to be sent immediately.

   ATTENTION
   Setting too short an interval can cause the recipient's e-mail inbox to fill *very* quickly.

9. Select one of the following options:
   - Select **Send to** and enter an e-mail address for a user to send a test e-mail to a specific user.
   - Select **Send to all users enabled for notification** to send a test e-mail to all users already set to receive notification.

10. Click **Send Test E-mail** to test the e-mail 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. If you are using an SMTP mail server, also verify that the SMTP ID and password information was entered correctly.

11. Click **OK** to save your work and close the **E-mail Event Notification Setup** dialog box.

Defining filters

The **Define Filter** dialog box, shown in Figure 353, allows you to define event filters by product, event category, and severity. You can define event filters on SAN products, IP products, or Hosts.

Setting up basic event filtering

To set up advanced event filtering on the selected events for a user, complete the following steps.

1. Select **Server** > **Users.**

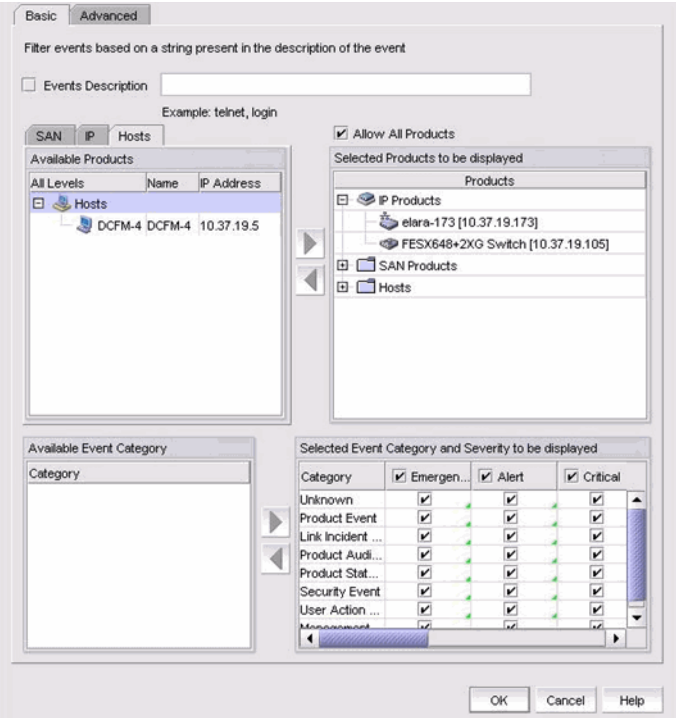
   The **Users** dialog box displays.

2. Select a user in the **Users** table and click **Edit**.

   The **Edit User** dialog box displays.

3. Select the **E-mail Notification Enable** check box and click the **Filter** link.

   The **Define Filter** dialog box displays.



Filter events based on a string present in the description of the event

☐ Events Description

Example: telnet, login

☑ Allow All Products

Available Products

All Levels	Name	IP Address
⊟ Hosts		
DCFM-4	DCFM-4	10.37.19.5

Selected Products to be displayed

Products
⊟ IP Products
elara-173 [10.37.19.173]
FESX648+2XG Switch [10.37.19.105]
⊞ SAN Products
⊞ Hosts

Available Event Category

Category

Selected Event Category and Severity to be displayed

Category	☑ Emergen...	☑ Alert	☑ Critical
Unknown	☑	☑	☑
Product Event	☑	☑	☑
Link Incident ...	☑	☑	☑
Product Audi...	☑	☑	☑
Product Stat...	☑	☑	☑
Security Event	☑	☑	☑
User Action ...	☑	☑	☑

FIGURE 353 Define Filter - Basic tab dialog box

4. Select which product type you are defining (SAN, IP, or Host) and click the appropriate tab.
5. Click the **Event Description** check box and enter a description of the event in the field.
6. Click the **Allow all products** check box to control whether or not all products are always displayed.
   - When selected (the default), all products, even newly-added products, are added to the **Selected Products to be displayed** list.
   - If de-selected, only the products listed in the **Selected Products to be displayed** list are shown in the Master Log and all newly-added products are added to the **Available** list.
7. Select one or more event categories from the **Available Event Category** list and click the right arrow button to move it to the **Selected Event Category and Severity** list. You can move any or all event categories.
8. Select at least one severity for each event. Severity options include Emergency, Alert, Critical, Error, Warning, Notice, Debug, Info, and Unknown.

NOTE
If you delete event actions that are part of the filtering criteria, they will not display in the Master Log, which displays in the lower left area of the main window, and lists all events and alerts that have occurred on the managed networks.

Setting up advanced event filtering

To set up advanced event filtering on the selected events for a user, complete the following steps.

1. Select **Server > Users.**

   The **Users** dialog box displays.

2. Select a user in the **Users** table and click **Edit**.

   The **Edit User** dialog box displays.

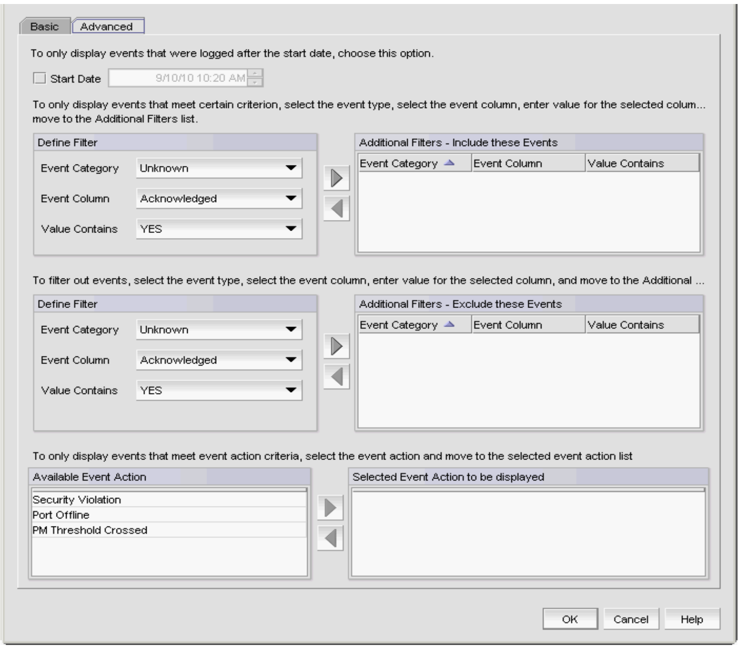
3. Select the **E-mail Notification Enable** check box and click the **Filter** link.

   The **Define Filter** dialog box displays.

4. Click **Advanced Filtering.**

   The **Define Filter—Advanced Event Filtering** dialog box displays.

5. Click the **Include Events** tab.



To only display events that were logged after the start date, choose this option.

□ Start Date 9/10/10 10:20 AM

To only display events that meet certain criterion, select the event type, select the event column, enter value for the selected colum... move to the Additional Filters list.

Define Filter

Event Category: Unknown

Event Column: Acknowledged

Value Contains: YES

Additional Filters - Include these Events

Event Category	Event Column	Value Contains

To filter out events, select the event type, select the event column, enter value for the selected column, and move to the Additional ...

Define Filter

Event Category: Unknown

Event Column: Acknowledged

Value Contains: YES

Additional Filters - Exclude these Events

Event Category	Event Column	Value Contains

To only display events that meet event action criteria, select the event action and move to the selected event action list

Available Event Action

Security Violation
Port Offline
PM Threshold Crossed

Selected Event Action to be displayed

FIGURE 354 **Define Filter - Advanced tab dialog box**

6. Click the **Start Date** check box to display only the events that were logged after the specified start date. The default start date and time is the current date and time.

7. To include events in the event filter, complete the following steps.

   a. Select the event type you want to include from the **Event Category** list.

      All event types are listed in alphabetical order.

   b. Select the event column for the event from the **Event Column** list.

      All event columns are listed in alphabetical order.

   c. Enter all or part of the event type value in the **Value Contains** field.

d. Click the right arrow button to move the event type to the **Additional Filters - Include these Events** list.

e. To add additional filters, repeat step a through step d.

8. To exclude events from the event filter, complete the following steps.

NOTE
You can configure a maximum of ten filters to be included.

a. Select the event type you want to remove from the **Event Category** list.

All event types are listed in alphabetical order.

b. Select the event column for the event from the **Event Column** list.

All event columns are listed in alphabetical order.

c. Enter all or part of the event type value in the **Value Contains** field.

d. Click the right arrow button to move the event type to the **Additional Filters - Exclude these Events** list.

e. To remove additional filters, repeat step a through step d.

9. To display an available event action, select the event action from the **Available Event Action** list and click the right arrow button to move it to the **Selected Event Action to be displayed** list.

10. Click **OK**.

The **Define Filter** dialog box displays.

11. Click **OK** to close **Define Filter** dialog box.

Viewing events

The **All Events** dialog box enables you to view all events that have occurred on the selected switch, even events that were filtered using advanced filtering criteria.

To view events for a selected device, complete the following steps.

1. Right-click a switch from the device tree or connectivity map.

2. Select **Events** from the list.

The **All Events** dialog box displays.

SNMP traps

Simple network management protocol (SNMP) provides a means to monitor and control network products and to manage configurations, statistics, performance, and security through authentication and privacy protocols.

The Management application allows you to configure SNMP traps. The SNMP configuration tasks are described in the following sections.

- "Defining filters"
- "Adding a trap recipient to one or more switches"
- "Removing a trap recipient from one or more switches"
- "SNMP trap forwarding"
- "Adding a trap destination"
- "Adding a new trap filter"
- "Event reception"
- "Adding an SNMP v3 credential"
- "Adding an SNMP v1 or v2c community string"
- "Importing a new MIB into the Management application"
- "Trap customization"
- "Unregistering a registered trap"
- "Customizing a registered trap definition"
- "Reverting the customization of a registered trap to default"

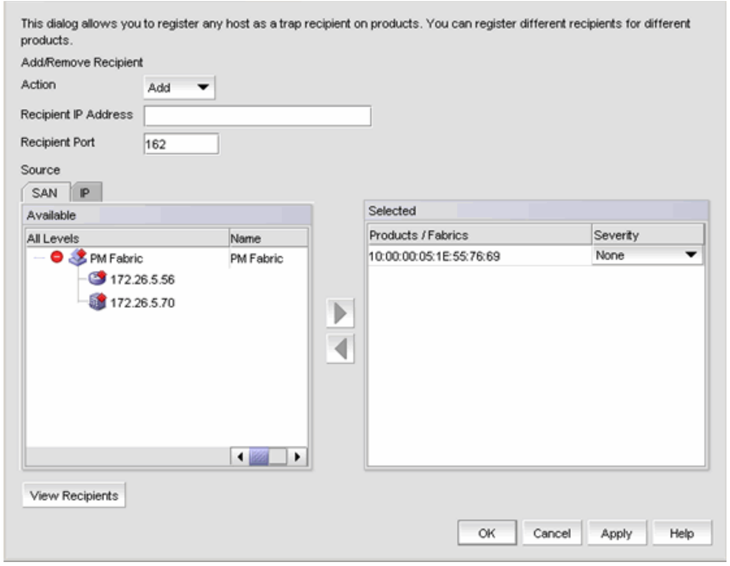
Adding a trap recipient to one or more switches

The **SNMP Trap Recipients** dialog box allows you to register any recipient as a trap recipient on selected products. You can register different recipients for different products.

NOTE
You can register and unregister other recipient servers on the Fabric OS switches on a per-fabric basis. For IP products, you can perform registration only at the switch level.

1. Select **Monitor** > **SNMP Setup** > **Product Trap Recipients**.

   The **SNMP Trap Recipients** dialog box, shown in Figure 355, displays.



This dialog allows you to register any host as a trap recipient on products. You can register different recipients for different products.

Action: Add

Recipient IP Address:

Recipient Port: 162

Products / Fabrics	Severity
10:00:00:05:1E:55:76:69	None

FIGURE 355 SNMP Trap Recipients dialog box

2. Click **Add** from the **Action** list.
3. Enter the IP address of the SNMP trap receiver (the recipient server) in the **Recipient IP Address** field. This is a mandatory field. IPv4 addresses are accepted, but a Domain Name System (DNS) name is not accepted.
4. Enter the SNMP trap port of the recipient in the **Recipient Port** field. This is a mandatory field. Valid numeric values range from 1 through 65535 and 162 is the default.
5. Select the fabric or switches from the **Available** list and click the right arrow button to move it to the **Selected** list. You can select multiple products.

NOTE
For IP products and product groups, only switches are available to select.

6. If the selected product is a SAN fabric, select a severity from the **Severity** list. Severity levels can be one of the following: None, Critical, Error, Warning, Info, or Debug. The Severity list is disabled for IP products (None is the default).
7. Click the **View Recipients** button to list the recipients that correspond to a selected fabric or product from the **Available** list.

   The **Trap Recipients - Fabric** dialog box or the **Trap Recipients - IP address** dialog box (depending on which product you selected), displays a list of configured recipients.
8. Click **OK.**

   The Management application registers the recipient IP address as an SNMP trap recipient. The SNMP version and credentials from the SNMP profile (for example, SNMP v3) are registered.

Removing a trap recipient from one or more switches

1. Select **Monitor > SNMP Setup > Product Trap Recipients.**

   The **SNMP Trap Recipients** dialog box, shown in Figure 355, displays.

2. Click **Remove** from the **Action** list.
3. Enter the IP address of the SNMP trap port (the recipient server) in the **Recipient IP Address** field.
4. Select the fabric or switches from the **Available** list.

   NOTE
   For IP products, only switches are available to select.

5. Click **OK.**

   The Management application removes the recipient from the managed switches.

SNMP trap forwarding

The **SNMP Trap Forwarding** dialog box allows the Management application to forward received SNMP traps to product trap recipients.

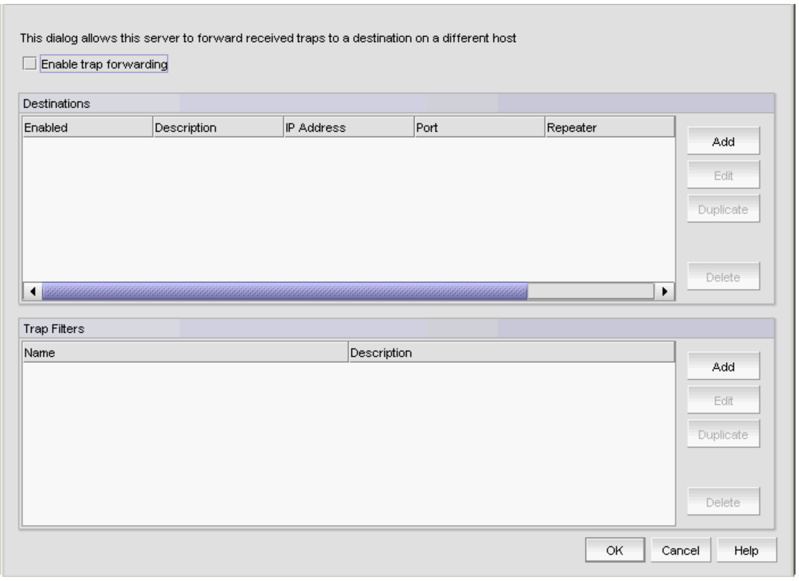
You can use the SNMP Trap Forwarding feature to set up filters to determine which traps will be forwarded. The filters can be one of the following:

- Severity of the trap
- Available products type
- Trap type
- Message types (application messages or pseudo events)

Perform the following steps to forward SNMP traps.

Select **Monitor > SNMP Setup > Trap Forwarding.**

The **SNMP Trap Forwarding** dialog box, shown in Figure 356, displays.



This dialog allows this server to forward received traps to a destination on a different host

□ Enable trap forwarding

Destinations

Enabled	Description	IP Address	Port	Repeater

Trap Filters

Name	Description

FIGURE 356 SNMP Trap Forwarding dialog box

The **SNMP Trap Forwarding** dialog box allows you to perform the following tasks:

- Add a trap destination.
- Edit a selected trap destination.
- Duplicate a selected trap destination.
- Delete a selected trap destination.

Adding a trap destination

The **Add Trap Destination** dialog box allows you to configure destinations for forwarding SNMP traps.

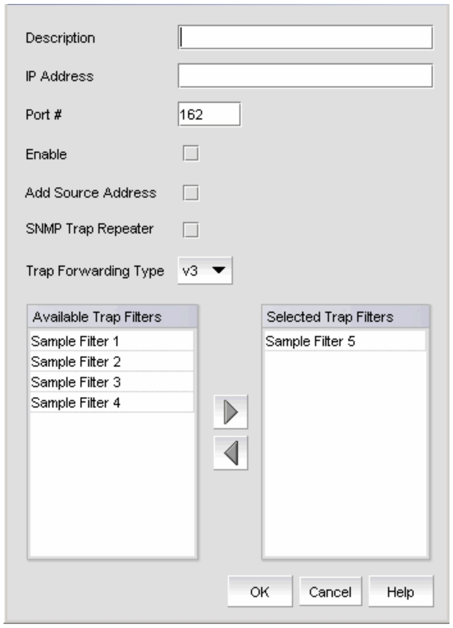
1. Select **Monitor** > **SNMP Setup** > **Trap Forwarding.**

   The **SNMP Trap Forwarding** dialog box, shown in Figure 356, displays.

2. Click the **Enable trap forwarding** check box.

3. Click **Add** in the **SNMP Trap Forwarding** dialog box.

   The **Add Trap Destination** dialog box, shown in Figure 357, displays.



Description

IP Address

Port # 162

Enable □

Add Source Address □

SNMP Trap Repeater □

Trap Forwarding Type v3

Available Trap Filters
Sample Filter 1
Sample Filter 2
Sample Filter 3
Sample Filter 4

Selected Trap Filters
Sample Filter 5

FIGURE 357 Add Trap Destination dialog box

4. Enter a general description of the trap destination in the **Description** field.
5. Enter the IP address of the trap destination in the **IP Address** field. This is a mandatory field. IPv4 and IPv6 addresses are accepted but a DNS name is not accepted.
6. Enter the SNMP trap listening port of the recipient in the **Port #** field. This is a mandatory field. Valid numeric values range from 1 through 65535.
7. Click the **Enable** check box to enable trap forwarding.
8. Click the **Add Source Address** check box.
9. Click the **SNMP Trap Repeater** check box. When enabled, all traps, whether the source is managed or unmanaged, are forwarded. When disabled, only traps from the selected products are forwarded.
10. Select the trap forwarding type from the list. Supported SNMP types are v1, v2c, and v3.
11. You can choose not to select a filter (zero), or you can select up to five filters from the **Available Filters** list. Click the right arrow button to move them to the **Selected Filters** list.
12. Click **OK**.

Adding a new trap filter

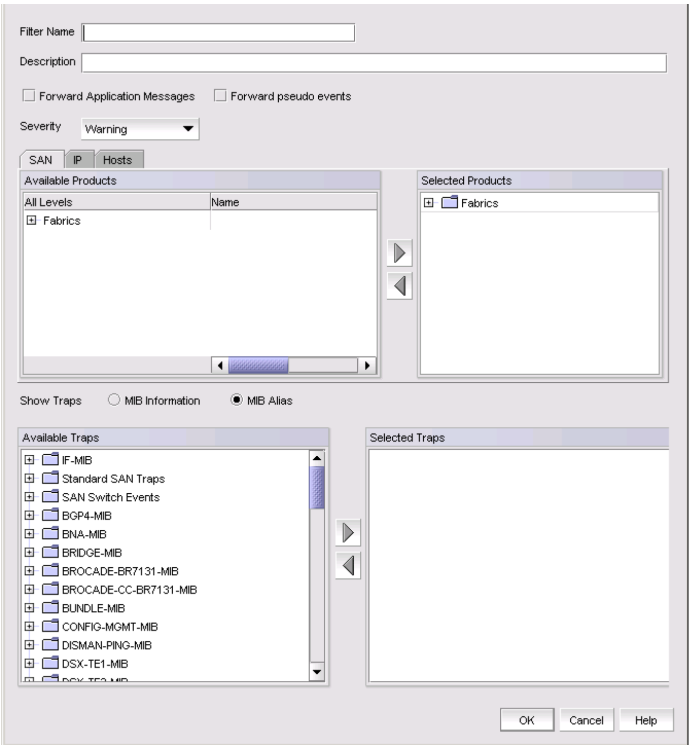
The **Add Trap Filter** dialog box allows you to configure trap filters for forwarding SNMP traps. You can add trap filters on SAN products, IP products, or Hosts.

1. Select **Monitor > SNMP Setup > Trap Forwarding.**

   The **SNMP Trap Forwarding** dialog box displays.

2. Click **Add** in the **Trap Filters** area of the **SNMP Trap Forwarding** dialog box.

   The **Add Trap Filter** dialog box, shown in Figure 358, displays.



Filter Name

Description

□ Forward Application Messages □ Forward pseudo events

Severity: Warning

Show Traps ○ MIB Information ● MIB Alias

FIGURE 358 Add Trap Filter dialog box

3. Select the SAN, IP, or Host tab. Depending on the tab selected, the products available to which you can add a trap filter display in the **Available Products** list.
4. Enter a unique name for the trap filter in the **Filter Name** field.
5. Enter a general description of the trap filter in the **Description** field.
6. Click the **Forward Application Messages** check box to forward application events.
7. Click the **Forward pseudo events** check box to forward pseudo events.
8. Select a severity level from the **Severity** list. The severity level can be one of the following, and appear in descending order of severity.
   - Emergency
   - Alert
   - Critical
   - Error

- Warning
- Notice
- Info
- Debug

Traps with the selected severity and those with higher severity levels are forwarded. For example, by default, Critical severity is selected. Therefore, traps with Critical, Alert, and Emergency severity levels are forwarded. To have all traps forwarded, select Debug, the lowest severity level.

9. By default, all traps are listed in the Available Traps list, under the folders for the MIB to which they belong. You can limit the list by selecting one of the following MIB types:
   - MIB Information - click the check box if you want the default SNMP name for the traps to be displayed.
   - MIB Alias - click the check box if you want the aliases for traps to be displayed.
10. After limiting the list of available traps, expand the MIB folder to which the trap you want belongs under the Available Trap Type list and select that trap. Click the right arrow button to move it to the Selected Trap Type list.
11. Click OK.

Event reception

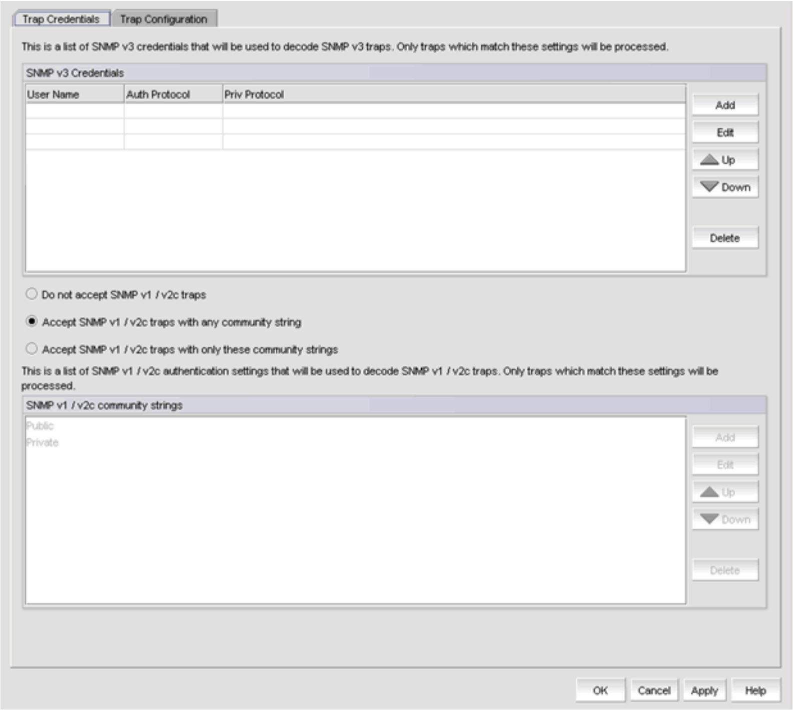
The Event Reception feature provides an interface to add the credentials and community strings required to decode traps. You can use the Event Reception dialog box to configure the trap message, severity, and alias name that is used by the Event Processor.

The Event Reception dialog box contains two tabs:

- The Trap Credentials tab allows you to configure the server to accept or drop SNMP traps and add SNMP credentials and community strings for decoding traps.
- The Trap Configuration tab allows you to customize the trap description or message, severity, and alias name.

To access the Event Reception dialog box, select Monitor > SNMP > Event Reception.

The Event Reception dialog box displays.



This is a list of SNMP v3 credentials that will be used to decode SNMP v3 traps. Only traps which match these settings will be processed.

SNMP v3 Credentials

User Name	Auth Protocol	Priv Protocol

○ Do not accept SNMP v1 / v2c traps

● Accept SNMP v1 / v2c traps with any community string

○ Accept SNMP v1 / v2c traps with only these community strings

This is a list of SNMP v1 / v2c authentication settings that will be used to decode SNMP v1 / v2c traps. Only traps which match these settings will be processed.

SNMP v1 / v2c community strings

Public
Private

FIGURE 359 Event Reception dialog box - Trap Credentials dialog box

The Management application can receive SNMP v1 traps from Brocade SAN switches and directors that have any SNMP community strings. It can receive SNMP v3 traps and informs from these SAN products.

The Table 49 explains the combinations of security and authentication, which will help you when you make your SNMP credentials configuration decisions.

TABLE 49 SNMP security and authentication

SNMP credential type	Privacy protocol	Authentication	Result
v1	No authentication No privacy protocol	Community string	Uses a community string to match for authentication.
v2c	No authentication No privacy protocol	Community string	Uses a community string to match for authentication.
v3	No authentication No privacy protocol	User name	Uses a user name to match for authentication.
v3	Authentication No privacy protocol	MD5[1] or SHA[2]	Provides authentication based on the HMAC-MD5[3] or HMAC-SHA algorithms.

TABLE 49 SNMP security and authentication (Continued)

SNMP credential type	Privacy protocol	Authentication	Result
v3	Authentication Privacy protocol	MD5 or SHA	Provides authentication based on the HMAC-MD or HMAC-SHA algorithms. Provides privacy based on CBC_DES[4] or CFB_AES_128[5].

[1] MD5 - message digest algorithm 5

[2] SHA - secure hash algorithm

[3] HMAC - hash-based message authentication

[4] CBC - cipher block chaining

[5] CFB - cipher feedback

By default, the Management application receives SNMP v1 and v2c traps from Brocade IP products that have any SNMP community strings. You can accept or restrict SNMP v1 and v2c traps by clicking one of the following check boxes in the **Event Reception** dialog box:

- Do not accept SNMP v1/v2c traps

  Use this option to turn off receiving SNMP v1\v2c traps. If selected, the Management application will not receive any SNMP v1 and v2c traps.

- Accept SNMP v1/v2c traps with any community string

  Use this option to turn on receiving SNMP v1 and v2c traps with any community string.

- Accept SNMP v1/v2c traps with only these community strings

  Use this option to turn on receiving SNMP v1 and v2c traps with only the specified community strings.

For information about how to configure SNMP credentials, refer to "Adding an SNMP v3 credential" on page 837 or "Adding an SNMP v1 or v2c community string" on page 838.

Adding an SNMP v3 credential

To add an SNMP v3 credential, complete the following steps:

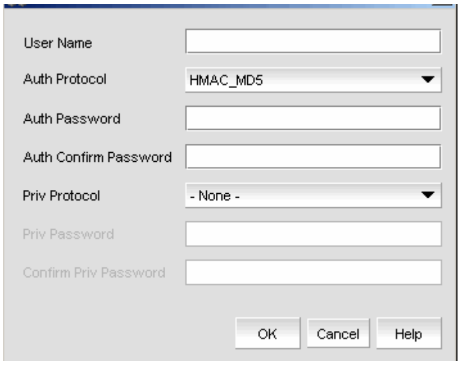
1. Select **Monitor > SNMP Setup > Event Reception.**

   The **Event Reception** dialog box displays.

2. Select an SNMP v3 credential from the **SNMP v3 Credentials** list on the **Event Reception** dialog box.

3. Click **Add.**

   The **Add SNMP v3 Credentials** dialog box, shown in Figure 360, displays.


User Name

Auth Protocol HMAC_MD5

Auth Password

Auth Confirm Password

Priv Protocol - None -

Priv Password

Confirm Priv Password

FIGURE 360 SNMP v3 Credentials dialog box

4. Type the user name in the **User Name** field.

   For configurations that do not have authentication or privacy, the Management application uses the user name to match for authentication.

5. Select an authentication protocol from the **Auth Protocol** list. You can select -None-, HMAC-MD5, or HMAC_SHA. HMAC_MD5 is the default.

   If you select no authentication, the Management application uses the user name to match for authentication.

6. Type a password in the **Auth Password** field and re-type the password in the **Auth Confirm Password** field.

7. Select a privacy protocol from the **Priv Protocol** list. You can select -None-, CBC_DES, or CFB_AES_128.

   If you select no privacy, the Management application uses the user name to match for authentication.

8. Type a password in the **Priv Password** field and re-type the password in the **Confirm Priv Password** field.

9. Click **OK.**

Adding an SNMP v1 or v2c community string

To add an SNMP v1 or v2c community string credential, complete the following steps:

1. Select **Monitor** > **SNMP Setup** > **Event Reception.**

   The **Event Reception** dialog box displays.

2. Click the **Accept SNMPv1/v2c traps with only these community strings** button.

3. Click **Add.**

   The **SNMP v1/v2c Community String** dialog box, shown in Figure 361, displays.

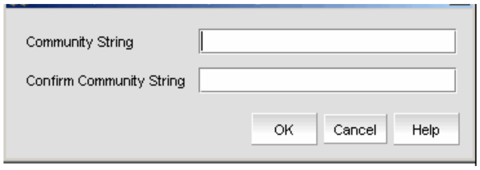


FIGURE 361 SNMP v1/v2 Community String dialog box

4. Enter a unique community string in the **Community String** field, which will be used to match for authentication in SNMP v1 and v2c configurations. This field is case-sensitive.
5. Re-enter the string in the **Confirm Community String** field.
6. Click **OK**.

Importing a new MIB into the Management application

The SNMP traps that the Management application receives must be registered in the Management application in order for these traps to be available. To register a trap, you must first identify the MIB file that contains the trap information in the mibs_to_compile.txt file. Then, you must register the traps using the **Event Reception** dialog box.

Follow the procedure below to add the MIB file that contains the trap you want to register to mibs_to_compile.txt.

1. Go to <*install-dir*>\conf\mibs\ (Windows) or <*install-dir*>/conf/mibs/ (UNIX) directory and copy the MIB file into that directory. You may want to copy the MIB into a subdirectory of that directory.
2. In the <*install-dir*>\conf\mibs\ (Windows) or <*install-dir*>/conf/mibs/ (UNIX) directory, search for the mibs_to_compile.txt file.
3. Using a text editor, open the mibs_to_compile.txt file and add the MIB information to the document.

   When adding the MIB information, be aware of the following rules:

   - MIBs are compiled in the order that they are listed in the mibs_to_compile.txt file.
   - You can add composite MIB files (more than one MIB in a single file).
   - MIB filenames in the mibs_to_compile.txt file are case-sensitive. Make sure the case of the file name you enter matches the case of the actual MIB file. Also, be sure to enter the complete path of the MIB file, or the portion relative to the mibs directory.

   The following is an example of how to add the two Cisco MIB files.

   ```
   #
   # Cisco Mibs
   #
   CISCO-SMI.mib
   CISCO-CONFIG-COPY-MIB.mib
   #
   # End Cisco Mibs
   #
   ```

4. Save the file.

   The Management application recompiles all the MIB files. If compilation is successful, the traps can now be registered in the **Event Reception** dialog box.

   NOTE
   If there are compilation errors, you can view the errors in the server log <*install dir*>\logs\server\server.log (Windows) or <*install dir*>/logs/server/server.log (UNIX).

5. If you make changes to the MIB file, open the mibs_to_compile.txt file and save the file.

   The Management application recompiles the MIB files and reloads the changes.

Trap customization

The **Trap Configuration** tab of the **Event Reception** dialog box enables you to configure the following settings:

- Register and unregister traps of various management information bases (MIBs)
- Customize trap description messages based on varbinds and severity and specify alias names.

Registering traps

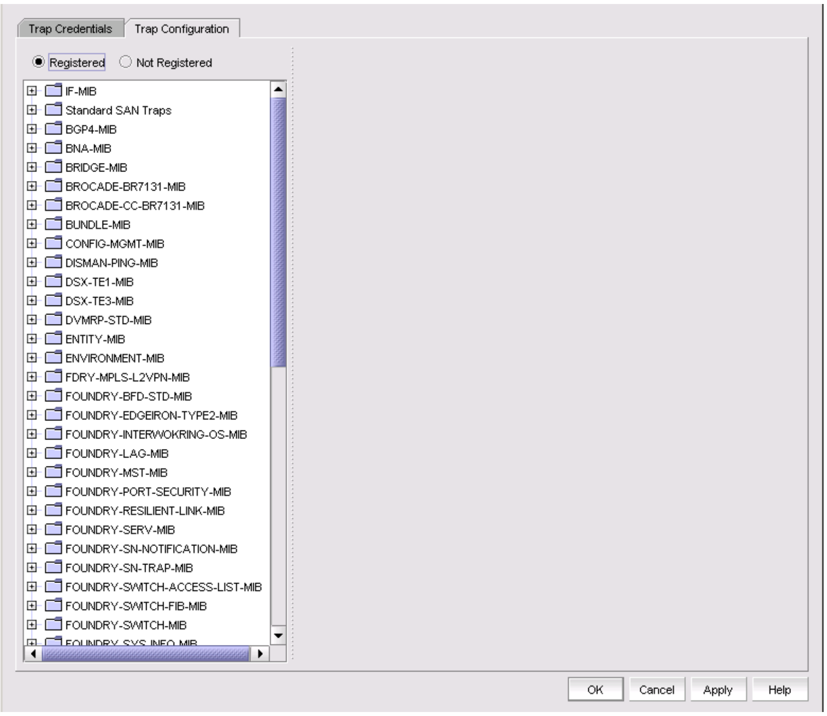
Traps must be registered in the Event Reception dialog box to make them available. Perform the following steps to register traps.

1. Select **Monitor** > **SNMP Setup** > **Event Reception**.
2. Click the **Trap Configuration** tab.

   The **Trap Configuration** tab of the **Event Reception** dialog box, shown in Figure 362, displays.

   The **Registered** and **Not Registered** buttons at the top of the Traps tree serves as a filter for the traps. If there are unregistered traps, they are listed when you select the **Not Registered** button.

   Traps appear under each MIB folder. The MIB folders correspond to the MIBs identified in the mibs_to_compile.txt file.



● Registered ○ Not Registered

- IF-MIB
- Standard SAN Traps
- BGP4-MIB
- BNA-MIB
- BRIDGE-MIB
- BROCADE-BR7131-MIB
- BROCADE-CC-BR7131-MIB
- BUNDLE-MIB
- CONFIG-MGMT-MIB
- DISMAN-PING-MIB
- DSX-TE1-MIB
- DSX-TE3-MIB
- DVMRP-STD-MIB
- ENTITY-MIB
- ENVIRONMENT-MIB
- FDRY-MPLS-L2VPN-MIB
- FOUNDRY-BFD-STD-MIB
- FOUNDRY-EDGEIRON-TYPE2-MIB
- FOUNDRY-INTERWOKRING-OS-MIB
- FOUNDRY-LAG-MIB
- FOUNDRY-MST-MIB
- FOUNDRY-PORT-SECURITY-MIB
- FOUNDRY-RESILIENT-LINK-MIB
- FOUNDRY-SERV-MIB
- FOUNDRY-SN-NOTIFICATION-MIB
- FOUNDRY-SN-TRAP-MIB
- FOUNDRY-SWITCH-ACCESS-LIST-MIB
- FOUNDRY-SWITCH-FIB-MIB
- FOUNDRY-SWITCH-MIB
- FOUNDRY-SYS-INFO-MIB

FIGURE 362 Trap Configuration tab of the Event Reception dialog box

3. Expand a folder for a MIB to display the traps in the MIB. If the list is too long, use the Search tool to find a MIB or trap.
4. Select the trap you want to register.

   The SNMP name and Object Identification (OID) of the trap appear at the top line of the configuration pane. Also, the status of the trap shows **Not Registered**, which is the default definition of the trap.

   Details about the trap appear in the fields beneath the **MIB Name** field.

   Trap details supply the following information:

   - The name of the MIB to which the trap belongs.
   - Information about the trap.
   - Any variable bindings (varbinds) that the trap uses. Information about the varbind, its name, OID, and type is displayed.
5. Enter the following information:
   a. Select the severity level you want to assign to the trap from the **Severity** list. If you do not select a severity, it defaults to Emergency.
   b. Type the message you want to display for this trap in the **Message** field. If the trap has varbinds, use $#, where # represents the varbind number, to indicate the varbind. You must enter a message.
   c. Type an alias string that serves as a second name for the trap in the **MIB Alias** field. This string might be more understandable to users. This parameter is optional. The Event Processor uses this alias, and this alias is displayed in the Event Action.

6. When you have finished, click **OK** to accept your entries.

   The status of the trap changes to **Registered - Customized** and the trap appears in the Event Log.

Unregistering a registered trap

You can unregister only the traps that you have registered. You cannot unregister traps that come with the Management application by default. Perform the following steps if you want to unregister a trap that you registered.

1. Select **Monitor > SNMP Setup > Event Reception**.
2. Click the **Trap Configuration** tab.
3. Click the **Registered** button.

   The Trap tree displays the MIBs that contain the registered traps.
4. Expand a MIB folder to display the traps that have been registered for that MIB.
5. Select a trap to display its current definition.
6. Click the **Unregister Trap** button.
7. Click **OK**.

   Once unregistered, the status of the trap changes to **Not Registered**.

Customizing a registered trap definition

Perform the following steps to modify the definitions of registered traps.

1. Click the **Trap Configuration** tab.
2. Click the **Registered** button.

   The Trap tree displays the MIBs that contain the registered traps.
3. Expand a MIB folder to display the traps that have been registered for that MIB.
4. Select a trap to display is current definition. You can change the severity, message, or alias of the trap.
5. When you have finished, click **OK** or **Apply** to accept your entries.

   If you modified a default trap, its status changes from **Registered - Default** to **Registered - Customized**.

Reverting the customization of a registered trap to default

Perform the following step to revert to the default definitions of registered-customized traps.

1. Click the **Trap Configuration** tab.
2. Click the **Registered** button.

   The Trap tree displays the MIBs that contain the registered traps.
3. Expand a MIB folder to display the traps that have been registered for that MIB.
4. Select a trap to display its current definition.

5. If the trap has been customized, a button labeled **Default** is availab.e. Click **Default** to revert the previous changes to its default.

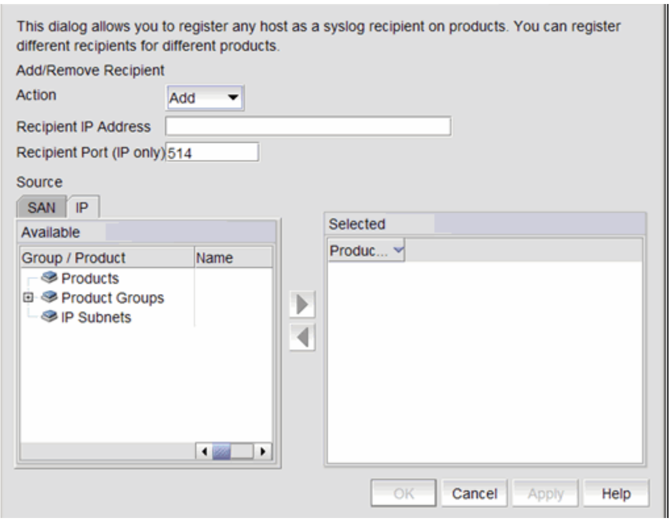
Syslogs

Use the **Options** dialog box to automatically register the Management application server as the syslog recipient on all managed SAN and IP products. The syslog listening port number is 514 by default. If you change the port number from 514, auto-registration is disabled.

Adding a syslog recipient

1. Select **Monitor** > **Syslog Configuration** > **Product Syslog Recipients.**

   The **Syslog Recipients** dialog box, shown in Figure 363, displays.



This dialog allows you to register any host as a syslog recipient on products. You can register different recipients for different products.

Add/Remove Recipient

Action: Add

Recipient IP Address:

Recipient Port (IP only): 514

FIGURE 363 Syslog Recipients dialog box

2. Select **Add** from the **Action** list.
3. Enter the IP address of the syslog port (the recipient server) in the **Recipient IP Address** field. This is a mandatory field. IPv4 addresses are accepted but a DNS name is not accepted.
4. Enter the syslog port of the recipient in the **Recipient Port** field. The default value is 514. Valid numeric values range from 1 through 65535.
5. Select the fabric or switches from the **Available** list and click the right arrow button to move it to the **Selected** list. You can select multiple products.

   NOTE
   For IP products, only switches are available to select.

6. Click **OK.**

   The Management application registers the recipient IP address as a syslog recipient.

Removing a syslog recipient

1. Select **Monitor** > **Syslog Configuration** > **Product Trap Recipients.**

   The **Syslog Recipients** dialog box displays.

2. Select **Remove** from the **Action** list.
3. Enter the IP address of the syslog port (the recipient server) in the **Recipient IP Address** field.
4. Select the fabric or switches from the **Available** list.
5. Click **OK.**

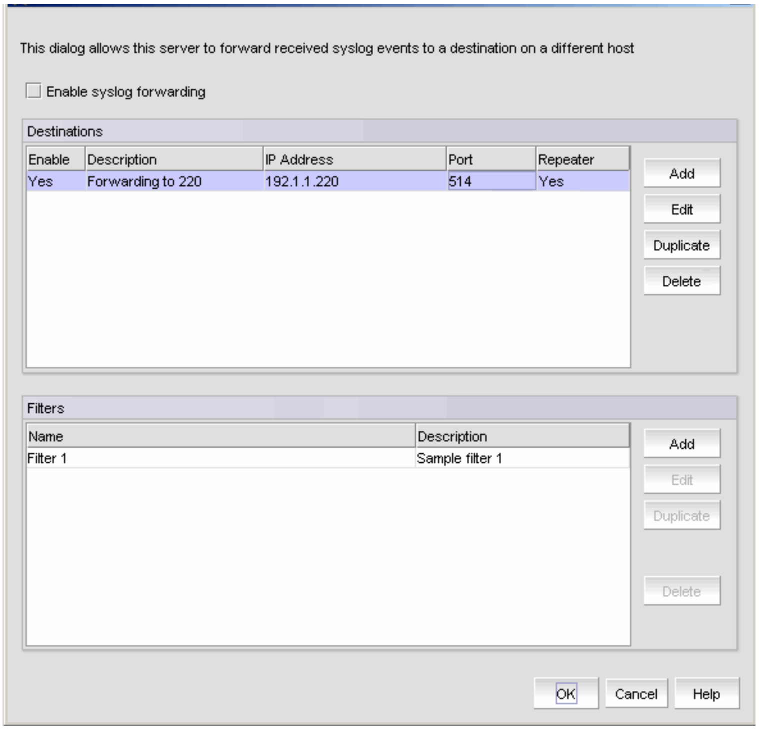
   The Management application removes the recipient from the managed switches.

Syslog forwarding

The **Syslog Forwarding** dialog box enables the Management application to forward syslog events to a destination on another host. You can use the Syslog Forwarding feature to set up filters to determine which syslog events will be forwarded.

1. Select **Monitor** > **Syslog Configuration** > **Syslog Forwarding.**

   The Syslog **Forwarding** dialog box, shown in Figure 364, displays.



This dialog allows this server to forward received syslog events to a destination on a different host

☐ Enable syslog forwarding

Destinations

Enable	Description	IP Address	Port	Repeater
Yes	Forwarding to 220	192.1.1.220	514	Yes

Filters

Name	Description
Filter 1	Sample filter 1

FIGURE 364 Syslog Forwarding dialog box

The **Syslog Forwarding** dialog box allows you to perform the following tasks:

- Add a syslog destination.
- Edit a selected syslog destination.
- Duplicate a selected syslog destination.
- Delete a selected syslog destination.

Adding a syslog destination

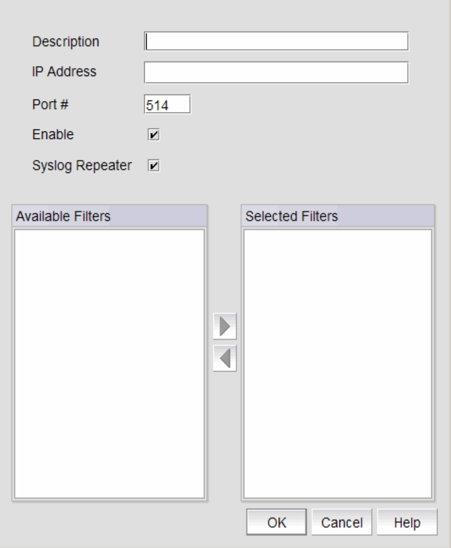
The **Add Syslog Destination** dialog box allows you to configure destinations for forwarding syslog events.

1. Select **Monitor** > **Syslog Configuration** > **Syslog Forwarding**.

   The **Syslog Forwarding** dialog box displays.

2. Click the **Enable syslog forwarding** check box.
3. Click **Add**.

   The **Add Syslog Destination** dialog box, shown in Figure 365, displays. Enable and Syslog Repeater are enabled by default.



Description

IP Address

Port # 514

Enable ☑

Syslog Repeater ☑

FIGURE 365 Add Syslog Destination dialog box

4. Enter a general description of the syslog destination in the **Description** field.
5. Enter the IP address of the syslog destination in the **IP Address** field. This is a mandatory field. IPv4 and IPv6 addresses are accepted but a DNS name is not accepted.
6. Enter the syslog listening port of the recipient in the **Port #** field. This is a mandatory field. Valid numeric values range from 1 through 65535. The default is 514.
7. Click the **Enable** check box to enable syslog forwarding to this recipient.
8. Click the **Syslog Repeater** check box if you want to forward all syslogs, whether the source is managed or unmanaged. If the Syslog Repeater feature is disabled, syslogs from the managed products are sent to the server. If no filter is selected, then syslogs from all products are sent.
9. You can choose not to select a filter (zero) or you can select up to five filters from the **Available Filters** list. Click the right arrow button to move them to the **Selected Filters** list. This is enabled only when **Syslog Repeater** is not checked.
10. Click **OK**.

Adding a syslog filter

You can add a syslog filter on SAN products, IP products, or Hosts.

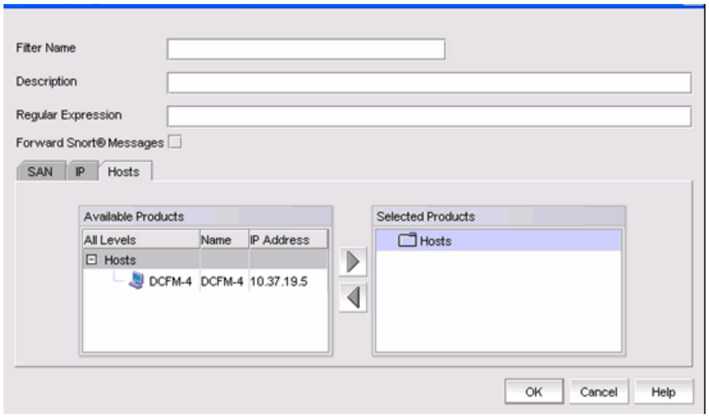
1. Select **Monitor** > **Syslog Configuration** > **Syslog Forwarding**.

   The **Syslog Forwarding** dialog box displays.

2. Click the **Enable syslog forwarding** check box.

3. Click **Add** in the **Filters** list.

   The **Add Syslog Filter** dialog box, shown in Figure 366, displays.



All Levels	Name	IP Address
⊟ Hosts		
DCFM-4	DCFM-4	10.37.19.5

FIGURE 366 Add Syslog Filter dialog box

4. Select the SAN, IP, or Host tab. Depending on the tab selected, the products available to which you can add a syslog filter display in the **Available Products** list.

5. Enter a unique name for the syslog filter in the **Filter Name** field.

6. Enter a general description of the syslog filter in the **Description** field. This field is case insensitive.

7. (Optional) For additional filtering, enter a text string using from 1 to 512 metacharacters or wild card symbols in the **Regular Expression** field. The regular expression is used to describe a pattern in text. You can use an asterisk (*) to indicate a wildcard, as in the following examples:

   - *cdef: Matches a message ending with cdef
   - abc*: Matches a message beginning with abc
   - *abc*: Matches a message that contains abc

8. Click the Forward Snort® Messages check box to turn on Snort message forwarding. See "Snort message forwarding" on page 860 for more information.

9. Select the product from the **Available Products** list and click the right arrow button to move it to the **Selected Products** list.

10. Click **OK**.

Event action definitions

To reduce the amount of events being logged in the Management application database, the Event Actions dialog box allows you to control what events the Management application monitors, on which products they are to be monitored, how often they are to be monitored, and what to do when the monitored events are generated. This information can be defined by creating an event action definition.

For example, you can create an event action definition if you want the Management application to monitor link up and link down traps only, and only on products that belong to Product Group 1. Furthermore, you may want these traps to be logged in the Management application database only if they occur 10 times within a 5-minute interval. You may also want an e-mail message sent to a network administrator when these traps are generated.

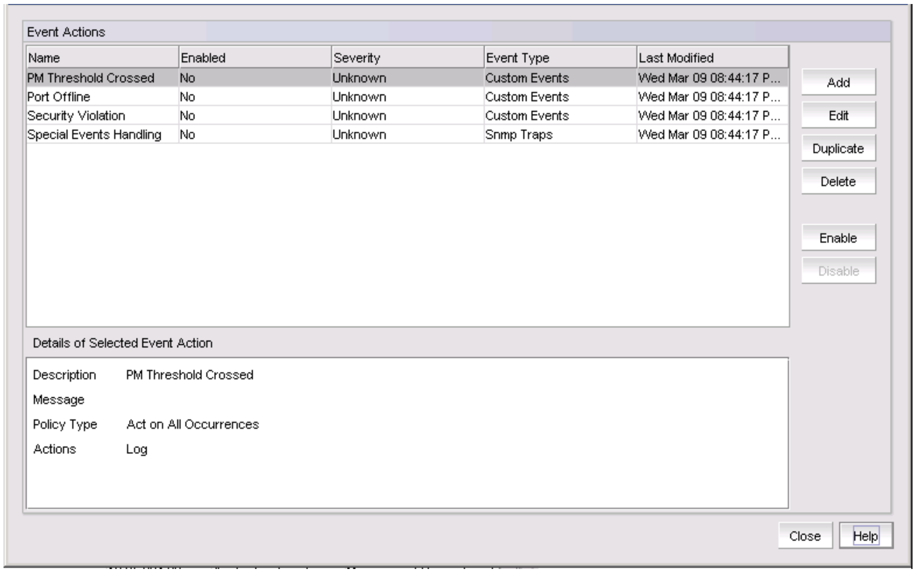
In another case, you may not want to log any occurrence of Topology Change traps from Product Group 2. You may also want to disable a port on a product if an event that resembles an attack on the network occurs at a certain frequency.

Creating an event action definition

Perform the following steps to create an event action definition.

1. Select **Monitor** > **Event Processing** > **Event Actions.**

   The **Event Actions** dialog box, shown in Figure 367, displays.



Event Actions

Name	Enabled	Severity	Event Type	Last Modified
PM Threshold Crossed	No	Unknown	Custom Events	Wed Mar 09 08:44:17 P...
Port Offline	No	Unknown	Custom Events	Wed Mar 09 08:44:17 P...
Security Violation	No	Unknown	Custom Events	Wed Mar 09 08:44:17 P...
Special Events Handling	No	Unknown	Snmp Traps	Wed Mar 09 08:44:17 P...

Details of Selected Event Action

Description PM Threshold Crossed
Message
Policy Type Act on All Occurrences
Actions Log

FIGURE 367 Event Actions dialog box

2. Click **Add** to display the **Identification** pane of the **Add Event Action** dialog box.
3. Enter a name and description for the event action and click the **Enabled** check box.
4. Click **Next** to advance to the **Events** pane.

   By default, the **Events** pane of the **Add Event Action** dialog box displays, as shown in Figure 368.

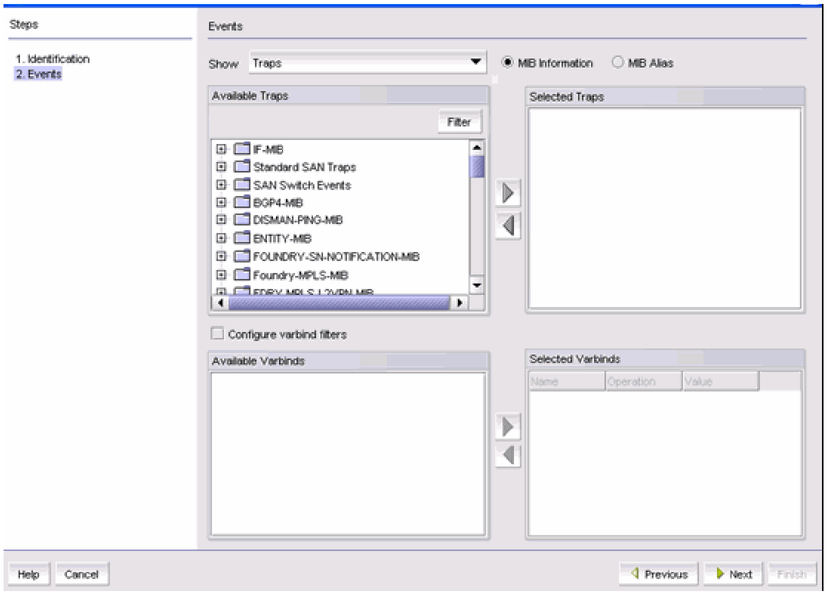


FIGURE 368 Add Events dialog box - Events pane

5. Select one of the following event types from the **Show** list:

   - Traps (default)
   - Application Events
   - Pseudo Events
   - Custom Events

   Depending on what event type you select, a box listing the available events or pseudo events displays.

6. By default, all traps are listed in the **Available Traps** list, under the folders for the MIB to which they belong. You can limit the list by doing any of the following:

   - Click one of the following buttons:
     - **MIB Information**, if you want the default SNMP name for the traps to be displayed.
     - **MIB Alias**, if you want the aliases for the traps to be displayed.
   - Use the Trap Filter tool to limit the trap list to the trap severities you want. To use this tool, click the **Filter** button to display the **Trap Filters** dialog box.

7. After limiting the list of available traps, expand the MIB folder to which the trap you want belongs under the **Available Traps** list and select that trap. Click the right arrow button to move it to the **Selected Traps** list.

8. If you selected **Application Events** in step 5, select the application events in the left table and use the arrow buttons to move them to the right.

9. If you selected **Pseudo Events** in step 5, select one or more of the pseudo events you created that you want to include in the definition, then click the right arrow button to move it to the **Selected Pseudo Events** list.

10. If you selected **Custom Events** in step 5, click Next to accept the defaults; otherwise, select the Event Category, Severity, Message ID, and Description Contains, as required.

11. Select **Configure varbind filters** to configure filters on varbind values (see “Configuring varbind filters” on page 849 for more information). If you do not want to configure varbind filters, click **Next**.

    The **Sources** pane of the **Add Event Action** dialog box is displayed. You can use the search tool to search for sources.

Configuring varbind filters

If actions must be confirmed based on a trap variable binding value (varbinds), select the **varbind filters** check box on the **Events** pane of the **Add Event Action** dialog box. This enables you to configure filters on varbind values for this event action.

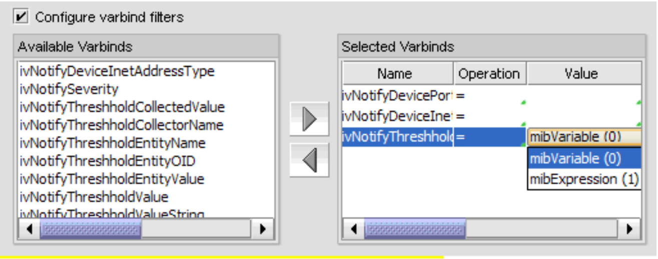
NOTE
Varbind filter configuration is only available if you selected Traps in step 5 of “Creating an event action definition” on page 847.

The varbinds for the selected trap are listed in the **Available Varbinds** list, shown in Figure 369.

1. Select **Monitor > Event Processing > Event Actions.**

   The **Event Actions** dialog box displays.

2. Click **Next** to advance to the **Events** pane.



☑ Configure varbind filters

Available Varbinds

ivNotifyDeviceInetAddressType
ivNotifySeverity
ivNotifyThreshholdCollectedValue
ivNotifyThreshholdCollectorName
ivNotifyThreshholdEntityName
ivNotifyThreshholdEntityOID
ivNotifyThreshholdEntityValue
ivNotifyThreshholdValue
ivNotifyThreshholdValueString

Selected Varbinds

Name	Operation	Value
ivNotifyDevicePor	=	
ivNotifyDeviceIne	=	
ivNotifyThreshhold	=	mibVariable (0)

mibVariable (0)
mibExpression (1)

FIGURE 369 Available varbinds and Selected varbinds dialog box

3. Select the varbind you want to include in the configuration and click the right arrow button to move it to the **Selected Varbinds** list.

   If you selected more than one trap and those traps have the same varbinds, then their varbinds are listed in the **Available Varbinds** box. However, if the traps you selected have different varbinds, the **Available Varbinds** box is empty.

4. For each varbind in the **Selected Varbinds** list, select one of the following operations for the condition you want to filter:

   - = – Equal to
   - != – Not equal
   - < – Less than
   - > – Greater than
   - >= – Greater than or equal to
   - <= – Less than or equal to

- in – Matches collection
- not_in – Does not match collection
- ~ – Arbitrary Unicode regular expression

5. Enter the value of the varbind. The value you enter must conform to the data type required by the varbind. For example, if the varbind expects an integer and you enter a text string, your entry will be rejected. Alternatively, you can select values from dropdown choices, as shown in Figure 369.

6. Click **Next.**

   The **Sources** pane of the **Add Event Action Sources** dialog box displays. Proceed to "Selecting source address products and ports" on page 850.

Selecting source address products and ports

The **Sources** pane of the **Add Event Action** dialog box, shown in Figure 370, allows you to enter the IP address, the world wide name, or the name of the source. Alternatively, you can select source address products to use as event senders from the available list of sources. You can select from the available list of SAN products, IP products, or Hosts by selecting the appropriate tab.

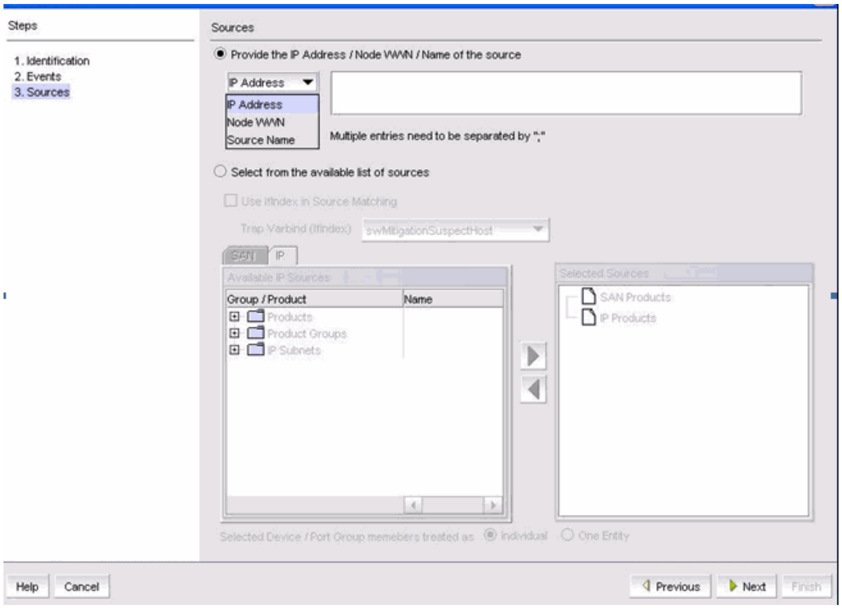


FIGURE 370 Sources pane of the Add Event Action dialog box

Perform the following steps to configure the identity of the source.

1. Select **Monitor** > **Event Processing** > **Event Actions.**

   The **Event Actions** dialog box displays.

2. Click **Next** to advance to the **Sources** pane.

3. Select the **Use Ifindex in source matching** check box if you want to use ifIndex to filter traps on a specific port of a product; otherwise, the filter is applied globally on a product.

4. If the **Use IfIndex in source matching** check box is selected, select the varbind to be used from the **Trap Varbind (IfIndex)** list.

5. Select the event senders you want from the **Available Sources** list, then click the right arrow button to move them in the **Selected Sources** box.

   NOTE
   The selected source count cannot exceed 100.

6. If you selected a product group or port group as event senders, select one of the following group members:

   NOTE
   The **Selected Product/Port Group members treated as** parameter is not available if you selected **Use Ifindex in source matching** (step 4).

   - **Individual**: Each member of the group will be treated as an individual entity by the Event Actions runtime engine as it monitors the specified event. The action is applied individually to products, access points, and sensors. For example, a policy is to be applied when two link down traps occur. If Product A and Product B both send link down traps, the policy will not be applied. The policy will be applied if Product A sends two link down traps.
   - **One Entity**: The entire group will be treated as one entity by the Event Actions runtime engine as it monitors the specified event. The action is applied to the entire group. For example, a policy is to be applied when two link down traps occur. If Product A and Product B both send link down traps, the policy will be applied. If Product A sends two link down traps, the policy is applied. It will also be applied if Product B sends two link down traps.

7. Click **Next**.

   The **Policy** pane of the **Add Event Action** dialog box displays. Proceed to “Configuring event action policies”.

Configuring event action policies

The **Policy** pane of the **Add Event Action** dialog box, shown in Figure 371, allows you to define the frequency of the event, enter a message for an event that will be displayed in the event log, and specify the event severity.

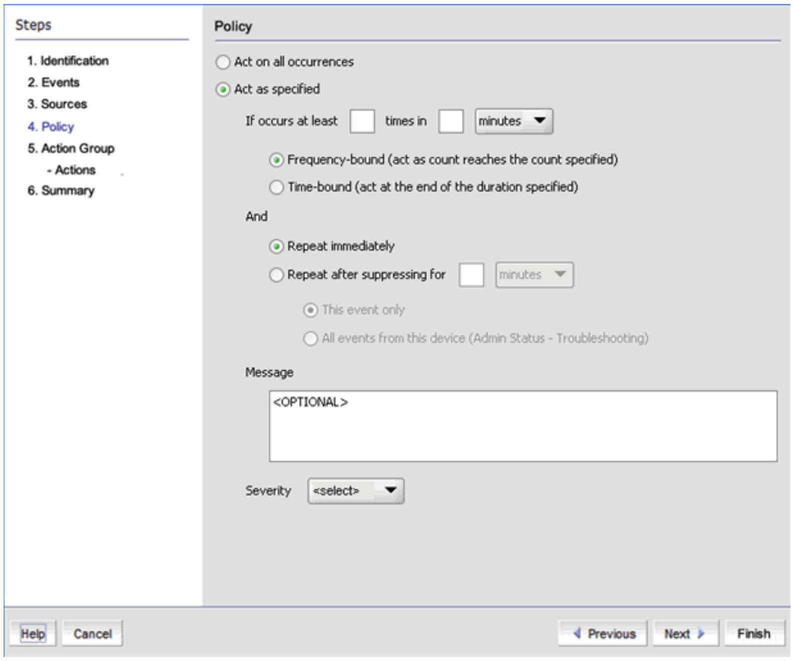


FIGURE 371 Policy pane of the Event Action dialog box

1. Click **Act on all occurrences** (default) if you want the action to be triggered each time the selected events occur.

2. Click **Act as specified** if you want the action to be triggered only when the occurrence of the event meets the specified criteria.

3. Click **If occurs at least __ times in __minutes** if you want the action to be applied only if the event occurs at a certain frequency. Then specify the frequency by selecting one of the following options:

   - Click **Frequency bound (act as count reaches the count specified)** if you want the Management application to perform the specified action once the specified number of occurrences has occurred *during* the specified duration. For example, if you want the action to be applied when 10 link down traps occur during a one-minute interval, then the specified action will be applied as soon as 10 link down traps occur, even though the one-minute duration has not elapsed.

- Click **Time bound (act at the end of the duration specified)** if you want the Management application to perform the specified action once the specified number of occurrences has occurred *and* the specified duration has elapsed. For example, if you want the action to be applied when 10 link down traps occur during a one-minute duration, the Management application waits until 10 link down traps occur and one minute has elapsed before the defined action is applied. There is a one-second delay for the action to be applied.

  For either option, if the number of occurrences has not been met and the time duration has elapsed, the observation window is advanced to the next occurrence after the first occurrence on the current window.

4. **And** - Indicate how often the policy is to be repeated. You can choose one of the following options:

   - **Repeat immediately** - Repeats the policy as soon as the specified action has been applied.
   - **Repeat after suppressing for ____ minutes or hours** - If this parameter is selected, the policy will not be applied to the product for the specified duration of time. Enter the duration in minutes or hours. You can suppress the policy just for the events specified in the policy or for any event that occurs on the product. Once the duration expires, the policy can be repeated.
   - **This event only** - If you select this option, the policy will not be repeated for the specified duration of time only if the events specified in this policy occur. For example, a policy is set to log link down traps if they occur 10 times within one minute and this parameter is selected to repeat the policy after 20 minutes. If 10 traps occur in one minute, the Management application policy waits for 20 minutes before it starts listening for new link down traps.
   - **All events for this device (Admin Status–Troubleshooting)** - This option is available if you have the Troubleshoot Device privilege in your Management application user account or role. It places the product in troubleshooting mode if the criteria in the policy are meet. For example, a policy is set to log link down traps if they occur 10 times within one minute. If 10 traps occur in one minute, and the **Repeat after suppressing for ____minutes or hours** parameter is set to 20 minutes, the Management application policy stops listening to *any* event for 20 minutes. After 20 minutes, the product returns to normal operating mode and the policy takes effect again.

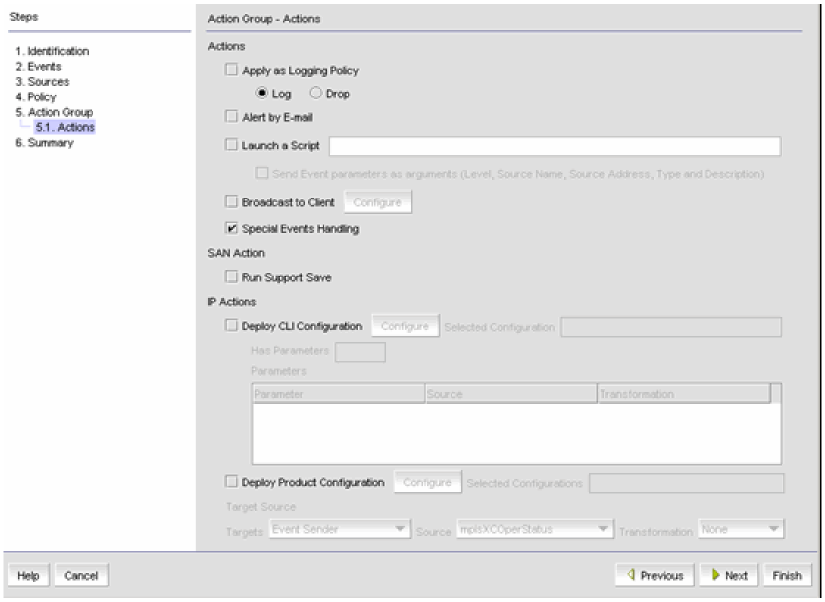
5. In the **Message** field, enter the message that will be displayed in the Event Log for the generated event. This entry replaces the default message that is displayed for a trap. Also, this message is used as the Event Action message and is displayed in single quotes on the Event Log report.

   NOTE
   The **Message** parameter is required if you selected **One Entity** for the **Selected Product/Port Group members treated as** parameter on the **Sources** pane of the **Add Event Action** dialog box. It is optional if you selected **Individual** for that parameter.

6. From the **Severity** list, select the severity you want to assign to the generated event.
7. Click **Next.**
8. The **Actions Group - Actions** pane of the **Edit Event Action** dialog box displays. Proceed to “Editing event actions”.

Editing event actions

The **Edit Event Action Group - Actions** dialog box, shown in Figure 372, defines what action the Management application takes when the criteria are met.



Steps

1. Identification
2. Events
3. Sources
4. Policy
5. Action Group
   - 5.1. Actions
6. Summary

Action Group - Actions

Actions

□ Apply as Logging Policy

● Log ○ Drop

□ Alert by E-mail

□ Launch a Script

□ Send Event parameters as arguments (Level, Source Name, Source Address, Type and Description)

□ Broadcast to Client

☑ Special Events Handling

SAN Action

□ Run Support Save

IP Actions

□ Deploy CLI Configuration

Selected Configuration

Has Parameters

Parameters

Parameter	Source	Transformation

□ Deploy Product Configuration

Selected Configurations

Target Source

Targets: Event Sender

Source: mplsXCOperStatus

Transformation: None

FIGURE 372 Action Group - Actions pane of the Edit Event Action dialog box

1. Select **Apply as a Logging Policy** to indicate whether or not you want the event occurrence to be logged in the Management application database:
   - Select **Log** to log the occurrence in the Management application database and master log.
   - Select **Drop** to not log the occurrence in the Management application database or master log.

   NOTE
   If the policy specifies **Act as specified** on the **Policy** pane of the **Add Event Action** dialog box, and you select **Log** for this parameter, only events that meet the criteria defined in the **Act as specified** area are logged. For example, if the event is logged when 10 link down traps occur during a one-minute interval, then one record will be logged after 10 link down traps occur. If you want all 10 link down traps to be logged, then create a policy where **Act on all occurrences** is selected on the **Policy** pane of the **Add Event Action** dialog box.

2. Select the **Alert by E-mail** check box if you want an e-mail message to be sent to an administrator if the policy criteria have been met.

3. Select the **Launch a Script** check box if you want to execute to an external script file when the matching criteria have been met, and then enter the script in the accompanying field.

4. Select the **Broadcast to Client** check box, and click **Configure** to broadcast a message to all the clients when the matching criteria have been met.

   NOTE
   The remaining parameters are not available if a non-Brocade product is selected as an event sender.

   The **Broadcast Message** dialog box displays.

   a. Select a severity level from the list.

   b. Type a message in the **Message Content** field.

   c. Click **OK**.

5. The **Special Events Handling** check box is enabled by default. Leave it enabled if you want the event action to be added to the Special Event Handling event action category. Refer to "Special events handling" for more complete information.

6. Select the **Deploy CLI Configuration** check box and click **Configure** if you want to deploy a configuration from CLI Configuration Manager to products if the policy criteria have been met. You can only deploy a CLI configuration for IP products.

   NOTE
   If the CLI configuration you chose from CLI Configuration Manager contains a non-Brocade product as a target, the configuration will not be deployed to the non-Brocade product.

7. You can either select an existing CLI configuration or create a new one and select that configuration. After selecting a CLI configuration, the name of the CLI configuration is displayed in the **Selected Configuration** field.

   - **Has Parameters** - Displays **Yes** if the CLI configuration has parameters that require values to be entered before it can be deployed, and displays **No** if no parameter needs to be defined.
   - The **Parameters** list lists the parameters that need to be defined in the configuration.
     - The **Parameter** column displays the parameter and its variables in the CLI configuration.
     - The **Source** column lists the appropriate SNMP attributes for the parameters. Each attribute contains a specific parameter value, such as an IP address. Select the attribute you want from the list.
     - The **Transformation** column uses the product IP addresses and MAC addresses listed in the Address Finder. If the Address Finder list is empty, the product or port will not be found. From this column, specify what you want Event Processor to do with the value in the attribute:

       Find Device: Find the product with the IP address in the attribute and deploy the CLI configuration to that product.

       Find Port: Find the port on a product with the IP address in the attribute and deploy the CLI configuration to that port.

       Find Intruder MAC: Find the product with the IP address in the attribute that matches the intruder MAC address and deploy the CLI configuration to that product.

       None: Event Processor only reports occurrence of the products.

8. Select the **Deploy Product Configuration** check box if you want to deploy a payload from the Configuration Wizard to the products if the policy criteria have been met.

   NOTE
   If the configuration payload you choose from the Configuration Wizard contains a non-Brocade product as a target, the payload will not be deployed to the non-Brocade product.

9. From the **Target** list, select the product (the target source) to which the payload will be deployed:

   - **Event Sender**: Deploy the payload to the product that sent the event. If the event was sent by a non-Brocade product, the event action will not be deployed to that product.
   - **Derived from**: Deploy the payload to the product that matches the IP address as specified in the attribute of the selected source. If the matching product is a non-Brocade product, the event action will not be deployed to that product.
   - **Specified in the Config**: Deploy the payload to the product that is specified in the payload. If the configuration you choose contains a non-Brocade product as a target, the configuration will not be deployed to the non-Brocade product.

10. If you selected **Derived from** as the target in step 9, select the attribute from the **Source** list.

11. From the **Transformation** column, specify what you want Event Processor to do with the value in the attribute:

    - **None** - Event Processor only reports the occurrence of the product.
    - **Find Device** - Find the product with the IP address in the attribute and deploy the payload to that product.

    The **Transformation** column uses the product IP addresses and MAC addresses listed in the Address Finder. If the Address Finder list is empty, the product or port will not be found.

12. Click **Next** to display the **Action Group - Email Settings** pane of the **Add Event Action** dialog box if you selected **Alert by E-mail**. If you did not select **Alert by E-mail**, you will advance to the **Summary** page.

Special events handling

The following special error conditions are examples of events that are categorized as Special Events Handling events, a separate category that appears in the **Name** list of the **Event Actions** dialog box. All pre-selected events are SNMP traps.

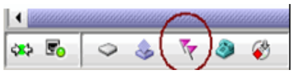
- Invalid T1 zone configuration event
- 48-blade inserted into a non-Virtual Fabric chassus
- Port fencing Fabric Watch trap, when a port is fenced

Though these error conditions are automatically considered “special events handling” events, you can add or edit any event action and mark the action as a special event for special events handling using the **Actions** pane of the **Edit Event Action** dialog box.

See step 5 of “Editing event actions” on page 854 for information on enabling special events handling for an event using the **Actions** pane of the **Edit Event Action** dialog box.

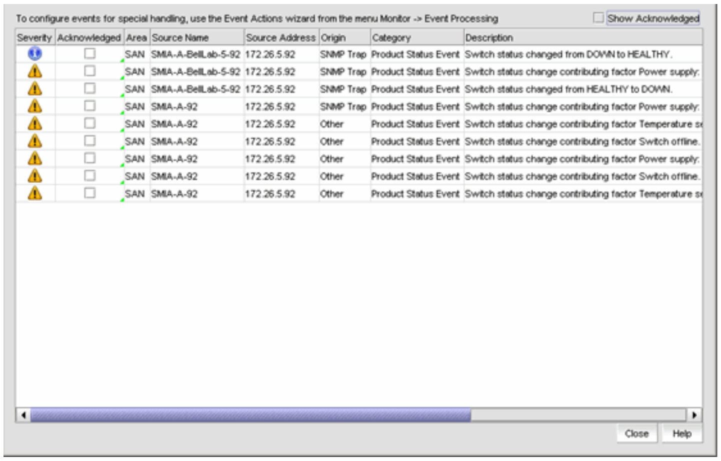
Acknowledging special events

When the Management application receives and processes events selected as special events, the following status bar icon displays.



1. Click the special events icon to launch the **Special Events** dialog box, shown in Figure 373.

   The dialog lists the most recent 1000 events that have been identified as special events.



To configure events for special handling, use the Event Actions wizard from the menu Monitor -> Event Processing

□ Show Acknowledged

Severity	Acknowledged	Area	Source Name	Source Address	Origin	Category	Description
ⓘ	□	SAN	SMIA-A-BellLab-5-92	172.26.5.92	SNMP Trap	Product Status Event	Switch status changed from DOWN to HEALTHY.
⚠	□	SAN	SMIA-A-BellLab-5-92	172.26.5.92	SNMP Trap	Product Status Event	Switch status change contributing factor Power supply:
⚠	□	SAN	SMIA-A-BellLab-5-92	172.26.5.92	SNMP Trap	Product Status Event	Switch status changed from HEALTHY to DOWN.
⚠	□	SAN	SMIA-A-92	172.26.5.92	SNMP Trap	Product Status Event	Switch status change contributing factor Power supply:
⚠	□	SAN	SMIA-A-92	172.26.5.92	Other	Product Status Event	Switch status change contributing factor Temperature s
⚠	□	SAN	SMIA-A-92	172.26.5.92	Other	Product Status Event	Switch status change contributing factor Switch offline.
⚠	□	SAN	SMIA-A-92	172.26.5.92	Other	Product Status Event	Switch status change contributing factor Power supply:
⚠	□	SAN	SMIA-A-92	172.26.5.92	Other	Product Status Event	Switch status change contributing factor Switch offline.
⚠	□	SAN	SMIA-A-92	172.26.5.92	Other	Product Status Event	Switch status change contributing factor Temperature s

FIGURE 373 Special Events dialog box

2. Click the **Acknowledged** check box that corresponds to the special event you want to acknowledge.

   If an event is marked as acknowledged either in the **Special Events** dialog box or the **Master Log**, the event is acknowledged in both places.

3. To view all acknowledged special events, click the **Show Acknowledged** check box in the upper right corner of the dialog box. This check box is disabled by default.

   The acknowledged special events display, sorted by the last event server time.

Configuring event action e-mail settings

The **Action Group - E-mail Settings** pane of the **Add Event Action** dialog box, shown in Figure 374, allows you to select e-mail recipients from a list, add new e-mail recipients, and compose e-mail messages.

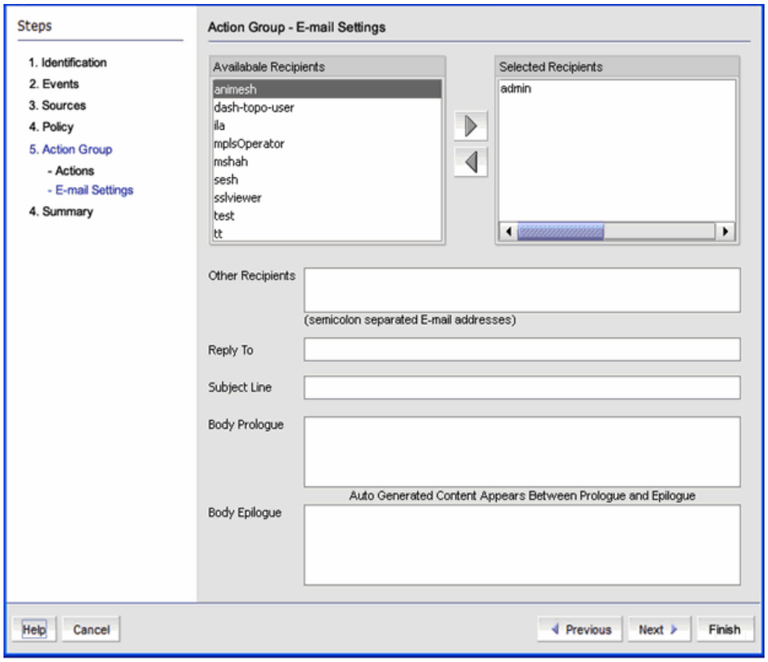


FIGURE 374 Action Group - E-mail Settings pane of the Add Event Action dialog box

1. (Optional) Select the Management application user to whom the e-mail message will be sent from the **Available Recipients** list, and click the right arrow button to move the recipient to the **Selected Recipients** list.

NOTE
Make sure the user you select has an e-mail address defined in a user account.

2. Add additional e-mail recipient addresses in the **Other Recipients** field. Separate multiple e-mail addresses with a semicolon. At least one e-mail address must be specified by either selecting an available recipient from the list (step 1) or typing an e-mail recipient.
3. If you want the e-mail message for the alert to display a description on the subject line, enter the text in the **Subject Line** field.
4. If you want a prologue to be inserted at the beginning of the e-mail message, enter up to 255 characters in the **Body Prologue** field. The event action message follows the prologue.
5. If you want an epilogue to be placed at the end of the e-mail message, enter up to 255 characters in the **Body Epilogue** field.

NOTE
The prologue, the event action message, and the epilogue form the body of the e-mail alert.

6. Click **Finish**.

   The **Summary** pane of the **Edit Event Action** dialog box displays an overview of the e-mail configuration you are creating.

7. Review your entries and take one of the following actions:

   - Click **Finish** to approve the configuration.
   - Click **Previous** to return to the **Action Group - E-mail Settings** pane of the
   - dialog box.
   - Click **Cancel** to cancel the operation.

Creating a new event action definition by copying an existing one

You can create a new event action definition by copying one that is in the **Event Actions** list.

1. Select **Monitor > Event Processing > Event Actions.**

   The **Event Actions** dialog box displays.

2. Select the definition that you want to copy from the **Event Actions** list.
3. Click the **Duplicate** button to display the **Duplicate Event Actions** dialog box.

   The name of the event action is the name of the selected action with the word “copy” appended. For example, Action1 becomes Action1 copy.

4. Enter a new name for the definition.
5. Change the description of the definition, if needed. You can perform this action in any of the Add Event Action panes.
6. Click **Finish** to save the new definition.

Modifying an event action definition

Use caution when you modify an event action. Saving changes to an event action definition resets the runtime information for the events in the definition.

Perform the following steps to modify an event action definition.

1. Select **Monitor > Event Processing > Event Actions.**

   The **Event Actions** dialog box displays.

2. Select the definition that you want to edit from the **Event Actions** list.
3. Click **Edit** to display the **Edit Event Action** dialog box.
4. Make the changes you want to make to the definition. You can perform this action in any of the Add Event Action panes.
5. Click **Finish** to save your definition.

Deleting an event action definition

Perform the following steps to delete an event action definition.

1. Select **Monitor** > **Event Processing** > **Event Actions**.

   The **Event Actions** dialog box displays.

2. Select the definition that you want to delete from the **Event Actions** list.
3. Click **Delete**.

   A message displays asking you to confirm the deletion request.

4. Click **Yes** to delete the definition, or **No** to cancel the request.

Snort message forwarding

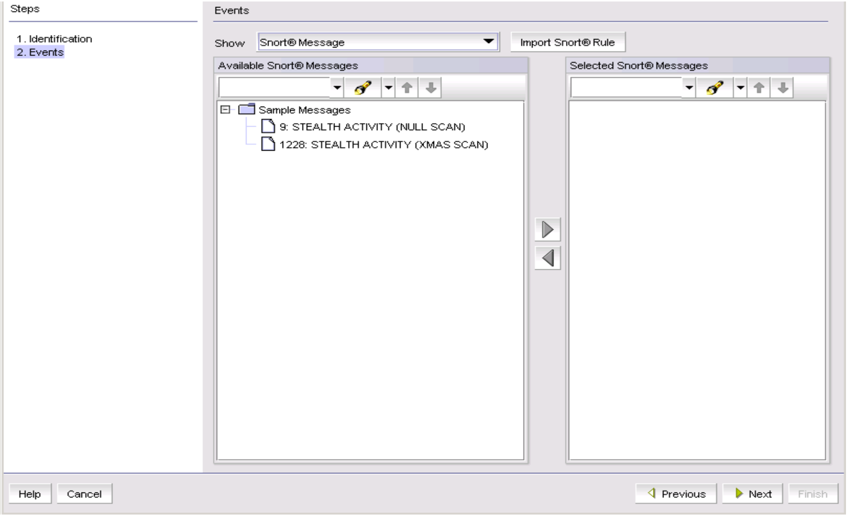
Snort is a third-party tool that monitors network traffic in real time. When Snort detects dangerous payloads or other abnormal behavior, it sends an alert to Syslog in real time. You can turn Snort messages on or off using the **Add Syslog Filter** dialog box

By default, the Forward Snort© Messages feature is not enabled. You must enable it to have Snort messages forwarded to the configured Syslog destinations.

To forward Snort messages, complete the following steps:

1. In the **Add Syslog Filter** dialog box, click the **Forward Snort® Messages** check box (see step 8 in "Adding a syslog filter" on page 846).
2. From the **Identification** pane of the **Add Event Action** dialog box, click **Next** to advance to the **Events** pane. See "Creating an event action definition" on page 847 for complete instructions on event actions.

   The **Events** pane of the **Add Event Action** dialog box displays, as shown in Figure 375. Snort® Message is the default in the **Show** list.



9: STEALTH ACTIVITY (NULL SCAN)
1228: STEALTH ACTIVITY (XMAS SCAN)

FIGURE 375 Events pane of the Add Event Action dialog box

3. Click the **Import Snort® Rule** button.

   The **Import Snort® Rule File** dialog box displays, as shown in Figure 376.

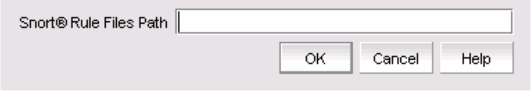


FIGURE 376 Import Snort® Rule File dialog box

4. Enter the complete path of the Snort rule file located on the Syslog server.
5. Click **OK** to import the Snort rules.
6. While still in the **Add Event Action** dialog box, continue to click **Next** until you advance to the **Action Group - Actions** pane.
7. Select the **Deploy CLI Configuration** check box and click **Configure** if you want to deploy a configuration from CLI Configuration Manager to products if the policy criteria have been met. You can only deploy a CLI configuration for IP products.

NOTE
If the CLI configuration you chose from CLI Configuration Manager contains a non-Brocade product as a target, the configuration will not be deployed to the non-Brocade product.

8. Select one of the following existing CLI configuration parameter sources from the Parameter list:
   - Source IP — the source IP address of the attack.
   - Source Port — the source port of the attack.
   - Destination IP — the destination IP address of the attack.
   - Destination Port — the destination port of the attack.
9. Continue to advance through the Add Event Action dialog box. The **Summary** pane of the **Edit Event Action** dialog box displays an overview of the e-mail configuration you are creating.
10. Review your entries and take one of the following actions:
    - Click **Finish** to approve the configuration.
    - Click **Previous** to return to the **Action Group - E-mail Settings** pane of the dialog box.
    - Click **Cancel** to cancel the operation.

Pseudo events

A pseudo event is a combination of different SNMP traps that you decide would constitute a single event. For example, there are two separate SNMP traps for link up and link down occurrences. You might decide that these two occurrences should be just one event.

Displaying pseudo event definitions

Perform the following steps to display the properties of a pseudo event.

1. Select **Monitor** > **Event Processing** > **Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 377, displays.

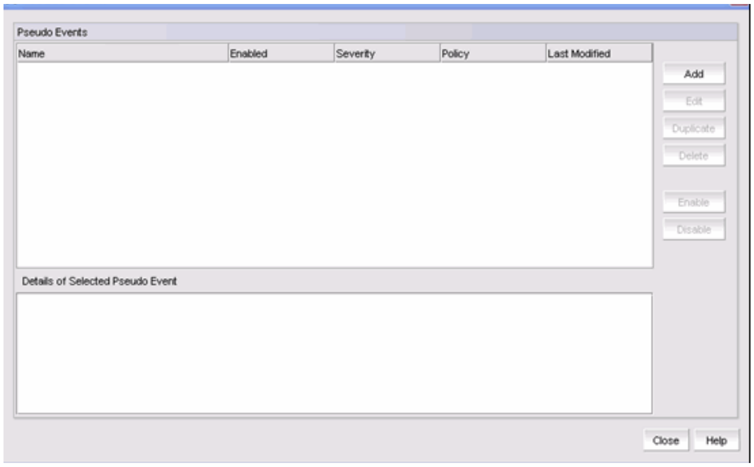


FIGURE 377 Pseudo Events dialog box

2. To view additional information for a definition, select a definition from the list. Additional information displays in the **Details of Selected Pseudo Event** list at the bottom of the dialog box.

Creating pseudo event definitions

Perform the following steps to create a pseudo event.

1. Select **Monitor** > **Event Processing** > **Pseudo Events**.

   The **Pseudo Events** dialog box displays.

2. Click **Add**.
3. The **Identification** pane of the **Add Pseudo Event** dialog box displays.
4. Type a unique name for the pseudo event. Duplicate names are not allowed.
5. Select the check box to enable the pseudo event or clear the check box to disable the pseudo event.
6. Click **Next**.

   The **Policy** pane of the **Add Pseudo Event** dialog box, shown in Figure 378, displays.

Setting pseudo event policies

The **Policy** pane of the **Add Pseudo Event** dialog box is displayed in Figure 378.

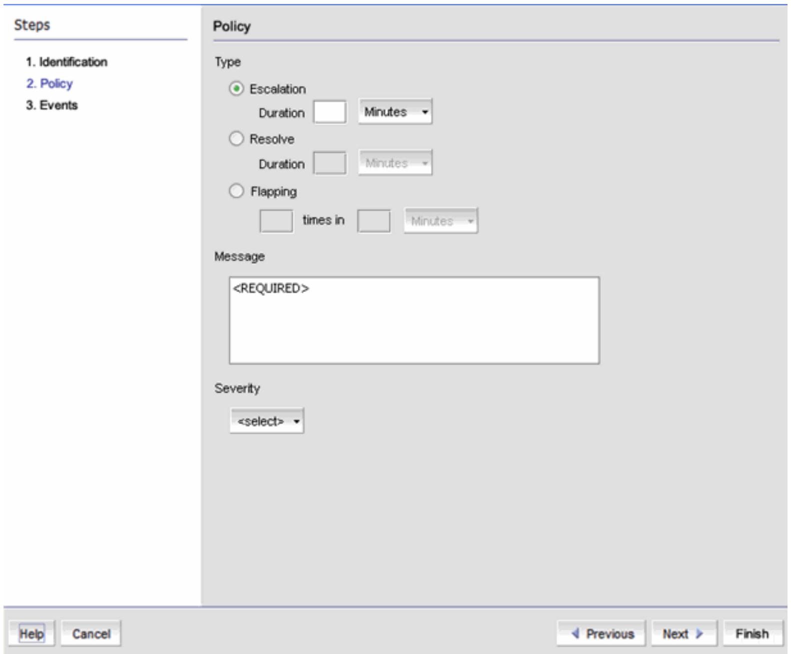


FIGURE 378 Policy pane of the Add Pseudo Event dialog box

1. Click the **Escalation** button to create an escalation policy, and then enter the duration of time that the Management application waits before performing the specified action. Specify the escalation time in minutes or hours.

   When an event occurs, an escalation policy waits for a duration of time to see if the event remains in that state. If it does, then the specified action in the definition is performed.

   Refer to "Adding a pseudo event on the escalation policy" on page 866 for complete instructions.

2. Click the **Resolve** button to create a resolve policy, and then enter the duration of time the Event Processor waits before generating the pseudo event. Specify the resolve time in minutes or hours.

   When a down event occurs, a resolving policy waits for a duration to see if the events remain in that state. If the event does remain in the down state, a resolving pseudo event is generated by the Event Processor.

   Refer to "Creating an event action with a pseudo event on the resolving policy" on page 869 for complete instructions.

3. Click the **Flapping** button to create a flapping policy, and then enter the number of occurrences and the duration of time before the Management application performs the action specified in an event action. Specify the number of flapping times in minutes or hours.

   The flapping policy checks to see if the event consistently transitions between two opposite states during a specified length of time. If it does, then the specified action in the definition is performed.

Refer to “Creating an event action with a pseudo event on the flapping policy” on page 870 for complete instructions.

4. Enter a description in the **Message** field. This description is displayed in the event log for this pseudo event.The event log displays the exact text you enter in this field; therefore, this message should describe the events in the event action policy.
5. Select a severity from **Severity** list. You must assign a severity to the pseudo event.
6. Click **Next**.

   The **Events** pane of the **Add Pseudo Event** dialog box, shown in Figure 379, displays.

Filtering pseudo event traps

The **Events** pane contains a **Selected Down Trap** list and a **Selected Up Trap** list. The **Selected Down Trap** list defines the traps for the down state of a product or an interface. The **Selected Up Trap** list defines the traps for the up state of the product or an interface.

1. Select **Monitor > Event Processing > Pseudo Events.**

   The **Pseudo Events** dialog box displays.
2. Click **Add.**

   The **Events** pane of the **Add Pseudo Event** dialog box is shown in Figure 379.
3. Click **Next** to navigate to the Events pane.

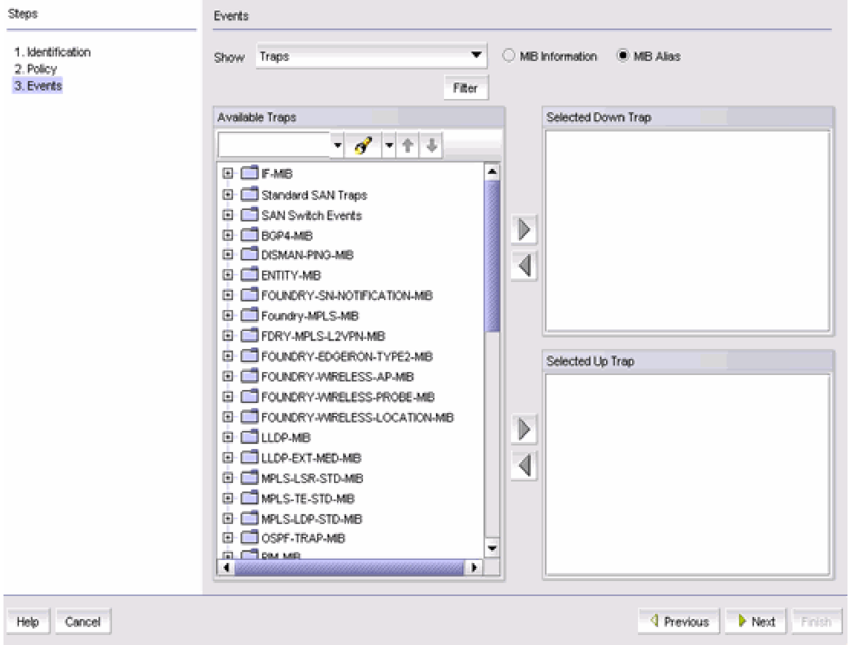


FIGURE 379 Events pane of the Add Pseudo Event dialog box

4. From the **Available Traps** list, select the trap for the down state of a product or interface.
5. You can change the text associated with the selected trap by doing any of the following:

- Click one of the following buttons:
  - **MIB Information**, if you want the default SNMP name for the traps to be displayed.
  - **MIB Alias**, if you want the aliases for the traps to be displayed.
- Use the Trap Filter tool to limit the trap severity. To use this tool, click the **Filter** button to display the **Trap Filters** dialog box.

6. After limiting the list of available traps, expand the MIB folder to which the trap you want belongs under the **Available Traps** list, or right-click to select that trap. Click the right arrow button to move it to the **Selected Traps** list.

7. Select a trap for the up state of the condition. (Follow step 6 through step 9.)

NOTE
You must select a down and an up trap. You cannot select the same trap for the up and down conditions.

8. Click **Next** to advance to the **Summary** pane.

9. Click **Finish** to save your definition. The new pseudo event appears on the **Pseudo Event** list on the **Pseudo Event** dialog box.

Creating a pseudo event definition by copying an existing definition

You can create a pseudo event definition by copying an existing definition. Perform the following steps.

1. Select **Monitor** > **Event Processing** > **Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 377, displays.

2. Select the pseudo event definition that you want to copy from the **Pseudo Events** list.

   Click the **Duplicate** button to display the **Duplicate Pseudo Event** dialog box.

   The name of the event action is the name of the selected action with the word “copy” appended. For example, Event1 becomes Event1 copy.

3. Enter a new name for the pseudo event definition.

4. Make the changes you want to make to the definition. Refer to “Creating pseudo event definitions” on page 862 for details.

5. Click **Finish** to save your definition.

Editing a pseudo event definition

Use caution when you modify pseudo events. Saving changes to a pseudo event definition resets the run-time information for that pseudo event.

1. Select **Monitor** > **Event Processing** > **Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 377, displays.

2. Select the pseudo event definition that you want to edit from the **Pseudo Events** list.
3. Click the **Edit** button to display the **Edit Pseudo Event** dialog box.
4. Make the changes you want to make to the definition. Refer to "Creating pseudo event definitions" on page 862 for details.
5. Click **Finish** to save your definition.

Deleting a pseudo event

Use caution when you delete pseudo events. Deleting a pseudo event definition discards the run-time information for that pseudo event.

1. Select **Monitor** > **Event Processing** > **Pseudo Events**.

   The **Pseudo Events** dialog box, shown in Figure 377, displays.

2. Select the pseudo event definition that you want to delete from the **Pseudo Events** list.
3. Click **Delete**.

   A message displays, prompting you to confirm the deletion request.

4. Click **Yes** to delete the selected definition.

   The definition is removed from the Pseudo Events list.

Adding a pseudo event on the escalation policy

Use the escalation policy to be notified if a critical event occurs on a product, port, or system. When the event occurs, the escalation policy waits for a duration of time to see if the event remains in that state. If it does, then the specified action in the definition is performed.

The following two-part procedure uses both the **Identification** pane of the **Add Pseudo Events** dialog box and the **Add Event Actions** dialog box to create an event action with the escalation policy.

1. Select **Monitor** > **Event Processing** > **Pseudo Events**.

   The **Pseudo Events** dialog box displays.

2. Click **Add**.

   The **Add Pseudo Event Identification** dialog box displays.

3. Enter a name and description for the pseudo event.
4. Click the **Enabled** check box to enable the event, and click **Next**.

   The **Policy** pane of the **Add Pseudo Event Policy** dialog box displays.

5. Click the **Escalation** button, and then enter the duration of time the Event Processor will wait before generating the pseudo event. Specify the escalation time in minutes or hours.

6. Click **Next**.

   The **Events** pane of the Add Pseudo **Event** dialog box displays.

7. Select a critical event, such as LinkDown, and click the right arrow button to move it to the **Selected Down Trap** list.
8. Select a remediation event, such as LinkUp, and click the right arrow button to move it to the **Selected Up Trap** list.
9. Click **Next** to advance to the **Summary** pane.
10. Click **Finish** to complete the pseudo event configuration.

    Now, you must create a new event action definition using the **Add Event Actions** dialog box.

Creating an event action with a pseudo event on the escalation policy

1. Select **Monitor > Event Processing > Event Actions.**

   The **Event Actions** dialog box displays.

2. Click **Add** to display the **Identification** pane of the **Add Event Action** dialog box.
3. Enter a name and description for the event action and click the **Enabled** check box to enable the event.
4. Click **Next** to display the **Events** pane.

   By default, the **Events** pane of the **Add Event Action** dialog box displays.

5. Select the **Pseudo Events** event type from the **Show** list.

   The available pseudo events display.

6. Select the pseudo event you created and click **Next.**

   The **Sources** pane of the **Add Event Action** dialog box displays.

7. Select the source that you will use to monitor this event from the **Selected Sources** list.
8. Click **Next** to advance to the **Policy** pane of the **Add Event Action** dialog box.

   The **Policy** pane of the **Add Event Action** dialog box displays.

9. Click the **Act on all occurrences** button if you want the action to be triggered each time the selected events occur.
10. Click **Next** to advance to the **Action Group-Actions** pane of the **Edit Event Action** dialog box.

    The **Action Group-Actions** pane of the **Edit Event Action** dialog box displays.

11. Select the **Alert by E-mail** check box. An e-mail notification will be sent to the designated e-mail recipient if the policy criteria have been met.
12. Click **Next** to display the **Action Group - Email Settings** pane of the **Add Event Action** dialog box.

    The **Action Group - Email Settings** pane of the **Add Event Action** dialog box allows you to select e-mail recipients from a list, add new e-mail recipients, and compose e-mail messages.

13. Select the Management application user to whom the e-mail message will be sent from the **Available Recipients** list, and click the right arrow button to move the recipient to the **Selected Recipients** list.

NOTE
Make sure the user you select has an e-mail address defined in a user account.

14. Add additional e-mail recipient addresses in the **Other Recipients** field. Separate multiple e-mail addresses with a semicolon.
15. If you want the e-mail message for the alert to display a description on the subject line, enter the text in the **Subject Line** field.
16. If you want a prologue to be inserted at the beginning of the e-mail message, enter up to 255 characters in the **Body Prologue** field. The event action message follows the prologue.
17. If you want an epilogue to be placed at the end of the e-mail message, enter up to 255 characters in the **Body Epilogue** field.

NOTE
NOTE: The prologue, the event action message, and the epilogue form the body of the e-mail alert.

18. Click **Next** to advance to the **Summary** pane.
19. Click **Finish**.

    The **Summary** pane of the **Edit Event Action** dialog box displays an overview of the e-mail configuration you are creating.

For more information about adding an event action, refer to "Event action definitions" on page 847.

Adding a pseudo event on the resolving policy

When a down event occurs, a resolving policy waits for a specified duration to see if the events remain in that state. If the event does remain in the Down state, a resolving pseudo event is generated by the Event Processor.

The following two-part procedure uses both the **Add Pseudo Events** dialog box and the **Add Event Actions** dialog box to create an event action with the resolving policy.

1. Select **Monitor > Event Processing > Pseudo Events.**

    The **Pseudo Events** dialog box displays.

2. Click **Add**.

    The **Identification** pane of the **Add Pseudo Event** dialog box displays.

3. Enter a name and description for the pseudo event, and click the **Enabled** check box to enable the event.
4. Click **Next.**

    The **Policy** pane of the **Add Pseudo Event** dialog box displays.

5. Click the **Resolve** button, and then enter the duration of time the Event Processor will wait before generating the pseudo event. Specify the resolve time in minutes or hours.

6. Click **Next**.

   The **Events** pane of the **Add Pseudo Event Events** dialog box displays.

7. Select a critical event, such as LinkDown, and click the right arrow button to move it to the **Selected Down Trap** list.

8. Select a remediation event, such as LinkUp, and click the right arrow button to move it to the **Selected Up Trap** list.

9. Click **Finish** to complete the pseudo event configuration.

   Now, you must create a new event action definition using the **Add Event Actions** dialog box.

Creating an event action with a pseudo event on the resolving policy

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.

2. Click **Add** to display the **Identification** pane of the **Add Event Action** dialog box.

3. Enter a name and description for the event action and click the **Enabled** check box to enable the event.

4. Click **Next** to display the **Events** pane.

   By default, the **Events** pane of the **Add Event Action** dialog box displays.

5. Select the **Pseudo Events** event type from the **Show** list.

   The available pseudo events display.

6. Select the pseudo event you created and click **Next**.

   The **Sources** pane of the **Add Event Action** dialog box displays.

7. Select the source that you will use to monitor this event from the **Selected Sources** list.

8. Click **Next** to advance to the **Policy** pane of the **Event Action** dialog box.

   The **Policy** pane of the **Event Action** dialog box displays.

9. Define the frequency of the event's occurrence that would trigger the action.

   - Click the **Act on all occurrences** button if you want the action to be triggered each time the selected events occur.
   - Click the **Act as specified** button if you want the action to be triggered only when the occurrence of the event meets the specified criteria.

10. Click **Next** to advance to the **Action Group-Actions** pane of the **Edit Event Action** dialog box.

    The **Action Group-Actions** pane of the **Edit Event Action** dialog box displays.

11. Select **Apply as a Logging Policy** to indicate whether or not you want the event occurrence to be logged in the Management application database:

    - Select **Log** to log the occurrence in the Management application database.
    - Select **Drop** to not log the occurrence in the Management application database.

12. Click **Next** to advance to the **Summary** pane.
13. Click **Finish**.

For more information about adding an event action, refer to “Event action definitions” on page 847.

Adding a pseudo event on the flapping policy

The flapping policy checks to see if the event consistently transitions between two opposite states during a specified length of time. If it does, then the specified action in the definition is performed.

The following two-part procedure uses both the **Add Pseudo Events** dialog box and the **Add Event Actions** dialog box to create an event action with the flapping policy.

1. Select **Monitor > Event Processing > Pseudo Events**.

   The **Pseudo Events** dialog box displays.
2. Click **Add**.

   The **Identification** pane of the **Add Pseudo Event** dialog box displays.
3. Enter a name and description for the pseudo event, and click the **Enabled** check box to enable the event.
4. Click **Next**.

   The **Policy** pane of the **Add Pseudo Event** dialog box displays.
5. Click the **Flapping** button, and then enter the duration of time the Event Processor will wait before generating the pseudo event. Specify the number of flapping times in minutes or hours.
6. Click **Next**.

   The **Events** pane of the Add **Pseudo Event** dialog box displays.
7. Select a critical event, such as LinkDown, and click the right arrow button to move it to the **Selected Down Trap** list.
8. Select a remediation event, such as LinkUp, and click the right arrow button to move it to the **Selected Up Trap** list.
9. Click **Next** to advance to the **Summary** pane.
10. Click **Finish** to complete the pseudo event configuration.

    Now, you must create a new event action definition using the **Add Event Actions** dialog box.

Creating an event action with a pseudo event on the flapping policy

1. Select **Monitor > Event Processing > Event Actions**.

   The **Event Actions** dialog box displays.
2. Click **Add** to display the **Identification** pane of the **Add Event Action** dialog box.
3. Enter a name and description for the event action and click the **Enabled** check box to enable the event.
4. Click **Next** to display the **Events** pane.

   By default, the **Add Event Action - Traps** dialog box displays.

5. Select the **Pseudo Events** event type from the **Show** list.

   The available pseudo events display.

6. Select the pseudo event you created in step 1 through step 10, and click **Next**.

   The **Sources** pane of the **Add Event Action** dialog box displays.

7. Select the source that you will use to monitor this event from the **Selected Sources** list.

8. Click **Next** to advance to the **Policy** pane of the **Add Event Action** dialog box.

   The **Policy** pane of the **Add Event Action** dialog box displays.

9. Click the **Act on all occurrences** button if you want the action to be triggered each time the selected events occur.

10. Click **Next** to advance to the **Action Group-Actions** pane of the **Edit Event Action** dialog box.

    The **Action Group-Actions** pane of the **Edit Event Action** dialog box displays.

11. Select the **Deploy CLI Configuration** check box and click the **Configure** button if you want to deploy a configuration from CLI Configuration Manager to products if the policy criteria have been met.

    NOTE
    If the CLI configuration you chose from CLI Configuration Manager contains a non-Brocade as a target, the configuration will not be deployed to the non-Brocade product.

12. You can either select an existing CLI configuration or create a new one and select that configuration. After selecting a CLI configuration, the name of the CLI configuration is displayed in the **Selected Configuration** field.

    - **Has Parameters** - Displays **Yes** if the CLI configuration has parameters that require values to be entered before it can be deployed, and displays **No** if no parameter needs to be defined.
    - The **Parameters** list lists the parameters that need to be defined in the configuration.
      - The **Parameter** column displays the parameter and its variables in the CLI configuration.
      - The **Source** column lists the appropriate SNMP attributes for the parameters. Each attribute contains a specific parameter value, such as an IP address. Select the attribute you want from the list.
      - The **Transformation** column uses the product IP addresses and MAC addresses listed in the Address Finder. If the Address Finder list is empty, the product or port will not be found. From this column, specify what you want Event Processor to do with the value in the attribute:

        Find Device: Find the product with the IP address in the attribute and deploy the CLI configuration to that product.

        Find Port: Find the port on a product with the IP address in the attribute and deploy the CLI configuration to that port.

        Find Intruder MAC: Find the product with the IP address in the attribute that matches the intruder MAC address and deploy the CLI configuration to that product.

        None: The Event Processor only reports occurrence of the products.

13. Select the **Deploy Product Configuration** check box if you want to deploy a payload from the Configuration dialog box to the products if the policy criteria have been met.

14. Select the **Apply as a Logging Policy** check box to indicate whether or not you want the event occurrence to be logged in the Management application database:
    - Select **Log** to log the occurrence in the Management application database.
    - Select **Drop** to not log the occurrence in the Management application database.
15. Click **Next** to advance to the **Summary** pane.
16. Click **Finish**.

For more information about adding an event action, refer to "Event action definitions" on page 847.

Event custom reports

The **Event Custom Reports** dialog box allows you to manage customized event filter definitions and schedule when the definitions are run.

To access the dialog box, select **Reports > Event Custom Reports**.

The **Event Custom Reports** dialog box, shown in Figure 380, displays.

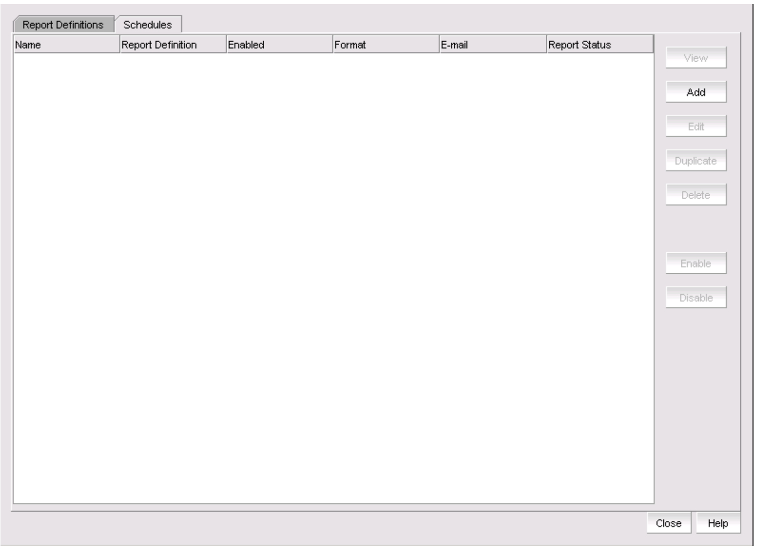


FIGURE 380 Event Custom Reports dialog box - Report Definitions tab

The **Event Custom Reports** dialog box has two tabs.

- The **Report Definitions** tab lists all the previously created report definition objects. This tab enables you to add a new definition or modify, delete, or duplicate existing report definitions.
- The **Schedules** tab lists all the previously created schedules on the report definition. This tab enables you to add a new schedule or modify, delete, or duplicate existing schedules. Users cannot view, edit, or share a schedule that was created by another user.

Defining report settings

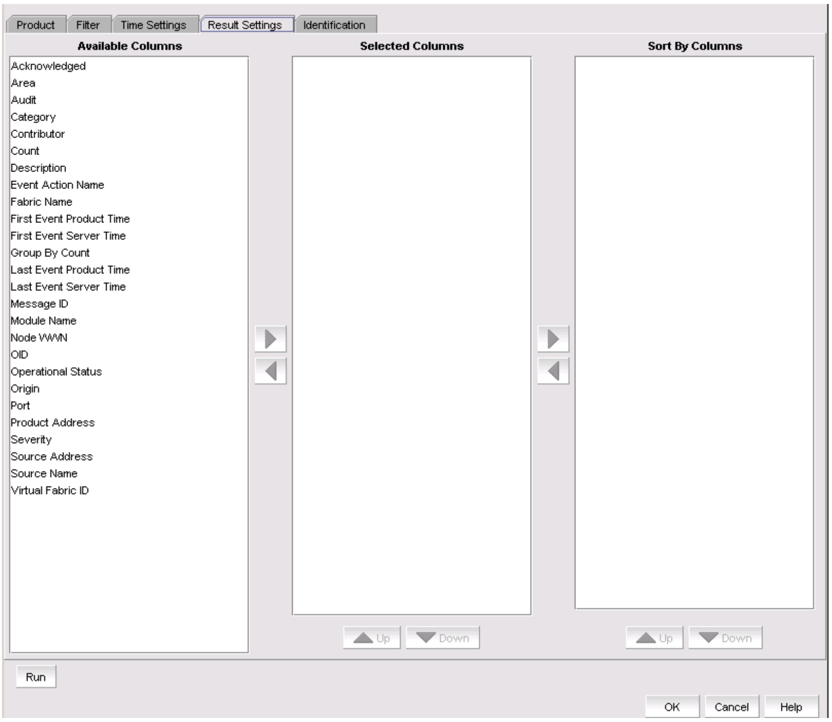
Complete the following steps to define report settings. You must first enter a name and title on the Identification tab before you can run the result settings.

1. Select Reports > Event Custom Reports.

   The Event Custom Reports dialog box displays.

2. Click the Add button.
3. The Add/Edit Report Definition dialog box - Product tab displays.
4. Click the Result Settings tab.

   The Add/Edit Report Definition dialog box - Result Settings tab displays.



Acknowledged
Area
Audit
Category
Contributor
Count
Description
Event Action Name
Fabric Name
First Event Product Time
First Event Server Time
Group By Count
Last Event Product Time
Last Event Server Time
Message ID
Module Name
Node WWN
OID
Operational Status
Origin
Port
Product Address
Severity
Source Address
Source Name
Virtual Fabric ID

FIGURE 381 Add/Edit Report Definition dialog box - Result Settings tab

---

NOTE
The Available Column box lists the attributes you can include in the report. Each attribute represents a column on the report.

---

5. Select the attribute you want, then click the right arrow to move your selection to the Selected Columns list. To remove an attribute from the Selected Columns list, select the attribute that you want to remove, then click the left arrow button.

   For products that support stacking, the Port column shows the port.

6. Data for all attributes is sorted in ascending order and is sorted in the sequence that the attributes appear in the **Sort By Columns** list. In the **Selected Columns** list, select which attribute will be used to sort the generated report. Then click the right arrow button to move your selection to the **Sort by Columns** list. To remove an entry from the **Sort by Columns** list, select the entry, then click the left arrow button.
7. Click **OK** to save the definition, **Run** to launch the report, or click the **Identification** tab to display the parameters that you use to identify the definition

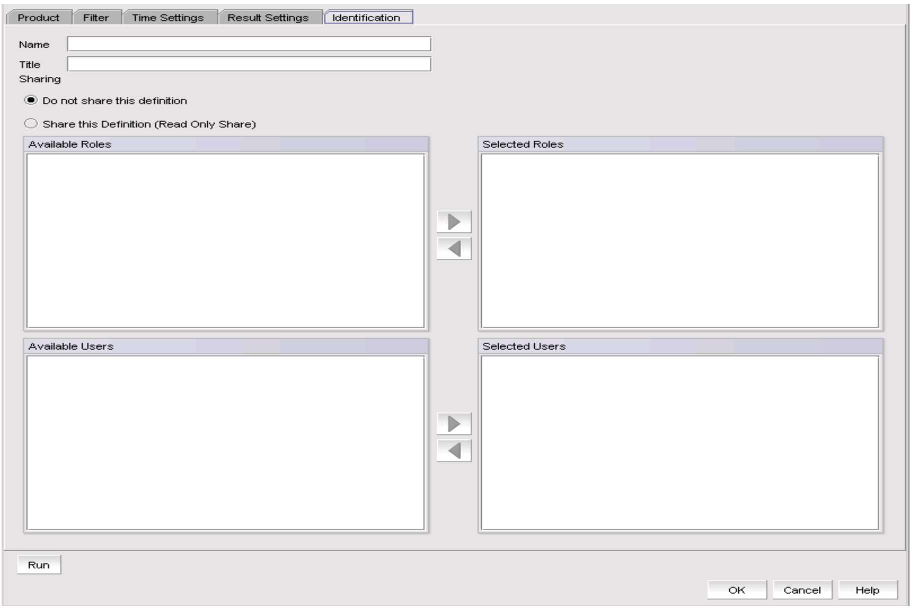
Defining the report identity

Complete the following steps to define the report identity.

1. Select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.
2. Click the **Add** button.
3. The **Add/Edit Report Definition** dialog box - **Product** tab displays.
4. Click the **Identification** tab.

   The **Add/Edit Report Definition dialog box - Identification tab** displays.



● Do not share this definition

○ Share this Definition (Read Only Share)

FIGURE 382 Add/Edit Report Definition dialog box - Identification tab

5. In the **Name** field, enter a name for the definition.

   This name appears under the **Name** column on the **Report Definitions** tab of the **Event Custom Reports** dialog box. This name must be unique. This is a required parameter.
6. In the **Title** field, enter a title for the definition, which will be used as the title of a generated report. This is a required parameter.

7. Click the **Do not share this definition** button if you do not want to share this definition with other Management application users.

   If you select this button, no Management application users will see this definition on the **Report Definitions** tab of the **Event Custom Reports** dialog box when they log in.

8. Click the **Share this definition (Read only)** button if you want other Management application users to have Read Only permission for this definition.

   If you selected the **Share this definition (Read only)** button, a list of Management application roles appears in the **Available Roles** list.

9. Select the roles that will have view and run access to this definition, then press the right arrow button to move the role in the **Selected Roles** list.

   NOTE
   All Management application users who have the selected roles will be able to view, copy, and run the definition.

10. You can share the available users definition with specific Management application users. If you click the **Share this definition (Read only)** button, a list of Management application user accounts appears in the **Available Users** list.

11. Select the user account that will be able to view and run this definition, then press the right arrow button to move that user account in the **Selected Users** list.

12. Click **OK** to save the definition, or click **Run** to launch the report.

Filtering a report definition

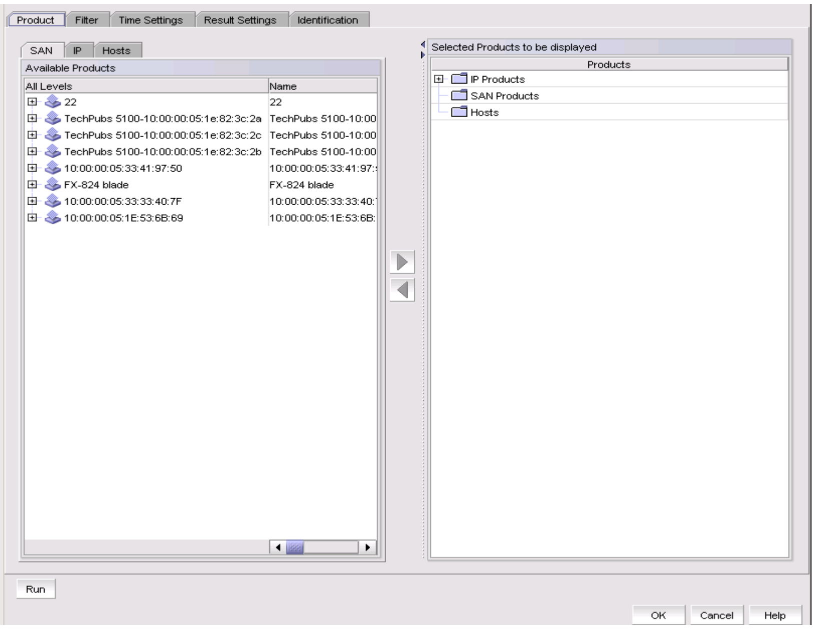
Complete the following steps to filter a report definition. You must first enter a name and title on the **Identification** tab and select at leat one column in the **Results Setting** tab to run or save a filter. You can select from the available list of SAN products, IP products, or Hosts by selecting the appropriate tab.

1. Select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.

2. Click the **Add** button.

3. The **Add/Edit Report Definition** dialog box - **Product** tab, shown in Figure 383, displays.



All Levels	Name
22	22
TechPubs 5100-10:00:00:05:1e:82:3c:2a	TechPubs 5100-10:00
TechPubs 5100-10:00:00:05:1e:82:3c:2c	TechPubs 5100-10:00
TechPubs 5100-10:00:00:05:1e:82:3c:2b	TechPubs 5100-10:00
10:00:00:05:33:41:97:50	10:00:00:05:33:41:97:
FX-824 blade	FX-824 blade
10:00:00:05:33:33:40:7F	10:00:00:05:33:33:40:
10:00:00:05:1E:53:6B:69	10:00:00:05:1E:53:6B:

FIGURE 383 Add/Edit Report Definition dialog box - Product Tab

4. Click the **Filter** tab.

   The **Add/Edit Report Definition** dialog box - **Filter** tab, shown in Figure 384, displays.

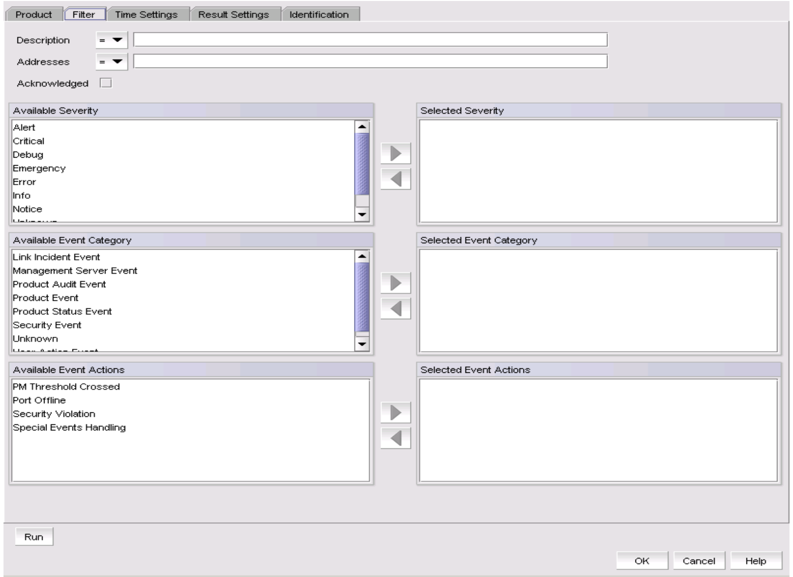


FIGURE 384 Add/Edit Report Definition dialog box - Filter tab

5. To limit the search results to traps, syslog, and pseudo event messages with a specific text string, enter the text string in the **Description** field.

6. To limit the search results to traps, syslog, and pseudo event messages from a specific IP address, enter the IP address in the **Addresses** field. You can enter multiple IP addresses. Separate each address with a comma.

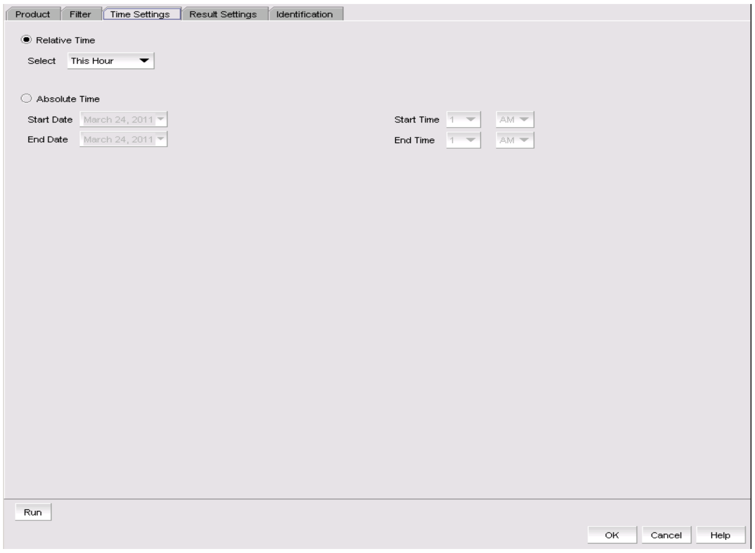
7. Select the **Acknowledge** check box if you want messages that have been acknowledged to be included in the report.
8. Select the severity from the **Available Severity** list, and click the right arrow button to move your selection to the **Selected Severity** list. Events with the selected severity are included in the report.
9. Select the event type you want to include in the report from the **Available Event Category** list. Click the right arrow button to move your selection to the **Selected Event Category** list.
10. Select the event action you want to include in the report from the **Available Event Actions** list. Click the right arrow button to move your selection to the **Selected Event Actions** list.
11. Click **OK** to save the definition, **Run** to launch the report, or click the **Time Settings** tab on the **Add/Edit Report Definition** dialog box if you want to filter the events by date and time.

Filtering events by date and time

Complete the following steps to filter events by date and time.

1. Select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.
2. Click the **Add** button.
3. The **Add/Edit Report Definition** dialog box - **Product** tab displays.
4. Click the **Time Settings** tab.



● Relative Time

Select: This Hour

○ Absolute Time

Start Date: March 24, 2011 | Start Time: 1 | AM

End Date: March 24, 2011 | End Time: 1 | AM

FIGURE 385 Add/Edit Report Definition dialog box - Time Settings tab

5. Choose between relative time (the default) and absolute time.
   - Click **Relative Time** if you want to filter traffic based on when the report is generated, and then select a relative time from the **Range** list. Relative time is calculated based on the date and time the report is generated.
   - Click **Absolute Time** if you want to filter traffic sent at a specific date and time.
     a. Select the specific start date from the **Start Date** list.
     b. Select the specific hour time from the **Start Time** list, and select AM or PM.
     c. Select the specific end date from the **End Date** list.
     d. Select the specific hour for the end time from the **End Time** list, and select AM or PM.
6. Click **OK** to save the definition, **Run** to launch the report.

Creating a new definition by copying an existing definition

Perform the following steps to copy an existing definition.

1. Select the definition you want to copy from the **Report Definitions** tab of the **Event Custom Reports** dialog box.
2. Click **Duplicate.**

   The name of the definition is the name of the selected definition with the word "copy" appended. For example, SelectedPortName becomes SelectedPortName copy.
3. Click the **Identification** tab to enter a new name and description for the new definition.
4. Make changes to the report as required.
5. Perform one of the following tasks when you are finished modifying the definition:
   - Click **OK** to save the report.
   - Click **Cancel** to discard your changes and exit from the **Report Definitions** tab of the **Event Custom Reports** dialog box.
   - Click **Reset** to discard your changes without exiting from the **Report Definitions** tab of the **Event Custom Reports** dialog box.
   - Click **Run** to launch the report.

The new definition is added to the **Report Definitions** tab of the **Event Custom Reports** dialog box.

Editing a report definition

For your definitions, you can modify the definition and save the changes you have made. For a shared definition from another user, you can modify the definition, then run that definition to obtain the desired report; however, you will not be able to save your changes. Complete the following steps to edit a definition.

1. Click the **Report Definitions** tab and select the definition you want to modify.
2. Click **Edit**.
3. When the **Add/Edit Report Definition** dialog box displays, modify the definition. (Refer to "Filtering a report definition" on page 875.)
4. When you have finished, perform one of the following tasks:
   - If you own this definition, the **OK** button is available. Click **OK** to save your changes.
   - Click **Run** to generate the report.
   - Click **Cancel** to discard your changes and exit the **Report Definitions** tab of the **Event Custom Reports** dialog box.

Deleting a report definition

You can delete a definition if it belongs to your user. Perform the following steps to delete a definition.

1. To access the dialog box, select **Reports > Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.
2. Click the **Report Definitions** tab of the **Event Custom Reports** dialog box and select the definition you want to delete.
3. Click the **Delete** button.

   A message displays, prompting you to confirm the deletion.
4. Click **Yes** to delete the definition or **No** to cancel your request.

Event custom report schedules

Click the **Schedules** tab, shown in Figure 386, to display its contents. The **Schedules** list shows the definitions that have been scheduled to automatically run at a specified date and time.

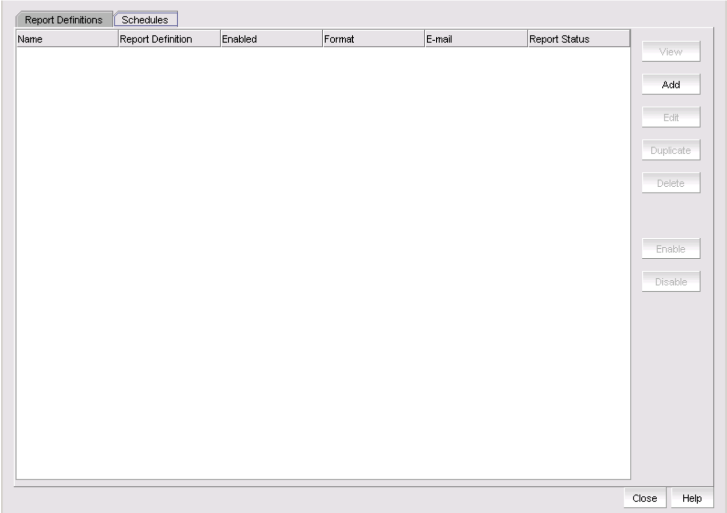


FIGURE 386 Schedules tab of the Event Custom Report dialog box

From the **Schedules** tab of the **Event Custom Reports** dialog box, you can perform the following tasks:

- **View**—Displays the report data of the scheduled report definition. The **View** button is not enabled for a report that is listed as Not Available.
- **Add**—Launches the **Add Schedule** dialog box.
- **Edit**—Launches the **Edit Schedule** dialog box with the selected schedule information pre-populated.
- **Duplicate**—Creates a copy of the selected report schedule.
- **Delete**—Deletes the selected schedule from the **Schedules** list.
- **Enable**—Enables the selected schedule.
- **Disable**—Disables the selected schedule.

Adding an event report schedule

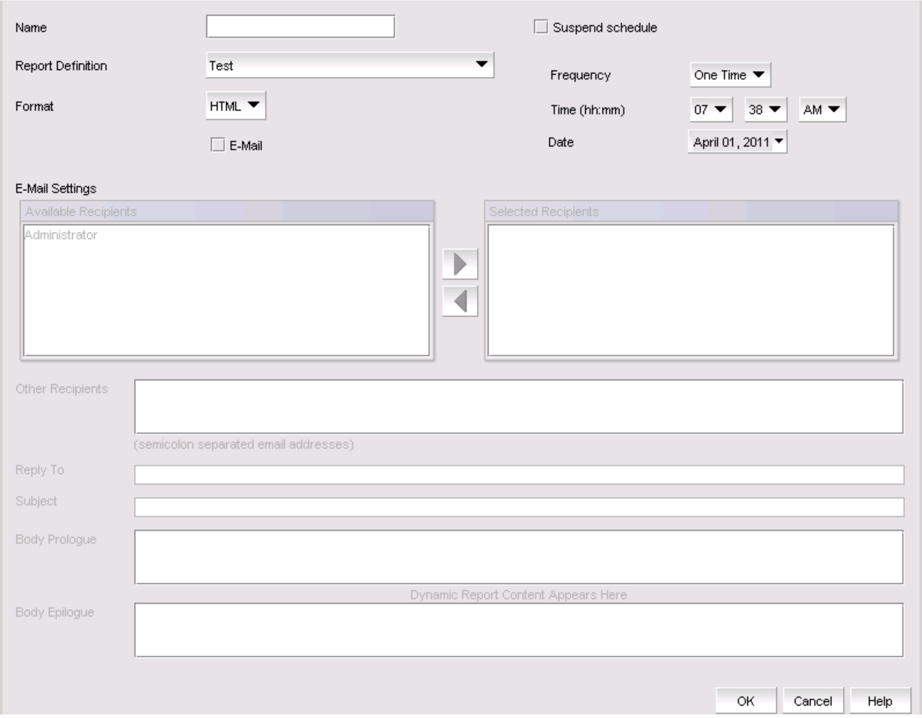
The **Add Schedule** dialog box, shown in Figure 387, allows you to select an existing report definition and configure the parameters for when the report is run and to whom the report is sent.

1. Select **Reports** > **Event Custom Reports**.

   The **Event Custom Reports** dialog box displays.

2. Click the **Schedules** tab.
3. Click the **Add** button.

   The **Add Schedule** dialog box displays.



Name

Report Definition: Test

Format: HTML

□ E-Mail

□ Suspend schedule

Frequency: One Time

Time (hh:mm): 07 38 AM

Date: April 01, 2011

E-Mail Settings

Available Recipients

Administrator

Selected Recipients

Other Recipients

(semicolon separated email addresses)

Reply To

Subject

Body Prologue

Dynamic Report Content Appears Here

Body Epilogue

FIGURE 387 Add Schedule dialog box

4. Enter the name of the new schedule in the **Name** field. You must enter a unique name for the schedule. The name can be up to 64 characters in length and it is case-sensitive.
5. Select the **Suspend schedule** check box if you want to disable the schedule. For example, you may want to temporarily prevent a report from being generated until further notice. You can clear the check mark to resume the automatic generation of the report.
6. Select the report definition you want to schedule from the **Report Definition** list. If a report is deleted, the corresponding schedule will be deleted.
7. Select one of the following periods from the **Frequency** list:
   - One Time
   - **Hourly**—If you selected **Hourly** as the schedule type, **Minutes past the hour** appears. Select the minutes after the hour when the definition report will be generated.
   - Daily—If you selected Daily as the schedule type,Time (hh:mm) appears.

- **Weekly**—If you selected **Weekly** as the schedule type, **Day of the week** appears. Select the day of the week when the report will be generated.
- **Monthly**—If you selected **Monthly** as the schedule type, **Day of the month** appears. Select the day of the month when the report will be generated.
- Yearly

8. Select a report format from the **Format** list: HTML or CSV.
9. Select the time when the report will be generated. Indicate the hour, minute, and whether it is AM or PM. This parameter appears if you selected any schedule type except **Hourly.**
10. Select the **E-mail** check box if you want the report to be sent to e-mail recipients. The server limits the displayed or sent report to 1000 records.
11. Indicate the date when the report is generated. Open the calendar and select the date. This parameter appears if you selected **One Time** or **Yearly** as the schedule type.
12. Enter an e-mail address to which the e-mail recipient can send a response. This is a mandatory field.
13. Select the user to whom the report will be sent. Click the right arrow button to move that user name to the **Selected Recipients** list. Click the left arrow button to remove the name from the **Selected Recipients** list and return it to the **Available Recipients** list.

NOTE
Make sure an e-mail address is configured in the user's account for the selected user.

14. Enter other e-mail addresses to which the report should be sent in the **Other Recipients** field, separating multiple addresses with a semicolon. At least one from the Application Recipients or Other Recipients must be entered.
15. In the **Subject Line** field, enter the text that you want to appear in the subject line of the e-mail message. You can leave this field empty.
16. If you want introductory text to be included at the beginning of the e-mail message, enter the text in the **Body Prologue** field.   The maximum number of character supported by the **Body Prologue** field is 256.

Event logs

You can view all events that take place 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 logs are described in the following list:

- **Audit Log.** Displays all 'Application Events' raised by the application modules and all Audit Syslog messages from the switches and Brocade HBAs.
- **Product Event Log.** Displays all 'Product Event' type events from all discovered switches and Brocade HBAs.
- **Fabric Log.** (SAN only) Displays 'Product Events', 'Device Status', and 'Product Audit' type events for all discovered fabrics.
- **FICON Log.** Displays all the 'RLIR' and 'LRIR' type events, for example, 'link incident' type events.
- **Product Status Log.** (SAN only) Displays events which indicate a change in Switch Status for all discovered switches and Brocade HBAs.
- **Security Log.** Displays all security events for the discovered switches.
- **Syslog Log.** Displays syslog messages from switches and HBAs.

The Management application also has an event notification feature. By configuring event notification, you can specify when the application should alert you of an event. For details, refer to "Configuring e-mail notification" on page 824.

For information about the Master Log interface, fields, and icons, refer to "Master Log" on page 14.

Viewing event 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 security events, open a specific log through the **Logs** dialog box.

NOTE
You can also launch the Fabric logs and the Product Status logs from the Status bar.

To view a log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Logs** dialog box displays the kind of log you selected.

2. Review the information in the log.
3. Click **Close.**

Copying part of a log entry

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy part of a log, complete the following steps.

1. Select **Monitor > Logs >** *<Log_Type>*.

   The *<Log_Type>* **Logs** dialog box displays the kind of log you selected.

2. Select the rows you want to copy.
   - To select contiguous rows, select the first row you want to copy, press Shift, and click the contiguous row or rows you want to copy.
   - To select non-contiguous rows, select the first row you want to copy, press CTRL, and click the additional row or rows you want to copy.
3. Right-click one of the selected rows and select **Copy Rows**.
4. Open the application to which you want to paste the data.
5. Click where you want to paste the data.
6. Press CTRL+V (or select **Edit > Paste** from the other application).

   All data and column headings are pasted.

7. Click **Close** to close the dialog box.

Copying an entire log entry

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy a log, complete the following steps.

1. Select **Monitor > Logs >** *<Log_Type>*.

   The *<Log_Type>* **Logs** dialog box displays the kind of log you selected.

2. Right-click a row and select **Copy Table**.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press CTRL+V (or select **Edit > Paste** from the other application).

   All data and column headings are pasted.

6. Click **Close** to close the dialog box.

Exporting the entire log

You can export the log data to a tab delimited text file.

To export a log, complete the following steps.

1. Select **Monitor > Logs >** <*Log_Type*>.

   The <*Log_Type*> **Log** dialog box displays the kind of log you selected.

2. Right-click a row and select **Export Table**.

   The **Save table to a tab delimited file** dialog box displays.

3. Browse to the location where you want to export the data.
4. Enter a name for the file in the **File Name** field.
5. Click **Save**.

   All data and column headings are exported to the text file.

6. Click **Close** to close the dialog box.

E-mailing all event details from the Master Log

NOTE
You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to "Configuring e-mail notification" on page 824.

To e-mail event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **E-mail > All.**

   The **E-mail** dialog box displays.

3. Enter the e-mail address of the person to receive the e-mail in the **To** field.
4. Enter your e-mail address in the **From** field.
5. Click **OK.**

E-mailing selected event details from the Master Log

NOTE
You must configure e-mail notification before you can e-mail event details from the Master Log. To configure e-mail notification, refer to "Configuring e-mail notification" on page 824.

To e-mail event details from the Master Log, complete the following steps.

1. Select the events that you want to e-mail.
2. Right-click the selected events in the Master Log.
3. Select **E-mail > Selection.**

   The **E-mail** dialog box displays.

4. Enter the e-mail address of the person to receive the e-mail in the **To** field.

5. Enter your e-mail address in the **From** field.
6. Click **OK**.

Displaying event details from the Master Log

You can view detailed information for an event.

To display event details from the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select **Properties**.

   The **Event Details** dialog box displays.
3. Review the information.

TABLE 50 Event details

Event Field	Description
Count	Number of times this event occurred on the host.
Resolved	Whether or not the event has been resolved.
Message	The message associated with the event.
Time (Switch)	The time the event occurred and the switch on which it occurred.
Probable Cause	The probable cause of the event.
Module Name	The module name.
Source Address	The source address.
Audit	The audit.
Status	The switch operational status.
Severity	The event severity.
Source Name	The source of the event.
Virtual Fabric ID	The virtual fabric identifier.
Message ID	The message text.
Recommended Action	The recommended action.
Contributors	The contributor to this event.
Time (Host)	The time this event occurred and the host on which it occurred.

4. Click **Close** to close the **Event Details** dialog box.

Copying part of the Master Log

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy part of the Master Log, complete the following steps.

1. Select the rows you want to copy in the Master Log.
   - To select contiguous rows, select the first row you want to copy, press Shift, and click the contiguous row or rows you want to copy.
   - To select non-contiguous rows, select the first row you want to copy, press CTRL, and click the additional row or rows you want to copy.
2. Right-click one of the selected rows and select Table > Copy Rows.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press CTRL+V (or select Edit > Paste from the other application).

   All data and column headings are pasted.

Copying the entire Master Log

You can copy data from logs to other applications. Use this to analyze or store the data using another tool.

To copy the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select Table > Copy Table.
3. Open the application to which you want to paste the data.
4. Click where you want to paste the data.
5. Press CTRL+V (or select Edit > Paste from the other application).

   All data and column headings are pasted.

Exporting the Master Log

You can export the Master Log to a tab delimited text file. Use this to analyze or store the data using another tool.

To export the Master Log, complete the following steps.

1. Right-click an entry in the Master Log.
2. Select Table > Export Table.

   The Save table to a tab delimited file dialog box displays.
3. Browse to the location where you want to export the data.
4. Enter a name for the file in the File Name field.

5. Click **Save**.

   All data and column headings are exported to the text file.

6. Click **Close** to close the dialog box.

Filtering events in the Master Log

You can filter the events that display in the Master Log on the main window. By default, all event types display in the **Selected Events** table.

For more information about the Master Log, refer to “Master Log” on page 14.

NOTE
The e-mail filter in the Management application is overridden by the firmware e-mail filter. When the firmware determines that certain events do not receive e-mail notification, an e-mail is not sent for those events even when the event type is added to the **Selected Events** table in the **Define Filter** dialog box.

To filter events, complete the following steps.

1. Click **Filter** in the Master Log.

   The **Define Filter** dialog box displays.

2. Select from the following to include or exclude products.
   - To include an event type in the filter, select the event from the **Available Products** list and click the right arrow.
   - To exclude an event type from the filter, select the event from the **Selected Products to be displayed** list and click the left arrow.

3. Select from the following to include or exclude event types.
   - To include an event type in the filter, select the event category from the **Available Event Category** list and click the right arrow.
   - To exclude an event type from the filter, select the event from the **Selected Event Category and Severity to be displayed** list and click the left arrow.

4. From the **Selected Event Category and Severity to be displayed** list, select one of the following severity levels to assigned to the selected event action:
   - Emergency
   - Alert
   - Critical
   - Errors
   - Warning
   - Notice
   - Info
   - Debug
   - Unknown

   Clear the severity level check boxes to turn off the filter for the selected events.

5. Click **OK**.

Chapter

Technical Support 31

In this chapter

Server and client support save

You can use Technical Support to collect supportSave data for the Management server and clients.

Server Support save data includes:-

- Engineering logs
- Events
- Configuration files
- Operating system-specific information
- Environment information
- Vital CPU, memory, network resources
- Agent and driver logs
- Install logs
- Core files

Client Support save data includes:-

- Client Log Files
- Client data model log

Capturing Server and Client support save data

To capture both server and client support save files, complete the following steps.

1. Select **Monitor** > **Technical Support** > **SupportSave**.

   The **SupportSave** dialog box displays.
2. Select the **Server SupportSave** check box to run supportsave on the server.
3. Enter a file name for the server support save file in the **File Name** field.

   The default file name is DCM-SS-*Time_Stamp*.

4. Select the **Include Database** check box to include the database in the support save and choose one of the following options.

   - Select the **Partial** (Excludes historical performance data and events) option to exclude historical performance data and events from the database capture.
   - Select the **Full** option to capture the entire database.

   Clear the **Include Database** check box to exclude the database in the support save.

5. Select the **Client SupportSave** check box to run supportsave on the client.

6. Enter a file name for the client support save file in the **File Name** field.

   The default file name is DCM-Client-SS-*Time_Stamp*.

7. Click **OK** on the **SupportSave** dialog box.

8. Click **OK** on the message.

   The application generates separate master logs to show the status of the Server and Client Support save collection.

   You cannot change the destination directory for Server and Client support save. Here are the default directories:

   - Server Support save location: Install_Home/support
   - Client Support save location: Install_Home/Management_Application_Name/Server IP/support

   NOTE
   Server support save initiated from the remote client is only available on the server. However, you can copy the server support save from the **View Repository** dialog box (using the **Save** button) to the remote client location.

Capturing Server support save data

To capture server support save files, complete the following steps.

1. Select **Monitor > Technical Support > SupportSave**.

   The **SupportSave** dialog box displays.

2. Select the **Server SupportSave** check box to run supportsave on the server.

3. Make sure the **Client SupportSave** check box is clear.

4. Enter a file name for the server support save file in the **File Name** field.

   The default file name is DCM-SS-*Time_Stamp*.

5. Select the **Include Database** check box to include the database in the support save and choose one of the following options.

   - Select the **Partial** (Excludes historical performance data and events) option to exclude historical performance data and events from the database capture.
   - Select the **Full** option to capture the entire database.

   Clear the **Include Database** check box to exclude the database in the support save.

6. Click **OK** on the **SupportSave** dialog box.
7. Click **OK** on the message.

   The application generates separate master logs to show the status of the Server Support save collection.

Capturing Client support save data

To capture client support save files, complete the following steps.

1. Select **Monitor > Technical Support > SupportSave**.

   The **SupportSave** dialog box displays.
2. Select the **Client SupportSave** check box to run supportsave on the client.
3. Make sure the **Server SupportSave** check box is clear.
4. Enter a file name for the client support save file in the **File Name** field.

   The default file name is DCM-Client-SS-*Time_Stamp*.
5. Click **OK** on the **SupportSave** dialog box.
6. Click **OK** on the message.

   The application generates separate master logs to show the status of the Client Support save collection.

Client support save using a command line interface

Use the following procedures to capture client support save files through the command line interface (CLI).

Capturing client support save using the CLI (Windows)

To capture client support save files through the CLI, complete the following steps.

1. Go to *User_Home*/*Management_Application_Name_Folder*/Server IP.
2. Run the clientsupportsave.bat file.
3. Define a capture location by typing `clientsupportsave` <*path*> in the CLI. If the path has spaces, enclose it in double quotes.

   By default, the capture location is *User_Home*/*Management_Application_Name_Folder*/Server IP/support.
4. Use an archive tool to create a ZIP file of the support save.

Capture client support save using the CLI (Linux)

To capture client support save files through the CLI, complete the following steps.

1. Go to /root /*Management_Application_Name_Folder*/Server IP.
2. Run the clientsupportsave.sh file.

3. Define a capture location by typing `sh clientsupportsave` <*path*> in the CLI. If the path has spaces, enclose it in double quotes.

   By default, the capture location is /root /*Management_Application_Name_Folder*/Server IP/support.

4. Use an archive tool to create a ZIP file of the support save.

Device technical support

You can use Technical Support to collect supportSave data (such as, RASLOG, TRACE and so on) and switch events from Fabric OS devices. You can gather technical data for M-EOS devices using the device's Element Manager.

To gather technical support information for the Management application server, refer to "Capturing technical support information" on page 233.

Scheduling technical support information collection

NOTE
The switch must be running Fabric OS 5.2.X or later to collect technical support data.

NOTE
Scheduling technical support data collection is not supported on Host products.

NOTE
You must have the SupportSave privilege to perform this task.

To capture technical support and event information for specified devices, complete the following steps.

1. Select **Monitor > Technical Support > Product/Host SupportSave**.

   The **Technical SupportSave** dialog box displays.

2. Click the **Schedule** tab.
3. Select the **Enable scheduled Technical Support Data** check box.
4. Select how often you want the scheduled collection to occur from the **Frequency** list.
5. Select the start date for the scheduled collection from the **Start Date** list.

   This list is only available when you select Weekly or Monthly from the **Frequency** list.

6. Select the time you want the scheduled collection to begin from the **Start Time Hour** and **Minute** lists.
7. Right-click in the **Available SAN Products** table and select **Expand All**.
8. Select the switches you want to collect data for in the **Available SAN Products** table and click the right arrow to move them to the **Selected Switches** table.
9. Select how often you want to purge the support data from the **Purge Support Data** list.
10. Click **OK** on the **Technical SupportSave** dialog box.

11. Click **OK** on the confirmation message.

    Technical supportSave dats for SAN devices is saved to the following directory: *Install_Home*\data\ftproot\technicalsupport\

    Technical supportSave uses the following naming convention for the SAN device support save files: Supportinfo-Day-mm-dd-yyyy-hh-mm-ss\Switch_Type-Switch_IP_Address-Switch_WWN.

    Data collection may take 20-30 minutes for each selected switch. This estimate my increase depending on the number of switches selected. Check the Master Log for status information.

Starting immediate technical support information collection

NOTE
The switch must be running Fabric OS 5.2.X or later to collect technical support data.

NOTE
The HBA must be a managed Brocade HBA.

NOTE
You must have the SupportSave privilege to perform this task.

To capture technical support and event information for specified devices, complete the following steps.

1. Select **Monitor > Technical Support > Product/Host SupportSave**.

   The **Technical SupportSave** dialog box displays.

2. Click the **Generate Now** tab, if necessary.
3. Click the **SAN Products** tab, if necessary, and complete the following steps.
   a. Right-click in the **Available SAN Products** table and select **Expand All**.
   b. Select the switches you want to collect data for in the **Available SAN Products** table and click the right arrow to move them to the **Selected Products and Hosts** table.
4. **IP**Click the **Hosts** tab, if necessary, and complete the following steps.
   a. Right-click in the **Available Hosts** table and select **Expand All**.
   b. Select the hosts you want to collect data for in the **Available Hosts**table and click the right arrow to move them to the **Selected Products and Hosts** table.

5. Click OK on the Technical SupportSave dialog box.

   Data collection may take 20-30 minutes for each selected switch. This estimate my increase depending on the number of switches selected.

   The Technical SupportSave Status dialog box displays with the following details.

Field	Description
Product Name	The name of the product.
IP Address	The product's IP address.
Product Type	The type of product.
Progress	The status of the supportsave. On products running Fabric OS 7.0 or later, this field shows the percentage complete and is updated every minute. For M-EOS, Internetwork OS and Host products, as well as Fabric OS products running 6.4 or earlier, this field cannot display the percentatge (only displays In Progress and Completed).
Status	The status of the support save, for example, Sucess or Failure.

   Technical supportSave data for SAN devices is saved to the following directory: *Install_Home*\data\ftproot\technicalsupport\

   Technical supportSave uses the following naming convention for the SAN device support save files: Supportinfo-Day-mm-dd-yyyy-hh-mm-ss*Switch_Type-Switch_IP_Address-Switch_WWN.*

Viewing the technical support repository

You can only view technical support save files that are captured in the default location. Table__ details the default locations for the technical support save files.

TABLE 51 Technical support save defaults

Type	Default locaiton	Default naming convention
Client SupportSave	*Install_Home*\support	DCM-Client-SS-Time_Stamp
Server SupportSave	*Install_Home*\Server_IP\support	DCM-SS-Time_Stamp
Host (discovered from the SAN tab)	*Install_Home*\data\ftproot\technicalsupport\	Supportinfo-Day-mm-dd-yyyy-hh-mm-ss\Switch_Type-Switch_IP_Address-Switch_WWN
Host (discovered from the IP tab)	*Install_Home*\data\ftproot\technicalsupport\ipproducts	IPProd-DCB-Time_Stamp
IP Product	*Install_Home*\data\ftproot\technicalsupport\ipproducts	IPProd-Device_Display_Name-IP_Address-Time_Stamp
SAN Product	*Install_Home*\data\ftproot\technicalsupport\	Supportinfo-Day-mm-dd-yyyy-hh-mm-ss\Switch_Type-Switch_IP_Address-Switch_WWN
Auto Trace Dump	*Install_Home*\data\ftproot\technicalsupport\	Supportinfo-Day-mm-dd-yyyy-hh-mm-ss\Switch_Type-Switch_IP_Address-Switch_WWN

To view the technical support repository, complete the following steps.

1. Select **Monitor > Technical Support > View Repository.**

   The **Technical Support Repository** dialog box displays.

2. Review the techncial support repository details:

Field/Component	Description
Available SupportSave and Upload Failure Data Capture Files table	Select the support data file you want to view. Displays the following information: **File Name**—The name of the supportSave file. **Size (MB)**—The name of the supportSave file. **Last Modified**—The date the supportSave file was generated. **Type**—The type of file (Client, Server, SAN Product, Host, or First Failure Data Capture).
E-mail button	Click to e-mail the support data file. For the procedure, refer to "E-mailing technical support information" on page 896.
FTP button	Click to copy the support data file to an external FTP server. For the procedure, refer to "Copying technical support information to an external FTP server" on page 896.
Save button	Click to save a copy of the support data. For the procedure, refer to "Saving technical support information to another location" on page 895.
Delete button	Click to delete the support data file. For the procedure, refer to "Deleting technical support files from the repository" on page 897.

3. Click **OK** on the **Technical Support Repository** dialog box.

Saving technical support information to another location

To save technical support information to a location other than the default, complete the following steps.

1. Select **Monitor > Technical Support > View Repository.**

   The **Technical Support Repository** dialog box displays.

2. Select a device support save file and click **Save.**

   The **Save** dialog box displays.

3. Browse to the location where you want to save the support file.
4. Click **Save** on the **Save** dialog box.
5. Click **OK** on the message.
6. Click **OK** on the **Technical Support Repository** dialog box.

E-mailing technical support information

NOTE
You cannot e-mail technical support information using a remote client.

To e-mail technical support information, complete the following steps.

1. Select **Monitor > Technical Support > View Repository.**

   The **Technical Support Repository** dialog box displays.

2. Select the file you want to e-mail in the table.
3. Click **E-mail** to e-mail the event and supportsave files (zip).

   You must configure the Management application e-mail server before you can define the e-mail action. For more information, refer to "Configuring e-mail notification" on page 824.

   The **E-mail** dialog box displays.

4. Enter the e-mail address of the person to receive the e-mail in the **To** field.
5. Enter your e-mail address in the **From** field.
6. Click **OK.**

   The e-mail is sent and the **Technical Support Repository** dialog box closes automatically.

Copying technical support information to an external FTP server

NOTE
You cannot copy technical support information to an external FTP server using a remote client.

To copy the Support Save data located in the built-in FTP server to an external FTP server, complete the following steps.

1. Select **Monitor > Technical Support > View Repository.**

   The **Technical Support Repository** dialog box displays.

2. Select the file you want to copy in the table.
3. Click **FTP** to send the switch event and supportsave files (zip) by FTP.

   The **FTP Credentials** dialog box displays.

4. Enter the network address or domain name of the external FTP server in the **Network Address** field.
5. Enter your user name and password.
6. Enter the root directory where you want to copy the data on the external FTP server in the **Root Directory** field.
7. Click **OK.**

   The data is copied and the **Technical Support Repository** dialog box closes automatically.

Deleting technical support files from the repository

To delete a technical support file from the repository, complete the following steps.

1. Select Monitor > Technical Support > View Repository.

   The Technical Support Repository dialog box displays.

2. Select the file you want to delete in the table.
3. Click Delete.
4. Click OK on the Technical Support Repository dialog box.

Upload failure data capture

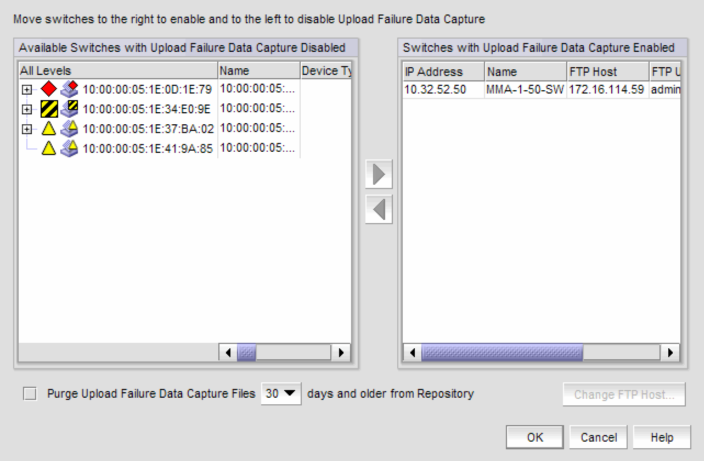
You can use upload failure data capture to enable, disable, and purge failure data capture files as well as configure the FTP Host for the switch.

NOTE
Upload failure data capture is only supported on Fabric OS devices.

Enabling upload failure data capture

1. Select Monitor > Technical Support > Upload Failure Data Capture.

   The Upload Failure Data Capture dialog box displays.



Move switches to the right to enable and to the left to disable Upload Failure Data Capture

Available Switches with Upload Failure Data Capture Disabled

All Levels	Name	Device Ty
⊞ ◆ 10:00:00:05:1E:0D:1E:79	10:00:00:05:...	
⊞ ▨ 10:00:00:05:1E:34:E0:9E	10:00:00:05:...	
⊞ △ 10:00:00:05:1E:37:BA:02	10:00:00:05:...	
△ 10:00:00:05:1E:41:9A:85	10:00:00:05:...	

Switches with Upload Failure Data Capture Enabled

IP Address	Name	FTP Host	FTP U
10.32.52.50	MMA-1-50-SW	172.16.114.59	admin

□ Purge Upload Failure Data Capture Files 30 days and older from Repository

FIGURE 388 Upload Failure Data Capture dialog box

2. Select a one or more devices on which you want to enable automatic trace dump from the Available Switches with Upload Failure Data Capture Disabled table.
3. Click the right arrow button.

   The selected devices move from the Available Switches with Upload Failure Data Capture Disabled table to the Switches with Upload Failure Data Capture Enabled table.

4. Click OK on the Upload Failure Data Capture dialog box.
5. Click OK on the confirmation message, if necessary.

Disabling upload failure data capture

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

1. Select Monitor > Technical Support > Upload Failure Data Capture.

   The Upload Failure Data Capture dialog box displays.
2. Select one or more devices on which you want to disable automatic trace dump from the Available Switches with Upload Failure Data Capture Enabled table.
3. Click the left arrow button.

   The selected devices move from the Switches with Upload Failure Data Capture Enabled table to the Available Switches with Upload Failure Data Capture Disabled table.
4. Click OK on the Upload Failure Data Capture dialog box.
5. Click OK on the confirmation message, if necessary.

Purging upload failure data capture files

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

1. Select Monitor > Technical Support > Upload Failure Data Capture.

   The Upload Failure Data Capture dialog box displays.
2. Select the Purge Upload Failure Data Capture Files check box to enable purging the trace dump files.
3. Select how often (days) you want to purge the trace dump data from the Purge Upload Failure Data Capture Files list.
4. Click OK on the Upload Failure Data Capture dialog box.

Configuring the upload failure data capture FTP server

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

NOTE
Some external FTP software (such as, Filezilla and Xlight) are not supported.

1. Select Monitor > Technical Support > Upload Failure Data Capture.

   The Upload Failure Data Capture dialog box displays.
2. Select a device from the Available Switches with Upload Failure Data Capture Enabled table.

3. Click **Change FTP Host.**

   The **Change FTP Server** dialog box displays.

4. Choose one of the following options:

   - Select the **Use** *Management_Application* option to use the Management application FTP server.
   - Select the **Custom** option and complete the following steps to configure a FTP server for the selected device.

     a. Enter the server's IP address in the **Host IP** field.

     b. Enter a user name for the server in the **User Name** field.

     c. Enter a password for the server in the **Password** field.

     d. Enter the path to where the trace dump data is saved in the **Directory Path** field.

5. Click **Test** to test the server credentials.
6. Click **OK** on the **Change FTP Host** dialog box.
7. Click **OK** on the **Upload Failure Data Capture** dialog box.
8. Click **OK** on the confirmation message, if necessary.

Saving the upload failure data capture repository

NOTE
Upload Failure Data Capture is only supported on Fabric OS devices.

1. Select **Monitor > Technical Support > View Repository.**

   The **Repository** dialog box displays.

2. Select the **Switches** tab to view upload failure data capture information.
3. Select the trace dump file you want to save and click **Save.**
4. Browse to the location you want to save the file and click **OK.**
5. Click **OK** on the **Repository** dialog box.

Chapter

Reports 32

In this chapter

SAN report types

Presenting and archiving data about a SAN is equally as important as gathering the data. Through the Management application, you can generate reports about the SAN. You can send the reports to network administrators, support consultants, and others interested in the SAN's architecture, or archive them for future reference.

The following standard report types are available from the **Generate Reports** dialog box:

- **Fabric Ports.** Lists discovered ports including used and unused ports. Port data for each fabric is divided into three parts: Fabric-wide port details, Switch-wide port details, and individual port details.
- **Fabric Summary.** Lists information about discovered fabrics including fabric and switch details, device information, and ISL and trunk summary.

The following device specific reports are available through the **Monitor** (**Monitor > Performance > Historical Report**) or **Reports** menu and right-click menus:

- **Performance.** Lists historical performance-related data.

NOTE
Performance reports require a SAN Trial or Licensed versionLicensed version.

- **Zone.** Lists zoning objects.

Generating SAN reports

To generate reports, complete the following steps.

1. Select **Reports** > **Generate.**

   The **Generate Reports** dialog box displays.

2. Select the types of reports you want to generate.

   - Fabric Ports
   - Fabric Summary

3. Select the fabrics for which you want to generate reports.

4. Click **OK.**

   The generated reports display in the **View Reports** dialog box.

   NOTE
   Hyperlinks in reports are active only as long as the source data is available.

5. Click **Close** to close the **View Reports** dialog box.

6. Click **Yes** on the “are you sure you want to close” message.

Viewing SAN reports

You can view any report generated in the SAN. To view reports, complete the following steps.

1. Select **Reports** > **View** or click the **View Report** icon.

   The **View Reports** dialog box displays.

2. Select the report you want to view in the **All Reports** list.

   If you do not see the report you want to view, generate it first by following the instructions in “Generating SAN reports” on page 902.

   You can select reports by Time, Report Type, or User.

3. Use the buttons in the table below to navigate through and resize the report.

Icon	Description
⏮	First—Click to return to the first page in the report. Greyed out when you are on the first page.
◀	Previous—Click to return to the previous page in the report. Grayed out when you are on the first page of the report.
▶	Next—Click to move to the next page in the report. Grayed out when you are on the last page of the report.
⏭	Last—Click to move to the last page in the report. Greyed out when you are on the last page of the report.

Icon	Description
🗋	Actual Size—Click to display the report at its actual size.
🗋	Fit to Page—Click to resize the report to display entirely in the view.
⊓	Fit to Width—Click to resize the report to fit in the view by width.
⊕	Zoom In—Click to zoom in on the report.
⊖	Zoom Out—Click to zoom out on the report.

4. Click **Show in Browser** to view the selected report in your default browser window.
5. Click **Close** to close the **View Reports** dialog box.
6. Click **Yes** on the “are you sure you want to close” message.

Exporting SAN reports

To export reports, complete the following steps.

1. Select **Reports** > **View** or click the **View Report** icon.

   The **View Reports** dialog box displays.
2. Select the report you want to export in the **All Reports** list.

   If you do not see the report you want to export, generate it first by following the instructions in “Generating SAN reports” on page 902.

   You can select reports by Time, Report Type, or User.
3. Select the format (**PDF**, **HTML**, or **XML**) you want to export to from the list to the left of the **Export** button.
4. Click **Export.**

   The **Save** dialog box displays.
5. Browse to the file location where you want to save the report and click **Save.**
6. Click **Close** to close the **View Reports** dialog box.
7. Click **Yes** on the “are you sure you want to close” message.

Printing SAN reports

You can print reports through an internet browser.

1. Select **Reports** > **View.**

   The **View Reports** dialog box displays.

2. Select the report you want to print 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 SAN reports" on page 902.

   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. Close the Web browser.
7. Click **Close** in the **View Reports** dialog box.
8. Click **Yes** on the "are you sure you want to close" message.

Deleting SAN reports

To delete reports, complete the following steps.

1. Select **Reports** > **View** or click the **View Report** icon.

   The **View Reports** dialog box displays.

2. Select the report you want to delete in the **All Reports** list.

   If you do not see the report you want to view, generate it first by following the instructions in "Generating SAN reports" on page 902.

   You can select reports by Time, Report Type, or User.

3. Click **Delete Report.**

   ATTENTION
   Once you click **Delete Report**, the report is deleted without confirmation.

4. Click **Close** to close the **View Reports** dialog box.
5. Click **Yes** on the "are you sure you want to close" message.

Generating SAN performance reports

NOTE
Performance reports require a SAN Trial or Licensed version.

To generate a historical performance report for a device, complete the following steps.

1. Select the device for which you want to generate a performance report.
2. Choose one of the following options:
    - Select **Monitor > Performance > Historical Report**.

      OR
    - Right-click the device and select **Performance > Historical Report**.

   The **HIstorical Performance Table** dialog box displays.
3. Filter the historical data by completing the following steps.
    a. Select the number of results to display from the **Display** list.

    b. Select the ports from which you want to gather performance data from the **From** list.

       If you select **Custom**, complete the following steps.

       1. Select the type of ports from the **Show** list.
       2. Right-click a device in the **Available** table and select **Expand All**.
       3. Select the ports (**Ctrl** or **Shift** + click to select multiple ports.) from which you want to gather performance data from the **Available** table and click the right arrow button. The selected ports move to the Select Ports table.
       4. Click **OK**.

    c. Select the historical period from which you want to gather performance data from the **For** list.

       If you select **Custom**, complete the following steps.

       1. Select the **Last** option and enter the number of minutes, hours, or days.
          OR
          Select the **From** option and enter the date and time.
       2. Click **OK**.

    d. Select the granularity at which you want to gather performance data from the **Granularity** list.

    e. Select the measure by which you want to gather performance data from the **Measures** list.

       To select more than one measure, click the **Additional Measures** expand arrows and select the check box for each additional measure.

    f. Save this configuration by selecting **Save**.

       The **Save Favorites** dialog box displays. This enables you to save the selected configuration so that you can use it to generate the same type of report at a later date.

       1. Enter a name for the configuration in the **Favorites Name** field.
       2. Click **OK**.

g. Click **Apply**.

The selected report automatically displays in the **View Reports** dialog box.

NOTE
Hyperlinks in reports are active only as long as the source data is available.

To print the selected report, refer to "Printing SAN reports" on page 904.

To export the selected report, refer to "Exporting SAN reports" on page 903.

To delete the selected report, refer to "Deleting SAN reports" on page 904.

4. Click the close button (X) to close the **View Reports** dialog box.
5. Click the close button (X) to close the **HIstorical Performance Table** dialog box.

For more information about performance, refer to "Performance Data" on page 753.

Generating SAN zoning reports

The Management application enables you to generate a report for the current zone DB in the fabric. To generate a report for the edited zone DB, you must save it to the fabric first. Make sure no one else is making changes to the same area prior to submitting or your changes may be lost.

To generate zoning reports, complete the following steps.

1. Select **Configure > Zoning** or right -click the device and select **Zoning**.

   The **Zoning** dialog box displays.
2. Click **Report**.
3. Click **OK** on the message.

   The selected report automatically displays in the **View Reports** dialog box.

   NOTE
   Hyperlinks in reports are active only as long as the source data is available.

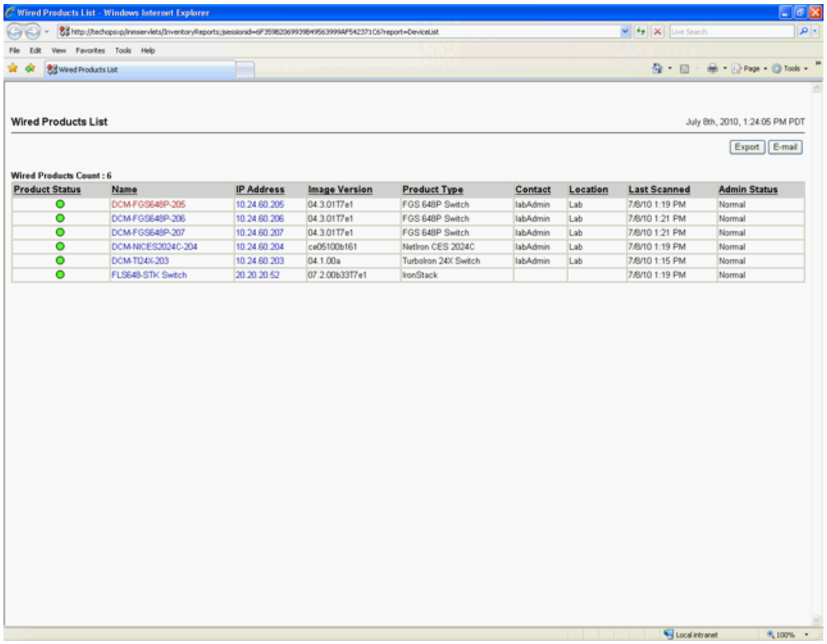
   To print the selected report, refer to "Printing SAN reports" on page 904.

   To export the selected report, refer to "Exporting SAN reports" on page 903.

   To delete the selected report, refer to "Deleting SAN reports" on page 904.
4. Click **Close** to close the **View Reports** dialog box.
5. Click **Yes** on the "are you sure you want to close" message.

For more information about zoning, refer to “Zoning” on page 575.

FIGURE 389



Wired Products List - Windows Internet Explorer
http://techopsxp/inmservlets/InventoryReports;jsessionid=6F359B206993984956399AF542371C6?report=DeviceList
Live Search
File Edit View Favorites Tools Help
Wired Products List
Page Tools
Export
E-mail
Local intranet
100%

Wired Products List

July 8th, 2010, 1:24:05 PM PDT

Wired Products Count : 6

Product Status	Name	IP Address	Image Version	Product Type	Contact	Location	Last Scanned	Admin Status
●	DCM-FGS648P-205	10.24.60.205	04.3.01T7e1	FGS 648P Switch	labAdmin	Lab	7/8/10 1:19 PM	Normal
●	DCM-FGS648P-206	10.24.60.206	04.3.01T7e1	FGS 648P Switch	labAdmin	Lab	7/8/10 1:21 PM	Normal
●	DCM-FGS648P-207	10.24.60.207	04.3.01T7e1	FGS 648P Switch	labAdmin	Lab	7/8/10 1:21 PM	Normal
●	DCM-NICES2024C-204	10.24.60.204	ce05100b161	NetIron CES 2024C	labAdmin	Lab	7/8/10 1:19 PM	Normal
●	DCM-TI24X-203	10.24.60.203	04.1.00a	TurboIron 24X Switch	labAdmin	Lab	7/8/10 1:15 PM	Normal
●	FLS648-STK Switch	20.20.20.52	07.2.00b33T7e1	IronStack			7/8/10 1:19 PM	Normal

Appendix

Application menus

A

In this appendix

Dashboard main menus

The menu bar is located at the top of the main window. The following table outlines the many functions available on each menu.

Menu	Command	Command Options
Server Menu		
	Users. Select to configure users and user groups.	
	User Profile. Select to configure user profiles.	
	Active Sessions. Select to display the active Management application sessions.	
	Server Properties. Select to display the Server properties.	
	Options. Select to configure the Management application options.	
	Exit. Select to close the Management Client.	
View Menu		
	Show Main Tab. Select to choose which tab to display.	
		Dashboard. Select to show the dashboard.
		SAN. Select to show the SAN tab.
		IP. Select to show the IP tab.
	Widgets. Select to choose which widgets to display.	
		SAN Status. Select to show the SAN Operational Status widget.
		SAN Inventory. Select to show the SAN Inventory widget.
		Status. Select to show the Status widget.
		Events. Select to show the Events widget.
Help Menu		
	Contents. Select to open the Online Help.	
	Find. Select to search the Online Help.	

Menu	Command	Command Options
	License. Select to view or change your License information.	
	About *Management_Application_Name*. Select to view the application information, such as the company information and release number.	

SAN main menus

The menu bar is located at the top of the main window. The following table outlines the many functions available on each menu.

Menu	Command	Command Options
Server Menu		
	Users. Select to configure users and user groups.	
	User Profile. Select to configure user profiles.	
	Active Sessions. Select to display the active Management application sessions.	
	Server Properties. Select to display the Server properties.	
	Options. Select to configure the Management application options.	
	Exit. Select to close the Management Client.	
Edit Menu		
	Copy. Select to copy information and move it to another location.	
	Show Connections. Select to show connections in a group.	
	Select All. Select to select all objects in the Connectivity Map and Product List.	
	Properties. Select to display the selected objects properties.	

Menu	Command	Command Options
View Menu		
	Show Main Tab. Select to choose which tab to display.	
		Dashboard. Select to show the dashboard.
		SAN. Select to show the SAN tab.
		IP. Select to show the IP tab.
	Show Panels. Select to select which panels to display.	
		All Panels. Select to show all panels.
		Topology Map. Select to only show the topology map.
		Product List. Select to only show the Product List.
		Master Log. Select to only show the Master Log.
	Manage View. Select to set up the Management 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.
	Zoom. Select to configure the zoom percentage.	
	Show. Select to determine what products display.	
		Fabrics Only. Select to display only fabrics.
		Groups Only. Select to display only groups.
		All Products. Select to display all products.
		All Ports. Select to display all ports.
	Enable Flyover Display/Device Tips. Select to enable flyover display.	
	Show Ports. Select to show utilized ports on the selected device.	
	Connected End Devices. Select to show or hide all connected end devices.	
		Include Virtual Devices check box. Select to include virtual devices.
		Hide All. Select to hide all connected end devices.
		Show All. Select to show all connected end devices.
		Custom. Select to set a custom display for all connected end devices.
		MyCustomList. Lists all custom views.

Menu	Command	Command Options
	Map Display. Select to customize a group's layout to make it easier to view the SAN and manage its 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.
	Product Label. Select to configure which product labels display.	
		Name. Select to display the product name as the product label.
		Node WWN. Select to display the node name as the product label.
		IP Address. Select to display the IP Address (IPv4 or IPv6 format) as the product label.
		Domain ID. Select to display the domain ID as the product label.
		Zone Alias. Select to display the zone alias as the product label.
	Port Label. Select to configure which port labels display.	
		Name. Select to display the name as the port label.
		Port #. Select to display the port number as the port label.
		Port Address. Select to display the port address as the port label.
		Port WWN. Select to display the port world wide name as the port label.
		User Port #. Select to display the user port number as the port label.
		Slot/Port #. Select to display the slot/port number as the port label.
		Zone Alias. Select to display the zone alias 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 Connectivity Map) that are connected to other devices.
		UnOccupied Product Ports. Select to display the ports of the devices (shown in the Connectivity Map) that are not connected to any other device.
		Attached Ports. Select to display the attached ports of the target devices.
		Switch to Switch Connections. Select to display the switch-to-switch connections.

Menu	Command	Command Options
Discover Menu		
	Fabrics. Select to discover fabrics.	
	Host Adapters . Select to discover hosts.	
	VM Manager. Select to discover VM managers.	
	Host Port Mapping. Select to manually map HBA ports to a host.	
	Storage Port Mapping. Select to manually map Storage Ports to a Storage Device or other Storage Ports.	
Configure Menu		
	Element Manager. Select to configure the selected device.	
		Hardware. Select to launch the Element Manager or Web Tools application for the selected device.
		Ports. Select to launch Web Tools - Port Administraton for the selected device.
		Admin. Select to launch Web Tools - Switch Administraton for the selected device.
		Router Admin. Select to launch Web Tools - FCR Administration for the selected device.
		Name Server. Select to launch Web Tools - Name Server for the selected device.
	Configuration. Select to manage the selected device.	
		Save. Select to save device configurations to the repository.
		Save Running to Startup. Select to save the DCB running configuration to the startup configuration on selected switches. Requires at least one discovered DCB switch.
		Restore. Select to restore device configurations from the repository.
		Configuration Repository. Select to manage device configurations from the repository.
		Schedule Backup. Select to schedule configuration backup.
		Replicate. Select to replicate the switch Configuration or Security.
		Swap Blades. Select to swap blades.
	Firmware Management. Select to download firmware to devices.	
	Host. Select to manage a selected host.	
		Adapter Software. Select to launch HCM.
	Deployment. Select to manage deployment.	
	Encryption. Select to configure encryption for your SAN.	

Menu	Command	Command Options
	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.	
	FCIP Tunnels. Select to configure tunnels and circuits on FCIP-capable devices.	
	High Integrity Fabric. Select to activate the following on M-EOS and Fabric OS devices: • On M-EOS switches, HIF activates fabric binding, switch binding, insistent domain ID and RSCNs. • On Fabric OS switches, HIF activates SCC policy, sets Insistent Domain ID and sets Fabric Wide Consistency Policy for SCC in tolerant mode.	
	Virtual Fabric. Select to configure logical switches for your SAN.	
		Enable. Select to enable virtual fabrics for your SAN.
		Disable. Select to disable virtual fabrics for your SAN.
		Logical Switches. Select to configure logical switches for your SAN.
	Names. Select to provide familiar simple names to fabrics, products, and ports in your SAN.	
	Routing. Select to manage a selected router.	
		Configuration. Select to view the R_Ports on a router.
		Domain IDs. Select to configure the router domain IDs.
	Zoning. Select to configure zones.	
		Fabric. Select to configure fabric zones.
		List Zone Members. Select to display all members in a zone.
		LSAN Zoning (Device Sharing). Select to configure LSAN zones.
		Set Change Limits. Select to set zone limits for zone activation.
	DCB. Select to manage a DCB switch, port, or link aggregation group (LAG).	
	FCoE. Select to manage an FCoE port.	
	Port Auto Disable. Select to configure port auto disable flag on individual FC_ports or all ports on a selected device, as well as unblock currently blocked ports.	
	Security. Select to manage security.	
		L2 ACL. Select to configure Layer 2 Access Control Lists on products and ports.
	Fabric Assigned WWN. Select to configure fabric assigned world wide names to a switch port or AG port.	

Menu	Command	Command Options
	VLANs. Select to launch the VLAN Manager.	
	Allow/Prohibit Matrix. (Enterprise Licensed version Only) Select to allow FICON users to configure an Allow/Prohibit Matrix table. You can select any matrix tables and compare them either vertically or horizontally.	
	FICON. (Enterprise Licensed version Only) Select to configure FICON.	
		Configure Fabric. Select to configure cascaded FICON from the selected fabric.
		Merge Fabrics. Select to merge the selected fabrics.
	Port Groups. Select to configure a group of ports from one or more switches within the same fabric.	
	FC Troubleshooting. Select to troubleshoot your SAN.	
		Trace Route. Select to view the route information between two device ports.
		Device Connectivity. Select to view the connectivity information for two devices.
		Fabric Device Sharing. Select to determine if the selected fabrics are configured to share devices.
		Diagnostic Port Test. Select to run a dialgnostic port test.
	FCIP Troubleshooting. Select to troubleshoot FCIP.	
		Ping. Select to perform a zoning check between the selected device port WWNs.
		Trace Route. Select to view the route information from a source port on the local device to a destination port on another device.
		Performance. Select to view IP performance between two devices.

Menu	Command	Command Options
Monitor Menu.		
	Performance. Select to monitor SAN devices.	
		View Utilization. Select to display connection utilization.
		View Bottlenecks. Select to display bottlenecks.
		HIstorical Data Collection. Select how to monitor historical data by choosing one of the following options: • Enable SAN Wide • Enable Selected • Disable All
		End-to-End Monitors. Select to monitor -end connections.
		Bottlenecks. Select to monitor bottlenecks.
		Clear Counters. Select to clear all port statistics counters.
		Favorites. Select a custom favorite.
		Top Talkers. Select to monitor performance through a real-time list of top conversations for a switch or port along with related information.
		Real-Time Graph. Select to monitor performance through a graph, which displays transmit and receive data. The graphs show real-time data.
		Historical Graph. Select to monitor performance through a graph, which displays transmit and receive data. The graphs show historical data.
		Historical Report. Select to monitor a performance through a table, which displays transmit and receive data. The table shows historical data.
		Bottleneck Graph. Select to monitor bottleneck through a graph.
	Policy Monitor. Select to manage best practice policies.	
	Port Connectivity. Select to view port connectivity on the selected device.	
	Port Optics (SFP). Select to display the properties associated with a selected small form-factor pluggable (SFP) transceiver on the selected device.	

Menu	Command	Command Options
	Fabric Watch. Select to manage fabric watch.	
		Configure. Select to launch Fabric Watch.
		Port Fencing. Select to configure port fencing to protect your SAN from repeated operational or security problems experienced by ports.
		Frame Monitor. Select to configure frame monitors.
		Performance Thresholds. Select to monitor thresholds.
	Technical Support. Select to configure technical support data.	
		SupportSave. Select to capture server and client support data.
		Product/Host SupportSave. (Fabric OS devices only) Select to configure technical support data collection.
		Upload Failure Data Capture. Select to configure capture failure data for Fabric OS devices.
		View Repository. Select to view repository data.
	Event Notification. Select to configure the Management application to send event notifications at specified time intervals.	
		E-mail. Select to configure the Management application to send event notifications through e-mail.
		Call Home. Select to configure the Management Server to automatically dial-in to or send an E-mail to a support center to report system problems.
	Event Processing. Select to configure event processing.	
		Pseudo Events. Select to configure pseudo events.
		Event Actions. Select to configure events actions.
	SNMP Setup. Select to configure SNMP traps.	
		Trap Forwarding. Select to configure trap forwarding.
		Product Trap Recipients. Select to register a host as a trap recipient.
		Event Reception. Select to configure the server to accept or drop traps and specify SNMP credentials and community strings, which are required to decode traps on receiving them.
		Informs. Select to enable or disable SNMP informs on the device.
	Syslog Configuration. Select to configure Syslog for the Management server.	
		Syslog Forwarding. Select to configure Syslog forwarding.
		Product Syslog Recipients. Select to register a host as a syslog recipient.

Menu	Command	Command Options
	Events. Select to display all events triggered on the selected device.	
	Logs. Select to display logs.	
		Audit. Select to display a history of user actions performed through the application (except login/logout).
		Fabric. Select to display the events related to the selected fabric.
		FICON. Select to display the FICON events related to the selected device or fabric.
		Product Event. Select to display errors related to SNMP traps and Client-Server communications.
		Product Status. Select to display operational status changes of managed products.
		Security. Select to display security information.
		Syslog. Select to display Syslog events related to the selected device or fabric.
	Track Fabric Changes. Select to track fabric changes on the selected fabric.	
	Accept Change(s). Select to accept changes to the selected fabric.	
	Accept All Changes. Select to all accept changes all available fabrics in the current view.	
Reports Menu		
	Event Custom Reports. Select to generate custom event reports.	
	Generate. Select to determine which reports to run.	
	View. Select to view reports through the application or through an internet browser.	
Tools Menu		
	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.	
	Plug-in for SCOM. Select to configure a SCOM server.	
	Tools List (determined by user settings). Select to open a software application. You can configure the **Tools** menu to display different software applications. Recommended tools to include in this menu include an internet browser, the command prompt application, and Notepad.	

Menu	Command	Command Options
Help Menu		
	Contents. Select to open the Online Help.	
	Find. Select to search the Online Help.	
	License. Select to view or change your License information.	
	About *Management_Application_Name*. Select to view the application information, such as the company information and release number.	

SAN shortcut menus

You can use the Management application interface main menu to configure, monitor, and troubleshoot your SAN components. The instructions for using these features are documented in the subsequent chapters of this manual.

For each SAN component, you can optionally right-click the component and a shortcut menu displays. The table below details the command options available for each component.

Component	Menu/Submenu Commands	Comments
FC Fabric or Backbone Fabric		
	Zoning	
	LSAN Zoning (Device Sharing)	Only enabled for Backbone fabrics.
	Performance > End-to-End Monitors Real-Time Graph Historical Graph Historical Report	
	Events	
	Configure FCIP Tunnels	Only launches the wizard when FCIP-capable switches are in the selected fabric.
	High Integrity Fabric	
	Fabric Binding	
	Router Configuration	
	Routing Domain IDs	
	Technical Support > Product/Host SupportSave Upload Failure Data Capture View Repository	
	View > Port List Node List	
	Track Fabric Changes check box	
	Accept Changes	

Component	Menu/Submenu Commands	Comments
	Trace Route	
	Connected End Devices > Include Virtual Devices check box Hide All Show All Custom MyCustomList	
	Create Meta SAN View	Only available for Backbone fabrics.
	Create View Automatically	Automatically creates a view with the selected fabric. View name is same as the current label.
	Map Display	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Collapse or Expand	Only available from Connectivity Map
	Table > Copy '*Fabric_Name*' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Device Group		
	Host Port Mapping	Only available for hosts or host group.
	Zoning	Only available for switch group.
	Storage Port Mapping	Only available for storage group.
	Map Display	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.

Component	Menu/Submenu Commands	Comments
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Collapse or Expand	Only available from Connectivity Map
Fabric OS Switch/Chassis/Access Gateway		
	Element Manager > Hardware Ports Admin Router Admin Name Server	
	Configuration > Save Save Running to Startup (DCB-capable switch) Restore Schedule Backup Configuration Repository Replicate > Configuration Security Swap Blades	
	Logical Switches > *List_of_Logical_Switches* (Fabric OS only) (Virtual Fabric-capable switches only)	Only available from Product List.
	Firmware Management	
	Zoning	Does not display when switch is in a Core Switch group, Chassis group or Isolated device group, or when it is in Access Gateway mode.
	DCB (DCB-capable switch)	
	FCoE (DCB-capable switch)	
	Allow / Prohibit Matrix	Only available for Fabric OS devices. Only enabled when the Fabric OS device is FICON-capable and has the Enhanced Group Management license.

Component	Menu/Submenu Commands	Comments
	Technical Support > Product/Host SupportSave Upload Failure Data Capture View Repository	
	Port Connectivity	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Port Optics (SFP)	
	Port Fencing	
	Performance > Top Talkers Clear Counters Real-Time Graph Historical Graph Historical Report	
	Events	
	Enable / Disable > Enable Disable	
	Telnet	
	Telnet through Server	
	<User-defined menu item>	Configured in Setup Tools. May be more than one item.
	Setup Tools	
	Product	Only enabled when the fabric is tracked, and the product is removed and joins another fabric.
	Other Ports > <Fabric Name 1> <Fabric Name 2>	Does not display when an Access Gateway mode device is attached to multiple fabrics.
	Accept Change	Only enabled in tracked FC Fabrics. Only enabled when a plus or minus icon is present.
	Show Ports check box	
	Show Connections	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.

Component	Menu/Submenu Commands	Comments
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
M-EOS Switch/Director		
	Zoning	
	Element Manager	
	Performance > Real-Time Graph Historical Graph Historical Report	
	Events	
	Port Connectivity	
	Port Fencing	
	Web Server	
	<User-defined menu item>	Configured in Setup Tools. May be more than one item.
	Telnet	Disabled when the device does not have an IP address assigned or discovered.
	Telnet through Server	Disabled when the device does not have an IP address assigned or discovered.
	Setup Tools	
	Product	Only enabled when the fabric is tracked, and the product is removed and joins another fabric.
	Accept Change	
	Show Ports	
	Show Connections	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.

Component	Menu/Submenu Commands	Comments
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Core Switch		
	Element Manager	Only available from Product List.
	Enable/Disable Virtual Fabric (Fabric OS only)	Only available from Product List.
	Logical Switches > *List_of_Logical_Switches* (Fabric OS only)	Only available from Product List.
	Configuration > (Fabric OS only) Save Restore Schedule Backup Configuration Repository Replicate > Configuration Security Swap Blades	
	Firmware Management (Fabric OS only)	
	Events	
	Technical Support > (Fabric OS only) Product/Host SupportSave Upload Failure Data Capture View Repository	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.

Component	Menu/Submenu Commands	Comments
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
DCB		
	Element Manager > Hardware Ports Admin Router Admin Name Server	Launches Web Tools.
	Configuration > Save Save Running to Startup Restore Configuration Repository Schedule Backup Replicate > Configuration Security	
	Enable / Disable > Enable Disable	
	Firmware Management	
	Swap Blades	Only available from chassis.
	Zoning	
	DCB	
	FCoE	
	VLAN	
	Allow / Prohibit Matrix	
	Security > L2 ACL	

Component	Menu/Submenu Commands	Comments
	Performance > Clear Counters Top Talkers Real-Time Graph Historical Graph Historical Report Bottleneck Graph	
	Fabric Watch > Configure Port Fencing Frame Monitor Performance Thresholds	
	Technical Support > Product / Host SupportSave Upload Failure Data Capture** View Repository	
	Events	
	Port Connectivity	
	Port Optics (SFP)	
	Telnet	
	Telnet through Server	
	<User-defined menu item>	
	Setup Tools	
	Product	Only enabled when the fabric is tracked, and the product is removed and joins another fabric.
	<Other Ports > <Fabric Name 1> <Fabric Name 2>	Visible only for AGs that are attached to multiple fabrics.
	Show Ports	
	Accept Changes	
	Show Connections	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.

Component	Menu/Submenu Commands	Comments
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
HBA, iSCSI Host, and HBA Enclosure		
	Element Manager	Launches Element Manager for Fabric OS HBAs discovered using JSON agent. Launches blank window for unmanaged Fabric OS HBAs.
	Host Port Mapping	Only available for Brocade, Emulex, and Qlogic HBAs and HBA enclosures.
	Performance > Real Time Graphs	Disabled when all ports are offline. Does not display for Node Origin and Routed instance in a routed fabric.
	LightPulse Utility/NT	Only available for Emulex devices. Launches with Origin in context for routed device.
	Emulex Configuration Tool	Only available for Emulex devices. Launches with Origin in context for routed device.
	SANSurfer	Only available for Qlogic HBAs.
	<User-defined menu item>	Configured in Setup Tools. May be more than one item.
	Host	Only available in Fabric view for managed HBAs.
	Setup Tools	
	Show Ports	
	Show Connections	
	Fabric > Fabric1 Fabric2	Only available for HBAs under the Host node.
	Origin	Only available for HBAs under the Host node or devices routed in. Not available for enclosures.
	Destination	Only available for devices routed out. Not available for enclosures.

Component	Menu/Submenu Commands	Comments
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Expand All	Only available from Product List.
	Collapse All	Only available from Product List.
	Properties	
Storage, iSCSI Storage, and Storage Enclosure		
	Storage Port Mapping	Disabled for routed device.
	<User defined menu item>	
	Setup Tools	
	Show Ports	
	Show Connections	
	Origin	Only available for devices routed in. Not available for enclosures.
	Destination	Only available for devices routed out. Not available for enclosures.
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Router Phantom Domains		
	Accept Change	Only available for tracked FC Fabrics. Only enabled when a plus or minus icon is present.
	Show Connections	Displays as disabled because this component does not display in the Connectivity Map.
	Origin	

Component	Menu/Submenu Commands	Comments
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Switch Port FC		
	Performance > Real-Time Graph Historical Graph Historical Report	
	Zoning	
	List Zone Members	
	Enable / Disable > Enable Disable	
	Connected Port	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Collapse All	Only available from Product List.

Component	Menu/Submenu Commands	Comments
	Properties	
HBA and iSCSI Initiator		
	Host Port Mapping	Only available for Brocade, Emulex, and Qlogic HBAs and HBA enclosures.
	Performance > Real Time Graphs	Disabled when all ports are offline.
	FC Security Protocol	Only available for Managed JSON HBA Ports. Only available when you have the Security Privilege.
	Zoning	
	List Zone Members	
	Connected Port	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
HBA Port		
	Host Port Mapping	Does not display for routed devices.
	Performance > Real Time Graphs	Only available for occupied, managed ports. Disabled when all ports are offline.
	FC Security Protocol	Only available for Managed JSON HBA Ports. Only available when you have the Security Privilege.
	Zoning	
	List Zone Members	
	Connected Port	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.

Component	Menu/Submenu Commands	Comments
	Expand All	Only available from Product List.
	Collapse All	Only available from Product List.
	Properties	
Storage Node		
	Storage Port Mapping	
	Show Ports	Does not display for routed devices.
	Show Connections	
Storage FC and iSCSI Storage port		
	Storage Port Mapping	
	Zoning	
	List Zone Members	
	Connected Port	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Giga-Bit Ethernet Port		
	Performance > Real-Time Graph	
	Modify	Launches Element Manager.
	IP Troubleshooting > Ping Trace Route Performance	
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.

Component	Menu/Submenu Commands	Comments
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
Connection		
	Properties	
FCIP Tunnel		
	Properties	
Trunk		
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	Only available from Product List.
	Table > Copy '*Device_Name* Group' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Only available from Product List.
	Properties	
White Area of the Connectivity Map		
	Accept All Changes	
	Zoom	
	Zoom In	
	Zoom Out	
	Map Display	
	Expand	
	Collapse	

Component	Menu/Submenu Commands	Comments
	Export	
White Area of the Product List		
	Port Display > Occupied Product Ports UnOccupied Product Ports Attached Ports Switch to Switch Connections	
	Table > Copy '*Component*' Copy Row Copy Table Export Row Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	
Product List		
	Table > Copy '*Component*' Copy Table Export Table Search Select All Size All Columns To Fit Expand All Collapse All Customize	Some form of this shortcut menu is available for all tables in the Management interface.

Appendix

Call Home Event Tables

B

In this appendix

This section provides information about the specific events that display when using Call Home. This information is shown in the following Event Tables.

Call Home Event Table

Event Reason Code	FRU Code / Event Type	Description	Severity
N/A	Ethernet Event	Switch is not reachable.	3
N/A	SW-Missing	Switch is missing from Fabric.	3
10	None/SW	Login Server unable to synchronize databases.	2
11	None/SW	Login Server database found to be invalid.	2
20	None/SW	Name Server unable to synchronize databases.	2
21	None/SW	Name Server database found to be invalid.	2
40	None/SW	Operator panel has failed.	2
50	None/SW	Management Server unable to synchronize databases.	2
51	None/SW	Management Server database found to be invalid.	2
60	None/SW	Fabric Controller unable to synchronize databases.	2
61	None/SW	Fabric Controller database found to be invalid.	2
82	CTP/SW	Port is blocked by port fencing.	0
86	None/Info	Continuous Incident detection and Reporting CIDR threshold value exceeded.	0
90	None/SW	Database replication time out.	2
92	BKP/HW	Backplane NVRAM failure.	3
200	None/SW	Power supply AC voltage failure.	3
201	PWR/HW	Power supply DC voltage failure.	3

Event Reason Code	FRU Code / Event Type	Description	Severity
202	PWR/HW	Power supply thermal failure.	3
208	PWR/HW	Power supply false shutdown.	3
210	PWR/HW	Power supply i2c bus failure.	3
300	FAN/HW	A cooling fan propeller has failed.	3
301	FAN/HW	A cooling fan propeller has failed (two failed propellers).	3
302	FAN/HW	A cooling fan propeller has failed.	3
303	FAN/HW	A cooling fan propeller has failed.	3
304	FAN/HW	A cooling fan propeller has failed.	3
305	FAN/HW	A cooling fan propeller has failed.	3
306	FAN/HW	A cooling fan propeller in FAN2 FRU type has failed.	3
307	FAN/HW	A cooling fan propeller in FAN2 FRU type has failed.	3
322	FAN/HW	Front top fan FRU failed.	3
323	FAN/HW	Front bottom fan FRU failed.	3
324	FAN/HW	Rear top fan FRU failed.	3
325	FAN/HW	Rear bottom fan FRU failed.	3
400	CTP/HW	Power-up diagnostic failure.	3
411	CTP/SW	Firmware fault occurred.	3
413	CTP/HW	Backup CTP power-on self test failure.	3
414	CTP/HW	Backup CTP failure.	3
419	CTP/INFO	Board NVRAM failure.	3
425	CTP/HW	CTP DRAM mismatch.	3
428	CTP/HW	CTP hardware component failure.	3
433	CTP/SW	Non-recoverable Ethernet fault.	3
440	CTP/HW	Embedded Port fatal error.	3
473	CTP/SW	CTP shutdown due to failure.	3
483	CTP/SW	Partition shutdown due to failure.	3
488	CTP/HW	Critical CTP failure on single CTP system.	3

# CONSRV Events Table

Event Reason Code	FRU Code/Event Type	Description	Severity
504	DVP/LIM/HW	M-EOS: Port module failure.	3
506	DVP/PORT	Fibre Channel port failure	3
509	DVP/PORT	Fibre Channel path failure.	0
511	LIM/DVP	LIM SPP failure.	3
514	DVP/ LIM/PORT	SFP/XFP optics failure.	3
517	LIM	LIM SPP Offline.	3
530	LIM/DVP	LIM Power-up diagnostic failure.	3
536	LIM/DVP	Internal Frame Error port anomaly - threshold exceeded.	2
604	SBAR/SWM/HW	M-EOS: SBAR module failure.	3
607	SBAR/SWM/HW	M-EOS: Switch contains no operational SBAR cards.	4
610	SWM/INFO	SWM BMAC Link Down.	0
622	SBAR/INFO	SWM powered off	0
625	SBAR/INFO	SWM NV RAM failure.	0

# Thermal Event Reason Codes Table

Event Reason Code	FRU Code/Event Type	Description	Severity
800	DVP/LIM/HW	High temperature warning.	3
801	DVP/LIM/HW	Critically hot temperature warning.	3
802	DVP/LIM/HW	M-EOS: Port card shutdown due to thermal violations.	3
805	SWM/SBAR/HW	High temperature warning.	3
806	SWM/SBAR/HW	Critically hot temperature warning.	3
807	SWM/SBAR/HW	M-EOS: SBAR module shutdown due to thermal violations.	3
810	CTP/HW	High temperature warning.	3
811	CTP/HW	Critically hot temperature warning.	3
812	CTP/HW	CTP shutdown due to thermal violations.	3
850	CTP/HW	System shutdown due to CTP thermal threshold violations.	4

Brocade Events Table

Event Reason Code	FRU Code/Event Type	Description	Severity
1009	MS-1009	Error in registered link incident record (RLIR)	4
1402	FW-1402	Flash usage is out of range (Fabric OS version 6.0 or earlier)	3
1426	FW-1426	Faulty or Missing Power supply	3
1427	FW-1427	Faulty Power supply	3
1428	FW-1428	Missing Power supply	3
1429	FW-1429	Problem in power supply arrangement	3
1430	FW-1430	Faulty Temperature sensors	3
1431	FW-1431	Faulty fans	3
1432	FW-1432	Faulty WWN Cards	3
1433	FW-1433	Faulty CPs	3
1434	FW-1434	Faulty Blades	3
1435	FW-1435	Flash usage is out of range (Fabric OS version 6.1 or later)	3
1436	FW-1436	Marginal port	3
1437	FW-1437	Faulty Port	3
1438	FW-1438	Faulty or Missing SFPs	3

User Privileges

In this appendix

About user privileges

The Management application provides the User Administrator with a high level of control over what functions individual users can see and 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 the Management application's method of providing role-based access control (RBAC) to the software's user administrator.

In the Management application privileges are assigned to roles and devices are assigned to areas of responsibility (AOR). Privileges and devices are not directly assigned to users; users receive privileges and obtain access to devices from the roles and AORs to which they are assigned. You can assign multiple roles and AORs to a single user.

The following tables define all the privileges in the Management application and the behavior of the application if the privilege is not given, read only, or read/write.

TABLE 52 Application privileges and behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
Active Session Management	Allows you view active client sessions and disconnect an unwanted user.	Disables the **Active Sessions** command from the **Server** menu.	Enables the **Active Sessions** command from the **Server** menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **Active Sessions** command from the **Server** menu. Enables all commands and functions on the dialog box.
Call Home	Allows you to configure call home centers, devices, and event filters.	Disables the **Call Home** command on the **Monitor > Event Notification** menu.	Enables the **Call Home** command on the **Monitor > Event Notification** menu. Enables the **Add**, **Edit**, **Remove**, **Edit Centers**, and **Show/Hide Centers** buttons as well as the **Enabled** check boxes on the dialog box; however, disables the **OK** and **Apply** buttons on the **Call Home**, **Call Home Event Filter**, and **Configure Call Home Center** dialog box boxes.	Enables the **Call Home** command on the **Monitor > Event Notification** menu. Enables all functions in the dialog box.
Configuration Management	Allows you to access the **Configuration Management** dialog box and perform configuration upload and replication.	Disables **Save**, **Restore**, **Configuration Repository**, and **Schedule Backup** under **Configure > Switch** and the **Configuration** command under **Configure > Switch > Replicate.**	Enables **Configuration Repository** under **Configure > Switch.** Only viewing of saved configuration is supported. Configuration upload and replication are disabled.	Enables all commands under **Configure > Switch**. Allows you to perform configuration upload, download and restore.
DCB Management	Allows you to configure DCB devices.	Disables the **DCB** command from the **Configure** menu.	Enables the **DCB** command from the **Configure** menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **DCB** command from the **Configure** menu. Enables all commands and functions on the dialog box.
Element Manager	Allows you to access the device element manager.	Disables the Element Manager command.	Enables the Element Manager command. Allows you to open the Element Manager; however, disables all functions.	Enables the Element Manager command. Allows you to perform all Element Manager functions.
Element Manager - Product Administration **NOTE** This privilege affects M-EOS and M-EOSn switch product Element Managers.	An Element Manager privilege that enables most functionally.	Disables the functions described in the *Element Manager User Manual* for which you do not have rights. Displays the message, "You do not have rights to perform this action."	Same as No Privilege.	Enables the functions described in the *Element Manager User Manual*.

TABLE 52 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
E-mail Event Notification Setup	Allows you to define the e-mail server used to send e-mail.	Disables **Event Notification E-mail** command on the **Monitor** menu and the E-**mail Event Notification Setup** button in the **Users** dialog box. Disables the **E-mail** option in the Master Log shortcut menu. 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?”.	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.	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.
Event Management	Allows you to define rules with event triggers and actions.	Disables the **Event Policies** menu item.	Enables access to the **Event Policies** menu item and allows existing rules to be selected and viewed. Disables all action buttons on the tab.	Enables access to the **Event Policies** menu item and enables all functions on the tab.
Fabric Watch	Fabric Watch—Allows you to launch Fabric Watch. Port Fencing—Allows you to configure the function that logs ports out of fabrics automatically if they are misbehaving. Frame Monitor—Allows you to monitor frames. Performance Thresholds—Allows you to configure performance thresholds.	Disables the **Fabric Watch** command from the **Monitor** menu.	Enables the **Fabric Watch** commands from the **Monitor** menu. DIsables the funtions on the **Port Fencing** dialog box. DIsables the funtions on the **Frame Monitor** dialog box. DIsables the funtions on the **Configure Thresholds** dialog box.	Enables the **Fabric Watch** commands from the **Monitor** menu. Enables you to launch Fabric Watch. Enables all functions on the **Port Fencing** dialog box. Enables all functions on the **Frame Monitor** dialog box. Enables the funtions on the **Configure Thresholds** dialog box.

TABLE 52 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Fault Management	Allows you to control access to the **SNMP Trap Registration and Forwarding** dialog box, the **Event Storage** option of the **Options** dialog box, the **Syslog Registration and Forwarding** dialog box, as well as the **Export** and **Clear** functions in the **Event Log** dialog box and the **Show** and **Hide** functions in the **Customize Columns** dialog box.	Disables the **SNMP Trap** and **Syslog configuration** commands from the **Monitor** menu. Disables the **Event Storage** option on the **Options** dialog box. If you do not have other read/write privileges to **Options** dialog box functions, disables the **Server > Options** command. Enables the **Logs >** *<Log_Type>* from the **Monitor** menu.	Enables the **SNMP Trap** and **Syslog configuration**, commands from the **Monitor** menu. Enables the **Event Storage** option on the **Options** dialog box. Enables the **Server > Options** command. Only enables the **Cancel** function for the dialog box boxes. Enables the **Logs >** *<Log_Type>* from the **Monitor** menu.	Enables the **SNMP Trap** and **Syslog configuration**, commands from the **Monitor** menu. Enables the following functions from the dialog box boxes: • configure Management server registration • configure TRAP or Syslog forwarding • register other servers as a recipient • apply changes Enables the **Server > Options** command. Enables the **Event Storage** option on the **Options** dialog box. Enables the following functions from the dialog box: • configure max events • configure event purging policy • apply changes Enables the following functions from the **Master Log** right-click menu: • Clear events • Show events • Hide events • Export events Note that the **Export** command on the **Master Log** right-click menu also requires the Export privilege because it launches the **Export** dialog box. Enables the **Clear** and **Export** buttons on the individual log dialog box boxes.
FCoE Management	Allows you to configure FCoE devices.	Disables the **FCoE** command from the **Configure** menu.	Enables the **FCoE** command from the **Configure** menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **FCoE** command from the **Configure** menu. Enables all commands and functions on the dialog box.

TABLE 52 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Firmware Management	Allows you to download firmware to selected switches and manage the firmware repository.	Disables the **Firmware Management** command from the **Configure** menu and right-click menu.	Enables the **Firmware Management** command from the **Configure** menu and right-click menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **Firmware Management** command from the **Configure** menu and right-click menu. Enables all commands and functions on the dialog box.
Host Adapter Management	Allows you to configure a host.	Disables the **Element Manager** command on the right-click menu and the **Element Manager > HCM** command on the **Configure** menu.	Disables the **Element Manager** command on the right-click menu and the **Element Manager > HCM** command on the **Configure** menu.	Enables the **Element Manager** command on the right-click menu and the **Element Manager > HCM** command on the **Configure** menu.
L2 ACL	Allows you to configure a layer 2 access control list.	Disables the **Security > L2 ACL** command on the **Configure** menu.	Enables the **Security > L2 ACL** command on the **Configure** menu. Disables all funtions on the dialog box.	Enables the **Security > L2 ACL** command on the **Configure** menu. Enables all funtions on the dialog box.
License Update	Allows you to update your license. Allows you to control access to the **License** dialog box from the **Help** menu.	Disables the **License** command on the **Help** menu.	Enables the **License** command on the **Help** menu; however, disables the **Update** and **OK** buttons.	Enables the **License** command on the **Help** menu and enables you to change the license key.
Performance	Allows you to configure the performance subsystem, the display of performance graphs, and threshold settings.	Disables entire **Performance** submenu of the **Monitor** menu as well as the right-click **Performance Graph(s)** command on ports and switch products. Disables the **Port Optics** command on the right-click menu. Disables the **Performance** button in the **CEE Configuration** dialog box.	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).	Enables entire **Performance** submenu of 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). Enables the **Port Optics** command on the right-click menu.

TABLE 52 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Properties Edit	Allows you to edit many director and switch properties.	Enables the **Properties** command on **Edit** menu and right-click menus. Disables edit function (removes green triangles) from editable property fields. Disables the **Names** command on the **Configure** menu.	Enables the **Properties** command on **Edit** menu and right-click menus. Disables edit function (removes green triangles) from editable property fields. Enables the **Names** command on the **Configure** menu; however, disables all edit functions in the dialog box.	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. Enables the **Names** command on the **Configure** menu and enables all functions in the dialog box.
Reports	Allows you to generate and view the following reports: • Fabric Ports • Fabric Summary	Disables the **View** command and the **Generate** command on the **Reports** menu. If this privilege is removed and the Event Management privilege is assigned then this message appears: <title: <Product> Message> <Warning>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. <<OK>>	Enables the **View** command on the **Reports** menu. Disables the **Generate** command on the **Reports** menu.	Enables the **View** command and the **Generate** command on the **Reports** menu.
Security	Allows you to enable and configure SANtegrity features.	Disables the **Security** command from the **Configure > Switch > Replicate** menu. Disables the **Security Log** command on the **Monitor > Logs** menu. Disables the **Security Misc** command from the **Server > Options** menu.	Disables the **Security** command from the **Configure > Switch > Replicate** menu. Enables the **Security Log** command on the **Monitor > Logs** menu. Enables the **Security Misc** command from the **Server > Options** menu; however, disables the functions.	Enables the **Security** command from the **Configure > Switch > Replicate** menu. Enables the **Security Log** command on the **Monitor > Logs** menu. Enables the **Security Misc** command from the **Server > Options** menu. Enables all functions in the dialog box boxes.
Server Backup	Allows you to control the function that copies (backs up) the application data files to another disk.	Disables the **Backup Now** and **Configure** commands on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the **Options** dialog box.	Disables the **Configure** command on the Backup icon right-click menu on the application status bar. Disables all controls for Backup on the **Options** dialog box.	Enables the **Backup Now** and **Configure** commands on the Backup icon right-click menu on the application status bar. Enables all functions for Backup on the **Options** dialog box.

TABLE 52 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
Server Software Configuration	Allows you to configure some of the properties of the client and server of the management application.	Disables the **Software Configuration Parameters** folder and subpages in the **Options** dialog box. The configuration cannot be viewed.	Enables the **Software Configuration Parameters** folder and subpages in the **Options** dialog box; however, disables the **OK** and **Apply** buttons when any of the subpages are selected.	Enables the **Software Configuration Parameters** folder and subpages in the **Options** dialog box. Enables all functions when any of those subpages are selected.
Setup Tools	Allows you to define and place commands on product icons and in the **Tools** menu.	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: <title: <Product> Message> <Warning>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.	Enables the **Setup Tools** command on the Tools menu; however, disables the **OK** button.	Enables the **Setup Tools** command on the **Tools** menu. Enables all functions in the **Setup Tools** dialog box.
Technical Support Data Collection	Allows you to capture support data from Fabric OS switches.	Disables the **SupportSave**, **Upload Failure Data Capture**, and **View Repository** commands from the **Monitor > Technical Support** menu and right-click menu.	Enables the **View Repository** command from the **Monitor > Technical Support** menu and right-click menu. Disables the **SupportSave** and **Upload Failure Data Capture** commands from the **Monitor > Technical Support** menu and right-click menu.	Enables the **SupportSave**, **Upload Failure Data Capture**, and **View Repository** commands from the **Monitor > Technical Support** menu and right-click menu. Enables all functions on the dialog box boxes.

TABLE 52 Application privileges and behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
User Management	Allows you to create and define users and groups, as well as assign privileges and views to groups.	Disables the **Users** command on the main **Server** menu and the **Users** button on the main tool bar.	Enables the **Users** command on the **Server** menu and the **Users** button on the main tool bar; however, disables the **Add**, **Edit**, and **Remove Users**, **Add and Remove Groups**, and **OK** buttons on the **Users** dialog box. Enables the **Edit Groups** button to display the **Group** dialog box (with **OK** button disabled).	Enables the **Users** command on the **Server** menu and the **Users** button on the main tool bar. Enables all functions on the **Users** dialog box and the secondary **Group** dialog box.
Virtual Network Management	Allows you to perform VMM based host discovery and management.	Disables the **VM Manager** command on the **Discover** menu.	Enables the **VM Manager** command on the **Discover** menu. Disables all funtions on the dialog box.	Enables the **VM Manager** command on the **Discover** menu. Enables all funtions on the dialog box.
VLAN Manager	Allows you to manage VLAN Management	Disables the VLAN Manager command.	Enables the VLAN Manager command; however, disables functions on the dialog box..	Enables the VLAN Manager command and all functions on the dialog box.
Web Services	Allows you to use Web Services API.			

TABLE 53 SAN privileges and application behavior

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - Discovery Setup	Allows you to configure discovery setup.	Disables **Setup** on the **Discover** menu and toolbar.	Enables **Setup** on the **Discover** menu and toolbar. Allows you to open the **Discover Setup** dialog box; however, disables all functions.	Enables **Setup** on the **Discover** menu and toolbar. Enables all functions in the **Discover Setup** dialog box.
SAN - Element Manager - Product Maintenance **NOTE** This privilege affects M-EOS and M-EOSn switch product Element Managers.	An Element Manager privilege that enables maintenance functions.	Disables the functions described in the *Element Manager User Manual* for which you do not have rights. Displays the message, “You do not have rights to perform this action.”	Same as No Privilege.	Enables the functions described in the *Element Manager User Manual*.
SAN - Fabric Binding	Allows you to configure fabric binding.	Disables the **Fabric Binding** command.	Enables the **Fabric Binding** command; however, disables funtions on the dialog box.	Enables the **Fabric Binding** command and all funtions on the dialog box.
SAN - Element Manager - Product Operation **NOTE** This privilege affects M-EOS and M-EOSn switch product Element Managers.	An Element Manager privilege that enables operator functions.	Disables the functions described in the Element Manager User Manual for which you do not have rights.	Displays the message, “You do not have rights to perform this action.” Same as No Privilege.	Enables the functions described in the Element Manager User Manual.
SAN - Fabric Tracking	Allows you to define the current devices and connections present in a fabric as a baseline and to highlight any changes to that baseline.	Disables the **Track Fabric Changes** and **Accept Changes** commands on the **Monitor** menu and right-click menus of **Fabrics**.	Same as no privilege.	Enables the **Track Fabric Changes** and **Accept Changes** commands on the **Monitor** menu and right-click menus of **Fabrics**.
SAN - FCIP Management	Allows you to configure FCIP tunnels and troubleshooting of IP interfaces (IP performance, IP ping and IP trace route).	Disables the **Configure > FCIP Tunnel** and **Configure > IP Troubleshooting** commands. Disables the **FCIP Tunnel** command on the Fabric right-click menu.	Enables the **Configure > FCIP Tunnel** and **Configure > IP Troubleshooting** commands. Only enables the **Cancel** function for the dialog box boxes.	Enables the **Configure > FCIP Tunnel** and **Configure > IP Troubleshooting** commands. Enables all commands and functions on the associated dialog box boxes. Also enables all commands on the **FCIP Tunnels** tab in the device’s **Properties** dialog box.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - FICON Management	Allows you to configure Cascade FICON Fabric and Cascade FICON Fabric Merge. Also allows you to configure block ports and allow/prohibit matrix on active configuration or any offline configurations.	Disables the **Configure Fabric**, **Merge Fabrics** commands on the **Configure > FICON** menu. Disables the **Allow/Prohibit Matrix** command from the **Configure** menu and right-click menu.	Disables the **Configure Fabric**, **Merge Fabrics** commands on the **Configure > FICON** menu. Enables the **Allow/Prohibit Matrix** command from the **Configure** menu and right-click menu. Disables all commands and functions on the **Configure Allow/Prohibit Matrix** dialog box except the **Close** and **Help**.	Enables the **Configure Fabric**, **Merge Fabrics** commands on the **Configure > FICON** menu. Enables the **Allow/Prohibit Matrix** command from the **Configure** menu and right-click menu. Enables all commands and functions on the associated dialog box boxes.
SAN - High Integrity Fabric	For Fabric OS devices, allows you to set Fabric Binding and Insistent Domain IDs. For M-EOS devices, allows you to activate the High Integrity Fabric, which activates Fabric Binding, Switch Binding, Insistent Domain ID, Rerouting Delay, and Domain RSCNs.	Disables the **High Integrity Fabric** command from the **Configure** menu.	Enables the **High Integrity Fabric** command from the **Configure** menu. Disables all commands and functions on the dialog box except the **Cancel** and **Help**.	Enables the **High Integrity Fabric** command from the **Configure** menu. Disables all commands and functions on the dialog box.
SAN - Logical Switch Configuration	Allows you to create a new logical switch, assign and remove ports from a logical switch, delete a logical switch, configure a logical fabric, and change the fabric ID of a logical switch. You must be assigned to the 'All Fabrics' resource group to access Logical Switch Configuration feature.	Disables the **Logical Switches** command from the **Configure** menu.	Enables the **Logical Switches** command from the **Configure** menu. Disables all functions from the dialog box except view. Also requires access to All Resources resource group to access the **Logical Switches** dialog box.	Enables the **Logical Switches** command from the **Configure** menu. Enables all commands and functions on the dialog box. Also requires access to All Resources resource group to access the **Logical Switches** dialog box.
SAN - Port Connectivity	Allows you to view all of the port details and connected devices.	Disables the **Port Connectivity** command from the **Monitor** menu and right-click menu.	Enables the **Port Connectivity** command from the **Monitor** menu and right-click menu.	Enables the **Port Connectivity** command from the **Monitor** menu and right-click menu.
SAN - Port Mapping - Host	Allows you to identify all the HBAs that are in the same server.	Disables the **Host Port Mapping** command from the **Discover** menu. Disables the **Server** right-click command on HBAs.	Enables **Host Port Mapping** command from the **Discover** menu and right-click menu; however, disables the **Create**, **Delete**, and **OK** buttons.	Enables **Host Port Mapping** command from the **Discover** menu and right-click menu. Enables all functions in the **Servers** dialog box.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - Port Mapping - Storage	Allows you to construct multi-port storage systems out of individual storage ports.	Disables the **Storage Port Mapping** command from **Discover** menu and right-click menus for Storage products and ports in the tree and map.	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.	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.
SAN - Properties - Add/Delete Columns	Allows you to define new properties as well as remove them.	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.	Same as No Privilege.	Enables the **Add**, **Edit**, and **Delete** properties commands and buttons in the **Create View** and **Edit View** dialog box boxes, the **Product List** column header right-click menu, and the Property Sheet property header right-click menu.
SAN - Routing Configuration	Allows you to configure Routing and domain IDs of phantom switches.	Disables the **Routing Configuration** and **Routing Domain IDs** commands from the **Configure** menu and right-click menu.	Disables the **Routing Configuration** and **Routing Domain IDs** commands from the **Configure** menu and right-click menu.	Enables the **Routing Configuration** and **Routing Domain IDs** commands from the **Configure** menu and right-click menu. Enables all functions in the dialog box boxes.
SAN - SCOM Management				
SAN - SMIA Operations	Allows you to access the CIMOM (Common Information Model Object Manager) server and the SMIA Configuration Tool.	Disables the **Configure SMI Agent** button from the Server Console. Disables the SMIA Configuration Tool Java web start application.	Enables the **Configure SMI Agent** button from the Server Console. Enables the SMIA Configuration Tool Java web start application. However, disables all functions in the dialog box.	Enables the **Configure SMI Agent** button from the Server Console. Enables the SMIA Configuration Tool Java web start application. Enables all functions in the dialog box.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - Storage Encryption Configuration	Allows you to configure storage encryption configuration, including selecting storage devices and LUNs, viewing and editing switch, group, or engine properties, viewing and editing storage device encryption properties, and initiating manual LUN re-keying.	Disables the **Encryption** command from the **Configure** menu.	Enables the **Encryption** command from the **Configure** menu. Disables all functions from the dialog box except view.	Enables the **Encryption** command from the **Configure** menu. Enables the following functions from the dialog box: • viewing and editing switch, group, or engine properties • viewing and editing storage device encryption properties • selecting storage devices and LUNs • initiating manual LUN re-keying. Disables all other functions from the **Configure Encryption** dialog box.
SAN - Storage Encryption Key Operation	Allows you to configure storage encryption key operation, including selecting storage devices and LUNs, viewing switch, group, or engine properties, viewing storage device encryption properties, initiating manual LUN re-keying, enabling and disabling an engine, zeroizing an engine, restoring a Master Key, and all smart card operations.	Disables the **Encryption** command from the **Configure** menu.	Enables the **Encryption** command from the **Configure** menu. Disables all functions from the dialog box except view.	Enables the **Encryption** command from the **Configure** menu. Enables the following functions from the dialog box: • viewing switch, group, or engine properties • viewing storage device encryption properties • selecting storage devices and LUNs • initiating manual LUN re-keying. • enabling and disabling an engine • zeroizing an engine • restoring a Master Key • all smart card operations Disables all other functions from the **Configure Encryption** dialog box.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - Storage Encryption Security	Allows you to configure storage encryption security, including creating a new encryption group, adding a switch to an existing group, zeroizing an encryption engine, backing up or restoring a master key, and enabling encryption functions after a power cycle.	Disables all functions from the dialog box except view. The **Encryption** command from the **Configure** menu is enabled and disabled by the Storage Encryption Configuration privilege.	Disables all functions from the dialog box except view. The **Encryption** command from the **Configure** menu is enabled and disabled by the Storage Encryption Configuration privilege.	Enables the **Encryption** command from the **Configure** menu. Enables the following functions from the dialog box: • creating a new encryption group • adding a switch to an existing group • zeroizing an encryption engine • backing up or restoring a master key • enabling encryption functions after a power cycle • changing key vaults for an encryption group. • create/edit/delete High Availability (HA) Clusters. • removing switches from encryption groups. • enable/disable encryption engines. • create new master keys (backup and restore of master keys is already listed)
SAN - Troubleshooting	Allows you to run device connectivity check, fabric device sharing check and trace route.	Disables the **Device**, **Fabric Device Sharing**, **Connectivity and Trace Route** commands under **Configure > FC Troubleshooting.** Disables the **Configuration Wizard** command under the **Configure** menu.	Disables the **Device Connectivity**, **Fabric Device Sharing**, and **Trace Route** commands under **Configure > FC Troubleshooting.**	Enables the **Device Connectivity**, **Fabric Device Sharing**, and **Trace Route** commands under **Configure > FC Troubleshooting.** Enables all functions in the dialog box boxes.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - View Management	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.	Disables the **Create View**, **Copy View**, **Edit View**, **Delete View**, and **Connectivity View** commands in the **View > Manage View** menu and the first tab header on the main desktop. Allows you to select an assigned view but not create or change. Disables the **Create View Automatically** command in the shortcut menu.	Enables the **Create View** and **Edit View** commands in the **View > Manage View** menu and the first tab header on the main desktop; however, disables the **OK** button in the **Create View** and **Edit View** dialog box boxes. Disables the **Copy View**, **Delete View**, and **Connectivity View > Create** and **Refresh** commands. Allows you to select an assigned view but not create or change.	Activates all view commands in the **View > Manage View** menu and the first tab header on the main desktop. Enables all functions in the dialog box boxes.
SAN - Zoning - LSAN	Allows you to edit and activate LSAN zones for the LSAN fabrics that are available within the **Zoning** dialog box. Prerequisite: Both the backbone fabrics as well as all directly connected edge fabrics must be added to a resource group and a user with LSAN Zoning privilege must be assigned to this specific resource group.	Disables the **Zoning > LSAN Zoning (Device Sharing)** command on the **Configure** menu. In **Zoning** dialog box, the **Zoning Scope** list does not include *LSAN_<FabricName>* as an entry.	Enables the **Zoning > LSAN Zoning (Device Sharing)** command on the **Configure** menu. In **Zoning** dialog box, the **Zoning Scope** list includes LSAN_<FabricName> as an entry, if discovered. If LSAN_<FabricName> is selected, LSAN zone contents are loaded into the **Zoning** dialog box. Disables LSAN zone functions on all dialog box boxes. Disables all online zone database editing, activation, and persisting functions. In **Zoning** dialog box, enables the **Cancel** and **Help** buttons. In the **Potential Members** table, enables all functions in the right-click menu. In the **LSAN Zones** table, enables the **Search** functions in the right-click menu.	Enables all LSAN zone functions on all dialog box boxes.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - Zoning - Set Edit Limits	Allows you to set the number of zoning edit operations that can be performed on a fabric zone database before activating a zone configuration.	Disables the **Zoning > Set Edit Limits** command from the **Configure** menu.	Enables the **Zoning > Set Edit Limits** command from the **Configure** menu. Disables all commands and functions on the dialog box except the **Close** and **Help**.	Enables the **Zoning > Set Edit Limits** command from the **Configure** menu. Enables all commands and functions on the dialog box.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - Zoning Activation (Fabric and offline zone database) **NOTE** You must also have the Zoning Offline and Zoning Online privileges to launch the **Zoning** dialog box. **NOTE** You must also have the LSAN privilege to launch the **Activate LSAN Zones** dialog box from the **Zone Database (DB)** tab of the **Zoning** dialog box.	Allows you to activate a zone configuration selected in the **Zoning** dialog box.	Disables the **Activate**, **Deactivate**, and **Zoning Policies** buttons in the **Zoning** dialog box.	Enables the **Zoning Policies** button; however, you cannot perform any operations within the **Zoning** dialog box. Disables the **Activate** and **Deactivate** buttons in the **Zoning** dialog box.	Enables the **Activate**, **Deactivate**, and **Zoning Policies** buttons in the **Zoning** dialog box.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - Zoning Offline **NOTE** You must also have the Zoning Activation privilege to enable the Activate button. **NOTE** You must also have the Zoning g Online privilege to enable the **Save to Switch**, **Activate**, **Deactivate**, and **Rollback** functions in the **Zoning** dialog box and the **Save** function in the **Compare/Merge** dialog box.	Allows you to edit the zone database in offline mode and save the zone database to the repository or to the switch.	In **Zoning** dialog box, the **Zone DB** list includes offline zones; however, if an offline zone is selected, the contents are not loaded into the **Zoning** dialog box. Only displays the Fabric Zone DB (if you have the Zoning Online privilege) in the **Zone DB** list. Disables the **Save As** function from **Zone DB Operation** list for Fabric Zone DBs. Disables the **Save To** function on the **Active Zone Config** tab.	In **Zoning** dialog box, the **Zone DB** list includes offline zones. If you select an offline zone, the contents are loaded into the **Zoning** dialog box. Disables all offline zone DB editing, activating, and persisting functions. In **Zoning** dialog box, enables the **Cancel** and **Help** buttons and the **Compare** and **Export** functions in the **Zone DB Operation** list. On the **Zone DB** tab, enables the find buttons. On the **Active Zone Config** tab, enables the **Zone Member Display** list and **Report** button. In the **Compare/Merge** dialog box, enables the **Cancel** and **Help** buttons. In the **Potential Members** table, enables all functions in the right-click menu. In the **Zones** table, enables the **Port Label**, **Search**, and **Properties** (not editable) functions in the right-click menu. In the **Zone Configs** table, enables the **Properties** (not editable) function in the right-click menu.	Enables all functions on the **Zoning** dialog box.

TABLE 53 SAN privileges and application behavior (Continued)

Privilege	Description	No Privilege	Read-Only	Read/Write
SAN - Zoning Online **NOTE** You must also have the Zoning Activation privilege to enable the Activate button. **NOTE** You must also have the Zoning g Offline privilege to enable the **Save As** function in the in the **Zoning** and **Compare/Merge** dialog box boxes.	Allows you to edit any of the fabric zone databases in the available fabrics within the **Zoning** dialog box from the client side and then save to the switch.	In **Zoning** dialog box, the **Zone DB** list includes online and offline zones; however, if an online zone is selected, the contents are not loaded into the **Zoning** dialog box. To launch offline zones you must have the Zoning Offline privilege. Disables all zone database editing and switch pushing functions.	In **Zoning** dialog box, the **Zone DB** list includes online and offline zones. If you select an online zone, the contents are loaded into the **Zoning** dialog box. To launch offline zones you must have the Zoning Offline privilege. Disables all online zone database editing, activation, and persisting functions. In **Zoning** dialog box, enables the **Cancel** and **Help** buttons and the **Compare** and **Export** functions in the **Zone DB Operation** list. On the **Zone DB** tab, enables the find buttons. On the **Active Zone Config** tab, enables the **Zone Member Display** list and **Report** button. In the **Compare/Merge** dialog box, enables the **Cancel** and **Help** buttons. In the **Potential Members** table, enables all functions in the right-click menu. In the **Zones** table, enables the **Port Label**, **Search**, and **Properties** (not editable) functions in the right-click menu. In the **Zone Configs** table, enables the **Properties** (not editable) function in the right-click menu.	Enables all functions on the **Zoning** dialog box.

About Roles and Access Levels

The Management application provides pre-configured roles (SAN System Administrator, IP System Administrator, Security Administrator, Zone Administrator, Security Officer, Operator, and Network Administrator); however, the SAN System Administrator can also create roles manually (refer to "Creating a new role" on page 152 for instructions.)

TABLE 54 Application Features and Role Access Levels

Feature	Roles with Read/Write Access	Roles with Read-Only Access
Active Session Management	SAN System Administrator, Security Officer	Operator
Call Home	SAN System Administrator, Operator	
Configuration Management	SAN System AdministratorNetwork Administrator	Operator
DCB Management	SAN System Administrator, Network Administrator	Security Administrator, Security Officer
E-mail Event Notification Setup	SAN System Administrator, Operator	
Element Manager	SAN System Administrator,	
Element Manager - Product Administration	SAN System Administrator,	
Event Management	SAN System Administrator, Network Administrator	Operator
Fabric Watch	SAN System Administrator,	
Fault Management	SAN System AdministratorNetwork Administrator	Operator
FCoE Management	SAN System Administrator, Network Administrator	Security Administrator, Zone Administrator, Security Officer, Operator
Firmware Management	SAN System AdministratorNetwork Administrator	Operator
Host Adapter Management	SAN System Administrator, Security Officer, Host Administrator	Operator
L2 ACL	SAN System Administrator, Security Administrator	
License Update	SAN System Administrator	Operator
Performance	SAN System Administrator, Host Administrator, Network Administrator	Operator
Properties Edit	SAN System Administrator, , Host Administrator	Operator
Reports	SAN System AdministratorNetwork Administrator	Operator
Security	SAN System Administrator, , Security Administrator, Security Officer, Host Administrator	Operator
Server Backup	SAN System Administrator, Product Administrator, Operator	

TABLE 54 Application Features and Role Access Levels (Continued)

Feature	Roles with Read/Write Access	Roles with Read-Only Access
Server Software Configuration	SAN System Administrator	Operator
Setup Tools	SAN System Administrator	Operator
Technical Support Data Collection	SAN System Administrator	Operator
User Management	SAN System Administrator, Security Officer	Operator
Virtual Network Management	SAN System Administrator	Operator
VLAN Manager	SAN System Administrator	Operator
Web Services	SAN System Administrator	Operator

TABLE 55 SAN Features and Role Access Levels

Feature	Roles with Read/Write Access	Roles with Read-Only Access
SAN- Discovery Setup	SAN System Administrator, Host Administrator	Operator
SAN - Element Manager	SAN System Administrator,	
SAN - Element Manager - Product Operation	SAN System Administrator, Operator	
SAN- Fabric Binding	SAN System Administrator, Security Administrator, Security Officer	Operator
SAN- Fabric Tracking	SAN System Administrator	Operator
SAN- FCIP Management	SAN System Administrator	Operator
SAN- FICON Management	SAN System Administrator	Operator
SAN- High Integrity Fabric	SAN System Administrator, Security Administrator, Security Officer	Operator
SAN- Logical Switch Configuration	SAN System Administrator	
SAN- Port Connectivity	SAN System Administrator	
SAN- Port Mapping - Host	SAN System Administrator, Security Officer, Host Administrator	Operator
SAN- Port Mapping - Storage	SAN System Administrator	Operator
SAN- Properties - Add/Delete Columns	SAN System Administrator, Host Administrator	Operator
SAN- Routing Configuration	SAN System Administrator	Operator
SAN- SCOM Management	SAN System Administrator	
SAN- SMIA Operations	SAN System Administrator	Operator

TABLE 55 SAN Features and Role Access Levels (Continued)

Feature	Roles with Read/Write Access	Roles with Read-Only Access
SAN- Storage Encryption Configuration	SAN System Administrator,, Security	Operator
SAN- Storage Encryption Key Operations	SAN System Administrator, Security Administrator, Security Officer	
SAN- Storage Encryption Security	SAN System Administrator, Security Administrator	Operator
SAN- Troubleshooting	SAN System Administrator	
SAN- View Management	SAN System Administrator, Security Administrator, Zone Administrator, Network Administrator, Security Officer, Operator, Host Administrator	
SAN- LSAN Zoning	SAN System Administrator, Zone Administrator	Operator
SAN- Zoning Set Edit Limits	SAN System Administrator	Zone Administrator, Operator
SAN- Zoning Activation	SAN System Administrator, Zone Administrator	Operator
SAN- Zoning Offline	SAN System Administrator, Zone Administrator	Operator
SAN- Zoning Online	SAN System Administrator, Zone Administrator	Operator

Appendix

Regular Expressions

D

This appendix presents a summary of Unicode regular expression constructs that you can use in the Management application.

TABLE 56 Characters

Construct	Matches
x	The character x
\\	The backslash character
\0n	The character with octal value 0n (0 <= n <= 7)
\0nn	The character with octal value 0nn (0 <= n <= 7)
\0mnn	The character with octal value 0mnn (0 <= m <= 3, 0 <= n <= 7)
\xhh	The character with hexadecimal value 0xhh
\uhhhh	The character with hexadecimal value 0xhhhh
\t	The tab character ('\u0009')
\n	The newline (line feed) character ('\u000A')
\r	The carriage-return character ('\u000D')
\f	The form-feed character ('\u000C')
\a	The alert (bell) character ('\u0007')
\e	The escape character ('\u001B')
\cx	The control character corresponding to x

TABLE 57 Character classes

Construct	Matches
[abc]	a, b, or c (simple class)
[^abc]	Any character except a, b, or c (negation)
[a-zA-Z]	a through z or A through Z, inclusive (range)
[a-d[m-p]]	a through d, or m through p: [a-dm-p] (union)
[a-z&&[def]]	d, e, or f (intersection)
[a-z&&[^bc]]	a through z, except for b and c: [ad-z] (subtraction)
[a-z&&[^m-p]]	a through z, and not m through p: [a-lq-z](subtraction)

TABLE 58 Pre-defined character classes

Construct	Matches
.	Any character (may or may not match line terminators)
\d	A digit: [0-9]
\D	A non-digit: [^0-9]
\s	A whitespace character: [\t\n\x0B\f\r]
\S	A non-whitespace character: [^\s]
\w	A word character: [a-zA-Z_0-9]
\W	A non-word character: [^\w]

TABLE 59 POSIX character classes (US-ASCII only)

Construct	Matches
\p{Lower}	A lower-case alphabetic character: [a-z]
\p{Upper}	An upper-case alphabetic character:[A-Z]
\p{ASCII}	All ASCII:[\x00-\x7F]
\p{Alpha}	An alphabetic character:[\p{Lower}\p{Upper}]
\p{Digit}	A decimal digit: [0-9]
\p{Alnum}	An alphanumeric character:[\p{Alpha}\p{Digit}]
\p{Punct}	Punctuation: One of !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~
\p{Graph}	A visible character: [\p{Alnum}\p{Punct}]
\p{Print}	A printable character: [\p{Graph}\x20]
\p{Blank}	A space or a tab: [\t]
\p{Cntrl}	A control character: [\x00-\x1F\x7F]
\p{XDigit}	A hexadecimal digit: [0-9a-fA-F]
\p{Space}	A whitespace character: [\t\n\x0B\f\r]

TABLE 60 java.lang.Character classes (simple java character type)

Construct	Matches
\p{javaLowerCase}	Equivalent to java.lang.Character.isLowerCase()
\p{javaUpperCase}	Equivalent to java.lang.Character.isUpperCase()
\p{javaWhitespace}	Equivalent to java.lang.Character.isWhitespace()
\p{javaMirrored}	Equivalent to java.lang.Character.isMirrored()

TABLE 61 Classes for Unicode blocks and categories

Construct	Matches
\p{InGreek}	A character in the Greek block (simple block)
\p{Lu}	An uppercase letter (simple category)
\p{Sc}	A currency symbol
\P{InGreek}	Any character except one in the Greek block (negation)
[\p{L}&&[^\p{Lu}]]	Any letter except an uppercase letter (subtraction)

TABLE 62 Boundary matches

Construct	Matches
^	The beginning of a line
$	The end of a line
\b	A word boundary
\B	A non-word boundary
\A	The beginning of the input
\G	The end of the previous match
\Z	The end of the input but for the final terminator, if any
\z	The end of the input

TABLE 63 Greedy quantifiers

Construct	Matches
X?	X, once or not at all
X*	X, zero or more times
X+	X, one or more times
X{n}	X, exactly n times
X{n,}	X, at least n times
X{n,m}	X, at least n but not more than m times

TABLE 64 Reluctant quantifiers

Construct	Matches
X??	X, once or not at all
X*?	X, zero or more times
X+?	X, one or more times
X{n}?	X, exactly n times
X{n,}?	X, at least n times
X{n,m}?	X, at least n but not more than m times

TABLE 65 Possessive quantifiers

Construct	Matches
X?+	X, once or not at all
X*+	X, zero or more times
X++	X, one or more times
X{n}+	X, exactly n times
X{n,}+	X, at least n times
X{n,m}+	X, at least n but not more than m times

TABLE 66 Logical operators

Construct	Matches
XY	X followed by Y
X|Y	Either X or Y
(X)	X, as a capturing group

TABLE 67 Back references

Construct	Matches
\n	Whatever the nth capturing group matched
Quotation	
\	Nothing, but quotes the following character
\Q	Nothing, but quotes all characters until \E
\E	Nothing, but ends quoting started by \Q

TABLE 68 Special constructs (non-capturing)

Construct	Matches
(?:X)	X, as a non-capturing group
(?idmsux-idmsux)	Nothing, but turns match flags on–off
(?idmsux-idmsux:X)	X, as a non-capturing group with the given flags on–off
(?=X)	X, through zero-width positive lookahead
(?!X)	X, through zero-width negative lookahead
(?<=X)	X, through zero-width positive lookbehind
(?<!X)	X, through zero-width negative lookbehind
(?>X)	X, as an independent, non-capturing group

Appendix

Database Fields

E

In this appendix

Tables

Views

Database tables and fields

Advanced Call Home

NOTE
The primary keys are marked by an asterisk (*).

TABLE 69 ACH_CALL_CENTER

Field	Definition	Format	Size
ID *		int	
NAME	Name of the Call Center.	varchar	256

TABLE 70 ACH_CALL_CENTER_CONFIG

Field	Definition	Format	Size
KEY_ *	Key to identify the specific configuration of the Call Center.	varchar	256
CALL_CENTER_ID *	ID of the Call Center.	int	
VALUE	Value of specific configuration identified by Key of the Call Center.	varchar	256

TABLE 71 ACH_EVENT_FILTER_MAP

Field	Definition	Format	Size
FILTER_ID *	ID of the event filter.	int	
EVENT_ID *	Event ID which needs to be associated with the filter.	int	

TABLE 72 ACH_EVENT

Field	Definition	Format	Size
ID *		int	
REASON_CODE	Reason code of the event.	varchar	256
FRU_CODE	FRU code of the event.	varchar	256
DESCRIPTION	Description of the event.	varchar	256
SEVERITY	Severity of the event.	int	
TYPE	Type of the event.	varchar	256

TABLE 73 ACH_INFO

Field	Definition	Format	Size
ID*		int	
SWITCH_WWN	WWN of the switch.	varchar	23
FILTER_ID	If an event filter is assigned to the switch - the filter ID if no filter is assigned - null.	int	
CALL_CENTER_ID	ID of the call center to which the switch is assigned.	int	
SUPPORT_SAVE	1 = Support save is enabled for the switch. 0 = Support save is disabled for the switch.	smallint	
MANAGED_ELEMENT_ID	Managed element Id for the device. Default value is -1.	int	

TABLE 74 ACH_FILTER

Field	Definition	Format	Size
ID*		int	
NAME	Name of the event filter.	varchar	256
DESCRIPTION	Description of the event filter.	varchar	256

Capability

TABLE 75 CAPABILITY_

Field	Definition	Format	Size
NAME *	Name of the capability.	varchar	256
DESCRIPTION	Optional detailed description about the capability.	varchar	512

TABLE 76 CARD_CAPABILITY

Field	Definition	Format	Size
CARD_ID *	DB ID of the card.	int	
CAPABILITY_ *	Name of the capability detected on the card.	varchar	256
ENABLED	1 = the capability is enabled on the card. Default value is 0.	int	

TABLE 77 VIRTUAL_SWITCH_CAPABILITY

Field	Definition	Format	Size
VIRTUAL-SWITCH_ID *	DB ID of virtual switch.	int	
CAPABILITY_ *	Name of capability detected on virtual switch.	varchar	256
ENABLED	1 = the capability is enabled on the virtual switch.	int	

TABLE 78 CARD

Field	Definition	Format	Size
ID *		int	
CORE_SWITCH_ID *	Core switch DB ID.	int	
SLOT_NUMBER	The number of the physical slot in the chassis where the blade is plugged in. For fixed blades, SlotNumber is zero.	smallint	
TYPE	ID of the blade to identify the type.	smallint	
EQUIPMENT_TYPE	The type of the blade. It is either SW BLADE or CP BLADE.	varchar	16
STATE	State of the blade, such as ENABLED or DISABLED.	varchar	32
POWER_STATE	State of power supply to the blade.	varchar	16
ATTN_STATE		varchar	32
SERIAL_NUMBER	Factory serial number of the blade.	varchar	32
PART_NUMBER	The part number assigned by the organization responsible for producing or manufacturing the blade.	varchar	32
TRUNKING_SUPPORTED	1 = trunking is supported on this blade.	smallint	
FICON_DISABLED	1 = FICON is disabled on this blade.	smallint	
IP_ADDRESS	IP address of first Ethernet management port for a given slot with intelligent blade.	char	64
SUBNET_MASK	Mask of first Ethernet man.agement port for a given slot with intelligent blade.	varchar	64
DEFAULT_GATEWAY	Gateway IP address Ethernet management for a given slot with intelligent blade.	varchar	64
PRIMARY_FW_VERSION	Primary firmware version of applications on this blade. Applicable only for AP_BLADE.	varchar	48
SECONDARY_FW_VERSION	Secondary firmware version applications on this blade. Applicable only for AP_BLADE.	varchar	48

TABLE 78 CARD (Continued)

Field	Definition	Format	Size
FCIP_CIRCUIT_CAPABLE	The blade is capable of creating FCIP Circuits. 1 = true. 0 = false. Default value is 0.	smallint	
FCIP_LICENSED	FCIP Advanced Extension Licensing is available. 1 = available. 0 = not licensed. -1 = not supported. Default value is -1.	smallint	
MAX_FCIP_TUNNELS	The maximum number of tunnels that can be created in this slot. -1 = not supported. Default value is -1.	int	
MAX_FCIP_CIRCUITS	Describes the maximum number of circuits that can be created in this slot. -1 = not supported. Default value is -1.	int	
CP_BLADE_INDEX	CP blade index. Default value is -1.	smallint	
CP_HA_STATE	CP’s HA state information like Active/Stand by.	varchar	128
ETHERNET_IPV6_ADDRESS	IPV6 address of Ethernet management port for the blade.	varchar	64
ETHERNET_IPV6_GATEWAY	IPV6 Gateway address of Ethernet management port for the blade.	varchar	64

TABLE 79 CORE_SWITCH_CAPABILITY

Field	Definition	Format	Size
CORE_SWITCH_ID *	DB ID.	int	
CAPABILITY_ *	Name of the capability detected on the core switch.	varchar	256
ENABLED	1 = the capability is enabled on the core switch. Default value is 0.	int	

Client_view

TABLE 80 USER_

Field	Definition	Format	Size
ID *		int	
NAME	User name.	varchar	128
DESCRIPTION	User description.	varchar	512
PASSWORD	User password.	varchar	512
EMAIL	User e-mail ID.	varchar	1024

TABLE 80 USER_ (Continued)

Field	Definition	Format	Size
NOTIFICATION_ENABLED	Flag for e-mail notification. Default value is 0.	smallint	
FULL_NAME	User''s Full Name.	varchar	512
PHONE_NUMBER	User''s Phone number.	varchar	32
INVALID_LOGIN_COUNT	This is a counter filed to identify the number of invalid login attempts. Note: After successful login this filed will be set to NULL. Default value is 0.	smallint	
LOCKED_OUT_DATETIME	The date time stamp when a user got locked out because of exceeding max number of invalid login attempts.	timestamp	
STATUS	User''s account status: 0=Disabled 1=Enabled Default value is 1.	smallint	
SOURCE_OF_CREATION	To identify the source for creating the user account. 0= User created through Management applciation Client 1= User created when authenticated through external server. Note: At present there is no direct use of this field however this can be referred in future to build certain reports. Default value is 0.	smallint	

TABLE 81 USER_PREFERENCE

Field	Definition	Format	Size
USER_NAME *	User name whose preferences are saved. It corresponds to user_name in USER_table.	varchar	128
CATEGORY *	The name for a set of related preferences.	varchar	128
CONTENT	The set of preferences saved as name-value pairs.	text	

TABLE 82 CLIENT_VIEW

Field	Definition	Format	Size
ID *		int	
USER_NAME	The Management application user name.	varchar	128
NAME	Client view name.	varchar	255
DESCRIPTION	Client View description.	varchar	255

TABLE 83 CLIENT_VIEW_COLUMN

Field	Definition	Format	Size
ID *		int	
NAME	Column name.	varchar	255

TABLE 83 CLIENT_VIEW_COLUMN (Continued)

Field	Definition	Format	Size
ENTITY_CATEGORY	Either "fabric" or "product (switch or device)" or "port"; or combination of these 3 basic categories. Default value is 0.	varchar	128
COLUMN_INDEX	0 = Predefined column. 1 = First user-defined column. 2 = Second user-defined column. 3 = Third user-defined column. Default value is 0.	small int	
DESCRIPTION	Column description, typically populated for user-defined columns.	varchar	255
ICON_ID	Not used.	int	
VISIBLE	1 = all predefined / fixed columns. 0 = user-defined columns. Default value is 0.	smallint	
EDITABLE	1 = column is editable. 0 = column is not editable. Default value is 1.	smallint	

TABLE 84 CLIENT_VIEW_MEMBER

Field	Definition	Format	Size
CLIENT_VIEW_ID *	Foreign key to CLIENT_VIEW table.	int	
FABRIC_ID *	Foreign key to FABRIC table.	int	

TABLE 85 FABRIC

Field	Definition	Format	Size
ID *		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric: 0 = legacy fabric. 1 = base fabric. 2 = logical fabric.	smallint	
SECURE	1 = it is a secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric	smallint	

TABLE 85 FABRIC (Continued)

Field	Definition	Format	Size
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

Collector

TABLE 86 FABRIC_CHECKSUM

Field	Definition	Format	Size
FABRIC_ID *	Fabric ID, foreign key to the FABRIC table.	int	
CHECKSUM_KEY *	Type of checksum, e.g. device data or zone data.	varchar	32
CHECKSUM	Actual checksum value.	varchar	16

TABLE 87 FABRIC_COLLECTION

Field	Definition	Format	Size
FABRIC_ID *	Fabric ID, foreign key to the FABRIC table.	int	
COLLECTOR_NAME *	Name of the collector, e.g., NameServerInfoCollector, TopologyCollector, ZoneInfoCollector, ActiveZoneInfoCollector.	varchar	256
SEED_SWITCH_IP	IP address of the switch which serves as the seed switch. This is the switch from which above mentioned fabric level collectors get their information.	varchar	128
LAST_SEED_SW_MODIFICATION	Timestamp of the seed switch, when the particular HTML page was changed last. Note that this is not when the last time collection was done.	timestamp	

TABLE 88 COLLECTOR

Field	Definition	Format	Size
NAME *	Name of the collector registered with the collection framework.	varchar	256
CLASS_NAME	Java class name which serves as the collector.	varchar	256
DESCRIPTION	Collector description, usually not used.	varchar	512

TABLE 89 FABRIC

Field	Definition	Format	Size
ID *		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric (0:legacy fabric, 1: base fabric, 2: logical fabric).	smallint	
SECURE	1 = it is a secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted,i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 90 COLLECTOR_END_TIMESTAMP

Field	Definition	Format	Size
COLLECTOR_SOURCE *	Internal key for switches and fabrics for which collection is undertaken.	varchar	256
COLLECTOR_NAME *	Collection name, Java class used to collect specific fabric or switch information.	varchar	256
TIMESTAMP_	When the last successful collection is done.	timestamp	
LAST_COLLECTED_STATUS	Status of the last collection, successful or not. 200 is for successful. Values are standard HTTP protocol values.	smallint	

TABLE 91 VIRTUAL_SWITCH_COLLECTION

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual switch.	int	
COLLECTOR_NAME *	Collector name.	varchar	256
LAST_VIRTUAL_SW_ MODIFICATION	Last modified time on switch.	timestamp	

TABLE 92 VIRTUAL_SWITCH_CHECKSUM

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual switch.	int	
CHECKSUM_KEY *	Checksum key.	varchar	32
CHECKSUM	Checksum value.	varchar	16

TABLE 93 CORE_SWITCH_CHECKSUM

Field	Definition	Format	Size
CORE_SWITCH_ID *	DB ID.	int	
CHECKSUM_KEY *	Checksum type.	varchar	32
CHECKSUM	Checksum value.	varchar	16

TABLE 94 CORE_SWITCH_COLLECTION

Field	Definition	Format	Size
CORE_SWITCH_ID *	Core switch ID.	int	
COLLECTION_NAME *	Collector name.	varchar	256
LAST_CORE_SW_ MODIFICATION	Last core switch modification time.	timestamp	

TABLE 95 SECURITY_POLICY

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID *	DB ID of virtual_switch.	int	
POLICY_NUMBER*	IPSec Policy Number. The number can range from 1 to 32.	smallint	

TABLE 95 SECURITY_POLICY (Continued)

Field	Definition	Format	Size
POLICY_TYPE*	Type of the Policy. The possible values are IKE or IPSec	smallint	
ENCRYPTION_ALGORITHM	Encryption Algorithm for the policy.The following are the possible Encryption: NONE,DES,3DES,AES-128,AES-256,AES-CM-128 or AES-CM-256.	varchar	32
AUTHENTICATION_ALGORITHM	Authentication Algorithm for the policy: NONE SHA-1 MD5 AES-XCBC	varchar	32
PERFECT_FORWARD_POLICY_ENABLED	Perfect Forward Secrecy for the policy. The possible values are 0 or 1.	smallint	
DIFFIE_HELLMAN_GROUP	Diffie-Hellman Group used in PFS negotiation.	smallint	
SECURITY_ASSOC_LIFE	Association lifetime in seconds.	double precision	
SECURITY_ASSOC_LIFE_IN_MB	Security association lifetime in megabytes.	double precision	

Config

TABLE 96 FIRMWARE_SWITCH_DETAIL

Field	Definition	Format	Size
FIRMWARE_ID*	ID for the firmware file.	int	
SWITCH_TYPE*	Switch type that supports this firmware file.	smallint	
REBOOT_REQUIRED	Reboot required flag for the switch type.	smallint	
NUMFILES	Number of files in the firmware.	int	

TABLE 97 FIRMWARE_FILE_DETAIL

Field	Definition	Format	Size
ID*		int	
FIRMWARE_NAME	Name of the firmware file.	varchar	64
MAJOR_VERSION	Major version bit from the firmware version.	smallint	
MINOR_VERSION	Minor version bit from the firmware version.	smallint	
MAINTENANCE	Maintenance bit from the firmware version.	smallint	
PATCH	Patch bit from the firmware version.	varchar	64
PHASE	Phase bit from the firmware version.	varchar	64
RELEASE_DATE	Release date of the firmware file.	timestamp	
IMPORTED_DATE	Imported date of the file to the Management applciation.	timestamp	
FIRMWARE_FILE_SIZE	Firmware file size.	int	

TABLE 97 FIRMWARE_FILE_DETAIL (Continued)

Field	Definition	Format	Size
FIRMWARE_LOCATION	Firmware file location in the Management applciation repository.	varchar	1024
RELEASE_NOTES_ LOCATION	Release notes file location in theManagement applciation repository.	varchar	1024
FIRMWARE_REPOSITORY_ TYPE	Repository type to identify the FTP server: 0 = internal FTP. 1 = external FTP.	smallint	

TABLE 98 SWITCH_PLATFORM

Field	Definition	Format	Size
SWITCH_TYPE*	Switch type.	smallint	
DESCRIPTION	Description of the switch type.	varchar	256
SPEED	Switch maximum speed.	smallint	
MULTI_CP_CAPABLE	Switch is multi-CP capable or not.	smallint	

TABLE 99 FTP_SERVER

Field	Definition	Format	Size
ID*		int	
TYPE	Type indicates the FTP is internal or external. 0 = internal. 1 = external.	smallint	
IP	FTP server IP address.	varchar	64
USER_NAME	FTP server user name.	varchar	64
PASSWORD	FTP server user password.	varchar	64
ROOT_DIRECTORY	FTP server root directory location.	varchar	1024
PORT	Port on which FTP server is configured.	int	

TABLE 100 SWITCH_TYPE_FIRMWARE_VERSION

Field	Definition	Format	Size
SWITCH_TYPE*	Switch type.	smallint	
MIN_FOS_VERSION*	Supported minimum firmware version.	varchar	64
MAX_FOS_VERSION	Supported maximum firmware version.	varchar	64

TABLE 101 SWITCH_CONFIG

Field	Definition	Format	Size
ID*		int	
NAME	Name of the switch configurations uploaded from the switch either on demand or through scheduler	varchar	64
SWITCH_ID	ID of the switch from which the configuration has been uploaded.	int	

TABLE 101 SWITCH_CONFIG (Continued)

Field	Definition	Format	Size
BACKUP_DATE_TIME	The date/time stamp at which the configuration has been uploaded.	timestamp	
CONFIG_DATA	The actual switch configuration data.	text	
CEE_CONFIG_DATA	Switch configuration data for CEE	text	
KEEP_COPY	The column value (1) helps to preserve the configuration even after the expiration of its age.	smallint	
CREATED_BY	The column value helps to figure out who triggered the configuration upload operation.	varchar	64

CONFIG_TYPE	Configuration Type
	FC=0
	CEE_RUNNING=1
	CEE_STARTUP=2
	INVALID=-1
	Default value is 0.
		smallint	

COMMENTS	Brief comments about this configuration.	varchar	256

Connected end devices

TABLE 102 CED_APPLICATION

Field	Definition	Format	Size
ID*		int	
NAME	Name of the application. Application represents a collection of active zones in a fabric.	varchar	24
FABRIC_ID	ID of the fabric for which the application is created.	int	

TABLE 103 CED_APPLICATION_MEMBER

Field	Definition	Format	Size
APPLICATION_ID*	Auto-generated DB CED_Application table ID.	int	
ZONE_ID*	Auto-generated DB Zone table ID which joins as a member of the application.	int	

TABLE 104 CED_USER_PREFERENCE

Field	Definition	Format	Size
USER_NAME*	User Name carried from _USER table.	varchar	128
FABRIC_ID*	Fabric ID carried from Fabric table.	int	
APPLICATION_ID	CED application ID representing the group of end devices to be displayed in the fabric.	int	

Device

TABLE 105 DEVICE_PORT

Field	Definition	Format	Size
ID*		int	
NODE_ID	DB ID of the device node to which this port belongs.	int	
DOMAIN_ID	Domain ID of the switch to which this device port is attached.	int	
WWN	Device port WWN.	char	23
SWITCH_PORT_WWN	WWN of the switch port to which this device port is attached.	char	23
NUMBER	Switch port number to which this device is attached.	smallint	
PORT_ID	Device port ID.	varchar	6
TYPE	Device port type, such as N or NL.	varchar	32
SYMBOLIC_NAME	Device port symbolic name.	varchar	256
FC4_TYPE	FC payload protocol.	varchar	64
COS	FC class of service.	varchar	16
IP_PORT		varchar	63
HARDWARE_ADDRESS		varchar	32
TRUSTED	1 if found at discovery time or user has entrusted this device port explicitly. Default value is 0.	smallint	
CREATION_TIME	When the device port was discovered, i.e., created in the DB. default is ’now()’.	timestamp	
MISSING	1 if that device port is missing from the fabric. Default value is 0.	smallint	
MISSING_TIME	Time when it misses.	timestamp	
NPV_PHYSICAL	Update NPV device type on this given device port. The value "npvPhysical" on the device port will be 1 when the device port has reference to a device node of DEVICE_TYPE value 0 i.e. physical. It points to a switch port to which at least one other device port points; and that other pointing device port has reference to a device node of DEVICE_TYPE value 2 (NPV).	smallint	
EDGE_SWITCH_PORT_WWN	Edge switch port WWN will be the same as the Switch_Port_WWN except in the case of devices behind the AG. This field will be updated by the name server info collector, added for the feature support of AG WWN N port mapping. This is a null able field. It is used to determine which mapping is used by the AG.	char	23

TABLE 106 FICON_DEVICE_PORT

Field	Definition	Format	Size
DEVICE_PORT_ID*	Value for the device port to which these FICON properties are applied.	int	
TYPE_NUMBER		varchar	16
MODEL_NUMBER	Ficon device model number, such as S18.	varchar	64
MANUFACTURER	Manufacturer of the device, typically IBM.	varchar	64
MANUFACTURER_PLANT	Plant number where the device is manufactured.	varchar	64
SEQUENCE_NUMBER	Device sequence number.	varchar	32
TAG	FICON device property, e.g., 809a or 809b.	varchar	16
FLAG	FICON device property, e.g., 0x10 (hex).	varchar	8
PARAMS	FICON device property string, e.g., Valid channel port.	varchar	16

TABLE 107 DEVICE_NODE

Field	Definition	Format	Size
ID*		int	
FABRIC_ID	Fabric DB ID to which this device node belongs.	int	
WWN	Device node WWN.	char	23
TYPE	Initiator or target or both or unknown.	varchar	32
DEVICE_TYPE	0 = physical 1 = virtual 2 = NPV 3 = iSCSI 4 = both physical & virtual	smallint	
SYMBOLIC_NAME	Device node symbolic name.	varchar	256
FDMI_HOST_NAME	Device node FDMI host name.	varchar	128
VENDOR	Device node vendor.	varchar	64
CAPABILITY_		varchar	16
TRUSTED	1 = the node is trusted for "fabric tracking. Default value is 0.	smallint	
CREATION_TIME	Timestamp when the record is created by the Management application server. Default is ’now()’.	timestamp	
MISSING	1 = the device node is missing from the fabric. Default value is 0.	smallint	
MISSING_TIME	Time when the device node missed.	timestamp	
PROXY_DEVICE	One of the device ports of this device node has translated domain. That device port is set as the Proxy Device and this Device Node is treated as virtual by assigning a value of 1 to this field. Default value is 0.	smallint	

TABLE 107 DEVICE_NODE (Continued)

Field	Definition	Format	Size
AG	1 = the device node is actually an AG connected to a switch in the fabric. Default value is 0.	smallint	
PREVIOUS_MISSING_STATE	Default value is 0.	smallint	

TABLE 108 DEVICE_ENCLOSURE_MEMBER

Field	Definition	Format	Size
ENCLOSURE_ID*	DEVICE_ENCLOSURE table ID.	int	
DEVICE_PORT_WWN*	WWN Of Device Port.	char	23
DEVICE_PORT_ID	Device_Port table ID.	int	

TABLE 109 DEVICE_ENCLOSURE

Field	Definition	Format	Size
ID*		int	
NAME	Name of the Device enclosure.	varchar	256
TYPE	Type of Device enclosure - Storage Array/Server.	varchar	32
ICON	Type of Icon.	int	
OS	Operating System.	varchar	256
APPLICATIONS	Application which created device enclosure.	varchar	256
DEPARTMENT	Department using this device enclosure.	varchar	256
CONTACT	Contact person details.	varchar	256
LOCATION	Location of physical setup.	varchar	256
DESCRIPTION	Description if any.	varchar	256
COMMENT_	Comments if any.	varchar	256
IP_ADDRESS	IP Address if assigned by user.	varchar	128
VENDOR	Vendor name.	varchar	256
MODEL	Device enclosure Model.	varchar	256
SERIAL_NUMBER	Serial Number given for the entity.	varchar	256
FIRMWARE	Firmware running on the device which is not applicable for device enclosure logical entity.	varchar	256
USER_DEFINED_VALUE1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE3	User-defined custom value.	varchar	256
HCM_AGENT_VERSION	Version of the HCM agent running on the host	varchar	32
OS_VERSION	Operating system version for the enclosure	varchar	256
CREATED_BY	Module which created this enclosure: 0->Manual, 1->HBA 2->VM. Default value is 0.	int	

TABLE 109 DEVICE_ENCLOSURE (Continued) (Continued)

Field	Definition	Format	Size
TRACK_CHANGES	Flag to enable/disable tracking. Default value is 0.	smallint	
LAST_UPDATE_TIME	Last time at which the host information was updated.	timestamp	
LAST_UPDATE_MODULE	Module which updated the host information.	smallint	
TRUSTED	Flag to mark the enclosure trusted. Default value is 0.	smallint	
CREATION_TIME	Time when enclosure was created. Default is 'now()'.	timestamp	
MISSING	Flag to indicate missing enclosure. Default value is 0.	smallint	
MISSING_TIME	Time when the enclosure is found to be missing.	timestamp	
HOST_NAME	Host Name corresponding to the Device Enclsoure.	varchar	256
SYSLOG_REGISTERED	SysLog flag that indicates if syslog has been enabled or not.	smallint	
VIRTUALIZATION	If this enclosure is a host, this column indicates whether the host is running a virtualization hypervisor. 0 = unknown 1 = no supported hypervisor present 2 = VMware ESX 3 = Microsoft Hyper-V. Default value is 0.	smallint	
MANAGED_ELEMENT_ID	A unique managed element ID for a managed host.If the device enclosure is manually created (does not represent a managed host) then the field is null. Also a foreign key reference to the MANAGED_ELEMENT table.	int	

TABLE 110 FABRIC

Field	Definition	Format	Size
ID*		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric: 0 = legacy fabric 1 = base fabric 2 = logical fabric	smallint	
SECURE	1 = it is secured fabric.	smallint	

TABLE 110 FABRIC (Continued)

Field	Definition	Format	Size
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when the fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when the fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 113 USER_DEEFINED_DEVICE_DETAIL

Field	Definition	Format	Size
WWN*	Device node or device port WWN.	char	23
NAME	User-assigned device name.	varchar	256
TYPE	User set device type (initiator or target).	varchar	32
IP_ADDRESS	Device IP address.	varchar	256
CONTACT	User-assigned contact.	varchar	256
LOCATION	User-assigned device location.	varchar	256
DESCRIPTION	User-assigned description.	varchar	256
USER_DEFINED_VALUE1	User-assigned arbitrary value.	varchar	256
USEER_DEFINED_VALUE2	User-assigned arbitrary value.	varchar	256
USER_DEFINED_VALUE3	User-assigned arbitrary value.	varchar	256

EE- Monitor

TABLE 115 EE_MONITOR_STATS

Field	Definition	Format	Size
ID*		int	
EE_MONITOR_ID	References to the ID in EE_MONITOR table.	int	

TABLE 115 EE_MONITOR_STATS (Continued)

Field	Definition	Format	Size
CREATION_TIME	The polling time.	timestamp	
ACTIVE_STATE	State of collection 0 = failed 1 = success	smallint	
TX	Transmit (TX) value in bytes.	double precision	
RX	Receive (RX) value in bytes.	double precision	
CRCERRORS	Number of CRC errors.	double precision	

TABLE 116 EE_MONITOR_STATS_30MIN

Field	Definition	Format	Size
ID*		int	
EE_MONITOR_ID		int	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
TX		double precision	
RX		double precision	
CRCERRORS		double precision	

TABLE 117 EE_MONITOR_STATS_2HOUR

Field	Definition	Format	Size
ID*		int	
EE_MONITOR_ID		int	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
TX		double precision	
RX		double precision	
CRCERRORS		double precision	

TABLE 118 EE_MONITOR

Field	Definition	Format	Size
ID*		int	
MONITOR_ID	The Number (Index) given by the switch when user creates End-End monitor on the switch.	int	
SWITCH_PORT_ID	References the ID in SWITCH_PORT table.	int	
SOURCE_PORT_ID	References the ID in DEVICE_PORT table and this is an initiator for EE monitor.	int	

TABLE 118 EE_MONITOR (Continued)

Field	Definition	Format	Size
DEST_PORT_ID	References the ID in DEVICE_PORT table and this is a target for EE monitor.	int	
NAME	Name of the End_End Monitor.	varchar	124
ERROR CODE	Error code returned from the switch, when enabling End-End monitor is attempted on the switch.	int	
STATUS	Status of creating the End-End monitor on the switch. It can be either failed or succeeded.	smallint	

TABLE 119 EE_MONITOR_STATS_1DAY

Field	Definition	Format	Size
ID*		int	
EE_MONITOR_ID		int	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
TX		double precision	
RX		double precision	
CRCERRORS		double precision	

Event/FM

TABLE 120 RECIPIENT_TYPE

Field	Definition	Format	Size
ID*		int	
TYPE	Type of the recipient (Syslog or SNMP).	varchar	20

TABLE 121 SOURCE_OBJECT_TYPE

Field	Definition	Format	Size
ID*		int	
TYPE_NAME	Type of the object to which the event applies, such as Fabric, Switch or Port.	char	64
DESCRIPTION	Description of the object	varchar	255

TABLE 122 EVENT_TYPE

Field	Definition	Format	Size
ID*		int	
TYPE_CODE	Event Type Code.	char	64
DESCRIPTION	Description of the Event Rule.	varchar	255

TABLE 123 MESSAGE_RECIPIENT

Field	Definition	Format	Size
ID*		int	
DESCRIPTION	Description about recipient.	varchar	256
IP_ADDRESS	IP Address of the recipient.	varchar	128
PORT	Port number of the recipient.	int	
RECIPIENT_TYPE_ID	Recipient Type (Syslog or SNMP).	int	
ENABLED	If forwarding to destination is enabled.	smallint	
SOURCE_ADDRESS_ADDED	If source address is added as another varbind in trap. -1 for Syslog i.e RECIPIENT_TYPE_ID: 2. Default value is -1.	smallint	
REPEATER_ENABLED	If filtering is disabled. -1 for Syslog i.e RECIPIENT_TYPE_ID: 2. Default value is -1.	smallint	
VERSION	Snmp version(v1/v2/v3)	varchar	8

TABLE 124 EVENT_SUB_TYPE

Field	Definition	Format	Size
ID*		int	
EVENT_TYPE_ID	Unique Event Sub type ID	int	
DESCRIPTION	Description of Event Sub Type	varchar	255

TABLE 125 SNMP_CREDENTIALS

Field	Definition	Format	Size
ID*		int	
VIRTUAL_SWITCH_ID	Virtual switch ID for which this instance of the SNMP credentials apply.	int	
RECIPIENT_ID	Refers to recipient in the MESSAGE_RECIPIENT table.	int	255
PORT_NUMBER	Port number of the SNMP agent on the switch for get and set requests.	smallint	
RETRY_COUNT	Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.	smallint	
TIMEOUT	Timeout value in seconds for a get/set request to the SNMP agent. Default value is 5.	smallint	
VERSION	SNMP agent version running on the switch, as in SNMPv1 or SNMPv3.	varchar	6
READ_COMMUNITY_ STRING	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to a device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64

TABLE 125 SNMP_CREDENTIALS (Continued)

Field	Definition	Format	Size
WRITE_COMMUNITY_ STRING	The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
USER_NAME	A human-readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
CONTEXT_NAME	Text ID associated with the user, used by SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.	varchar	128
AUTH_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. Supported values are: usmNoAuthProtocol usmHMACMD5AuthProtocol usmHMACSHAAuthProtocol This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
AUTH_PASSWORD	The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
PRIV_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. Supported values are: usmNoPrivProtocol usmDESPrivProtocol This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
PRIV_PASSWORD	The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
SNMP_INFORMS_ENABLED	Flag to denote whether SNMP informs option is enabled or disabled. Default value is 0.	smallint	

TABLE 126 SYSLOG_EVENT

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	Switch ID.	int	
SOURCE_NAME	Source Name from which the event originated.	varchar	32
SOURCE_ADDR	IP Address from which the event originated.	varchar	32
EVENT_SOURCE	Source from which the event is generated.	varchar	32
STATUS	Status of the event.	varchar	32
PRIORITY	Priority of the event. Default priority is 7.	int	

TABLE 126 SYSLOG_EVENT (Continued)

Field	Definition	Format	Size
EVENT_NUMBER	Sequence number of the event.	int	
EVENT_COUNT	Number of occurrences of the event.	int	
AUDIT	Audit file of the syslog message.	varchar	10
FIRST_OCCURENCE_ SWITCH_TIME	First occurrence switch time.	timestamp	
LAST_OCCURENCE_ SWITCH_TIME	Last occurrence switch time.	timestamp	
FIRST_OCCURENCE_ HOST_TIME	Last occurrence switch time.	timestamp	
LAST_OCCURENCE_HOST_ TIME	Last occurrence host time.	timestamp	
MODULE	Module of the event.	varchar	10
MESSAGE_ID	Message ID of the event.	varchar	20
DESCRIPTION	Description of the event.	varchar	512
PROBABLE_CAUSE	Probable root cause of the event.	varchar	512
RECOMMENDED_ACTION	Recommended action for the event.	varchar	512
CONTRIBUTORS	Contributors of the syslog event.	varchar	512

TABLE 127 EVENT

Field	Definition	Format	Size
ID*		int	
ME_ID	Weak reference to MANAGED_ELEMENT_ID present in MANAGED_ELEMENT table. This can be a null and hence maintained as a weak reference.	int	
SEVERITY	Default value is 7.	int	
AREA	Indicates whether the event corresponds to SAN/IP/Application/SAN and IP. Default value is 0.	smallint	
ACKNOWLEDGED	0 =Unack. 1 =Ack Default value is 0.	smallint	
SOURCE_NAME	Name of the source from which the event originated.	varchar	255
SOURCE_ADDR	Source's IP address.	varchar	50
EVENT_ORIGIN_ID		int	
EVENT_CATEGORY_ID		int	
EVENT_MODULE_ID		int	
EVENT_DESCRIPTION_ID	Weak reference to ID in EVENT_DESCRIPTION table.	int	
LAST_OCCURRENCE_HOST _TIME	Last occurrence host time; this is set to GMT time.	timestamp	

TABLE 127 EVENT (Continued)

Field	Definition	Format	Size
EVENT_COUNT	Number of occurrences of the event.. Default value is 1.	int	
RESOLVED	Resolution status of the event. Default value is 0.	smallint	
ACKED_TIME	Time at which the event is acknowledged.	Timestamp	
FIRST_OCCURRENCE_HOST_TIME	First occurrence host time; this is set to GMT time.	timestamp	10
EVENT_AUDIT	Flag to indicate if the event is audited.	varchar	255
EVENT_KEY	This field is a combination of ModuleName and EventNumber which is unique within the given module.	varchar	
EVENT_ACTION_ID	Weak reference to ACTION ID present in EVENT_ACTION table. This can be a null and hence maintained as a weak reference.	int	
DEVICE_GROUP_ID	Weak reference to DEVICE GROUP ID present in DEVICE_GROUP table. This can be a null and hence maintained as a weak reference.	int	
PORT_GROUP_ID	Weak reference to PORT_GROUP ID present in PORT_GROUP table. This can be a null and hence maintained as a weak reference.	int	

TABLE 128 RAS_LOG

Field	Definition	Format	Size
MSG_ID*	Message ID of the event.	varchar	15
MODULE_ID	Module ID of the event.	varchar	10
SEVERITY	Severity of the event.	varchar	10
CAUSE	Probable root cause for the event.	varchar	4096
ACTION	Recommended action for the event.	varchar	4096
OLD_MSG_ID	Old message ID.	varchar	45

TABLE 129 EVENT_NOTIFICATION

Field	Definition	Format	Size
ID*		int	
STATUS	Status of Event Notification. value will be 0 if disabled, 1 otherwise. Default value is 0.	smallint	
SERVER_NAME	E-mail (SMTP) server name.	varchar	256
REPLY_ADDRESS	Reply E-mail address.	varchar	50
SEND_ADDRESS	E-mail address for which a Test E-mail notification is to be sent.	varchar	512
SMTP_PORT	SMTP Port number. Default value is 25.	int	

TABLE 129 EVENT_NOTIFICATION (Continued)

Field	Definition	Format	Size
USER_NAME	User name for authentication.	varchar	256
PASSWORD	Password for authentication.	varchar	256
NOTIFICATION_INTERVAL	Time interval between successive event notifications.	int	
NOTIFICATION_UNIT	Time interval Unit: 0 = Seconds 1 = Minutes 2 = Hours Default value is 0.	smallint	
TEST_OPTION	Time interval Unit: 0 = Send test to configured e-mail address. 1 = Send test to all enabled users. Default value is 0.	smallint	
SSL_ENABLED	Default value is 0.	smallint	

TABLE 130 EVENT_RULE

Field	Definition	Format	Size
ID*		int	
NAME	Name of the Event Rule.	varchar	255
TYPE	Event Rule Type: 0 = Port Offline 1 = PM Threshold crossed 2 = Security Violation 4 = Event	int	
DESCRIPTION	Description about the Event Rule.	varchar	512
OPERATOR1	AND operator used to append the rule.	varchar	12
EVENT_TYPE_ID	The Selected Event type ID from the Event type combo box.	int	
OPERATOR2	AND operator used to append the rule.	varchar	12
MESSAGE_ID	Message ID provided by the user.	varchar	20
OPERATOR3	AND operator used to append the rule.	varchar	12
IP_ADDRESS	Source IP Address.	varchar	1024
OPERATOR4	AND operator used to append the rule.	varchar	12
WWN	Source WWN.	varchar	1024
OPERATOR5	AND operator used to append the rule.	varchar	12
COUNT	Count of the specified event.	int	
OPERATOR6	AND operator used to append the rule.	varchar	12
DURATION	Duration of the specified event.	bigint	
STATE	State of the rule: 0 = Disabled 1 = Enabled	smallint	

TABLE 130 EVENT_RULE (Continued)

Field	Definition	Format	Size
SEVERITY_LEVEL	Event severity level. Default value is 4.	int	
SOURCE_NAME	Name of the source.	varchar	1024
DESCRIPTION_CONTAINS	Description pattern about the rule.	varchar	255
LAST_MODIFIED_TIME	Rules last edited time.	timestamp	
SELECTED_TIME_UNIT	Timestamp unit of the selected rule: 0 = second 1 = Minutes 2 = Hours Default value is 1.	smallint	

TABLE 131 EVENT_RULE_ACTION

Field	Definition	Format	Size
ID*		int	
RULE_ID	The rule ID present in the Event_Rule Table.	int	
NAME	Name of the Event Rule Action: Launch Script = for launch script Send E-mail = for send e-mail Raise Event = for broadcast message	varchar	255

TYPE	Name of the action:
	script = for Launch Script
	e-mail = for E-mail
	message = for Broadcast message
		varchar	30

FIELD1	Data for the selected action.	varchar	512
FIELD2	Data for the selected action.	varchar	512
FIELD3	Data for the selected action.	varchar	512
FIELD4	Data for the selected action.	varchar	512
STATE	State of the Action: 0 = Action Disabled 1 = Action Enabled Default value is 0.	smallint	

Fabric

TABLE 132 SAN

Field	Definition	Format	Size
ID*		int	
NAME	Name of this SAN.	varchar	256
CONTACT	Contact person for this SAN.	varchar	256
LOCATION	Location of this SAN.	varchar	256
DESCRIPTION	Description.	varchar	256

TABLE 132 SAN (Continued)

Field	Definition	Format	Size
STATS_COLLECTION	1 = statistics collection is enabled; otherwise, 0. Default value is 0.	smallint	
CREATION_TIME	time at which this record was created. Default value is ’now()’.	timestamp	
LAST_UPDATE_TIME	time when this was last updated. Default value is ’now()’.	timestamp	

TABLE 133 FABRIC

Field	Definition	Format	Size
ID*		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric: 0 = legacy fabric 1 = base fabric 2 = logical fabric Default value is 0.	smallint	
SECURE	1 = it is a secured fabric. Default value is 0.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric. Default value is 0.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric. Default value is 1.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric. Default value is 0.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked. Default value is 0.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric. Default value is 0.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created. Default value is ’now()’.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	

TABLE 133 FABRIC (Continued)

Field	Definition	Format	Size
LAST_UPDATE_TIME	Time when fabric was last updated. Default value is ’now()’.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone configuration which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256
PRINCIPAL_SWITCH_WWN	WWN of the principal switch of the fabric	char	23
ZONE_TRANSACTION_TIMEOUT	Number of seconds that a ZONE_TRANSACTION can be idle Default value is 180.	int	
FABRIC_MODEL	Default value is 1.	smallint	
LAST_FAILURE_TIMESTAMP		timestamp	
LAST_SUCCESSFUL_TIMESTAMP		timestamp	
ENHANCED_TI_ZONE_SUPPORT	Holds the value if the fabric has enhanced TI Zone support or not. Default: 0 Values: 0|1.	smallint	

TABLE 135 FABRIC_MEMBER

Field	Definition	Format	Size
FABRIC_ID*	Fabric ID, foreign key to FABRIC table.	int	
VIRTUAL_SWITCH_ID*	ID of the virtual switch which is a member of this fabric, foreign key to VIRTUAL_SWITCH table.	int	
TRUSTED	1 = the switch is a trusted member of the fabric. Either found in the initial discovery or user subsequently entrusted the switch by user action. Default Value is 0.	smallint	
CREATION_TIME	When the switch became a member. Default Value is ’now()’.	timestamp	
MISSING	1 = it is missing from the fabric. Default Value is 0.	smallint	
MISSING_TIME	When it is missed from the fabric; null if the member is entrusted.	timestamp	
LAST_UPDATE		bigint	

FC Port Stats

TABLE 136 FC_PORT_STATS

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	References the ID in CORE_SWITCH table.	int	
PORT_ID	References the ID in SWITCH_PORT table.	int	
TX	Transmission (TX) value in bytes.	double precision.	
RX	Receive (RX) value in bytes.	double precision.	
TX_UTILIZATION	Transmit utilization value in percentage.	double precision.	
RX_UTILIZATION	Receive utilization value in percentage.	double‘ precision.	
CREATION_TIME	The polling time.	timestamp	
ACTIVE_STATE	State of collection: 0 = failed 1 = success	smallint	
LINKFAILURES	Number of link failures.	double precision.	
TXLINKRESETS	Number of transmit link failures.	double precision.	
RXLINKRESETS	Number of receive link failures.	double precision.	
SYNCLOSSES	Number of sync losses.	double precision.	
SIGNALLOSSES	Number of signal losses.	double precision.	
SEQUENCEERRORS	Number of sequence errors.	double precision.	
INVALIDTRANSMISSIONS	Number of invalid transmission errors.	double precision.	
CRCERRORS	Number of CRC errors.	double precision.	

TABLE 137 FC_PORT_STATS_30MIN

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double precision.	

TABLE 137 FC_PORT_STATS_30MIN (Continued)

Field	Definition	Format	Size
RX		double precision.	
TX_UTILIZATION		double precision.	
RX_UTILIZATION		double precision.	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
LINKFAILURES		double precision.	
TXLINKRESETS		double precision.	
RXLINKRESETS		double precision.	
SYNCLOSSES		double precision.	
SIGNALLOSSES		double precision.	
SEQUENCEERRORS		double precision.	
INVALIDTRANSMISSIONS		double precision.	
CRCERRORS		double precision.	
DATA_GAPS_IN5MIN		smallint	

TABLE 138 FC_PORT_STATS_2HOUR

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double precision.	
RX		double precision.	
TX_UTILIZATION		double precision.	
RX_UTILIZATION		double precision.	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	

TABLE 138 FC_PORT_STATS_2HOUR (Continued)

Field	Definition	Format	Size
LINKFAILURES		double precision.	
TXLINKRESETS		double precision.	
RXLINKRESETS		double precision.	
SYNCLOSSES		double precision.	
SIGNALLOSSES		double precision.	
SEQUENCEERRORS		double precision.	
INVALIDTRANSMISSIONS		double precision.	
CRCERRORS		double precision.	
DATA_GAPS_IN5MIN		smallint	
DATA_GAPS_IN30MIN		smallint	

TABLE 139 FC_PORT_STATS_1DAY

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double precision.	
RX		double precision.	
TX_UTILIZATION		double precision.	
RX_UTILIZATION		double‘ precision.	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
LINKFAILURES		double precision.	
TXLINKRESETS		double precision.	
RXLINKRESETS		double precision.	
SYNCLOSSES		double precision.	

TABLE 139 FC_PORT_STATS_1DAY (Continued)

Field	Definition	Format	Size
SIGNALLOSSES		double precision.	
SEQUENCEERRORS		double precision.	
INVALIDTRANSMISSIONS		double precision.	
CRCERRORS		double precision.	
DATA_GAPS_IN5MIN		smallint	
DATA_GAPS_IN30MIN		smallint	
DATA_GAPS_IN2HOUR		smallint	

FCIP

TABLE 140 FCIP_TUNNEL

Field	Definition	Format	Size
ID*		int	
ETHERNET_PORT_ID	GigE Port ID on which the tunnel is created.	int	
TUNNEL_ID	Tunnel ID for that GigE Port.	smallint	
VLAN_TAG	VLAN Tag on the tunnel (if present).	int	
SOURCE_IP	Source IP on which the tunnel is created.	char	64
DEST_IP	Destination IP on the other end of tunnel.	char	64
LOCAL_WWN	Local port WWN for the tunnel.	char	23
REMOTE_WWN_RESTRICT	Remote Port WWN for the tunnel.	char	23
COMMUNICATION_RATE	Bandwidth specified for the tunnel.	double	
MIN_RETRANSMIT_TIME	FCIP Tunnel Parameter.	int	
SELECTIVE_ACK_ENABLED	FCIP Tunnel Parameter.	smallint	
KEEP_ALIVE_TIMEOUT	FCIP Tunnel Parameter.	int	
MAX_RETRNASMISSION	FCIP Tunnel Parameter.	int	
PATH_MTU_DISCOVERY_ENABLED	FCIP Tunnel Parameter.	smallint	
WAN_TOV_ENABLED	FCIP Tunnel Parameter.	smallint	
TUNNEL_STATUS	Tunnel Status (Active/Inactive).	int	

TABLE 142 FCIP_PORT_TUNNEL_MAP

Field	Definition	Format	Size
SWITCHPORT_ID*	Switch Port ID.	int	
TUNNEL_ID*	FCIP Tunnel ID.	int	

TABLE 143 FCIP_TUNNEL_DETAILS

Field	Definition	Format	Size
TUNNEL_ID*	Tunnel ID for that GigE Port.	int	
COMPRESSION_ENABLED	Whether Compression is enabled on that tunnel.	smallint	
TURBO_WRITE_ENABLED	Whether TurboWrite is enabled on that tunnel.	smallint	
TAPE_ACCELERATION_ENABLED	Whether TapeAccelaration is enabled on that tunnel.	smallint	
IKE_POLICY_NUM	The IKE Policy on the tunnel.	int	
IPSEC_POLICY_NUM	The IPSEC Policy on the tunnel.	int	
PRESHARED_KEY	The Preshared Key on the tunnel.	char	32
FICON_TAPE_READ_BLOCK_ID_ENABLED	Whether Ficon_Tape_Read_Block is enabled on that tunnel.	smallint	

TABLE 143 FCIP_TUNNEL_DETAILS (Continued)

Field	Definition	Format	Size
FICON_TIN_TIR_ EMULATION_ENABLED	Whether Ficon_Tin_Tir_Emulation is enabled on that tunnel.	smallint	
FICON_DEVICE_LEVEL_ ACK_EMULATION_ENABLED	Whether Device_Level_Ack_Emulation is enabled on that tunnel.	smallint	
FICON_TAPE_WRITE_MAX_ PIPE	The value for this on the tunnel.	int	
FICON_TAPE_READ_MAX_ PIPE	The value for this on the tunnel.	int	
FICON_TAPE_WRITE_MAX_ OPS	The value for this on the tunnel.	int	
FICON_TAPE_READ_MAX_ OPS	The value for this on the tunnel.	int	
FICON_TAPE_WRITE_TIMER	The value for this on the tunnel.	int	
FICON_TAPE_MAX_WRITE_ CHAIN	The value for this on the tunnel.	int	
FICON_OXID_BASE	The value for this on the tunnel.	int	
FICON_XRC_EMULATION_ ENABLED	Whether XRC Emulation is enabled on the tunnel.	smallint	
FICON_TAPE_WRITE_ EMULATION_ENABLED	Whether this is enabled on that tunnel.	smallint	
FICON_TAPE_READ_ EMULATION_ENABLED	Whether this is enabled on that tunnel.	smallint	
FICON_DEBUG__FLAGS	FICON_DEBUG_FLAGS for that particular tunnel.	double	

FCIP Tunnel Stats

TABLE 144 FCIP_TUNNEL_STATS

Field	Definition	Format	Size
ID*		int	
TUNNEL_DBID	References the ID in FCIP_TUNNEL table.	int	
SWITCH_ID	References the ID in CORE_SWITCH table.	int	
CREATION_TIME	The polling time.	timestamp	
TX	Transmit (TX) value in bytes.	double precision	
RX	Receive (RX) value in bytes.	double precision	
TX_UTILIZATION	Transmit utilization value in percentage.	double precision	
RX_UTILIZATION	Receive utilization value in percentage.	double precision	
DROPPED_PACKETS	The number of dropped packets.	double precision	
COMPRESSION	The compression value.	double precision	
LATENCY	The latency value.	double precision	
LINK_RETRANSMITS	The number of link retransmits.	double precision	

TABLE 144 FCIP_TUNNEL_STATS (Continued)

Field	Definition	Format	Size
ACTIVE_STATE	State of collection: 0 = failed 1 = success	smallint	
RTT_BY_TO	Counter of retransmit packet by timeout.	double precision	
RTT_BY_DUP_ACK	Counter of retransmit packet by duplicate Ack.	double precision	
DUP_ACK	Counter of duplicate Ack	double precision	
RTT	Detected RTT for calculating window size	double precision	
TCP_OOO	Counter of TCP out of order	double precision	
SLOW_START	SlowStart status from stage 1 to 8	double precision	

TABLE 145 FCIP_TUNNEL_STATS_30MIN

Field	Definition	Format	Size
ID*		int	
TUNNEL_DBID		int	
SWITCH_ID		int	
CREATION_TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED_PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
LINK_RETRANSMITS		double precision	
ACTIVE_STATE		smallint	
RTT_BY_TO	Counter of retransmit packet by timeout.	double precision	
RTT_BY_DUP_ACK	Counter of retransmit packet by duplicate Ack.	double precision	
DUP_ACK	Counter of duplicate Ack	double precision	
RTT	Detected RTT for calculating window size	double precision	
TCP_OOO	Counter of TCP out of order	double precision	
SLOW_START	SlowStart status from stage 1 to 8	double precision	

TABLE 146 FCIP_TUNNEL_STATS_2HOUR

Field	Definition	Format	Size
ID*		int	
TUNNEL_DBID		int	
SWITCH_ID		int	

TABLE 146 FCIP_TUNNEL_STATS_2HOUR (Continued)

Field	Definition	Format	Size
CREATION_TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED_PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
LINK_RETRANSMITS		double precision	
ACTIVE_STATE		smallint	
RTT_BY_TO	Counter of retransmit packet by timeout.	double precision	
RTT_BY_DUP_ACK	Counter of retransmit packet by duplicate Ack.	double precision	
DUP_ACK	Counter of duplicate Ack	double precision	
RTT	Detected RTT for calculating window size	double precision	
TCP_OOO	Counter of TCP out of order	double precision	
SLOW_START	SlowStart status from stage 1 to 8	double precision	

TABLE 147 FCIP_TUNNEL_STATS_1DAY

Field	Definition	Format	Size
ID*		int	
TUNNEL_DBID		int	
SWITCH_ID		int	
CREATION_TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED_PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
LINK_RETRANSMITS		double precision	
ACTIVE_STATE		smallint	
RTT_BY_TO	Counter of retransmit packet by timeout.	double precision	
RTT_BY_DUP_ACK	Counter of retransmit packet by duplicate Ack.	double precision	
DUP_ACK	Counter of duplicate Ack	double precision	
RTT	Detected RTT for calculating window size	double precision	

TABLE 147 FCIP_TUNNEL_STATS_1DAY (Continued)

Field	Definition	Format	Size
TCP_OOO	Counter of TCP out of order	double precision	
SLOW_START	SlowStart status from stage 1 to 8	double precision	

GigE Port Stats

TABLE 148 FCIP_TUNNEL

Field	Definition	Format	Size
ID*		int	
TUNNEL_ID	Tunnel ID for that GigE Port.	smallint	
VLAN_TAG	VLAN Tag on the tunnel (if present). Default value is -1.	int	
SOURCE_IP	Source IP on which the tunnel is created.	char	64
DEST_IP	Destination IP on the other end of tunnel.	char	64
LOCAL_WWN	Local port WWN for the tunnel.	char	23
REMOTE_WWN_RESTRICT	Remote Port WWN for the tunnel.	char	23
COMMUNICATION_RATE	Bandwidth specified for the tunnel.	double precision	
MIN_RETRANSMIT_TIME	FCIP Tunnel Parameter.	int	
SELECTIVE_ACK_ENABLED	FCIP Tunnel Parameter.	smallint	
KEEP_ALIVE_TIMEOUT	FCIP Tunnel Parameter.	int	
MAX_RETRANSMISSION	FCIP Tunnel Parameter.	int	
WAN_TOV_ENABLED	Is WAN TOV enabled. Default value is 0.	smallint	
TUNNEL_STATUS	Tunnel Status (Active/Inactive).	int	
DESCRIPTION	Description for the created tunnel.	varchar	64
FICON_TRB_ID_ENABLED	Whether Ficon_Tape_Read_Block is enabled on that tunnel. Default value is 0.	smallint	
FICON_TT_EMUL_ENABLED	Whether Ficon_Tin_Tir_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_DLA_EMUL_ENABLED	Whether Device_Level_Ack_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_TAPE_WRITE_MAX_PIPE	The Value for FICON_TAPE_WRITE_MAX_PIPE on the tunnel. Default value is -1.	int	
FICON_TAPE_READ_MAX_PIPE	The Value for FICON_TAPE_READ_MAX_PIPE on the tunnel. Default value is -1.	int	
FICON_TAPE_WRITE_MAX_OPS	The Value for FICON_TAPE_WRITE_MAX_OPS on the tunnel. Default value is -1.	int	
FICON_TAPE_READ_MAX_OPS	The Value for FICON_TAPE_READ_MAX_OPS on the tunnel. Default value is -1.	int	

TABLE 148 FCIP_TUNNEL (Continued)

Field	Definition	Format	Size
FICON_TAPE_WRITE_TIMER	The Value for FICON_TAPE_WRITE_TIMER on the tunnel. Default value is -1.	int	
FICON_TAPE_MAX_WRITE_CHAIN	The Value for FICON_TAPE_MAX_WRITE_CHAIN on the tunnel. Default value is -1.	int	
FICON_OXID_BASE	The Value for FICON_OXID_BASE on the tunnel. Default value is -1.	int	
FICON_XRC_EMULATION_ENABLED	Whether Xrc_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_TW_EMUL_ENABLED	Whether Ficon_Tape_Write_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_TR_EMUL_ENABLED	Whether Ficon_Tape_Read_Emulation is enabled on that tunnel. Default value is 0.	smallint	
FICON_DEBUG_FLAGS	FICON_DEBUG_FLAGS for that particular tunnel. Default value is -1.	double precision	
REMOTE_WWN	Configured WWN of the Remote Node.	char	64
CDC	CDC Flag. Default value is 0.	smallint	
ADMIN_STATUS	Admin Status of the Tunnel. Default value is 0.	smallint	
CONTROL_L2_COS	Class of service as defined by IEEE 802.1p for tunnel. Default value is -1.	int	
DSCP_CONTROL	DiffServe marking for control frame. Default value is -1.	int	
TRUNKING_ALGORITHM	Trunking Algorithm. Default value is -1.	int	
EXTENDED_TUNNEL	Indicates if the tunnel is an Extended Tunnel (i.e. new Tunnel type on the switch). Default value is 0.	smallint	
VIRTUAL_SWITCH_ID	Refers to the virtual switch to which the tunnel record belongs to.	int	
CIRCUIT_COUNT	The number of circuits configured on the tunnel. Default value is 1.	smallint	
MISMATCHED_CONFIG_DETAILS	Details of the reasons as to why the tunnel is down.	varchar	2048
LAST_UPDATE		bigint	
SLOT_NUMBER	SLOT_NUMBER on which the VE Port of the tunnel exists. Default value is 0.	int	
FICON_ENABLED	Is Ficon enabled. Default: 0, Values: 0|1. Default value is 0.	smallint	

TABLE 148 FCIP_TUNNEL (Continued)

Field	Definition	Format	Size
TPERF_ENABLED	Is Tperf enabled. Default: 0, Values: 0|1. Default value is 0.	smallint	
AUTH_KEY	This is the preshared-key to be used during IKE authentication.	varchar	128
CONNECTED_COUNT	Active connections count. Default value is 1.	smallint	
TUNNEL_STATUS_STRING	Tunnel Status string value from switch for the tunnel.	varchar	256
COMPRESSION_MODE	Compression mode value (0,1,2,3). Default value is 0.	smallint	
TURBO_WRITE_ENABLED	Whether turbo write (fast write) is enabled or not (0,1). Default value is 0.	smallint	
TAPE_ACCELERATION_ENABLED	Whether turbo write (fast write) is enabled or not (0,1). Default value is 0.	smallint	
IPSEC_ENABLED	Default value is 0.	smallint	
PRESHARED_KEY	The preshared key on tunnel.	char	32

TABLE 149 GIGE_PORT_STATS

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	References the ID in CORE_SWITCH table.	int	
PORT_ID	References the ID in SWITCH_PORT table.	int	
CREATION_TIME	The polling time.	timestamp	
TX	Transmit (TX) value in bytes.	double precision	
RX	Receive (RX) value in bytes.	double precision	
TX_UTILIZATION	Transmit utilization (TX%) value in percentage.	double precision	
RX_UTILIZATION	Receive utilization (RX%) value in percentage.	double precision	
DROPPED_PACKETS	Number of dropped packets.	double precision	
COMPRESSION	The compression value.	double precision	
LATENCY	The latency value.	double precision	
BANDWIDTH	The bandwidth value.	double precision	

TABLE 150 GIGE_PORT_STATS_30MIN

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
CREATION_TIME		timestamp	

TABLE 150 GIGE_PORT_STATS_30MIN (Continued)

Field	Definition	Format	Size
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED_PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
BANDWIDTH		double precision	

TABLE 151 GIGE_PORT_STATS_2HOUR

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
CREATION_TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED_PACKETS		double precision	
COMPRESSION		double precision	
LATENCY		double precision	
BANDWIDTH		double precision	

TABLE 152 GIGE_PORT_STATS_1DAY

Field	Definition	Format	Size
ID*		int	
SWITCH_ID		int	
PORT_ID		int	
CREATION_TIME		timestamp	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
DROPPED_PACKETS		double precision	
COMPRESSION		double precision	

TABLE 152 GIGE_PORT_STATS_1DAY (Continued)

Field	Definition	Format	Size
LATENCY		double precision	
BANDWIDTH		double precision	

TABLE 155 ISL

Field	Definition	Format	Size
ID*		int	
FABRIC_ID	Fabric DB ID.	int	
SOURCE_DOMAIN_ID	Source domain ID.	int	
SOURCE_PORT_NUMBER	Source port number.	smallint	
DEST_DOMAIN_ID	Destination domain ID.	int	
DEST_PORT_NUMBER	Destination port number.	smallint	
COST	The cost of the link.	int	
TYPE	The type of link.	smallint	
TRUSTED	1 = ISL is trusted 0 = ISL is not trusted Default value is 0.	smallint	
CREATION_TIME	Time at which this record was created. Default value is 'now()'.	timestamp	
MISSING	1 = ISL is missing 0 = ISL is not missing Default value is 0.	smallint	
MISSING_TIME	Time at which ISL went missing.	timestamp	

TABLE 156 FABRIC

Field	Definition	Format	Size
ID*		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256
TYPE	Type of fabric: 0 = legacy fabric 1 = base fabric 2 = logical fabric	smallint	
SECURE	1 = it is a secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	

TABLE 156 FABRIC (Continued)

Field	Definition	Format	Size
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone set which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 157 ISL_TRUNK_MEMBER

Field	Definition	Format	Size
GROUP_ID*	ISL_TRUNK_GROUP DB ID.	int	
PORT_NUMBER*	Port number of member port.	smallint	

TABLE 158 ISL_TRUNK_GROUP

Field	Definition	Format	Size
ID*		int	
VIRTUAL_SWITCH_ID	Virtual switch DB ID.	int	
MASTER_USER_PORT	Port number of master port.	smallint	

License

TABLE 159 LICENSE_FEATURE_MAP

Field	Definition	Format	Size
LICENSE_ID*	Foreign Key (SWITCH_LICENSE.ID) and is part of the primary key.	int	
FEATURE_ID*	Foreign Key (LICENSED_FEATURE.ID) and is part of the primary.	int	

TABLE 160 LICENSED_FEATURE

Field	Definition	Format	Size
ID*		int	
NAME	License feature name, a short text description.	varchar	64
DESCRIPTION	Optional detailed description about the license feature.	varchar	256

TABLE 161 SWITCH_LICENSE

Field	Definition	Format	Size
ID*		int	
CORE_SWITCH_ID	Refers to the entry in the CORE_SWITCH table.	int	
LICENSE_KEY	Stores the license key obtained from the switch.	varchar	256

TABLE 162 CORE_SWITCH

Field	Definition	Format	Size
ID*		int	
IP_ADDRESS	IP address of the switch.	varchar	128
WWN	Chassis WWN.	char	23
NAME	Switch name.	varchar	64
TYPE	SWBD type number as given by Fabric OS. Default value is 0.	smallint	
MODEL	Model type of the switch: 0 = Unknown 1 = Not applicable 2 = Fabric OS switch 3 = M-EOS switch	smallint	
FIRMWARE_VERSION	Embedded (Fabric OS or M-EOS) software version.	varchar	128
VENDOR	Switch vendor.	varchar	256
MAX_VIRTUAL_SWITCHES	Maximum virtual switches allowed on this physical switch. Default vaue is 1.	smallint	
NUM_VIRTUAL_SWITCHES	Actual number of virtual switches carved out of this physical switch. 0 means it is not operating in Virtual Fabric model. Default value is 0.	smallint	
REACHABLE	Whether reachable by HTTP.	smallint	
UNREACHABLE_TIME	When the switch became unreachable from HTTP.	timestamp	
OPERATIONAL_STATUS	Operational status as reported by the embedded software..	varchar	128
CREATION_TIME	Time when this record was created by the Management application. Default is ’now()’.	timestamp	
LAST_SCAN_TIME	Time when this record was last updated.	timestamp	

TABLE 162 CORE_SWITCH (Continued)

Field	Definition	Format	Size
LAST_UPDATE_TIME	1 = the Management application server is registered with the switch to receive Syslog. Default is 'now()'.	timestamp	
SYSLOG_REGISTERED	1 = Syslog is enabled for this switch. Default value is 0.	smallint	
CALL_HOME_ENABLED	1 = call home is enabled for this switch. Default value is 1.	smallint	
SNMP_REGISTERED	1 = the Management application server is registered with the switch to receive SNMP traps. Default value is 0.	smallint	
USER_IP_ADDRESS	User-assigned IP address. This is used for M-EOS switches where Fabric OS seed switch fails to get the IP address of the M-EOS switch.	varchar	128
NIC_PROFILE_ID	NIC profile of the Management application server host used by this switch to communicate in interactive configuration and other operations. It determines which Management application host IP used by this switch.	int	
MANAGING_SERVER_IP_ ADDRESS	IP address(v4/v6) of the Management applciation server which is currently managing the M-model switch. Used for M-EOS switch only. It does not apply to Fabric OS switches.	varchar	128
VF_ENABLED	Default value is 0.	smallint	
VF_SUPPORTED	Default value is 0	smallint	
MANAGED_ELEMENT_ID	A unique managed element ID for this physical switch. Also a foreign key reference to the MANAGED_ELEMENT table.	int	
NAT_PRIVATE_IP_ADDRESS	NAT private IP Address. Feature available from NMS DC Eureka release onwards. During a successful NAT translation the Private IP that gets translated will be stored in this field. The new translated IP Address will be stored in the existing IP_ADDRESS field. All the NAT look up will be done using the NAT Private IP Address.	varchar	128
ALTERNATE_IP_ADDRESS	Alternate IP address of the switch. Feature available from Eureka release onwards. During fabric discovery the column will be populated based on the values in the fabricinfo.html. If Management applciation server is IPV6 capable, then we store the switchetherIP NVP else we store the switchetherIPV6. So could be either IPV4 or IPV6 address. If there exists any NAT translation, translated IP will be used.	varchar	128

Encryption Device

TABLE 163 KEY VAULT

Field	Definition	Format	Size
ID*		int	
IP_ADDRESS	The IP Address (IPv4, IPv6, or hostname) of the key vault.	varchar	512
PORT_NUMBER	The TCP port number for the key vault.	int	
PUBLIC_CERTIFICATE	The key vault's public key certificate. Switches use this to establish a secure connection to the key vault.	varchar	4096
CRETIFICATE_LABEL	A text name to identify the certificate.	varchar	64
POSITION	Whether this key vault is the primary key vault or the backup key vault: 0 = primary 1 = backup	smallint	

TABLE 164 CRYPTO_SWITCH

Field	Definition	Format	Size
SWITCH_ID*	Primary key. The value is the same as the primary key of a record in the VIRTUAL_SWITCH table	int	
ENCRYPTION_GROUP_ID	Foreign key to the ENCRYPTION_GROUP table. Identifies the Encryption Group that this switch belongs to. Null indicates the switch is not part of an Encryption Group.	int	
GROUP_LEADER_POSITION	No longer used. Previously indicated whether this switch is the group leader. Use GROUP_LEADER_ID in the ENCRYPTION_GROUP table instead.	smallint	
TAPE_ENCRYPTION	No longer used. Previously enabled or disabled tape encryption at the switch level. This feature has been removed from Fabric OS. Default value is 0.	smallint	
TAPE_KEY_POLICY	No longer used. Previously used to configure a separate data encryption key per volume or per group. This feature has been removed from Fabric OS. Default value is 0.	smallint	
PRIMARY_VAULT_LINK_ STATUS	The status of the link key for the primary key vault. Link keys are used only for NetApp LKM key vaults. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	
BACKUP_VAULT_LINK_ STATUS	The status of the link key for the backup key vault. Link keys are used only for NetApp LKM key vaults. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	

TABLE 164 CRYPTO_SWITCH (Continued)

Field	Definition	Format	Size
CP_CERTIFICATE	The public key certificate, in PEM format, of the switch's Control Processor module. This certificate is exchanged with other switches to establish secure communication between switches in an Encryption Group.	varchar	4096
KAC_CERTIFICATE	The public key certificate, in PEM format, of the switch's Key Archive Client module. This certificate is installed on key vaults to establish secure communication between this switch and the key vault.	varchar	4096
PRIMARY_VAULT_ CONNECTIVITY_STATUS	The status of the network connection between this switch and the primary key vault. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	
BACKUP_VAULT_ CONNECTIVITY_STATUS	The status of the network connection between this switch and the backup key vault. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	

TABLE 165 ENCRYPTION GROUP

Field	Definition	Format	Size
ID*		int	
NAME	User-assigned name for this encryption group.	varchar	64
LEADER_SWITCH_ID	Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that currently provides central configuration and reporting capabilities for the encryption group. This column may be null if the group leader is not in a discovered fabric.	int	
LEADER_SWITCH_WWN	The Node WWN of the current group leader switch. Each encryption group has one group leader switch.	char	23
DEPLOYMENT_MODE	Indicates Transparent (0) or Non Transparent (1) deployment mode. Only Transparent mode is currently supported. All switches in the Encryption Group share the same deployment mode. Transparent mode uses re-direction zones to preserve existing zoning of physical hosts and targets. Non-transparent mode requires zoning changes to zone physical hosts with Virtual Targets and to zone Virtual Initiators with physical targets.	smallint	
FAILBACK_MODE	Indicates Automatic (0) or Manual (1) failback. Failback occurs when a previously unavailable Encryption Engine comes back online. In Auto mode, the restored EncryptionEngine resumes encrypting all traffic for target containers configured on the Encryption Engine. In manual mode, encryption continues running on the backup encryption engines until manually changed.	smallint	

TABLE 165 ENCRYPTION GROUP (Continued)

Field	Definition	Format	Size
SYSTEM_CARD_REQUIRED	Boolean value that indicates whether a System Card (smart card) must be inserted in the Encryption Engine to enable the engine after power-up. This feature is not yet supported.	smallint	
ACTIVE_MASTER_KEY_STATUS	The operational status of the "master key" or "Key Encryption Key (KEK)" used to encrypt Data Encryption Keys in a key vault. Not used for NetApp LKM key vaults. 0 = not used 1 = required but not present 2 = present but not backed up 3 = okay	smallint	
ALT_MASTER_KEY_STATUS	The operational status of an alternate "master key" used to access older data encryption keys. Not used for NetApp LKM key vaults. 0 = not used 1 = not present 3 = okay	smallint	
QUORUM_SIZE	The number of authentication cards required to approve certain secure operations. This feature is not yet supported.	smallint	
RECOVERY_SET_SIZE	No longer used. Previously used to indicate the number of smart cards used to back up a Master Key. The number of cards is now specified when the backup is created, and not persisted in the database.	smallint	
KEY_VAULT_TYPE	Indicates the type of key vault used by switches in this Encryption Group. 0 = NetApp Lifetime Key Manager (LKM) 1 = RSA Key Manager (RKM) 2 = Internal key storage (for demo use only)	smallint	
PRIMARY_KEY_VAULT_ID	Foreign key reference to the KEY_VAULT record that describes the primary key vault for this Encryption Group. Null if no primary key vault is configured.	int	
BACKUP_KEY_VAULT_ID	Foreign key reference to the KEY_VAULT record that describes the backup key vault for this Encryption Group. Null if no backup key vault is configured.	int	
GROUP_LEADER_STATUS	Stores the status of the Group leader node	int	

TABLE 166 ENCRYPTION_TAPE_POOL

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	No longer used. Tape pools used to belong to specific switches, but are now shared by all switches in an encryption group.	int	
ENCRYPTION_ENGINE_ID	No longer used. Tape pools used to belong to specific encryption engines, but are now shared by all encryption engines in an encryption group.	int	

TABLE 166 ENCRYPTION_TAPE_POOL (Continued)

Field	Definition	Format	Size
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP record that describes which Encryption Group this tape pool belongs to.	int	
TAPE_POOL_NAME	User-supplied name or number for the tape pool. This is the same name or number specified in the tape backup application. Numbers are stored in hex.	varchar	64
TAPE_POOL_OPERATION_MODE	Specifies which type of encryption should be used by tape volumes in this tape pool. 0 = Native 1 = DF-compatible.	smallint	
TAPE_POOL_POLICY	Specifies whether tape volumes in this tape pool should be encrypted. 0 = encrypted 1 = cleartext	smallint	
KEY_EXPIRATION	Number of days each data encryption key for this tape pool should be used. After the configured number of days, a new data encryption key is automatically generated for any further tape volumes in this pool. 0 = no expiration.	int	
TAPE_POOL_LABEL_TYPE	Indicates whether the TAPE_POOL_NAME field is a name or a number. 0 = name 1 = number	smallint	

TABLE 167 RECOVERY_CARD_GROUP_MAPPING

Field	Definition	Format	Size
ID*		int	
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP for which a recovery card is registered.	int	
SMART_CARD_ID	Foreign key reference to the SMART_CARD that is registered as a recovery card for the encryption group.	int	
POSITION_	The position of the card within the recovery card set. 1 = first card, 2 = second card, etc.	int	

TABLE 168 ENCRYPTION_GROUP_MEMBER

Field	Definition	Format	Size
ID*		int	
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP record that identifies the encryption group that this member switch belongs to.	int	
MEMBER_IP_ADDRESS	The management IP address (IPv4, IPv6, or hostname) of the member switch.	varchar	128

TABLE 168 ENCRYPTION_GROUP_MEMBER (Continued)

Field	Definition	Format	Size
MEMBER_WWN	The Node WWN of the member switch.	char	23
MEMBER_STATUS	The reachability status of the member switch as seen by the group leader switch. For possible values see the enum definition in the DTO class. Default value is 0.	smallint	

TABLE 169 QUORUM_CARD_GROUP_MAPPING

Field	Definition	Format	Size
ID*		int	
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP for which an authorization card is registered.	int	
SMART_CARD_ID	Foreign key reference to the SMART_CARD that is registered as an authorization card for the encryption group.	int	

TABLE 170 HA CLUSTER

Field	Definition	Format	Size
ID*		int	
NAME	User-supplied name for the HA Cluster.	varchar	64
ENCRYPTION_GROUP_ID	Foreign key reference to the ENCRYPTION_GROUP that contains this HA Cluster.	int	
MEMBER_LIST	A comma-separated list of Encryption Engines in the HA Cluster. Each engine is identified by a switch node WWN, followed by a slash “/”, followed by the slot number. The slot number is 0 if the switch does not have removable blades.	varchar	256

TABLE 171 SMART CARD

Field	Definition	Format	Size
GROUP_NAME	The name of the Encryption Group used to initialize the card. For recovery set cards, this identifies which group's master key is backed up on the card.	varchar	64
CREATION_TIME	The date and time that the card was initialized. For recovery set cards, this is the date and time the master key was written to the card.	timestamp	256

TABLE 172 ENCRYPTION ENGINE

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that contains this encryption engine.	int	
SLOT NUMBER	For chassis switches, the slot or blade that contains the encryption engine. Always 0 for switches with a single embedded encryption engine.	smallint	64
STATUS	Not used. Previously used to indicate the engine's operational status. Replaced by EE_STATE.	smallint	64
HA_CLUSTER_ID	Foreign key reference to an HA_CLUSTER record. Identifies the HA Cluster that this engine belongs to. Null if this engine does not belong to an HA Cluster.	int	64
SYSTEM_CARD_ID	Foreign key reference to the SMART_CARD record that identifies the System Card required to enable this engine. Null if no System Card has been registered yet. This feature is not yet supported.	int	256
SYSTEM_CARD_STATUS	Indicates whether a System Card is currently inserted in the Encryption Engine, and whether the card is valid or not. This feature is not yet supported.	smallint	4096
WWN_POOLS_AVAILABLE	Not used. Previously used to indicate the number of WWN pools remaining for allocation on this encryption engine. This feature is no longer supported.	int	64
STATE	Administrative state for this engine: 0 = disabled 1 = enabled	smallint	64
SP_CERTIFICATE	The public key certificate, in PEM format, for the Security Processor within the Encryption Engine. Used to create link keys for NetApp LKM key vaults.	varchar	4096
EE_STATE	The operational status of this Encryption Engine. For possible values, see the enum definition in the DTO class.	int	

Encryption Container

TABLE 173 CRYPTO HOST

Field	Definition	Format	Size
ID*		int	
CRYPTO_TARGET_CONTAINER_ID	Foreign key reference to the CRYPTO_TARGET_CONTAINER that contains this host.	int	
VI_NODE_WWN	Node WWN of Virtual Initiator that represents this host.	char	23
VI_PORT_WWN	Port WWN of Virtual Initiator that represents this host.	char	23
HOST_PORT_WWN	Physical (real) host’s Port WWN	char	23
HOST_NODE_WWN	Physical (real) host’s Node WWN	char	23

TABLE 174 CRYPTO TARGET CONTAINER

Field	Definition	Format	Size
ID*		int	
ENCRYPTION_ENGINE_ID	Foreign key reference to the ENCRYPTION_ENGINE that owns this container.	int	
NAME	A user-supplied name for the container.	varchar	64
VT_NODE_WWN	The Node WWN of the Virtual Target that represents the real physical target device.	char	23
VT_PORT_WWN	The Port WWN of the Virtual Target that represents the real physical target device.	char	23
FAILOVER_STATUS	Indicates whether this container’s target is being encrypted by the encryption engine on which the container is configured (value 0) or by another encryption engine in the HA Cluster (value 1).	smallint	
DEVICE_STATUS	The physical target storage device operational status when the virtual initiator last attempted to access the target. For possible values, see the enum definition in the DTO class.	smallint	
DEVICE_TYPE	Indicates whether the target storage device is a disk (0) or tape (1) device.	smallint	
TARGET_PORT_WWN	The Port WWN of the physical target storage device associated with this container.	char	23
TARGET_NODE_WWN	The Node WWN of the physical target storage device associated with this container	char	23

TABLE 175 CRYPTO LUN

Field	Definition	Format	Size
ID*		int	
CRYPTO_TARGET_ CONTAINER_ID	Foreign key reference to the CRYPTO_TARGET_CONTAINER that contains the host for which these LUNs are configured.	int	

TABLE 175 CRYPTO LUN (Continued)

Field	Definition	Format	Size
SERIAL_NUMBER	The LUN serial number, used to identify the physical LUN.	varchar	64
ENCRYPTION_STATE	Boolean. True (1) if LUN is being encrypted. False (0) if cleartext.	smallint	
STATUS	Not currently used but left in for possible future use. Replaced by LUN_STATE.	smallint	
REKEY_INTERVAL	The number of days that data encryption keys should be used before automatically generating a new key. 0 = infinite, i.e., no re-keying.	int	
VOLUME_LABEL_PREFIX	A user-configured string used to construct the Brocade-specific volume label on encrypted tapes. Ignored for disk LUNs.	varchar	256
LAST_REKEY_DATE	The last time a data encryption key was generated for this LUN. REKEY_INTERVAL days after this date, a new key will be generated.	timestamp	
LAST_REKEY_STATUS	The success or failure of the most recent re-keying operation, if any. This field is not currently used, but is left in the hope that Fabric OS will support it in the future. Only valid for disk LUNs.	smallint	
LAST_REKEY_PROGRESS	Indicates whether a re-key operation is in progress. 0 = no re-keying in progress. > 0 = percentage done of re-keying operation in progress. Only valid for disk LUNs.	smallint	
CURRENT_VOLUME_LABEL	If a tape session is in progress, this is the volume label for the currently mounted tape. Only valid for tape LUNs.	varchar	2048
PRIOR_ENCRYPTION_STATE	Not used. When configuring a new disk LUN, this field indicates whether the LUN is already encrypted (1) or cleartext (0). This information does not need to be persisted. Only valid for disk LUNs.	smallint	
ENCRYPTION_FORMAT	If ENCRYPTION_STATE is true, ENCRYPTION_FORMAT indicates the type of encryption. 0 = cleartext, 1 = DF-compatible, 2 = native.	smallint	
ENCRYPT_EXISTING_DATA	Not used. When configuring a disk LUN that was previously cleartext and is to be encrypted, this property tells the switch whether or not to start a re-keying operation to encrypt the existing LUN data. This property does not need to be persisted.	smallint	
DECRYPT_EXISTING_DATA	Not used. When configuring disk LUN that was previously encrypted and is to become cleartext, this property tells the switch whether or not to start a re-keying operation to decrypt the existing LUN data. This property does not need to be persisted. This feature is no longer supported in Fabric OS.	smallint	
KEY_ID	Hex-encoded binary key vault ID for the current data encryption key for this LUN. This ID may be used to locate the data encryption key in the key vault	varchar	64

TABLE 175 CRYPTO LUN (Continued)

Field	Definition	Format	Size
CRYPTO_HOST_ID	Foreign key reference to the CRYPTO_HOST that uses this LUN.	int	
LUN_NUMBER	The Logical Unit Number of the LUN, as seen by the LUNs host. This may be an integer (0 - 65565) or a WWN-format 8-byte hex number.	varchar	23
BLOCK_SIZE	'The LUN's Logical Block Size, in bytes. Only valid for disk LUNs.	int	
TOTAL_BLOCKS	The total number of logical blocks in the LUN. Multiplying BLOCK_SIZE by TOTAL_BLOCKS gives the LUN size in bytes.	int	
LUN_STATE	LUN operational status, such as OK or disabled for various reasons. For possible values see the enum definition in CryptoClientConstants.	int	
LUN_FLAGS	Bitmap of LUN options. The only option currently used is bit 0 (least significant) which indicates that the LUN must be manually enabled because it has been disabled due to inconsistent metadata detected.	bigint	

TABLE 176 ENCRYPTION ENGINE

Field	Definition	Format	Size
ID*		int	
SWITCH_ID	Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that contains this encryption engine.	int	
SLOT_NUMBER	For chassis switches, the slot or blade that contains the encryption engine. Always 0 for switches with a single embedded encryption engine.	smallint	
STATUS	Not used. Previously used to indicate the engine's operational status. Replaced by EE_STATE.	smallint	
HA_CLUSTER_ID	Foreign key reference to an HA_CLUSTER record. Identifies the HA Cluster that this engine belongs to. Null if this engine does not belong to an HA Cluster.	int	
SYSTEM_CARD_ID	Foreign key reference to the SMART_CARD record that identifies the System Card required to enable this engine. Null if no System Card has been registered yet. This feature is not yet supported.	int	
SYSTEM_CARD_STATUS	Indicates whether a System Card is currently inserted in the Encryption Engine, and whether the card is valid or not. This feature is not yet supported.	smallint	
WWN_POOLS_AVAILABLE	Not used. Previously used to indicate the number of WWN pools remaining for allocation on this encryption engine. This feature is no longer supported.	int	
STATE	Administrative state for this engine: 0 = disabled 1 = enabled	smallint	

TABLE 176 ENCRYPTION ENGINE (Continued)

Field	Definition	Format	Size
SP_CERTIFICATE	The public key certificate, in PEM format, for the Security Processor within the Encryption Engine. Used to create link keys for NetApp LKM key vaults.	varchar	4096
EE_STATE	The operational status of this Encryption Engine. For possible values, see the enum definition in the DTO class.	int	

Meta SAN

TABLE 179 LSAN_DEVICE

Field	Definition	Format	Size
ID*		int	
BB_FABRIC_ID	Backbone fabric DB ID.	int	
FCR_FABRIC_ID	FID assigned to edge fabric.	int	
DEVICE_PORT_WWN	Device port WWN of physical device.	char	23
PHYSICAL_PID	PID of physical device.	char	6

TABLE 180 LSAN_PROXY_DEVICE

Field	Definition	Format	Size
FCR_FABRIC_ID*	FID assigned to edge fabric	int	
PROXY_PID*	Proxy device PID	char	6
STATE	State of the device	varchar	128
LSAN_DEVICE_ID*	LSAN_DEVICE record reference	int	

TABLE 181 FCR_ROUTE

Field	Definition	Format	Size
ID*		int	
BB_FABRIC_ID	Backbone fabric DB ID.	int	
FCR_FABRIC_ID	FID assigned to edge fabric.	int	
SWITCH_WWN	WWN of the router switch.	varchar	128
NR_PORT_ID	Route parameter.	int	
FCRP_COST	Route parameter.	int	
EX_PORT_WWN	Ex_port WWN.	varchar	128

TABLE 182 FABRIC

Field	Definition	Format	Size
ID*		int	
SAN_ID	Foreign key to SAN table; usually 1 since there is only one SAN.	int	
SEED_SWITCH_WWN	WWN of the virtual switch used as seed switch to discover the fabric.	char	23
NAME	User-assigned fabric name.	varchar	256
CONTACT	User-assigned "contact" for the fabric.	varchar	256
LOCATION	User-assigned "location" for the fabric.	varchar	256
DESCRIPTION	User-assigned fabric description.	varchar	256

TABLE 182 FABRIC (Continued)

Field	Definition	Format	Size
TYPE	Type of fabric: 0 = legacy fabric 1 = base fabric 2 = logical fabric	smallint	
SECURE	1 = it is a secured fabric.	smallint	
AD_ENVIRONMENT	1 = there are user-defined ADs in this fabric.	smallint	
MANAGED	1 = it is an actively "monitored" fabric; otherwise, it is an "unmonitored" fabric.	smallint	
MANAGEMENT_STATE	Bit map to indicate various management indications for the fabric.	smallint	
TRACK_CHANGES	1 = changes (member switches, ISL and devices) in the fabric are tracked.	smallint	
STATS_COLLECTION	1 = statistics collection is enabled on the fabric.	smallint	
CREATION_TIME	When the fabric record is inserted, i.e., created.	timestamp	
LAST_FABRIC_CHANGED	Time when fabric last changed.	timestamp	
LAST_SCAN_TIME		timestamp	
LAST_UPDATE_TIME	Time when fabric was last updated.	timestamp	
ACTIVE_ZONESET_NAME	Name of the zone set which is effective / active in that fabric.	varchar	256
USER_DEFINED_VALUE_1	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_2	User-defined custom value.	varchar	256
USER_DEFINED_VALUE_3	User-defined custom value.	varchar	256

TABLE 183 IFL

Field	Definition	Format	Size
ID*		int	
EDGE_FABRIC_ID	Edge Fabric ID.	int	
EDGE_PORT_WWN	Edge Fabric Port WWN.	varchar	128
BB_FABRIC_ID	Backbone Fabric ID.	int	
BB_PORT_WWN	Backbone Fabric Port WWN.	varchar	128
BB_RA_TOV	Backbone RA TOV.	int	
BB_ED_TOV	Backbone ED TOV.	int	
BB_PID_FORMAT	Backbone PID Format.	smallint	

Network

TABLE 185 IP_INTERFACE

Field	Definition	Format	Size
ID*		int	
ETHERNET_PORT_ID	GigE Port ID.	int	
IP_ADDRESS	IP address on the Ip_interface.	varchar	64
NET_MASK	Subnet mask for the interface.	varchar	64
MTU_SIZE	MTU Size for that interface.	int	
CHECKSUM	Check Sum.	varchar	64

TABLE 186 IP_ROUTE

Field	Definition	Format	Size
ID*		int	
ETHERNET_PORT_ID	GigE Port ID.	int	
PORT_NUMBER	Port Number related to the GigE Port.	int	
SLOT_NUMBER	Slot Number related to the GigE Port.	int	
NET_MASK	Subnet Mask for the Route.	varchar	64
GATEWAY	Gateway for the Route.	varchar	64
IP_ADDRESS	IP Address created after "”&”" operation of gateway.	varchar	64
METRIC	Metric.	int	
FLAG	Flag.	int	
CHECKSUM	Check Sum.	varchar	64

Others

TABLE 187 SYSTEM_PROPERTY

Field	Definition	Format	Size
NAME*	The name of the property.	char	64
VALUE	The value for the property.	varchar	2048

TABLE 188 OUI_VENDOR

Field	Definition	Format	Size
OUI*	Vendor OUI, 6-digit hexadecimal number which can have leading digits as zero.	char	6
VENDOR	Vendor name.	varchar	64
VENDOR_CATEGORY	Default is ‘none’.	varchar	32

TABLE 189 OUI_GUESSED_DEVICE_MAP

Field	Definition	Format	Size
OUI*	Vendor OUI.	char	6
TYPE	Guessed device type for this vendor.	varchar	32

TABLE 190 FEATURE

Field	Definition	Format	Size
FEATURE_ID*	ID used to uniquely identify the feature.	int	6
NAME	Name of the feature.	varchar	256
DESCRIPTION	Description for the feature.	varchar	256

TABLE 191 FEATURE_EDITION_MAP

Field	Definition	Format	Size
FEATURE_ID*	ID used to uniquely identify the feature.	int	
EDITION_MASK	Used to associate a feature to the edition (Reserved for future).	int	

Port Fencing

TABLE 192 PORT_FENCING_POLICY

Field	Definition	Format	Size
ID*		int	
NAME	Name of the policy. The length of the field should be 62 because M-Model switch supports only maximum 62 characters.	varchar	62
TYPE	0 = ISL Protocol 1 = Link 2 = Security	smallint	
THRESHOLD_LIMIT	Threshold Limits for M-Model Switch.	int	
THRESHOLD_DURATION	Duration In minutes for M-Model Switch.	int	
DEFAULT_POLICY	1 = the default port fencing policies. 0 = the non-default policies. The default port fencing policies are: For ISL - Default Protocol Error Policy For Link Violation type - Default Link Level Policy For Security - Default Security Policy	smallint	
B_THRESHOLD_LIMIT	Threshold Limits for B-Model Switch (Not Supported).	int	
B_THRESHOLD_DURATION	Duration in minutes for B-Model Switch (Not Supported).	int	

TABLE 193 PORT_FENCING_POLICY_MAP

Field	Definition	Format	Size
ID*		int	
POLICY_ID	Foreign key to ID column of PORT_FENCING_POLICY table.	int	
LEVEL	0 = All Fabric 1 = Fabric 2 = Core Switch Group 3 = Switch 4 = Port Type 5 = Port List	smallint	
SUB_LEVEL	1 = E_Port 2 = F_Port 3 = FL_Port, Fabric WWN, Switch WWN	char	23
NODE	WWN of Node which policy assigned.	char	23
INHERITANCE	Directly assigned or inherited from root level. 0 = Directly assigned 1 = Indirectly assigned	smallint	

Quartz

TABLE 194 QRTZ_JOB_DETAILS

Field	Definition	Format	Size
JOB_NAME*	Name of the job.	varchar	80
JOB_GROUP*	Name of the job group.	varchar	80
DESCRIPTION	Description of the job (optional).	varchar	120
JOB_CLASS_NAME	The instance of the job that will be executed.	varchar	128
IS_DURABLE	Whether the job should remain stored after it is orphaned.	boolean	
IS_VOLATILE	Whether the job should not be persisted in the JobStore for re-use after program restarts.	boolean	
IS_STATEFUL	Whether the job implements the interface StatefulJob.	boolean	
REQUESTS_RECOVERY	Instructs the scheduler whether or not the job should be re-executed if a "recovery" or "fail-over" situation is encountered.	boolean	
JOB_DATA	To persist the job-related and application-related informations.	bytea	

TABLE 195 QRTZ_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
JOB_NAME	Name of the job.	varchar	80

TABLE 195 QRTZ_TRIGGERS (Continued)

Field	Definition	Format	Size
JOB_GROUP	Name of the job group.	varchar	80
IS_VOLATILE	Whether the trigger should be persisted in the JobStore for re-use after program restarts.	boolean	
DESCRIPTION	A description for the trigger instance - may be useful for remembering/displaying the purpose of the trigger, though the description has no meaning to Quartz.	varchar	120
NEXT_FIRE_TIME	The next fire time in milliseconds.	numeric	13,0
PREV_FIRE_TIME	The previous fired time in milliseconds.	numeric	13,0
TRIGGER_STATE	The state of the trigger (viz. Error, wait,etc.)	varchar	16
TRIGGER_TYPE	The type of the trigger (Simple,cron).	varchar	8
START_TIME	The job start time.	numeric	13,0
END_TIME	The job end time (-1 means infinite).	numeric	13,0
CALENDAR_NAME		varchar	80
MISFIRE_INSTR	Instructs the scheduler to execute the misfired job.	smallint	
JOB_DATA	Persists the job-related info.	bytea	

TABLE 196 QRTZ_SIMPLE_TRIGGERS

Field	Definition	Format	size
TRIGGER_NAME*	Name of the trigger	varchar	80
TRIGGER_GROUP*	name of the trigger group	varchar	80
REPEAT_COUNT	number of times to repeat	numeric	13,0
REPEAT_INTERVAL	interval for first and second job	numeric	13,0
TIMES_TRIGGERED	Number of times the corresponding trigger fired	numeric	13,0

TABLE 197 QRTZ_FIRED_TRIGGERS

Field	Definition	Format	size
ENTRY_ID*	Fired instance ID.	varchar	95
TRIGGER_NAME	Name of the trigger.	varchar	80
TRIGGER_GROUP	Name of the trigger group.	varchar	80
IS_VOLATILE	Whether the job should not be persisted in the JobStore for re-use after the program restarts.	boolean	
INSTANCE_NAME	Trigger instance name.	varchar	80
FIRED_TIME	The trigger fired time.	numeric	13,0
STATE	The fired trigger job state.	varchar	16
JOB_NAME	Name of the job.	varchar	80
JOB_GROUP	Name of the job group.	varchar	80

TABLE 197 QRTZ_FIRED_TRIGGERS (Continued)

Field	Definition	Format	size
IS_STATEFUL	Whether the job implements the interface StatefulJob.	boolean	
REQUESTS_RECOVERY	True or false.	boolean	

TABLE 198 QRTZ_JOB_LISTENERS

Field	Definition	Format	Size
JOB_NAME*	Name of the job.	varchar	80
JOB_GROUP*	Name of the job group.	varchar	80
JOB_LISTENER*	Job listener action class instance.	varchar	80

TABLE 199 QRTZ_CRON_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
CRON_EXPRESSION	The CRON trigger Expression (ex:"0 0 12 * * ?" - meaning:Fire at 12pm (noon) every day).	varchar	80
TIME_ZONE_ID	Given "cron" expression resolved with respect to the TimeZone.	varchar	80

TABLE 200 QRTZ_BLOB_TRIGGERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
BLOB_DATA	The Scheduler info.	bytea	

TABLE 201 QRTZ_JTRIGGER_LISTENERS

Field	Definition	Format	Size
TRIGGER_NAME*	Name of the trigger.	varchar	80
TRIGGER_GROUP*	Name of the trigger group.	varchar	80
TRIGGER_LISTENER*	The listener action.	varchar	80

TABLE 202 QRTZ_SCHEDULER_STATE

Field	Definition	Format	Size
INSTANCE_NAME*	Instance of the scheduler.	varchar	80
LAST_CHECKIN_TIME	Last fired time in milliseconds.	numeric	13,0
CHECKIN_INTERVAL	Repeat interval.	numeric	13,0
RECOVERER	Misfire instruction.	varchar	80

TABLE 203 QRTZ_LOCKS

Field	Definition	Format	Size
LOCK_NAME*	Resource identification name assigned by user.	varchar	40

TABLE 204 QRTZ_CALENDARS

Field	Definition	Format	Size
CALENDAR_NAME*	Name of the Calendar.	varchar	80
CALENDAR	Calendar object.	bytea	

TABLE 205 QRTZ_PAUSED_TRIGGER_GRPS

Field	Definition	Format	Size
TRIGGER_GROUP*	Name of the trigger group.	varchar	80

Reports

TABLE 206 REPORT_TYPE

Field	Definition	Format	Size
ID*	Meta Data for available reports.	int	
NAME	Report name.	varchar	128
DESCRIPTION	Report type description.	varchar	256

TABLE 207 GENERATED_REPORT

Field	Definition	Format	Size
ID*		int	
NAME	Report name.	varchar	256
TYPE_ID	Report type.	int	
EFCM_USER	Management applciation user who has generated this report.	varchar	128
REPORT_OBJECT	Report object BLOB.	bytea	
TIMESTAMP_	Timestamp when the report is generated.	timestamp	
FABRIC_NAME	Fabric Name.	varchar	256

Role Based Access Control

TABLE 208 USER_ROLE_MAP

Field	Definition	Format	Size
USER_NAME*	User name.	varchar	128
ROLE_ID*	Role ID, which is mapped for the user.	int	

TABLE 209 ROLE

Field	Definition	Format	Size
ID*		int	
NAME	Role name.	varchar	128
DESCRIPTION	Role description.	varchar	512
HIDDEN	Field to identify whether the role is Hidden from users or not. Values: 0= Not Hidden 1= Hidden Currently, only "All Users" Role is hidden and other roles are visible to user. Default value is 0.	smallint	

TABLE 210 ROLE_PRIVILEGE_MAP

Field	Definition	Format	Size
ROLE_ID*	User role ID.	int	
PRIVILEGE_ID*	Privilege ID.	int	
PERMISSION	Privilege permission: 1 = RO 2 = RW 0 = No privilege Default value is 0.	smallint	

TABLE 211 PRIVILEGE

Field	Definition	Format	Size
ID*		int	
NAME	Privilege Name.	varchar	128
AREA	Privilege Area. 0= Application 1= SAN 2= IP	smallint	

TABLE 212 PRIVILEGE_GROUP_MAP

Field	Definition	Format	Size
GROUP_ID*	Privilege group ID.	int	
PRIVILEGE_ID*	Privilege ID.	int	128

TABLE 213 PRIVILEGE_GROUP

Field	Definition	Format	Size
ID*		int	
NAME	Privilege group name.	varchar	128

TABLE 215 USER_

Field	Definition	Format	Size
ID *		int	
NAME	User name.	varchar	128
DESCRIPTION	User description.	varchar	512
PASSWORD	User password.	varchar	512
EMAIL	User e-mail ID.	varchar	1024
NOTIFICATION_ENABLED	Flag for e-mail notification. Default value is 0.	smallint	
FULL_NAME	User''s Full Name.	varchar	512
PHONE_NUMBER	User''s Phone number.	varchar	32
INVALID_LOGIN_COUNT	This is a counter filed to identify the number of invalid login attempts. Note: After successful login this filed will be set to NULL. Default value is 0.	smallint	
LOCKED_OUT_DATETIME	The date time stamp when a user got locked out because of exceeding max number of invalid login attempts.	timestamp	
STATUS	User''s account status: 0=Disabled 1=Enabled Default value is 1.	smallint	
SOURCE_OF_CREATION	To identify the source for creating the user account. 0= User created through Management applciation Client 1= User created when authenticated through external server. Note: At present there is no direct use of this field however this can be referred in future to build certain reports. Default value is 0.	smallint	

TABLE 216 USER_RESOURCE_MAP

Field	Definition	Format	Size
USER_NAME*	User name.	varchar	128
RESOURCE_GROUP_ID*	Resource group name, which is mapped for the user.	int	

TABLE 217 RESOURCE_GROUP

Field	Definition	Format	Size
ID*		int	
NAME	Resource group name.	varchar	128
DESCRIPTION	Resource group description.	varchar	512

TABLE 218 RESOURCE_FABRIC_MAP

Field	Definition	Format	Size
RESOURCE_GROUP_ID*	Resource group ID.	int	
FABRIC_ID*	Fabric ID, which is in the resource group.	int	

SNMP

TABLE 220 SNMP_CREDENTIALS

Field	Definition	Format	Size
ID*		int	
VIRTUAL SWITCH_ID	Virtual switch ID for which this instance of the SNMP credentials apply.	int	
RECIPIENT_ID	Recipient in the MESSAGE_RECIPIENT table.	int	
POR)_NUMBER	Port number of the SNMP agent on the switch for get and set requests.	smallint	
RETRY_COUNT	Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.	smallint	
TIMEOUT	Timeout value in seconds for a get/set request to the SNMP agent. Default value is 5.	smallint	
VERSION	SNMP agent version running on the switch, as in SNMPv1 or SNMPv3.	varchar	6
READ_COMMUNITY_ STRING	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to a device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
WRITE_COMMUNITY_ STRING	The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to a device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
USER_NAME	A human readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
CONTEXT_NAME	Text ID associated with the user, used by the SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.	varchar	128
AUTH_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. The supported values for this field are: usmNoAuthProtocol, usmHMACMD5AuthProtocol, and usmHMACSHAAuthProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
AUTH_PASSWORD	The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64

TABLE 220 SNMP_CREDENTIALS (Continued)

Field	Definition	Format	Size
PRIV_PROTOCOL	An indication of whether messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. The current values for this field are: usmNoPrivProtocol and usmDESPrivProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
PRIV_PASSWORD	The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64

TABLE 221 SNMP_PROFILE

Field	Definition	Format	Size
NAME*	A text string representing a set of SNMP agent profile. When created, one or more virtual switches could refer to this profile for its SNMP credentials unless a unique set of SNMP credentials has been defined in SNMP_CREDENTIAL.	varchar	256
PORT_NUMBER	Port number of the SNMP agent on the switch for get and set requests	smallint	
RETRY_COUNT	Number of times to retry if get/set request to the SNMP agent times out. Default value is 3.	smallint	
TIMEOUT	Timeout value in seconds before for a get/set request to the SNMP agent. Default value is 5.	smallint	
VERSION	SNMP agent version running on the switch as in SNMPv1 and SNMPv3	varchar	6
READ_COMMUNITY_STRING	The SNMP Read-Only Community String is like a password. It is sent along with each SNMP Get-Request and allows (or denies) access to device. The default value is "public". This is applicable if the agent is configured to operate in SNMPv1.	varchar	64
WRITE_COMMUNITY_STRING	The SNMP Write-Only Community String is like a password. It is sent along with each SNMP Set-Request and allows (or denies) access to a device. The default value is "private". This is applicable if the agent is configured to operate in SNMPv1	varchar	64
USER_NAME	A human-readable string representing the name of the user. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
CONTEXT_NAME	A text ID associated with the user, used by SNMP agent to provide different views. This is applicable if the agent is configured to operate in SNMPv3.	varchar	128

TABLE 221 SNMP_PROFILE (Continued)

Field	Definition	Format	Size
AUTH_PROTOCOL	An indication of whether or not messages sent or received on behalf of this user can be authenticated and if so, which authentication protocol to use. The supported values for this field are: usmNoAuthProtocol, usmHMACMD5AuthProtocol, and usmHMACSHAAuthProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
AUTH_PASSWORD	The localized secret key used by the authentication protocol for authenticating messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
PRIV_PROTOCOL	An indication of whether or not messages sent or received on behalf of this user can be encrypted and if so, which privacy protocol to use. The current values for this field are: usmNoPrivProtocol and usmDESPrivProtocol. This is applicable if the agent is configured to operate in SNMPv3.	varchar	16
PRIV_PASSWORD	The localized secret key used by the privacy protocol for encrypting and decrypting messages. This is applicable if the agent is configured to operate in SNMPv3.	varchar	64
SNMP_INFORMS_ENABLED	To denote whether SNMP informs option is enabled or disabled Default value is 0.	smallint	

TABLE 222 SNMP_V3_FORWARDING_CREDENTIAL

Field	Definition	Format	Size
ID*		int	
USER_NAME	USM user name.	varchar	64
CONTEXT_NAME	USM context name.	VARCHAR	128
AUTH_PROTOCOL	Authorization protocol.	VARCHA	16
AUTH_PASSWORD	Authorization password.	VARCHAR	64
PRIV_PROTOCOL	Privilege protocol.	VARCHAR	16
PRIV_PASSWORD	Privilege password.	VARCHAR	64

Stats

TABLE 223 FAVORITES

Field	Definition	Format	Size
ID*		int	
NAME	Name of the favorite.	varchar	64
USER_	The application user credentials.	varchar	128
TOP_N	The top number of ports(5,10,15,20).	varchar	40
SELECTION_FILTER	Types of ports (FC/FCIP/GE) and -End Monitors.	varchar	40
FROM_TIME	The time interval in which the graph is shown. Time interval can be predefined or custom. If FROM_TIME is Custom, the user can choose the number of minutes/hours/days or specify the time interval.	varchar	40
CUSTOM_LAST_VALUE	The number of minutes/hours/days. It becomes null in two cases. 1. When the value of FROM_TIME is not Custom. 2. When FROM_TIME is Custom, and user chooses the time interval (CUSTOM_FROM and CUSTOM_TO)	int	
CUSTOM_TIME_UNIT	The unit type (Minutes, Hours, Days) of the CUSTOM_LAST_VALUE.	varchar	40
CUSTOM_FROM	The starting time.	timestamp	
CUSTOM_TO	The ending time.	timestamp	
GRANULARITY	The granularity.	varchar	40
THRESHOLD	The reference line.	int	
MAIN_MEASURE	The measure of FC/FCIP/GE.	varchar	40
ADDITIONAL_MEASURE	The additional measures.	int	

TABLE 224 USER_

Field	Definition	Format	Size
ID *		int	
NAME	User name.	varchar	128
DESCRIPTION	User description.	varchar	512
PASSWORD	User password.	varchar	512
EMAIL	User e-mail ID.	varchar	1024
NOTIFICATION_ENABLED	Flag for e-mail notification. Default value is 0.	smallint	
FULL_NAME	User''s Full Name.	varchar	512
PHONE_NUMBER	User''s Phone number.	varchar	32
INVALID_LOGIN_COUNT	This is a counter filed to identify the number of invalid login attempts. Note: After successful login this filed will be set to NULL. Default value is 0.	smallint	

TABLE 224 USER_ (Continued)

Field	Definition	Format	Size
LOCKED_OUT_DATETIME	The date time stamp when a user got locked out because of exceeding max number of invalid login attempts.	timestamp	
STATUS	User''s account status: 0=Disabled 1=Enabled Default value is 1.	smallint	
SOURCE_OF_CREATION	To identify the source for creating the user account. 0= User created through Management applciation Client 1= User created when authenticated through external server. Note: At present there is no direct use of this field however this can be referred in future to build certain reports. Default value is 0.	smallint	

TABLE 225 STATS_AGING

Field	Definition	Format	Size
ID*		int	
FIVE_MIN_VALUE	Configured maximum samples value for the five minute table.	int	
THIRTY_MIN_VALUE	Configured maximum samples value for the thirty minute table.	int	
TWO_HR_VALUE	Configured maximum samples value for the two hour table.	int	
ONE_DAY_VALUE	Configured maximum samples value for the one day table.	int	
MAX_SAMPLES_VALUE	The maximum number of samples value, i.e., 3456.	int	
INTERPOLATE	Whether interpolation is enabled or disabled.	smallint	

TABLE 226 MARCHING_ANTS

Field	Definition	Format	Size
ID*		int	
THRESHOLD1_VALUE	The marching ants low boundary threshold value (T1).	int	
THRESHOLD2_VALUE	The marching ants high boundary threshold value (T2).	int	

TABLE 227 DEFAULT_FAVORITES

Field	Definition	Format	Size
ID	Name of the favorite.	int	
NAME	The topnumber of ports (5,10,15,20).	varchar	64

TABLE 227 DEFAULT_FAVORITES (Continued)

Field	Definition	Format	Size
TOP_N	Types of ports (FC/FCIP/GE) and -End Monitors.	varchar	40
SELECTION_FILTER	The time interval in which the graph is shown.	varchar	40
FROM_TIME	Always null. The default favorite is not customized.	varchar	40
CUSTOM_LAST_VALUE	Always null. The default favorite is not customized.	int	
CUSTOM_TIME_UNIT	Always null. The default favorite is not customized.	varchar	40
CUSTOM_FROM	Always null. The default favorite is not customized.	timestamp	
CUSTOM_TO	The default five minutes granularity.	timestamp	
GRANULARITY	Always null.	varchar	40
THRESHOLD	The measure Tx MBps or Rx MBps based on DEFAULT_FAVORITES.NAME	int	
MAIN_MEASURE	The Additional measures based on the FAVORITE.MAIN_MEASURE	varchar	40
ADDITIONAL_MEASURE	The Additional measures based on the FAVORITE.MAIN_MEASURE	int	

Switch

TABLE 228 VIRTUAL-SWITCH

Field	Definition	Format	Size
ID*		int	
LOGICAL_ID	Logical ID of the switch.	smallint	
NAME	Switch name.	varchar	64
WWN	WWN of the switch.	char	23
VIRTUAL_FABRIC_ID	Virtual fabric ID. If VF enabled then will have the VFID; otherwise it will be -1.	smallint	
DOMAIN_ID	Domain ID of the switch.	smallint	
BASE_SWITCH	1 = this is a base switch; otherwise, 0.	smallint	
SWITCH_MODE	2 = switch is in AG mode; otherwise, 0.	smallint	
ROLE	Role of the switch.	varchar	32
FCS_ROLE	FCS role of the switch.	varchar	16
AD_CAPABLE	1 = switch is AD-capable.	smallint	
FABRIC_IDID_MODE	Fabric IDID mode.	smallint	
OPERATIONAL_STATUS	Operation status of switch.	varchar	128
MAX_ZONE_CONFIG_SIZE	Maximum size of zone configuration on the switch.	int	
CREATION_TIME	Time at which this record was created.	timestamp	
LAST_UPDATE_TIME	Time when this record was last updated.	timestamp	
USER_NAME	User name of the switch.	varchar	128
PASSWORD	Password.	varchar	128
MANAGEMENT_STATE	Various states as per manageability software like the Management application.	int	
STATE	State of the switch.	varchar	32
STATUS	Status of the switch.	varchar	32
STATUS_REASON	Reason for the status.	varchar	2048
USER_DEFINED_VALUE1		varchar	256
USER_DEFINED_VALUE2		varchar	256
USER_DEFINED_VALUE3		varchar	256
CORE_SWITCH_ID	Core switch DB ID.	int	
INTEROP_MODE	Mode in which this switch is operating.	smallint	
CRYPTO_CAPABLE	0 = the switch is not crypto-enabled; if capable it will have a non-zero value.	smallint	
FCR-CAPABLE	0 = the switch is not FCR-enabled; if capable it will have a non-zero value.	smallint	
FCIP_CAPABLE	0 = the switch is not FCIP-enabled; if capable it will have a non-zero value.	smallint	

TABLE 229 CORE_SWITCH

Field	Definition	Format	Size
ID*		int	
IP_ADDRESS	IP address of the switch.	varchar	128
WWN	Chassis WWN.	char	23
NAME	Switch name.	varchar	64
TYPE	SWBD type number as given by Fabric OS. Default value is 0.	smallint	
MODEL	Model type of the switch: 0 = Unknown 1 = Not applicable 2 = Fabric OS switch 3 = M-EOS switch	smallint	
FIRMWARE_VERSION	Embedded (Fabric OS or M-EOS) software version.	varchar	128
VENDOR	Switch vendor.	varchar	256
MAX_VIRTUAL_SWITCHES	Maximum virtual switches allowed on this physical switch. Default vaue is 1.	smallint	
NUM_VIRTUAL_SWITCHES	Actual number of virtual switches carved out of this physical switch. 0 means it is not operating in Virtual Fabric model. Default value is 0.	smallint	
REACHABLE	Whether reachable by HTTP.	smallint	
UNREACHABLE_TIME	When the switch became unreachable from HTTP.	timestamp	
OPERATIONAL_STATUS	Operational status as reported by the embedded software..	varchar	128
CREATION_TIME	Time when this record was created by the Management application. Default is ’now()’.	timestamp	
LAST_SCAN_TIME	Time when this record was last updated.	timestamp	
LAST_UPDATE_TIME	1 = the Management application server is registered with the switch to receive Syslog. Default is ’now()’.	timestamp	
SYSLOG_REGISTERED	1 = Syslog is enabled for this switch. Default value is 0.	smallint	
CALL_HOME_ENABLED	1 = call home is enabled for this switch. Default value is 1.	smallint	
SNMP_REGISTERED	1 = the Management application server is registered with the switch to receive SNMP traps. Default value is 0.	smallint	
USER_IP_ADDRESS	User-assigned IP address. This is used for M-EOS switches where Fabric OS seed switch fails to get the IP address of the M-EOS switch.	varchar	128

TABLE 229 CORE_SWITCH (Continued)

Field	Definition	Format	Size
NIC_PROFILE_ID	NIC profile of the Management application server host used by this switch to communicate in interactive configuration and other operations. It determines which Management application host IP used by this switch.	int	
MANAGING_SERVER_IP_ ADDRESS	IP address(v4/v6) of the Management applciation server which is currently managing the M-model switch. Used for M-EOS switch only. It does not apply to Fabric OS switches.	varchar	128
VF_ENABLED	Default value is 0.	smallint	
VF_SUPPORTED	Default value is 0	smallint	
MANAGED_ELEMENT_ID	A unique managed element ID for this physical switch. Also a foreign key reference to the MANAGED_ELEMENT table.	int	
NAT_PRIVATE_IP_ADDRESS	NAT private IP Address. Feature available from NMS DC Eureka release onwards. During a successful NAT translation the Private IP that gets translated will be stored in this field. The new translated IP Address will be stored in the existing IP_ADDRESS field. All the NAT look up will be done using the NAT Private IP Address.	varchar	128
ALTERNATE_IP_ADDRESS	Alternate IP address of the switch. Feature available from Eureka release onwards. During fabric discovery the column will be populated based on the values in the fabricinfo.html. If Management applciation server is IPV6 capable, then we store the switchetherIP NVP else we store the switchetherIPV6. So could be either IPV4 or IPV6 address. If there exists any NAT translation, translated IP will be used.	varchar	128

TABLE 230 NIC_PROFILE

Field	Definition	Format	Size
ID*		int	
NAME	The name of the network interface in the format network interface name / host address.	varchar	255
IP_ADDRESS	The host address of the interface.	varchar	128

TABLE 232 SWITCH_MODEL

Field	Definition	Format	Size
ID*		int	
SWBD_TYPE	Switch type number, universally used by all the Management application module implementation.	smallint	
SUBTYPE	Switch subtype. At present no subtypes for existing model records are defined. Default value is 0.	smallint	

TABLE 232 SWITCH_MODEL (Continued)

Field	Definition	Format	Size
DESCRIPTION	Model description, such as FC link speed, port count and whether multi-card (director) class switch or other type of switch. Default is ‘Not Available’.	varchar	256
MODEL	Switch model string.	varchar	32
REMARK	Remarks, such as an internal project name.	varchar	64

TABLE 233 PURGED_SWITCH

Field	Definition	Format	Size
WWN*	WWN of the switch.	char	23
NAME	Name of the switch.	varchar	64
VIRTUAL_FABRIC_ID	Virtual fabric ID. Default value is 0.	smallint	
USER_NAME	Switch user name.	varchar	64
PASSWORD	Switch password.	varchar	128
IP_ADDRESS	IP address.	varchar	128
PORT_NUMBER	SNMP port number.	smallint	
RETRY_COUNT	Retry count.	smallint	
TIMEOUT	SNMP time out value.	smallint	
VERSION	SNMP version.	varchar	6
READ_COMMUNITY_STRING	Read community string.	varchar	64
WRITE_COMMUNITY_STRING	Write community string.	varchar	64
SNMP_USER_NAME	SNMP user name.	varchar	128
CONTEXT_NAME	SNMP context name.	varchar	128
AUTH_PROTOCOL	SNMP auth protocol.	varchar	16
AUTH_PASSWORD	snmp auth password	varchar	64
PRIV_PROTOCOL	snmp priv protocol	varchar	16
PRIV_PASSWORD	snmp priv password	varchar	64
TYPE	Default value is 0.	smallint	

Switch details

TABLE 234 CORE_SWITCH_DETAILS

Field	Definition	Format	Size
CORE_SWITCH_ID*	DB ID.	int	
ETHERNET_MASK	Subnet mask.	char	64

TABLE 234 CORE_SWITCH_DETAILS (Continued)

Field	Definition	Format	Size
FC_MASK	Subnet mask for FC IP.	char	64
FC_IP	Fibre Channel IP address.	char	64
FC_CERTIFICATE		smallint	
SW_LICENSE_ID		char	23
SUPPLIER_SERIAL_ NUMBER	Serial number of the chassis.	varchar	32
PART_NUMBER	The part number assigned by the organization responsible for producing or manufacturing the PhysicalElement.	varchar	32
CHECK_BEACON	1 = beacon is turned on; otherwise, 0.	smallint	
TIMEZONE	Time zone configured on the switch.	varchar	32
MAX_PORT	Number of maximum ports physically allowed on the switch.	smallint	
CHASSIS_SERVICE_TAG		varchar	32
BAY_ID		varchar	32
TYPE_NUMBER		varchar	32
MODEL_NUMBER	Switch model number / string.	varchar	32
MANUFACTURER	The name of the organization responsible for producing the chassis. This might be different from the vendor if the product is shipped by an OEM with a private label.	varchar	32
PLANT_OF_MANUFACTURER	Plant where the switch is manufactured.	varchar	32
SEQUENCE_NUMBER	Serial number of the switch.	varchar	32
TAG	An arbitrary string that uniquely identifies the chassis and serves as its physical key. The Tag property contains the WWN of the license switch (LicenseWWN).	varchar	32
ACT_CP_PRI_FW_VERSION	Active CP primary firmware version.	varchar	128
ACT_CP_SEC_FW_VERSION	Active CP secondary firmware version.	varchar	128
STBY_CP_PRI_FW_VERSION	Standby CP primary firmware version.	varchar	128
STBY_CP_SEC_FW_VERSION	Standby CP secondary firmware version.	varchar	128
TYPE	SWBD number as assigned by embedded SW depending upon the switch type / platform. Default value is 0.	smallint	
EGM_CAPABLE	1 = the switch is EGM-capable. Default value is 0.	smallint	
SUB_TYPE	SWBD sub type number.	varchar	32
PARTITION	Default value is 0.	smallint	

TABLE 234 CORE_SWITCH_DETAILS (Continued)

Field	Definition	Format	Size
MAX_NUM_OF_BLADES	Required by SMIA to populate Brocade_Chassis.MaxNumOfBlades property. It indicates the max no of blades that can be present in a chassis.	smallint	
VENDOR_VERSION	Required by integrated SMI agent to populate Brocade_Product.Version property.	varchar	32
VENDOR_PART_NUMBER	Required by integrated SMI agent to populate Brocade_Product.SKUNumber property.	varchar	32
SNMP_INFORMS_ENABLED	Flag to denote whether SNMP informs option in the switch is enabled or disabled. Default value is 0.	smallint	
RNID_SEQUENCE_NUMBER		varchar	32
CONTACT		varchar	256
LOCATION		varchar	256
DESCRIPTION		varchar	256
FIRMWARE_VERSION		varchar	128

TABLE 235 CORE_SWITCH

Field	Definition	Format	Size
ID*		int	
IP_ADDRESS	IP address of the switch.	varchar	128
WWN	Chassis WWN.	char	23
NAME	Switch name.	varchar	64
TYPE	SWBD type number as given by Fabric OS. Default value is 0.	smallint	
MODEL	Model type of the switch: 0 = Unknown 1 = Not applicable 2 = Fabric OS switch 3 = M-EOS switch	smallint	
FIRMWARE_VERSION	Embedded (Fabric OS or M-EOS) software version.	varchar	128
VENDOR	Switch vendor.	varchar	256
MAX_VIRTUAL_SWITCHES	Maximum virtual switches allowed on this physical switch. Default vaue is 1.	smallint	
NUM_VIRTUAL_SWITCHES	Actual number of virtual switches carved out of this physical switch. 0 means it is not operating in Virtual Fabric model. Default value is 0.	smallint	
REACHABLE	Whether reachable by HTTP.	smallint	
UNREACHABLE_TIME	When the switch became unreachable from HTTP.	timestamp	
OPERATIONAL_STATUS	Operational status as reported by the embedded software..	varchar	128

TABLE 235 CORE_SWITCH (Continued)

Field	Definition	Format	Size
CREATION_TIME	Time when this record was created by the Management application. Default is ’now()’.	timestamp	
LAST_SCAN_TIME	Time when this record was last updated.	timestamp	
LAST_UPDATE_TIME	1 = the Management application server is registered with the switch to receive Syslog. Default is ’now()’.	timestamp	
SYSLOG_REGISTERED	1 = Syslog is enabled for this switch. Default value is 0.	smallint	
CALL_HOME_ENABLED	1 = call home is enabled for this switch. Default value is 1.	smallint	
SNMP_REGISTERED	1 = the Management application server is registered with the switch to receive SNMP traps. Default value is 0.	smallint	
USER_IP_ADDRESS	User-assigned IP address. This is used for M-EOS switches where Fabric OS seed switch fails to get the IP address of the M-EOS switch.	varchar	128
NIC_PROFILE_ID	NIC profile of the Management application server host used by this switch to communicate in interactive configuration and other operations. It determines which Management application host IP used by this switch.	int	
MANAGING_SERVER_IP_ ADDRESS	IP address(v4/v6) of the Management applciation server which is currently managing the M-model switch. Used for M-EOS switch only. It does not apply to Fabric OS switches.	varchar	128
VF_ENABLED	Default value is 0.	smallint	
VF_SUPPORTED	Default value is 0	smallint	
MANAGED_ELEMENT_ID	A unique managed element ID for this physical switch. Also a foreign key reference to the MANAGED_ELEMENT table.	int	
NAT_PRIVATE_IP_ADDRESS	NAT private IP Address. Feature available from NMS DC Eureka release onwards. During a successful NAT translation the Private IP that gets translated will be stored in this field. The new translated IP Address will be stored in the existing IP_ADDRESS field. All the NAT look up will be done using the NAT Private IP Address.	varchar	128
ALTERNATE_IP_ADDRESS	Alternate IP address of the switch. Feature available from Eureka release onwards. During fabric discovery the column will be populated based on the values in the fabricinfo.html. If Management applciation server is IPV6 capable, then we store the switchetherIP NVP else we store the switchetherIPV6. So could be either IPV4 or IPV6 address. If there exists any NAT translation, translated IP will be used.	varchar	128

Switch port

TABLE 237 GIGE_PORT

Field	Definition	Format	Size
ID*		int	
SWITCH_PORT_ID	ID for the GigE Port in SWITCH_PORT.	int	
PORT_NUMBER	GigE Port Number(0 for ge0 and 1 for ge1).	int	
SLOT_NUMBER	Slot number on which the GigE Port is present.	int	
ENABLED	Enabled or disabled. Default value is 0.	smallint	
SPEED	Port speed details. Default value is 0.	bigint	
MAX_SPEED	Port maximum speed supported.	bigint	
MAC_ADDRESS	MAC Address of that port.	varchar	64
PORT_NAME	GigE Port Name.	varchar	64
OPERATIONAL_STATUS	LED status.	int	
LED_STATE	LED status.	smallint	
SPEED_LED_STATE	GigE Port type details.	smallint	
PORT_TYPE	Port type for the GigE Port.	varchar	64
PERSISTENTLY_DISABLED	Whether the GigE Port is persistently disabled.	smallint	
INTERFACE_TYPE		smallint	
CHECKSUM		varchar	16
FCIP_CAPABLE	1 = FCIP capable; otherwise, 0. Default value is 2.	smallint	
ISCSI_CAPABLE	1 = ISCSI capable; otherwise, 0. Default value is 2.	smallint	
REMOTE_MAC_ADDRESS	MAC address of attached port of the 10G GigE Port.	varchar	64
INBAND_MANAGEMENT_STATUS	1 = Inband Management status is enabled; otherwise, 0. Default value is 0.	smallint	
OCCUPIED	Default value is 0.	smallint	
LAST_UPDATE		bigint	

TABLE 238 SWITCH_PORT

Field	Definition	Format	Size
ID*		int	
VIRTUAL_SWITCH_ID	DB ID of virtual_switch to which this port belongs.	int	
WWN	WWN of the port.	char	23
NAME	User friendly name of the port.	char	32
SLOT_NUMBER	Slot number. Default value is 0.	int	

TABLE 238 SWITCH_PORT (Continued)

Field	Definition	Format	Size
PORT_NUMBER	The logical port number of the user port. There is no assumption of any relation to the physical location of a port within a chassis.	smallint	
USER_PORT_NUMBER	User port number. Unique port number in a chassis.	smallint	
PORT_ID	Port ID of this port.	varchar	8
PORT_INDEX	Number used for identifying port in zoning.	smallint	
AREA_ID	Area number the port is assigned to.	smallint	
MAC_ADDRESS	MAC address of this port.	varchar	64
PORT_MOD		varchar	64
TYPE	Port type. The specific mode currently enabled for the port.	varchar	16
FULL_TYPE	Port type.	varchar	128
STATUS	The current status of the switch port.	varchar	64
HEALTH		varchar	16
STATUS_MESSAGE	Status message if any.	varchar	255
PHYSICAL_PORT	1 = it is a physical port 0 = it is a virtual port Default value is 1.	smallint	
LOCKED_PORT_TYPE	Locked port type.	varchar	16
CATEGORY		smallint	
PROTOCOL		varchar	16
SPEED	Actual speed at which the port is currently operating.	varchar	64
SPEEDS_SUPPORTED	Supported speed values.	varchar	32
MAX_PORT_SPEED	The maximum speed the port is capable of supporting, in bits per second.	int	
DESIRED_CREDITS	How many BB credits are desired for the port.	int	
BUFFER_ALLOCATED	How many BB credits are allocated for the port.	int	
ESTIMATED_DISTANCE	The estimated physical distance of the connection between ports.	int	
ACTUAL_DISTANCE	The physical distance of the connection on the port in relation to the other port.	int	
LONG_DISTANCE_SETTING	Whether long distance enabled.	int	
DEGRADED_PORT	Whether a port is degraded or not.	varchar	16
REMOTE_NODE_WWN	Node WWN of the attached port.	varchar	255
REMOTE_PORT_WWN	WWN of the attached port.	varchar	255
LICENSED	1 = the port is licensed; otherwise, 0.	smallint	
SWAPPED	1 = port is swapped; otherwise, 0.	smallint	
TRUNKED	1 = port is trunked; otherwise, 0.	smallint	
TRUNK_MASTER	1 = the port is trunk master; otherwise, 0.	smallint	

TABLE 238 SWITCH_PORT (Continued)

Field	Definition	Format	Size
PERSISTENT_DISABLE	1 = port is persistently disabled.	smallint	
FICON_SUPPORTED	1 = FICON is supported; otherwise, 0.	smallint	
BLOCKED	1 = port is blocked; otherwise, 0.	smallint	
PROHIBIT_PORT_NUMBERS		varchar	1024
PROHIBIT_PORT_COUNT		smallint	
NPIV	Whether NPIV mode is enabled.	smallint	
NPIV_CAPABLE	Instance NPIV mode capability: 1 = indicates port has NPIV capability 2 = NPIV license is enabled	smallint	
NPIV_ENABLED	Whether NPIV mode is enabled.	smallint	
FC_FAST_WRITE_ENABLED	1 = FC fast write is enabled.	smallint	
ISL_RRDY_ENABLED		smallint	
RATE_LIMIT_CAPABLE		smallint	
RATE_LIMITED		smallint	
QOS_CAPABLE		smallint	
QOS_ENABLED		smallint	
TUNNEL_CONFIGURED		smallint	
FCIP_TUNNEL_UP		smallint	
FCR_FABRIC_ID		smallint	
FCR_INTEROP_MODE		smallint	
CALCULATED_STATUS		varchar	64
USER_DEFINED_VALUE1		varchar	256
USER_DEFINED_VALUE2		varchar	256
USER_DEFINED_VALUE3		varchar	256
KIND		varchar	32
STATE		varchar	64
PREVIOUS_STATUS	This table can hold the same values as STATUS column. But this will be holding the previous status of the PORT. These values to be populated by switch asset collector.	varchar	64
AUTO_DISABLE_CONFIGURED	To represent auto disable configuration state (set by user). Default value is 0.	smallint	
AUTO_DISABLED	To represent auto disabled status (set by switch). Default value is 0.	smallint	
OCCUPIED	Default value is 0.	smallint	
LAST_UPDATE		bigint	
PORT_BIT_MASK	F-Port trunk bit mask value. Default value is 0.	int	

TABLE 238 SWITCH_PORT (Continued)

Field	Definition	Format	Size
LOGICAL_PORT_NUMBER	F-Port trunk logical port number. Default value is -1.	smallint	
DEFAULT_AREA_ID	Default Area id of F-Port trunk port. Default value is -1.	smallint	
LOGICAL_PORT_WWN	Logical port WWN of F-Port trunk group.	char	23
PREVIOUS_TYPE	This fields copies the old state of the port type. The field could be used to track the state change information for the switch port type. SwitchAssetCollector sets this field during the collection time. SMIA requested this information but could be used by any module which needs to track the type state change.	varchar	16
LATENCY_DETECT_SUPPORTED	Whether the port supports latency detection. 1 means true and 0 means false	smallint	
PREVIOUS_STATE	Fields copies the old state of the port . The field could be used to track the state change information for the switch port . SwitchAssetCollector sets this field during the collection time. SMIA requested this information but could be used by any module which needs to track the state change.	varchar	64
EPORT_DISABLED	Represents the eportDisabled field from switch.html. Values populated by SwitchAssetcollector during the collection time. Possible values includes 0 and 1. Default value is -1.	smallint	
SPEED_NEGOTIATED	This column indicates if the port speed is negotiated or not. If port speed is negotiated then value is 1 else it will be 0. Default value is -1.	smallint	

TABLE 240 N2F_PORT_MAP

Field	Definition	Format	Size
ID*		int	
VIRTUAL_SWITCH_ID	Virtual switch ID of AG for N to F_port mapping, foreign key to VIRTUAL_SWITCH table.	int	
N_PORT	Port number of port type N_Port which is being mapped, One N_Port can be mapped to multiple F_ports.	smallint	
F_PORT	Port number of port type F_Port which is being mapped.	smallint	

TABLE 242 FPORT_TRUNK_GROUP

Field	Definition	Format	Size
ID*		int	
VIRTUAL_SWITCH_ID	Virtual switch ID where this F_Port Trunk Group is defined.	int	

TABLE 242 FPORT_TRUNK_GROUP (Continued)

Field	Definition	Format	Size
MASTER_USER_PORT	User port number for the master port of this trunk.	smallint	
WWN	WWN of the trunk group.	char	23
TRUNK_AREA	User-assigned area number used to group together F_ports of the trunk.	smallint	

TABLE 243 FPORT_TRUNK_MEMBER

Field	Definition	Format	Size
GROUP_ID*	Foreign key to the PORT_TRUNK_GROUP table.	int	
PORT_NUMBER*	Member user port number.	smallint	
WWN	Member port WWN.	char	23

TABLE 244 VIRTUAL_SWITCH

Field	Definition	Format	Size
ID*		int	
LOGICAL_ID	Logical ID of the switch.	smallint	
NAME	Switch name.	varchar	64
WWN	WWN of the switch.	char	23
VIRTUAL_FABRIC_ID	Virtual fabric ID. If VF enabled then will have the VFID; otherwise, it will be -1	smallint	
DOMAIN_ID	Domain ID of the switch.	smallint	
BASE_SWITCH	1 = this is a base switch; otherwise, 0.	smallint	
SWITCH_MODE	2 = switch is in AG mode; otherwise, 0.	smallint	
ROLE	Role of the switch.	varchar	32
FCS_ROLE	FCS role of the switch.	varchar	16
AD_CAPABLE	1 = switch is AD-capable.	smallint	
FABRIC_IDID_MODE	Fabric IDID mode.	smallint	
OPERATIONAL_STATUS	Operation status of switch.	varchar	128
MAX_ZONE_CONFIG_SIZE	Maximum size of zone configuration on the switch.	int	
CREATION_TIME	Time at which this record was created.	timestamp	
LAST_UPDATE_TIME	Time when this record was last updated.	timestamp	
USER_NAME	User name of the switch.	varchar	128
PASSWORD	Password.	varchar	128
MANAGEMENT_STATE	Various states as per manageability software like the Management application.	int	
STATE	State of the switch.	varchar	32
STATUS	Status of the switch.	varchar	32
STATUS_REASON	Reason for the status.	varchar	2048
USER_DEFINED_VALUE_1		varchar	256

TABLE 244 VIRTUAL_SWITCH (Continued)

Field	Definition	Format	Size
USER_DEFINED_VALUE_2		varchar	256
USER_DEFINED_VALUE_3		varchar	256
CORE_SWITCH_ID	Core switch DB ID.	int	
INTEROP_MODE	Mode in which this switch is operating.	smallint	
CRYPTO_CAPABLE	0 = the switch is not crypto-enabled; if capable it will have non-zero value	smallint	
FCR_CAPABLE	0 = the switch is not FCR-enabled; if capable it will have non-zero value	smallint	
FCIP_CAPABLE	0 if the switch is not FCIP-enabled; if capable it will have non-zero value	smallint	

Switch SNMP info

Threshold

TABLE 246 SWITCH_THRESHOLD_SETTING

Field	Definition	Format	Size
SWITCH_ID*	References the ID in CORE_SWITCH table.	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table.	int	
STATUS	The status of applied to the switch.	smallint	
OVERRIDDEN	Policy is overridden or not overridden.	smallint	
DESCRIPTION	Description about the status of policy applied to the switch.	varchar	100

TABLE 247 THRESHOLD_POLICY

Field	Definition	Format	Size
ID*		int	
NAME	Name of the policy.	varchar	100
TYPE	Type of the policy.	varchar	20
DESCRIPTION	Description about the policy.	varchar	100

TABLE 248 FABRIC_THRESHOLD_SETTING

Field	Definition	Format	Size
FABRIC_ID*	References the ID in FABRIC table	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table	int	

TABLE 249 VIRTUAL_SWITCH

Field	Definition	Format	Size
ID*		int	
LOGICAL_ID		smallint	
NAME		varchar	64
WWN		char	23
VIRTUAL_FABRIC_ID	Default value is 0.	smallint	
DOMAIN_ID		smallint	
BASE_SWITCH	Default value is 0.	smallint	
SWITCH_MODE	Default value is 0.	smallint	
ROLE		varchar	32
FCS_ROLE		varchar	16
AD_CAPABLE	Default value is 0.	smallint	
FABRIC_IDID_MODE		smallint	
OPERATIONAL_STATUS		varchar	128
MAX_ZONE_CONFIG_SIZE	Defaultis 0.	int	
CREATION_TIME	Defaultis 'now()'.	timestamp	
LAST_UPDATE_TIME	Defaultis 'now()'.	timestamp	
USER_NAME		varchar	128
PASSWORD		varchar	128
MANAGEMENT_STATE		bigint	
STATE		varchar	32
STATUS		varchar	32
STATUS_REASON		varchar	2048
USER_DEFINED_VALUE_1		varchar	256
USER_DEFINED_VALUE_2		varchar	256
USER_DEFINED_VALUE_3		varchar	256
CORE_SWITCH_ID		int	
INTEROP_MODE	Default value is 0.	smallint	
CRYPTO_CAPABLE	Default value is 0.	smallint	
FCR_CAPABLE	Default value is 0.	smallint	
FCIP_CAPABLE	Default value is 0.	smallint	
FCOE_CAPABLE	If the switch supports FCoE. Default value is 0.	smallint	
L2_CAPABLE	If the switch supports L2.	smallint	
L3_CAPABLE	If the switch supports L3.	smallint	
LF_ENABLED	Logical Fabric Enabled/Disabled for a Virtual Switch. Default value is 0.	smallint	

TABLE 249 VIRTUAL_SWITCH (Continued)

Field	Definition	Format	Size
DEFAULT_LOGICAL_SWITCH	Check to see whether virtual switch is a default logical switch or not. 1 is true and 0 is false. Default value is 0.	smallint	
FEATURES_SUPPORTED	Contains the features supported as a bit mask. Default value is 0.	int	
FMS_MODE	Default value is 0.	smallint	
DYNAMIC_LOAD_SHARING	Default value is 0.	smallint	
PORT_BASED_ROUTING	Default value is 0.	smallint	
IN_ORDER_DELIVERY	Default value is 0.	smallint	
INSISTENT_DID_MODE	Default value is 0.	smallint	
LAST_SCAN_TIME		timestamp	
DOMAIN_MODE_239	Default value is 0.	smallint	
DOMAIN_ID_OFFSET	Default value is 96.	smallint	
PREVIOUS_OPERATIONAL_STATUS	This table can hold the same values as OEPRATION_STATUS column. But this will be holding the previous OPERATIONAL_STATUS of the Virtual switch. These values to be populated by FCS during Fabric Refresh task	varchar	128
FCOE_LOGIN_ENABLED	The FCoE Login Management Status of the switch. Default value is 0.	smallint	
FCIP_CIRCUIT_CAPABLE	Whether the switch can create FCIP Circuits. 1 means true and 0 means false. Default value is 0.	smallint	
DISCOVERED_PORT_COUNT	Reflects the number of managed ports in the discovered switch. Default value is 0.	smallint	
LAST_PORT_MEMBERSHIP_CHANGE		bigint	
MAX_FCIP_TUNNELS	The maximun number of tunnels that can be created in this switch,-1 means not supported. Default value is -1.	int	
MAX_FCIP_CIRCUITS	The maximun number of circuits that can be created in this switch, -1 means not supported. Default value is -1.	int	
FCIP_LICENSED	FCIP Advanced Extension Licensing is available. 1 means licensed and 0 means not licensed, -1 means not supported. Default value is -1.	smallint	
ADDRESSING_MODE	This column to represent the logical switch addressing modes to assign Port Addresses, There are three different addressing modes supported. Fixed (0), Flat or 10 bit (1), Dynamic (2). Default value is -1.	smallint	

TABLE 249 VIRTUAL_SWITCH (Continued)

Field	Definition	Format	Size
PREVIOUS_STATE	This fields copies the old state of the switch . The field could be used to track the state change information for the switch.These values to be populated by FCS during Fabric Refresh task.SMIA requested this information but could be used by any module which needs to track the state change	varchar	32
MANAGED_ELEMENT_ID	A unique managed element ID for this virtual switch. Also a foreign key reference to the MANAGED_ELEMENT table.	int	
HIF_ENABLED	The HIF Enabled bit on the switch. Values are 1 for enabled and 0 for not enabled. -1 the default, stands for not supported and will be used for older firmwares. Default value is -1.	smallint	

TABLE 250 PM_MEASURE

Field	Definition	Format	Size
ID*		int	
DESCRIPTION	The description of the measure.	varchar	64
NAME	Name of the measure.	varchar	32

TABLE 251 THRESHOLD_MEASURE

Field	Definition	Format	Size
MEASURE_ID*	References the ID In PM_MEASURE table, where all measures are defined.	int	
HIGH_BOUNDARY	Configured high boundary threshold value for measure ID.	int	
LOW_BOUNDARY	Configured low boundary threshold value for measure ID.	int	
BUFFER_SIZE	Configured buffer size for measure ID.	int	
POLICY_ID*	References the ID in THRESHOLD_POLICY table.	int	

User Interface

TABLE 252 AVAILABLE_FLYOVER_PROPERTY

Field	Definition	Format	Size
ID*		int	
NAME	Name of the available property to be included in the flyover display.	varchar	40

TABLE 252 AVAILABLE_FLYOVER_PROPERTY (Continued)

Field	Definition	Format	Size
TYPE	The flyover property type: 0 = Product property 1 = Connection property	smallint	
DEFAULT_SELECTION	AVAILABLE_FLYOVER_PROPERTY DEFAULT_SELECTION 1 = default selected product/connection property 0 = not included in the default list.	smallint	

TABLE 253 SELECTED_FLYOVER_PROPERTY

Field	Definition	Format	Size
PROPERTY_ID*	Refers to Flyover_Property ID from AVAILABLE_FLYOVER_PROPERTY table.	int	
USER_NAME*	The name of the user who selected the property to be shown on flyover.	varchar	128
POSITION_	The user preferred position of the selected flyover property.	int	

TABLE 254 TOOL_APP

Field	Definition	Format	Size
TOOL_MENU_TEXT*	Text to be displayed for the Tool Menu.	varchar	256
TOOL_ID	A Tool in the TOOL_PATH table where the tools are defined.	int	
PARAMETERS	Default path for launching the tool.	varchar	256
KEY_STROKE	Short cut key stroke to the application.	varchar	30

TABLE 255 TOOL_PATH

Field	Definition	Format	Size
ID*		int	
TOOL_NAME	Name of the tool.	varchar	256
PATH	Path of the tool where installed or available.	varchar	1057
WORKING_FOLDER	Working folder for that application.	varchar	512

TABLE 256 PRODUCT_APP

Field	Definition	Format	Size
ID*		int	
MENU_TEXT	Name of the product menu.	varchar	256
PROP1_KEY	First condition name to be satisfied by a selected product to launch a particular tool.	varchar	256
PROP1_VALUE	First condition value to be satisfied by a selected product to launch a particular tool.	varchar	256

TABLE 256 PRODUCT_APP (Continued)

Field	Definition	Format	Size
PROP2_KEY	Second condition name to be satisfied by a selected product to launch a particular tool.	varchar	256
PROP2_VALUE	Second condition value to be satisfied by a selected product to launch a particular tool.	varchar	256
TOOL_ID	The tool to be used for launching the application.	int	
PARAMETERS	Link to that application.	varchar	256
IP_SELECTED	Selected IP Address option.	smallint	
WWN_SELECTED	Selected WWN option.	smallint	

TABLE 257 ZONE_DB

Field	Definition	Format	Size
ID*	PK of the owning fabric.	int	
FABRIC_ID	Zone DB name for offline Zone DBs.	int	
NAME	Offline Zone DB (1 = offline).	varchar	256
OFFLINE	Created timestamp.	smallint	
CREATED	Last modified timestamp.	timestamp	
LAST_MODIFIED	Last modified timestamp.	timestamp	
LAST_APPLIED	Last saved to switch timestamp.	timestamp	
CREATED_BY	Created by user name.	varchar	128
LAST_MODIFIED_BY	Last modified by user name.	varchar	128
LAST_APPLIED_BY	Last saved to switch user name.	varchar	128
DEFAULT_ZONE_STATUS	All access or no access when no active zone configuration.	smallint	
ZONE_TXN_SUPPORTED	Zoning commands support transaction.	smallint	
MCDATA_DEFAULT_ZONE	McData switch default zoning mode.	smallint	
MCDATA_SAFE_ZONE	McData switch safe zoning mode.	smallint	
ZONE_CONFIG_SIZE	Zone configuration string length.	int	

TABLE 258 ZONE_DB_USERS

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of the owning zone DB.	int	
USER_NAME	List of users currently editing this zone DB.	varchar	128

TABLE 259 LSAN_ZONE

Field	Definition	Format	Size
ID*		int	
BB_FABRIC_ID	Backbone fabric DB ID.	int	

TABLE 259 LSAN_ZONE (Continued)

Field	Definition	Format	Size
EDGE_FABRIC_ID	FID assigned to edge fabric.	int	
NAME	LSAN zone name.	varchar	128
BACKBONE	0= is not a backbone lsan zone, 1= is a backbone lsan zone. Default value is 0.	smallint	

TABLE 260 LSAN_ZONE_MEMBER

Field	Definition	Format	Size
LSAN_ZONE_ID*	LSAN_ZONE record reference.	int	
MEMBER_PORT_WWN*	Zone member WWN.	char	23

TABLE 261 ZONE_DB_CONTENT

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of the owning offline zone DB.	int	
CONTENT	Saved online content before offline was saved to switch.	text	
TI_CONTENT	TI_CONTENT saved online TI zone content before offline was saved to switch.	text	
DEFINED		text	
ACTIVE		text	

Zoning 2

TABLE 262 ZONE_ALIAS_IN_ZONE

Field	Definition	Format	Size
ZONE_ALIAS_ID*	PK of the zone alias.	int	
ZONE_ID*	PK of the zone.	int	23

TABLE 263 ZONE_ALIAS

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of the owning ZONE_DB.	int	
NAME	The zone alias name.	varchar	64

TABLE 264 ZONE_ALIAS_MEMBER

Field	Definition	Format	Size
ID*		int	
TYPE	Zone alias member type: 2 = WWN 4 = D,P	smallint	
VALUE	Member value (D,P or WWN).	varchar	256
ZONE_ALIAS_ID	PK of the owning zone alias.	int	

TABLE 265 ZONE_IN-ZONE_SET

Field	Definition	Format	Size
ZONE_SET_ID*	PK of the owning zone set.	INT	
ZONE_ID*	PK of the owning zone.	INT	

TABLE 266 ZONE

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK the owning ZONE_DB.	int	
NAME	The zone name.	varchar	64
TYPE	The zone type.	int	
SUB_TYPE	The zone subtype.	int	
ACTIVATE	For TI zones only, zone is activated. Default value is 0.	smallint	
CONFIGURED_FAILOVER	Configured Failover state of the TI Zone.	smallint	
CONFIGURED_ACTIVATE	Configured active state of the TI Zone.	smallint	
ENABLED_FAILOVER	Enabled Failover state of the TI Zone.	smallint	
ENABLED_ACTIVATE	Enabled Active state of the TI Zone.	smallint	

TABLE 267 ZONE_DB

Field	Definition	Format	Size
ID*		int	
FABRIC_ID	PK of the owning fabric.	int	
NAME	Zone DB name for offline Zone DBs.	varchar	256
OFFLINE	Offline Zone DB (1 = offline).	smallint	
CREATED	Created timestamp.	timestamp	
LAST_MODIFIED	Last modified timestamp.	timestamp	
LAST_APPLIED	Last saved to switch timestamp.	timestamp	
CREATED_BY	Created by user name.	varchar	128
LAST_MODIFIED_BY	Last modified by user name.	varchar	128
LAST_APPLIED_BY	Last saved to switch user name.	varchar	128

TABLE 267 ZONE_DB (Continued)

Field	Definition	Format	Size
DEFAULT_ZONE_STATUS	All access or no access when no active zone configuration.	smallint	
ZONE_TXN_SUPPORTED	Zoning commands support transaction.	smallint	
MCDATA_DEFAULT_ZONE	McData switch default zoning mode.	smallint	
MCDATA_SAFE_ZONE	McData switch safe zoning mode.	smallint	
ZONE_CONFIG_SIZE	Zone configuration string length.	int	
ZONE_AVAILABLE_SIZE	Available zone DB size in the switch. Default value is -1.	int	

TABLE 268 ZONE_SET

Field	Definition	Format	Size
ID*		int	
ZONE_DB_ID	PK of owning zone DB.	int	
NAME	Zone set name.	varchar	64
ACTIVE	1 = active zone set 0 = otherwise.	smallint	

TABLE 269 ZONE_MEMBER

Field	Definition	Format	Size
ID*		int	
TYPE	Member type: 2 = WWN 4 = D,P	smallint	
VALUE	Member value (D,P or WWN).	varchar	256
ZONE_ID	PK of owning zone.	int	

TABLE 270 AD_GROUP

Field	Definition	Format	Size
ID *		int	
NAME	Name of the active directory group.	varchar	256
EMAIL	Active Directory Group Email Address.	varchar	1024
SOURCE_SERVER_NETWORK_ADDRESS	The LDAP Server Network Address from which the Active directory group is fetched	varchar	255

TABLE 271 AD_GROUP_AOR_MAP

Field	Definition	Format	Size
AD_GROUP_ID	Active directory group ID	int	
AOR_ID		int	

TABLE 272 AD_GROUP_ROLE_MAP

Field	Definition	Format	Size
AD_GROUP_ID	Active directory group ID	int	
ROLE_ID		int	

TABLE 273 AOR

Field	Definition	Format	Size
ID*		int	
NAME		varchar	128
DESCRIPTION		varchar	512

TABLE 274 AOR_DEVICE_GROUP_MAP

Field	Definition	Format	Size
AOR_ID	ID of the AOR.	int	
DEVICE_GROUP_ID	The Product Group which is in the AOR.	int	

TABLE 275 AOR_DEVICE_MAP

Field	Definition	Format	Size
AOR_ID	ID of AOR	int	
DEVICE_ID	The DEVICE ID can be IP Product or ServerIron ID which is in the AOR	int	

TABLE 276 AOR_FABRIC_MAP

Field	Definition	Format	Size
AOR_ID	ID of AOR	int	
FABRIC_ID	FABRIC ID which is in the AOR	int	

TABLE 277 AOR_HOST_MAP

Field	Definition	Format	Size
AOR_ID	ID of AOR	int	
HOST_ID	HOST ID which is in the AOR	int	

TABLE 278 AOR_INM_PORT_GROUP_MAP

Field	Definition	Format	Size
AOR_ID	ID of AOR	int	
PORT_GROUP_ID	IP of port group	int	

TABLE 279 AUTO_TRACE_DUMP

Field	Definition	Format	Size
CORE_SWITCH_ID		int	
ENABLED	The enabled/disabled state of automatic trace dump transfer on the switch	smallint	
PROTOCOL	The protocol Unknown(0)/FTP(1)/SCP(2) to be used for transfer	smallint	
IP_ADDRESS	The Host IP Address	varchar	64
USER_NAM	The user name	varchar	64
LOCATION	Directory location where trace dump files are to be saved	varchar	1024
PASSWORD	The user password	varchar	64

TABLE 280 BOOT_IMAGE_DRIVER_MAP

Field	Definition	Format	Size
ID		int	
MAJOR_VERSION	Major Version bit from Boot Image file	smallint	
MINOR_VERSION	Minor Version bit from Boot Image file	smallint	
MAINTENANCE	Maintenance Version bit from Boot Image file	smallint	
PATCH	Patch Version bit from Boot Image file	varchar	32
MD5_HASH	MD5 hash value for Boot Image file	varchar	64
SUPPORTED_DRIVERS	Compatible HCM Drivers delimited by comma	varchar	256

TABLE 281 BOOT_IMAGE_FILE_DETAILS_

Field	Definition	Format	Size
ID		int	
DRIVER_MAPPING_ID		int	
BOOT_IMAGE_NAME	Name of Boot Image file	varchar	64
MAJOR_VERSION	Major Version bit from Boot Image file	smallint	
MINOR_VERSION	Minor Version bit from Boot Image file	smallint	
MAINTENANCE	Maintenance Version bit from Boot Image file	smallint	
PATCH	Patch Version bit from Boot Image file	varchar	32
IMPORTED_DATE	Imported date of Boot Image file	timestamp	
RELEASE_DATE	Release date of Boot Image file	timestamp	
RELEASE_NOTES_LOCATI ON	Release notes location in Management applciation Repository	varchar	1024
LOCATION	Boot Image file location in Management applciation Repository	varchar	1024

TABLE 282 BOOT_LUN_SEQUENCE

Field	Definition	Format	Size
ID		int	
NAME	Name of the Boot LUN Sequence	varchar	64
FABRIC_ID	PK of the owning fabric	INT	

TABLE 283 BOOT_LUN_SEQUENCE_DETAIL

Field	Definition	Format	Size
ID *		int	
BOOT_LUN_SEQ_ID	PK of the owning Boot LUN Sequence	char	23
PORT_WWN	WWN of the port in the Boot LUN Sequenc	int	
LUN_NUM	LUN number of the port in the Boot LUN Sequence	int	
SEQUENCE_NUM	Sequence number of the port in the Boot LUN Sequence		

TABLE 284 CEE_PORT

Field	Definition	Format	Size
ID		int	
GIGE_PORT_ID	FK to GIGE_PORT	int	
VIRTUAL_SWITCH_ID	FK to owning VIRTUAL_SWITCH	int	
IF_INDEX	Interface index	int	
IF_NAME	Interface name	varchar	64
IF_MODE	Gige port mode (L2, L3, none)	varchar	8
L2_MODE	L2 mode (hybrid, trunk, access)	varchar	32
VLAN_ID	List of VLAN this port belongs to	text	
LAG_ID	LAG ID this port belongs to	int	
IP_ADDRESS	Port''s configured IP address	varchar	128
MAC_ADDRESS	Port''s MAC address	varchar	64
PORT_SPEED	Speed in Gb/sec. The default value is 0.	int	
ENABLED	State. The default value is 0.	smallint	
OCCUPIED	The default value is 0.	smallint	
LAST_UPDATE		bigint	
MAC_ACL_POLICY	stores the MAC ACL policy information of the port	varchar	64
NET_MASK	Netmask of the IPAddress of the port	varchar	128
PROTOCOL_DOWN_REASON	Reason for the port''s operational state being down	varchar	512
QOS_TYPE	QoS Type (Cee-Map, TrafficClass Map, FCoE map)	varchar	32

TABLE 284 CEE_PORT (Continued)

Field	Definition	Format	Size
QOS_NAME	Name of the QoS Map set on the port	varchar	64
DOT1X_ENABLED	Indicate if 802.1x authentication is enabled on this port. The default value is 0.	smallint	

TABLE 285 CLIENT_VIEW_MEMBER_HOST

Field	Definition	Format	Size
CLIENT_VIEW_ID	Primary key of CLIENT_VIEW table	int	
HOST_ID	Primary key of DEVICE_ENCLOSURE table	int	

TABLE 286 CLUSTER

Field	Definition	Format	Size
ID *	Arbitrary integer to identify the cluster.	int	
NAME	User-assigned name to identify the cluster. Names should be unique to avoid user confusion, but the database does not enforce uniqueness.	varchar	64
IP_ADDRESS	The primary hostname or IP address for managing the cluster as a single entity. The definition of primary depends on the clustering technology.	varchar	64

TABLE 287 CLUSTER_MEMBER

Field	Definition	Format	Size
CLUSTER_ID	Identifies the cluster containing a member.	int	
DEVICE_ENCLOSURE_ID	Identifies a member of the cluster.	int	32

TABLE 288 CNA_ETH_PORT

Field	Definition	Format	Size
ID	ID of the Eth port	int	
ETH_DEV	Ethernet device	varchar	64
ETH_LOG_LEVEL	The default value is 1.	int	
NAME	Name of the port	varchar	256
MAC_ADDRESS	MAC Address	varchar	64
IOC_ID	IO controller ID. The default value is 0.	varchar	64
HARDWARE_PATH	Hardware path of the port	varchar	256
STATUS	Status of the Eth port. The default value is -1.	varchar	64
CNA_PORT_ID	ID of the parent port	int	
CREATION_TIME		timestamp	
CURRENT_MAC_ADDRESS	User definable Mac address which is by default same as built in Mac address	varchar	64

TABLE 289 CNA_PORT

Field	Definition	Format	Size
ID	Primary key autogenerated ID	int	
PORT_NUMBER	Port number of the CNA port	int	
PORT_WWN	Port WWN of the port	char	23
NODE_WWN	Node WWN of the port	char	23
PHYSICAL_PORT_TYPE	Port type CNA/FC	varchar	32
NAME	Name of the port	varchar	256
MAC_ADDRESS	MAC address of the port.	varchar	64
MEDIA	Media of the port	varchar	64
CEE_STATE	State of the port.	varchar	64
HBA_ID	ID of the port.	int	
CREATION_TIME		timestamp	
FACTORY_PORT_WWN	Factory configured Port WWN defined for the CNA port in HCM	varchar	23
FACTORY_NODE_WWN	Factory configured Node WWN defined for the CNA port in HC	varchar	23
PREBOOT_CREATED	Flag to identify vports created during preboot and will accept string values True/false/empty	varchar	23

TABLE 290 COLLECTION_END_TIMESTAMP

Field	Definition	Format	Size
COLLECTOR_SOURCE		varchar	256
COLLECTOR_NAME		varchar	256
TIMESTAMP_		timestamp	
LAST_COLLECTED_STATUS	The default value is 0.	smallint	
FIRST_COLLECTION_TIMESTAMP		timestamp	
SUCCESSFUL_RUNS		bigint	
FAILED_RUNS		bigint	
LAST_FAILURE_TIMESTAMP		timestamp	
LAST_SUCCESSFUL_TIMESTAMP		timestamp	

TABLE 291 COLLECTOR_END_TIMESTAMP

Field	Definition	Format	Size
COLLECTOR_SOURCE *	Internal key for switches and fabrics for which collection is undertaken.	varchar	256
COLLECTOR_NAME *	Collection name, Java class used to collect specific fabric or switch information.	varchar	256

TABLE 291 COLLECTOR_END_TIMESTAMP (Continued)

Field	Definition	Format	Size
TIMESTAMP_	When the last successful collection is done.	timestamp	
LAST_COLLECTED_STATUS	Status of the last collection, successful or not. 200 is for successful. Values are standard HTTP protocol values.	smallint	

TABLE 292 CRYPTO_HOST

Field	Definition	Format	Size
ID		int	
CRYPTO_TARGET_CONTAINER_ID	Foreign key reference to the CRYPTO_TARGET_CONTAINER that contains this host.	int	
VI_NODE_WWN	Node WWN of Virtual Initiator that represents this host.	char	23
VI_PORT_WWN	Port WWN of Virtual Initiator that represents this host.	char	23
HOST_PORT_WWN	Physical (real) host''s Port WWN	char	23
HOST_NODE_WWN	Physical (real) host''s Node WWN	char	23

TABLE 293 CRYPTO_LUN

Field	Definition	Format	Size
ID		int	
CRYPTO_TARGET_CONTAINER_ID	Foreign key reference to the CRYPTO_TARGET_CONTAINER that contains the host for which these LUNs are configured.	int	
SERIAL_NUMBER	The LUN serial number, used to identify the physical LUN.	varchar	256
ENCRYPTION_STATE	Boolean. True (1) if LUN is being encrypted. False (0) if cleartext.'; The default value is 0.	smallint	
STATUS	Not currently used but left in for possible future use. Replaced by LUN_STATE. The default value is 0.	smallint	
REKEY_INTERVAL	The number of days that data encryption keys should be used before automatically generated a new key. 0 = infinite, i.e., no re-keying.	int	
VOLUME_LABEL_PREFIX	A user-configured string used to construct the Brocade-specific volume label on encrypted tapes. Ignored for disk LUNs.	varchar	256
LAST_REKEY_DATE	The last time a data encryption key was generated for this LUN. REKEY_INTERVAL days after this date, a new key will be generated.	timestamp	
LAST_REKEY_STATUS	The success or failure of the most recent re-keying operation, if any. This field is not currently used, but is left in the hope that FOS will support it in the future. Only valid for disk LUNs. The default value is 0.	smallint	

TABLE 293 CRYPTO_LUN (Continued)

Field	Definition	Format	Size
LAST_REKEY_PROGRESS	Indicates whether a re-key operation is in progress. 0 = no re-keying in progress. > 0 = percentage done of re-keying operation in progress. Only valid for disk LUNs. The default value is 0.	smallint	
CURRENT_VOLUME_LABEL	If a tape session is in progress, this is the volume label for the currently mounted tape. Only valid for tape LUNs.	varchar	2048
PRIOR_ENCRYPTION_STATE	Not used. When configuring a new disk LUN, this field indicates whether the LUN is already encrypted (1) or cleartext (0). This information does not need to be persisted. Only valid for disk LUNs.	smallint	
ENCRYPTION_FORMAT	If ENCRYPTION_STATE is true, ENCRYPTION_FORMAT indicates the type of encryption. 0 = cleartext, 1 = DF-compatible, 2 = native.	smallint	
ENCRYPT_EXISTING_DATA	Not used. When configuring a disk LUN that was previously cleartext and is to be encrypted, this property tells the switch whether or not to start a re-keying operation to encrypt the existing LUN data. This property does not need to be persisted.	smallint	
DECRYPT_EXISTING_DATA	Not used. When configuring disk LUN that was previously encrypted and is to become cleartext, this property tells the switch whether or not to start a re-keying operation to decrypt the existing LUN data. This property does not need to be persisted. This feature is no longer supported in FOS.	smallint	
KEY_ID	Hex-encoded binary key vault ID for the current data encryption key for this LUN. This ID may be used to locate the data encryption key in the key vault.	varchar	64
CRYPTO_HOST_ID	Foreign key reference to the CRYPTO_HOST that uses this LUN.	int	
LUN_NUMBER	The Logical Unit Number of the LUN, as seen by the LUNs host. This may be an integer (0 - 65565) or a WWN-format 8-byte hex number.	varchar	64
BLOCK_SIZE	The LUN''s Logical Block Size, in bytes. Only valid for disk LUNs.	int	
TOTAL_BLOCKS	The total number of logical blocks in the LUN. Multiplying BLOCK_SIZE by TOTAL_BLOCKS gives the LUN size in bytes.	int	
LUN_STATE	LUN operational status, such as OK or disabled for various reasons. For possible values see the enum definition in CryptoClientConstants. The default value is 0.	int	

TABLE 293 CRYPTO_LUN (Continued)

Field	Definition	Format	Size
LUN_FLAGS	Bitmap of LUN options. The only option currently used is bit 0 (least significant) which indicates that the LUN must be manually enabled because it has been disabled due to inconsistent metadata detected. The default value is 0.	bigint	
ENCRYPTION_ALGORITHM	Stores the Encryption Algorithm used to encrypt/decrypt data on the LUN	varchar	512
KEY_ID_STATE	State of the Key ID retrieval from Key Vault. The default value is 0.	smallint	
REKEY_SESSION_NUMBER	Unique Rekey session number. The default value is 0.	int	
PERCENTAGE_COMPLETE	% of rekey completion. The default value is 0.	int	
REKEY_ROLE	Rekey Role definition. The default value is 0.	smallint	
CURRENT_LBA	Current Logical Block address for the rekey session in progress. The default value is 0.	int	
LUN_STATE_STRING	Lun state string.	varchar	2048
NEW_LUN	This field specifies that when a LUN is added to its container, indicate that it''s a new LUN to be used in SRDF Configuration. Feature available only from 6.4 release onwards and for RSA key vaults. CryptoLun collector and CryptoLunBean fills in this value. The default value is -1.	smallint	
NEW_LUN_TYPE	This field indicates the role of the LUN configured in the SRDF mode. The values could be R1, R2 or UNKNOWN. Feature available only from 6.4 release onwards and for RSA key vaults. CryptoLuncollector fills in this value.	varchar	64

TABLE 294 CRYPTO_TARGET_CONTAINER

Field	Definition	Format	Size
ID		int	
ENCRYPTION_ENGINE_ID	Foreign key reference to the ENCRYPTION_ENGINE that owns this container.	int	
NAME	A user-supplied name for the container.	varchar	64
VT_NODE_WWN	The Node WWN of the Virtual Target that represents the real physical target device.	char	23
VT_PORT_WWN	The Port WWN of the Virtual Target that represents the real physical target device.	char	23

TABLE 294 CRYPTO_TARGET_CONTAINER (Continued)

Field	Definition	Format	Size
FAILOVER_STATUS	Indicates whether this container''s target is being encrypted by the encryption engine on which the container is configured (value 0) or by another encryption engine in the HA Cluster (value 1). Default value is 0..	smallint	
FAILOVER_STATUS_2	Failover status from the HA Cluster peer.	smallint	
DEVICE_STATUS	The physical target storage device operational status when the virtual initiator last attempted to access the target. For possible values, see the enum definition in the DTO class. Default value is 0.	smallint	
DEVICE_TYPE	Indicates whether the target storage device is a disk (0) or tape (1) device. Default value is 0.	smallint	
TARGET_PORT_WWN	The Port WWN of the physical target storage device associated with this container.	char	23
TARGET_NODE_WWN	The Node WWN of the physical target storage device associated with this container.	char	23
CONTAINER_FIELD_DATA	Container metadata information	varchar	256
CONFIGURATION_STATUS	Configuration status. Default value is 0.	smallint	
FRONT_END_N_PORT_NUMBER	Indicates N_Port number where CISCO Fabric will be connected when BES is in AG Mode. Default value is -1.	smallint	

TABLE 295 DEVICE_PORT_GIGE_PORT_LINK

Field	Definition	Format	Size
DEVICE_PORT_ID	The primary key of the DevicePort	int	
GIGE_PORT_ID	The primary key of the GigEPort.	int	
DIRECT_ATTACH	Indicates whether the device port is directly attached to the CEE 10G TE port.	smallint	

TABLE 296 DEVICE_PORT_MAC_ADDRESS_MAP

Field	Definition	Format	Size
DEVICE_PORT_ID	The primary key of the DevicePort.	int	
MAC_ADDRESS	Mac address of device.	varchar	64

TABLE 297 ENCRYPTION_ENGINE

Field	Definition	Format	Size
ID		int	
SWITCH_ID	Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that contains this encryption engine.	int	
SLOT_NUMBER	For chassis switches, the slot or blade that contains the encryption engine. Always 0 for pizza-box switches with a single embedded encryption engine.	smallint	
STATUS	Not used. Previously used to indicate the engine''s operational status. Replaced by EE_STATE. The default value is 0.	smallint	
HA_CLUSTER_ID	Foreign key reference to an HA_CLUSTER record. Identifies the HA Cluster that this engine belongs to. Null if this engine does not belong to an HA Cluster.	int	
SYSTEM_CARD_STATUS	Indicates whether a System Card is currently inserted in the Encryption Engine, and whether the card is valid or not. This feature is not yet supported. The default value is 'disabled'.	varchar	256
WWN_POOLS_AVAILABLE	Not used. Previously used to indicate the number of WWN pools remaining for allocation on this encryption engine. This feature is no longer supported.	int	
STATE	Administrative state for this engine. 0 = disabled, 1 = enabled. The default value is 0.	smallint	
SP_CERTIFICATE	The public key certificate, in PEM format, for the Security Processor within the Encryption Engine. Used to create link keys for Decru LKM key vaults.	varchar	4096
EE_STATE	The operational status of this Encryption Engine. For possible values, see the enum defintion in the DTO class The default value is 0.	int	
HA_CLUSTER_STATUS	Stores the status of the HA Cluster to which the engine is a pair participant The default value is 0.	smallint	
ROUTING_MODE		smallint	
MEDIA_TYPE		char	50
LINK_IP_ADDRESS	Local EE - BP Link IP Address, If there are no links the IP Address could be 0.0.0.0	varchar	64
LINK_NET_MASK	Local EE - BP Link IP new mask	varchar	64
LINK_GW_IP_ADDRESS	Local EE- BP Gateway Address	varchar	64
LINK_MAC_ADDRESS	Local EE Link MAC Address	varchar	64

TABLE 297 ENCRYPTION_ENGINE (Continued)

Field	Definition	Format	Size
LINK_MTU	Local EE Link MTU. The default value is -1.	int	
LINK_STATE	Local EE State says whether link is down or up	varchar	256
REBALANCE_REQUIRED	This field indicates whether a rebalance operation is required on the Encryption Engine. It can take two values, One(1) indicating that rebalance is required on the Encryption Engine and zero(0) indicating that no rebalance is required on the Encryption Engine. Encryption Engine is said to be unbalanced when the disk and Tape containers are not evenly balanced on the hosting engine. The default value is 0.	smallint	

TABLE 298 ENCRYPTION_GROUP

Field	Definition	Format	Size
ID		int	
NAME	User-assigned name for this encryption group.	varchar	64
LEADER_SWITCH_ID	'Foreign key reference to both the VIRTUAL_SWITCH table and the CRYPTO_SWITCH table (both switch tables use the same primary key values). Identifies the switch that currently provides central configuration and reporting capabilities for the encryption group. This column may be null if the group leader is not in a discovered fabric.	int	
LEADER_SWITCH_WWN	The Node WWN of the current group leader switch. Each encryption group has one group leader switch.	char	23
DEPLOYMENT_MODE	Indicates Transparent (0) or NonTransparent (1) deployment mode. Only Transparent mode is currently supported. All switches in the Encryption Group share the same deployment mode. Transparent mode uses re-direction zones to preserve existing zoning of physical hosts and targets. Non-transparent mode requires zoning changes to zone physical hosts with Virtual Targets and to zone Virtual Initiators with physical targets. The default value is 0.	smallint	
FAILBACK_MODE	Indicates Automatic (0) or Manual (1) failback. Failback occurs when a previously unavailable Encryption Engine comes back online. In Auto mode, the restored Encryption Engine resumes encrypting all traffic for target containers configured on the Encryption Engine. In manual mode, encryption continues running on the backup encryption engines until manually changed. The default value is 0.	smallint	

TABLE 298 ENCRYPTION_GROUP (Continued)

Field	Definition	Format	Size
SYSTEM_CARD_REQUIRED	Boolean value that indicates whether a System Card (smart card) must be inserted in the Encryption Engine to enable the engine after power-up. This feature is not yet supported. The default value is 0.	smallint	
ACTIVE_MASTER_KEY_ STATUS	The operational status of the "master key" or "Key Encryption Key (KEK)" used to encrypt Data Encryption Keys in a key vault. Not used for Decru LKM key vaults. 0 = not used, 1 = required but not present, 2 = present but not backed up, 3 = okay. The default value is 0.	smallint	
ALT_MASTER_KEY_STATUS	The operational status of an alternate "master key" used to access older data encryption keys. Not used for Decru LKM key vaults. 0 = not used, 1 = not present, 3 = okay. The default value is 0.	smallint	
QUORUM_SIZE	The number of authentication cards required to approve certain secure operations. This feature is not yet supported. The default value is 0.	smallint	
RECOVERY_SET_SIZE	No longer used. Previously used to indicate the number of smart cards used to back up a Master Key. The number of cards is now specified when the backup is created, and not persisted in the database. The default value is 0.	smallint	
KEY_VAULT_TYPE	Indicates the type of key vault used by switches in this Encryption Group. 0 = Decru Lifetime Key Manager (LKM), 1 = RSA Key Manager (RKM), 2 = Brocade internal key storage (for demo use only). The default value is 0.	smallint	
PRIMARY_KEY_VAULT_ID	Foreign key reference to the KEY_VAULT record that describes the primary key vault for this Encryption Group. Null if no primary key vault is configured.	int	
BACKUP_KEY_VAULT_ID	Foreign key reference to the KEY_VAULT record that describes the backup key vault for this Encryption Group. Null if no backup key vault is configured.	int	
GROUP_LEADER_STATUS	Stores the status of the Group leader node	int	
SRDF_MODE	This field denotes whether the SRDF support is enabled or not. Feature available only from 6.4 release onwards and for RSA key vaults. EncryptionGroup collector and EncryptionGroupBean fills in this value. The default value is -1.	smallint	

TABLE 299 ETHERNET_CLOUD

Field	Definition	Format	Size
ID		int	
SWITCH_ID	The unique id of the switch this cloud is associated to.	int	

TABLE 300 ETHERNET_ISL

Field	Definition	Format	Size
ID		int	
SOURCE_PORT_ID	The unique id of the source port.	int	
DEST_PORT_ID	The unique id of the destination port.	int	
MISSING		smallint,	
MISSING_TIME		timestamp	
TRUSTED		smallint,	
CREATION_TIME		timestamp	

TABLE 301 EVENT_CALL_HOME

Field	Definition	Format	Size
ID		int	
EVENT_ID		int	
EVENT_NUMBER	Event Number field was introduced to handle Call home use case for MEOS switches. MEOS events have unique event number for each call home events that will be sent as a part of call home messages. Call home customers(Connect EMC, IGS Cather) are using this field. The default value is 0.	int	
FRU_CODE	This column was introduced to handle Call home use cases for MEOS switches. ACH module will be depending on this value to create call home messages and dispatch it to call home centers. This field is mandatory for all call home centers	int	
REASON_CODE	Used by CallHome feature	int	
FRU_POSITION	Used by CallHome feature	int	

TABLE 302 EVENT_CATEGORY

Field	Definition	Format	Size
ID	0 - Unknown 1 - Product Event 2 - Link Incident Event 3 - Product Audit Event 4 - Product Status Event 5 - Security Event 6 - User Action Event 7 - Management Server Event	int	
DESCRIPTION		varchar	50

TABLE 303 EVENT_DESCRIPTION

Field	Definition	Format	Size
ID		int	
DESCRIPTION		varchar	1024

TABLE 304 EVENT_DETAILS

Field	Definition	Format	Size
ID		int	
EVENT_ID		int	
FIRST_OCCURRENCE_SWITCH_TIME		timestamp	
LAST_OCCURRENCE_SWITCH_TIME		timestamp	
CONTRIBUTORS	Populated only for SAN events	varchar	512
OPERATIONAL_STATUS	Populated only for SAN events - check the constants	varchar	255
NODE_WWN	Populated only for SAN events	varchar	23
PORT_WWN	Populated only for SAN events	varchar	23
OID		varchar	50
VIRTUAL_FABRIC_ID	Virtual Fabric Id of the switch	smallint	
UNIT	From INM EVENT_MAIN table	smallint	
SLOT	From INM EVENT_MAIN table	int	
PORT	From INM EVENT_MAIN table	int	
PRODUCT_ADDRESS		varchar	
RAS_LOG_ID	Reference to RAS_LOG table. This will be used to retrieve Probable cause and Recommended cause information in addition to showing MESSAGE_ID information retrieved from SAN switches.	varchar	

TABLE 305 EVENT_FWD_FILTER

Field	Definition	Format	Size
ID		int	
NAME	Filter Name	varchar	32
DESCRIPTION		varchar	256
TYPE	Filter Type (SNMP/ SYSLOG)	smallint	
APPLICATION_ENABLED	If Application Events enabled	smallint	
SNORT_ENABLED	If Snort Messages enabled	smallint	
PSUDO_ENABLED	If Pseudo Events enabled	smallint	
REGULAR_EXP	Common filtering message for Syslog Forwarding	varchar	512
SEVERITY	Emergency(0), Alert(1), Critical(2), Error(3), Warning(4), Notice(5), Info(6), Debug (7). Traps with selected severity and those with higher severity will be forwarded.	smallint	

TABLE 306 EVENT_FWD_FILTER_DEV_GROUP_MAP

Field	Definition	Format	Size
FILTER_ID		int	
DEVICE_GROUP_ID		int	

TABLE 307 EVENT_FWD_FILTER_ME_MAP

Field	Definition	Format	Size
FILTER_ID		int	
ME_ID		int	

TABLE 308 EVENT_FWD_FILTER_RECIPIENT_MAP

Field	Definition	Format	Size
FILTER_ID		int	
RECIPIENT_ID		int	

TABLE 309 EVENT_FWD_FILTER_TRAP_OID

Field	Definition	Format	Size
ID		int	
FILTER_ID		int	
OID_VALUE		varchar	256
OID_NAME		varchar	64

TABLE 310 EVENT_INSTANCE

Field	Definition	Format	Size
ID		int	
EVENT_POLICY_ID	Foreign Key to Event_Policy Table	int	
EVENT_KEY	A String Key string which identifies a specific instance of an Event.	varchar	64
STRING_PATTERN	A Regular expression pattern string which can be used to match an Event instance.	varchar	1024
CATEGORY	A small integer which identifies the Category of an Event instance. 0 - Unknown 1 - Product Event 2- Link Incident Event 3 - Product Audit Event 4- Product Status Event 5 - Security Event 6- User Action Event 7- Management Server Event. The default value is 0.	smallint	
SEVERITY	The Severity of the Event that is logged per Event Policy 0- Unknown 1- Emergency 2- Alert 3- Critical 4- Error 5- Warning 6- Notice 7- Info 8- Debug. The default value is 0.	smallint	
SEQUENCE_NUMBER	The sequence number of an event instance that''s specific to the policy. The default value is 0.	smallint	
MSG_IDS	Stores the Message ID(s) configured for Custom Event Type	varchar	512

TABLE 311 EVENT_MODULE

Field	Definition	Format	Size
ID	The default value is 0.	int	
DESCRIPTION		varchar	256

TABLE 312 EVENT_ORIGIN

Field	Definition	Format	Size
ID	0 - Unknown 1 - Trap 2 - Syslog 3 - Snort 4 - Pseudoevent 5 - Application Events 6 - Others	int	
DESCRIPTION		varchar	50

TABLE 313 **EVENT_POLICY**

Field	Definition	Format	Size
ID		int	
TYPE	Even Policy Type 0 - Pseudo Event 1 - Event Action	smallint	
NAME	The Name of the Event Policy	varchar	256
DESCRIPTION	The Description of the Event Policy	varchar	1024
STATUS	Administrative status of the Event Policy 0 - disabled 1- enabled	smallint	
LAST_MODIFIED_TIME	The Severity of the Event that is logged per Event Policy 0- Unknown 1- Emergency 2- Alert 3- Critical 4- Error 5- Warning 6- Notice 7- Info 8- Debug';	timestamp	
SEVERITY	The Event Policy Sub Type Escalation (0), Resolving (1), Flapping (2),Repeating (3). The default value is 0.	smallint	
MESSAGE		varchar	256
SUB_TYPE	The Event Policy Sub Type Escalation (0), Resolving (1), Flapping (2),Repeating (3)	smallint	
EVENT_ORIGIN	0- SNMP Trap 1- Application Event 2- Pseudo Event 3- Snort 4- Pseudo Event 5- Custom Event	smallint	
PROPERTIES	The property string which is used to define various parameters that are associated with an Event Policy such as flapping time and durations etc	varchar	2048

TABLE 314 **EVENT_POLICY_SOURCE_ENTRY**

Field	Definition	Format	Size
ID		int	
EVENT_POLICY_ID	Foreign Key to Event_Policy Table	int	
MANAGEMENT_ELEMENT_ID	A soft reference key to the Management Element ID. Do not maintain it as a foreign key constraints. The default value is 0.	int	
INTERFACE_ID	A soft reference key to the Interface ID. Do not maintain it as a foreign key constraints. The default value is 0.	int	
DEVICE_GROUP_ID	A reference key to the Device Group Do not maintain it as a foreign key constraints. The default value is 0.	int	
PORT_GROUP_ID	A reference key to the Port Group Do not maintain it as a foreign key constraints. The default value is 0.	int	

TABLE 314 EVENT_POLICY_SOURCE_ENTRY (Continued)

Field	Definition	Format	Size
SOURCE_SELECTION_TYPE	Option selected to give Source Information 0- IPAddress/Node wwn/Name provided 1- Source selected from available list of sources. The default value is 0.	smallint	
IP_ADDRESS	IP address of source	varchar	1024
WWN	Node WWN of source	varchar	1024
SOURCE_NAME	Source Name	varchar	1024

TABLE 315 EVENT_PROCESSOR_MAP

Field	Definition	Format	Size
PROCESSOR_CLASS_NAME	The fully qualified processor class name which will be invoked for the corresponding event id in this table. Column added as part of the Event Processing Framework	varchar	1024
EVENT_ID	The Event Id is the Trap OID on which the corresponding processor needs to act up on . Column added as part of the Event Processing Framework	varchar	1024

TABLE 316 FABRIC_ZONING_EDIT_RESTRICTION

Field	Definition	Format	Size
ID		int	
FABRIC_ID	PK of the owning fabric	int	
CHANGE_COUNT	Count of the maximum changes allowed in active zone config in the fabric.The default value is 0.	int	

TABLE 317 FCIP_CIRCUIT_PORT_MAP

Field	Definition	Format	Size
CIRCUIT_ID		int	
SWITCH_PORT_ID	SWITCH_PORT_ID of one end of the circuit	int	

TABLE 318 FCIP_TUNNEL_CIRCUIT

Field	Definition	Format	Size
ID		int	
TUNNEL_ID	Tunnel ID to which the circuit belongs to	int	
CIRCUIT_NUMBER	Circuit Number of the Circuit from the switch	smallint	
COMPRESSION_ENABLED	Whether Compression is enabled on that circuit	smallint	
TURBO_WRITE_ENABLED	Whether TurboWrite is enabled on that circuit'	smallint	

TABLE 318 FCIP_TUNNEL_CIRCUIT (Continued)

Field	Definition	Format	Size
TAPE_ACCELERATION_ENABLED	Whether TapeAccelaration is enabled on that circuit	smallint	
IKE_POLICY_NUM	The IKE Policy on the circuit.The default value is -1.	int	
IPSEC_POLICY_NUM	The IPSEC Policy on the circuit'. The default value is -1	int	
PRESHARED_KEY	The preshared Key on the circuit	char(	32
SOURCE_IP	SOURCE_IP of the circuit	varchar	64
DEST_IP	DESTINATION_IP of the circuit	varchar	64
VLAN_TAG	VLAN Tag of the circuit. The default value is -1	int	
SELECTIVE_ACK	Select acknowledgement flag.The default value is 0.	smallint	
QOS_MAPPING	QOS Mapping. The default value is 0.	smallint	
PATH_MTU_DISCOVERY	MTU Discovery Path. The default value is 0.	smallint	
MIN_COMM_RATE	Minimum communication Speed. The default value is 0.	int	
MAX_COMM_RATE	Maximum communication Speed. The default value is 0.	int	
MIN_RETRANSMIT_TIME	Minimum Retransmission Time. The default value is -1	int	
MAX_RETRANSMIT_TIME	Maximum retransmission time. The default value is -1	int	
KEEP_ALIVE_TIMEOUT	Keep Alive timeout. The default value is -1	int	
ADMIN_STATUS	Is admin status enabled. The default value is 0.	smallint	
METRIC	Circuit metric to set priority. The default value is -1	int	
DATA_L2_COS	Class of service as defined by IEEE 802.1p for circuit. The default value is -1.	int	
DSCP_DATA	DiffServe marking for Data Frame. The default value is -1	int	

TABLE 318 FCIP_TUNNEL_CIRCUIT (Continued)

Field	Definition	Format	Size
MAX_RETRANSMISSIONS	Max number of Retransmission attempts on the circuit. The default value is 0.	int	
SLOT_NUMBER	Slot number of the circuit. The default value is 0.	smallint	
VE_PORT_NUMBER	VE port number of the tunnel to which the circuit belongs.	int	
SECURITY_FLAG	Security Flag associated with the circuit. The default value is 0.	int	
DSCP_CONTROL	Diffserve marking for control frame. The default value is 0.	int	
CIRCUIT_STATUS	Status of the circuit. The default value is 0.	smallint	
ENABLED	Is circuit enabled. Default: 0, Values: 0|1. The default value is 0.	smallint	
MISMATCHED_CONFIGURATIONS	If a tunnel is down due to mismatched configurations on local and remote end, this property specifies the list of such mismatched configurations.	varchar	1024
CIRCUIT_STATUS_STRING	Circuit Status string value from switch for the tunnel	varchar	256
L2COS_F_CLASS	The default value is 0.	smallint	
L2_COS_HIGH	The default value is 0.	smallint	
L2_COS_MEDIUM	The default value is 0.	smallint	
L2_COS_LOW	The default value is 0.	smallint	
DSCP_F_CLASS	The default value is 0.	smallint	
DSCP_HIGH	The default value is 0.	smallint	
DSCP_MEDIUM	The default value is 0.	smallint	
DSCP_LOW	The default value is 0.	smallint	

TABLE 319 FCIP_TUNNEL_PERFORMANCE

Field	Definition	Format	Size
TUNNEL_ID	Primary key of the Switch Port	int	
SWITCH_ID	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	int	
TX	'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	double precision	
RX	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.	double precision	
TX_UTILIZATION	The computed value of TX based on speed of port	double precision	
RX_UTILIZATION	The computed value of RX based on speed of port	double precision	
DROPPED_PACKETS	Number of TCP packets dropped	double precision	
COMPRESSION	Compression ratio	bigint	
LATENCY	Round trip time (latency) in milliseconds	int	
LINK_RETRANSMITS	Number of segments retransmitted	double precision	

TABLE 319 FCIP_TUNNEL_PERFORMANCE (Continued)

Field	Definition	Format	Size
RTT_BY_TIME_OUT	Counter of retransmit packets due to timeout	double precision	
RTT_BY_DUP_ACK	Counter of retransmit packets due to duplicate acknowledgement'	double precision	
DUPLICATE_ACK	Counter of duplicate acknowledgement packets	double precision	
ROUND_TRIP_TIME	Round trip time in milliseconds	double precision	
TCP_OUT_OF_ORDER	Counter of TCP out-of-order.	double precision	
SLOW_START	Counter of slow starts	double precision	
LAST_UPDATE_TIME	'Time when this stats record was updated	timestamp	

TABLE 320 FCOE_DEVICE

Field	Definition	Format	Size
DEVICE_NODE_ID	The primary key of the DeviceNode.	int	
DIRECT_ATTACH	Indicates whether the fcoe device is directly attached to the switch''s TE port or to a cloud.	smallint	
ATTACH_ID	The primary key of the port (if direct attached) or cloud (if not direct attached).	int	
MAC_ADDRESS	Mac address of device.	varchar	64

TABLE 321 FRU

Field	Definition	Format	Size
ID		int	
CORE_SWITCH_ID		int	
TAG	provides the TAG number of FRU element, requested by SMIA and values filled in by Switch Asset Collector. Field probably contains information such as asset tag or serial number data. This value varies depending on the type of physical package	varchar	64
PART_NUMBER	provides the part number of the FRU element, requested by SMIA and values filled in by Switch Asset Collector. Field probably contains the part number assigned by the organization responsible for producing or manufacturing the physical element	varchar	64
SERIAL_NUMBER	provides the serial number of the FRU element, requested by SMIA and values filled in by Switch Asset Collector	varchar	64

TABLE 321 FRU (Continued)

Field	Definition	Format	Size
VENDOR_PART_ NUMBER	provides the Vendor-assigned part number of this package, requested by SMIA and values filled in by Switch Asset Collector	varchar	64
VENDOR_SERIAL_ NUMBER	provides the Vendor-assigned serial number of this package, requested by SMIA and values filled in by Switch Asset Collector'	varchar	64
CAN_BE_FRUED	provides whether this element can be removed from the switch, requested by SMIA and values filled in by Switch Asset Collector. Maps to IsRemovable field in the html. The default value is -1.	int	
SLOT_NUMBER	provides the slot number of this FRU element , requested by SMIA and values filled in by Switch Asset Collector.The default value is -1.	int	
MANUFACTURER_DATE	provides the manufactured date of this FRU element, requested by SMIA and values filled in by Switch Asset Collector	timestamp	
UPDATE_DATE	provides the updated date of this FRU element, requested by SMIA and values filled in by Switch Asset Collector	timestamp	
VERSION		varchar	32
MANUFACTURER	provides the manufacturer of this FRU element ,requested by SMIA and values filled in by Switch Asset Collector	varchar	64
VENDOR_EQUIPMENT_T YPE	provides the vendor equipment type of the FRU element, requested by SMIA and values filled in by Switch Asset Collector	varchar	32
OPERATIONAL_STATUS	provides the operational status of the FRU element, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. The default value is -1.	int	
TOTAL_OUTPUT_POWER	provides the total power output of the power supply FRU element, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. this field is applicable only for the power supply FRU element. The default value is -1.	bigint	
SPEED	provides the speed of the FAN FRU element, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. this field is applicable only for the FAN FRU element. The default value is -1.	int	
CREATION_TIME	provides the record creation time, standard columns for Management applciation and values filled in by Switch Asset Collector	timestamp	
LAST_UPDATE_TIME	provides the record creation time, standard columns for Management applciation and values filled in by Switch Asset Collector	timestamp	

TABLE 321 FRU (Continued)

Field	Definition	Format	Size
PREVIOUS_OP_STATUS	provides the previous operational status of FRU element, requested by SMIA and values filled in by Switch Asset Collector. Helps identify the operational status transitions. The default value is -1.	int	
VENDOR	This holds the vendor name information for FRU	varchar	256

TABLE 322 GIGE_PORT_ETHERNET_CLOUD_LINK

Field	Definition	Format	Size
ID		int	
CLOUD_ID		int	
SWITCH_PORT_ID	The unique id of the switch TE port that this member connects to.	int	
TRUSTED		smallint	
CREATION_TIME		timestamp	
MISSING		smallint	
MISSING_TIME		timestamp	

TABLE 323 HBA

Field	Definition	Format	Size
ID		int	
HOST_ID	Primary key.	int	
NAME	User defined name of the HBA	varchar	128
POWER_MODE	Power mode of the HBA	varchar	256
MODEL	Model code of the HBA	varchar	256
MODEL_DESCRIPTION	Model description for the HBA	varchar	256
OPERATING_STATUS	Current operating status of the HBA: 1: Enabled/0: Disabled. The default value is 0.	smallint	
CHIP_REVISION	Revision level of the chip used in the HBA	varchar	64
HARDWARE_PATH		varchar	256
SERIAL_NUMBER	Serial number of the HBA	varchar	64
TEMPERATURE	Temperatur of HBA. Both in Celsius/Fahrenheit	varchar	16
USERNAME		varchar	256
PASSWORD		varchar	256
MANAGEMENT_STATE	Management state bit mask, Managed/Auth failed etc. The default value is -1.	int	

TABLE 323 HBA (Continued)

Field	Definition	Format	Size
MANAGEMENT_INTERFACE	Management interface bit mask, JSON/WMI/SMI etc . The default value is -1.	int	
DRIVER_VERSION	The version level of the host adapter driver	varchar	256
DRIVER_NAME	The name of the HBA driver	varchar	256
FIRMWARE_VERSION	The version level of the firmware	varchar	256
BIOS_VERSION	The version level of the BIOS	varchar	256
PCI_REG_VENDOR_ID	The identifier of the PCI Register''s vendor	varchar	32
PCI_REG_DEVICE_ID	The device ID of the PCI Register	varchar	32
PCI_REG_SUBSYSTEM_ID	The ID of the PCI subsystem	varchar	32
PCI_REG_SUBSYS_VENDOR_ID	The ID of the PCI subsystem vendor.	varchar	32
PCI_REG_LANE_COUNT	The number of PCI lanes, in Gbps, each way between the PCI slot and the adapter. The default value is 8.	int	
PCI_REG_NEG_LANE_COUNT	The set number of PCI lanes that were initially negotiated. The default value is 8.	int	
PCI_REG_GENERATION	PCI generation	varchar	256
TRUSTED	The default value is 1.	smallint	
CREATION_TIME		timestamp	
MISSING	The default value is 0.	smallint	
MISSING_TIME		timestamp	
CIM_NAMESPACE	Reflects the CIM namespace used to discover the HBA	varchar	128
CARD_TYPE	FC for HBA, CNA for CNA. The default value is ‘FC’.	varchar	32
WWN	WWN of the adapter	varchar	23
HCM_AGENT_VERSION	Version of HCM agent used to managed the HBA	varchar	128
MAC_ADDRESS	Adapter mac address	varchar	64
MAX_SPEED_SUPPORTED	The maximum port speed that is supported on the port, in Gb/s. The default value is 0.	int	
VPD_PRODUCT_DESCRIPTION	Description of the product	varchar	256
VPD_PART_NUMBER	Part Number of the device	varchar	32
VPD_EC_LEVEL	EC Level of the device	varchar	32
VPD_FRU_NUMBER	FRU number of the device	varchar	32
VPD_SERIAL_NUMBER	serial number of the device	varchar	32

TABLE 323 HBA (Continued)

Field	Definition	Format	Size
VPD_PW	PW details of the device	varchar	32
VPD_EDC	EDC details of the device	varchar	32
VPD_MDC	MDC details of the device	varchar	32
VPD_FABRIC_GEOGRAPHY	FABRIC_GEOGRAPHY of the device	varchar	256
VPD_LOCATION	LOCATION of the device	varchar	256
VPD_MANUFACTURER_ID	MANUFACTURER_ID of the device	varchar	256
VPD_PCI_GEOGRAPHY	PCI_GEOGRAPHY of the device	varchar	256
VPD_VENDOR_DATA	VENDOR_DATA of the device	varchar	256
VPD_EXT_CAPABILITY	EXT_CAPABILITY of the device	varchar	256
VPD_OEM	OEM details of the device	varchar	256
VPD_OEM_INFO	OEM related information of the device	varchar	256

TABLE 324 HBA_NODE_MAP

Field	Definition	Format	Size
DEVICE_NODE_ID	Primary key from the Device Node table	int	
HBA_ID	Primary key from the HBA table	int	

TABLE 325 HOST_DISCOVERY_REQUEST

Field	Definition	Format	Size
ID	Autogenerated primary key	int	
HOST_NAME	Hostname: IP address or host name	varchar	256
DEVICE_ENCLOSURE_ID		int	
REQUEST_GROUP_ID	Primary key from the request group table. Null allowed	int	
HOST_DISCOVERY_OPTION_ID	This id is a foreign key to the id in the host_discovery_option table. The default value is -1.	int	
VM_MANAGEMENT_STATE	The status of VM Discovery indicating success or failure. The default value is 0.	int	
JSON_MANAGEMENT_STATE	The status of HBA discovery using JSON agent, indicating success or failure. The default value is 0.	int	

TABLE 325 HOST_DISCOVERY_REQUEST (Continued)

Field	Definition	Format	Size
CIM_MANAGEMENT_STATE	The status of HBA Discovery using CIM, indicating success or failure. The default value is 0.	int	
MANAGEMENT_STATE	Reflects the status of the request E.g. 0-> Completed, 1->Add Pending 2->Delete Pending 3->Edit Pending 4->Delete Failed. The default value is 1.	int	

TABLE 326 HOST_DISCOVERY_REQ_GROUP

Field	Definition	Format	Size
ID	Auto generated primary key	int	
NAME	Unique name for the host request. The default value is ‘ New Host Group'.	varchar(	256
DISCOVERY_OPTIONS_ID	Primary key from the host discovery options table. Points to the associated discovery options	int	
MANAGEMENT_STATE	Reflects the status of the request E.g. 0-> Completed, 1->Delete Pending. The default value is 0.	int	

TABLE 327 KEY_VAULT

Field	Definition	Format	Size
ID		int	
IP_ADDRESS	The IP Address (IPv4, IPv6, or hostname) of the key vault	varchar(	512
PORT_NUMBER	The TCP port number for the key vault	int	
PUBLIC_CERTIFICATE	The key vault''s public key certificate. Switches use this to establish a secure connection to the key vault	varchar(	4096
CERTIFICATE_LABEL	A text name to identify the certificate	varchar(	256
POSITION_	Specifies whether this key vault is the primary key vault or the backup key vault. 0 = primary, 1 = backup.	smallint	

TABLE 328 LAG

Field	Definition	Format	Size
ID		int	
VIRTUAL_SWITCH_ID	FK to owning VIRTUAL_SWITCH	int	
LAG_ID	LAG ID	int	
IF_INDEX	Interface index	int	
IF_NAME	Interface name	varchar	64
ENABLED	LAG is enabled=1, disabled=0	smallint	

TABLE 328 LAG (Continued)

Field	Definition	Format	Size
LAG_MODE	Static or dynamic (1=dynamic, 2=static)	smallint	
ACTIVE	LACP active or passive (1=active, 2=passive) valid if mode=dynamic	smallint	
TYPE	Trunking type (1=standard, 2=brocade, 3=hybrid)	smallint	
IF_MODE	L2 or L3 mode	varchar	8
L2_MODE	Type of L2 mode (default=access	varchar	32
MAC_ACL_POLICY	stores the MAC ACL policy information of the LAG	varchar	64
VLAN_LIST	Comma separated vlan id list.	text	
MAC_ADDRESS		varchar	64
IP_ADDRESS	Primary IPAddress of the LAG	varchar	128
NET_MASK	Netmask of the Primary IPAddress of the LAG	varchar	128

TABLE 329 LAG_MEMBER

Field	Definition	Format	Size
ID		int	
LAG_ID	FK to owning LAG	int	
NAME	Member name	varcha	64
TYPE	currently not used. The default value is 0.	smallint	
MEMBER_MODE	Dynamic Mode Active/passive. The default value is 0.	smallint	

TABLE 330 LICENSE

Field	Definition	Format	Size
ID		int	
LICENSE_KEY		varchar	1024
SERIAL_NO		varchar	255
CREATION_TIME	Time at which this license key is added	timestamp	
TYPE	Type of license: 0 - Trial, 1 - Permanent. The default value is 0.	smallint	
SUB_TYPE	Sub Type of license: 0 - Base, 1 - Addon. The default value is 0.	smallint	
VALID	Is this license still considered: 0 - No, 1 - Yes. The default value is 1.	smallint	

TABLE 331 LICENSE_RULE

Field	Definition	Format	Size
ID		int	
NAME	Name of the license rule	varchar	

TABLE 331 LICENSE_RULE (Continued)

Field	Definition	Format	Size
DESCRIPTION	Description of the rule	varchar	
SCOPE	Scope of the rule - is it applicable to Fabric, switch or ports	varchar	
CATEGORY	Category of the rule - is it used by unknown - 0, asset collection - 1, or 2 - the license manager service	smallint	
ENABLE	Whether the rule needs to be considered or not. 1 - consider, 0 - do not consider for calculation. The default value is 1.	smallint	

TABLE 332 LOCK

Field	Definition	Format	Size
NAME	The name of this transaction synchronization lock. The name should be upper case and should describe the activity being synchronized, such as MANAGED_ELEMENT_CREATION.	varchar	40
LAST_USED_BY	Identifies the transaction that last updated this lock record, such as IP_DISCOVERY. This field is primarily here just to have something to modify. The new value does not need to be different than the previous value.	varchar	40
LAST_USED_TIME	Optional time when the lock was last modified. Might be useful for debugging someday.	timestamp	

TABLE 333 MANAGED_ELEMENT

Field	Definition	Format	Size
ID	An ID that is unique across managed elements of all types: SAN physical switches, SAN logical switches, IP switches, and hosts. Also the primary key for the MANAGED_ELEMENT table.	int	
PLACEHOLDER	Not used. iBatis/Abator requires at least one non-serial column to generate correct objects. The default value is 0.	int	

TABLE 334 NPORT_WWN_MAP

Field	Definition	Format	Size
ID		int	
VIRTUAL_SWITCH_ID	AG switch reference on which the Nport wwn mapping resides.	int	
N_PORT	N Port through which AG is connected to the edge switch	smallint	
DEVICE_PORT_WWN	Device Port which is mapped to the N port. This device could be offline device as well.	char	23

TABLE 335 PASSWORD_HISTORY

Field	Definition	Format	Size
USER_NAME		varchar	128
PASSWORD_UPDATED_ DATETIME	The date and time the user updated password recently.	timestamp	
PREVIOUS_PASSWORD	User''s Previous password	varchar	512

TABLE 336 PHANTOM_PORT

Field	Definition	Format	Size
ID		int	
WWN	The Wwn of the phantom port.	char	23
VIRTUAL_SWITCH_ID	The id of the phantom switch.	int	
PORT_NUMBER	The port number of the phantom port. The default value is -1.	smallint	
PORT_ID	The portId of the phantom port. The default value is 000000.	varchar	8
SPEED	The speed of the phantom port. The default value is 0.	int	
MAX_SPEED	The max speed of the phantom port. The default value is 0.	int	
TYPE	The portType of the phantom port.The default value is 'Unknown'.	varchar	16
REMOTE_NODE_WWN	The remote node wwn(for E-ports only). Attached port device info must be retrieved from DevicePort table.	char	23
REMOTE_PORT_WWN	The remote port wwn(for E-ports only). Attached port device info must be retrieved from DevicePort table.	char	23
PHANTOM_TYPE	The phantom type of the port, either front or xlate	int	
BB_FABRIC_ID		int	

TABLE 337 PORT_BOTTLENECK_CONFIG

Field	Definition	Format	Size
SWITCH_PORT_ID	The database ID of the switch port that the configuration belongs to.	int	
BOTTLENECK_DETECT _ENABLED	Flag indicates if bottleneck detection is enabled or not. The default value is 0.	smallint	
ALERTS_ENABLED	Flag indicates if bottleneck detection alerts is enabled or not.The default value is -1.	smallint	
CONGESTION_ THRESHOLD	Value of bottleneck detection congestion threshold in percent. The default value is -1.	double precision	
LATENCY_THRESHOLD	Value of bottleneck detection latency threshold in percent. The default value is -1.	double precision	

TABLE 337 PORT_BOTTLENECK_CONFIG (Continued)

Field	Definition	Format	Size
WINDOW_	Value of bottleneck detection latency window in millisecond. The default value is 0.	int	
QUIET_TIME	Value of bottleneck detection quiet time in millisecond. The default value is 0.	int	
CREATION_TIME	Creation time of the record.	timestamp	
LAST_UPDATE_TIME	Last update time of the record.	timestamp	

TABLE 338 PORT_BOTTLENECK_STATUS

Field	Definition	Format	Size
SWITCH_PORT_ID	The database ID of the switch port that the status belongs to.	int	
STATUS	Flag indicates bottleneck status of the switch port.	smallint	

TABLE 339 PORT_GROUP

Field	Definition	Format	Size
ID		int	128
NAME		varchar	256
DESCRIPTION		varchar	
TYPE		int	
USER_NAME		varchar	128
FABRIC_ID		int	

TABLE 340 PORT_GROUP_MEMBER

Field	Definition	Format	Size
ID		int	
PORT_GROUP_ID		int	
SWITCH_PORT_ID		int	

TABLE 341 QRTZ_TRIGGER_LISTENERS

Field	Definition	Format	Size
TRIGGER_NAME		varchar	80
TRIGGER_GROUP		varchar	80
TRIGGER_LISTENER		varchar	80

TABLE 342 RESOURCE_HOST_MAP

Field	Definition	Format	Size
RESOURCE_GROUP_ID	Resource Group ID	int	
HOST_ID	HOST_ID,which is in the resource group	int	

TABLE 343 SSL_KEY_PASSWORD

Field	Definition	Format	Size
ID		int	
KEY_PASSWORD_ALIAS	Key Password Alias is the alias name used for the encrypted key password. This alias name is used to identify the password in client UI.	varchar	16
KEY_PASSWORD	SSL keys are protected by passwords, and these passwords are used during key import operation from device. The key password is stored encrypted in the tables.	varchar	256

TABLE 344 AOR_VIP_SERVER_MAP

Field	Definition	Format	Size
AOR_ID	The column holds ID of an AOR. It is Foreign Key and refers to ID column of AOR table	int	
VIP_SERVER_ID	The column holds ID of VIP Server. It is Foreign Key and refers to ID column of VIP_SERVER table	int	

TABLE 345 IP_DEVICE_LICENSE

Field	Definition	Format	Size
ID	Primary Key field for the DEVICE_LICENSE	int	
DEVICE_ID	This is the foreign key reference to the Device table	int	
HASH	A unique hash for identifying a license entry in the device. This helps to traverse through the entries with same package name and LID.	varchar	24
PACKAGE_NAME	Name of the license package. Package defines the features enabled by the license. Example:SW-NI-CES-2024-L3U	varchar	64
LICENSE_ID	License ID of the chassis or the line module for which, this entry displays license information.Example: fJucJFgFHG	varchar	24
LICENSE_TYPE	The type of the license, which can be either normal or trial. Values are: permanent(1), trial(2).The default value is 1.	smallint	
EXPIRY_DATE	Expiry Date of the trial license. For normal license, the value is 0.	varchar	19

TABLE 345 IP_DEVICE_LICENSE (Continued)

Field	Definition	Format	Size
PRECEDENCE	Defines the priority of a particular trial license among those having the same package and License ID. This is primarily used for determining which license to use, when there are many trial and normal licenses with same package name and LID. The value range is (0..65535)	int	
LICENSE_STATE	This indicates the state of the license. Possible values:invalid(1),unused(2),active(3),expired(4)	smallint	

TABLE 346 VIP_SERVER_BINDING

Field	Definition	Format	Size
ID	Primary Key field for the VIP_SERVER_BINDING	int	
DEVICE_ID	This is the foreign key reference key to the Device Table	int	
VIRTUAL_SERVER_IP_ADDRESS	The IP Address for the Virtual Server	varchar	128
VIRUTAL_SERVER_PORT	The Port number of the Virtual Server	int	
REAL_SERVER_IP_ADDRESS	The IP Address for the Real Server	varchar	128
REAL_SERVER_PORT	The Port Number for the Real Server	int	

TABLE 347 VIP_SERVER

Field	Definition	Format	Size
ID	Primary Key field for the VIP_SERVER	int	
TYPE	Even Policy Type 0? Virtual Server 1 ? Real Server	smallint	
DEVICE_ID	This is the foreign key reference key to the Device Table	int	
IP_ADDRESS	The IP Address for the Virtual Server or Real Server	varchar	128
NAME	The Name of Virtual Server or Real Server	varchar	256

TABLE 348 ZONE_TRANSACTION

Field	Definition	Format	Size
FABRIC_ID	The id of the fabric on which the zoning transaction is open. This is the primary key for this table and is a foreign key from the FABRIC table where ZONE_TR.FABRIC_ID == FABRIC.ID	int	
USER_NAME	The Management applciation username of the cimclient who has opened the zoning transaction on the fabric. This is a valid Management applciation username in the Management applciation db	varchar	128
LAST_TIME_USED	The last time this transaction was used for	timestamp	

TABLE 349 ZONE_IN_ZONE_SET

Field	Definition	Format	Size
ZONE_SET_ID	PK of the owning zone set	int	
ZONE_ID	PK of the owning zone	int	

TABLE 350 ZONE_DB_CONFIG

Field	Definition	Format	Size
ID		int	
ZONE_DB_ID	PK of the owning zone DB	int	
DEFINED_CONTENT	defined zone raw config string, wrapped with $ to prevent special char trimming	text	
ACTIVE_CONTENT	active zone raw config string	text	
TI_ZONE_CONTENT	ti zone raw config string	text	

TABLE 351 WT_ARCHIVE

Field	Definition	Format	Size
FIRMWARE_VERSION	Firmware version for which jar files are downloaded	varchar	128
JAR_LIST	List of jar files as comma separated string	varchar	256

TABLE 352 V_PORT_DETAIL

Field	Definition	Format	Size
DEVICE_PORT_ID	Primary key from the owner device port table.	int	
STATE	Flag to indicate whether port is online or offline	varchar	32
FCP_INITIATOR	The role of the virtual port; for example, FCP Initiator	varchar	256
SWITCH_IP	IP of the switch, the V port is connected to	varchar	128
VF_ID	VF ID for the V port	smallint	

TABLE 353 V_CENTER_HOST

Field	Definition	Format	Size
ID		int	
HOST	The FQDN or the ip address of the host	varchar	256
PORT	The port of the VCENTER server on the host. The default value is 443 .	int	
USER_NAME	The username to login into the VCENTER	varchar	64
PASSWORD	The password to login into the VCENTER	varchar	64
VERSION	The version of VCENTER. The default value is 4.0 .	varchar	10
TOKEN_ID	The id to map the each VCENTER on the host	varchar	64
STATUS	Status of Plug-in registration to the vCenter server. The default value is 'REGISTERED'.	varchar	32

TABLE 354 VIRTUAL_FCOE_PORT

Field	Definition	Format	Size
ID		int	
VIRTUAL_SWITCH_ID	The unique id of switch the virtual fcoe port belongs to.	int	
PORT_WWN	WWN of port	varchar	64
PORT_SPEED	Will be 10G.	varchar	32
PORT_TYPE	Will be Virtual-FCoE-Port	varchar	16
ENABLED	Enabled/disabled	smallint	
STATUS	Status	varchar	64
TRUNK_INDEX	Trunk index	smallint	
PORT_NUMBER	Port number	smallint	
NAME	Name	varchar	64
SLOT_NUMBER	The Slot number in the switch to which this Virtual FCoE Port belongs	int	
VLAN_ID	Comma Separated values of the VLANs associated with this Virtual FCoE Port	varchar	64
DEVICE_COUNT	The number of devices associated with this Virtual FCoE Port. The default value is 0.	smallint	
PEER_MAC	The Peer FCF MAC if this Virtual FCoE Port is a FCoE VE-port	varchar	

TABLE 355 VIRTUAL_FCOE_PORT_MAC_MEMBER

Field	Definition	Format	Size
VIRTUAL_FCOE_PORT_ID	The unique id of virtual fcoe port the member belongs to	int	
MAC_ADDRESS	Mac address of member.	varchar	64

TABLE 356 VIRTUAL_FCOE_PORT_STAT

Field	Definition	Format	Size
ID		int	
SWITCH_ID		int	
PORT_ID		int	
TX	The number of valid frames sent from the port	double precision	
RX	The number of valid frames received at this port	double precision	
TX_UTILIZATION	The computed value of TX based on speed of port (for MarchingAnts)	double precision	
RX_UTILIZATION	The computed value of RX based on speed of port (for MarchingAnts)	double precision	
CREATION_TIME	The time this stats record was created	timestamp	
ACTIVE_STATE	Used for error scenario	smallint	
LINK_FAILURES	Link failures	double precision	
TX_LINK_RESETS	TX Link resets	double precision	
RX_LINK_RESETS	RX link resets	double precision	
SYNC_LOSSES	Synchronization losses	double precision	
SIGNAL_LOSSES	Signal losses	double precision	
SEQUENCE_ERRORS	Sequence Errors	double precision	
INVALID_TX	Invalid transmissions	double precision	
CRC_ERRORS	Cyclic Redundancy check error	double precision	

TABLE 357 VIRTUAL_FCOE_PORT_STAT_1DAY

Field	Definition	Format	Size
ID		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	

TABLE 357 VIRTUAL_FCOE_PORT_STAT_1DAY (Continued)

Field	Definition	Format	Size
RX_UTILIZATION		double precision	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
LINK_FAILURES		double precision	
TX_LINK_RESETS		double precision	
RX_LINK_RESETS		double precision	
SYNC_LOSSES		double precision	
SIGNAL_LOSSES		double precision	
SEQUENCE_ERRORS		double precision	
INVALID_TX		double precision	
CRC_ERRORS		double precision	
DATA_GAPS_5MIN		smallint	
DATA_GAPS_30MIN	Data gap in 2 hours table	smallint	
DATA_GAPS_30MIN2		smallint	

TABLE 358 VIRTUAL_FCOE_PORT_STAT_2HR

Field	Definition	Format	Size
ID		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	

TABLE 358 VIRTUAL_FCOE_PORT_STAT_2HR (Continued)

Field	Definition	Format	Size
CREATION_TIME		double precision	
ACTIVE_STATE		timestamp	
LINK_FAILURES		double precision	
TX_LINK_RESETS		double precision	
RX_LINK_RESETS		double precision	
SYNC_LOSSES		double precision	
SIGNAL_LOSSES		double precision	
SEQUENCE_ERRORS		double precision	
INVALID_TX		double precision	
CRC_ERRORS		double precision	
DATA_GAPS_5MIN		smallint	
DATA_GAPS_30MIN	Data gap in 30 minutes table	smallint	

TABLE 359 VIRTUAL_FCOE_PORT_STAT_30M

Field	Definition	Format	Size
ID		int	
SWITCH_ID		int	
PORT_ID		int	
TX		double precision	
RX		double precision	
TX_UTILIZATION		double precision	
RX_UTILIZATION		double precision	
CREATION_TIME		smallint	
ACTIVE_STATE		double precision	
LINK_FAILURES		double precision	

TABLE 359 VIRTUAL_FCOE_PORT_STAT_30M (Continued)

Field	Definition	Format	Size
TX_LINK_RESETS		double precision	
RX_LINK_RESETS		double precision	
SYNC_LOSSES		double precision	
SIGNAL_LOSSES		double precision	
SEQUENCE_ERRORS		double precision	
INVALID_TX		double precision	
CRC_ERRORS		double precision	
DATA_GAPS_5MIN	Data gap in 5 minutes table	smallint	

TABLE 360 VIRTUAL_MACHINE

Field	Definition	Format	Size
ID	Uniquely identifies the virtual machine.	int	
HOST_ID	Identifies the server that contains this VM.	int	
HYPERVISOR_VM_ID	The VM number assigned by the hypervisor. Some hypervisors identify VMs by number as well as by name. The default value is 0.	int	
NAME	User-assigned name for the VM	varchar	80
DESCRIPTION	Optional user-entered notes describing the VM. (Annotation in VMware terminology.)	varchar	256
OS	Operating system name and version	varchar	64
STATUS	VM status. 0 = stopped, 1 = running, 2 = suspended. The default value is 0.	smallint	
VCPU_COUNT	Number of virtual CPUs used by the VM. The default value is 0.	int	
CPU_RESOURCES	Summary of CPU resource configuration. Format may depend on VM vendor	varchar	64
MEM_RESOURCES	Summary of memory resource configuration. Format may depend on VM vendor.	varchar	64
IP_ADDRESS	The primary IPv4 or IPv6 IP address used by the VM on the management LAN, if any. Primary is defined by the VM vendor	varchar	32
HOSTNAME	The primary hostname assigned to this VM	varchar	128
BOOT_TIME	The date and time the VM was last started.	timestamp	64

TABLE 360 VIRTUAL_MACHINE (Continued)

Field	Definition	Format	Size
DATASTORE_NAME	The user-assigned name for the VMs datastore. The datastore holds the VMs virtual disks, swap file, and configuration data	varchar	
DATASTORE_LOCATION	The location of the VMs datastore May be a SAN target disk or a locally-attached host disk folder. For VMware, this is a target LUN name.	varchar	
NODE_WWN	The Node WWN for this VM. If NPIV is not being used, this will be the same as the Node WWN in the host''s DEVICE_ENCLOSURE record. If NPIV is being used, each VM has a unique Node WWN.	char	23
UUID		varchar	64

TABLE 361 USER_STATE_MAP

Field	Definition	Format	Size
USER_NAME		varchar	128
STATE	Current user state. The possible values are: 0: Locked out by user manager 1: Locked Out Threshold Reached 2: Password Expired 3: Password History Policy Violated 4: Password Format Policy Violated Note: This numeric state value will be mapped to associated ENUM at DTO side	smallint	

TABLE 362 USER_AOR_MAP

Field	Definition	Format	Size
USER_NAME		varchar	128
AOR_ID	AOR ID where user has membership.	smallint	

TABLE 363 USER_DEFINED_DEVICE_DETAIL

Field	Definition	Format	Size
WWN		char	23
NAME		varchar	256
TYPE		varchar	32
IP_ADDRESS		varchar	63
CONTACT		varchar	256
LOCATION		varchar	256
DESCRIPTION		varchar	256

TABLE 363 USER_DEFINED_DEVICE_DETAIL (Continued)

Field	Definition	Format	Size
USER_DEFINED_VALUE1		varchar	256
USER_DEFINED_VALUE2		varchar	256
USER_DEFINED_VALUE3		varchar	256

TABLE 364 SWITCH_BOTTLENECK_CONFIG

Field	Definition	Format	Size
VIRTUAL_SWITCH_ID	The database ID of the switch that the configuration belongs to	int	
BOTTLENECK_DETECT_ENABLED s	'Flag indicates if bottleneck detection is enabled or not. The default value is 0.	smallint	
ALERTS_ENABLED	Flag indicates if bottleneck detection alerts is enabled or not. The default value is 0.	smallint	
CONGESTION_THRESHOLD	Value of bottleneck detection congestion threshold in percent. The default value is ‘9 0’.	double precision	
LATENCY_THRESHOLD	Value of bottleneck detection latency threshold in percent. The default value is ‘1 0’.	double precision	
WINDOW_	Value of bottleneck detection latency window in millisecond. The default value is 3 0 0.	int	
QUIET_TIME	Value of bottleneck detection quiet time in millisecond. The default value is 3 0 0.	int	
CREATION_TIME	Creation time of the record	timestamp	
LAST_UPDATE_TIME	Last update time of the record	timestamp	

TABLE 365 SWITCH_PORT_PERFORMANCE

Field	Definition	Format	Size
PORT_ID	Primary key of the Switch Port.	int	
SWITCH_ID	Primary key of Virtual Switch which this port is present	int	
TX	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	double precision	
RX	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	double precision	
TX_UTILIZATION	The computed value of TX based on speed of port	double precision	

TABLE 365 SWITCH_PORT_PERFORMANCE (Continued)

Field	Definition	Format	Size
RX_UTILIZATION	'The computed value of RX based on speed of port	double precision	
LINK_FAILURE	Count of link failures. This count is part of the Link Error Status Block (LESB). (FC-PH 29.8). Note, this is a Fibre Channel only stat	double precision	
TX_LINK_RESETS	Count of Link resets. This is the number of LRs received. Note, this is a Fibre Channel only stat	double precision	
RX_LINK_RESETS	Count of Link resets. This is the number LRs transmitted. Note, this is a Fibre Channel only stat	double precision	
SYNC_LOSSES	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.	double precision	
SIGNAL_LOSSES	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	double precision	
SEQUENCE_ERRORS	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	double precision	
INVALID_TRANSMISSIONS	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	double precision	
CRC_ERRORS	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.'	double precision	
LAST_UPDATE_TIME	Time when this stats record was updated	timestamp	

TABLE 366 SWITCH_TE_PORT_PERFORMANCE

Field	Definition	Format	Size
PORT_ID	Primary key of the Switch Port	int	
SWITCH_ID	Primary key of Virtual Switch which this port is present	int	
TX	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.	double precision	

TABLE 366 SWITCH_TE_PORT_PERFORMANCE (Continued)

Field	Definition	Format	Size
RX	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	double precision	
TX_UTILIZATION	The computed value of TX based on speed of port	double precision	
RX_UTILIZATION	The computed value of RX based on speed of port	double precision	
RX_EOF	Total number of frames received at this port	double precision	
UNDERFLOW_ERROR	The total number of packets received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.	double precision	
OVERFLOW_ERRORS	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed	double precision	
CRC_ERRORS	The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)	double precision	
ALIGNMENT_ERRORS	'The number of frames detected that contain partial octets and don''t pass the FCS check.	double precision	
RUN_TIME_ERRORS	The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets) and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).	double precision	
EXCESS_COLL_ERRORS	Increments when the port unsuccessfully transmits a packet 16 consecutive times	double precision	
EXCESS_FCTRL_ERRORS	Increments when the port applies flow control 16 consecutive times	double precision	
LOST_FCTRL_ERRORS	The number of packets lost (if flow control is diabled) or number of packets retransmitted by the originator due to flow control (if flow control is enabled)	double precision	
TOO_LONG_ERRORS	The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error)	double precision	
LAST_UPDATE__TIME	Time when this stats record was updated	timestamp	

TABLE 367 SWITCH_TE_PORT_STATS

Field	Definition	Format	Size
ID		int	
SWITCH_ID	The primary key of the switch	int	
PORT_ID	The primary key of the port	int	
TRANSMIT_OK	'The number of valid frames sent from the port	double precision	
RECEIVE_OK	The number of valid frames received at this port.	double precision	
TRANSMIT_OK_PERCENT_UTIL	The computed value of transmit_ok based on speed of port (for MarchingAnts)	double precision	
RECEIVE_OK_PERCENT_UTIL	The computed value of receive_ok based on speed of port (for MarchingAnts)	double precision	
CREATION_TIME	The time this stats record was created.	timestamp	
ACTIVE_STATE	Used for error scenario	smallint	
RECEIVE_EOF	Total number of frames received at this port	double precision	
UNDERFLOW_ERRORS	Internal error. A normal ratio of this counter to the Transmit OK counter is 1% or less.	double precision	
OVERFLOW_ERRORS	Internal error. A normal ratio of this counter to the Transmit OK counter is 1% or less.	double precision	
CRC_ERRORS	The number of packets received that had a length (excluding framing bits,but including FCS octets) of between 64 and 1518 octets and had a bad Frame-Check Sequence (FCS) with either an FCS Error or an Alignment Error.	double precision	
ALIGNMENT_ERRORS	The number of frames detected that contain partial octets and don''t pass the FCS check	double precision	
RUNT_ERRORS	The number of frames detected that are less than the minimum permitted frame size and have a good FCS	double precision	
EXCESS_COLL_ERRORS	Increments when the port unsuccessfully transmits a packet 16 consecutive times	double precision	
EXCESS_FCTRL_ERRORS	Increments when the port applies flow control 16 consecutive times.	double precision	
LOST_FCTRL_ERRORS	The number of packets lost (if flow control is disabled) or number of packets retransmitted by the originator due to flow control (if flow control is enabled)	double precision	
TOO_LONG_ERRORS	The number of frames detected that exceed the maximum permitted frame size.	double precision	

TABLE 368 SWITCH_TE_PORT_STATS_1DAY

Field	Definition	Format	Size
ID		int	
SWITCH_ID		int	
PORT_ID		int	
TRANSMIT_OK		double precision	
RECEIVE_OK		double precision	
TRANSMIT_OK_PERCENT_UTIL		double precision	
RECEIVE_OK_PERCENT_UTIL		double precision	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
RECEIVE_EOF		double precision	
UNDERFLOW_ERRORS		double precision	
OVERFLOW_ERRORS		double precision	
CRC_ERRORS		double precision	
ALIGNMENT_ERRORS		double precision	
RUNT_ERRORS		double precision	
EXCESS_COLL_ERRORS		double precision	
EXCESS_FCTRL_ERRORS		double precision	
LOST_FCTRL_ERRORS		double precision	
TOO_LONG_ERRORS		double precision	
DATA_GAPS_IN_5MIN		smallint	
DATA_GAPS_IN_30MIN		smallint	
DATA_GAPS_IN_2HR		smallint	

TABLE 369 SWITCH_TE_PORT_STATS_2HR

Field	Definition	Format	Size
ID		int	
SWITCH_ID		int	
PORT_ID		int	
TRANSMIT_OK		double precision	
RECEIVE_OK		double precision	
TRANSMIT_OK_PERCENT_UTIL		double precision	
RECEIVE_OK_PERCENT_UTIL		double precision	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
RECEIVE_EOF		double precision	
UNDERFLOW_ERRORS		double precision	
OVERFLOW_ERRORS		double precision	
CRC_ERRORS		double precision	
ALIGNMENT_ERRORS		double precision	
RUNT_ERRORS		double precision	
EXCESS_COLL_ERRORS		double precision	
EXCESS_FCTRL_ERRORS		double precision	
LOST_FCTRL_ERRORS		double precision	
TOO_LONG_ERRORS		double precision	
DATA_GAPS_IN_5MIN		smallint	
DATA_GAPS_IN_30MIN		smallint	

TABLE 370 SWITCH_TE_PORT_STATS_30MIN

Field	Definition	Format	Size
ID		int	
SWITCH_ID		int	

TABLE 370 SWITCH_TE_PORT_STATS_30MIN (Continued)

Field	Definition	Format	Size
PORT_ID		int	
TRANSMIT_OK		double precision	
RECEIVE_OK		double precision	
TRANSMIT_OK_PERCENT_UTIL		double precision	
RECEIVE_OK_PERCENT_UTIL		double precision	
CREATION_TIME		timestamp	
ACTIVE_STATE		smallint	
RECEIVE_EOF		double precision	
UNDERFLOW_ERRORS		double precision	
OVERFLOW_ERRORS		double precision	
CRC_ERRORS		double precision	
ALIGNMENT_ERRORS		double precision	
RUNT_ERRORS		double precision	
EXCESS_COLL_ERRORS		double precision	
EXCESS_FCTRL_ERRORS		double precision	
LOST_FCTRL_ERRORS		double precision	
TOO_LONG_ERRORS		double precision	
DATA_GAPS_IN_5MIN		smallint	

TABLE 371 SYSTEM_CARD_ENGINE_MAPPING

Field	Definition	Format	Size
ID		int	
ENCRYPTION_ENGINE_ID	Foreign key reference to the ENCRYPTION_ENGINE for which a system card is registered	int	
SMART_CARD_ID	Foreign key reference to the SMART_CARD that is registered as a system card for the encryption engine.	int	

TABLE 372 TOPO_MAP_IMAGE

Field	Definition	Format	Size
ID		int	
NAME	Image name in the foo.png format	varchar	256
IMAGE_OBJECT	'Image Object BLOB	bytea	

TABLE 373 SMART_CARD

Field	Definition	Format	Size
ID		int	
CARD_TYPE	Indicates how this smart card is configured: 0 = authorization card. The default value is 0.	smallint	
CARD_INFO	Additional smart card details. For recovery set cards, the details include the recovery set size and the card''s position within the set; e.g., 2 of 5	varchar	64
CARDCN_ID	A unique name for the card, derived from the card''s serial number and usage	varchar	64
FIRST_NAME	Optional first name of the person responsible for this card.	varchar	64
LAST_NAME	Optional last name of the person responsible for this card	varchar	64
NOTES	User-supplied notes about the card.	varchar	256
PUBLIC_CERTIFICATE	The public key certificate of the card, in PEM format. Used to validate the card and set up a secure communications channel to the card.	varchar	4096
CERTIFICATE_LABEL	User-supplied name for the card''s public key certificate	varchar	256
GROUP_NAME	The name of the Encryption Group used to initialize the card. For recovery set cards, this identifies which group''s master key is backed up on the card.	varchar	64
CREATION_TIME	The date and time that the card was initialized. For recovery set cards, this is the date and time the master key was written to the card. The default value is 'now()'.	timestamp	

TABLE 374 SNMP_DATA_1DAY

Field	Definition	Format	Size
ID		int	
MIB_OBJECT_ID		int	
TARGET_TYP		numeric	(2,0)
TARGET_ID		int	

TABLE 374 SNMP_DATA_1DAY (Continued)

Field	Definition	Format	Size
VALUE		double precision	
TIME_IN_SECONDS		int	
COLLECTOR_ID		int	
MIB_INDEX		char	256

TABLE 375 SNMP_DATA_2HOUR

Field	Definition	Format	Size
ID		int	
MIB_OBJECT_ID		int	
TARGET_TYPE		numeric	(2,0)
TARGET_ID		int	
VALUE		double precision	
TIME_IN_SECONDS		int	
COLLECTOR_ID		int	
MIB_INDEX		char	256

TABLE 376 SNMP_DATA_30MIN

Field	Definition	Format	Size
ID	Primary key autogenerated ID	int	
MIB_OBJECT_ID	MIB OID used for collection	int	
TARGET_TYPE	Target/Source type can be device:0 or interface/ports:1	numeric	(2,0)
TARGET_ID	DB Id of the target which can be device or interface	int	
VALUE	Value collected by the engine	double precision	
TIME_IN_SECONDS	Time at which collection occured in seconds	int	
COLLECTOR_ID	DB Id of the collector object used for collection	int	
MIB_INDEX	MIB index used for collection if applicable	char	256

TABLE 377 SNMP_EXPR_DATA_1DAY

Field	Definition	Format	Size
ID		int	
EXPRESSION_ID		int	
TARGET_TYPE		smallint	
TARGET_ID		int	
VALUE		double precision	

TABLE 377 SNMP_EXPR_DATA_1DAY (Continued)

Field	Definition	Format	Size
TIME_IN_SECONDS		int	
COLLECTOR_ID		int	

TABLE 378 SNMP_EXPR_DATA_2HOUR

Field	Definition	Format	Size
ID		int	
EXPRESSION_ID		int	
TARGET_TYPE		smallint	
TARGET_ID		int	
VALUE		double precision	
TIME_IN_SECONDS		int	
COLLECTOR_ID		int	

TABLE 379 SNMP_EXPR_DATA_30MIN

Field	Definition	Format	Size
ID	Primary key autogenerated ID	int	
EXPRESSION_ID	DB ID of the expression object used for collection	int	
TARGET_TYPE	Target/Source type can be device:0 or interface/ports:1'	smallint	
TARGET_ID	DB Id of the target which can be device or interface	int	
VALUE	Value collected by the engine'	double precision	
TIME_IN_SECONDS	Time at which collection occured in seconds	int	
COLLECTOR_ID	DB Id of the collector object used for collection	int	

TABLE 380 SNMP_TRAP_CREDENTIAL

Field	Definition	Format	Size
ID	PK for the table to uniquely identify the record	int	
VERSION	to identify the version of Credentials: v1v2c and v3 are the values	varchar	6
COMMUNITY_STRING	to decode the v1/v2c traps	varchar	64
USER_NAME	user access name for v3 trap	varchar	64
AUTH_PROTOCOL	authentication protocol used for v3 traps	varchar	16
AUTH_PASSWORD	authentication password for v3 traps	varchar	64
PRIV_PROTOCOL	privacy protocol used for v3 traps	varchar	16
PRIV_PASSWORD		varchar	64
POSITION_	order of credentials to authenticate v1/v2c or v3 traps	int	

TABLE 381 SENSOR

Field	Definition	Format	Size
ID		int	
CORE_SWITCH_ID		int	
SENSOR_ID	Identifies the sensor device , requested by SMIA and values filled in by Switch Asset Collector. Maps to Device Id in the html page. The default value is -1.	int	
CURRENT_READING	Identifies the current temperature reading sensor, requested by SMIA and values filled in by Switch Asset Collector, Maps to value field in the html page. The default value is -1.	bigint	
TYPE	The default value is -1.	int	
SUB_TYPE	The default value is -1.	int	
DESCRIPTION	Provides the description of the temperature sensor, requested by SMIA and values filled in by Switch Asset Collector	varchar	128
STATUS	provides the status of the sensor, requested by SMIA and values filled in by Switch Asset Collector,Values could be 0 or 1. 0 means faulty and 1 is ok.The default value is -1.	int	
OPERATIONAL_STATUS	provides the operational status of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. The default value is -1.	int	
PART_NUMBER	provides the part number of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above	varchar	64
SERIAL_NUMBER	provides the serial number of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above	varchar	64
VERSION	provides the version of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above	varchar	32
CREATION_TIME	provides the record creation time, standard columns for Management applciation and values filled in by Switch Asset Collector	timestamp	
LAST_UPDATE_TIME	provides the record last updated time, standard columns for Management applciation and values filled in by Switch Asset Collector	timestamp	
FRU_TYPE	provides the type of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. The values represents FAN,PS, SLOT etc. The default value is -1.	int	

TABLE 381 SENSOR (Continued)

Field	Definition	Format	Size
UNIT_NUMBER	provides the unit number of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above . This the gives the index of the unit. For SLOT FRU, this will be slot number. For FAN fru, this will be fan number. The default value is -1.	int	
STATE	provides the state of the sensor, requested by SMIA and values filled in by Switch Asset Collector will be available only from FOS 6.4 switches and above. This gives the value whether the FRU is On or Off . The default value is -1.	int	

TABLE 382 SCOM_HOST

Field	Definition	Format	Size
ID		int	
HOST	The FQDN or the ip address of the host	varchar	256
DOMAIN	The domain of the SCOM server host	varchar	256
USER_NAME	The domain user to login into the SCOM Server	varchar	64
PASSWORD	The password to login into the SCOM Server	varchar	64
VERSION	The version of SCOM. Default is 6.1.7221.0 which is SCOM 2007 R2. The default value is '6.1.7221.0' .	varchar	32
TOKEN_ID	Unique ID for each SCOM host	varchar	32
STATUS	Status of Plug-in registration to the SCOM server where 0-registered, 1-unregistered, 2-authentication failed, 3-not reachable	int	

TABLE 383 HOST_DISCOVERY_OPTION

Field	Definition	Format	Size
ID	Auto generated primary key	int	
DISCOVER_JSON	Flag to indicate JSON agent based discovery. The default value is 1.	smallint	
JSON_USERNAME	Username for the JSON agent	varchar	128
JSON_PASSWD	Password for the JSON agent	varchar	512
DISCOVER_CIM	Flag to indicate CIM based discovery. on/off. The default value is 0.	smallint	
CIM_IMPL	CIM implemenation used. 1: SMI, 2: WMI. The default value is 0.	smallint	
CIM_USERNAME	Username for the CIM based agent	varchar	128
CIM_PASSWORD	Password for the CIM based agent'	varchar	512

TABLE 383 HOST_DISCOVERY_OPTION (Continued)

Field	Definition	Format	Size
CIM_NAMESPACE	CIM Namespace. The default value is 'root/brocade	varchar	128
CIM_PORT	Port number used for the CIM agent. The default value is 5988.	int	
DISCOVER_VM	Flag to indicate VM discovery for a host. On/Off'. The default value is 0.	smallint	
VM_USERNAME	Username to be used for VM discovery	varchar	128
VM_PASSWORD	Password to be used for VM discovery	varchar	512
JSON_PORT	Port Number used for the Json agent. The default value is 34568.	int	
VM_PORT	Port Number used for the VM agent. The default value is 443.	int	
*Application_Name*_USER_NAME	Management applciation User Name of the user who generated the last operation on the request	varchar	255
*Application_Name*_SERVER_ADDRESS	Management applciation Server address which generated the last operation on this request	varchar	50

TABLE 384 HBA_TARGET

Field	Definition	Format	size
DEVICE_PORT_ID	Primary key from the Device port table	int	
HBA_REMOTE_PORT_LUN_ID	Primary key from the HBA Remote port lun table	int	
BOOT_LUN	Flag to indicate of the LUN is bootable. The default value is -1.	smallint	
TRUSTED	The default value is 1.	smallint	
CREATION_TIME	Creation time of the entry	timestamp	
MISSING	Flag to indicate if the remote LUN is missing. The default value is 0.	smallint	
MISSING_TIME	Time at which the LUN is marked missing.	timestamp	
TARGET_ID	The identifier of the target device as reported by each HBA port. The default value is 0.	int	

TABLE 385 HBA_REMOTE_PORT_LUN

Field	Definition	Format	size
ID	Auto generated primary key	int	
HBA_REMOTE_PORT_ID	Primary key of owner row in Remote Port	int	
FCP_LUN	The logical unit number of Fibre Channel Protocol (FCP) device. The default value is 0.	varchar	16
CAPACITY	The capacity of the logical unit. The default value is 0.	int	

TABLE 385 HBA_REMOTE_PORT_LUN (Continued)

Field	Definition	Format	size
BLOCK_SIZE	The block size of the logical unit, in bytes (for example, 512 Bytes). The default value is 0.	int	
VENDOR	The vendor of the device to which the logical unit is assigned	varchar	256
PRODUCT_ID	The product identifier of the device to which the logical unit is assigned	varchar	256
PRODUCT_VERSION	The revision level of the device to which the logical unit is assigned.	varchar	256
PRODUCT_SERIAL_NO	The serial number of the device to which the logical unit is assigned	varchar	256
TARGET_WWN	The world wide name of the target devic	char	23
PHYSICAL_LUN	'If there is a lun connected to a remote port, then it represents a value 1 indicating it is a physical lun otherwise it is a dummy lun with value 0. The default value is 1.	smallint	
LUN_ID	IS lun id	varchar	32

TABLE 386 HBA_REMOTE_PORT

Field	Definition	Format	Size
ID	Autogenerate primary column	int	
SYMBOLIC_NAME		varchar	256
PORT_WWN	The world wide name of the remote device''s port.	char	23
NODE_WWN	The world wide name of the remote device	char	23
NAME	The name associated with the device	varchar	256
FC_ADDRESS	FC Address for the port in hex	varchar	6
FRAME_DATA_SIZE	The frame size, in bytes, of the device. The default value is 512.	int	
SPEED	The default value is 0.	int	
STATE	Indicates whether the device is online or offline. The default value is ‘Offline’.	varchar	64
SUPPORTED_COS		varchar	32
DEVICE_TYPE	The type of the device; for example, Disk or Tape.	varchar	64
BIND_TYPE	The persistent bind type. The default value is 0.	smallint	
TARGET_ID	The identifier of the target device. The default value is 0.	int	
ROLE	The role of the device (target or initiator)	varchar	64
VENDOR	The vendor of the device	varchar	256
PRODUCT_ID	The device''s identifier.	varchar	256
PRODUCT_VERSION	Field which stores information regarging target rate limiting on the remote port	varchar	256

TABLE 386 HBA_REMOTE_PORT (Continued)

Field	Definition	Format	Size
QOS_PRIORITY	QOS Priority on the target. The default value is 'Unknown'.	varchar	64
QOS_FLOW_ID	QOS Flow ID on the target. The default value is 0.	varchar	64
CURRENT_SPEED	Current speed of the remote port, as enforced by TRL. The default value is 0.	varchar	64
TRL_ENFORCED	The default value is 0.	varchar	16
BUS_NO	Channel number in the PCI Bus. The default value is 0.	varchar	32
FCP_IM_STATE	Indicates whether the Fibre Channel Protocol Input Method (FCP-IM) is online or offline.	varchar	128
IO_LATENCY_MIN	Minimum IO Latency value (< 79) in milliseconds and is calculated when HBA port starts SCSI (FCP) exchanges	varchar	32
IO_LATENCY_MAX	IO Latency value in milliseconds and is calculated when HBA port starts SCSI (FCP) exchanges	varchar	32
IO_LATENCY_AVERAGE	Average IO Latency value in milliseconds and is calculated when HBA port starts SCSI (FCP) exchanges	varchar	32
DATA_RETRANSMISSION_SUPPORT	Field to indicate whether the remote port supports data retransmission.0 would mean unsupported and nonzero value implies supported. The default value is 0.	smallint	
REC_SUPPORT	Field to indicate whether the remote port supports the REC ELS command Channel number in the PCI Bus.Zero would mean unsupported and nonzero value implies supported. The default value is 0.	smallint	
TASK_RENTRY_IDENT_SUPPORT	The number of PRLI responses from the target to the initiator and begins when HBA Port starts FCP exchanges.Zero would mean unsupported and nonzero value implies supported. The default value is 0.	int	
CONFIRMED_COMPLETIONS_SUPPORT	The number of confirmed completions on the remote port and begins when HBA Port starts FCP exchanges.Zero would mean unsupported and nonzero value implies supported. The default value is 0.	int	

TABLE 387 HBA_PORT

Field	Definition	Format	Size
DEVICE_PORT_ID	Primary key on the owner Device port table	int	
CONFIGURED_STATE	Indicates whether the port is enabled or disabled. The default value is 0.	smallint	
CONFIGURED_SPEED	The configured speed of the port. E.g. Auto-negotiate	varchar	64

TABLE 387 HBA_PORT (Continued)

Field	Definition	Format	Size
CONFIGURED_TOPOLOGY	The topology setting. The default value is 1.	int	
MAX_SPEED_SUPPORTED	The maximum port speed that is supported on the port, in Gb/s. The default value is 0.	int	
OPERATING_STATE	Indicates whether the link is online or offline. The default value is 0.	smallint	
OPERATING_TOPOLOGY	The topology setting at which the port is operating. The default value is 1.	int	
SUPPORTED_FC4_TYPES		varchar	32
SUPPORTED_COS		varchar	32
TRUSTED	The default value is 1.	smallint	
CREATION_TIME	The default value is ‘ now() ‘.	timestamp	
MISSING	The default value is 0.	smallint	
MISSING_TIME		timestamp	
OPERATING_SPEED	Operating speed of the hba port. The default value is 0.	varchar	64
CNA_PORT_ID	Nullable foreign key, related FC pot with the CNA port	int	
PORT_NWWN	Node WWN for the HBA port	varchar	23
PHYSICAL_PORT_WWN	Physical Ports WWN in case of V port	varchar	128
SWITCH_IP	IP of the switch, HBA port is connected to	varchar	23
PRINCIPAL_SWITCH_WWN	WWN of the principal switch of the fabric, HBA is connected to	varchar	128
HBA_ID	HBA ID of the HBA this port belongs to	int	
PORT_NUMBER	The default value is -1.	smallint	
NAME	Name defined for the HBA port in HCM	varchar	
FACTORY_PORT_WWN	Factory configured Port WWN defined for the HBA port in HCM	varchar	
FACTORY_NODE_WWN	Factory configured Node WWN defined for the HBA port in HCM	varchar	
PREBOOT_CREATED	Flag to identify vports created during preboot	varchar	

TABLE 388 HBA_PORT_DETAIL

Field	Definition	Format	Size
DEVICE_PORT_ID	Device port id acts as the primary key	int	
PERSISTENT_BINDING	The default value is 0.	smallint	
FABRIC_NAME		varchar	64
BOOT_OVER_SAN	Flag to indicate whether boot over SAN is enabled or not.. The default value is 0.	smallint	
BOOT_OPTION	The default value is 0.	smallint	

TABLE 388 HBA_PORT_DETAIL (Continued)

Field	Definition	Format	Size
BOOT_SPEED	The default value is 0.	int	
BOOT_TOPOLOGY	The default value is 1.	int	
BB_CREDIT	The maximum number of receive buffer. The default value is 8.	int	
FRAME_DATA_FIELD_SIZE	The default value is 512.	int	
HARDWARE_PATH	Indicates whether MPIO is enabled or disabled		
V_PORT_COUNT	Number of logical ports. The default value is 0.	int	
QUEUE_DEPTH	The number of I/O operations that can be run in parallel on a device. The default value is 0.	int	
INTERRUPT_CONTROL_COALESCE	Indicates whether interrupt control is on or off. The default value is 0.	smallint	
INTERRUPT_CONTROL_LATENCY	Sets the interrupt control latency value.. The default value is 0.	int	
INTERRUPT_CONTROL_DELAY	Sets the interrupt control delay value.. The default value is 0.	int	
BEACON_STATE	Indicates whether beaconing is on or off.. The default value is 0.	smallint	
LINK_BEACON_STATE	Indicates whether link beaconing is on or off.. The default value is 0.	smallint	
MPIO_MODE_STATE	Indicates whether multipathing mode is on or off.. The default value is 0.	smallint	
PATH_TIME_OUT	The value between 0 to 60 that specifies the time out session. Note you can only enable or edit the path time out when MPIO is disabled. The default value is 0.	int	
LOGGING_LEVEL	The port logging level. Values include Log Critical, Log Error, Log Warning, and Log Info. The default value is 0.	smallint	
TARGET_RATE_LIMIT	The default value is 0.	smallint	
DEFAULT_RATE_LIMIT	The default value is 0.	int	
VF_MODE	The default value is 0.	smallint	
RECIEVE_BUFFER_CREDIT	The default value is 48.	varchar	64
TRANSMIT_BUFFER_CREDIT	The default value is 8.	varchar	64

TABLE 388 HBA_PORT_DETAIL (Continued)

Field	Definition	Format	Size
FCSP_AUTH_STATE	Indicates whether FC-SP authentication is on or off. The default value is 0.	smallint	
FCSP_STATUS	The status of FC-SP authentication. The default value is 'Disabled'.	varchar	32
FCSP_ALGORITHM	The configured authentication algorithm. The default value is 'MD5'.	varchar	64
FCSP_GROUP	The DH Group (DH Null, group 0 is the only option). The default value is 0.	smallint	
FCSP_ERROR_STATUS	The health status of the Fibre Channel Security Protocol parameters	varchar	256
QOS_CONFIGURED_STATE	Indicates whether QoS is enabled or disabled. The default value is 0.	smallint	
QOS_OPERATING_STATE	QOS Operating state. The default value is 'Disabled'.	varchar	256
QOS_TOTAL_BB_CREDIT	The number of receive buffers. The default value is 2.	varchar	16
QOS_PRIORITY_LEVEL	QoS priority levels. Values include High, Medium, and Low	varchar	32
QOS_HIGH_BW_ALLOCATIO N	Percentage of bandwidth allocation for the High priority level.	varchar	32
QOS_MEDIUM_BW_ALLOCA TION	Percentage of bandwidth allocation for the Medium priority level	varchar	32
QOS_LOW_BW_ALLOCATIO N	Percentage of bandwidth allocation for the Low priority level.	varchar	32
MEDIA	media of port	varchar	64
IOC_ID	IO controller ID	int	
PREBOOT_DISABLED	Boolean value indicating if port was disabled during preboot.. The default value is 0.	smallint	

TABLE 389 HBA_PORT_FCOE_DETAILS

Field	Definition	Format	Size
DEVICE_PORT_ID		int	
BANDWIDTH	The default value is 0.	int	
FIP_STATE		varchar	64
DISCOVERY_PRIORITY		varchar	256
FCF_FCMAP		varchar	256
FCF_FPMA_MAC		varchar	64
FCF_MAC		varchar	64
FCF_MODE		varchar	256
FCF_NAMEID		varchar	256
FCPIM_MPIO_MODE	The default value is 0.	smallint	

TABLE 389 HBA_PORT_FCOE_DETAILS (Continued)

Field	Definition	Format	Size
PORT_LOG_ENABLED	The default value is 0.	smallint	
MAX_FRAME_SIZE	The default value is 512.	int	
MTU	The default value is 0.	int	
PATH_TOV	The default value is 0.	int	
SCSI_QUEUE_DEPTH	The default value is 0.	int	
STATE		varchar	64
SUPPORTED_CLASS		varchar	256
TRL_SPEED	The default value is 0.	int	
TRL_STATE	The default value is 0.	smallint	
PG_ID		varchar	32
PRIORITIES		varchar	128
FCOE_MAC		varchar	64
IOC_ID		int	

TABLE 390 VM_CONNECTIVITY

Field	Definition	Format	Size
ID	The database id of the connectivity data of a host associated to a VCENTER	int	
VCENTER_ID	The VCENTER id	int	
HYPERVISOR_HOST	The hypervisor host managed by the VCENTER id	varchar	256
VM_NAME	The name of the VM	varchar	80
HYPERVISOR_VM_ID	The unique id for the VM allocated by the hypervisor host	int	
PATH_NAME	The name of the VM LUN Path	varchar	128
ADAPTER_PORT_WWN	The wwn of the adapter por	varchar	23
ADAPTER_PORT_STATUS	The operating status of the adapter port'	smallint	
TARGET_PORT_WWN	The wwn of the Target port	varchar	23
LUN_CAN_NAME	The canonical name of the LUN	varchar	128
FS_TYPE	Virtual Machine file system type	varchar	32
ADAPTER_NODE_WWN		char	23
FABRIC_ID		int	
ADAPTER_PORT_TYPE	The type of the port eg. 1 for vport, 0 for physical port. The default value is 0.	int	
STORAGE_VENDOR		varchar	128
STORAGE_MODEL		varchar	128

TABLE 391 VM_HOST

Field	Definition	Format	Size
ID	Identifies a server running a supported hypervisor. The ID value is the same as the ID of the corresponding DEVICE_ENCLOSURE record.	int	
NODE_WWN	The Node WWN for this host.	char	23
HYPERVISOR_NAME	Hypervisor name and version, such as VMware ESX Server v3.5.0	varchar	64
HYPERVISOR_TYPE	Numeric hypervisor type ID. 1 = VMware, 2 = Hyper-V. The default value is 0.	smallint	
CPU_COUNT	Number of CPUs in the server. The default value is 0.	int	
CPU_TYPE	Text summary of CPU hardware, such as: Intel(R) Xeon(TM) CPU 2.6 GHz	varchar	64
CPU_RESOURCES	Text summary of CPU resources, such as "20 GHz total, 15 GHz reserved". May be a different format for different VM vendors	varchar	64
MEM_RESOURCES	Text summary of memory resources, such as "7 GB total, 5 GB reserved". May be a different format for different VM vendors	varchar	64
LICENSE_SERVER	IP address or hostname of VM Hypervisor''s license server.	varchar	128
BOOT_TIME	Date and time that the host was last started	timestamp	

TABLE 392 VM_LUN

Field	Definition	Format	Size
ID	Uniquely identifies this LUN	int	
HOST_ID	Identifies the server that accesses this LUN.	int	
NAME	The VM-assigned device name for this LUN, such as vmhba1:0:0. For VMware, this is the canonical name.'	varchar	512
NODE_WWN	The Node WWN for the storage device (target) that contains this LUN	char	23
VENDOR	Vendor name, such as Seagate.	varchar	64
MODEL	Target model name, such as ST581	varchar	64
SERIAL_NUMBER	The device''s serial number	varchar	64
TYPE	0 = disk, 1 = tape. The default value is 0.	smallint	
CAPACITY	For disks, the disk capacity in GB. The default value is 0.	double precision	
STATUS	The status reported by the host. 0 = offline, 1 = online. The default value is 0.	smallint	

TABLE 392 VM_LUN (Continued)

Field	Definition	Format	Size
PATH_POLICY	Determines how multiple paths to this LUN are used. 0 = fixed, 1 = Most Recently Used, 2 = Round Robin. The default value is 0.	smallint	
UUID	Universal unique ID	varchar	64

TABLE 393 VM_PATH

Field	Definition	Format	Size
ID		int	
HOST_ID	Identifies the host containing this path. This is a foreign key reference to VM_HOST.ID	int	
VM_ID	Identifies the VM using this path to a LUN. If the path is used by the host hypervisor instead of a VM, VM_ID is 0. When non-zero, this value matches VIRTUAL_MACHINE.ID	int	
LUN_ID	Identifies the LUN that is assigned to the VM. Not a foreign key, but the value matches VM_LUN.ID	int	
NAME	The VM-assigned name for this path. For VMware, this is the device name, such as vmhba0:0:1.	varchar	128
FABRIC_ID	Identifies the fabric that contains this path. Not a foreign key reference. Copied here for convenience. Determined by locating the HBA port WWN or target port WWN in the DEVICE_PORT table. Zero if the fabric is not managed. The default value is 0.	int	
HBA_PORT_WWN	The HBAs physical port WWN for this path	char	23
VM_PORT_WWN	The initiator port WWN used by the VM. If NPIV is used, this is a virtual port WWN assigned by the VM to this HBA port. If NPIV is not used, this WWN is the same as the HBA Port WWN	char	23
TARGET_PORT_WWN	The port WWN of the destination target.	char	23
ENABLED	'0 = path disabled, 1 = path enabled. The default value is 0.	smallint	
ACTIVE	0 = path inactive, 1 = path active. The default value is 0.	smallint	
PREFERRED	0 = not preferred, 1 = preferred path. The preferred path is used whenever available when the path policy is Fixed.The default value is 0.	smallint	
USAGE	Identifies how a VMware VM uses this LUN. 0 = NA (used for Hyper-V), 1 = VMFS (datastores), 2 = RDM (Raw Device Mapping). The default value is 0.	smallint	
HBA_NODE_WWN	The HBA physical node WWN for this path	char	23

TABLE 393 VM_PATH (Continued)

Field	Definition	Format	Size
VM_NODE_WWN	The initiator node WWN used by the VM. If NPIV is used, this is a virtual node WWN assigned to the VM. If NPIV is not used, this WWN is the same as the node WWN of one of the HBAs in the host.	char	23
TARGET_NODE_WWN	The node WWN of the destination target	char	23
HBA_NAME	The hypervisor device name of the HBA used in this path, such as vmhba1	varchar	64

Views

BOOT_IMAGE_FILE_DETAILS_INFO

```
create or replace view BOOT_IMAGE_FILE_DETAILS_INFO as
select
    BOOT_IMAGE_FILE_DETAILS.BOOT_IMAGE_NAME,
    BOOT_IMAGE_FILE_DETAILS.MAJOR_VERSION,
    BOOT_IMAGE_FILE_DETAILS.MINOR_VERSION,
    BOOT_IMAGE_FILE_DETAILS.MAINTENANCE,
    BOOT_IMAGE_FILE_DETAILS.PATCH,
    BOOT_IMAGE_FILE_DETAILS.IMPORTED_DATE,
    BOOT_IMAGE_FILE_DETAILS.RELEASE_DATE,
    BOOT_IMAGE_FILE_DETAILS.RELEASE_NOTES_LOCATION,
    BOOT_IMAGE_FILE_DETAILS.LOCATION,
    BOOT_IMAGE_DRIVER_MAP.SUPPORTED_DRIVERS
from
    BOOT_IMAGE_FILE_DETAILS,
    BOOT_IMAGE_DRIVER_MAP
where
    BOOT_IMAGE_FILE_DETAILS.DRIVER_MAPPING_ID= BOOT_IMAGE_DRIVER_MAP.ID;
```

CEE_PORT_INFO

```
create or replace view CEE_PORT_INFO as
select
    GIGE_PORT.ID,
    GIGE_PORT.SWITCH_PORT_ID,
    GIGE_PORT.PORT_NUMBER,
    CEE_PORT.ID AS CEE_PORT_ID,
    CEE_PORT.VIRTUAL_SWITCH_ID,
    CEE_PORT.IF_INDEX,
    CEE_PORT.IF_NAME,
    CEE_PORT.IF_MODE,
    CEE_PORT.L2_MODE,
    CEE_PORT.VLAN_ID,
    CEE_PORT.LAG_ID,
    CEE_PORT.IP_ADDRESS,
    CEE_PORT.MAC_ADDRESS,
    CEE_PORT.PORT_SPEED,
    CEE_PORT.ENABLED,
    CEE_PORT.OCCUPIED,
    CEE_PORT.LAST_UPDATE,
    CEE_PORT.NET_MASK,
    CEE_PORT.PROTOCOL_DOWN_REASON,
    CEE_PORT.MAC_ACL_POLICY,
    CEE_PORT.QOS_TYPE,
    CEE_PORT.QOS_NAME,
    CEE_PORT.DOT1X_ENABLED,
    CORE_SWITCH.IP_ADDRESS as PHYSICAL_SWITCH_IP,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    GIGE_PORT.OPERATIONAL_STATUS,
    GIGE_PORT.MAX_SPEED,
    GIGE_PORT.PORT_TYPE,
    GIGE_PORT.REMOTE_MAC_ADDRESS,
    GIGE_PORT.SLOT_NUMBER,
    VIRTUAL_SWITCH.WWN,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.STATE
from
    CEE_PORT, GIGE_PORT, SWITCH_PORT, VIRTUAL_SWITCH, CORE_SWITCH
where
    CEE_PORT.GIGE_PORT_ID = GIGE_PORT.ID
    and GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID
    and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

CNA_PORT_DETAILS_INFO

```
create or replace view CNA_PORT_DETAILS_INFO as
select
    CNA_PORT.ID,
    CNA_PORT.PORT_NUMBER,
    CNA_PORT.PORT_WWN,
    CNA_PORT.NODE_WWN,
    CNA_PORT.PHYSICAL_PORT_TYPE,
    CNA_PORT.NAME,
    CNA_PORT.MAC_ADDRESS,
    CNA_PORT.MEDIA,
    CNA_PORT.CEE_STATE,
    CNA_PORT.HBA_ID,
    CNA_PORT.CREATION_TIME as CNA_PORT_CREATION_TIME,
    CNA_ETH_PORT.ID as ETH_PORT_ID,
    CNA_ETH_PORT.ETH_DEV,
    CNA_ETH_PORT.ETH_LOG_LEVEL,
    CNA_ETH_PORT.NAME as ETH_PORT_NAME,
    CNA_ETH_PORT.MAC_ADDRESS as ETH_MAC_ADDRESS,
    CNA_ETH_PORT.IOC_ID,
    CNA_ETH_PORT.HARDWARE_PATH,
    CNA_ETH_PORT.STATUS,
    CNA_ETH_PORT.CREATION_TIME as ETH_PORT_CREATION_TIME,
    CNA_ETH_PORT.CURRENT_MAC_ADDRESS as CURRENT_MAC_ADDRESS
from
    CNA_PORT
        left outer join CNA_ETH_PORT on CNA_PORT.ID = CNA_ETH_PORT.CNA_PORT_ID;
```

CNA_PORT_INFO

```
create or replace view CNA_PORT_INFO as
```

```
select
    CNA_PORT.ID,
    CNA_PORT.PORT_NUMBER,
    CNA_PORT.PORT_WWN,
    CNA_PORT.NODE_WWN,
    CNA_PORT.PHYSICAL_PORT_TYPE,
    CNA_PORT.NAME,
    CNA_PORT.MAC_ADDRESS,
    CNA_PORT.MEDIA,
    CNA_PORT.CEE_STATE,
    CNA_PORT.HBA_ID,
    CNA_PORT.CREATION_TIME as CNA_PORT_CREATION_TIME,
    CNA_ETH_PORT.ID as ETH_PORT_ID,
    CNA_ETH_PORT.ETH_DEV,
    CNA_ETH_PORT.ETH_LOG_LEVEL,
    CNA_ETH_PORT.NAME as ETH_PORT_NAME,
    CNA_ETH_PORT.MAC_ADDRESS as ETH_MAC_ADDRESS,
    CNA_ETH_PORT.IOC_ID,
    CNA_ETH_PORT.HARDWARE_PATH,
    CNA_ETH_PORT.STATUS,
    CNA_ETH_PORT.CREATION_TIME as ETH_PORT_CREATION_TIME,
    HBA_PORT.DEVICE_PORT_ID
from
    CNA_PORT
        left outer join HBA_PORT on CNA_PORT.ID = HBA_PORT.CNA_PORT_ID
        left outer join CNA_ETH_PORT on CNA_PORT.ID = CNA_ETH_PORT.CNA_PORT_ID;
```

CORE_SWITCH_DETAILS_INFO

```
create or replace view CORE_SWITCH_DETAILS_INFO as
select
   CORE_SWITCH.ID,
   CORE_SWITCH.IP_ADDRESS,
   CORE_SWITCH.WWN,
   CORE_SWITCH.NAME,
   CORE_SWITCH.TYPE,
   CORE_SWITCH.MODEL,
   CORE_SWITCH.FIRMWARE_VERSION,
   CORE_SWITCH.VENDOR,
   CORE_SWITCH.MAX_VIRTUAL_SWITCHES,
   CORE_SWITCH.NUM_VIRTUAL_SWITCHES,
   CORE_SWITCH.REACHABLE,
   CORE_SWITCH.UNREACHABLE_TIME,
   CORE_SWITCH.OPERATIONAL_STATUS,
   CORE_SWITCH.CREATION_TIME,
   CORE_SWITCH.LAST_SCAN_TIME,
   CORE_SWITCH.LAST_UPDATE_TIME,
   CORE_SWITCH.SYSLOG_REGISTERED,
   CORE_SWITCH.CALL_HOME_ENABLED,
   CORE_SWITCH.SNMP_REGISTERED,
   CORE_SWITCH.USER_IP_ADDRESS,
   CORE_SWITCH.NIC_PROFILE_ID,
   CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS,
   CORE_SWITCH.VF_ENABLED,
   CORE_SWITCH.VF_SUPPORTED,
   CORE_SWITCH.MANAGED_ELEMENT_ID as CORE_MANAGED_ELEMENT_ID,
   CORE_SWITCH_DETAILS.ETHERNET_MASK,
   CORE_SWITCH_DETAILS.FC_MASK,
   CORE_SWITCH_DETAILS.FC_IP,
   CORE_SWITCH_DETAILS.FC_CERTIFICATE,
   CORE_SWITCH_DETAILS.SW_LICENSE_ID,
   CORE_SWITCH_DETAILS.SUPPLIER_SERIAL_NUMBER,
   CORE_SWITCH_DETAILS.PART_NUMBER,
   CORE_SWITCH_DETAILS.CHECK_BEACON,
   CORE_SWITCH_DETAILS.TIMEZONE,
   CORE_SWITCH_DETAILS.MAX_PORT,
   CORE_SWITCH_DETAILS.CHASSIS_SERVICE_TAG,
   CORE_SWITCH_DETAILS.BAY_ID,
   CORE_SWITCH_DETAILS.TYPE_NUMBER,
   CORE_SWITCH_DETAILS.MODEL_NUMBER,
   CORE_SWITCH_DETAILS.MANUFACTURER,
   CORE_SWITCH_DETAILS.PLANT_OF_MANUFACTURER,
   CORE_SWITCH_DETAILS.SEQUENCE_NUMBER,
   CORE_SWITCH_DETAILS.TAG,
   CORE_SWITCH_DETAILS.ACT_CP_PRI_FW_VERSION,
   CORE_SWITCH_DETAILS.ACT_CP_SEC_FW_VERSION,
   CORE_SWITCH_DETAILS.STBY_CP_PRI_FW_VERSION,
   CORE_SWITCH_DETAILS.STBY_CP_SEC_FW_VERSION,
   CORE_SWITCH_DETAILS.EGM_CAPABLE,
   CORE_SWITCH_DETAILS.SUB_TYPE,
   CORE_SWITCH_DETAILS.PARTITION,
   CORE_SWITCH_DETAILS.MAX_NUM_OF_BLADES,
   CORE_SWITCH_DETAILS.VENDOR_VERSION,
   CORE_SWITCH_DETAILS.VENDOR_PART_NUMBER,
   CORE_SWITCH_DETAILS.RNID_SEQUENCE_NUMBER,
   CORE_SWITCH_DETAILS.CONTACT,
   CORE_SWITCH_DETAILS.LOCATION,
   CORE_SWITCH_DETAILS.DESCRIPTION
from
   CORE_SWITCH LEFT OUTER JOIN CORE_SWITCH_DETAILS
   on CORE_SWITCH_DETAILS.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

CRYPTO_HOST_LUN_INFO

```
create or replace view CRYPTO_HOST_LUN_INFO as
select
   LUN.CRYPTO_HOST_ID,
   LUN.ID CRYPTO_LUN_ID,
   LUN.LUN_NUMBER,
   LUN.CRYPTO_TARGET_CONTAINER_ID,
   LUN.SERIAL_NUMBER,
   LUN.ENCRYPTION_STATE,
   LUN.STATUS,
   LUN.REKEY_INTERVAL,
   LUN.VOLUME_LABEL_PREFIX,
   LUN.LAST_REKEY_DATE,
   LUN.LAST_REKEY_STATUS,
   LUN.LAST_REKEY_PROGRESS,
   LUN.CURRENT_VOLUME_LABEL,
   LUN.PRIOR_ENCRYPTION_STATE,
   LUN.ENCRYPTION_FORMAT,
   LUN.ENCRYPT_EXISTING_DATA,
   LUN.DECRYPT_EXISTING_DATA,
   LUN.KEY_ID,
   LUN.BLOCK_SIZE,
   LUN.TOTAL_BLOCKS,
   LUN.LUN_STATE,
   LUN.LUN_FLAGS,
   LUN.ENCRYPTION_ALGORITHM,
   LUN.KEY_ID_STATE,
   LUN.REKEY_SESSION_NUMBER,
   LUN.PERCENTAGE_COMPLETE,
   LUN.REKEY_ROLE,
   LUN.CURRENT_LBA,
   LUN.LUN_STATE_STRING,
   LUN.NEW_LUN,
   LUN.NEW_LUN_TYPE,
   CRYPTO_HOST.HOST_PORT_WWN,
   CRYPTO_HOST.HOST_NODE_WWN
from
   CRYPTO_LUN LUN,
   CRYPTO_HOST
where
   LUN.CRYPTO_HOST_ID = CRYPTO_HOST.ID;
```

CRYPTO_TARGET_ENGINE_INFO

```
create or replace view CRYPTO_TARGET_ENGINE_INFO as
select
   CRYPTO_TARGET_CONTAINER.ID TARGET_CONTAINER_ID,
   CRYPTO_TARGET_CONTAINER.NAME,
   CRYPTO_TARGET_CONTAINER.VT_NODE_WWN,
   CRYPTO_TARGET_CONTAINER.VT_PORT_WWN,
   CRYPTO_TARGET_CONTAINER.FAILOVER_STATUS,
   CRYPTO_TARGET_CONTAINER.FAILOVER_STATUS_2,
   CRYPTO_TARGET_CONTAINER.DEVICE_STATUS,
   CRYPTO_TARGET_CONTAINER.DEVICE_TYPE,
   CRYPTO_TARGET_CONTAINER.TARGET_PORT_WWN,
   CRYPTO_TARGET_CONTAINER.TARGET_NODE_WWN,
   CRYPTO_TARGET_CONTAINER.CONTAINER_FIELD_DATA,
   CRYPTO_TARGET_CONTAINER.CONFIGURATION_STATUS,
   CRYPTO_TARGET_CONTAINER.FRONT_END_N_PORT_NUMBER,
   ENCRYPTION_ENGINE.STATUS ENCRYPTION_ENGINE_STATUS,
   ENCRYPTION_ENGINE.HA_CLUSTER_ID,
   ENCRYPTION_ENGINE.SYSTEM_CARD_STATUS,
   ENCRYPTION_ENGINE.WWN_POOLS_AVAILABLE,
   ENCRYPTION_ENGINE.STATE ENCRYPTION_ENGINE_STATE,
   ENCRYPTION_ENGINE.ID ENCRYPTION_ENGINE_ID,
   CRYPTO_SWITCH.SWITCH_ID SWITCH_ID,
   CRYPTO_SWITCH.ENCRYPTION_GROUP_ID ENCRYPTION_GROUP_ID
from
   CRYPTO_TARGET_CONTAINER,
   ENCRYPTION_ENGINE,
   CRYPTO_SWITCH
where
   CRYPTO_TARGET_CONTAINER.ENCRYPTION_ENGINE_ID = ENCRYPTION_ENGINE.ID
   and CRYPTO_SWITCH.SWITCH_ID = ENCRYPTION_ENGINE.SWITCH_ID;
```

SWITCH_INFO

```
create or replace view SWITCH_INFO as
select
    CORE_SWITCH.ID as PHYSICAL_SWITCH_ID,
    CORE_SWITCH.NAME as PHYSICAL_SWITCH_NAME,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    CORE_SWITCH.OPERATIONAL_STATUS as PHYSICAL_OPERATIONAL_STATUS,
    CORE_SWITCH.TYPE,
    CORE_SWITCH.MAX_VIRTUAL_SWITCHES,
    CORE_SWITCH.NUM_VIRTUAL_SWITCHES,
    CORE_SWITCH.FIRMWARE_VERSION,
    CORE_SWITCH.VENDOR,
    CORE_SWITCH.REACHABLE,
    CORE_SWITCH.UNREACHABLE_TIME,
    CORE_SWITCH.MODEL,
    CORE_SWITCH.SYSLOG_REGISTERED,
    CORE_SWITCH.SNMP_REGISTERED,
    CORE_SWITCH.CALL_HOME_ENABLED,
    CORE_SWITCH.USER_IP_ADDRESS,
    CORE_SWITCH.NIC_PROFILE_ID,
    CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS,
    CORE_SWITCH.VF_ENABLED,
    CORE_SWITCH.VF_SUPPORTED,
    CORE_SWITCH.MANAGED_ELEMENT_ID as CORE_MANAGED_ELEMENT_ID,
    CORE_SWITCH.NAT_PRIVATE_IP_ADDRESS,
    CORE_SWITCH.ALTERNATE_IP_ADDRESS,
    VIRTUAL_SWITCH.ID,
    VIRTUAL_SWITCH.NAME,
    VIRTUAL_SWITCH.OPERATIONAL_STATUS,
    VIRTUAL_SWITCH.SWITCH_MODE,
    VIRTUAL_SWITCH.AD_CAPABLE,
    VIRTUAL_SWITCH.WWN,
    VIRTUAL_SWITCH.ROLE,
    VIRTUAL_SWITCH.FCS_ROLE,
    VIRTUAL_SWITCH.DOMAIN_ID,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
    VIRTUAL_SWITCH.BASE_SWITCH,
    VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE,
    VIRTUAL_SWITCH.CREATION_TIME,
    VIRTUAL_SWITCH.LAST_UPDATE_TIME,
    VIRTUAL_SWITCH.USER_NAME,
    VIRTUAL_SWITCH.PASSWORD,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.STATE,
    VIRTUAL_SWITCH.STATUS,
    VIRTUAL_SWITCH.STATUS_REASON,
    VIRTUAL_SWITCH.FABRIC_IDID_MODE,
    VIRTUAL_SWITCH.LOGICAL_ID,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_1,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_2,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_3,
    VIRTUAL_SWITCH.INTEROP_MODE,
    VIRTUAL_SWITCH.CRYPTO_CAPABLE,
    VIRTUAL_SWITCH.FCR_CAPABLE,
    VIRTUAL_SWITCH.FCIP_CAPABLE,
    VIRTUAL_SWITCH.LF_ENABLED,
    VIRTUAL_SWITCH.FCOE_CAPABLE,
    VIRTUAL_SWITCH.L2_CAPABLE,
    VIRTUAL_SWITCH.L3_CAPABLE,
    VIRTUAL_SWITCH.DEFAULT_LOGICAL_SWITCH,
    VIRTUAL_SWITCH.FEATURES_SUPPORTED,
    VIRTUAL_SWITCH.FMS_MODE,
    VIRTUAL_SWITCH.DYNAMIC_LOAD_SHARING,
    VIRTUAL_SWITCH.PORT_BASED_ROUTING,
    VIRTUAL_SWITCH.IN_ORDER_DELIVERY,
    VIRTUAL_SWITCH.INSISTENT_DID_MODE,
    VIRTUAL_SWITCH.PREVIOUS_OPERATIONAL_STATUS,
    VIRTUAL_SWITCH.LAST_SCAN_TIME,
    VIRTUAL_SWITCH.DOMAIN_MODE_239,
    VIRTUAL_SWITCH.DOMAIN_ID_OFFSET,
    VIRTUAL_SWITCH.DISCOVERED_PORT_COUNT,
    VIRTUAL_SWITCH.FCOE_LOGIN_ENABLED,
    VIRTUAL_SWITCH.LAST_PORT_MEMBERSHIP_CHANGE,
    VIRTUAL_SWITCH.FCIP_CIRCUIT_CAPABLE,
    VIRTUAL_SWITCH.MAX_FCIP_TUNNELS,
    VIRTUAL_SWITCH.MAX_FCIP_CIRCUITS,
    VIRTUAL_SWITCH.FCIP_LICENSED,
    VIRTUAL_SWITCH.ADDRESSING_MODE,
    VIRTUAL_SWITCH.PREVIOUS_STATE,
    VIRTUAL_SWITCH.MANAGED_ELEMENT_ID,
    VIRTUAL_SWITCH.HIF_ENABLED,
    FABRIC_MEMBER.FABRIC_ID,
    FABRIC_MEMBER.TRUSTED,
    FABRIC_MEMBER.MISSING,
    FABRIC_MEMBER.MISSING_TIME,
    FABRIC.MANAGED as FABRIC_MANAGED,
    FABRIC.PRINCIPAL_SWITCH_WWN,
    FABRIC.SEED_SWITCH_WWN
from
    CORE_SWITCH,
    VIRTUAL_SWITCH,
    FABRIC_MEMBER,
    FABRIC
where
    VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
    and FABRIC_MEMBER.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and FABRIC_MEMBER.FABRIC_ID = FABRIC.ID;
```

DEVICE_INFO

```
create or replace view DEVICE_INFO as
select distinct
  DEVICE_NODE.ID as DEVICE_NODE_ID,
  DEVICE_NODE.WWN as DEVICE_NODE_WWN,
  DEVICE_NODE.TYPE as DEVICE_NODE_TYPE,
  DEVICE_NODE.SYMBOLIC_NAME as DEVICE_NODE_SYMBOLIC_NAME,
  DEVICE_NODE.DEVICE_TYPE,
  DEVICE_NODE.FDMI_HOST_NAME,
  DEVICE_NODE.VENDOR,
  DEVICE_NODE.CAPABILITY_,
  DEVICE_NODE.AG,
  DEVICE_PORT.ID as DEVICE_PORT_ID,
  DEVICE_PORT.DOMAIN_ID as DEVICE_PORT_DOMAIN_ID,
  DEVICE_PORT.WWN as DEVICE_PORT_WWN,
  DEVICE_PORT.NUMBER,
  DEVICE_PORT.PORT_ID,
  DEVICE_PORT.TYPE as DEVICE_PORT_TYPE,
  DEVICE_PORT.SYMBOLIC_NAME as DEVICE_PORT_SYMBOLIC_NAME,
  DEVICE_PORT.FC4_TYPE,
  DEVICE_PORT.IP_PORT,
  DEVICE_PORT.HARDWARE_ADDRESS,
  DEVICE_PORT.TRUSTED as DEVICE_PORT_TRUSTED,
  DEVICE_PORT.MISSING as DEVICE_PORT_MISSING,
  DEVICE_PORT.COS,
  DEVICE_PORT.NPV_PHYSICAL,
  SWITCH_PORT.ID as SWITCH_PORT_ID,
  SWITCH_PORT.WWN as SWITCH_PORT_WWN,
  SWITCH_PORT.NAME as SWITCH_PORT_NAME,
  SWITCH_PORT.SLOT_NUMBER,
  SWITCH_PORT.PORT_NUMBER,
  SWITCH_PORT.PORT_INDEX,
  SWITCH_PORT.TYPE as SWITCH_PORT_TYPE,
  SWITCH_PORT.FULL_TYPE as SWITCH_PORT_FULL_TYPE,
  SWITCH_PORT.STATUS as SWITCH_PORT_STATUS,
  SWITCH_PORT.HEALTH as SWITCH_PORT_HEALTH,
  SWITCH_PORT.SPEED,
  SWITCH_PORT.MAX_PORT_SPEED,
  SWITCH_PORT.NPIV,
  SWITCH_PORT.NPIV_CAPABLE,
  SWITCH_PORT.CALCULATED_STATUS,
  SWITCH_PORT.AREA_ID,
  SWITCH_PORT.PHYSICAL_PORT,
  SWITCH_PORT.CATEGORY,
  SWITCH_PORT.PERSISTENT_DISABLE,
  SWITCH_PORT.BLOCKED,
  SWITCH_PORT.FCR_INTEROP_MODE,
  SWITCH_INFO.IP_ADDRESS,
  SWITCH_INFO.PHYSICAL_SWITCH_WWN,
  SWITCH_INFO.FIRMWARE_VERSION,
  SWITCH_INFO.REACHABLE,
  SWITCH_INFO.SYSLOG_REGISTERED,
  SWITCH_INFO.SNMP_REGISTERED,
  SWITCH_INFO.ID as VIRTUAL_SWITCH_ID,
  SWITCH_INFO.NAME as VIRTUAL_SWITCH_NAME,
  SWITCH_INFO.OPERATIONAL_STATUS,
  SWITCH_INFO.SWITCH_MODE,
  SWITCH_INFO.WWN as VIRTUAL_SWITCH_WWN,
  SWITCH_INFO.DOMAIN_ID as VIRTUAL_SWITCH_DOMAIN_ID,
  SWITCH_INFO.VIRTUAL_FABRIC_ID,
  SWITCH_INFO.BASE_SWITCH,
  SWITCH_INFO.STATE as VIRTUAL_SWITCH_STATE,
  SWITCH_INFO.STATUS as VIRTUAL_SWITCH_STATUS,
  SWITCH_INFO.FABRIC_ID,
  SWITCH_INFO.CRYPTO_CAPABLE
from
  DEVICE_NODE, DEVICE_PORT, SWITCH_PORT, SWITCH_INFO
where
  DEVICE_PORT.NODE_ID = DEVICE_NODE.ID and
  DEVICE_PORT.SWITCH_PORT_WWN = SWITCH_PORT.WWN and
  SWITCH_PORT.VIRTUAL_SWITCH_ID = SWITCH_INFO.ID and
  DEVICE_NODE.FABRIC_ID = SWITCH_INFO.FABRIC_ID;
```

N2F_PORT_MAP_INFO

```
create or replace view N2F_PORT_MAP_INFO as
select
    N2F_PORT_MAP.VIRTUAL_SWITCH_ID,
    N2F_PORT_MAP.N_PORT,
    N2F_PORT_MAP.F_PORT,
    AG_N_PORT.REMOTE_PORT_WWN as EDGE_SWITCH_PORT_WWN,
    AG_F_PORT.WWN as AG_F_PORT_WWN,
    AG_F_PORT.REMOTE_NODE_WWN,
    AG_F_PORT.REMOTE_PORT_WWN as DEVICE_PORT_WWN
from
```

```
    N2F_PORT_MAP,
    SWITCH_PORT AG_N_PORT,
    SWITCH_PORT AG_F_PORT
where
    N2F_PORT_MAP.VIRTUAL_SWITCH_ID = AG_N_PORT.VIRTUAL_SWITCH_ID
    and N2F_PORT_MAP.N_PORT = AG_N_PORT.USER_PORT_NUMBER
    and N2F_PORT_MAP.VIRTUAL_SWITCH_ID = AG_F_PORT.VIRTUAL_SWITCH_ID
    and N2F_PORT_MAP.F_PORT = AG_F_PORT.USER_PORT_NUMBER;
```

DEVICE_NODE_INFO

```
create or replace view DEVICE_NODE_INFO as
select
    DEVICE_NODE.ID,
    DEVICE_NODE.FABRIC_ID,
    DEVICE_NODE.WWN,
   DEVICE_NODE.TYPE,
    DEVICE_NODE.DEVICE_TYPE,
    DEVICE_NODE.SYMBOLIC_NAME,
    DEVICE_NODE.FDMI_HOST_NAME,
    DEVICE_NODE.VENDOR,
    DEVICE_NODE.CAPABILITY_,
    DEVICE_NODE.TRUSTED,
    DEVICE_NODE.CREATION_TIME,
    DEVICE_NODE.MISSING,
    DEVICE_NODE.MISSING_TIME,
    DEVICE_NODE.PROXY_DEVICE,
    DEVICE_NODE.AG,
    DEVICE_NODE.PREVIOUS_MISSING_STATE,
    USER_DEFINED_DEVICE_DETAIL.NAME,
    USER_DEFINED_DEVICE_DETAIL.TYPE as USER_DEFINED_TYPE,
    USER_DEFINED_DEVICE_DETAIL.IP_ADDRESS,
    USER_DEFINED_DEVICE_DETAIL.CONTACT,
    USER_DEFINED_DEVICE_DETAIL.LOCATION,
    USER_DEFINED_DEVICE_DETAIL.DESCRIPTION,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE1,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE2,
    USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE3,
    FABRIC.PRINCIPAL_SWITCH_WWN as PRINCIPAL_WWN
from
    DEVICE_NODE
        left outer join USER_DEFINED_DEVICE_DETAIL
            on DEVICE_NODE.WWN = USER_DEFINED_DEVICE_DETAIL.WWN
        left outer join FABRIC
            on DEVICE_NODE.FABRIC_ID = FABRIC.ID;
```

DEVICE_PORT_INFO

```
create or replace view DEVICE_PORT_INFO as
select
   DEVICE_PORT.ID,
   DEVICE_PORT.NODE_ID,
   DEVICE_PORT.DOMAIN_ID,
   DEVICE_PORT.WWN,
    DEVICE_PORT.SWITCH_PORT_WWN,
   DEVICE_PORT.NUMBER,
   DEVICE_PORT.PORT_ID,
    DEVICE_PORT.TYPE,
   DEVICE_PORT.SYMBOLIC_NAME,
   DEVICE_PORT.FC4_TYPE,
   DEVICE_PORT.COS,
   DEVICE_PORT.IP_PORT,
   DEVICE_PORT.HARDWARE_ADDRESS,
   DEVICE_PORT.TRUSTED,
   DEVICE_PORT.CREATION_TIME,
   DEVICE_PORT.MISSING,
   DEVICE_PORT.MISSING_TIME,
    DEVICE_PORT.NPV_PHYSICAL,
    DEVICE_PORT.EDGE_SWITCH_PORT_WWN,
   FICON_DEVICE_PORT.TYPE_NUMBER,
   FICON_DEVICE_PORT.MODEL_NUMBER,
   FICON_DEVICE_PORT.MANUFACTURER,
   FICON_DEVICE_PORT.MANUFACTURER_PLANT,
   FICON_DEVICE_PORT.SEQUENCE_NUMBER,
   FICON_DEVICE_PORT.TAG,
   FICON_DEVICE_PORT.FLAG,
   FICON_DEVICE_PORT.PARAMS,
   USER_DEFINED_DEVICE_DETAIL.NAME,
   USER_DEFINED_DEVICE_DETAIL.TYPE as USER_DEFINED_TYPE,
   USER_DEFINED_DEVICE_DETAIL.IP_ADDRESS,
   USER_DEFINED_DEVICE_DETAIL.CONTACT,
   USER_DEFINED_DEVICE_DETAIL.LOCATION,
   USER_DEFINED_DEVICE_DETAIL.DESCRIPTION,
   USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE1,
   USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE2,
   USER_DEFINED_DEVICE_DETAIL.USER_DEFINED_VALUE3,
    DEVICE_NODE.WWN as DEVICE_NODE_WWN,
    DEVICE_NODE.FDMI_HOST_NAME,
    DEVICE_NODE.SYMBOLIC_NAME as DEVICE_SYMBOLIC_NAME,
    DEVICE_NODE.AG as AG_PORT,
    coalesce(SWITCH_PORT.NAME, VIRTUAL_FCOE_PORT.NAME) as SWITCH_PORT_NAME,
    coalesce (SWITCH_PORT.TYPE, VIRTUAL_FCOE_PORT.PORT_TYPE) as SWITCH_PORT_TYPE,
    SWITCH_PORT.LOGICAL_PORT_WWN,
    coalesce(VS1.WWN, VS2.WWN) as SWITCH_WWN,
    FABRIC.PRINCIPAL_SWITCH_WWN as PRINCIPAL_WWN,
    FABRIC.ID as FABRIC_ID
from
   DEVICE_PORT
       left outer join USER_DEFINED_DEVICE_DETAIL
           on DEVICE_PORT.WWN = USER_DEFINED_DEVICE_DETAIL.WWN
       left outer join FICON_DEVICE_PORT
           on DEVICE_PORT.ID = FICON_DEVICE_PORT.DEVICE_PORT_ID
        left outer join DEVICE_NODE
            on DEVICE_PORT.NODE_ID = DEVICE_NODE.ID
        left outer join SWITCH_PORT
            on DEVICE_PORT.SWITCH_PORT_WWN = SWITCH_PORT.WWN
        left outer join VIRTUAL_FCOE_PORT
            on DEVICE_PORT.SWITCH_PORT_WWN = VIRTUAL_FCOE_PORT.PORT_WWN
        left outer join VIRTUAL_SWITCH VS1
            on SWITCH_PORT.VIRTUAL_SWITCH_ID = VS1.ID
        left outer join VIRTUAL_SWITCH VS2
            on VIRTUAL_FCOE_PORT.VIRTUAL_SWITCH_ID = VS2.ID
        left outer join FABRIC
            on DEVICE_NODE.FABRIC_ID = FABRIC.ID;
```

DEV_PORT_GIGE_PORT_LINK_INFO

```
create or replace view DEV_PORT_GIGE_PORT_LINK_INFO as
select
    DEVICE_PORT_GIGE_PORT_LINK.DEVICE_PORT_ID,
    DEVICE_PORT_GIGE_PORT_LINK.GIGE_PORT_ID,
    DEVICE_PORT_GIGE_PORT_LINK.DIRECT_ATTACH,
    DEVICE_PORT.TRUSTED,
    DEVICE_PORT.CREATION_TIME,
    DEVICE_PORT.MISSING,
    DEVICE_PORT.MISSING_TIME
from
    DEVICE_PORT_GIGE_PORT_LINK,
    DEVICE_PORT
where
    DEVICE_PORT_GIGE_PORT_LINK.DEVICE_PORT_ID = DEVICE_PORT.ID;
```

DEV_PORT_MAC_ADDR_MAP_INFO

```
create or replace view DEV_PORT_MAC_ADDR_MAP_INFO as
select
    DEVICE_PORT_MAC_ADDRESS_MAP.DEVICE_PORT_ID,
    DEVICE_PORT_MAC_ADDRESS_MAP.MAC_ADDRESS,
    DEVICE_NODE.ID as DEVICE_NODE_ID,
    DEVICE_NODE.FABRIC_ID,
    DEVICE_PORT.TRUSTED,
    DEVICE_PORT.CREATION_TIME,
    DEVICE_PORT.MISSING,
    DEVICE_PORT.MISSING_TIME
from
    DEVICE_PORT_MAC_ADDRESS_MAP,
    DEVICE_PORT,
    DEVICE_NODE
where
    DEVICE_PORT_MAC_ADDRESS_MAP.DEVICE_PORT_ID = DEVICE_PORT.ID
    and DEVICE_PORT.NODE_ID = DEVICE_NODE.ID;
```

ETHERNET_ISL_INFO

```
create or replace view ETHERNET_ISL_INFO as
select
    ETHERNET_ISL.ID as ETHERNET_ISL_ID,
    ETHERNET_ISL.SOURCE_PORT_ID,
    ETHERNET_ISL.DEST_PORT_ID,
    ETHERNET_ISL.TRUSTED,
    ETHERNET_ISL.CREATION_TIME,
    ETHERNET_ISL.MISSING,
    ETHERNET_ISL.MISSING_TIME,
    SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID as SOURCE_SWITCH_ID,
    SOURCE_SWITCH_PORT.USER_PORT_NUMBER as SOURCE_PORT_NUMBER,
    SOURCE_SWITCH_PORT.TYPE as SOURCE_PORT_TYPE,
    SOURCE_VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID as SOURCE_VIRTUAL_FABRIC_ID,
    DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID as DEST_SWITCH_ID,
    DEST_SWITCH_PORT.USER_PORT_NUMBER as DEST_PORT_NUMBER,
    DEST_SWITCH_PORT.TYPE as DEST_PORT_TYPE,
    DEST_VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID as DEST_VIRTUAL_FABRIC_ID
from
```

```
    ETHERNET_ISL,
    GIGE_PORT       SOURCE_GIGE_PORT,
    VIRTUAL_SWITCH  SOURCE_VIRTUAL_SWITCH,
    SWITCH_PORT     SOURCE_SWITCH_PORT,
    GIGE_PORT       DEST_GIGE_PORT,
    VIRTUAL_SWITCH  DEST_VIRTUAL_SWITCH,
    SWITCH_PORT     DEST_SWITCH_PORT
where
    SOURCE_GIGE_PORT.ID  = ETHERNET_ISL.SOURCE_PORT_ID and
    SOURCE_GIGE_PORT.SWITCH_PORT_ID = SOURCE_SWITCH_PORT.ID and
    SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID = SOURCE_VIRTUAL_SWITCH.ID and
    DEST_GIGE_PORT.ID  = ETHERNET_ISL.DEST_PORT_ID and
    DEST_GIGE_PORT.SWITCH_PORT_ID = DEST_SWITCH_PORT.ID and
    DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID = DEST_VIRTUAL_SWITCH.ID;
```

EVENT_DETAILS_INFO

```
create or replace view EVENT_DETAILS_INFO as
select
    EVENT.ID as ID,
    EVENT.ME_ID as ME_ID,
    EVENT.SEVERITY as SEVERITY,
    EVENT.AREA as AREA,
    EVENT.ACKNOWLEDGED as ACKNOWLEDGED,
    EVENT.SOURCE_NAME as SOURCE_NAME,
    EVENT.SOURCE_ADDR as SOURCE_ADDR,
    EVENT.LAST_OCCURRENCE_HOST_TIME as LAST_OCCURRENCE_HOST_TIME,
    EVENT.FIRST_OCCURRENCE_HOST_TIME as FIRST_OCCURRENCE_HOST_TIME,
    EVENT.EVENT_COUNT as EVENT_COUNT,
    EVENT.EVENT_KEY as EVENT_KEY,
    EVENT.EVENT_AUDIT as AUDIT,
    EVENT.RESOLVED as RESOLVED,
    EVENT.ACKED_TIME as ACKED_TIME,
    EVENT.EVENT_ACTION_ID as EVENT_ACTION_ID,
    EVENT.DEVICE_GROUP_ID as DEVICE_GROUP_ID,
    EVENT.PORT_GROUP_ID as PORT_GROUP_ID,
    EVENT_ORIGIN.ID as ORIGIN,
    EVENT_CATEGORY.ID as EVENT_CATEGORY,
    EVENT_DESCRIPTION.DESCRIPTION as DESCRIPTION,
    EVENT_MODULE.ID as MODULE,
    EVENT_DETAILS.RAS_LOG_ID as RAS_LOG_ID,
    EVENT_DETAILS.PRODUCT_ADDRESS as PRODUCT_ADDRESS,
    EVENT_DETAILS.CONTRIBUTORS as CONTRIBUTORS,
    EVENT_DETAILS.NODE_WWN as NODE_WWN,
    EVENT_DETAILS.PORT_WWN as PORT_WWN,
    EVENT_DETAILS.OPERATIONAL_STATUS as OPERATIONAL_STATUS,
    EVENT_DETAILS.FIRST_OCCURRENCE_SWITCH_TIME as FIRST_OCCURRENCE_SWITCH_TIME,
    EVENT_DETAILS.LAST_OCCURRENCE_SWITCH_TIME as LAST_OCCURRENCE_SWITCH_TIME,
    EVENT_DETAILS.VIRTUAL_FABRIC_ID as VIRTUAL_FABRIC_ID,
    EVENT_DETAILS.UNIT as UNIT,
    EVENT_DETAILS.SLOT as SLOT,
    EVENT_DETAILS.PORT as PORT,
    EVENT_DETAILS.OID,
    EVENT_CALL_HOME.EVENT_NUMBER as EVENT_NUMBER,
    EVENT_CALL_HOME.FRU_CODE as FRU_CODE,
    EVENT_CALL_HOME.REASON_CODE as REASON_CODE,
    EVENT_CALL_HOME.FRU_POSITION as FRU_POSITION
from
    EVENT
```

```
        left outer join EVENT_ORIGIN on EVENT.EVENT_ORIGIN_ID = EVENT_ORIGIN.ID
        left outer join EVENT_CATEGORY on EVENT.EVENT_CATEGORY_ID =
EVENT_CATEGORY.ID
        left outer join EVENT_MODULE on EVENT.EVENT_MODULE_ID = EVENT_MODULE.ID
        left outer join EVENT_DESCRIPTION on EVENT.EVENT_DESCRIPTION_ID =
EVENT_DESCRIPTION.ID
        left outer join EVENT_DETAILS on EVENT.ID = EVENT_DETAILS.EVENT_ID
       left outer join EVENT_CALL_HOME on EVENT.ID = EVENT_CALL_HOME.EVENT_ID;
```

EVENT_INFO

```
create or replace view EVENT_INFO as
select
    EVENT.ID as ID,
    EVENT.ME_ID as ME_ID,
    EVENT.SEVERITY as SEVERITY,
    EVENT.AREA as AREA,
    EVENT.ACKNOWLEDGED as ACKNOWLEDGED,
    EVENT.SOURCE_NAME as SOURCE_NAME,
    EVENT.SOURCE_ADDR as SOURCE_ADDR,
    EVENT.LAST_OCCURRENCE_HOST_TIME as LAST_OCCURRENCE_HOST_TIME,
    EVENT.FIRST_OCCURRENCE_HOST_TIME as FIRST_OCCURRENCE_HOST_TIME,
    EVENT.EVENT_COUNT as EVENT_COUNT,
    EVENT.EVENT_AUDIT as AUDIT,
    EVENT.EVENT_ACTION_ID,
    EVENT_ORIGIN.ID as ORIGIN,
    EVENT_CATEGORY.ID as EVENT_CATEGORY,
    EVENT_DESCRIPTION.DESCRIPTION as DESCRIPTION,
    EVENT_MODULE.ID as MODULE,
    EVENT_DETAILS.RAS_LOG_ID as RAS_LOG_ID,
    EVENT_DETAILS.PRODUCT_ADDRESS as PRODUCT_ADDRESS,
    EVENT_DETAILS.CONTRIBUTORS as CONTRIBUTORS,
    EVENT_DETAILS.NODE_WWN as NODE_WWN,
    EVENT_DETAILS.OPERATIONAL_STATUS as OPERATIONAL_STATUS,
    EVENT_DETAILS.FIRST_OCCURRENCE_SWITCH_TIME as FIRST_OCCURRENCE_SWITCH_TIME,
    EVENT_DETAILS.LAST_OCCURRENCE_SWITCH_TIME as LAST_OCCURRENCE_SWITCH_TIME,
    EVENT_DETAILS.VIRTUAL_FABRIC_ID as VIRTUAL_FABRIC_ID
from
    EVENT
        left join EVENT_DETAILS on EVENT.ID = EVENT_DETAILS.EVENT_ID,
EVENT_ORIGIN, EVENT_CATEGORY, EVENT_MODULE, EVENT_DESCRIPTION
       where EVENT.EVENT_ORIGIN_ID = EVENT_ORIGIN.ID and EVENT.EVENT_CATEGORY_ID
= EVENT_CATEGORY.ID and EVENT.EVENT_MODULE_ID = EVENT_MODULE.ID
```

FABRIC_INFO

```
create or replace view FABRIC_INFO as
select
   FABRIC.ID,
   FABRIC.SAN_ID,
   FABRIC.SEED_SWITCH_WWN,
   FABRIC.NAME,
   FABRIC.ACTIVE_ZONESET_NAME,
   FABRIC.MANAGEMENT_STATE,
   FABRIC.LAST_FABRIC_CHANGED,
   FABRIC.SECURE,
   FABRIC.AD_ENVIRONMENT,
   FABRIC.MANAGED,
    FABRIC.CONTACT,
    FABRIC.LOCATION,
    FABRIC.DESCRIPTION,
    FABRIC.CREATION_TIME,
    FABRIC.LAST_SCAN_TIME,
    FABRIC.LAST_UPDATE_TIME,
    FABRIC.TRACK_CHANGES,
    FABRIC.TYPE,
     FABRIC.USER_DEFINED_VALUE_1,
     FABRIC.USER_DEFINED_VALUE_2,
     FABRIC.USER_DEFINED_VALUE_3,
    FABRIC.PRINCIPAL_SWITCH_WWN,
    FABRIC.ZONE_TRANSACTION_TIMEOUT,
     FABRIC.FABRIC_MODEL,
     FABRIC.ENHANCED_TI_ZONE_SUPPORT,
     VIRTUAL_SWITCH.ID as SEED_SWITCH_ID,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
     VIRTUAL_SWITCH.INTEROP_MODE,
    CORE_SWITCH.IP_ADDRESS as SEED_SWITCH_IP_ADDRESS,
    (select count(*) from FABRIC_MEMBER
         where FABRIC_MEMBER.FABRIC_ID = FABRIC.ID) as SWITCH_COUNT
from
    FABRIC, CORE_SWITCH, VIRTUAL_SWITCH, FABRIC_MEMBER
where
    FABRIC.SEED_SWITCH_WWN = VIRTUAL_SWITCH.WWN and
    VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID and
    FABRIC_MEMBER.FABRIC_ID = FABRIC.ID;
```

FCIP_TUNNEL_CIRCUIT_INFO

```
create or replace view FCIP_TUNNEL_CIRCUIT_INFO as
select
     FCIP_TUNNEL_CIRCUIT.ID,
     FCIP_TUNNEL_CIRCUIT.TUNNEL_ID,
     FCIP_TUNNEL_CIRCUIT.CIRCUIT_NUMBER,
     FCIP_TUNNEL_CIRCUIT.COMPRESSION_ENABLED,
     FCIP_TUNNEL_CIRCUIT.TURBO_WRITE_ENABLED,
     FCIP_TUNNEL_CIRCUIT.TAPE_ACCELERATION_ENABLED,
     FCIP_TUNNEL_CIRCUIT.IKE_POLICY_NUM,
     FCIP_TUNNEL_CIRCUIT.IPSEC_POLICY_NUM,
     FCIP_TUNNEL_CIRCUIT.PRESHARED_KEY,
     FCIP_TUNNEL_CIRCUIT.SOURCE_IP,
     FCIP_TUNNEL_CIRCUIT.DEST_IP,
     FCIP_TUNNEL_CIRCUIT.VLAN_TAG,
     FCIP_TUNNEL_CIRCUIT.SELECTIVE_ACK,
     FCIP_TUNNEL_CIRCUIT.QOS_MAPPING,
     FCIP_TUNNEL_CIRCUIT.PATH_MTU_DISCOVERY,
     FCIP_TUNNEL_CIRCUIT.MIN_COMM_RATE,
     FCIP_TUNNEL_CIRCUIT.MAX_COMM_RATE,
     FCIP_TUNNEL_CIRCUIT.MIN_RETRANSMIT_TIME,
     FCIP_TUNNEL_CIRCUIT.MAX_RETRANSMIT_TIME,
     FCIP_TUNNEL_CIRCUIT.KEEP_ALIVE_TIMEOUT,
     FCIP_TUNNEL_CIRCUIT.ADMIN_STATUS,
     FCIP_TUNNEL_CIRCUIT.METRIC,
     FCIP_TUNNEL_CIRCUIT.DATA_L2_COS,
     FCIP_TUNNEL_CIRCUIT.DSCP_DATA,
     FCIP_TUNNEL_CIRCUIT.MAX_RETRANSMISSIONS,
     FCIP_TUNNEL_CIRCUIT.SLOT_NUMBER,
     FCIP_TUNNEL_CIRCUIT.VE_PORT_NUMBER,
     FCIP_TUNNEL_CIRCUIT.SECURITY_FLAG,
     FCIP_TUNNEL_CIRCUIT.DSCP_CONTROL,
     FCIP_TUNNEL_CIRCUIT.CIRCUIT_STATUS,
     FCIP_TUNNEL_CIRCUIT.ENABLED,
     FCIP_TUNNEL_CIRCUIT.MISMATCHED_CONFIGURATIONS,
     FCIP_TUNNEL_CIRCUIT.CIRCUIT_STATUS_STRING,
     FCIP_TUNNEL_CIRCUIT.L2COS_F_CLASS,
     FCIP_TUNNEL_CIRCUIT.L2_COS_HIGH,
     FCIP_TUNNEL_CIRCUIT.L2_COS_MEDIUM,
     FCIP_TUNNEL_CIRCUIT.L2_COS_LOW,
     FCIP_TUNNEL_CIRCUIT.DSCP_F_CLASS,
     FCIP_TUNNEL_CIRCUIT.DSCP_HIGH,
     FCIP_TUNNEL_CIRCUIT.DSCP_MEDIUM,
     FCIP_TUNNEL_CIRCUIT.DSCP_LOW,
     GIGE_PORT.PORT_NUMBER GIGE_PORT_NUMBER,
     GIGE_PORT.SLOT_NUMBER GIGE_PORT_SLOT_NUMBER,
     FCIP_CIRCUIT_PORT_MAP.SWITCH_PORT_ID GIGE_PORT_ID,
     SWITCH_PORT.VIRTUAL_SWITCH_ID,
     SWITCH_PORT.USER_PORT_NUMBER
 from
     FCIP_TUNNEL_CIRCUIT
         left outer join FCIP_CIRCUIT_PORT_MAP on
             FCIP_CIRCUIT_PORT_MAP.CIRCUIT_ID = FCIP_TUNNEL_CIRCUIT.ID
         left outer join GIGE_PORT
             on FCIP_CIRCUIT_PORT_MAP.SWITCH_PORT_ID = GIGE_PORT.ID
         left outer join SWITCH_PORT
             on GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID;
```

FCIP_TUNNEL_INFO

```
create or replace view FCIP_TUNNEL_INFO as
select
   FCIP_TUNNEL.ID,
   FCIP_TUNNEL.TUNNEL_ID,
   FCIP_TUNNEL.VLAN_TAG,
   FCIP_TUNNEL.SOURCE_IP,
   FCIP_TUNNEL.DEST_IP,
   FCIP_TUNNEL.LOCAL_WWN,
   FCIP_TUNNEL.REMOTE_WWN_RESTRICT,
   FCIP_TUNNEL.COMMUNICATION_RATE,
   FCIP_TUNNEL.MIN_RETRANSMIT_TIME,
   FCIP_TUNNEL.SELECTIVE_ACK_ENABLED,
   FCIP_TUNNEL.KEEP_ALIVE_TIMEOUT,
   FCIP_TUNNEL.MAX_RETRANSMISSION,
   FCIP_TUNNEL.WAN_TOV_ENABLED,
   FCIP_TUNNEL.TUNNEL_STATUS,
   FCIP_TUNNEL.DESCRIPTION,
   FCIP_TUNNEL.FICON_TRB_ID_ENABLED,
   FCIP_TUNNEL.FICON_TT_EMUL_ENABLED,
   FCIP_TUNNEL.FICON_DLA_EMUL_ENABLED,
   FCIP_TUNNEL.FICON_TAPE_WRITE_MAX_PIPE,
   FCIP_TUNNEL.FICON_TAPE_READ_MAX_PIPE,
   FCIP_TUNNEL.FICON_TAPE_WRITE_MAX_OPS,
   FCIP_TUNNEL.FICON_TAPE_READ_MAX_OPS,
   FCIP_TUNNEL.FICON_TAPE_WRITE_TIMER,
   FCIP_TUNNEL.FICON_TAPE_MAX_WRITE_CHAIN,
   FCIP_TUNNEL.FICON_OXID_BASE,
   FCIP_TUNNEL.FICON_XRC_EMULATION_ENABLED,
   FCIP_TUNNEL.FICON_TW_EMUL_ENABLED,
   FCIP_TUNNEL.FICON_TR_EMUL_ENABLED,
   FCIP_TUNNEL.FICON_DEBUG_FLAGS,
   FCIP_TUNNEL.REMOTE_WWN,
   FCIP_TUNNEL.CDC,
   FCIP_TUNNEL.ADMIN_STATUS,
   FCIP_TUNNEL.CONTROL_L2_COS,
   FCIP_TUNNEL.DSCP_CONTROL,
   FCIP_TUNNEL.TRUNKING_ALGORITHM,
   FCIP_TUNNEL.EXTENDED_TUNNEL,
   FCIP_TUNNEL.VIRTUAL_SWITCH_ID,
   FCIP_TUNNEL.CIRCUIT_COUNT,
   FCIP_TUNNEL.MISMATCHED_CONFIG_DETAILS,
   FCIP_TUNNEL.SLOT_NUMBER,
   FCIP_TUNNEL.FICON_ENABLED,
   FCIP_TUNNEL.TPERF_ENABLED,
   FCIP_TUNNEL.AUTH_KEY,
   FCIP_TUNNEL.CONNECTED_COUNT,
   FCIP_TUNNEL.TUNNEL_STATUS_STRING,
   FCIP_TUNNEL.COMPRESSION_MODE,
   FCIP_TUNNEL.TURBO_WRITE_ENABLED,
   FCIP_TUNNEL.TAPE_ACCELERATION_ENABLED,
   FCIP_TUNNEL.IPSEC_ENABLED,
   FCIP_TUNNEL.PRESHARED_KEY,
   PORT.WWN as VIRTUAL_PORT_WWN,
   PORT.REMOTE_PORT_WWN as REMOTE_PORT_WWN,
   PORT.REMOTE_NODE_WWN as REMOTE_NODE_WWN,
   PORT.ID as SWITCH_PORT_ID,
   PORT.PORT_NUMBER as SWITCH_PORT_NUMBER,
   PORT.USER_PORT_NUMBER as USER_PORT_NUMBER,
   PORT.PORT_INDEX,
   PORT.STATUS_MESSAGE
from
   FCIP_TUNNEL
     left outer join
     FCIP_PORT_TUNNEL_MAP on
     FCIP_PORT_TUNNEL_MAP.TUNNEL_ID = FCIP_TUNNEL.ID
     left outer join SWITCH_PORT PORT
            on FCIP_PORT_TUNNEL_MAP.SWITCHPORT_ID = PORT.ID;
```

FCOE_DEVICE_INFO

```
create or replace view FCOE_DEVICE_INFO as
select
    FCOE_DEVICE.DEVICE_NODE_ID,
    FCOE_DEVICE.DIRECT_ATTACH,
    FCOE_DEVICE.ATTACH_ID,
    FCOE_DEVICE.MAC_ADDRESS,
    DEVICE_NODE.TRUSTED,
    DEVICE_NODE.CREATION_TIME,
    DEVICE_NODE.MISSING,
    DEVICE_NODE.MISSING_TIME
from
    FCOE_DEVICE,
    DEVICE_NODE
where
    FCOE_DEVICE.DEVICE_NODE_ID = DEVICE_NODE.ID;
```

FRU_INFO

```
create or replace view FRU_INFO as
select
    FRU.ID,
    FRU.CORE_SWITCH_ID,
    FRU.TAG,
    FRU.PART_NUMBER,
    FRU.SERIAL_NUMBER,
    FRU.VENDOR_PART_NUMBER,
    FRU.VENDOR_SERIAL_NUMBER,
    FRU.CAN_BE_FRUED,
    FRU.SLOT_NUMBER,
    FRU.MANUFACTURER_DATE,
    FRU.UPDATE_DATE,
    FRU.VERSION,
    FRU.MANUFACTURER,
    FRU.VENDOR_EQUIPMENT_TYPE,
    FRU.OPERATIONAL_STATUS,
    FRU.TOTAL_OUTPUT_POWER,
    FRU.SPEED,
    FRU.CREATION_TIME,
    FRU.LAST_UPDATE_TIME,
    FRU.PREVIOUS_OP_STATUS,
    FRU.VENDOR,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    VIRTUAL_SWITCH.SWITCH_MODE as VIRTUAL_SWITCH_MODE
from
    FRU,
    CORE_SWITCH,
    VIRTUAL_SWITCH
where
    FRU.CORE_SWITCH_ID = CORE_SWITCH.ID and
    FRU.CORE_SWITCH_ID = VIRTUAL_SWITCH.CORE_SWITCH_ID;
```

GIGE_PORT_ECLOUD_LINK_INFO

```
create or replace view GIGE_PORT_ECLOUD_LINK_INFO as
select
    GIGE_PORT_ETHERNET_CLOUD_LINK.ID,
    GIGE_PORT_ETHERNET_CLOUD_LINK.SWITCH_PORT_ID as GIGE_PORT_ID,
    GIGE_PORT_ETHERNET_CLOUD_LINK.CLOUD_ID,
    GIGE_PORT_ETHERNET_CLOUD_LINK.TRUSTED,
    GIGE_PORT_ETHERNET_CLOUD_LINK.CREATION_TIME,
    GIGE_PORT_ETHERNET_CLOUD_LINK.MISSING,
    GIGE_PORT_ETHERNET_CLOUD_LINK.MISSING_TIME,
    GIGE_PORT.SWITCH_PORT_ID,
    GIGE_PORT.PORT_TYPE,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.USER_PORT_NUMBER,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID
from
    GIGE_PORT_ETHERNET_CLOUD_LINK,
    GIGE_PORT,
    SWITCH_PORT,
    VIRTUAL_SWITCH
where
    GIGE_PORT_ETHERNET_CLOUD_LINK.SWITCH_PORT_ID = GIGE_PORT.ID and
    GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID and
    SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID;
```

GIGE_PORT_INFO

```
create or replace view GIGE_PORT_INFO as
select
   GIGE_PORT.ID,
   GIGE_PORT.SWITCH_PORT_ID,
   GIGE_PORT.PORT_NUMBER,
   GIGE_PORT.SLOT_NUMBER,
   GIGE_PORT.ENABLED,
   GIGE_PORT.SPEED,
   GIGE_PORT.MAX_SPEED,
   GIGE_PORT.MAC_ADDRESS,
   GIGE_PORT.PORT_NAME,
   GIGE_PORT.OPERATIONAL_STATUS,
   GIGE_PORT.LED_STATE,
   GIGE_PORT.SPEED_LED_STATE,
   GIGE_PORT.PORT_TYPE,
   GIGE_PORT.PERSISTENTLY_DISABLED,
   GIGE_PORT.INTERFACE_TYPE,
   GIGE_PORT.CHECKSUM,
   GIGE_PORT.FCIP_CAPABLE,
   GIGE_PORT.ISCSI_CAPABLE,
   GIGE_PORT.REMOTE_MAC_ADDRESS,
   GIGE_PORT.INBAND_MANAGEMENT_STATUS,
   GIGE_PORT.LAST_UPDATE,
   SWITCH_PORT.VIRTUAL_SWITCH_ID,
   SWITCH_PORT.USER_PORT_NUMBER,
   SWITCH_PORT.PORT_INDEX,
   VIRTUAL_SWITCH.WWN as VIRTUAL_SWITCH_WWN,
   CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN
from
   GIGE_PORT, SWITCH_PORT, CORE_SWITCH, VIRTUAL_SWITCH
where
   GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID and
   SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID and
   VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

HBA_PORT_DETAILS_INFO

```
create or replace view HBA_PORT_DETAILS_INFO as
select
    HBA_PORT.DEVICE_PORT_ID,
    HBA_PORT.CONFIGURED_STATE,
    HBA_PORT.CONFIGURED_SPEED,
    HBA_PORT.CONFIGURED_TOPOLOGY,
    HBA_PORT.MAX_SPEED_SUPPORTED,
    HBA_PORT.OPERATING_STATE,
    HBA_PORT.OPERATING_TOPOLOGY,
    HBA_PORT.SUPPORTED_FC4_TYPES,
    HBA_PORT.SUPPORTED_COS,
    HBA_PORT.TRUSTED as HBA_PORT_TRUSTED,
    HBA_PORT.CREATION_TIME as HBA_PORT_CREATION_TIME,
    HBA_PORT.MISSING as HBA_PORT_MISSING,
    HBA_PORT.MISSING_TIME as HBA_PORT_MISSING_TIME,
    HBA_PORT.OPERATING_SPEED,
    HBA_PORT.CNA_PORT_ID,
    HBA_PORT.PORT_NWWN,
    HBA_PORT.PHYSICAL_PORT_WWN,
    HBA_PORT.SWITCH_IP,
    HBA_PORT.PRINCIPAL_SWITCH_WWN,
    HBA_PORT.HBA_ID,
    HBA_PORT.PORT_NUMBER,
    HBA_PORT.NAME,
    HBA_PORT.FACTORY_PORT_WWN,
    HBA_PORT.FACTORY_NODE_WWN,
    HBA_PORT.PREBOOT_CREATED,
    HBA_PORT_DETAIL.PERSISTENT_BINDING,
    HBA_PORT_DETAIL.FABRIC_NAME,
    HBA_PORT_DETAIL.BOOT_OVER_SAN,
    HBA_PORT_DETAIL.BOOT_OPTION,
    HBA_PORT_DETAIL.BOOT_SPEED,
    HBA_PORT_DETAIL.BOOT_TOPOLOGY,
    HBA_PORT_DETAIL.BB_CREDIT,
    HBA_PORT_DETAIL.FRAME_DATA_FIELD_SIZE,
    HBA_PORT_DETAIL.HARDWARE_PATH,
    HBA_PORT_DETAIL.V_PORT_COUNT,
    HBA_PORT_DETAIL.QUEUE_DEPTH,
    HBA_PORT_DETAIL.INTERRUPT_CONTROL_COALESCE,
    HBA_PORT_DETAIL.INTERRUPT_CONTROL_LATENCY,
    HBA_PORT_DETAIL.INTERRUPT_CONTROL_DELAY,
    HBA_PORT_DETAIL.BEACON_STATE,
    HBA_PORT_DETAIL.LINK_BEACON_STATE,
    HBA_PORT_DETAIL.MPIO_MODE_STATE,
    HBA_PORT_DETAIL.PATH_TIME_OUT,
    HBA_PORT_DETAIL.LOGGING_LEVEL,
    HBA_PORT_DETAIL.TARGET_RATE_LIMIT,
    HBA_PORT_DETAIL.DEFAULT_RATE_LIMIT,
    HBA_PORT_DETAIL.VF_MODE,
    HBA_PORT_DETAIL.RECIEVE_BUFFER_CREDIT,
    HBA_PORT_DETAIL.TRANSMIT_BUFFER_CREDIT,
    HBA_PORT_DETAIL.FCSP_AUTH_STATE,
    HBA_PORT_DETAIL.FCSP_STATUS,
    HBA_PORT_DETAIL.FCSP_ALGORITHM,
    HBA_PORT_DETAIL.FCSP_GROUP,
    HBA_PORT_DETAIL.FCSP_ERROR_STATUS,
    HBA_PORT_DETAIL.QOS_CONFIGURED_STATE,
    HBA_PORT_DETAIL.QOS_OPERATING_STATE,
    HBA_PORT_DETAIL.QOS_TOTAL_BB_CREDIT,
    HBA_PORT_DETAIL.QOS_PRIORITY_LEVEL,
    HBA_PORT_DETAIL.QOS_HIGH_BW_ALLOCATION,
    HBA_PORT_DETAIL.QOS_MEDIUM_BW_ALLOCATION,
    HBA_PORT_DETAIL.QOS_LOW_BW_ALLOCATION,
    HBA_PORT_DETAIL.MEDIA as MEDIA,
    HBA_PORT_DETAIL.IOC_ID as IOC_ID,
    HBA_PORT_DETAIL.PREBOOT_DISABLED,
    HBA_PORT_FCOE_DETAILS.BANDWIDTH as FCOE_BANDWIDTH,
    HBA_PORT_FCOE_DETAILS.FIP_STATE,
    HBA_PORT_FCOE_DETAILS.DISCOVERY_PRIORITY,
    HBA_PORT_FCOE_DETAILS.FCF_FCMAP,
    HBA_PORT_FCOE_DETAILS.FCF_FPMA_MAC,
    HBA_PORT_FCOE_DETAILS.FCF_MAC,
    HBA_PORT_FCOE_DETAILS.FCF_MODE,
    HBA_PORT_FCOE_DETAILS.FCF_NAMEID,
    HBA_PORT_FCOE_DETAILS.FCPIM_MPIO_MODE,
    HBA_PORT_FCOE_DETAILS.PORT_LOG_ENABLED,
    HBA_PORT_FCOE_DETAILS.MAX_FRAME_SIZE as FCOE_MAX_FRAME_SIZE,
    HBA_PORT_FCOE_DETAILS.MTU as FCOE_MTU,
    HBA_PORT_FCOE_DETAILS.PATH_TOV as FCOE_PATH_TOV,
    HBA_PORT_FCOE_DETAILS.SCSI_QUEUE_DEPTH as FCOE_SCSI_QUEUE_DEPTH,
    HBA_PORT_FCOE_DETAILS.STATE as FCOE_STATE,
    HBA_PORT_FCOE_DETAILS.SUPPORTED_CLASS as FCOE_SUPPORTED_CLASS,
    HBA_PORT_FCOE_DETAILS.TRL_SPEED as FCOE_TRL_SPEED,
    HBA_PORT_FCOE_DETAILS.TRL_STATE as FCOE_TRL_STATE,
    HBA_PORT_FCOE_DETAILS.PG_ID as FCOE_PG_ID,
    HBA_PORT_FCOE_DETAILS.PRIORITIES as FCOE_PRIORITIES,
    HBA_PORT_FCOE_DETAILS.FCOE_MAC
from
    HBA_PORT
        left outer join HBA_PORT_DETAIL
            on HBA_PORT.DEVICE_PORT_ID = HBA_PORT_DETAIL.DEVICE_PORT_ID
        left outer join HBA_PORT_FCOE_DETAILS
            on HBA_PORT.DEVICE_PORT_ID = HBA_PORT_FCOE_DETAILS.DEVICE_PORT_ID;
```

HBA_TARGET_INFO

```
create or replace view HBA_TARGET_INFO as
select
    HBA_TARGET.DEVICE_PORT_ID,
    HBA_TARGET.HBA_REMOTE_PORT_LUN_ID,
    HBA_TARGET.BOOT_LUN,
    HBA_TARGET.TRUSTED,
    HBA_TARGET.CREATION_TIME,
    HBA_TARGET.MISSING,
    HBA_TARGET.MISSING_TIME,
    HBA_TARGET.TARGET_ID as HBA_PORT_TARGET_ID,
    HBA_REMOTE_PORT.ID as HBA_REMOTE_PORT_ID,
    HBA_REMOTE_PORT.SYMBOLIC_NAME,
    HBA_REMOTE_PORT.PORT_WWN,
    HBA_REMOTE_PORT.NODE_WWN,
    HBA_REMOTE_PORT.NAME,
    HBA_REMOTE_PORT.FC_ADDRESS,
    HBA_REMOTE_PORT.FRAME_DATA_SIZE,
    HBA_REMOTE_PORT.SPEED,
    HBA_REMOTE_PORT.STATE,
    HBA_REMOTE_PORT.SUPPORTED_COS,
    HBA_REMOTE_PORT.DEVICE_TYPE,
    HBA_REMOTE_PORT.BIND_TYPE,
    HBA_REMOTE_PORT.TARGET_ID,
    HBA_REMOTE_PORT.ROLE,
    HBA_REMOTE_PORT.VENDOR,
    HBA_REMOTE_PORT.PRODUCT_ID,
    HBA_REMOTE_PORT.PRODUCT_VERSION,
    HBA_REMOTE_PORT.QOS_PRIORITY,
    HBA_REMOTE_PORT.QOS_FLOW_ID,
    HBA_REMOTE_PORT.CURRENT_SPEED,
    HBA_REMOTE_PORT.TRL_ENFORCED,
    HBA_REMOTE_PORT.BUS_NO,
    HBA_REMOTE_PORT_LUN.FCP_LUN,
    HBA_REMOTE_PORT_LUN.CAPACITY,
    HBA_REMOTE_PORT_LUN.BLOCK_SIZE,
    HBA_REMOTE_PORT_LUN.VENDOR as LUN_VENDOR,
    HBA_REMOTE_PORT_LUN.PRODUCT_ID as LUN_PRODUCT_ID,
    HBA_REMOTE_PORT_LUN.PRODUCT_VERSION as LUN_PRODUCT_VERSION,
    HBA_REMOTE_PORT_LUN.PRODUCT_SERIAL_NO,
    HBA_REMOTE_PORT_LUN.TARGET_WWN,
    HBA_REMOTE_PORT_LUN.PHYSICAL_LUN,
    HBA_REMOTE_PORT_LUN.LUN_ID,
    HBA_REMOTE_PORT.FCP_IM_STATE,
    HBA_REMOTE_PORT.IO_LATENCY_MIN,
    HBA_REMOTE_PORT.IO_LATENCY_MAX,
    HBA_REMOTE_PORT.IO_LATENCY_AVERAGE,
    HBA_REMOTE_PORT.DATA_RETRANSMISSION_SUPPORT,
    HBA_REMOTE_PORT.REC_SUPPORT,
    HBA_REMOTE_PORT.TASK_RENTRY_IDENT_SUPPORT,
    HBA_REMOTE_PORT.CONFIRMED_COMPLETIONS_SUPPORT
from
    HBA_TARGET, HBA_REMOTE_PORT, HBA_REMOTE_PORT_LUN
where
    HBA_TARGET.HBA_REMOTE_PORT_LUN_ID = HBA_REMOTE_PORT_LUN.ID and
    HBA_REMOTE_PORT.ID = HBA_REMOTE_PORT_LUN.HBA_REMOTE_PORT_ID;
```

HOST_DISCOVERY_REQUEST_INFO

```
create or replace view HOST_DISCOVERY_REQUEST_INFO as
select
    HOST_DISCOVERY_REQUEST.ID,
    HOST_DISCOVERY_REQUEST.HOST_NAME AS REQUEST_HOST_NAME,
    HOST_DISCOVERY_REQUEST.DEVICE_ENCLOSURE_ID,
    HOST_DISCOVERY_REQUEST.REQUEST_GROUP_ID,
    HOST_DISCOVERY_REQUEST.HOST_DISCOVERY_OPTION_ID,
    HOST_DISCOVERY_REQUEST.VM_MANAGEMENT_STATE,
    HOST_DISCOVERY_REQUEST.JSON_MANAGEMENT_STATE,
    HOST_DISCOVERY_REQUEST.CIM_MANAGEMENT_STATE,
    HOST_DISCOVERY_REQUEST.MANAGEMENT_STATE,
    HOST_DISCOVERY_OPTION.DISCOVER_JSON,
    HOST_DISCOVERY_OPTION.JSON_USERNAME,
    HOST_DISCOVERY_OPTION.JSON_PASSWD,
    HOST_DISCOVERY_OPTION.DISCOVER_CIM,
    HOST_DISCOVERY_OPTION.CIM_IMPL,
    HOST_DISCOVERY_OPTION.CIM_USERNAME,
    HOST_DISCOVERY_OPTION.CIM_PASSWORD,
    HOST_DISCOVERY_OPTION.CIM_NAMESPACE,
    HOST_DISCOVERY_OPTION.CIM_PORT,
    HOST_DISCOVERY_OPTION.DISCOVER_VM,
    HOST_DISCOVERY_OPTION.VM_USERNAME,
    HOST_DISCOVERY_OPTION.VM_PASSWORD,
    HOST_DISCOVERY_OPTION.JSON_PORT,
    HOST_DISCOVERY_OPTION.VM_PORT,
    HOST_DISCOVERY_OPTION.Application_Name_USER_NAME,
    HOST_DISCOVERY_OPTION.Application_Name_SERVER_ADDRESS,
    DEVICE_ENCLOSURE.NAME,
    DEVICE_ENCLOSURE.TYPE,
    DEVICE_ENCLOSURE.ICON,
    DEVICE_ENCLOSURE.OS,
    DEVICE_ENCLOSURE.APPLICATIONS,
    DEVICE_ENCLOSURE.DEPARTMENT,
    DEVICE_ENCLOSURE.CONTACT,
    DEVICE_ENCLOSURE.LOCATION,
    DEVICE_ENCLOSURE.DESCRIPTION,
    DEVICE_ENCLOSURE.COMMENT_,
    DEVICE_ENCLOSURE.IP_ADDRESS,
    DEVICE_ENCLOSURE.VENDOR,
    DEVICE_ENCLOSURE.MODEL,
    DEVICE_ENCLOSURE.SERIAL_NUMBER,
    DEVICE_ENCLOSURE.FIRMWARE,
    DEVICE_ENCLOSURE.USER_DEFINED_VALUE1,
    DEVICE_ENCLOSURE.USER_DEFINED_VALUE2,
    DEVICE_ENCLOSURE.USER_DEFINED_VALUE3,
    DEVICE_ENCLOSURE.HCM_AGENT_VERSION,
    DEVICE_ENCLOSURE.OS_VERSION,
    DEVICE_ENCLOSURE.CREATED_BY,
    DEVICE_ENCLOSURE.TRACK_CHANGES,
    DEVICE_ENCLOSURE.LAST_UPDATE_TIME,
    DEVICE_ENCLOSURE.LAST_UPDATE_MODULE,
    DEVICE_ENCLOSURE.TRUSTED,
    DEVICE_ENCLOSURE.CREATION_TIME,
    DEVICE_ENCLOSURE.MISSING,
    DEVICE_ENCLOSURE.MISSING_TIME,
    DEVICE_ENCLOSURE.HOST_NAME,
    DEVICE_ENCLOSURE.SYSLOG_REGISTERED,
    DEVICE_ENCLOSURE.VIRTUALIZATION,
    DEVICE_ENCLOSURE.MANAGED_ELEMENT_ID
from
    HOST_DISCOVERY_REQUEST
        join HOST_DISCOVERY_OPTION on
HOST_DISCOVERY_REQUEST.HOST_DISCOVERY_OPTION_ID = HOST_DISCOVERY_OPTION.ID
        left outer join DEVICE_ENCLOSURE on
HOST_DISCOVERY_REQUEST.DEVICE_ENCLOSURE_ID = DEVICE_ENCLOSURE.ID;
```

IFL_INFO

```
create or replace view IFL_INFO as
select
    IFL.ID as IFL_ID,
    IFL.EDGE_FABRIC_ID,
    (select distinct FCR_PORT.VIRTUAL_SWITCH_ID
        from SWITCH_PORT FCR_PORT
        where FCR_PORT.WWN = IFL.BB_PORT_WWN)
        as FCR_SWITCH_ID,
    IFL.EDGE_PORT_WWN,
    IFL.BB_FABRIC_ID,
    IFL.BB_PORT_WWN ,
    IFL.BB_RA_TOV,
    IFL.BB_ED_TOV,
    IFL.BB_PID_FORMAT,
    SWITCH_PORT.VIRTUAL_SWITCH_ID as EDGE_SWITCH_ID,
    SWITCH_PORT.ID as EDGE_PORT_ID,
    SWITCH_PORT.USER_PORT_NUMBER as EDGE_PORT_NUMBER,
    SWITCH_PORT.TYPE as EDGE_PORT_TYPE
from IFL
    left outer join SWITCH_PORT
        on IFL.EDGE_PORT_WWN = SWITCH_PORT.WWN;
```

ISL_INFO

```
create or replace view ISL_INFO as
select distinct
   ISL.ID,
   ISL.FABRIC_ID,
   ISL.COST,
   ISL.TYPE,
   ISL.SOURCE_DOMAIN_ID,
   ISL.SOURCE_PORT_NUMBER,
   ISL.MISSING,
   SOURCE_VIRTUAL_SWITCH.ID as SOURCE_SWITCH_ID,
   SOURCE_VIRTUAL_SWITCH.NAME as SOURCE_SWITCH_NAME,
   SOURCE_VIRTUAL_SWITCH.WWN as SOURCE_SWITCH_WWN,
    SOURCE_VIRTUAL_SWITCH.CORE_SWITCH_ID as SOURCE_CORE_SWITCH_ID,
    SOURCE_VIRTUAL_SWITCH.BASE_SWITCH as SOURCE_BASE_SWITCH,
    SOURCE_SWITCH_PORT.ID as SOURCE_SWITCH_PORT_ID,
   SOURCE_SWITCH_PORT.WWN as SOURCE_SWITCH_PORT_WWN,
   SOURCE_SWITCH_PORT.NAME as SOURCE_SWITCH_PORT_NAME,
    SOURCE_SWITCH_PORT.TYPE as PORT_TYPE,
    SOURCE_SWITCH_PORT.KIND as SOURCE_SWITCH_PORT_KIND,
    SOURCE_SWITCH_PORT.PHYSICAL_PORT as SOURCE_PHYSICAL_PORT,
    SOURCE_SWITCH_PORT.TRUNKED as SOURCE_SWITCH_PORT_TRUNKED,
    ISL.DEST_DOMAIN_ID,
   ISL.DEST_PORT_NUMBER,
   DEST_VIRTUAL_SWITCH.ID as DEST_SWITCH_ID,
   DEST_VIRTUAL_SWITCH.NAME as DEST_SWITCH_NAME,
    DEST_VIRTUAL_SWITCH.WWN as DEST_SWITCH_WWN,
    DEST_VIRTUAL_SWITCH.CORE_SWITCH_ID as DEST_CORE_SWITCH_ID,
    DEST_VIRTUAL_SWITCH.BASE_SWITCH as DEST_BASE_SWITCH,
   DEST_SWITCH_PORT.ID as DEST_SWITCH_PORT_ID,
   DEST_SWITCH_PORT.WWN as DEST_SWITCH_PORT_WWN,
    DEST_SWITCH_PORT.NAME as DEST_SWITCH_PORT_NAME,
    DEST_SWITCH_PORT.KIND as DEST_SWITCH_PORT_KIND,
    DEST_SWITCH_PORT.PHYSICAL_PORT as DEST_PHYSICAL_PORT,
    DEST_SWITCH_PORT.TRUNKED as DEST_SWITCH_PORT_TRUNKED,
    FABRIC.PRINCIPAL_SWITCH_WWN as PRINCIPAL_SWITCH_WWN
from
   ISL,
    FABRIC_MEMBER SOURCE_FABRIC_MEMBER,
    VIRTUAL_SWITCH         SOURCE_VIRTUAL_SWITCH,
    SWITCH_PORT   SOURCE_SWITCH_PORT,
    FABRIC_MEMBER DEST_FABRIC_MEMBER,
    VIRTUAL_SWITCH         DEST_VIRTUAL_SWITCH,
    SWITCH_PORT   DEST_SWITCH_PORT,
    FABRIC
where
   SOURCE_FABRIC_MEMBER.FABRIC_ID = ISL.FABRIC_ID and
   SOURCE_VIRTUAL_SWITCH.ID = SOURCE_FABRIC_MEMBER.VIRTUAL_SWITCH_ID and
   SOURCE_VIRTUAL_SWITCH.DOMAIN_ID = ISL.SOURCE_DOMAIN_ID and
   SOURCE_SWITCH_PORT.VIRTUAL_SWITCH_ID = SOURCE_VIRTUAL_SWITCH.ID and
    SOURCE_SWITCH_PORT.CATEGORY = 1 and
   SOURCE_SWITCH_PORT.USER_PORT_NUMBER = ISL.SOURCE_PORT_NUMBER and
   DEST_FABRIC_MEMBER.FABRIC_ID = ISL.FABRIC_ID and
   DEST_VIRTUAL_SWITCH.ID = DEST_FABRIC_MEMBER.VIRTUAL_SWITCH_ID and
   DEST_VIRTUAL_SWITCH.DOMAIN_ID = ISL.DEST_DOMAIN_ID and
   DEST_SWITCH_PORT.VIRTUAL_SWITCH_ID = DEST_VIRTUAL_SWITCH.ID and
    DEST_SWITCH_PORT.CATEGORY = 1 and
   DEST_SWITCH_PORT.USER_PORT_NUMBER = ISL.DEST_PORT_NUMBER and
    FABRIC.ID = ISL.FABRIC_ID;
```

ISL_TRUNK_INFO

```
create or replace view ISL_TRUNK_INFO as
select
    ISL_TRUNK_GROUP.ID,
    ISL_INFO.COST,
    ISL_INFO.TYPE,
    ISL_INFO.SOURCE_PORT_NUMBER,
    ISL_INFO.SOURCE_SWITCH_ID,
    SOURCE_CORE_SWITCH.IP_ADDRESS as SOURCE_SWITCH_IP_ADDRESS,
    SOURCE_VIRTUAL_SWITCH.WWN as SOURCE_SWITCH_WWN,
    ISL_INFO.SOURCE_DOMAIN_ID as MASTER_PORT,
    ISL_INFO.SOURCE_SWITCH_NAME,
    ISL_INFO.SOURCE_SWITCH_PORT_ID,
    ISL_INFO.DEST_PORT_NUMBER,
    ISL_INFO.DEST_SWITCH_ID,
    DEST_CORE_SWITCH.IP_ADDRESS as DEST_SWITCH_IP_ADDRESS,
    DEST_VIRTUAL_SWITCH.WWN as DEST_SWITCH_WWN,
    ISL_INFO.SOURCE_SWITCH_PORT_WWN,
    ISL_INFO.DEST_DOMAIN_ID as REMOTE_MASTER_PORT,
    ISL_INFO.DEST_SWITCH_NAME,
    ISL_INFO.DEST_SWITCH_PORT_ID
 from
    ISL_TRUNK_GROUP,
    ISL_INFO,
    CORE_SWITCH SOURCE_CORE_SWITCH,
    CORE_SWITCH DEST_CORE_SWITCH,
    VIRTUAL_SWITCH SOURCE_VIRTUAL_SWITCH,
    VIRTUAL_SWITCH DEST_VIRTUAL_SWITCH
where
    ISL_INFO.SOURCE_SWITCH_ID = ISL_TRUNK_GROUP.VIRTUAL_SWITCH_ID
    and ISL_INFO.SOURCE_PORT_NUMBER = ISL_TRUNK_GROUP.MASTER_USER_PORT
    and ISL_INFO.SOURCE_SWITCH_ID = SOURCE_VIRTUAL_SWITCH.ID
    and SOURCE_VIRTUAL_SWITCH.CORE_SWITCH_ID = SOURCE_CORE_SWITCH.ID
    and ISL_INFO.DEST_SWITCH_ID = DEST_VIRTUAL_SWITCH.ID
    and DEST_VIRTUAL_SWITCH.CORE_SWITCH_ID = DEST_CORE_SWITCH.ID;
```

NPORT_WWN_MAP_INFO

This view provides a consolidation between Nport WWN map and AG"s N and F ports. It considers only those N-Ports that are currently occupied i.e. having non-empty remote port wwn. This is required because NPort-WWN mapping might exist for NPorts that are not yet online and if a device is connected to AG through some F-Port that is mapped to some other N-Port that is online then AG will use that mapping.

```
create or replace view NPORT_WWN_MAP_INFO as
select
    NPORT_WWN_MAP.VIRTUAL_SWITCH_ID,
    NPORT_WWN_MAP.N_PORT,
    NPORT_WWN_MAP.DEVICE_PORT_WWN,
    AG_N_PORT.REMOTE_PORT_WWN as EDGE_SWITCH_PORT_WWN,
    AG_F_PORT.USER_PORT_NUMBER as F_PORT,
    AG_F_PORT.WWN as AG_F_PORT_WWN,
    AG_F_PORT.REMOTE_NODE_WWN
from
    NPORT_WWN_MAP,
    SWITCH_PORT AG_N_PORT,
    SWITCH_PORT AG_F_PORT
where
    NPORT_WWN_MAP.VIRTUAL_SWITCH_ID = AG_N_PORT.VIRTUAL_SWITCH_ID
    and NPORT_WWN_MAP.N_PORT = AG_N_PORT.USER_PORT_NUMBER
    and NPORT_WWN_MAP.VIRTUAL_SWITCH_ID =  AG_F_PORT.VIRTUAL_SWITCH_ID
    and NPORT_WWN_MAP.DEVICE_PORT_WWN = AG_F_PORT.REMOTE_PORT_WWN;
```

PHANTOM_PORT_INFO

```
create or replace view PHANTOM_PORT_INFO as
select
    PHANTOM_PORT.ID,
    PHANTOM_PORT.WWN,
    PHANTOM_PORT.VIRTUAL_SWITCH_ID,
    PHANTOM_PORT.PORT_NUMBER,
    PHANTOM_PORT.PORT_ID,
    PHANTOM_PORT.SPEED,
    PHANTOM_PORT.MAX_SPEED,
    PHANTOM_PORT.TYPE,
    PHANTOM_PORT.REMOTE_NODE_WWN,
    PHANTOM_PORT.REMOTE_PORT_WWN,
    PHANTOM_PORT.PHANTOM_TYPE,
    PHANTOM_PORT.BB_FABRIC_ID,
    VIRTUAL_SWITCH.WWN as VIRTUAL_SWITCH_WWN
from
    PHANTOM_PORT,
    VIRTUAL_SWITCH
where
    PHANTOM_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID;
```

PORT_BOTTLENECK_CONF_INFO

This view provides combine port bottleneck configuration and enough information from switch port for the client to identify the port.

```
create or replace view PORT_BOTTLENECK_CONF_INFO as
select
    PORT_BOTTLENECK_CONFIG.SWITCH_PORT_ID,
    PORT_BOTTLENECK_CONFIG.BOTTLENECK_DETECT_ENABLED,
    PORT_BOTTLENECK_CONFIG.ALERTS_ENABLED,
    PORT_BOTTLENECK_CONFIG.CONGESTION_THRESHOLD,
    PORT_BOTTLENECK_CONFIG.LATENCY_THRESHOLD,
    PORT_BOTTLENECK_CONFIG.WINDOW_,
    PORT_BOTTLENECK_CONFIG.QUIET_TIME,
    PORT_BOTTLENECK_CONFIG.CREATION_TIME,
    PORT_BOTTLENECK_CONFIG.LAST_UPDATE_TIME,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.TYPE,
    SWITCH_PORT.WWN
  from
    PORT_BOTTLENECK_CONFIG
        left outer join SWITCH_PORT
            on PORT_BOTTLENECK_CONFIG.SWITCH_PORT_ID = SWITCH_PORT.ID;
```

PORT_BOTTLENECK_STAT_INFO

This view provides combine port bottleneck status and enough information from the switch port for the client to identify the port.

```
create or replace view PORT_BOTTLENECK_STAT_INFO as
select
    PORT_BOTTLENECK_STATUS.SWITCH_PORT_ID,
    PORT_BOTTLENECK_STATUS.STATUS,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.TYPE
  from
    PORT_BOTTLENECK_STATUS
        left outer join SWITCH_PORT
            on PORT_BOTTLENECK_STATUS.SWITCH_PORT_ID = SWITCH_PORT.ID;
```

PORT_GROUP_INFO

```
create or replace view PORT_GROUP_INFO as
select
    SWITCH_PORT.ID as PORT_ID,
    SWITCH_PORT.NAME as SWITCH_PORT_NAME,
    SWITCH_PORT.WWN,
    SWITCH_PORT.HEALTH,
    SWITCH_PORT.STATUS,
    SWITCH_PORT.PORT_NUMBER,
    SWITCH_PORT.SLOT_NUMBER,
    SWITCH_PORT.FICON_SUPPORTED,
    SWITCH_PORT.STATE,
    SWITCH_PORT.USER_PORT_NUMBER,
    VIRTUAL_SWITCH.NAME as VIRTUAL_SWITCH_NAME,
    VIRTUAL_SWITCH.ID as SWITCH_ID,
    FABRIC.NAME as FABRIC_NAME,
    FABRIC.MANAGED as FABRIC_MANAGED,
    PORT_GROUP.ID as PORT_GROUP_ID,
    PORT_GROUP_MEMBER.ID as PORT_GROUP_MEMBER_ID
from
    SWITCH_PORT, VIRTUAL_SWITCH, FABRIC, FABRIC_MEMBER, PORT_GROUP_MEMBER,
PORT_GROUP
where
    VIRTUAL_SWITCH .ID = SWITCH_PORT.VIRTUAL_SWITCH_ID and
    FABRIC_MEMBER.VIRTUAL_SWITCH_ID = SWITCH_PORT.VIRTUAL_SWITCH_ID and
    FABRIC_MEMBER.FABRIC_ID = FABRIC.ID and
    SWITCH_PORT.ID = PORT_GROUP_MEMBER.SWITCH_PORT_ID and
    PORT_GROUP_MEMBER.PORT_GROUP_ID = PORT_GROUP.ID;
```

ROLE_PRIVILEGE_INFO

```
create or replace view ROLE_PRIVILEGE_INFO as
select
    ROLE.ID,
    ROLE.NAME as ROLE_NAME,
    ROLE.DESCRIPTION as ROLE_DESCRIPTION,
    ROLE.HIDDEN as ROLE_HIDDEN,
    PRIVILEGE.ID as PRIVILEGE_ID,
    PRIVILEGE.NAME as PRIVILEGE_NAME,
    PRIVILEGE.AREA as PRIVILEGE_AREA,
    ROLE_PRIVILEGE_MAP.PERMISSION
from
    ROLE,
    ROLE_PRIVILEGE_MAP,
    PRIVILEGE
where
    ROLE.ID = ROLE_PRIVILEGE_MAP.ROLE_ID and
    PRIVILEGE.ID = ROLE_PRIVILEGE_MAP.PRIVILEGE_ID;
```

SCOM_EE_MONITOR_INFO

This view provides combined ee_monitor, ee_monitor_stats, device_port and device_node tables to get the EE Monitor information for SCOM plug-in.

```
create or replace view SCOM_EE_MONITOR_INFO as
select distinct
    EE_MONITOR.NAME,
    EE_MONITOR.SWITCH_PORT_ID,
    EE_MONITOR.SOURCE_PORT_ID,
    EE_MONITOR.DEST_PORT_ID,
    EE_MONITOR_STATS.TX,
    EE_MONITOR_STATS.RX,
    EE_MONITOR_STATS.CRCERRORS,
    EE_MONITOR_STATS.CREATION_TIME,
    SOURCE_PORT.PORT_ID as SID,
    DEST_PORT.PORT_ID as DID,
    SOURCE_NODE.WWN as SOURCE_DEVICE_WWN,
    SOURCE_PORT.WWN as SOURCE_PORT_WWN,
    DEST_NODE.WWN as DEST_DEVICE_WWN,
    DEST_PORT.WWN as DEST_PORT_WWN,
    SOURCE_NODE.FABRIC_ID as SOURCE_FABRIC_ID,
    DEST_NODE.FABRIC_ID as DEST_FABRIC_ID,
    SOURCE_PORT.DOMAIN_ID as SOURCE_SWITCH_DOMAIN_ID,
    DEST_PORT.DOMAIN_ID as DEST_SWITCH_DOMAIN_ID
from
    DEVICE_PORT as SOURCE_PORT,
    DEVICE_PORT as DEST_PORT,
    DEVICE_NODE as DEST_NODE,
    DEVICE_NODE as SOURCE_NODE,
    EE_MONITOR,
    EE_MONITOR_STATS
where
    SOURCE_PORT.ID = EE_MONITOR.SOURCE_PORT_ID
    and EE_MONITOR.ID = EE_MONITOR_STATS.EE_MONITOR_ID
    and SOURCE_PORT.NODE_ID = SOURCE_NODE.ID
    and DEST_PORT.ID = EE_MONITOR.DEST_PORT_ID
    and DEST_PORT.NODE_ID = DEST_NODE.ID
    and EE_MONITOR_STATS.CREATION_TIME in (
        select MAX(CREATION_TIME)
        from EE_MONITOR_STATS
        group by EE_MONITOR_ID);
```

SENSOR_INFO

```
create or replace view SENSOR_INFO as
select
    SENSOR.ID,
    SENSOR.CORE_SWITCH_ID,
    SENSOR.SENSOR_ID,
    SENSOR.CURRENT_READING,
    SENSOR.TYPE,
    SENSOR.SUB_TYPE,
    SENSOR.DESCRIPTION,
    SENSOR.STATUS,
    SENSOR.OPERATIONAL_STATUS,
    SENSOR.PART_NUMBER,
    SENSOR.SERIAL_NUMBER,
    SENSOR.VERSION,
    SENSOR.CREATION_TIME,
    SENSOR.LAST_UPDATE_TIME,
    SENSOR.FRU_TYPE,
    SENSOR.UNIT_NUMBER,
    SENSOR.STATE,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    VIRTUAL_SWITCH.SWITCH_MODE as VIRTUAL_SWITCH_MODE
from
    SENSOR,
    CORE_SWITCH,
    VIRTUAL_SWITCH
where
    SENSOR.CORE_SWITCH_ID = CORE_SWITCH.ID and
    SENSOR.CORE_SWITCH_ID = VIRTUAL_SWITCH.CORE_SWITCH_ID;
```

SMART_CARD_USAGE_INFO

```
create or replace view SMART_CARD_USAGE_INFO as
select
    SC.ID SMART_CARD_ID,
    SC.CARD_TYPE,
    SC.CARD_INFO,
    SC.CARDCN_ID,
    SC.FIRST_NAME,
    SC.LAST_NAME,
    SC.NOTES,
    SC.CREATION_TIME,
    -1 ENGINE_ID,
    EG.ID ENCRYPTION_GROUP_ID,
    EG.NAME GROUP_NAME,
    -1 CARD_POSITION,
    -1 CRYPTO_SWITCH_ID,
    -1 SLOT_NUMBER
from
    SMART_CARD SC,
    ENCRYPTION_GROUP EG,
    QUORUM_CARD_GROUP_MAPPING QCGM
where
    QCGM.SMART_CARD_ID = SC.ID
    and EG.ID = QCGM.ENCRYPTION_GROUP_ID
    and SC.CARD_TYPE = 0
union
select
    SC.ID SMART_CARD_ID,
    SC.CARD_TYPE,
    SC.CARD_INFO,
    SC.CARDCN_ID,
    SC.FIRST_NAME,
    SC.LAST_NAME,
    SC.NOTES,
    SC.CREATION_TIME,
    -1 ENGINE_ID,
    EG.ID ENCRYPTION_GROUP_ID,
    EG.NAME GROUP_NAME,
    RCGM.POSITION_ CARD_POSITION,
    -1 CRYPTO_SWITCH_ID,
    -1 SLOT_NUMBER
from
```

```
    SMART_CARD SC,
    ENCRYPTION_GROUP EG,
    RECOVERY_CARD_GROUP_MAPPING RCGM
where
    SC.ID = RCGM.SMART_CARD_ID
    and EG.ID = RCGM.ENCRYPTION_GROUP_ID
    and SC.CARD_TYPE = 1
union
select
    SC.ID SMART_CARD_ID,
    SC.CARD_TYPE,
    SC.CARD_INFO,
    SC.CARDCN_ID,
    SC.FIRST_NAME,
    SC.LAST_NAME,
    SC.NOTES,
    SC.CREATION_TIME,
    EE.ID ENGINE_ID,
    -1 ENCRYPTION_GROUP_ID,
    '' GROUP_NAME,
    -1 CARD_POSITION,
    EE.SWITCH_ID CRYPTO_SWITCH_ID,
    EE.SLOT_NUMBER SLOT_NUMBER
from
    SMART_CARD SC,
    ENCRYPTION_ENGINE EE,
    SYSTEM_CARD_ENGINE_MAPPING SCEM
where
    SC.ID = SCEM.SMART_CARD_ID
    and EE.ID = SCEM.ENCRYPTION_ENGINE_ID
    and SC.CARD_TYPE = 2;
```

SWITCH_DETAILS_INFO

```
create or replace view SWITCH_DETAILS_INFO as
select
    CORE_SWITCH.ID as PHYSICAL_SWITCH_ID,
    CORE_SWITCH.NAME as PHYSICAL_SWITCH_NAME,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    CORE_SWITCH.OPERATIONAL_STATUS as PHYSICAL_OPERATIONAL_STATUS,
    CORE_SWITCH.TYPE,
    CORE_SWITCH.MAX_VIRTUAL_SWITCHES,
    CORE_SWITCH.FIRMWARE_VERSION,
    CORE_SWITCH.VENDOR,
    CORE_SWITCH.REACHABLE,
    CORE_SWITCH.UNREACHABLE_TIME,
    CORE_SWITCH.MODEL,
    CORE_SWITCH.SYSLOG_REGISTERED,
    CORE_SWITCH.SNMP_REGISTERED,
    CORE_SWITCH.USER_IP_ADDRESS,
    CORE_SWITCH.MANAGING_SERVER_IP_ADDRESS,
    CORE_SWITCH.CREATION_TIME as CS_CREATION_TIME,
    CORE_SWITCH.LAST_UPDATE_TIME as CS_LAST_UPDATE_TIME,
    CORE_SWITCH.NUM_VIRTUAL_SWITCHES,
    CORE_SWITCH.VF_ENABLED,
    CORE_SWITCH.VF_SUPPORTED,
    CORE_SWITCH.CALL_HOME_ENABLED,
    CORE_SWITCH.MANAGED_ELEMENT_ID as CORE_MANAGED_ELEMENT_ID,
    CORE_SWITCH.NAT_PRIVATE_IP_ADDRESS,
    CORE_SWITCH.ALTERNATE_IP_ADDRESS,
    VIRTUAL_SWITCH.ID,
    VIRTUAL_SWITCH.NAME,
    VIRTUAL_SWITCH.OPERATIONAL_STATUS,
    VIRTUAL_SWITCH.SWITCH_MODE,
    VIRTUAL_SWITCH.AD_CAPABLE,
    VIRTUAL_SWITCH.WWN,
    VIRTUAL_SWITCH.ROLE,
    VIRTUAL_SWITCH.FCS_ROLE,
    VIRTUAL_SWITCH.DOMAIN_ID,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
    VIRTUAL_SWITCH.BASE_SWITCH,
    VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE,
    VIRTUAL_SWITCH.CREATION_TIME,
    VIRTUAL_SWITCH.LAST_UPDATE_TIME,
    VIRTUAL_SWITCH.USER_NAME,
    VIRTUAL_SWITCH.PASSWORD,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.STATE,
    VIRTUAL_SWITCH.STATUS,
    VIRTUAL_SWITCH.STATUS_REASON,
    VIRTUAL_SWITCH.FABRIC_IDID_MODE,
    VIRTUAL_SWITCH.LOGICAL_ID,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_1,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_2,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_3,
    VIRTUAL_SWITCH.FMS_MODE,
    VIRTUAL_SWITCH.DYNAMIC_LOAD_SHARING,
    VIRTUAL_SWITCH.PORT_BASED_ROUTING,
    VIRTUAL_SWITCH.IN_ORDER_DELIVERY,
    VIRTUAL_SWITCH.INSISTENT_DID_MODE,
    VIRTUAL_SWITCH.FCR_CAPABLE,
    VIRTUAL_SWITCH.LAST_PORT_MEMBERSHIP_CHANGE,
    VIRTUAL_SWITCH.FCIP_CIRCUIT_CAPABLE,
    VIRTUAL_SWITCH.MAX_FCIP_TUNNELS,
    VIRTUAL_SWITCH.MAX_FCIP_CIRCUITS,
    VIRTUAL_SWITCH.FCIP_LICENSED,
    VIRTUAL_SWITCH.MANAGED_ELEMENT_ID,
    FABRIC_MEMBER.FABRIC_ID,
    FABRIC_MEMBER.TRUSTED,
    FABRIC_MEMBER.MISSING,
    FABRIC_MEMBER.MISSING_TIME,
    CORE_SWITCH_DETAILS.ETHERNET_MASK,
    CORE_SWITCH_DETAILS.FC_MASK,
    CORE_SWITCH_DETAILS.FC_IP,
    CORE_SWITCH_DETAILS.FC_CERTIFICATE,
    CORE_SWITCH_DETAILS.SW_LICENSE_ID,
    CORE_SWITCH_DETAILS.SUPPLIER_SERIAL_NUMBER,
    CORE_SWITCH_DETAILS.PART_NUMBER,
    CORE_SWITCH_DETAILS.CHECK_BEACON,
    CORE_SWITCH_DETAILS.TIMEZONE,
    CORE_SWITCH_DETAILS.MAX_PORT,
    CORE_SWITCH_DETAILS.CHASSIS_SERVICE_TAG,
    CORE_SWITCH_DETAILS.BAY_ID,
    CORE_SWITCH_DETAILS.TYPE_NUMBER,
    CORE_SWITCH_DETAILS.MODEL_NUMBER,
    CORE_SWITCH_DETAILS.MANUFACTURER,
    CORE_SWITCH_DETAILS.PLANT_OF_MANUFACTURER,
    CORE_SWITCH_DETAILS.SEQUENCE_NUMBER,
    CORE_SWITCH_DETAILS.TAG,
    CORE_SWITCH_DETAILS.ACT_CP_PRI_FW_VERSION,
    CORE_SWITCH_DETAILS.ACT_CP_SEC_FW_VERSION,
    CORE_SWITCH_DETAILS.STBY_CP_PRI_FW_VERSION,
    CORE_SWITCH_DETAILS.STBY_CP_SEC_FW_VERSION,
    CORE_SWITCH_DETAILS.TYPE as DETAILS_TYPE,
    CORE_SWITCH_DETAILS.EGM_CAPABLE,
    CORE_SWITCH_DETAILS.SUB_TYPE,
    CORE_SWITCH_DETAILS.PARTITION,
    CORE_SWITCH_DETAILS.MAX_NUM_OF_BLADES,
    CORE_SWITCH_DETAILS.SNMP_INFORMS_ENABLED,
    CORE_SWITCH_DETAILS.VENDOR_VERSION,
    CORE_SWITCH_DETAILS.VENDOR_PART_NUMBER,
    CORE_SWITCH_DETAILS.CONTACT,
    CORE_SWITCH_DETAILS.LOCATION,
    CORE_SWITCH_DETAILS.DESCRIPTION,
    CORE_SWITCH_DETAILS.RNID_SEQUENCE_NUMBER,
    CORE_SWITCH_DETAILS.FIRMWARE_VERSION as CSD_FIRMWARE_VERSION
from
    CORE_SWITCH,
    VIRTUAL_SWITCH,
    FABRIC_MEMBER,
    CORE_SWITCH_DETAILS
where
    VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
    and FABRIC_MEMBER.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and CORE_SWITCH_DETAILS.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

SWITCH_PORT_INFO

```
create or replace view SWITCH_PORT_INFO as
select
    SWITCH_PORT.ID,
    SWITCH_PORT.VIRTUAL_SWITCH_ID,
    SWITCH_PORT.WWN,
    SWITCH_PORT.NAME,
    SWITCH_PORT.SLOT_NUMBER,
    SWITCH_PORT.PORT_NUMBER,
    SWITCH_PORT.USER_PORT_NUMBER,
    SWITCH_PORT.PORT_ID,
    SWITCH_PORT.PORT_INDEX,
    SWITCH_PORT.AREA_ID,
    SWITCH_PORT.MAC_ADDRESS,
    SWITCH_PORT.PORT_MOD,
    SWITCH_PORT.TYPE,
    SWITCH_PORT.FULL_TYPE,
    SWITCH_PORT.STATUS,
    SWITCH_PORT.HEALTH,
    SWITCH_PORT.STATUS_MESSAGE,
    SWITCH_PORT.PHYSICAL_PORT,
    SWITCH_PORT.LOCKED_PORT_TYPE,
    SWITCH_PORT.CATEGORY,
    SWITCH_PORT.PROTOCOL,
    SWITCH_PORT.SPEED,
    SWITCH_PORT.SPEEDS_SUPPORTED,
    SWITCH_PORT.MAX_PORT_SPEED,
    SWITCH_PORT.DESIRED_CREDITS,
    SWITCH_PORT.BUFFER_ALLOCATED,
    SWITCH_PORT.ESTIMATED_DISTANCE,
    SWITCH_PORT.ACTUAL_DISTANCE,
    SWITCH_PORT.LONG_DISTANCE_SETTING,
    SWITCH_PORT.DEGRADED_PORT,
    SWITCH_PORT.REMOTE_NODE_WWN,
    SWITCH_PORT.REMOTE_PORT_WWN,
    SWITCH_PORT.LICENSED,
    SWITCH_PORT.SWAPPED,
    SWITCH_PORT.TRUNKED,
    SWITCH_PORT.TRUNK_MASTER,
    SWITCH_PORT.PERSISTENT_DISABLE,
    SWITCH_PORT.FICON_SUPPORTED,
    SWITCH_PORT.BLOCKED,
    SWITCH_PORT.PROHIBIT_PORT_NUMBERS,
    SWITCH_PORT.PROHIBIT_PORT_COUNT,
    SWITCH_PORT.NPIV,
    SWITCH_PORT.NPIV_CAPABLE,
    SWITCH_PORT.NPIV_ENABLED,
    SWITCH_PORT.FC_FAST_WRITE_ENABLED,
    SWITCH_PORT.ISL_RRDY_ENABLED,
    SWITCH_PORT.RATE_LIMIT_CAPABLE,
    SWITCH_PORT.RATE_LIMITED,
    SWITCH_PORT.QOS_CAPABLE,
    SWITCH_PORT.QOS_ENABLED,
    SWITCH_PORT.TUNNEL_CONFIGURED,
    SWITCH_PORT.FCIP_TUNNEL_UP,
    SWITCH_PORT.FCR_FABRIC_ID,
    SWITCH_PORT.FCR_INTEROP_MODE,
    SWITCH_PORT.CALCULATED_STATUS,
    SWITCH_PORT.USER_DEFINED_VALUE1,
    SWITCH_PORT.USER_DEFINED_VALUE2,
    SWITCH_PORT.USER_DEFINED_VALUE3,
    SWITCH_PORT.KIND,
    SWITCH_PORT.STATE,
    SWITCH_PORT.PREVIOUS_STATUS,
    SWITCH_PORT.LAST_UPDATE,
    SWITCH_PORT.OCCUPIED,
    SWITCH_PORT.PORT_BIT_MASK,
    SWITCH_PORT.LOGICAL_PORT_NUMBER,
    SWITCH_PORT.DEFAULT_AREA_ID,
    SWITCH_PORT.LOGICAL_PORT_WWN,
    SWITCH_PORT.LATENCY_DETECT_SUPPORTED,
    SWITCH_PORT.EPORT_DISABLED,
    SWITCH_PORT.SPEED_NEGOTIATED,
    VIRTUAL_SWITCH.WWN as VIRTUAL_SWITCH_WWN,
    VIRTUAL_SWITCH.ROLE as SWITCH_ROLE,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID as VIRTUAL_FABRIC_ID,
    VIRTUAL_SWITCH.DOMAIN_ID as DOMAIN_ID,
    VIRTUAL_SWITCH.INTEROP_MODE as INTEROP_MODE,
    CORE_SWITCH.TYPE as SWITCH_TYPE,
    CORE_SWITCH.FIRMWARE_VERSION as FIRMWARE_VERSION,
    CORE_SWITCH.IP_ADDRESS as IP_ADDRESS,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    CORE_SWITCH.MODEL as SWITCH_MODEL,
    CORE_SWITCH_DETAILS.MODEL_NUMBER as SWITCH_MODEL_NUMBER
from
    SWITCH_PORT, CORE_SWITCH, VIRTUAL_SWITCH, CORE_SWITCH_DETAILS
where
    SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID and
    VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID and
    CORE_SWITCH_DETAILS.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

SWITCH_SNMP_INFO

```
create or replace view SWITCH_SNMP_INFO as
select
    CORE_SWITCH.ID as PHYSICAL_SWITCH_ID,
    CORE_SWITCH.NAME as PHYSICAL_SWITCH_NAME,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    CORE_SWITCH.OPERATIONAL_STATUS as PHYSICAL_OPERATIONAL_STATUS,
    CORE_SWITCH.TYPE,
    CORE_SWITCH.MAX_VIRTUAL_SWITCHES,
    CORE_SWITCH.FIRMWARE_VERSION,
    CORE_SWITCH.VENDOR,
    CORE_SWITCH.REACHABLE,
    CORE_SWITCH.UNREACHABLE_TIME,
    CORE_SWITCH.MODEL,
    CORE_SWITCH_DETAILS.CONTACT,
    CORE_SWITCH_DETAILS.LOCATION,
    CORE_SWITCH_DETAILS.DESCRIPTION,
    VIRTUAL_SWITCH.ID,
    VIRTUAL_SWITCH.NAME,
    VIRTUAL_SWITCH.OPERATIONAL_STATUS,
    VIRTUAL_SWITCH.SWITCH_MODE,
    VIRTUAL_SWITCH.AD_CAPABLE,
    VIRTUAL_SWITCH.FCIP_CAPABLE,
    VIRTUAL_SWITCH.WWN,
    VIRTUAL_SWITCH.ROLE,
    VIRTUAL_SWITCH.FCS_ROLE,
    VIRTUAL_SWITCH.DOMAIN_ID,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
    VIRTUAL_SWITCH.BASE_SWITCH,
    VIRTUAL_SWITCH.MAX_ZONE_CONFIG_SIZE,
    VIRTUAL_SWITCH.CREATION_TIME,
    VIRTUAL_SWITCH.LAST_UPDATE_TIME,
    VIRTUAL_SWITCH.USER_NAME,
    VIRTUAL_SWITCH.PASSWORD,
    VIRTUAL_SWITCH.MANAGEMENT_STATE,
    VIRTUAL_SWITCH.STATE,
    VIRTUAL_SWITCH.STATUS,
    VIRTUAL_SWITCH.STATUS_REASON,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_1,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_2,
    VIRTUAL_SWITCH.USER_DEFINED_VALUE_3,
    FABRIC_MEMBER.FABRIC_ID,
    FABRIC_MEMBER.TRUSTED,
    FABRIC_MEMBER.MISSING,
    FABRIC_MEMBER.MISSING_TIME,
    coalesce(SNMP_CREDENTIALS.PORT_NUMBER, (select SNMP_PROFILE.PORT_NUMBER from 
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_PORT_NUMBER,
    coalesce(SNMP_CREDENTIALS.RETRY_COUNT, (select SNMP_PROFILE.RETRY_COUNT from 
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_RETRY_COUNT,
    coalesce(SNMP_CREDENTIALS.TIMEOUT, (select SNMP_PROFILE.TIMEOUT from 
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_TIMEOUT,
    coalesce(SNMP_CREDENTIALS.VERSION, (select SNMP_PROFILE.VERSION from 
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_VERSION,
    coalesce(SNMP_CREDENTIALS.READ_COMMUNITY_STRING, (select 
SNMP_PROFILE.READ_COMMUNITY_STRING from SNMP_PROFILE where 
SNMP_PROFILE.NAME='default')) as SNMP_READ_COMMUNITY_STRING,
    coalesce(SNMP_CREDENTIALS.WRITE_COMMUNITY_STRING, (select
SNMP_PROFILE.WRITE_COMMUNITY_STRING from SNMP_PROFILE where
SNMP_PROFILE.NAME='default')) as SNMP_WRITE_COMMUNITY_STRING,
    coalesce(SNMP_CREDENTIALS.USER_NAME, (select SNMP_PROFILE.USER_NAME from
SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_USER_NAME,
    coalesce(SNMP_CREDENTIALS.CONTEXT_NAME, (select SNMP_PROFILE.CONTEXT_NAME
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_CONTEXT_NAME,
    coalesce(SNMP_CREDENTIALS.AUTH_PROTOCOL, (select SNMP_PROFILE.AUTH_PROTOCOL
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_AUTH_PROTOCOL,
    coalesce(SNMP_CREDENTIALS.AUTH_PASSWORD, (select SNMP_PROFILE.AUTH_PASSWORD
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_AUTH_PASSWORD,
    coalesce(SNMP_CREDENTIALS.PRIV_PROTOCOL, (select SNMP_PROFILE.PRIV_PROTOCOL
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_PRIV_PROTOCOL,
    coalesce(SNMP_CREDENTIALS.PRIV_PASSWORD, (select SNMP_PROFILE.PRIV_PASSWORD
from SNMP_PROFILE where SNMP_PROFILE.NAME='default')) as SNMP_PRIV_PASSWORD,
    coalesce(SNMP_CREDENTIALS.SNMP_INFORMS_ENABLED, (select
SNMP_PROFILE.SNMP_INFORMS_ENABLED from SNMP_PROFILE where
SNMP_PROFILE.NAME='default')) as SNMP_INFORMS_ENABLED
from
    VIRTUAL_SWITCH
        left outer join CORE_SWITCH
            on VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
        left outer join CORE_SWITCH_DETAILS
            on CORE_SWITCH.ID = CORE_SWITCH_DETAILS.CORE_SWITCH_ID
        left outer join FABRIC_MEMBER
            on FABRIC_MEMBER.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
        left outer join SNMP_CREDENTIALS
            on VIRTUAL_SWITCH.ID = SNMP_CREDENTIALS.VIRTUAL_SWITCH_ID;
```

USER_ROLE_RESOURCE_INFO

```
create or replace view USER_ROLE_RESOURCE_INFO as
select
  RESOURCE_GROUP.ID RESOURCE_GROUP_ID,
  RESOURCE_GROUP.NAME RESOURCE_GROUP_NAME,
  ROLE.ID ROLE_ID,
  ROLE.NAME ROLE_NAME,
  USER_.NAME USER_NAME
from
  USER_,
  RESOURCE_GROUP,
  ROLE,
  USER_RESOURCE_MAP,
  USER_ROLE_MAP
where
  USER_ROLE_MAP.USER_NAME = USER_.NAME
  and USER_ROLE_MAP.ROLE_ID = ROLE.ID
  and USER_RESOURCE_MAP.RESOURCE_GROUP_ID = RESOURCE_GROUP.ID
  and USER_RESOURCE_MAP.USER_NAME = USER_.NAME;
```

VIRTUAL_FCOE_PORT_INFO

```
create or replace view VIRTUAL_FCOE_PORT_INFO as
select
    VIRTUAL_FCOE_PORT.ID,
    VIRTUAL_FCOE_PORT.VIRTUAL_SWITCH_ID,
    VIRTUAL_FCOE_PORT.PORT_WWN,
    VIRTUAL_FCOE_PORT.PORT_SPEED,
    VIRTUAL_FCOE_PORT.PORT_TYPE,
    VIRTUAL_FCOE_PORT.ENABLED,
    VIRTUAL_FCOE_PORT.STATUS,
    VIRTUAL_FCOE_PORT.TRUNK_INDEX,
    VIRTUAL_FCOE_PORT.PORT_NUMBER,
    VIRTUAL_FCOE_PORT.NAME,
    VIRTUAL_FCOE_PORT.SLOT_NUMBER,
    VIRTUAL_FCOE_PORT.VLAN_ID,
    VIRTUAL_FCOE_PORT.DEVICE_COUNT,
    VIRTUAL_FCOE_PORT.PEER_MAC,
    VIRTUAL_SWITCH.WWN as VIRTUAL_SWITCH_WWN,
    VIRTUAL_SWITCH.ROLE as SWITCH_ROLE,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID as VIRTUAL_FABRIC_ID,
    VIRTUAL_SWITCH.DOMAIN_ID as DOMAIN_ID,
    VIRTUAL_SWITCH.INTEROP_MODE as INTEROP_MODE,
    CORE_SWITCH.TYPE as SWITCH_TYPE,
    CORE_SWITCH.FIRMWARE_VERSION as FIRMWARE_VERSION,
    CORE_SWITCH.IP_ADDRESS as IP_ADDRESS,
    CORE_SWITCH.WWN as PHYSICAL_SWITCH_WWN,
    CORE_SWITCH.MODEL as SWITCH_MODEL,
    CORE_SWITCH_DETAILS.MODEL_NUMBER as SWITCH_MODEL_NUMBER
from
    VIRTUAL_FCOE_PORT, CORE_SWITCH, VIRTUAL_SWITCH, CORE_SWITCH_DETAILS
where
    VIRTUAL_FCOE_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID and
    VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID and
    CORE_SWITCH_DETAILS.CORE_SWITCH_ID = CORE_SWITCH.ID;
```

VM_CONNECTIVITY_INFO

This view provides combine fabric and VM information to derive end to end connectivity information for the VM.

```
create or replace view VM_CONNECTIVITY_INFO as
select
    DEVICE_PORT.SWITCH_PORT_WWN,
    DEVICE_PORT.DOMAIN_ID,
    DEVICE_PORT.NUMBER,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.NAME as CORE_NAME,
    VM_CONNECTIVITY.ID,
    VM_CONNECTIVITY.VCENTER_ID,
    VM_CONNECTIVITY.HYPERVISOR_HOST,
    VM_CONNECTIVITY.VM_NAME,
    VM_CONNECTIVITY.PATH_NAME,
    VM_CONNECTIVITY.ADAPTER_PORT_WWN,
    VM_CONNECTIVITY.TARGET_PORT_WWN,
    VM_CONNECTIVITY.LUN_CAN_NAME,
    VM_CONNECTIVITY.ADAPTER_PORT_STATUS,
    VM_CONNECTIVITY.FS_TYPE,
    VM_CONNECTIVITY.HYPERVISOR_VM_ID,
    VM_CONNECTIVITY.ADAPTER_PORT_TYPE,
    FABRIC.NAME as FABRIC_NAME,
    VIRTUAL_SWITCH.NAME as VIRTUAL_NAME,
    SWITCH_PORT.STATUS as SWITCH_PORT_STATUS,
    SWITCH_PORT.PORT_ID,
    SWITCH_PORT.PORT_NUMBER,
    USER_DEFINED_DEVICE_DETAIL.NAME as ADAPTER_PORT_NAME,
    VM_CONNECTIVITY.FABRIC_ID
```

```
from
    DEVICE_PORT
        left outer join USER_DEFINED_DEVICE_DETAIL
             on DEVICE_PORT.WWN = USER_DEFINED_DEVICE_DETAIL.WWN,
    CORE_SWITCH,
    SWITCH_PORT,
    VIRTUAL_SWITCH,
    VM_CONNECTIVITY,
    DEVICE_NODE,
    FABRIC
where
    VM_CONNECTIVITY.ADAPTER_PORT_WWN = DEVICE_PORT.WWN
    and DEVICE_PORT.SWITCH_PORT_WWN = SWITCH_PORT.WWN
    and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
    and DEVICE_PORT.NODE_ID = DEVICE_NODE.ID
    and DEVICE_NODE.FABRIC_ID = FABRIC.ID
union all
select
    DEVICE_PORT.SWITCH_PORT_WWN,
    DEVICE_PORT.DOMAIN_ID,
    DEVICE_PORT.NUMBER,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.NAME AS CORE_NAME,
    VM_CONNECTIVITY.ID,
    VM_CONNECTIVITY.VCENTER_ID,
    VM_CONNECTIVITY.HYPERVISOR_HOST,
    VM_CONNECTIVITY.VM_NAME,
    VM_CONNECTIVITY.PATH_NAME,
    VM_CONNECTIVITY.ADAPTER_PORT_WWN,
    VM_CONNECTIVITY.TARGET_PORT_WWN,
    VM_CONNECTIVITY.LUN_CAN_NAME,
    VM_CONNECTIVITY.ADAPTER_PORT_STATUS,
    VM_CONNECTIVITY.FS_TYPE,
    VM_CONNECTIVITY.HYPERVISOR_VM_ID,
    VM_CONNECTIVITY.ADAPTER_PORT_TYPE,
    FABRIC.NAME AS FABRIC_NAME,
    VIRTUAL_SWITCH.NAME AS VIRTUAL_NAME,
    SWITCH_PORT.STATUS AS SWITCH_PORT_STATUS,
    SWITCH_PORT.PORT_ID,
    SWITCH_PORT.PORT_NUMBER,
    USER_DEFINED_DEVICE_DETAIL.NAME AS ADAPTER_PORT_NAME,
    VM_CONNECTIVITY.FABRIC_ID
from
    DEVICE_PORT
        left join USER_DEFINED_DEVICE_DETAIL
            on DEVICE_PORT.WWN = USER_DEFINED_DEVICE_DETAIL.WWN,
    CORE_SWITCH,
    SWITCH_PORT,
    VIRTUAL_SWITCH,
    VM_CONNECTIVITY,
    DEVICE_NODE,
    FABRIC,
    DEVICE_PORT_MAC_ADDRESS_MAP,
    GIGE_PORT
where
    VM_CONNECTIVITY.ADAPTER_PORT_WWN = DEVICE_PORT.WWN
    and DEVICE_PORT.ID = DEVICE_PORT_MAC_ADDRESS_MAP.DEVICE_PORT_ID
    and DEVICE_PORT_MAC_ADDRESS_MAP.MAC_ADDRESS = GIGE_PORT.REMOTE_MAC_ADDRESS
    and GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID
    and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
    and DEVICE_PORT.NODE_ID = DEVICE_NODE.ID
    and DEVICE_NODE.FABRIC_ID = FABRIC.ID;
```

VM_EE_MONITOR_INFO

This view provides combined ee_monitor, ee_monitor_stats, device_port and device_node tables to get the EE Monitor information for vmplug-in.

```
create or replace view VM_EE_MONITOR_INFO as
select distinct
    EE_MONITOR.NAME,
    EE_MONITOR.SWITCH_PORT_ID,
    EE_MONITOR.SOURCE_PORT_ID,
    EE_MONITOR.DEST_PORT_ID,
    EE_MONITOR_STATS.TX,
    EE_MONITOR_STATS.RX,
    EE_MONITOR_STATS.CRCERRORS,
    EE_MONITOR_STATS.CREATION_TIME,
    SOURCE_PORT.PORT_ID as SID,
    DEST_PORT.PORT_ID as DID,
    SOURCE_NODE.WWN as SOURCE_DEVICE_WWN,
    SOURCE_PORT.WWN as SOURCE_PORT_WWN,
    DEST_NODE.WWN as DEST_DEVICE_WWN,
    DEST_PORT.WWN as DEST_PORT_WWN,
    SOURCE_NODE.FABRIC_ID as SOURCE_FABRIC_ID,
    DEST_NODE.FABRIC_ID as DEST_FABRIC_ID,
    SOURCE_PORT.DOMAIN_ID as SOURCE_SWITCH_DOMAIN_ID,
    DEST_PORT.DOMAIN_ID as DEST_SWITCH_DOMAIN_ID,
    VM_CONNECTIVITY.HYPERVISOR_VM_ID,
    VM_CONNECTIVITY.VM_NAME
from
    VM_CONNECTIVITY,
    DEVICE_PORT as SOURCE_PORT,
    DEVICE_PORT as DEST_PORT,
    DEVICE_NODE as DEST_NODE,
    DEVICE_NODE as SOURCE_NODE,
    EE_MONITOR,
    EE_MONITOR_STATS
where
    VM_CONNECTIVITY.ADAPTER_PORT_WWN = SOURCE_PORT.WWN
    and SOURCE_PORT.ID = EE_MONITOR.SOURCE_PORT_ID
    and EE_MONITOR.ID = EE_MONITOR_STATS.EE_MONITOR_ID
    and SOURCE_PORT.NODE_ID = SOURCE_NODE.ID
    and DEST_PORT.ID = EE_MONITOR.DEST_PORT_ID
    and DEST_PORT.NODE_ID = DEST_NODE.ID
    and EE_MONITOR_STATS.CREATION_TIME in (select MAX(CREATION_TIME) from
EE_MONITOR_STATS group by EE_MONITOR_ID);
```

VM_HOST_INFO

```
create or replace view VM_HOST_INFO as
select
   VM_HOST.ID               as HOST_ID,
   VM_HOST.NODE_WWN         as HOST_NODE_WWN,
   VM_HOST.HYPERVISOR_NAME,
   VM_HOST.HYPERVISOR_TYPE,
   VM_HOST.CPU_COUNT,
   VM_HOST.CPU_TYPE,
   VM_HOST.CPU_RESOURCES    as HOST_CPU_RESOURCES,
   VM_HOST.MEM_RESOURCES    as HOST_MEM_RESOURCES,
   VM_HOST.LICENSE_SERVER,
   VM_HOST.BOOT_TIME        as HOST_BOOT_TIME,
   CLUSTER.NAME             as CLUSTER_NAME,
   CLUSTER.IP_ADDRESS       as CLUSTER_ADDRESS,
   VIRTUAL_MACHINE.ID                  as VM_ID,
   VIRTUAL_MACHINE.HYPERVISOR_VM_ID,
   VIRTUAL_MACHINE.NAME                as VM_NAME,
   VIRTUAL_MACHINE.DESCRIPTION         as VM_DESCRIPTION,
   VIRTUAL_MACHINE.OS                  as VM_OS,
   VIRTUAL_MACHINE.STATUS              as VM_STATUS,
   VIRTUAL_MACHINE.VCPU_COUNT,
   VIRTUAL_MACHINE.CPU_RESOURCES       as VM_CPU_RESOURCES,
   VIRTUAL_MACHINE.MEM_RESOURCES       as VM_MEM_RESOURCES,
   VIRTUAL_MACHINE.IP_ADDRESS          as VM_IP_ADDRESS,
   VIRTUAL_MACHINE.HOSTNAME            as VM_HOSTNAME,
   VIRTUAL_MACHINE.BOOT_TIME           as VM_BOOT_TIME,
   VIRTUAL_MACHINE.DATASTORE_NAME,
   VIRTUAL_MACHINE.DATASTORE_LOCATION,
   VIRTUAL_MACHINE.NODE_WWN            as VM_NODE_WWN
from
   VM_HOST
   left outer join (CLUSTER join CLUSTER_MEMBER on CLUSTER_MEMBER.CLUSTER_ID =
CLUSTER.ID)
      on CLUSTER_MEMBER.DEVICE_ENCLOSURE_ID = VM_HOST.ID
   left outer join VIRTUAL_MACHINE
      on VM_HOST.ID = VIRTUAL_MACHINE.HOST_ID;
```

VM_LUN_INFO

```
create or replace view VM_LUN_INFO as
select
   VM_LUN.HOST_ID,
   VM_LUN.ID                as LUN_ID,
   VM_LUN.NAME              as LUN_NAME,
   VM_LUN.NODE_WWN,
   VM_LUN.VENDOR,
   VM_LUN.MODEL,
   VM_LUN.SERIAL_NUMBER,
   VM_LUN.TYPE,
   VM_LUN.CAPACITY,
   VM_LUN.STATUS            as LUN_STATUS,
   VM_LUN.PATH_POLICY,
   VM_PATH.ID               as PATH_ID,
   VM_PATH.VM_ID            as PATH_VM_ID,
   VM_PATH.NAME             as PATH_NAME,
   VM_PATH.FABRIC_ID,
   VM_PATH.HBA_PORT_WWN,
   VM_PATH.VM_PORT_WWN,
   VM_PATH.TARGET_PORT_WWN,
   VM_PATH.HBA_NODE_WWN,
   VM_PATH.VM_NODE_WWN,
   VM_PATH.TARGET_NODE_WWN,
   VM_PATH.HBA_NAME,
   VM_PATH.USAGE            as PATH_USAGE,
   VM_PATH.ENABLED          as PATH_ENABLED,
   VM_PATH.ACTIVE           as PATH_ACTIVE,
   VM_PATH.PREFERRED        as PATH_PREFERRED
from
   VM_LUN join VM_PATH on VM_LUN.ID = VM_PATH.LUN_ID;
```

VM_STATISTICS_INFO

This view gets the FC port statistics for the VM Connectivity data.

```
create or replace view VM_STATISTICS_INFO as
select distinct
    DEVICE_PORT.SWITCH_PORT_WWN,
    DEVICE_PORT.DOMAIN_ID,
    VM_CONNECTIVITY.HYPERVISOR_HOST,
    VM_CONNECTIVITY.ADAPTER_PORT_WWN,
    VM_CONNECTIVITY.ADAPTER_PORT_STATUS,
    VM_CONNECTIVITY.HYPERVISOR_VM_ID,
    VM_CONNECTIVITY.VM_NAME,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.NAME as CORE_NAME,
    FC_PORT_STATS.TX,
    FC_PORT_STATS.RX,
    FC_PORT_STATS.TX_UTILIZATION,
    FC_PORT_STATS.RX_UTILIZATION,
    FC_PORT_STATS.SYNCLOSSES,
    FC_PORT_STATS.SIGNALLOSSES,
    FC_PORT_STATS.SEQUENCEERRORS,
    FC_PORT_STATS.INVALIDTRANSMISSIONS,
    FC_PORT_STATS.CRCERRORS,
    FC_PORT_STATS.CREATION_TIME,
    VIRTUAL_SWITCH.NAME as VIRTUAL_NAME,
    SWITCH_PORT.STATUS as SWITCH_PORT_STATUS,
    SWITCH_PORT.PORT_ID,
    SWITCH_PORT.PORT_NUMBER
from
    DEVICE_PORT,
    VM_CONNECTIVITY,
    SWITCH_PORT,
    CORE_SWITCH,
    FC_PORT_STATS,
    VIRTUAL_SWITCH
where
    VM_CONNECTIVITY.ADAPTER_PORT_WWN = DEVICE_PORT.WWN
    and DEVICE_PORT.SWITCH_PORT_WWN = SWITCH_PORT.WWN
    and SWITCH_PORT.ID = FC_PORT_STATS.PORT_ID
    and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
    and FC_PORT_STATS.CREATION_TIME in (select MAX(CREATION_TIME) from
FC_PORT_STATS group by PORT_ID)
union
select
    DEVICE_PORT.SWITCH_PORT_WWN,
    DEVICE_PORT.DOMAIN_ID,
    VM_CONNECTIVITY.HYPERVISOR_HOST,
    VM_CONNECTIVITY.ADAPTER_PORT_WWN,
    VM_CONNECTIVITY.ADAPTER_PORT_STATUS,
    VM_CONNECTIVITY.HYPERVISOR_VM_ID,
    VM_CONNECTIVITY.VM_NAME,
    CORE_SWITCH.IP_ADDRESS,
    CORE_SWITCH.NAME as CORE_NAME,
    SWITCH_TE_PORT_STATS.TRANSMIT_OK,
    SWITCH_TE_PORT_STATS.RECEIVE_OK,
    SWITCH_TE_PORT_STATS.TRANSMIT_OK_PERCENT_UTIL,
    SWITCH_TE_PORT_STATS.RECEIVE_OK_PERCENT_UTIL,
    -1,-1,-1,-1,-1,
    SWITCH_TE_PORT_STATS.CREATION_TIME,
    VIRTUAL_SWITCH.NAME as VIRTUAL_NAME,
    SWITCH_PORT.STATUS as SWITCH_PORT_STATUS,
    SWITCH_PORT.PORT_ID,
    SWITCH_PORT.PORT_NUMBER
from
    DEVICE_PORT,
    VM_CONNECTIVITY,
    SWITCH_PORT,
    CORE_SWITCH,
    SWITCH_TE_PORT_STATS,
    VIRTUAL_SWITCH,
    DEVICE_PORT_MAC_ADDRESS_MAP,
    DEVICE_PORT_GIGE_PORT_LINK,
    GIGE_PORT
where
    VM_CONNECTIVITY.ADAPTER_PORT_WWN = DEVICE_PORT.WWN
    and DEVICE_PORT.ID = DEVICE_PORT_MAC_ADDRESS_MAP.DEVICE_PORT_ID
    and DEVICE_PORT_MAC_ADDRESS_MAP.MAC_ADDRESS = GIGE_PORT.REMOTE_MAC_ADDRESS
    and GIGE_PORT.SWITCH_PORT_ID = SWITCH_TE_PORT_STATS.PORT_ID
    and GIGE_PORT.SWITCH_PORT_ID = SWITCH_PORT.ID
    and SWITCH_PORT.VIRTUAL_SWITCH_ID = VIRTUAL_SWITCH.ID
    and VIRTUAL_SWITCH.CORE_SWITCH_ID = CORE_SWITCH.ID
    and SWITCH_TE_PORT_STATS.CREATION_TIME in (select max(CREATION_TIME) from
SWITCH_TE_PORT_STATS group by PORT_ID);
```

ZONE_DB_INFO

```
create or replace view ZONE_DB_INFO as
select
    ZONE_DB.ID,
    ZONE_DB.FABRIC_ID,
    ZONE_DB.OFFLINE,
    ZONE_DB.NAME,
    ZONE_DB.CREATED,
    ZONE_DB.CREATED_BY,
    ZONE_DB.LAST_MODIFIED,
    ZONE_DB.LAST_MODIFIED_BY,
    ZONE_DB.LAST_APPLIED,
    ZONE_DB.LAST_APPLIED_BY,
    ZONE_DB.DEFAULT_ZONE_STATUS,
    ZONE_DB.MCDATA_DEFAULT_ZONE,
    ZONE_DB.MCDATA_SAFE_ZONE,
    ZONE_DB.ZONE_TXN_SUPPORTED,
    ZONE_DB.ZONE_CONFIG_SIZE,
    ZONE_DB.ZONE_AVAILABLE_SIZE,
    ZONE_DB_CONFIG.ID AS CONFIG_ID,
    ZONE_DB_CONFIG.DEFINED_CONTENT,
    ZONE_DB_CONFIG.ACTIVE_CONTENT,
    ZONE_DB_CONFIG.TI_ZONE_CONTENT
from
    ZONE_DB, ZONE_DB_CONFIG
where
```

```
    ZONE_DB.ID = ZONE_DB_CONFIG.ZONE_DB_ID;
-- Name: access_control_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE access_control_entry (
    access_control_entry_id integer NOT NULL,
    access_control_list_id integer NOT NULL,
    sequence_num numeric(8,0) NOT NULL,
    is_permit numeric(1,0),
    is_log numeric(1,0),
    comments character varying(256),
    table_subtype character varying(32) NOT NULL
);

-- Name: access_control_group; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE access_control_group (
    access_control_group_id integer NOT NULL,
    name character varying(64) NOT NULL,
    user_id integer NOT NULL,
    is_public numeric(1,0),
    description character varying(255)
);

-- Name: access_control_list; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE access_control_list (
    access_control_list_id integer NOT NULL,
    access_control_group_id integer NOT NULL,
    acl_num numeric(8,0),
    acl_name character varying(256),
    is_standard_acl numeric(1,0),
    next_ace_sequence_num numeric(6,0)
);

-- Name: access_scope; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE access_scope (
    access_scope_id integer NOT NULL,
    access_level numeric(4,0) NOT NULL,
    name character varying(64) NOT NULL
);

-- Name: accessible_device; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE accessible_device (
    accessible_entity_id integer NOT NULL,
    device_id integer
);

-- Name: accessible_device_group; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE accessible_device_group (
    accessible_entity_id integer NOT NULL,
    device_group_id integer
);

-- Name: accessible_entity; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE accessible_entity (
    accessible_entity_id integer NOT NULL,
    type character varying(8),
    table_subtype character varying(32) NOT NULL,
    require_update numeric(1,0)
);

-- Name: accessible_port_group; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE accessible_port_group (
    accessible_entity_id integer NOT NULL,
    port_group_id integer
);

-- Name: accessible_vip_server; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE accessible_vip_server (
    accessible_entity_id integer NOT NULL,
    server_ip character varying(39) NOT NULL,
    server_mode character varying(39) NOT NULL,
    server_iron_ip character varying(39)
);

-- Name: acl_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE acl_spec (
    acl_spec_id integer NOT NULL,
    table_subtype character varying(32) NOT NULL
);

-- Name: adaptive_policy_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE adaptive_policy_entry (
    policy_entry_id integer NOT NULL,
    acl_spec_id integer,
    sequence_num numeric(6,0)
);

-- Name: address_group; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE address_group (
    address_group_id integer NOT NULL,
    name character varying(64) NOT NULL
);

-- Name: address_group_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE address_group_entry (
    address_group_entry_id integer NOT NULL,
    parent_address_group_id integer NOT NULL,
    child_address_group_id integer NOT NULL
);

-- Name: address_group_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE address_group_spec (
    address_spec_id integer NOT NULL,
    address_group_id integer
);

-- Name: address_group_subnet_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE address_group_subnet_entry (
    address_group_subnet_entry_id integer NOT NULL,
    ip_subnet_definition_id integer NOT NULL,
    address_group_id integer NOT NULL
);
```

```
-- Name: address_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE address_spec (
    address_spec_id integer NOT NULL,
    table_subtype character varying(32) NOT NULL
);

-- Name: alert; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE alert (
    alert_id integer NOT NULL,
    name character varying(32) NOT NULL,
    user_id integer NOT NULL,
    description character varying(255),
    status character(1),
    props_str character varying(2048),
    last_updated bigint,
    severity smallint,
    event_type character(2),
    messages character varying(255),
    actions integer
);

-- Name: ap; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ap (
    device_id integer NOT NULL,
    is_rogue numeric(1,0),
    is_known numeric(1,0),
    is_managed numeric(1,0),
    is_online numeric(1,0),
    is_relief numeric(1,0),
    nearby_sensor_device_id integer,
    ap_relief_status character varying(20),
    rssi integer,
    num_clients integer,
    is_suppressing numeric(1,0)
);

-- Name: ap_adc_config_per_fes; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ap_adc_config_per_fes (
    ap_adc_config_per_fes_id integer NOT NULL,
    device_id integer NOT NULL,
    scenario_id integer DEFAULT 2 NOT NULL,
    ip_address_pool character varying(4096),
    other character varying(1024)
);

-- Name: ap_block_mac_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ap_block_mac_entry (
    ap_block_mac_entry_id integer NOT NULL,
    block_mac_list_id integer,
    device_id integer
);

-- Name: ap_ids; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ap_ids (
    sqnum integer NOT NULL,
    time_stamp bigint,
    device_id integer NOT NULL,
    macaddr character varying(17),
    authenticated smallint,
    associated smallint,
    forwarding smallint,
    lastkeytype smallint,
    manualblock smallint,
    dynamicblock smallint,
    attemptsconsumed integer,
    attemptsremained integer,
    remainedcycletime integer,
    remainedblocktime integer
);

-- Name: ap_ids_last_saved; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ap_ids_last_saved (
    device_id integer NOT NULL,
    time_stamp bigint NOT NULL
);

-- Name: ap_ids_sqnum_seq; Type: SEQUENCE; Schema: dcm; Owner: dcmadmin
CREATE SEQUENCE ap_ids_sqnum_seq
    START WITH 1
    INCREMENT BY 1
    NO MAXVALUE
    NO MINVALUE
    CACHE 1;

-- Name: ap_mac_filter_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ap_mac_filter_entry (
    mac_filter_entry_id integer NOT NULL
);

-- Name: ap_plug_and_play; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ap_plug_and_play (
    ap_plug_and_play_id integer NOT NULL,
    device_id integer,
    interface_id integer,
    realm_policy_id integer,
    device_group_id integer,
    name character varying(64),
    status numeric(2,0) NOT NULL,
    mac_address character varying(32) NOT NULL,
    ip_address character varying(40),
    subnet_mask character varying(40),
    default_gateway character varying(40),
    country_code character varying(32),
    port_status numeric(2,0) NOT NULL,
    uieng_device_config_id integer,
    scenario_id integer
);

-- Name: ap_station; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ap_station (
    sqnum integer NOT NULL,
    time_stamp bigint NOT NULL,
    device_id integer NOT NULL,
    sys_up_time integer,
    ifindex integer,
    stationaddres character varying(40),
    authenticated smallint,
    associated smallint,
    isforwarding smallint,
    keytype smallint,
    lastauthenticatedtime bigint,
    associatedtime bigint,
    lastassociatedtime bigint,
    lastdisassociatedtime bigint,
    txpacketcount bigint,
    rxpacketcount bigint,
    txbytecount bigint,
    rxbytecount bigint,
    time_interval bigint,
    radio smallint,
    channel smallint
);

-- Name: ap_station_last_saved; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ap_station_last_saved (
    device_id integer NOT NULL,
    time_stamp bigint NOT NULL
);

-- Name: ap_station_sqnum_seq; Type: SEQUENCE; Schema: dcm; Owner: dcmadmin
CREATE SEQUENCE ap_station_sqnum_seq
    START WITH 1
    INCREMENT BY 1
    NO MAXVALUE
    NO MINVALUE
    CACHE 1;

-- Name: ap_usage; Type: VIEW; Schema: dcm; Owner: dcmadmin
CREATE VIEW ap_usage AS
    SELECT ap_station.device_id, ap_station.time_stamp, count(*) AS num_clients
FROM ap_station WHERE (ap_station.radio > 0) GROUP BY ap_station.device_id,
ap_station.time_stamp;

-- Name: apple_talk_cable_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE apple_talk_cable_vlan (
    vlan_db_id integer NOT NULL,
    vlan_id smallint NOT NULL
);

-- Name: atm_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE atm_interface (
    interface_id integer NOT NULL
);

-- Name: authentication_encryption; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE authentication_encryption (
    authentication_encryption_id integer NOT NULL,
    ssid_authentication_id integer NOT NULL,
    encryption_type numeric(2,0),
    is_shared numeric(1,0),
    data_encryption_on numeric(1,0),
    table_subtype character varying(32) NOT NULL,
    uiengine_realm_security_device_config_id integer
```

```
);

-- Name: block_mac_list; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE block_mac_list (
    block_mac_list_id integer NOT NULL,
    mac character varying(32) NOT NULL,
    radio_vap numeric(2,0),
    lockout_time character varying(64),
    last_seen_ap_id integer,
    last_time_seen character varying(64),
    device_group_id integer,
    is_full_device_group numeric(1,0),
    deployment_setting_id integer
);

-- Name: cfg_backup_archive; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE cfg_backup_archive (
    cfg_backup_archive_id integer NOT NULL,
    device_id integer NOT NULL,
    user_id integer NOT NULL,
    product_type character varying(32),
    version numeric(8,0),
    location character varying(255),
    date_time character varying(64),
    file_name character varying(64),
    is_baseline numeric(1,0),
    description character varying(1024),
    image_version character varying(64),
    cli_template_report_execution_id integer,
    cli_template_report_execution integer
);

-- Name: cfg_backup_detail; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE cfg_backup_detail (
    cfg_backup_detail_id integer NOT NULL,
    cfg_backup_archive_id integer,
    device_id integer NOT NULL,
    backup_type character(1),
    backup_deployment_execution_id integer,
    change_status character varying(256),
    change_summary character varying(8192),
    table_subtype character varying(32) NOT NULL
);

-- Name: cfg_file_revision; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE cfg_file_revision (
    cfg_file_revision_id integer NOT NULL,
    user_id integer NOT NULL,
    device_id integer NOT NULL,
    datetime character varying(32),
    image_version character varying(32),
    product_type character varying(32),
    file_name character varying(512) NOT NULL,
    file_type character varying(8) NOT NULL,
    revision_num numeric(4,0) NOT NULL,
    description character varying(64)
);
```

```
-- Name: cfg_restore_backup_detail; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE cfg_restore_backup_detail (
    cfg_backup_detail_id integer NOT NULL,
    user_id integer,
    cfg_file_revision_id integer
);

-- Name: chassis_component; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE chassis_component (
    chassis_component_id integer NOT NULL,
    device_id integer NOT NULL,
    name character varying(128),
    description character varying(128),
    class character varying(32),
    hw_revision character varying(64),
    fw_revision character varying(64),
    sw_revision character varying(64),
    serial_num character varying(32)
);

-- Name: cli_device_config_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE cli_device_config_entry (
    device_config_entry_id integer NOT NULL,
    cli_template_id integer
);

-- Name: cli_template; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE cli_template (
    cli_template_id integer NOT NULL,
    user_id integer NOT NULL,
    name character varying(256) NOT NULL,
    type numeric(2,0) NOT NULL,
    cli_cmd character varying,
    description character varying(512),
    device_username character varying(256),
    device_password character varying(256),
    date_time character varying(64),
    device_enable_username character varying(256),
    device_enable_password character varying(256),
    cli_filter character varying,
    has_parameters numeric(1,0) NOT NULL
);

-- Name: cli_template_reference; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE cli_template_reference (
    cli_template_reference_id integer NOT NULL,
    cli_template_id integer NOT NULL,
    refers_to_template_id integer NOT NULL
);

-- Name: cli_template_report; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE cli_template_report (
    cli_template_report_id integer NOT NULL,
    deployment_execution_id integer,
    user_id integer,
    is_available numeric(1,0),
    exec_option numeric(2,0),
    is_public numeric(1,0),
    content character varying,
    report_file_name character varying(256),
    template_report_type numeric(2,0)
);

-- Name: cli_template_report_execution; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE cli_template_report_execution (
    cli_template_report_execution_id integer NOT NULL,
    device_deployment_job_id integer,
    cli_template_id integer,
    content character varying,
    compare_status numeric(2,0)
);

-- Name: cli_template_target_device; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE cli_template_target_device (
    cli_template_target_device_id integer NOT NULL,
    device_id integer,
    cli_template_id integer
);

-- Name: cli_template_target_device_group; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE cli_template_target_device_group (
    cli_template_target_device_group_id integer NOT NULL,
    cli_template_id integer,
    device_group_id integer
);

-- Name: PERF_COLLECTOR; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE PERF_COLLECTOR (
    collector_id integer NOT NULL,
    name character varying(32) NOT NULL,
    status character(1),
    type numeric(2,0),
    polling_interval integer,
    created_time_seconds integer,
    props_str character varying(256)
);

-- Name: collector_mib_object_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE collector_mib_object_entry (
    collector_mib_object_entry_id integer NOT NULL,
    collector_id integer,
    mib_object_id integer
);

-- Name: collector_snmp_expression_entry; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE collector_snmp_expression_entry (
    collector_snmp_expression_entry_id integer NOT NULL,
    collector_id integer,
    expression_id integer
);
```

```
-- Name: collector_target_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE collector_target_entry (
    collector_target_entry_id integer NOT NULL,
    collector_id integer,
    target_id integer NOT NULL,
    prop_str character varying(8192),
    collector_target_entry_type integer
);

-- Name: collector_threshold_rearm_trigger; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE collector_threshold_rearm_trigger (
    collector_threshold_rearm_trigger_id integer NOT NULL,
    collector_id integer,
    fixed_threshold integer,
    stats_threshold integer,
    fixed_threshold_op integer,
    stats_threshold_op integer,
    threshold_trap_severity integer,
    fixed_rearm integer,
    stats_rearm integer,
    fixed_rearm_op integer,
    stats_rearm_op integer,
    rearm_trap_severity integer
);

-- Name: config_snapshot; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE config_snapshot (
    config_snapshot_id integer NOT NULL,
    device_id integer NOT NULL,
    device_config_id integer NOT NULL,
    datetime character(32) NOT NULL,
    comments character varying(512)
);

-- Name: deployment_backup_detail; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE deployment_backup_detail (
    cfg_backup_detail_id integer NOT NULL,
    deployment_execution_id integer,
    user_id integer
);

-- Name: deployment_execution; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE deployment_execution (
    deployment_execution_id integer NOT NULL,
    deployment_setting_id integer,
    deployment_time character varying(32),
    status character(1),
    pre_snapshot_deployment_execution_id integer,
    post_snapshot_deployment_execution_id integer,
    user_id numeric(10,0) DEFAULT 1 NOT NULL
);

-- Name: deployment_port_list; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE deployment_port_list (
    deployment_port_list_id integer NOT NULL,
    device_deployment_job_id integer NOT NULL,
    interface_id integer NOT NULL
);

-- Name: deployment_setting; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE deployment_setting (
    deployment_setting_id integer NOT NULL,
    scenario_id integer NOT NULL,
    user_id integer NOT NULL,
    is_write_to_ram numeric(1,0),
    is_reload numeric(1,0),
    deployment_mode character(1),
    do_pre_post_snapshot numeric(2,0) NOT NULL,
    cli_template_id integer NOT NULL,
    pre_post_deploy_setting_id integer NOT NULL,
    post_snapshot_delay integer NOT NULL
);

-- Name: device; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE device (
    device_id integer NOT NULL,
    ip_address character varying(255),
    alias_name character varying(512),
    host_name character varying(512),
    sys_name character varying(255),
    sys_contact character varying(255),
    description character varying(512),
    sys_location character varying(255),
    community_str_get character varying(512),
    community_str_set character varying(512),
    sys_oid character varying(255),
    super_user_password character varying(512),
    table_subtype character varying(32) NOT NULL,
    local_user_name character varying(512),
    local_password character varying(512),
    telnet_password character varying(512),
    radius_user_name character varying(512),
    radius_password character varying(512),
    tac_user_name character varying(512),
    tac_password character varying(512),
    tacplus_user_name character varying(512),
    tacplus_password character varying(512),
    is_router numeric(1,0),
    is_slb numeric(1,0),
    first_seen_time character varying(64),
    last_seen_time character varying(64),
    last_probe_time character varying(64),
    last_probe_status character varying(64),
    is_sflow_capable numeric(1,0),
    snmpv3_ro_auth_type character varying(1),
    snmpv3_ro_auth_username character varying(512),
    snmpv3_ro_auth_password character varying(512),
    snmpv3_ro_priv_protocol character varying(1),
    snmpv3_ro_priv_password character varying(512),
    snmpv3_rw_auth_type character varying(1),
    snmpv3_rw_auth_username character varying(512),
    snmpv3_rw_auth_password character varying(512),
    snmpv3_rw_priv_protocol character varying(1),
    snmpv3_rw_priv_password character varying(512),
    local_username_port_cfg character varying(512),
    local_password_port_cfg character varying(512),
    local_username_read_only character varying(512),
    local_password_read_only character varying(512),
    radius_username_port_cfg character varying(512),
    radius_password_port_cfg character varying(512),
    radius_username_read_only character varying(512),
    radius_password_read_only character varying(512),
    tac_username_port_cfg character varying(512),
    tac_password_port_cfg character varying(512),
    tac_username_read_only character varying(512),
    tac_password_read_only character varying(512),
    tacplus_username_port_cfg character varying(512),
    tacplus_password_port_cfg character varying(512),
    tacplus_username_read_only character varying(512),
    tacplus_password_read_only character varying(512),
    enable_password_port_cfg character varying(512),
    enable_password_read_only character varying(512),
    admin_status smallint,
    admin_status_duration integer,
    admin_status_last_updated bigint,
    memo_last_updated bigint,
    memo character varying(4096),
    tacplus_enable_username character varying(512),
    tacplus_enable_password character varying(512),
    oper_status smallint,
    oper_status_last_updated bigint,
    lldp_chassis_id_subtype smallint,
    lldp_chassis_id bytea,
    is_fdp_enabled numeric(1,0),
    is_cdp_enabled numeric(1,0),
    vendor character varying(64),
    is_foundry numeric(1,0),
    MANAGED_ELEMENT_ID int,
    NODE_WWN character varying(23) not null default '',
    SYSLOG_REGISTERED numeric(1) default 0,
    TRAP_REGISTERED numeric(1) default 0,
    PORT_COUNT integer default 0,
    SERIAL_NUMBER character varying(32) default '',
    CATEGORY integer default 0 not null,
    MPLS_MANAGE_STATE integer default 0 not null,
    license_port_count integer default 0 not null,
    licensed_features integer default 0 not null
);

-- Name: device_config; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE device_config (
    device_config_id integer NOT NULL,
    name character varying(255) NOT NULL,
    user_id integer NOT NULL,
    is_public numeric(1,0),
    description character varying(1024),
    is_port_based numeric(1,0) NOT NULL,
    is_independent numeric(1,0)
);

-- Name: device_config_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE device_config_entry (
    device_config_entry_id integer NOT NULL,
    name_key character varying(64) NOT NULL,
    device_config_id integer NOT NULL,
    value_str bytea NOT NULL,
    line_num smallint NOT NULL,
    key1 smallint,
    key2 smallint,
    ref_table_name character varying(64),
    table_id integer,
    table_subtype character varying(32) NOT NULL,
    type_key character varying(32)
);

-- Name: device_deployment_job; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE device_deployment_job (
    device_config_id integer NOT NULL,
    device_deployment_job_id integer NOT NULL,
    deployment_execution_id integer NOT NULL,
    device_id integer NOT NULL,
    status character(1) NOT NULL,
    error_code numeric(6,0),
    error_msg character varying(8192)
);

-- Name: device_group; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE device_group (
    device_group_id integer NOT NULL,
    name character varying(128) NOT NULL,
    user_id integer NOT NULL,
    description character varying(255),
    is_public numeric(1,0),
    is_internal numeric(1,0),
    table_subtype character varying(32) NOT NULL,
    is_ap_group numeric(1,0) DEFAULT 0 NOT NULL,
    is_sensor_group numeric(1,0) DEFAULT 0 NOT NULL,
    view_mask numeric(1,0),
    GROUP_TYPE integer default 0 not null
);

-- Name: device_group_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE device_group_entry (
    device_group_id integer NOT NULL,
    device_group_entry_id integer NOT NULL,
    device_id integer NOT NULL
);

-- Name: device_status; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE device_status (
    device_status_id integer NOT NULL,
    device_id integer NOT NULL,
    group_id integer,
    state_id integer NOT NULL,
    last_updated bigint NOT NULL
);

-- Name: discovery_cycle; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE discovery_cycle (
    discovery_cycle_id integer NOT NULL,
    discovery_profile_id integer NOT NULL,
    start_time numeric(20,0) NOT NULL,
    duration integer
);

-- Name: discovery_log; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE discovery_log (
    discovery_log_id integer NOT NULL,
    discovery_cycle_id integer NOT NULL,
    "timestamp" numeric(20,0),
    category smallint,
    device_ip character varying(40),
    messages character varying(4096)
);

-- Name: discovery_profile; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE discovery_profile (
    discovery_profile_id integer NOT NULL,
    discovery_profile_name character varying(255) NOT NULL
);

-- Name: discovery_profile_detail; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE discovery_profile_detail (
    discovery_profile_detail_id integer NOT NULL,
    discovery_profile_id integer NOT NULL,
    property_key character varying(255) NOT NULL,
    property_value character varying(512) NOT NULL
);

-- Name: ethernet_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ethernet_interface (
    interface_id integer NOT NULL
);

-- Name: events_main; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE events_main (
    messages_id integer,
    trap_log_id integer NOT NULL,
    trap_sender character varying(40) NOT NULL,
    "timestamp" bigint,
    severity smallint,
    is_ack numeric(1,0),
    log_type character(1),
    slot smallint,
    port smallint,
    device_id integer,
    event_action_id integer,
    device_group_id integer,
    port_group_id integer,
    trap_device_ip character varying(40),
    log_sub_type character(1),
    unit smallint
);

-- Name: events_messages; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE events_messages (
    messages character varying(512) NOT NULL,
    messages_id integer NOT NULL
);
```

```
-- Name: events; Type: VIEW; Schema: dcm; Owner: dcmadmin
CREATE VIEW events AS
    SELECT emain.trap_log_id, emain.trap_sender, emain."timestamp",
emain.severity, emsgs.messages, emain.is_ack, emain.log_type, emain.slot,
emain.port, emain.device_id, emain.event_action_id, emain.device_group_id,
emain.port_group_id, emain.trap_device_ip, emain.log_sub_type, emain.unit FROM
(events_main emain LEFT JOIN events_messages emsgs ON ((emain.messages_id =
emsgs.messages_id)));

-- Name: extended_access_control_entry; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE extended_access_control_entry (
    access_control_entry_id integer NOT NULL,
    src_port_spec_id integer,
    dest_address_spec_id integer NOT NULL,
    dest_port_spec_id integer,
    ip_protocol numeric(4,0),
    tcp_protocol_flag_id integer,
    precedence numeric(4,0),
    tos numeric(4,0),
    ip_priority numeric(2,0),
    priority_force numeric(2,0),
    priority_mapping numeric(2,0),
    dscp_marking numeric(2,0),
    dscp_mapping numeric(2,0),
    icmp_msg_type numeric(3,0),
    icmp_code numeric(3,0)
);

-- Name: fixed_policy_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE fixed_policy_entry (
    policy_entry_id integer NOT NULL
);

-- Name: flow_user; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE flow_user (
    user_id integer NOT NULL,
    user_name character varying(255),
    last_used integer
);

-- Name: foundry_ap; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE foundry_ap (
    device_id integer NOT NULL,
    product_type character varying(64),
    image_version character varying(64),
    is_vlan_feature_enabled numeric(1,0),
    management_vlan_id smallint,
    is_sensor numeric(1,0) DEFAULT 0,
    bssids character varying(128)
);

-- Name: foundry_device; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE foundry_device (
    device_id integer NOT NULL,
    image_version character varying(32),
    product_type character varying(32),
    feature_mask bytea,
    is_port_vlan_enabled numeric(1,0),
    architecture_type numeric(2,0),
    build_label character varying(64),
    ssl_slot numeric(4,0)
);

-- Name: foundry_module; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE foundry_module (
    module_id integer NOT NULL,
    serial_num character varying(32),
    dram_size numeric(4,0),
    boot_flash_size numeric(4,0),
    module_type numeric(4,0),
    code_flash_size numeric(4,0),
    expansion_module_type numeric(4,0),
    expansion_module_description character varying(128)
);

-- Name: foundry_physical_device; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE foundry_physical_device (
    physical_device_id integer NOT NULL,
    serial_number character varying(32),
    product_type character varying(32)
);

-- Name: foundry_physical_port; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE foundry_physical_port (
    physical_port_id integer NOT NULL,
    connector_type smallint,
    media_type smallint,
    gig_type smallint
);

-- Name: gbit_ethernet_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE gbit_ethernet_interface (
    interface_id integer NOT NULL
);

-- Name: global_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE global_vlan (
    global_vlan_db_id integer NOT NULL,
    name character varying(255) NOT NULL,
    context_device_id integer
);

-- Name: hostname_address; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE hostname_address (
    hostname_address_id integer NOT NULL,
    hostname character varying(64) NOT NULL,
    address_group_id integer NOT NULL
);

-- Name: hostname_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE hostname_spec (
    address_spec_id integer NOT NULL,
    name character varying(64) NOT NULL
);
```

```
-- Name: image_archive; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE image_archive (
    image_archive_id integer NOT NULL,
    product_type character varying(32) NOT NULL,
    feature_mask character varying(32),
    supported_type character varying(32) NOT NULL,
    flash_size integer,
    location character varying(255) NOT NULL,
    file_name character varying(64) NOT NULL,
    version_label character varying(32) NOT NULL,
    release_datetime character varying(64),
    special_key character varying(32),
    image_type numeric(1,0),
    build_label character varying(64)
);

-- Name: interface; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE interface (
    interface_id integer NOT NULL,
    switch_service_id integer,
    device_id integer NOT NULL,
    name character varying(255),
    identifier character varying(32) NOT NULL,
    table_subtype character varying(32) NOT NULL,
    tag_mode smallint,
    vlan_tag_type integer,
    untagged_vlan_id smallint,
    if_name character varying(64),
    lldp_port_id_subtype smallint,
    lldp_port_id bytea,
    is_fdp_enabled numeric(1,0),
    is_cdp_enabled numeric(1,0),
    port_status smallint,
    port_state smallint
);

-- Name: interface_status; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE interface_status (
    interface_status_id integer NOT NULL,
    interface_id integer NOT NULL,
    state_id integer NOT NULL,
    last_updated bigint NOT NULL
);

-- Name: ip_acl_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ip_acl_spec (
    acl_spec_id integer NOT NULL,
    access_control_list_id integer
);

-- Name: ip_address_range; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ip_address_range (
    ip_address_range_id integer NOT NULL,
    address_group_id integer NOT NULL,
    ip_address_low character varying(40),
    ip_address_high character varying(40)
);

-- Name: ip_address_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
```

```
CREATE TABLE ip_address_spec (
    address_spec_id integer NOT NULL,
    ip_address character varying(40) NOT NULL,
    wildcard_mask character varying(40)
);

-- Name: inm_ip_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE inm_ip_interface (
    ip_interface_id integer NOT NULL,
    ip_routing_service_id integer,
    interface_id integer,
    device_id integer NOT NULL,
    ip_subnet_id integer NOT NULL,
    ip_address character varying(40) NOT NULL,
    subnet_mask character varying(40)
);

-- Name: ip_routing_service; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ip_routing_service (
    service_id integer NOT NULL,
    vrf_name character varying(31)
);

-- Name: ip_subnet; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ip_subnet (
    ip_subnet_id integer NOT NULL,
    ip_address character varying(40),
    subnet_mask character varying(40),
    name character varying(64),
    description character varying(255),
    cidr_mask integer
);

-- Name: ip_subnet_definition; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ip_subnet_definition (
    ip_subnet_definition_id integer NOT NULL,
    ip_address character varying(40) NOT NULL,
    name character varying(64) NOT NULL,
    subnet_mask character varying(40)
);

-- Name: ip_subnet_definition_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ip_subnet_definition_spec (
    address_spec_id integer NOT NULL,
    ip_subnet_definition_id integer NOT NULL
);

-- Name: ip_subnet_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ip_subnet_vlan (
    vlan_db_id integer NOT NULL,
    ip_address character varying(40) NOT NULL,
    subnet_mask character varying(40) NOT NULL
);

-- Name: ipx_network_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ipx_network_vlan (
    vlan_db_id integer NOT NULL,
    network_number character varying(32) NOT NULL,
    frame_type numeric(4,0) NOT NULL
);

-- Name: ironclad_adaptive_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ironclad_adaptive_entry (
    policy_entry_id integer NOT NULL,
    normal_burst numeric(20,3),
    normal_burst_type character(1),
    max_burst numeric(20,3),
    max_burst_type character(1),
    conform_action numeric(2,0),
    exceed_action numeric(2,0),
    vlan_id numeric(4,0)
);

-- Name: jetcore_adaptive_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE jetcore_adaptive_entry (
    policy_entry_id integer NOT NULL,
    queue_num numeric(2,0),
    is_terathon numeric(1,0),
    terathon_max_burst numeric(20,3),
    terathon_max_burst_type character(1)
);

-- Name: l2_neighbor; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE l2_neighbor (
    l2_neighbor_id integer NOT NULL,
    interface_id integer NOT NULL,
    rmt_ip_address character varying(40),
    rmt_if_name character varying(64),
    last_seen_time integer NOT NULL,
    lldp_rem_chassis_id_subtype smallint,
    lldp_rem_chassis_id bytea,
    lldp_rem_port_id_subtype smallint,
    lldp_rem_port_id bytea
);

-- Name: l3_roaming_domain; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE l3_roaming_domain (
    l3_roaming_domain_id integer NOT NULL,
    mobility_domain_id integer
);

-- Name: l3_roaming_domain_device; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE l3_roaming_domain_device (
    l3_roaming_domain_device_id integer NOT NULL,
    l3_roaming_domain_id integer,
    device_id integer
);

-- Name: l3_roaming_peer_config; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE l3_roaming_peer_config (
    l3_roaming_peer_config_id integer NOT NULL,
    l3_roaming_domain_device_id integer,
    ip_address character varying(64),
    config_state character varying(1),
    time_stamp character varying(64)
);

-- Name: license_files; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE license_files (
    license_file_id integer NOT NULL,
    identifier character varying(255) NOT NULL,
    license_details character varying(255) NOT NULL,
    is_eval numeric(1,0) NOT NULL
);

-- Name: license_parameters; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE license_parameters (
    license_param_id integer NOT NULL,
    identifier character varying(255) NOT NULL,
    identifier_type character varying(255) NOT NULL,
    used_during_startup numeric(1,0) NOT NULL
);

-- Name: link; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE link (
    link_id integer NOT NULL,
    type character varying(1) NOT NULL,
    name character varying(255)
);

-- Name: location_ap; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE location_ap (
    location_ap_id integer NOT NULL,
    location_map_id integer,
    ap_plug_and_play_id integer,
    coord_x integer,
    coord_y integer
);

-- Name: location_map; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE location_map (
    location_map_id integer NOT NULL,
    site_id integer,
    bldg_id integer,
    floor numeric(3,0),
    zone numeric(3,0),
    image_file_name character varying(256),
    start_x integer,
    length integer
);

-- Name: location_map_list; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE location_map_list (
    location_map_list_id integer NOT NULL,
    location_map_id integer,
    location_ap_id integer
);

-- Name: location_name; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE location_name (
    location_name_id integer NOT NULL,
    name character varying(64) NOT NULL,
    type numeric(2,0)
);

-- Name: loopback_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE loopback_interface (
    interface_id integer NOT NULL
);

-- Name: mac_filter_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mac_filter_entry (
    mac_filter_entry_id integer NOT NULL,
    mac_filter_group_id integer,
    mac_filter_num numeric(8,0) NOT NULL,
    is_permit numeric(1,0),
    src_mac_address character varying(24) NOT NULL,
    src_address_mask character varying(24),
    table_subtype character varying(32) NOT NULL
);

-- Name: mac_filter_group; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mac_filter_group (
    mac_filter_group_id integer NOT NULL,
    user_id integer NOT NULL,
    name character varying(64) NOT NULL,
    description character varying(256),
    is_public numeric(1,0),
    is_wireless numeric(1,0)
);

-- Name: menu; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE menu (
    menu_id integer NOT NULL,
    caption character varying(32) NOT NULL,
    help_link character varying(18)
);

-- Name: menu_folder; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE menu_folder (
    privilege_id integer NOT NULL,
    open_icon_name character varying(64),
    close_icon_name character varying(64),
    menu_folder_id integer
);

-- Name: menu_item; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE menu_item (
    privilege_id integer NOT NULL,
    icon_name character varying(64),
    url character varying(256) NOT NULL,
    menu_folder_id integer,
    selected_icon_name character varying(64)
);

-- Name: metadata_feature; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE metadata_feature (
    feature_id integer NOT NULL,
    feature_type character varying(128) NOT NULL,
    feature_name character varying(128) NOT NULL,
    user_id integer NOT NULL,
    is_independent numeric(1,0) NOT NULL,
    xml_instance bytea NOT NULL,
    key1 character varying(128),
    key2 character varying(128),
    last_updated_time numeric(20,0),
    is_internal numeric(1,0)
);

-- Name: mib_object; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mib_object (
    mib_object_id integer NOT NULL,
    oid character varying(128) NOT NULL,
    name character varying(64),
    value_type numeric(2,0),
    target_type numeric(2,0)
);

-- Name: module; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE module (
    module_id integer NOT NULL,
    description character varying(128),
    num_ports numeric(4,0),
    table_subtype character varying(32) NOT NULL,
    is_present numeric(1,0),
    is_management_module numeric(1,0),
    num_cpus smallint DEFAULT 0 NOT NULL,
    hw_revision character varying(64),
    fw_revision character varying(64),
    sw_revision character varying(64)
);

-- Name: module_slot_present; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE module_slot_present (
    module_slot_present_id integer NOT NULL,
    module_id integer NOT NULL,
    slot_id integer NOT NULL
);

-- Name: module_type; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE module_type (
    module_type_id integer NOT NULL,
    module_type numeric(4,0),
    name character varying(32),
    description character varying(128),
    num_ports numeric(4,0)
);

-- Name: mpls_admin_group; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mpls_admin_group (
    mpls_admin_group_db_id integer NOT NULL,
    name character varying(255) NOT NULL,
    id integer NOT NULL,
    device_id integer NOT NULL
);

-- Name: mpls_admin_group_interface_relation; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE mpls_admin_group_interface_relation (
    mpls_admin_group_interface_relation_db_id integer NOT NULL,
    mpls_admin_group_db_id integer NOT NULL,
    interface_id integer NOT NULL
);

-- Name: mpls_lsp; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mpls_lsp (
    mpls_lsp_db_id integer NOT NULL,
    table_subtype character varying(32) NOT NULL,
    name character varying(255) NOT NULL,
    destination_ip_address character varying(255) NOT NULL,
    oper_status smallint NOT NULL,
    device_id integer NOT NULL
);

-- Name: mpls_path; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mpls_path (
    mpls_path_db_id integer NOT NULL,
    name character varying(255) NOT NULL,
    device_id integer NOT NULL
);

-- Name: mpls_path_hop; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mpls_path_hop (
    mpls_path_hop_db_id integer NOT NULL,
    hop_index integer NOT NULL,
    hop_ip_address character varying(255) NOT NULL,
    hop_type smallint NOT NULL,
    mpls_path_db_id integer NOT NULL
);

-- Name: mpls_rsvp_lsp; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mpls_rsvp_lsp (
    mpls_lsp_db_id integer NOT NULL,
    is_enabled numeric(1,0) NOT NULL,
    is_bypass numeric(1,0) NOT NULL,
    from_ip_address character varying(255),
    metric integer,
    path_select_mode smallint,
    path_select_path character varying(255),
    revert_timer integer,
    tie_breaking_mode smallint,
    is_use_lsp_for_ospf_shortcuts numeric(1,0)
);

-- Name: mpls_rsvp_lsp_actually_routed_hop; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE mpls_rsvp_lsp_actually_routed_hop (
    mpls_rsvp_lsp_actually_routed_hop_db_id integer NOT NULL,
    hop_index integer NOT NULL,
    hop_ip_address character varying(255) NOT NULL,
    mpls_lsp_db_id integer NOT NULL
);

-- Name: mpls_rsvp_lsp_admin_group; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE mpls_rsvp_lsp_admin_group (
    mpls_rsvp_lsp_admin_group_db_id integer NOT NULL,
    affinity_type smallint NOT NULL,
    mpls_admin_group_db_id integer NOT NULL,
    mpls_rsvp_lsp_admin_group_container_db_id integer NOT NULL
```

```
);

-- Name: mpls_rsvp_lsp_admin_group_container; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE mpls_rsvp_lsp_admin_group_container (
    mpls_rsvp_lsp_admin_group_container_db_id integer NOT NULL,
    mpls_rsvp_lsp_parameters_db_id integer,
    mpls_rsvp_lsp_frr_parameters_db_id integer
);

-- Name: mpls_rsvp_lsp_frr_parameters; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE mpls_rsvp_lsp_frr_parameters (
    mpls_rsvp_lsp_frr_parameters_db_id integer NOT NULL,
    bandwidth integer NOT NULL,
    hop_limit numeric(3,0) NOT NULL,
    is_facility_backup numeric(1,0) NOT NULL,
    setup_priority numeric(1,0) NOT NULL,
    hold_priority numeric(1,0) NOT NULL,
    mpls_lsp_db_id integer
);

-- Name: mpls_rsvp_lsp_parameters; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE mpls_rsvp_lsp_parameters (
    mpls_rsvp_lsp_parameters_db_id integer NOT NULL,
    is_adaptive numeric(1,0) NOT NULL,
    bfd_transmit integer,
    bfd_receive integer,
    bfd_multiplier integer,
    cos numeric(1,0),
    hop_limit numeric(3,0),
    is_cspf numeric(1,0) NOT NULL,
    mtu numeric(4,0),
    setup_priority numeric(1,0),
    hold_priority numeric(1,0),
    is_record_routes numeric(1,0) NOT NULL,
    reoptimize_timer integer,
    mpls_lsp_db_id integer,
    mpls_rsvp_lsp_path_db_id integer
);

-- Name: mpls_rsvp_lsp_path; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE mpls_rsvp_lsp_path (
    mpls_rsvp_lsp_path_db_id integer NOT NULL,
    path_type smallint NOT NULL,
    is_standby numeric(1,0) NOT NULL default 0,
    mpls_lsp_db_id integer NOT NULL,
    mpls_path_db_id integer NOT NULL
);

-- Name: mpls_rsvp_lsp_tunnel_resource; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE mpls_rsvp_lsp_tunnel_resource (
    mpls_rsvp_lsp_tunnel_resource_db_id integer NOT NULL,
    max_rate integer,
    mean_rate integer,
    max_burst integer,
    mpls_rsvp_lsp_parameters_db_id integer
```

```
);

-- Name: mpls_service; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mpls_service (
    mpls_service_db_id integer NOT NULL,
    name character varying(255) NOT NULL,
    vcid bigint NOT NULL,
    mpls_service_type smallint NOT NULL,
    vll_mode smallint,
    status smallint NOT NULL,
    conflicts integer NOT NULL,
    last_updated_time numeric(20,0)
);

-- Name: mpls_service_device_relation; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE mpls_service_device_relation (
    mpls_service_device_relation_db_id integer NOT NULL,
    mpls_service_db_id integer,
    device_id integer NOT NULL,
    table_subtype character varying(32) NOT NULL,
    name character varying(255) NOT NULL,
    cos smallint NOT NULL,
    mtu integer NOT NULL
);

-- Name: mpls_service_endpoint_relation; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE mpls_service_endpoint_relation (
    mpls_service_endpoint_relation_db_id integer NOT NULL,
    mpls_service_device_relation_db_id integer NOT NULL,
    interface_id integer NOT NULL,
    table_subtype character varying(32) NOT NULL,
    tag_mode smallint NOT NULL,
    vlan_id smallint NOT NULL,
    oper_status numeric(2,0) NOT NULL
);

-- Name: mpls_service_peer_relation; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE mpls_service_peer_relation (
    mpls_service_peer_relation_db_id integer NOT NULL,
    mpls_service_device_relation_db_id integer NOT NULL,
    peer_device_id integer,
    pw_index integer NOT NULL,
    peer_ip character varying(255),
    oper_status smallint NOT NULL
);

-- Name: mrp_ring; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mrp_ring (
    mrp_ring_id integer NOT NULL,
    ring_id numeric(8,0) NOT NULL,
    ring_name character varying(255),
    status smallint DEFAULT 1 NOT NULL,
    last_updated bigint NOT NULL
);

-- Name: mrp_ring_device; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE mrp_ring_device (
    mrp_ring_device_db_id integer NOT NULL,
    mrp_ring_id integer NOT NULL,
    device_id integer NOT NULL,
    port_vlan_db_id integer DEFAULT 0 NOT NULL,
    mrp_ring_name character varying(255),
    topo_grp_id integer DEFAULT 0 NOT NULL,
    state smallint NOT NULL,
    role smallint NOT NULL,
    hello_time integer NOT NULL,
    pre_fwd_time integer NOT NULL,
    pri_port_interface_id integer DEFAULT 0 NOT NULL,
    pri_port_state smallint NOT NULL,
    pri_port_type smallint NOT NULL,
    pri_port_active_interface_id integer DEFAULT 0 NOT NULL,
    sec_port_interface_id integer DEFAULT 0 NOT NULL,
    sec_port_state smallint NOT NULL,
    sec_port_type smallint NOT NULL,
    sec_port_active_interface_id integer DEFAULT 0 NOT NULL,
    rhp_tx bigint NOT NULL,
    rhp_rc bigint NOT NULL,
    state_changed integer NOT NULL,
    tc_bpdu_rc integer NOT NULL,
    status smallint DEFAULT 1 NOT NULL,
    last_updated bigint NOT NULL
);

-- Name: network_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE network_vlan (
    vlan_db_id integer NOT NULL
);

-- Name: physical_device; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE physical_device (
    physical_device_id integer NOT NULL,
    device_id integer NOT NULL,
    description character varying(255),
    num_slots numeric(4,0),
    table_subtype character varying(32) NOT NULL,
    unit_number numeric(2,0) DEFAULT 0 NOT NULL,
    unit_neighbor1 numeric(2,0),
    unit_neighbor2 numeric(2,0),
    unit_present numeric(1,0)
);

-- Name: physical_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE physical_interface (
    interface_id integer NOT NULL,
    physical_port_id integer,
    speed_in_mb integer,
    physical_address character varying(64),
    link_id integer,
    duplex_mode smallint,
    is_stacking_interface numeric(1,0),
    is_port_present integer DEFAULT 0
);

-- Name: physical_port; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE physical_port (
    physical_port_id integer NOT NULL,
    port_num smallint NOT NULL,
    module_id integer NOT NULL,
    is_port_present smallint,
    table_subtype character varying(32) NOT NULL
);

-- Name: policy; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE policy (
    policy_id integer NOT NULL,
    name character varying(64) NOT NULL,
    user_id integer,
    is_public numeric(1,0),
    description character varying(256)
);

-- Name: policy_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE policy_entry (
    policy_entry_id integer NOT NULL,
    policy_id integer,
    policy_type character(1),
    average_rate numeric(20,3),
    average_rate_type character(1),
    target_type character(1),
    table_subtype character varying(32) NOT NULL
);

-- Name: ip_port_group; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ip_port_group (
    port_group_id integer NOT NULL,
    name character varying(64) NOT NULL,
    user_id integer NOT NULL,
    description character varying(255),
    is_public numeric(1,0),
    is_ap_group numeric(1,0) DEFAULT 0 NOT NULL
);

-- Name: port_group_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE port_group_entry (
    port_group_entry_id integer NOT NULL,
    device_id integer NOT NULL,
    port_group_id integer NOT NULL,
    slot_num smallint,
    port_num smallint,
    unit_num smallint DEFAULT 0 NOT NULL
);

-- Name: port_range_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE port_range_spec (
    port_spec_id integer NOT NULL,
    operator character varying(8),
    start_port numeric(6,0),
    end_port numeric(6,0)
);

-- Name: port_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE port_spec (
    port_spec_id integer NOT NULL,
    table_subtype character varying(32) NOT NULL
);
```

```
-- Name: port_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE port_vlan (
    vlan_db_id integer NOT NULL,
    stp numeric(1,0),
    vlan_id smallint NOT NULL,
    qos smallint,
    global_vlan_db_id integer,
    stp_instance_id integer
);

-- Name: pos_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE pos_interface (
    interface_id integer NOT NULL
);

-- Name: inm_privilege; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE inm_privilege (
    privilege_id integer NOT NULL,
    name character varying(64) NOT NULL,
    description character varying(64),
    table_subtype character varying(32) NOT NULL
);

-- Name: privilege_dyn; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE privilege_dyn (
    privilege_dyn_id integer NOT NULL,
    name character varying(64) NOT NULL,
    flag numeric(2,0) NOT NULL
);

-- Name: privilege_menu; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE privilege_menu (
    privilege_id integer NOT NULL,
    menu_id integer,
    sequence numeric(6,0),
    help_link character varying(18),
    tool_tip character varying(128)
);

-- Name: protocol_definition; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE protocol_definition (
    protocol_definition_id integer NOT NULL,
    protocol numeric(4,0),
    name character varying(64)
);

-- Name: protocol_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE protocol_vlan (
    vlan_db_id integer NOT NULL,
    protocol numeric(4,0) NOT NULL
);

-- Name: pseudo_event; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE pseudo_event (
    pseudo_event_id integer NOT NULL,
    status character(1),
    policy_type character varying(32),
    severity smallint,
    user_id integer NOT NULL,
    last_updated bigint,
    name character varying(64) NOT NULL,
    messages character varying(255),
    policy_desc character varying(255)
);

-- Name: query_based_device_group; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE query_based_device_group (
    device_group_id integer NOT NULL,
    query_text character varying(512)
);

-- Name: radio_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE radio_interface (
    interface_id integer NOT NULL,
    radio_type numeric(2,0) NOT NULL,
    is_enabled numeric(1,0),
    is_auto_channel numeric(1,0),
    tx_power character varying(20),
    channel_number numeric(3,0),
    max_data_rate integer,
    beacon_rate integer,
    dtim integer,
    rts_threshold integer,
    is_turbo_mode numeric(1,0),
    radio_g_mode numeric(2,0),
    max_associated_clients numeric(3,0)
);

-- Name: realm_policy; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE realm_policy (
    realm_policy_id integer NOT NULL,
    user_id integer,
    ssid character varying(64) NOT NULL,
    description character varying(256),
    realm_name character varying(64)
);

-- Name: realm_upgrade_temp; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE realm_upgrade_temp (
    old_realm_id integer NOT NULL,
    radio_type numeric(2,0) NOT NULL,
    new_realm_id integer NOT NULL
);

-- Name: report_data_source; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE report_data_source (
    report_data_source_id integer NOT NULL,
    report_definition_id integer NOT NULL,
    device_id integer,
    device_group_id integer,
    interface_id integer,
    port_group_id integer,
    object_id integer,
    object_class_name character varying(256),
    object_id2 integer,
    object_class_name2 character varying(256)
```

```
);

-- Name: report_definition; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE report_definition (
    report_definition_id integer NOT NULL,
    name character varying(64) NOT NULL,
    category character varying(20) NOT NULL,
    user_id integer NOT NULL,
    type numeric(2,0) NOT NULL,
    last_modified character varying(64) NOT NULL,
    description character varying(128),
    definition character varying NOT NULL,
    is_with_data_source numeric(1,0),
    prompt numeric(1,0) DEFAULT 0,
    is_prompt_fields_filled numeric(1,0)
);

-- Name: report_definition_schedule; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE report_definition_schedule (
    report_definition_schedule_id integer NOT NULL,
    name character varying(64) NOT NULL,
    user_id integer NOT NULL,
    is_enable_email numeric(1,0),
    suspend_schedule numeric(1) not null,
    other_recipients character varying(255) default '' not null,
    replyto character varying(255) default '' not null,
    subject character varying(255),
    prologue character varying(255),
    epilogue character varying(255),
    report_format_type character varying(4),
    report_definition_id integer NOT NULL,
    schedule_entry_id integer,
    was_run numeric(1,0) DEFAULT 0
);

-- Name: report_definition_share; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE report_definition_share (
    report_definition_share_id integer NOT NULL,
    report_definition_id integer NOT NULL,
    role_id integer,
    user_id integer,
    permission numeric(2,0) NOT NULL
);

-- Name: rf_overview; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE rf_overview (
    unknown_total integer,
    unknown_up integer,
    unknown_down integer,
    known_total integer,
    known_up integer,
    known_down integer,
    rogue_total integer,
    rogue_up integer,
    rogue_down integer,
    managed_total integer,
    managed_up integer,
    managed_down integer,
    sensor_total integer,
    sensor_up integer,
    sensor_down integer,
    sensor_relief integer,
    last_viewed_timestamp bigint NOT NULL
);

-- Name: rf_overview_logs; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE rf_overview_logs (
    log_timestamp bigint NOT NULL,
    log_message character varying(512) NOT NULL
);

-- Name: rfmon_ap; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE rfmon_ap (
    sqnum integer NOT NULL,
    time_stamp bigint,
    device_id integer NOT NULL,
    sys_up_time integer,
    channelnumber integer,
    macaddress character varying(17),
    bssid character varying(17),
    rssi integer,
    ssidlen smallint,
    ssid character varying(256),
    ipaddress character varying(40),
    beaconinterval integer,
    authtype smallint,
    radiotype smallint,
    networkmode smallint,
    shortpreamblemode smallint,
    rsnsupported smallint,
    rsnvernum integer,
    protectedmode smallint,
    supergmode smallint,
    pcfApplication_Nameode smallint,
    wepenabled smallint,
    onexenabled smallint,
    channelagility integer,
    numberofclients integer,
    ratesupported character varying(256),
    extratesupported character varying(256),
    firstseen integer,
    lastupdated integer,
    mgmtpktsrx integer,
    ucastpktsrx integer,
    mcastpktsrx integer,
    bcastpktsrx integer,
    octetsrx integer,
    mgmtpktstx integer,
    ucastpktstx integer,
    mcastpktstx integer,
    bcastpktstx integer,
    octetstx integer,
    dtimcount integer,
    dtimperiod integer,
    onexeaptype integer,
    rsnencrypttype integer,
    totalframestx integer,
    totalframesrx integer,
    totalcrcerrframes integer,
    totalfragerrframes integer,
    totalretryframes integer,
    totalassocreq integer,
    totalassocresp integer,
    totalreassocreq integer,
    totalreassocresp integer,
    totalprobereq integer,
    totalproberesp integer,
    totalbeacon integer,
    totaldisassoc integer,
    totalauth integer,
    totaldeauth integer,
    totalcriticalalerts integer,
    totalmoderatealerts integer,
    totalminor integer
);

-- Name: rfmon_ap_last_saved; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE rfmon_ap_last_saved (
    device_id integer NOT NULL,
    time_stamp bigint NOT NULL
);

-- Name: rfmon_channel; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE rfmon_channel (
    sqnum integer NOT NULL,
    time_stamp bigint,
    device_id integer NOT NULL,
    sys_up_time integer,
    channelnum smallint,
    channelnumaps integer,
    channelnumstas integer,
    channelnummcastpkts integer,
    channelnumucastpkts integer,
    channelnumbcastpkts integer,
    channelnumofretries integer,
    channelnumoffragments integer,
    channelnumofcrcerr integer,
    channelnoiselevel integer
);

-- Name: rfmon_channel_last_saved; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE rfmon_channel_last_saved (
    device_id integer NOT NULL,
    time_stamp bigint NOT NULL
);

-- Name: rfmon_station; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE rfmon_station (
    sqnum integer NOT NULL,
    time_stamp bigint,
    device_id integer NOT NULL,
    sys_up_time integer,
    macaddress character varying(17),
    channelnumber integer,
    apmacaddress character varying(17),
    apchannelnumber smallint,
    authtype smallint,
    networkmode smallint,
    wepenabled smallint,
    cfpollable smallint,
    shortpreamblemode smallint,
    rsnsupported smallint,
    onexenabled smallint,
    shortslottime integer,
    failedreassocattempts integer,
    failedassocattempts integer,
    associateid integer,
    rssi integer,
    listeninterval integer,
    ssidlen smallint,
    ssid character varying(256),
    ipaddress character varying(40),
    deauthreasoncode integer,
    deassocreasoncode integer,
    ratesupported character varying(256),
    extratesupported character varying(256),
    firstseen integer,
    lastupdated integer,
    mgmtpktsrx integer,
    ucastpktsrx integer,
    mcastpktsrx integer,
    bcastpktsrx integer,
    octetsrx integer,
    mgmtpktstx integer,
    ucastpktstx integer,
    mcastpktstx integer,
    bcastpktstx integer,
    octetstx integer,
    authfailure integer,
    assocfailure integer
);

-- Name: rfmon_station_last_saved; Type: TABLE; Schema: dcm; Owner: dcmadmin; 
Tablespace:
CREATE TABLE rfmon_station_last_saved (
    device_id integer NOT NULL,
    time_stamp bigint NOT NULL
);

-- Name: ring_status; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ring_status (
    ring_status_id integer NOT NULL,
    mrp_ring_id integer NOT NULL,
    state_id integer NOT NULL,
    last_updated bigint NOT NULL
);

-- Name: rl_access_control_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin; 
Tablespace:
CREATE TABLE rl_access_control_entry (
    rl_access_control_entry_id integer NOT NULL,
    rl_access_control_list_id integer,
    table_subtype character varying(32) NOT NULL
);
```

```
-- Name: rl_access_control_group; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE rl_access_control_group (
    rl_access_control_group_id integer NOT NULL,
    name character varying(64) NOT NULL,
    user_id integer,
    is_public numeric(1,0),
    description character varying(256)
);

-- Name: rl_access_control_list; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE rl_access_control_list (
    rl_access_control_list_id integer NOT NULL,
    rl_acl_num numeric(8,0) NOT NULL,
    is_standard numeric(1,0) NOT NULL,
    rl_access_control_group_id integer
);

-- Name: rl_acl_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE rl_acl_spec (
    acl_spec_id integer NOT NULL,
    rl_access_control_list_id integer
);

-- Name: rl_extended_access_control_entry; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE rl_extended_access_control_entry (
    rl_access_control_entry_id integer NOT NULL,
    mac_address character varying(14)
);

-- Name: rl_standard_access_control_entry; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE rl_standard_access_control_entry (
    rl_access_control_entry_id integer NOT NULL,
    precedence numeric(4,0),
    precedence_mask numeric(6,0)
);

-- Name: inm_role; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE inm_role (
    role_id integer NOT NULL,
    access_scope_id integer,
    name character varying(64) NOT NULL,
    description character varying(64),
    is_device_access_role numeric(1,0) DEFAULT 0 NOT NULL
);

-- Name: role_accessible_entity; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE role_accessible_entity (
    role_accessible_entity_id integer NOT NULL,
    accessible_entity_id integer,
    role_id integer
);

-- Name: role_privilege; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE role_privilege (
    role_privilege_id integer NOT NULL,
    privilege_id integer NOT NULL,
    role_id integer NOT NULL
);

-- Name: routing_service; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE routing_service (
    service_id integer NOT NULL
);

-- Name: scenario; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE scenario (
    scenario_id integer NOT NULL,
    name character varying(256) NOT NULL,
    user_id integer NOT NULL,
    description character varying(1024),
    is_internal numeric(1,0) NOT NULL,
    creation_time character varying(16) NOT NULL,
    type_num integer DEFAULT 1 NOT NULL,
    mark_internal numeric(1,0) DEFAULT 0,
    is_wireless numeric(1,0)
);

-- Name: scenario_binding; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE scenario_binding (
    scenario_binding_id integer NOT NULL,
    scenario_id integer NOT NULL,
    device_config_id integer NOT NULL,
    sequence_num smallint,
    table_subtype character varying(32) NOT NULL
);

-- Name: scenario_device_binding; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE scenario_device_binding (
    device_id integer NOT NULL,
    scenario_binding_id integer NOT NULL
);

-- Name: scenario_device_group_binding; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE scenario_device_group_binding (
    scenario_binding_id integer NOT NULL,
    device_group_id integer NOT NULL
);

-- Name: scenario_dummy_binding; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE scenario_dummy_binding (
    scenario_binding_id integer NOT NULL
);

-- Name: scenario_interface_device_group; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE scenario_interface_device_group (
    device_group_id integer NOT NULL,
    scenario_id integer NOT NULL,
    group_type numeric(2,0) NOT NULL
);
```

```
-- Name: scenario_port_binding; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE scenario_port_binding (
    scenario_binding_id integer NOT NULL,
    interface_id integer NOT NULL
);

-- Name: scenario_port_group_binding; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE scenario_port_group_binding (
    port_group_id integer NOT NULL,
    scenario_binding_id integer NOT NULL
);

-- Name: schedule_email_user; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE schedule_email_user (
    schedule_email_user_id integer NOT NULL,
    report_definition_schedule_id integer,
    user_id integer,
    type numeric(2,0)
);

-- Name: schedule_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE schedule_entry (
    schedule_entry_id integer NOT NULL,
    module character varying(128) NOT NULL,
    user_id integer NOT NULL,
    minutes character varying(256),
    identity character varying(16) NOT NULL,
    hours character varying(64),
    week_days character varying(16),
    days character varying(128),
    months character varying(32),
    years character varying(64),
    type numeric(4,0),
    status character(1) NOT NULL,
    duration bigint DEFAULT 0 NOT NULL,
    table_name character varying(128)
);

-- Name: service; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE service (
    service_id integer NOT NULL,
    device_id integer NOT NULL,
    table_subtype character varying(32) NOT NULL
);

-- Name: service_group; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE service_group (
    service_group_id integer NOT NULL,
    name character varying(64) NOT NULL
);

-- Name: service_group_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE service_group_entry (
    service_group_entry_id integer NOT NULL,
    parent_service_group_id integer NOT NULL,
    child_service_group_id integer NOT NULL
```

```
);

-- Name: service_group_spec; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE service_group_spec (
    port_spec_id integer NOT NULL,
    service_group_id integer
);

-- Name: service_name_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE service_name_entry (
    service_name_entry_id integer NOT NULL,
    service_group_id integer NOT NULL,
    service_port_definition_id integer NOT NULL,
    name character varying(32)
);

-- Name: service_port_definition; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE service_port_definition (
    service_port_definition_id integer NOT NULL,
    port_num numeric(6,0),
    name character varying(32) NOT NULL,
    protocol numeric(4,0) DEFAULT 0 NOT NULL,
    is_user_defined numeric(1,0)
);

-- Name: service_port_range_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE service_port_range_entry (
    service_port_range_entry_id integer NOT NULL,
    service_group_id integer NOT NULL,
    port_num_low numeric(6,0),
    port_num_high numeric(6,0)
);

create table SFLOW_STAGING
(
  SLNUM bigserial not null,
  TIME_IN_SECONDS integer not null,
  DEVICE_ID integer not null,
  IN_UNIT smallint default 0,
  IN_SLOT smallint,
  IN_PORT smallint,
  OUT_UNIT smallint default 0,
  OUT_SLOT smallint,
  OUT_PORT smallint,
  IN_VLAN smallint,
  OUT_VLAN smallint,
  IN_PRIORITY smallint,
  OUT_PRIORITY smallint,
  SRC_MAC bytea,
  DEST_MAC bytea,
  L3_SRC_ADDR bytea,
  L3_DEST_ADDR bytea,
  L3_PROTOCOL integer not null,
  IP_TOS smallint,
  L4_PROTOCOL smallint,
  L4_SRC_PORT integer,
  L4_DEST_PORT integer,
  SRC_SUBNET_BITS smallint,
  DEST_SUBNET_BITS smallint,
  LOCAL_AS bigint,
  SRC_AS bigint,
  SRC_PEER_AS bigint,
  SFLOW_IP_ROUTE_INFO_ID integer,
  IP_FLOW_LABEL integer,
  SRC_USER integer,
  DEST_USER integer,
  FRAMES bigint not null,
  BYTES bigint not null,
  TCP_FLAGS smallint
);

create table SFLOW_STAGING_SLNUM
(
  MIN_SLNUM bigint
) with (autovacuum_vacuum_threshold=4);

-- Name: sflow_hour_summary; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
create table SFLOW_HOUR_SUMMARY
(
  SLNUM bigserial not null,
  TIME_IN_SECONDS integer not null,
  DEVICE_ID integer not null,
  IN_UNIT smallint default 0,
  IN_SLOT smallint,
  IN_PORT smallint,
  OUT_UNIT smallint default 0,
  OUT_SLOT smallint,
  OUT_PORT smallint,
  IN_VLAN smallint,
  OUT_VLAN smallint,
  IN_PRIORITY smallint,
  OUT_PRIORITY smallint,
  SRC_MAC bytea,
  DEST_MAC bytea,
  L3_SRC_ADDR bytea,
  L3_DEST_ADDR bytea,
  L3_PROTOCOL integer not null,
  IP_TOS smallint,
  L4_PROTOCOL smallint,
  L4_SRC_PORT integer,
  L4_DEST_PORT integer,
  SRC_SUBNET_BITS smallint,
  DEST_SUBNET_BITS smallint,
  LOCAL_AS bigint,
  SRC_AS bigint,
  SRC_PEER_AS bigint,
  SFLOW_IP_ROUTE_INFO_ID integer,
  IP_FLOW_LABEL integer,
  SRC_USER integer,
  DEST_USER integer,
  FRAMES bigint not null,
  BYTES bigint not null,
  TCP_FLAGS smallint
);
```

```
create table SFLOW_HOUR_SUMMARY_SLNUM (
  MAX_SLNUM bigint
) with (autovacuum_vacuum_threshold=4);

-- Name: sflow; Type: VIEW; Schema: dcm; Owner: dcmadmin
create or replace view SFLOW as
  select DEVICE_ID, IN_SLOT, IN_PORT, OUT_SLOT, OUT_PORT, L4_PROTOCOL, IP_TOS,
SRC_SUBNET_BITS, DEST_SUBNET_BITS, IN_PRIORITY, OUT_PRIORITY, IN_VLAN, OUT_VLAN,
L3_PROTOCOL, L4_SRC_PORT, L4_DEST_PORT, TIME_IN_SECONDS, SRC_MAC, DEST_MAC,
L3_SRC_ADDR, L3_DEST_ADDR, TCP_FLAGS, LOCAL_AS, SRC_AS, SRC_PEER_AS,
SFLOW_IP_ROUTE_INFO_ID, IP_FLOW_LABEL, SRC_USER, DEST_USER, FRAMES, BYTES,
IN_UNIT, OUT_UNIT
  from SFLOW_HOUR_SUMMARY
  where SLNUM <= (select MAX_SLNUM from SFLOW_HOUR_SUMMARY_SLNUM fetch first 1
rows only)
  union all
  select DEVICE_ID, IN_SLOT, IN_PORT, OUT_SLOT, OUT_PORT, L4_PROTOCOL, IP_TOS,
SRC_SUBNET_BITS, DEST_SUBNET_BITS, IN_PRIORITY, OUT_PRIORITY, IN_VLAN, OUT_VLAN,
L3_PROTOCOL, L4_SRC_PORT, L4_DEST_PORT, TIME_IN_SECONDS, SRC_MAC, DEST_MAC,
L3_SRC_ADDR, L3_DEST_ADDR, TCP_FLAGS, LOCAL_AS, SRC_AS, SRC_PEER_AS,
SFLOW_IP_ROUTE_INFO_ID, IP_FLOW_LABEL, SRC_USER, DEST_USER, FRAMES, BYTES,
IN_UNIT, OUT_UNIT
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only);

-- Name: sflow_checkpoint; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
create table SFLOW_CHECKPOINT
(
  TABLE_TO_DROP character varying(40)
);

-- Name: sflow_ip_route_info; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE sflow_ip_route_info (
    sflow_ip_route_info_id integer NOT NULL,
    local_pref integer,
    last_used_time integer,
    dst_as_path character varying(2048),
    communities character varying(1024)
);

-- Name: sflow_minute_bgp; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
create table SFLOW_MINUTE_BGP
(
  SLNUM bigserial not null,
  TIME_IN_SECONDS integer not null,
  DEVICE_ID integer not null,
  SRC_AS bigint,
  SFLOW_IP_ROUTE_INFO_ID integer,
  IN_VLAN smallint,
  OUT_VLAN smallint,
  FRAMES bigint not null,
  BYTES bigint not null
);

create table SFLOW_MINUTE_BGP_SLNUM (
  MAX_SLNUM bigint
) with (autovacuum_vacuum_threshold=4);
```

```
-- Name: sflow_minute_bgp_view; Type: VIEW; Schema: dcm; Owner: dcmadmin
create or replace view SFLOW_MINUTE_BGP_VIEW as
  select DEVICE_ID, TIME_IN_SECONDS, SRC_AS, SFLOW_IP_ROUTE_INFO_ID, IN_VLAN,
OUT_VLAN, FRAMES, BYTES
  from SFLOW_MINUTE_BGP
  where SLNUM <= (select MAX_SLNUM from SFLOW_MINUTE_BGP_SLNUM fetch first 1 rows
only)
  union all
  select DEVICE_ID, TIME_IN_SECONDS, SRC_AS, SFLOW_IP_ROUTE_INFO_ID, IN_VLAN,
OUT_VLAN, FRAMES, BYTES
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only)
  and SRC_AS != 0 OR SFLOW_IP_ROUTE_INFO_ID != 0;

-- Name: sflow_minute_l3; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
create table SFLOW_MINUTE_L3
(
  SLNUM bigserial not null,
  DEVICE_ID integer not null,
  TIME_IN_SECONDS integer not null,
  L3_PROTOCOL integer not null,
  L3_SRC_ADDR bytea,
  L3_DEST_ADDR bytea,
  L4_PROTOCOL smallint,
  FRAMES bigint not null,
  BYTES bigint not null,
  IN_VLAN smallint,
  OUT_VLAN smallint,
  TCP_FLAGS smallint
);

-- Name: sflow_minute_l3_pk; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
create table SFLOW_MINUTE_L3_SLNUM (
  MAX_SLNUM bigint
) with (autovacuum_vacuum_threshold=4);

-- Name: sflow_minute_l3_view; Type: VIEW; Schema: dcm; Owner: dcmadmin
create or replace view SFLOW_MINUTE_L3_VIEW as
  select DEVICE_ID, TIME_IN_SECONDS, L3_SRC_ADDR, L3_DEST_ADDR, L3_PROTOCOL,
L4_PROTOCOL, TCP_FLAGS, IN_VLAN, OUT_VLAN, FRAMES, BYTES
  from SFLOW_MINUTE_L3
  where SLNUM <= (select MAX_SLNUM from SFLOW_MINUTE_L3_SLNUM fetch first 1 rows
only)
  union all
  select DEVICE_ID, TIME_IN_SECONDS, L3_SRC_ADDR, L3_DEST_ADDR, L3_PROTOCOL,
L4_PROTOCOL, TCP_FLAGS, IN_VLAN, OUT_VLAN, FRAMES, BYTES
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only);

-- Name: sflow_minute_mac; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
create table SFLOW_MINUTE_MAC
(
  SLNUM bigserial not null,
  TIME_IN_SECONDS integer not null,
  DEVICE_ID integer not null,
  FRAMES bigint not null,
  BYTES bigint not null,
  IN_VLAN smallint,
  OUT_VLAN smallint,
  SRC_MAC bytea,
  DEST_MAC bytea
);

create table SFLOW_MINUTE_MAC_SLNUM (
  MAX_SLNUM bigint
) with (autovacuum_vacuum_threshold=4);

-- Name: sflow_minute_mac_view; Type: VIEW; Schema: dcm; Owner: dcmadmin
create or replace view SFLOW_MINUTE_MAC_VIEW as
  select DEVICE_ID, TIME_IN_SECONDS, SRC_MAC, DEST_MAC, IN_VLAN, OUT_VLAN, FRAMES, 
BYTES
  from SFLOW_MINUTE_MAC
  where SLNUM <= (select MAX_SLNUM from SFLOW_MINUTE_MAC_SLNUM fetch first 1 rows 
only)
  union all
  select DEVICE_ID, TIME_IN_SECONDS, SRC_MAC, DEST_MAC, IN_VLAN, OUT_VLAN, FRAMES, 
BYTES
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows 
only);

-- Name: sflow_minute_summary; Type: TABLE; Schema: dcm; Owner: dcmadmin; 
Tablespace:
create table SFLOW_MINUTE_SUMMARY
(
  SLNUM bigserial not null,
  TIME_IN_SECONDS integer not null,
  DEVICE_ID integer not null,
  FRAMES bigint not null,
  BYTES bigint not null
);

-- Name: sflow_minute_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
create table SFLOW_MINUTE_VLAN
(
  SLNUM bigserial not null,
  TIME_IN_SECONDS integer not null,
  DEVICE_ID integer not null,
  FRAMES bigint not null,
  BYTES bigint not null,
  IN_VLAN smallint,
  OUT_VLAN smallint
);

create table SFLOW_MINUTE_VLAN_SLNUM (
  MAX_SLNUM bigint
) with (autovacuum_vacuum_threshold=4);

-- Name: sflow_minute_vlan_view; Type: VIEW; Schema: dcm; Owner: dcmadmin
create or replace view SFLOW_MINUTE_VLAN_VIEW as
  select DEVICE_ID, TIME_IN_SECONDS, IN_VLAN, OUT_VLAN, FRAMES, BYTES
  from SFLOW_MINUTE_VLAN
  where SLNUM <= (select MAX_SLNUM from SFLOW_MINUTE_VLAN_SLNUM fetch first 1 rows 
only)
  union all
  select DEVICE_ID, TIME_IN_SECONDS, IN_VLAN, OUT_VLAN, FRAMES, BYTES
  from SFLOW_STAGING
  where SLNUM >= (select MIN_SLNUM from SFLOW_STAGING_SLNUM fetch first 1 rows
only);

-- Name: sflow_report_l3_source; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE sflow_report_l3_source (
    sflow_report_l3_source_id integer NOT NULL,
    report_definition_id integer NOT NULL,
    address_group_id integer,
    ip_subnet_definition_id integer
);

-- Name: sflow_report_l4_source; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE sflow_report_l4_source (
    sflow_report_l4_source_id integer NOT NULL,
    report_definition_id integer NOT NULL,
    service_port_definition_id integer,
    service_group_id integer
);

-- Name: sharing; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE sharing (
    sharing_id integer NOT NULL,
    object_type character varying(128),
    object_id integer,
    role_id integer,
    user_id integer,
    permission numeric(2,0)
);

-- Name: slot; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE slot (
    slot_id integer NOT NULL,
    physical_device_id integer NOT NULL,
    slot_num numeric(4,0) NOT NULL
);

-- Name: snmp_data; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE snmp_data (
    ID serial not null,
    mib_object_id integer NOT NULL,
    target_type numeric(2,0) NOT NULL,
    target_id integer NOT NULL,
    value double precision NOT NULL,
    time_in_seconds integer NOT NULL,
    collector_id integer NOT NULL,
    mib_index character varying(256) default '',
    constraint PK_SNMP_DATA primary key (ID)
);

-- Name: snmp_expr_data; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE snmp_expr_data (
    ID serial not null,
    expression_id integer NOT NULL,
    target_type smallint NOT NULL,
    target_id integer NOT NULL,
    value double precision NOT NULL,
    time_in_seconds integer NOT NULL,
    collector_id integer NOT NULL,
    constraint PK_SNMP_EXPR_DATA primary key (ID)
);

-- Name: snmp_expression; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
create table SNMP_EXPRESSION (
    EXPRESSION_ID serial not null,
    NAME character varying(64) not null,
    DESCRIPTION character varying(512),
    EQUATION character varying(1024)
);

-- Name: snmp_fwd_aa; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE snmp_fwd_aa (
    snmp_fwd_aa_id integer NOT NULL,
    trap_community character varying(64),
    trap_user character varying(32),
    auth_protocol character varying(8),
    auth_password character varying(64),
    priv_protocol character varying(8),
    priv_password character varying(64),
    engine_id character varying(64) NOT NULL
);

-- Name: snmp_fwd_dev_groups; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE snmp_fwd_dev_groups (
    snmp_fwd_dev_groups_id integer NOT NULL,
    device_group_id integer NOT NULL,
    device_group_name character varying(64) NOT NULL,
    snmp_fwd_filters_id integer NOT NULL
);

-- Name: snmp_fwd_dev_types; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE snmp_fwd_dev_types (
    snmp_fwd_dev_types_id integer NOT NULL,
    device_type character varying(32) NOT NULL,
    snmp_fwd_filters_id integer NOT NULL
);

-- Name: snmp_fwd_devices; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE snmp_fwd_devices (
    snmp_fwd_devices_id integer NOT NULL,
    device_id integer NOT NULL,
    ip_address character varying(40) NOT NULL,
    snmp_fwd_filters_id integer NOT NULL
);

-- Name: snmp_fwd_filters; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE snmp_fwd_filters (
    snmp_fwd_filters_id integer NOT NULL,
    filter_name character varying(255) NOT NULL,
    filter_desc character varying(512),
    is_enable character varying(8) DEFAULT 'Yes'::character varying NOT NULL,
    user_id integer NOT NULL,
    severity smallint,
    inm_event_flag integer DEFAULT 0 NOT NULL
);

-- Name: snmp_fwd_targets; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
```

```
CREATE TABLE snmp_fwd_targets (
    snmp_fwd_targets_id integer NOT NULL,
    is_enable character varying(8) DEFAULT 'Yes'::character varying NOT NULL,
    ip_address character varying(40) NOT NULL,
    snmp_trap_port integer DEFAULT 162 NOT NULL,
    snmp_version character varying(8) DEFAULT 'v2/v3'::character varying NOT NULL,
    snmp_notify_type character varying(1) DEFAULT '1'::character varying NOT NULL,
    snmp_to_nnm character varying(8) DEFAULT 'No'::character varying NOT NULL
);

-- Name: snmp_fwd_trap_oid; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE snmp_fwd_trap_oid (
    snmp_fwd_trap_oid_id integer NOT NULL,
    trap_oid_val character varying(256) NOT NULL,
    trap_oid_name character varying(64),
    snmp_fwd_filters_id integer NOT NULL
);

-- Name: snmp_target_filters; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE snmp_target_filters (
    snmp_target_filters_id integer NOT NULL,
    snmp_fwd_filters_id integer NOT NULL,
    snmp_fwd_targets_id integer NOT NULL
);

-- Name: ssid; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ssid (
    ssid_db_id integer NOT NULL,
    device_id integer,
    ssid character varying(64) NOT NULL,
    vap_num numeric(2,0) NOT NULL,
    realm_policy_id integer
);

-- Name: ssid_auth_8021x; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ssid_auth_8021x (
    ssid_authentication_id integer NOT NULL,
    broadcast_key_refresh_rate integer,
    session_key_refresh_rate integer,
    reauth_refresh_rate integer,
    dot1x_state numeric(2,0)
);

-- Name: ssid_authentication; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE ssid_authentication (
    ssid_authentication_id integer NOT NULL,
    ssid_db_id integer,
    realm_policy_id integer,
    authentication_type numeric(2,0),
    table_subtype character varying(32) NOT NULL,
    is_policy numeric(1,0),
    is_closed_system numeric(1,0),
    radio_type numeric(2,0),
    vlan_id smallint,
    max_clients numeric(4,0),
    vap_state numeric(1,0),
    uiengine_realm_settings_device_config_id integer
);
```

```
-- Name: ssl_certificate; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ssl_certificate (
    ssl_certificate_id integer NOT NULL,
    name character varying(255),
    location character varying(255),
    file_name character varying(255),
    key_id integer NOT NULL,
    cert_type numeric(2,0) NOT NULL,
    start_time numeric(20,0),
    expiration_time numeric(20,0),
    format numeric(2,0) NOT NULL,
    description character varying(1024),
    notification_time numeric(20,0) NOT NULL DEFAULT 0,
    notification_sent numeric(2,0) NOT NULL DEFAULT 0,
    notification_repeat numeric(2,0) NOT NULL DEFAULT 1,
    sync_device numeric(2,0) NOT NULL DEFAULT 0,
    certificate text NOT NULL DEFAULT ''
);

-- Name: ssl_certificate_key_device_binding; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE ssl_certificate_key_device_binding (
    ssl_certificate_key_device_binding_id integer NOT NULL,
    ssl_certificate_id integer,
    ssl_key_id integer,
    device_id integer NOT NULL
);

-- Name: ssl_key; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE ssl_key (
    ssl_key_id integer NOT NULL,
    name character varying(255),
    location character varying(255),
    file_name character varying(255),
    key_type character varying(2),
    encryption_type character varying(2),
    password character varying(255),
    description character varying(1024),
    strength integer NOT NULL DEFAULT 0,
    private_key text NOT NULL DEFAULT ''
);

-- Name: standard_access_control_entry; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE standard_access_control_entry (
    access_control_entry_id integer NOT NULL,
    src_address_spec_id integer NOT NULL
);

-- Name: state; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE state (
    state_id integer NOT NULL,
    category integer NOT NULL,
    state smallint NOT NULL,
    description character varying(255),
    status smallint NOT NULL
);

-- Name: stp_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
```

```
CREATE TABLE stp_entry (
    stp_entry_id integer NOT NULL,
    device_id integer NOT NULL,
    vlan_id integer NOT NULL,
    port_id character varying(32) NOT NULL,
    port_priority smallint NOT NULL,
    path_cost integer NOT NULL,
    port_state smallint NOT NULL,
    designated_cost integer NOT NULL,
    designated_root character varying(32) NOT NULL,
    designated_bridge character varying(32) NOT NULL,
    edge_port smallint NOT NULL,
    p2p smallint NOT NULL,
    oper_path_cost integer NOT NULL,
    port_role smallint NOT NULL,
    bpdu_tx integer NOT NULL,
    bpdu_rx integer NOT NULL,
    cfg_bpdu_rx integer NOT NULL,
    tcn_bpdu_rx integer NOT NULL,
    bridge_id character varying(32),
    last_updated numeric(20,0) NOT NULL
);

-- Name: stp_instance; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE stp_instance (
    stp_instance_id integer NOT NULL,
    instance_type numeric(2,0),
    instance_id numeric(4,0),
    device_id integer NOT NULL,
    stp_mode numeric(2,0),
    forward_delay numeric(2,0),
    max_age numeric(2,0),
    hello_time numeric(2,0),
    priority numeric(6,0),
    stp_version numeric(2,0)
);

-- Name: sub_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE sub_interface (
    sub_interface_id integer NOT NULL,
    interface_id integer NOT NULL,
    sub_interface_vc_id integer NOT NULL
);

-- Name: sub_port_vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE sub_port_vlan (
    vlan_db_id integer NOT NULL,
    port_vlan_db_id integer,
    is_dynamic numeric(1,0)
);

-- Name: switch_service; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE switch_service (
    service_id integer NOT NULL,
    vlan_8021q_tag integer,
    default_vlan_id smallint
);

-- Name: syslog_file_info; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE syslog_file_info (
    row_id integer NOT NULL,
    file_pointer bigint NOT NULL,
    file_name character varying(512)
);

-- Name: system_profile; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE system_profile (
    system_profile_id integer NOT NULL,
    new_installation_update_status character varying(64) NOT NULL,
    db_schema_string character varying(20),
    is_demo_version numeric(1,0),
    demo_expiration_datetime character varying(32),
    is_full_install numeric(1,0) DEFAULT 0,
    serial_number character varying(64),
    system_id character varying(32)
);

-- Name: table_sequence; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE table_sequence (
    table_name character varying(64) NOT NULL,
    id_value integer NOT NULL
);

-- Name: tcp_protocol_flag; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE tcp_protocol_flag (
    tcp_protocol_flag_id integer NOT NULL,
    is_established numeric(1,0)
);

-- Name: third_party_ap; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE third_party_ap (
    device_id integer NOT NULL,
    mac_address character varying(14)
);

-- Name: third_party_device; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE third_party_device (
    device_id integer NOT NULL,
    device_type character varying(64) NOT NULL
);

-- Name: topo_map; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE topo_map (
    topo_map_id serial NOT NULL,
    topo_map_userid integer,
    topo_map_key character varying(512),
    topo_map_imagename character varying(64),
    topo_map_sizex numeric(10,0),
    topo_map_sizey numeric(10,0)
);

-- Name: topo_mapcell; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE topo_mapcell (
    topo_mapcell_id serial NOT NULL,
    topo_map_id integer,
    topo_mapcell_key character varying(255),
    topo_mapcell_coord_x integer,
    topo_mapcell_coord_y integer
);
```

```
-- Name: trap_backup_detail; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE trap_backup_detail (
    cfg_backup_detail_id integer NOT NULL,
    cfg_change_user_name character varying(64),
    trap_log_id integer
);

-- Name: trunk_group_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE trunk_group_interface (
    interface_id integer NOT NULL
);

-- Name: trunk_group_member; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE trunk_group_member (
    trunk_group_member_id integer NOT NULL,
    interface_id integer NOT NULL,
    trunk_interface_id integer NOT NULL
);

-- Name: user_alert; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE user_alert (
    user_alert_id integer NOT NULL,
    user_id integer NOT NULL,
    alert_id integer NOT NULL,
    type numeric(2,0) NOT NULL
);

-- Name: user_profile_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE user_profile_entry (
    user_id integer NOT NULL,
    user_profile_entry_id integer NOT NULL,
    property_key character varying(255) NOT NULL,
    property_value character varying(512)
);

-- Name: user_pseudo_event; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE user_pseudo_event (
    user_pseudo_event_id integer NOT NULL,
    user_id integer NOT NULL,
    pseudo_event_id integer NOT NULL
);

-- Name: user_role; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE user_role (
    user_role_id integer NOT NULL,
    role_id integer NOT NULL,
    user_id integer NOT NULL
);

-- Name: users; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE users (
    user_id integer NOT NULL,
    user_name character varying(32),
    login_name character varying(255) NOT NULL,
    password character varying(512),
    phone_number character varying(32),
    status character(1) NOT NULL,
    user_type numeric(2,0) DEFAULT 0 NOT NULL,
    email_address1 character varying(255),
    email_address2 character varying(255),
    email_address3 character varying(255),
    email_address4 character varying(255),
    email_alertflag1 character(1),
    email_alertflag2 character(1),
    email_alertflag3 character(1),
    email_alertflag4 character(1),
    last_updated character varying(32),
    previous_passwords_used character varying(2500),
    nbi_identity_key character varying(255) DEFAULT ''::character varying NOT 
NULL,
    nbi_access_key character varying(512)
);

-- Name: vcid_pool; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace: 
CREATE TABLE vcid_pool (
    vcid_pool_db_id integer NOT NULL,
    device_id integer NOT NULL,
    vcid bigint NOT NULL
);

-- Name: vcid_pool_definition_container; Type: TABLE; Schema: dcm; Owner: 
dcmadmin; Tablespace: 
CREATE TABLE vcid_pool_definition_container (
    vcid_pool_definition_container_db_id integer NOT NULL,
    name character varying(255) NOT NULL,
    parent_db_id integer,
    is_current numeric(1) default 0
);

-- Name: vcid_pool_definition_value; Type: TABLE; Schema: dcm; Owner: dcmadmin; 
Tablespace: 
CREATE TABLE vcid_pool_definition_value (
    vcid_pool_definition_value_db_id integer NOT NULL,
    vcid_pool_definition_container_db_id integer NOT NULL,
    range_start bigint NOT NULL,
    range_end bigint NOT NULL
);

-- Name: virtual_circuit_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin; 
Tablespace: 
CREATE TABLE virtual_circuit_interface (
    interface_id integer NOT NULL
);

-- Name: virtual_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace: 
CREATE TABLE virtual_interface (
    interface_id integer NOT NULL
);

-- Name: vlan; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace: 
CREATE TABLE vlan (
    vlan_db_id integer NOT NULL,
    device_id integer NOT NULL,
    name character varying(32),
    table_subtype character varying(32) NOT NULL
```

```
);

-- Name: vlan_dynamic_interface_member; Type: TABLE; Schema: dcm; Owner:
dcmadmin; Tablespace:
CREATE TABLE vlan_dynamic_interface_member (
    vlan_interface_relation_id integer NOT NULL
);

-- Name: vlan_excluded_interface; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vlan_excluded_interface (
    vlan_interface_relation_id integer NOT NULL
);

-- Name: vlan_interface_member; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vlan_interface_member (
    vlan_interface_relation_id integer NOT NULL
);

-- Name: vlan_interface_relation; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vlan_interface_relation (
    vlan_interface_relation_id integer NOT NULL,
    vlan_db_id integer NOT NULL,
    interface_id integer NOT NULL,
    table_subtype character varying(32) NOT NULL,
    stp_port_priority smallint,
    stp_path_cost integer
);

-- Name: vlan_static_interface_member; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vlan_static_interface_member (
    vlan_interface_relation_id integer NOT NULL
);

-- Name: vll_device_relation; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vll_device_relation (
    mpls_service_device_relation_db_id integer NOT NULL,
    vll_mode smallint
);

-- Name: vll_endpoint_relation; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vll_endpoint_relation (
    mpls_service_endpoint_relation_db_id integer NOT NULL,
    pw_enet_pw_instance integer NOT NULL,
    cos smallint
);

-- Name: vpls_device_relation; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vpls_device_relation (
    mpls_service_device_relation_db_id integer NOT NULL,
    vpls_config_index integer NOT NULL,
    mac_limit integer
);
```

```
-- Name: vpls_endpoint_relation; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vpls_endpoint_relation (
    mpls_service_endpoint_relation_db_id integer NOT NULL
);

-- Name: vpnpt_authentication; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE vpnpt_authentication (
    vpnpt_authentication_id integer NOT NULL,
    vpnpt_policy_id integer,
    realm_policy_id integer
);

-- Name: vpnpt_policy; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE vpnpt_policy (
    vpnpt_policy_id integer NOT NULL,
    policy_num numeric(8,0) NOT NULL,
    policy_name character varying(32),
    user_id integer,
    description character varying(256)
);

-- Name: vpnpt_protocol; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE vpnpt_protocol (
    vpnpt_protocol_id integer NOT NULL,
    vpnpt_policy_id integer,
    protocol_type numeric(2,0),
    port_number numeric(5,0),
    protocol_name character varying(32)
);

-- Name: vpnpt_server; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE vpnpt_server (
    vpnpt_server_id integer NOT NULL,
    vpnpt_policy_id integer,
    server_ip_address character varying(40) NOT NULL,
    server_name character varying(40)
);

-- Name: wep; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE wep (
    authentication_encryption_id integer NOT NULL,
    key_length numeric(3,0),
    key_type numeric(2,0),
    key1 character varying(32),
    key2 character varying(32),
    key3 character varying(32),
    key4 character varying(32),
    tx_key_select numeric(2,0)
);

-- Name: wifi_auth; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE wifi_auth (
    slnum integer NOT NULL,
    time_in_seconds integer NOT NULL,
    event_type smallint NOT NULL,
    ip character varying(40) NOT NULL,
    mac character varying(12),
    auth_type character varying(10),
    xinfo character varying(64)
);

-- Name: wired_interface; Type: VIEW; Schema: dcm; Owner: dcmadmin
CREATE VIEW wired_interface AS
    SELECT l2.device_id, l2.device_ip_address, l2.physical_device_id,
l2.unit_number, l2.slot_id, l2.slot_num, l2.module_id, l2.physical_port_id,
l2.port_num, l2.interface_id, l2.name, l2.if_name, l2.identifier,
l2.table_subtype, l2.tag_mode, l2.speed_in_mb, l2.physical_address,
l2.duplex_mode, l3.ip_id, l3.ip_interface_id, l3.ip_address, l3.subnet_mask FROM
((SELECT DISTINCT d.device_id, d.ip_address AS device_ip_address,
pd.physical_device_id, pd.unit_number, s.slot_id, s.slot_num, msp.module_id,
pp.physical_port_id, pp.port_num, i.interface_id, i.name, i.if_name,
i.identifier, i.table_subtype, i.tag_mode, pi.speed_in_mb, pi.physical_address,
pi.duplex_mode FROM device d, physical_device pd, slot s, module_slot_present msp,
physical_port pp, physical_interface pi, interface i WHERE ((((((d.device_id =
pd.device_id) AND (pd.physical_device_id = s.physical_device_id)) AND (s.slot_id
= msp.slot_id)) AND (msp.module_id = pp.module_id)) AND (pp.physical_port_id =
pi.physical_port_id)) AND (pi.interface_id = i.interface_id)) AND
((i.table_subtype)::text <> 'RADIO_INTERFACE'::text))) l2 LEFT JOIN (SELECT
inm_ip_interface.interface_id AS ip_id, inm_ip_interface.ip_interface_id,
inm_ip_interface.ip_address, inm_ip_interface.subnet_mask FROM inm_ip_interface)
l3 ON ((l2.interface_id = l3.ip_id)));

-- Name: wired_mac_filter_entry; Type: TABLE; Schema: dcm; Owner: dcmadmin;
Tablespace:
CREATE TABLE wired_mac_filter_entry (
    mac_filter_entry_id integer NOT NULL,
    dest_mac_address character varying(24) NOT NULL,
    dest_address_mask character varying(24),
    ether_type character varying(24),
    operator character varying(5),
    frame_num character varying(6),
    description character varying(255)
);

-- Name: wireless_interface; Type: VIEW; Schema: dcm; Owner: dcmadmin
CREATE VIEW wireless_interface AS
    SELECT l2.device_id, l2.device_ip_address, l2.physical_device_id,
l2.unit_number, l2.slot_id, l2.slot_num, l2.module_id, l2.physical_port_id,
l2.port_num, l2.interface_id, l2.name, l2.if_name, l2.identifier, l2.speed_in_mb,
l2.physical_address, l2.interface_id AS radioif_id, wireless.radio_type,
wireless.is_enabled, wireless.is_auto_channel, wireless.tx_power,
wireless.channel_number, wireless.max_data_rate, wireless.beacon_rate,
wireless.dtim, wireless.rts_threshold, wireless.is_turbo_mode,
wireless.radio_g_mode, wireless.max_associated_clients FROM ((SELECT DISTINCT
d.device_id, d.ip_address AS device_ip_address, pd.physical_device_id,
pd.unit_number, s.slot_id, s.slot_num, msp.module_id, pp.physical_port_id,
pp.port_num, i.interface_id, i.name, i.if_name, i.identifier, pi.speed_in_mb,
pi.physical_address FROM device d, physical_device pd, slot s,
module_slot_present msp, physical_port pp, physical_interface pi, interface i
WHERE ((((((d.device_id = pd.device_id) AND (pd.physical_device_id =
s.physical_device_id)) AND (s.slot_id = msp.slot_id)) AND (msp.module_id =
pp.module_id)) AND (pp.physical_port_id = pi.physical_port_id)) AND
(pi.interface_id = i.interface_id)) AND ((i.table_subtype)::text =
'RADIO_INTERFACE'::text))) l2 LEFT JOIN (SELECT radio_interface.interface_id AS
radioif_id, radio_interface.radio_type, radio_interface.is_enabled,
radio_interface.is_auto_channel, radio_interface.tx_power,
radio_interface.channel_number, radio_interface.max_data_rate,
radio_interface.beacon_rate, radio_interface.dtim, radio_interface.rts_threshold,
radio_interface.is_turbo_mode, radio_interface.radio_g_mode,
radio_interface.max_associated_clients FROM radio_interface) wireless ON
((l2.interface_id = wireless.radioif_id)));

-- Name: wpa; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE wpa (
    authentication_encryption_id integer NOT NULL,
    cipher_mode numeric(2,0),
    wpa_mode numeric(2,0)
);

-- Name: wpa_psk; Type: TABLE; Schema: dcm; Owner: dcmadmin; Tablespace:
CREATE TABLE wpa_psk (
    authentication_encryption_id integer NOT NULL,
    key_type numeric(2,0),
    key_value character varying(128)
);
```

MANAGED_ELEMENT_INFO

Common managed element data used by custom DTO methods to identify the managed element type, and provide a link to the details table for the managed element. Some common managed element fields are included in this view so Fault Management can use this view to identify the managed element ID for an event source.

```
create or replace view MANAGED_ELEMENT_INFO as
select
    MANAGED_ELEMENT.ID as MANAGED_ELEMENT_ID,
    DEVICE.DEVICE_ID as IP_DEVICE_ID,
    coalesce(CS_ME.ID, CS_VS.ID) as CORE_SWITCH_ID,
    VIRTUAL_SWITCH.ID as VIRTUAL_SWITCH_ID,
    DEVICE_ENCLOSURE.ID as DEVICE_ENCLOSURE_ID,
    DEVICE.IP_ADDRESS as LAN_IP_ADDRESS,
    coalesce (CS_VS.IP_ADDRESS, CS_ME.IP_ADDRESS, DEVICE_ENCLOSURE.IP_ADDRESS) as
SAN_IP_ADDRESS,
    VIRTUAL_SWITCH.VIRTUAL_FABRIC_ID,
    coalesce (VIRTUAL_SWITCH.WWN, CS_ME.WWN, DEVICE.NODE_WWN) as NODE_WWN
from
    MANAGED_ELEMENT
        left outer join VIRTUAL_SWITCH on MANAGED_ELEMENT.ID =
VIRTUAL_SWITCH.MANAGED_ELEMENT_ID
        left outer join CORE_SWITCH CS_ME on (MANAGED_ELEMENT.ID =
CS_ME.MANAGED_ELEMENT_ID)
        left outer join CORE_SWITCH CS_VS on (CS_VS.ID =
VIRTUAL_SWITCH.CORE_SWITCH_ID)
        left outer join DEVICE on MANAGED_ELEMENT.ID = DEVICE.MANAGED_ELEMENT_ID
        left outer join DEVICE_ENCLOSURE on MANAGED_ELEMENT.ID =
DEVICE_ENCLOSURE.MANAGED_ELEMENT_ID;
```

SNMP_DATA_INFO

```
create or replace view SNMP_DATA_INFO as
select * from SNMP_DATA
union all
select * from SNMP_DATA_30MIN
union all
```

```
select * from SNMP_DATA_2HOUR
union all
select * from SNMP_DATA_1DAY;
```

SNMP_EXPR_DATA_INFO

```
create or replace view SNMP_EXPR_DATA_INFO as
select * from SNMP_EXPR_DATA
union all
select * from SNMP_EXPR_DATA_30MIN
union all
select * from SNMP_EXPR_DATA_2HOUR
union all
select * from SNMP_EXPR_DATA_1DAY;
```

SNMP_DATA_VIEW

```
create view SNMP_DATA_VIEW AS
        (        (         SELECT de.device_id, de.ip_address AS device_ip,
se.target_type, de.device_id AS target_id, de.sys_name AS target_name, 1 AS
collectible_type, se.expression_id AS collectible_id, se.collector_id, ( SELECT
perf_collector.name AS collector_name
                                   FROM perf_collector
                                  WHERE perf_collector.collector_id =
se.collector_id) AS collector_name, ( SELECT snmp_expression.name AS
collectible_name
                                   FROM snmp_expression
                                  WHERE snmp_expression.expression_id =
se.expression_id) AS collectible_name, ( SELECT snmp_expression.equation AS
collectible_detail
                                   FROM snmp_expression
                                  WHERE snmp_expression.expression_id =
se.expression_id) AS collectible_detail, se.value, se.time_in_seconds, '' AS
mib_index
                           FROM snmp_expr_data_info se
                      JOIN device de ON se.target_id = de.device_id
                     WHERE se.target_type = 0
                UNION ALL
                         SELECT de.device_id, de.ip_address AS device_ip,
sd.target_type, de.device_id AS target_id, de.sys_name AS target_name, 0 AS
collectible_type, sd.mib_object_id AS collectible_id, sd.collector_id, ( SELECT
perf_collector.name AS collector_name
                                   FROM perf_collector
                                  WHERE perf_collector.collector_id =
sd.collector_id) AS collector_name, ( SELECT (mib_object.name::text || '.'::text)
|| sd.mib_index::text AS collectible_name
                                   FROM mib_object
                               WHERE mib_object.mib_object_id = sd.mib_object_id)
AS collectible_name, ( SELECT mib_object.oid AS collectible_detail
                                   FROM mib_object
                               WHERE mib_object.mib_object_id = sd.mib_object_id)
AS collectible_detail, sd.value, sd.time_in_seconds, sd.mib_index
                           FROM snmp_data_info sd
                      JOIN device de ON sd.target_id = de.device_id
                     WHERE sd.target_type = 0::numeric)
        UNION ALL
```

```
                SELECT de.device_id, de.ip_address AS device_ip, sd.target_type,
ifs.interface_id AS target_id, ifs.if_name AS target_name, 0 AS collectible_type,
sd.mib_object_id AS collectible_id, sd.collector_id, ( SELECT perf_collector.name
AS collector_name
                           FROM perf_collector
                         WHERE perf_collector.collector_id = sd.collector_id) AS
collector_name, ( SELECT (mib_object.name::text || '.'::text) ||
sd.mib_index::text AS collectible_name
                           FROM mib_object
                          WHERE mib_object.mib_object_id = sd.mib_object_id) AS
collectible_name, ( SELECT mib_object.oid AS collectible_detail
                           FROM mib_object
                          WHERE mib_object.mib_object_id = sd.mib_object_id) AS
collectible_detail, sd.value, sd.time_in_seconds, sd.mib_index
                   FROM snmp_data_info sd
             JOIN interface ifs ON sd.target_type = 1::numeric AND sd.target_id =
ifs.interface_id
         JOIN device de ON ifs.device_id = de.device_id)
UNION ALL
         SELECT de.device_id, de.ip_address AS device_ip, se.target_type,
ifs.interface_id AS target_id, ifs.if_name AS target_name, 1 AS collectible_type,
se.expression_id AS collectible_id, se.collector_id, ( SELECT perf_collector.name
AS collector_name

                   FROM perf_collector
                  WHERE perf_collector.collector_id = se.collector_id) AS
collector_name, ( SELECT snmp_expression.name AS collectible_name
                   FROM snmp_expression
                  WHERE snmp_expression.expression_id = se.expression_id) AS
collectible_name, ( SELECT snmp_expression.equation AS collectible_detail
                   FROM snmp_expression
                  WHERE snmp_expression.expression_id = se.expression_id) AS
collectible_detail, se.value, se.time_in_seconds, '' AS mib_index
           FROM snmp_expr_data_info se
      JOIN interface ifs ON se.target_type = 1 AND se.target_id = ifs.interface_id
   JOIN device de ON ifs.device_id = de.device_id;
```

Index

Printed in USA

GA32-0940-00