



SANscreen User Manual

Version 2.9.45



Onaro Inc. • 46 Waltham Street • Boston, MA 02118

Phone 617.338.0068 • Fax 617.338.1444

COPYRIGHT © 2000-2005 by Onaro, Inc.

— All rights reserved. —

This manual and the information contained herein are confidential and proprietary to Onaro Inc. Only Onaro or its Licensees have the right to use the information. Any unauthorized use, disclosure or reproduction is a violation of the licenses and/or Onaro's proprietary rights and will be prosecuted to the full extent of the Law.

Company, brand, product, and service names are trademarks or registered trademarks of their respective holders.

SANscreen has been checked in accordance with Onaro, Inc. quality standards and has been found to comply with Onaro's published specifications.

DISCLAIMER

The information contained in this publication is subject to change without notice. ONARO, Inc. makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Onaro Inc. shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

LICENSES and COPYRIGHTS

Onaro® and SANscreen® are registered trademarks of ONARO, Inc. in the United States and other countries.

Other product names and/or slogans mentioned herein may be trademarks or registered trademarks of their respective companies.

Additional copyright information for third-party code provided with the product is set forth in the documentation.

Table of Contents

Preface	ix
Customer Service	ix
Quick Start Instructions	x
Icons	xi
Device and Menu Icons	xi
Table Management.....	xii
Detail Tab Icons.....	xii
Tool Icons (Topology View)	xiii
Other Icons	xiii
Acronyms.....	xiv
Navigation Tips.....	xv
Chapter 1 Introduction to SANscreen.....	1
Chapter 2 Working with the SANscreen Client.....	3
2.1 Accessing the SANscreen Client.....	4
2.1.1 Using the Start Menu	4
2.1.2 Using a Web Browser	5
2.2 Navigation Tree	6
2.3 The Main Table.....	8
2.4 The Topology Pane	9
2.4.1 Layers Control.....	10
2.4.2 Views Control	11
2.5 The Detail Panes	12
2.5.1 Properties Detail Pane	12
2.5.2 Paths Detail Pane	13
2.5.3 Ports Detail Pane	14
2.5.4 Zone Members Detail Pane	15
2.5.5 Volumes Detail Pane	16
2.5.6 Violations Detail Pane	17
2.5.7 Masking Detail Pane	18
2.5.8 Changes Detail Pane	20
2.6 SANscreen's Main Menu	21
2.6.1 File Menu	21
2.6.2 Edit Menu	21
2.6.3 View Menu	22

2.6.4 Action Menu	22
2.6.5 Help Menu.....	23
Chapter 3 Establishing Topology Layouts.....	25
3.1 The Topology Toolbar	26
3.2 The Topology Menu	27
3.3 Using Layouts.....	28
3.3.1 Exporting the Topology Layout	29
3.4 Working With Views	30
3.4.1 Create a View	30
3.4.2 Rename a View.....	31
3.4.3 Remove a View.....	31
3.5 Working With Groups	31
3.5.1 Focus on a Group	32
3.5.2 Create a Group (or Subgroup).....	33
3.5.3 Delete a Group.....	33
3.5.4 Rename a Group	34
3.6 Tools that Help View the SAN Topology	34
3.6.1 Zoom Tools	34
3.6.2 Expand/Collapse Mode.....	34
3.6.3 Determining Valid Actions.....	35
3.6.4 Changing Link Style	35
3.6.5 Hovering Over an Icon to Display Detail.....	36
3.7 Manually Identifying a Generic Device	37
3.8 Other Device-Related Activities.....	37
3.9 Managing a Device via Telnet or HTTP	39
Chapter 4 Viewing and Authorizing Logical Paths.....	41
4.1 Reviewing the Path List Main Table	41
4.2 Looking in Detail at an Access Path.....	43
4.3 Authorizing a Logical Path.....	45
Chapter 5 Viewing Authorized Paths	49
5.1 Reviewing the Authorized Path List Main Table.....	49
5.2 Looking in Detail at an Authorized Path	52
5.3 Analyzing the Violation For an Authorized Path.....	53
5.4 Authorization Activities	54
5.4.1 Authorizing a New Logical Path.....	54
5.4.2 Editing an Authorized Path	56
5.4.3 Deleting a Path's Authorization.....	56
Chapter 6 Identifying and Investigating Violations	59
6.1 Identifying Violations	59
6.2 Types of Violations	62

6.3 Root Cause Analysis of Violations	65
6.3.1 The Topology View	65
6.3.2 Detail Pane Data	65
6.3.4 Analyzing Violations	66
6.3.5 Displaying Tasks for Planned Violations	70
6.4 Correcting a Violation	71
Chapter 7 Defining and Validating Clusters	73
7.1 Defining Clusters	73
7.2 Validating Clusters	75
Chapter 8 Reviewing Changes	77
8.1 Working with the Change List	78
8.2 Using the Topology Pane to View History	80
8.2.1 Generating an HTML Report of Changes	81
Chapter 9 Assessing Vulnerabilities	83
9.1 Viewing Vulnerability Data	83
9.1.1 Establishing Vulnerability Thresholds	84
9.2 Vulnerability Types	85
9.2.1 Blocked Hosts	85
9.2.2 Disconnected Port Zone Members	86
9.2.3 Disconnected WWN Zone Members	86
9.2.4 High Fabric Port Usage	87
9.2.5 High Masking Fan-Out Ratio	87
9.2.6 High Volume Allocation	88
9.2.7 Incomplete Cluster Volume Sharing	88
9.2.8 Low Fabric Port Usage	89
9.2.9 Shared Volume Masking	89
9.2.10 Unused Masked Volumes	91
Chapter 10 Creating, Validating and Tracking Tasks	93
10.1 Plans Screen Overview	94
10.1.1 The Plans Action Menu	95
10.2 Creating a Change Plan	97
10.2.1 Adding a Task to the Task List	98
10.2.2 Defining Actions Using the Action Wizard	100
10.2.3 Importing and Updating Tasks From Excel	101
General Rules	101
Spreadsheet Format for Task Import	102
Steps to Follow to Import Tasks from a Spreadsheet	106
Steps to Follow for Task Update or Delete Via Spreadsheet Import	107
10.2.4 Defining Templates	108
Creating a New Template	109

Editing or Deleting a Template	109
Generating Tasks From a Template	110
10.2.5 Generating Tasks and Actions Using Templates	110
Generating Storage-To-Host Tasks	110
Generating Host-Decommission-Tasks	111
10.2.6 Exporting and Importing Tasks	112
10.3 Pre-Validating a Task	113
10.3.1 Reviewing Task Validating Results.....	113
10.3.2 Generate a Task Pre-Validation Report.....	115
10.4 Tracking Task Execution	116
10.5 Action Types.....	117
10.5.1 Add Controller to Storage	120
10.5.2 Add Controller to Tape.....	121
10.5.3 Add HBA to Host.....	122
10.5.4 Add Host	123
10.5.5 Add Hosts to Cluster	124
10.5.6 Add Ports to VSAN	125
10.5.7 Add Storage	126
10.5.8 Add Switch.....	127
10.5.9 Add Tape	129
10.5.10 Add Volume	130
10.5.11 Add Volume Map	131
10.5.12 Add Volume Mask.....	132
10.5.13 Add VSAN.....	134
10.5.14 Add Zone	135
10.5.15 Add Zone Member (by Switch Port).....	136
10.5.16 Add Zone Member (by WWN)	137
10.5.17 Authorize Path	138
10.5.18 Connect Port	139
10.5.19 Connect Ports	140
10.5.20 Disconnect Ports.....	141
10.5.21 Edit Authorized Path	142
10.5.22 Enable Zone Configuration	143
10.5.23 Remove Authorized Path.....	144
10.5.24 Remove Controller from a Storage	145
10.5.25 Remove Controller from a Tape	146
10.5.26 Remove HBA from a Host	147
10.5.27 Remove Ports from VSAN	148
10.5.28 Remove Volume	149
10.5.29 Remove Volume Map	150
10.5.30 Remove Volume Mask.....	151
10.5.31 Remove VSAN.....	153
10.5.32 Remove Zone	154

10.5.33 Remove Zone Member	155
10.5.34 Shutdown Host	156
10.5.35 Shutdown Storage	157
10.5.36 Shutdown Switch	158
10.5.37 Shutdown Tape	159
Chapter 11 Identifying Generic Devices	161
11.1 Identifying HBA Devices via Host Resolution	162
11.1.1 Configuring Host Resolution	163
Preferences Tab	163
Methods Tab	164
Storage Vendors Tab	164
Finishing Up	165
11.1.2 Configuring Regular Expressions	165
Finishing Up	167
11.2 Identifying Devices Manually	167
11.2.1 Identifying Devices Using the Identify Screen	167
11.2.2 Identifying Generic Devices From the Topology Pane	171
11.2.3 Identifying Generic Devices From the Generic Device List	171
Chapter 12 Viewing Inventory Data	173
12.1 Switches	173
12.1.1 Switch Properties Detail Tab	175
12.2 Hosts & Clusters	176
12.2.1 Host Properties Detail Tab	178
12.2.2 Adding Hosts to a Cluster and Related Processing	179
12.2.3 Viewing History	179
12.3 Storage Devices	180
12.4 Tapes	181
12.5 Generic Devices	182
12.5.1 Generic Device Properties Detail Tab	183
12.5.2 Identifying a Generic Device	183
12.6 Zones	184
12.6.1 Zone Members Detail Tab	185
12.7 Topology View	186
Chapter 13 Reports	187
13.1 Accessing the Reporting Capabilities	187
13.2 Custom Reports	189
13.3 Symmetrix Discovery Report	192
13.4 Trend Report	193
13.5 Changes Report	194
13.6 Task Report	196

Chapter 14 Auditing User Activities.....	197
Appendix A Copyright Notices	199
Appendix B Host Resolution Algorithms	201
B.1 Delimiter Technique Algorithm.....	201
B.2 Regular Expression Technique Algorithm	203

Figures

Figure 1: SANscreen Client Display Explained.....	3
Figure 2: Sample Topology Pane	9
Figure 3: Sample Path List.....	42
Figure 4: Selecting a Logical Path in the Path List, and the Topology Pane.....	44
Figure 5: Sample Authorized Path List	50
Figure 6: Selecting an Authorized Path and Viewing Changes	52
Figure 7: Sample Violation Display.....	60
Figure 8: Sample Change List	77
Figure 9: Change list with Violation	80
Figure 10: Sample Vulnerabilities Display	83
Figure 11: Sample Plans Screen	94

Tables

Table 1: Policy Options to Authorize a Path	46
Table 2: Action Types (Plans Processing).....	117

Preface

The *SANscreen User Manual* describes SANscreen functionality and usage, providing you with a thorough understanding of the features and procedures required to analyze and validate your storage network environment — and to notify you of problems, discover their root cause, and resolve them.

SANscreen assures successful SAN change and growth processes across complex storage environments. By following this manual, you will learn how to validate the change process, to discover and investigate problems, and to ensure continuous availability of your storage network while complying with existing requirements and policies.

Customer Service

For questions, comments, or suggestions, contact Onaro at:

support@onaro.com

or

617.338.0068

Onaro is proud of being not just a leading-edge technological innovator in the important area of SAN availability assurance, but also a customer-focused and service-oriented company.

We will be happy to hear from you!

Quick Start Instructions

Please follow the steps below to get SANscreen up and running as quickly as possible:

Task	For details see...
1. Install the SANscreen software.	The SANscreen <i>Installation and Administration</i> manual.
2. Access the SANscreen Portal and configure SANscreen.	The SANscreen <i>Installation and Administration</i> manual.
3. Access the SANscreen client.	Chapter 2 Working with the SANscreen Client
4. Discover and visualize the storage network by configuring the Data Sources for your SAN devices.	The SANscreen <i>Installation and Administration</i> manual.
5. Identify generic devices automatically.	Chapter 11 Identifying Generic Devices
6. Define host clusters.	Chapter 7 Defining and Validating Clusters
7. Visually lay out the SAN topology.	Chapter 3 Establishing Topology Layouts
8. Review the paths that SANscreen discovered.	Chapter 4 Viewing and Authorizing Logical Paths
9. Apply service-level policies to the paths in your SAN.	Chapter 5 Viewing Authorized Paths
10. Identify, investigate, and correct violations.	Chapter 6 Identifying and Investigating Violations
11. Review and correct vulnerabilities.	Chapter 9 Assessing Vulnerabilities
12. Review changes.	Chapter 8 Reviewing Changes
13. Plan and re-validate future tasks before implementation.	Chapter 10 Creating, Validating and Tracking Tasks
14. Obtain on-demand operational reports that detail your SAN information, including trend analysis and a change history.	Chapter 13 Reports
15. Audit user activities, as needed.	Chapter 14 Auditing User Activities

Icons

Device and Menu Icons

Icon	Represents...
	Violation(s). Displays green if a violation has been resolved.
	Authorized path(s).
	Path(s).
	Changes (history).
	Vulnerability(ies).
	Plans (future SAN changes).
	Switch(es).
	Host or cluster(s).
	Storage device(s).
	Tape device(s).
	Generic device(s). Shown as the lower form when used to <i>identify</i> generic devices.
	Zone(s).
	Topology.
	Acquisition unit(s). Acquisition units are discussed in the SANscreen <i>Installation and Administration</i> manual.
	Data sources(s). Data Sources are discussed in the SANscreen <i>Installation and Administration</i> manual.
	Fabric (s). Used to report fabric status in the change history.
	Link(s). Used to report link status in the change history.
	Adapter (i.e., fibre-channel network) card(s).

Table Management

Icon	Click to...
	Change (regroup) how records are presented.
	Reverse the order of fields in a column.
	Compress (collapse) data in a table.
	Expand data in a table.
	Clear all column filters.
	Select the time period for which to display information (today, this week, etc.).
	Filter the displayed information according to any of several options available in the drop-down menu.
	Open the list in a Web browser.

Detail Tab Icons

Icon	Toggles Display of the...
	Layer Control panel.
	View Control panel.
	Properties detail pane.
	Paths detail pane.
	Ports detail pane.
	Zone Members detail pane.
	Volumes detail pane.
	Violations detail pane.
	Masking detail pane.
	Change List detail pane.
	Errors detail pane (available from Plans processing).

Tool Icons (Topology View)

Tool	Used to...
	Toggle Layers — Display or hide the Layer Control panel.
	Toggle Views — Display or hide the View Control panel.
	Pan — Drag the topology display around on our screen.
	Select — Select individual devices in the topology display.
	Zoom To Fit — Fit all topology inside the area displayed.
	Zoom In — Zoom in to focus on a specific environment.
	Zoom Out — Zoom out to show more of the topology.
	Zoom Box — Enlarge and center the area where you drag the tool.
	Expand/Collapse Selection — Show/hide detail for the selected item (the group layout if you select a group (site), or individual ports if you select a host, switch, or storage device).
	Focus on Selected Group — Bring the currently selected group or site to the center of the topology display.
	Create a New Group — Open a dialog that lets you create a new group (typically a site).
	Delete Group — Delete the currently selected group.
	Rename Group — Rename the currently selected group.

Other Icons

Icon	Description
	Informational message (unknown).
	Work in progress.
	Warning (status).

Acronyms

Acronym	Description
AP	Authorized Path.
APL	Authorized Path List.
CSV	Comma Separated Values — A file format that can be saved from a spreadsheet application, and that's used by SANscreen to identify generic devices.
GB	Gigabytes.
GBIC	GigaBit Interface Converter.
GUI	Graphical User Interface.
HBA	Host Bus Adapter.
HTML	HyperText Markup Language.
HTTP	HyperText Transfer Protocol.
ISL	Inter-Switch Link
JRE	Java Run Time environment.
LUN	Logical Unit Number — used by a host to access a particular volume.
SPF	Single Point of Failure.
VSAN	Virtual Storage Area Network — A fibre channel network whose definition is similar to that of a VLAN.
WWN	World Wide Name.
XML	Extensible Markup Language — a file format that's used to export/import task actions.

Navigation Tips

Red, Red, Red

Color is important:

- When a path, text string, or field is highlighted in **red**, SANscreen has detected a problem in your SAN. A quick glance at the data presentation allows you to locate those items that need attention. Just look for the **red** highlights!
- A path displays **green** when it's operating normally.
- A path displays **purple** (magenta) when the cursor hovers over a link between devices to provide detailed pop-up information.

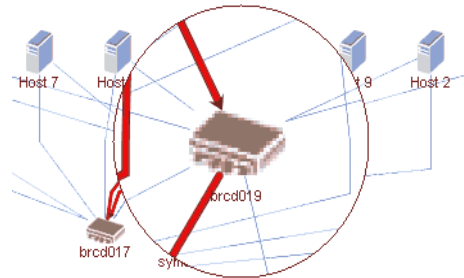
Refreshing the Screen

Use the <F5> key to refresh the SANscreen display with current data. You can set SANscreen to refresh automatically upon any change, using the Auto Refresh option from the View menu.

Magnifying Glass View

When working in the topology pane, you can create a magnifying-glass as follows:

- Hold down the middle mouse button if you have one, or press <Alt> *and*
- Left-click the mouse.

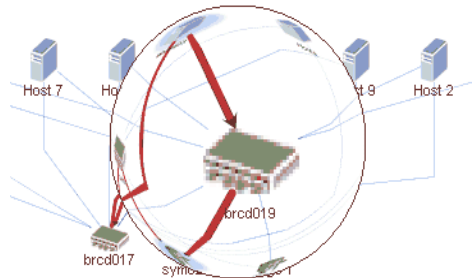


Drag the magnifying-glass over those areas you want to view in greater detail.

Fish-Bowl View

When working in the topology pane, you can generate a fish-bowl view as follows:

- Press <Alt - Shift> *and*
- Left-click the mouse.



Drag the circle over those areas you want to view in greater detail.

Required Fields

When using a form or wizard to enter data, all required fields are marked with an asterisk (*).

Numbers in Parentheses

In the headings of tables — and sometimes in a column heading or row data — you will sometimes see a number in parentheses, like this:  **Ports** (3).

These numbers indicate the quantity of the type of data they represent. For example, the number 3 in the heading shown above means that there are 3 ports listed in the table.

Adjusting Column Order

You can drag and drop columns in the SANscreen tables, to best view the data you’re infested in.

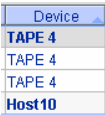
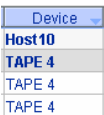
Adjusting Column Width

When you click the bars between columns in the heading row of any table, the cursor changes to a double-headed arrow. Drag the column width to the left or right to better view the data that’s most relevant to you. An ellipsis (...) in a field means the field size is smaller than its current content.

Double-clicking a double-headed arrow sets the column width to match the width of its widest cell.

Column Sorting (Ascending/Descending)

You can reverse the sort order of a column by clicking the column heading. With the column selected, an icon to the far right indicates whether the column is sorted in ascending or descending order:

		
columns is sorted...	ascending	descending

Right-click any column heading to return to the default column order.

You can sort by multiple columns, by selecting and sorting the columns in the desired order. If you sort first by one column, and then another, the table will sort first by the first column selected, and then the second, etc.

Filtering Table Data

You can filtering table data by clicking the filter symbol to the far left in the column's header (visible with the column selected):  Device.

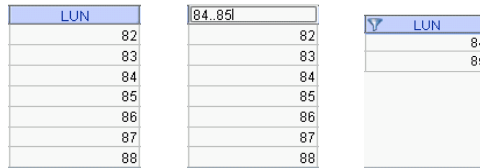
After you click this symbol, SANscreen clears the column header. Enter the filtering criteria you wish, then either hit <Enter> or click out of the column, to redisplay the table with only those entries that match the filtering criteria (i.e., that contain the text or numbers entered).



Entering then Displaying Filtering Criteria

To specify a range of numbers, enter *n..n*, for example: 50..100, entered in the volume capacity column, will display only volumes with a capacity between 50 and 100 GB.

In the example below, we first see an unfiltered list of LUNs (far left), then we enter filtering criteria for the list, then we see the filtered list (far right):



Specifying a Range of Values in the Filtering Criteria

Selecting and Deselecting in Tables

With the cursor positioned on any row of a table, click the left mouse button to select that row. This highlights the row, and displays information about the row in both the topology and detail panes, as appropriate to the processing. To select multiple rows:

- Click the left mouse button and drag down the table to select a range of consecutive rows, or hold down the <Shift> key and click the first and last rows in the range you want.
- Hold down the <Shift> key and click the first and last rows in the range you want.
- Hold down the <Ctrl> key to select/deselect multiple individual rows.

- Use <Ctrl-A> to select all rows.

To de-select a row, hold down the <Ctrl> key and left-click on the row to be de-selected.

Expanding and Collapsing Data in Tables

If the Expand  icon displays above a table, click it to view the maximum amount of detailed data available in the table.

Similarly, click the Collapse  icon to roll detailed data into one or more parent entries.

In some tables, individual rows can be expanded/compressed. These are marked with a plus sign  (click to expand) or a minus sign  (click to compress child members).

Right-Click Menus

Most SANscreen panes support right-click menus, which offer a selection of options appropriate for the current view, or the currently selected item. These options are also available from the Action menu.

Options that are not currently enabled are grayed in the menus.

Chapter 1

Introduction to SANscreen

SANscreen is a foundation solution in Onaro's suite of predictive SAN change solutions. SANscreen analyzes and validates SAN change processes, by continually tracking the impact of SAN changes and events.

As SANs continue to grow, SAN managers face increasing pressure to perform changes in complex environments, within strict time and resource constraints, to:

- Prevent SAN-related problems from happening.
- Detect and correct SAN-related problems rapidly.

SANscreen is designed to assist SAN managers in achieving these goals. Its patent-pending technology is based on the fundamental notion of SAN *logical access paths*. Each logical access path represents a relationship between a particular application on a given server, and its data on a storage device. Such a logical access path consists of a sequence of physically connected components, each of which is configured to allow data flow along that path (assuming proper zoning and masking).

Each logical access path has various properties that represent that path's availability, performance, and security. SANscreen ensures that all *authorized* access paths — and *only* authorized access paths — exist in the SAN and have the correct properties. This is critical, because any single SAN event, such as a local change, or a failure, can affect the existence and/or attributes of one or more logical access paths.

SANscreen supports all phases of the SAN change process. Specifically, SANscreen:

- Provides planning, simulation, and pre-validation of SAN changes.
- Enforces consistent, specific, action sequences for the execution of SAN changes.
- Performs extensive automatic post-validation.

For every SAN event, SANscreen:

- Ensures correctness, and notifies you of violations and vulnerabilities.
- Provides root-cause analysis of each violation.
- Keeps track of the event(s) in a time-based history repository, thereby facilitating the generation of summary information, and display of the SAN at any point in time.

When a violation occurs (often due to human error or a hardware failure), SANscreen detects it immediately, identifies the implications on its access path, and analyzes the impact and the root cause of the problem in a manner that enables rapid and effective corrective actions.

SANscreen is a completely non-intrusive solution. It inter-operates with virtually all SAN devices, does not require any host agents, does not affect the SAN data paths, and never changes the state anywhere in the SAN. SANscreen complements other storage management tools (such as SRM), and can interoperate with any enterprise solution, including event-management and change solutions.

By providing the above capabilities, SANscreen offers unique and significant value to enterprises, including:

- Reduced time, cost, and problems when implementing SAN changes. SANscreen lets you support larger SANs without a corresponding increase in the SAN management team.
- Reduced SAN problems with rapid detection and correction. SANscreen lowers the probability of outages and business disruptions.
- Increased overall SAN confidence, leading to controlled SAN growth and consolidation.

Chapter 2

Working with the SANscreen Client

The SANscreen client application provides a graphical user interface (GUI) to SANscreen's predictive change management solution. The client window is divided into five areas, illustrated in Figure 1:

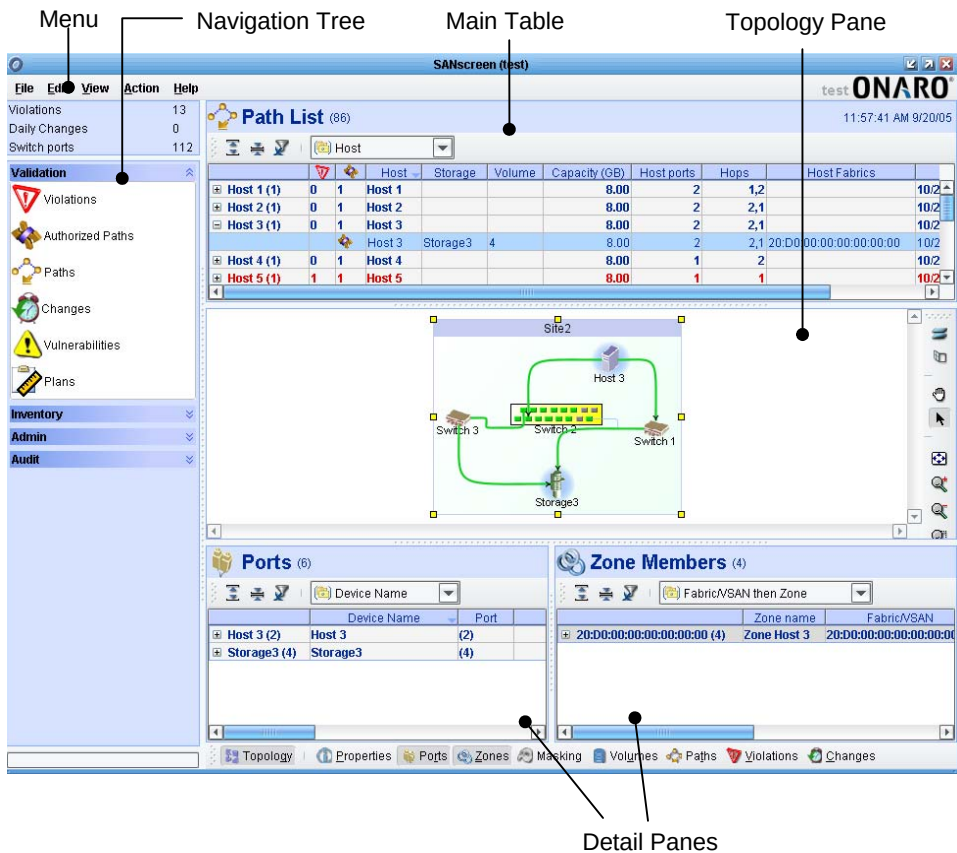


Figure 1: SANscreen Client Display Explained

This chapter first tells how to launch the SANscreen client, then describes each of these five panes and their uses, in order as follows:

- **Navigation Tree** (described starting on page 6), which provides icons used to switch between the various SANscreen views.
- **Main Table** (page 8), which displays detailed information corresponding to the current view (violations, authorized paths, etc.).
- **Topology Pane** (page 9), which provides a graphical representation of the SAN layout and data.
- **Detail Panes** (page 12), which provide detailed information about a selected row in the main table, or a selected device in the topology pane.
- **Menus** (page 21), from which you'll choose various actions and activities that are appropriate for the current view.

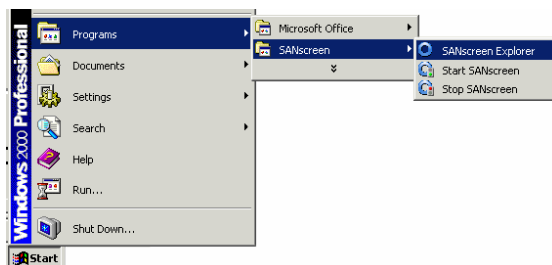
Note: SANscreen does not provide default or demo data. The examples in this chapter are based on a pre-configured SANscreen installation. Check with your SANscreen administrator to ensure that your enterprise's Data Sources were added correctly, and that your SAN data has been discovered by SANscreen already. Instructions to define Data Sources, and to import host data, are included in the SANscreen *Installation and Administration* manual.

2.1 Accessing the SANscreen Client

You can run the SANscreen client from the Start menu or from a Web browser, as detailed in the sections that follow.

2.1.1 Using the Start Menu

When launching the client from the same host where the SANscreen server is installed, use the Start menu as follows:



This opens a login window, illustrated to the right. Enter your user name and password, then click OK. If your user name is authorized through an LDAP server, your login name must include an @ sign followed by the domain (e.g., bob@US.onaro.com).



Note: The default (as-installed) user name is **admin**, and the password is **onaro**. It's a good idea to change these defaults as soon as possible after installation.

After a successful login, the main client screen opens.

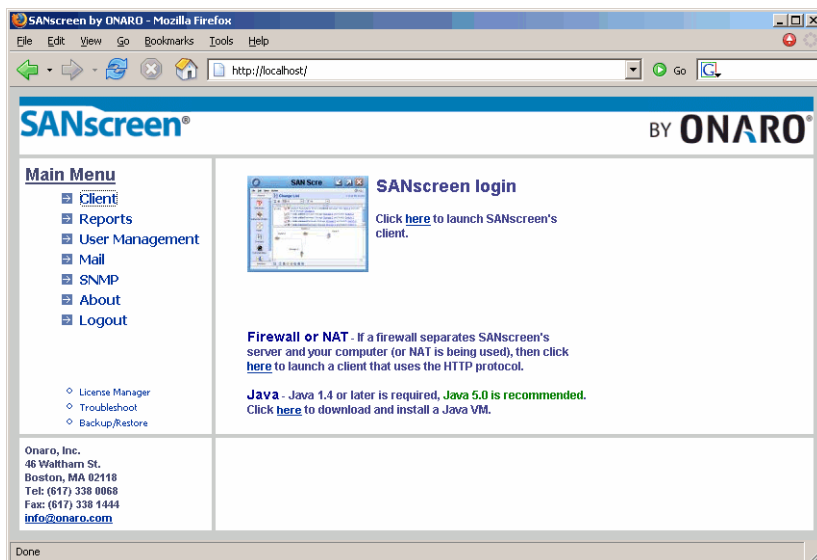
2.1.2 Using a Web Browser

From any Web browser, enter the following URL to access the administration portal on the SANscreen server. The port number will be either 80 or 8080, as configured at when the server was installed:

`http://<SANscreen_hostname>:<SANscreen_port>`

Note: If you're accessing the client from the SANscreen server, enter:
`http://localhost`

After connecting with the SANscreen portal, the server opens a window through which you can access various SANscreen Web services. Click the Client link at the top of the Main Menu (left) to access the client login. This is illustrated below:



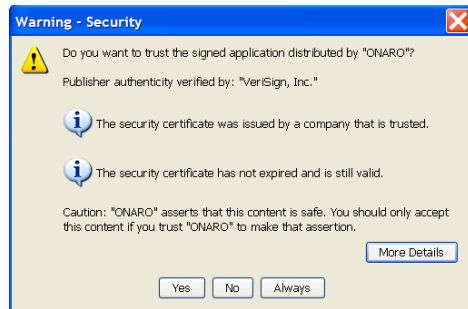
Request the login window by clicking [here](#) to launch SANscreen's client.

Note1: If the Java Run Time environment (JRE) is not installed on your PC, SANscreen displays a message indicating that you have to install it. The Java link will direct you to a Windows JRE installation. If you're running a different operating system, please refer to the Java download site at: <http://java.sun.com>.

Note2: If you are running an earlier version of the JRE, Onaro recommends that you upgrade to Java 5.0. SANscreen's client portal offers a link for the Windows JRE version.

Note3: If a firewall separates the client PC from the SANscreen server, you cannot use the regular method of communicating. Click **here** under the **Firewall or NAT** notice in this case, to initiate communication via HTTP.

Java opens a security window, illustrated to the right for Internet Explorer. Click Start (or OK, if using another browser), then proceed from the login window as described starting on page 5 (to enter your user name and password, etc.).



2.2 Navigation Tree

The pane on the far left side of the SANscreen window provides a navigation tree that let you switch between the various SANscreen views. Click any icon to display the corresponding SANscreen main table, topology pane, and/or detail tabs.

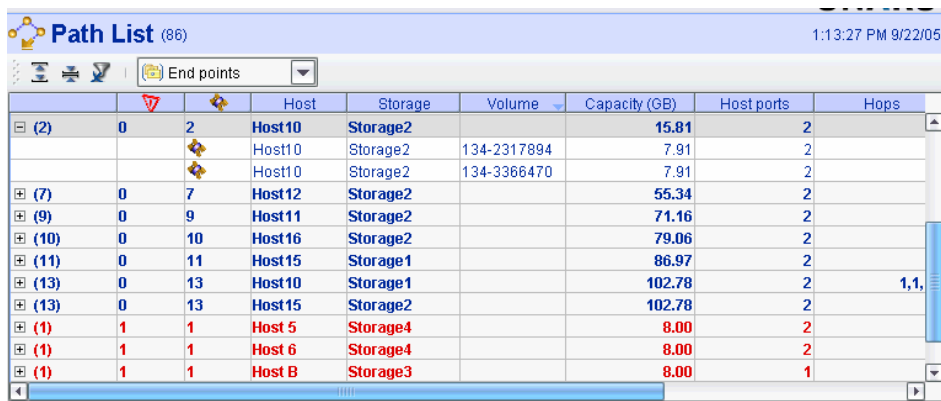
Note: Both panes contain the same icons. You can hide one of them using the **View** menu.

The icons are grouped into three categories:

Category	Icons	Description
Validation	 Violations  Authorized Paths  Paths  Changes  Vulnerabilities  Plans	Display information used to analyze your access paths and violations.
Inventory	 Switches  Hosts & Clusters  Storage Devices  Tapes  Generic Devices  Zones  Topology View	Display detailed information for all devices of a particular type, or for all defined zones; or display a high-level view of the SAN topology (last icon).
Admin	 Acquisition Units  Data Sources  Identify	Display information for each Data Source and Acquisition Unit, as described in the <i>SANscreen Installation and Administration</i> manual. Also used to identify devices that SANscreen detects but cannot identify.
Audit	 Audit	Audit the actions taken by each user.

2.3 The Main Table

The main table, which displays to the right of the navigation icons at the top of the window, displays detailed information that corresponds to the selected view. Every main table is specific to a particular view, as reflected by the title of the table (Path List, Task List, and so forth):



	Violation	End points	Host	Storage	Volume	Capacity (GB)	Host ports	Hops
(2)	0	2	Host10	Storage2		15.81	2	
			Host10	Storage2	134-2317894	7.91	2	
			Host10	Storage2	134-3366470	7.91	2	
(7)	0	7	Host12	Storage2		55.34	2	
(9)	0	9	Host11	Storage2		71.16	2	
(10)	0	10	Host16	Storage2		79.06	2	
(11)	0	11	Host15	Storage1		86.97	2	
(13)	0	13	Host10	Storage1		102.78	2	1,1
(13)	0	13	Host15	Storage2		102.78	2	
(1)	1	1	Host 5	Storage4		8.00	2	
(1)	1	1	Host 6	Storage4		8.00	2	
(1)	1	1	Host B	Storage3		8.00	1	

The color of each row reflects the current state of the item represented by that row. For example, a red row in the Path List main table indicates a path that is in violation of its currently defined policy. The Violation icon (red V) in the heading) has a number of 1 or greater if the row is red.

Time Stamp

The time stamp, at the top-right corner of the main table, indicates the exact time for which information is displayed. This is important, because SANscreen stores all past changes and events, and can provide an accurate change-level image of the SAN as of any point in time.

Note: SANscreen automatically refreshes the window and updates the time stamp when a change is acquired by the SANscreen server, if the View menu's Auto Refresh option is checked.

Refer to *Navigation Tips* (page xv) for instructions to arrange the column order, adjust column widths, and work with table data in general.

2.4 The Topology Pane

The topology pane appears below the main table, as appropriate to the current view. This pane uses icons and graphical elements to visualize the SAN data and analysis. Every SAN device is represented by an icon that represents the device type, while physical connections appear as lines connecting the icons.

Figure 2 shows a standard visualization of a small network as it appears in the topology pane:

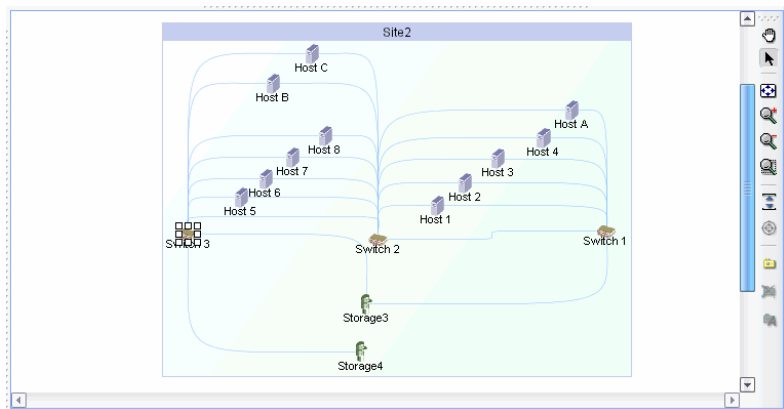
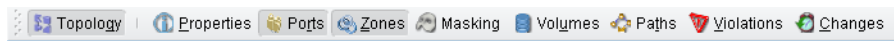


Figure 2: Sample Topology Pane

With the topology pane displayed, several detail tabs run across the bottom of the window:

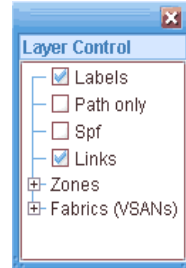


- Click the Topology tab to toggle display of the topology pane.
- Use the other tabs to display details about the component that's currently selected in the topology pane. Click on any icon, then click the detail tab for the information you want to see (component properties, paths, ports, etc.). Refer to page 12 for a discussion of these detail tabs.

Refer to *Navigation Tips* (page xv) for information about arranging and working with the topology pane. Also refer to *Chapter 3 Establishing Topology Layouts*, beginning on page 25.

2.4.1 Layers Control

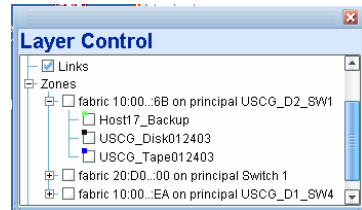
Choose View – Layers from the main menu (or click the Toggle Layers  icon in the toolbar) to toggle display of the Layer Control panel, which lets you show/hide various layers in the topology pane. This is particularly useful with large networks, where the image may become overcrowded if you include all the labels, paths, zones, and so forth. Use the Layer Control panel to control the display in this case, allowing you focus on the information that's most important at the time.



Each Layer Control setting can be turned on/off individually. Mark a checkbox to view the corresponding layer; un-mark the box to hide that layer:

- **Labels** — Toggles the display of device names beneath topology icons. This is useful to reduce clutter when viewing large networks. With Labels turned off, you can still view the name of a device by hovering over the device icon with the cursor, and viewing its pop-up information.
- **Path only** — Toggles a feature that displays only those devices that participate in the currently selected path (applicable only when the main table shows Paths, Authorized Paths, or Violations). When this feature is off (not marked), the topology view includes all devices.
- **SPF** — Toggles display of the icon used to mark a single point of failure (SPF) on the current path. Applicable when a path is selected in the main table. With SPF turned on, the symbol  appears next to any device that is the single point of failure on the selected path.
- **Links** — Toggles display of the links that connect devices in the network.
- **Zones** — Displays a list of fabrics defined in the SAN, and, for each fabric, the zones defined within that fabric. Click the  indicator to the left of the word Zone to display the fabrics, and the  indicator to the left of each fabric to display its zones.

To identify the devices in each zone in the topology display, mark the check box next to the zone whose devices you want to see (right). The color block at the upper left corner of the check box is the color that will surround each device in that zone. If you mark the fabric check box, SANscreen highlights all zones in the fabric in the topology display, each using a distinct color.



- **Fabrics** — Displays a list of fabrics defined in the SAN. Click the  indicator to the left of the word Fabrics to display this list.

With the list open, mark the check box next to any fabric to highlight the switches that are members of that fabric in the topology pane. The color block at the upper left corner of the check box is the color that will surround each switch in the selected fabric.

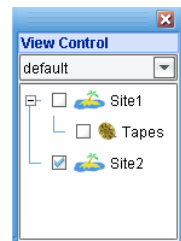
Note: VSAN-based fabrics cannot be highlighted.

2.4.2 Views Control

SANscreen lets you organize your topology icons into groups and subgroups. Each such group/subgroup is known as a *view*.

Views let you visualize your SAN devices according to a specific perspective. The groups are typically organized by location, type, usage, etc. You can create and save any number of views, as detailed in *Section 3.4 Working With Views*, starting on page 30.

Choose View – Views from the menu (or click the Toggle Views  icon in the toolbar) to toggle display of the View Control panel, then click any view in the drop-down list to display that view. The view must have been defined previously.



2.5 The Detail Panes

The detail panes are located at the bottom of the main SANscreen window. The detail panes are designed primarily to provide information about a selected device in the topology pane, but are used for other displays as well (e.g., for Inventory properties). For the Authorized Paths, Paths, and Violations displays, they also are useful to review changes.

The content of the various detail panes are described later on in this manual. If a tab is grayed, there is no data of that type to display.

You can manipulate the detail pane area in a number of ways, increasing or decreasing the number of details panes you see at any time.

- At the bottom of the pane, click a tab to display its corresponding detail pane. Click again to hide it. Detail tabs are grayed if they are not available from the current view.
- Alternatively, use the Tabs option from the View menu to open/close a detail pane. Mark a pane to open it; unmark a pane to close it.

With multiple panes open, drag the divider bars between the panes to view more or less data for any topic.

Change the data displayed in the detail panes by:

- Selecting a device icon in the topology view.
- Selecting a row in the main table (applicable with the Changes detail pane, and only for the Paths, Authorized Paths, and Violations displays).

In addition, you can expand, compress, sort, and filter detail-pane data, as detailed under to *Navigation Tips* (page xv).

2.5.1 Properties Detail Pane

The Properties pane displays the properties associated with the currently selected device. Properties are available for each SAN device, and the information displayed varies depending on the type of device. Select a device in the topology view, or from any main Inventory table (switches, hosts, etc.), to view its properties.

Details about the information displayed in the Properties panes are included where appropriate in this manual.

2.5.2 Paths Detail Pane

The Paths pane displays information about each known logical access path for the currently selected device. Select a device in the topology view, or from any main Inventory table, to display the following information for its paths:

Field	Description
	Violations icon — Displays if the path has a violation.
	Authorized Paths icon — Displays if a policy was defined for the path.
Host	Name of the host from which the path originates.
Storage	Name of the storage device where the data for this path resides.
Volume	Name of the volume where the data for this path resides (not applicable for tape devices).
Capacity (GB)	Size of the volume, in gigabytes (not applicable for tape devices).
Host Ports	Number of host ports that can access the storage (tape device or volume).
Hops	Number of switch devices the path traverses from the host to the storage. The comma-separated list shows the number of switch hops for each physical path. For example, one access path may have two potential physical paths, each with different number of switch devices.
Since	Date/time when the path was first discovered.
	Icon indicating that the path's policy, specified when the path was authorized, is currently designated as a Work In Progress (see page 47). No violations are tracked for a Work In Progress.

2.5.3 Ports Detail Pane

The Ports pane displays information about the ports on the currently selected device. Select a device in the topology view, or from any main Inventory table, to display the following information about the ports on that device. Please be aware that the specific information shown will vary, depending on the type of device:

Field	Description
Port	Applicable for switch and storage ports only. Port identifier.
Port WWN	WWN (World Wide Name) to identify the port.
Connected to	Device and port to which the port above is physically connected.
Fabric/VSAN	Fabric/VSAN on which the port is configured to operate.
State	Current state of the port (taken from the device itself). Please refer to the device documentation for an explanation of values.
Status	Applicable for switch and host ports only. Current status of the port (taken from the device itself). Please refer to the device documentation for an explanation of values.
Speed	Speed capability of the port (not applicable for tape devices).
GBIC	Type of GBIC (GigaBit Interface Converter) used for the port.
FC4	Applicable for switch ports only. FC4 (application layer) protocol, displayed as any subset/combination of the following values: BASIC_LINK EXTEND_LINK FCIP SCSI_FCP FC_SERVICES FC_SW SNMP FABRIC_SERVICES FABRIC DIAG VI

Field	Description
Firmware	Applicable for host ports only. Version of firmware running on the port.
Vendor	Applicable for host ports only. Name of the vendor who sells the port.
Model	Applicable for storage ports only. Manufacturer's model number.
Adapter WWN	Applicable for host ports only. WWN for the device port adapter.
Node WWN	Applicable for storage and host ports. WWN for the port's parent node.

2.5.4 Zone Members Detail Pane

The Zones pane displays a list of zones to which the currently selected device belongs (i.e., is a member of), together with information for each member in that zone.

Select a device in the topology view, or from any main Inventory table, to display its zone information. The details in this tab vary, depending on the type of device selected:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of zones reported in each row.
Zone Name	Name of the zone.
Fabric/VSAN	Fabric/VSAN in which this zone is configured.
Device Type	Type of device selected currently (Host, Storage, Tape, or Generic Device).
Device Name	Name and IP address for the device.
Status	Status of the zone-member device (taken from the device itself). Please refer to the device documentation for an explanation of values.
Member	Zone member information, as known to the Switch or Fabric zoning mechanism:

Field	Description
	- For WWN-based zoning, this is formatted as follows: (X) 10:B0:00:00:00:00:73 Where the value of X can be P, N, or G, to indicate that the WWN that follows belongs to a port, node, or generic device, respectively. - For switch-port based zoning, the formatting varies depending on the type of switch, but looks something like this: 13,fc0 (Switch 3) Where 13 represents the domain ID, and fc0 is the port name. Together these two fields uniquely identify the switch.
Type	Type of zoning used: WWN (for WWN-based) or Switch Port (switch-port-based).

2.5.5 Volumes Detail Pane

The Volumes pane shows information about volumes configured on a disk storage device, or for a host. Select a storage device or a host in the topology view, or in the Storage Devices or Hosts main table, to display its currently defined volumes. The exact detail will vary, depending on the device selected.

Each row corresponds to a specific volume:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of volumes reported in each row.
Storage	Name to identify the storage device.
Volume	Volume name.
Capacity (GB)	Size of the volume, in gigabytes.
Mapped Ports	Number of storage ports through which this volume is accessible.

Field	Description
Masked Hosts	Number of host ports that were defined, by the masking mechanism, as being able to access the specific volume.
Type	Vendor-specific type of volume (e.g., BCV).
Redundancy	Level of mirroring defined for the volume.

2.5.6 Violations Detail Pane

The Violations detail pane displays violations related to a specific device, or as of a particular time stamp. This pane is particularly useful from the:

- Topology pane, where you can click on an item and view the violations relating to that item.
- Changes pane, where you can click on a change and view the violations as of the selected change date/time.

For each violation, SANscreen displays the following information:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of violations reported in each row.
Planned	Icon () indicating that SANscreen has correlated one or more planned tasks with the violation.
Violation Type	Type of violation reported in this row.
Host	Name of the host from which the current path originates.
Storage	Name of the storage device where the data resides for the violating path. If there is no path for the violation (e.g., for a Path Outage violation), this is the storage device where the violation data resides.
Volume	Name of the volume where the data resides for this path (not applicable for tape devices). If there is no path for the violation (e.g., for a Path Outage violation), this is the volume where the violation data resides.

Field	Description
Capacity (GB)	Size of the volume, in gigabytes (not applicable for tape devices).
Host Ports	Number of host ports that can access the storage volume or tape device (blank if none), followed by the number required by the policy, in parenthesis. There is no number in parenthesis if the selected path is not authorized, or no host redundancy is specified in the policy. Please refer to page 47 for a description of the host-port policy requirements. This field is blank (i.e., unknown) for Path Outage violations.
Hops	Actual switch hops between the host and the storage (blank if unknown, as for a Path Outage violation); followed by the number required by the policy, in parenthesis. There is no number in parenthesis if the selected path is not authorized, or no switch-hop maximum is specified in the policy. Please refer to page 47 for a description of the switch-hop policy requirements.
Sharing	Level of volume sharing permitted by the host, as specified by the policy (Any, Cluster, or No Sharing). Please refer to page 47 for a description of the volume-sharing policy requirements.
Tasks	Comma-separated list of planned tasks that relate to the violation.

2.5.7 Masking Detail Pane

The Masking pane displays all disk volumes that are masked and/or mapped, for a particular disk storage device, or for a host. Select a storage device or a host in the topology view, or in the Storage Devices or Hosts main table, to display its currently defined volumes.

Note: SANscreen supports the planning of future volume mapping and masking operations. Please refer to *Section 10.5.11 Add Volume Map* (page 131) for a description of how to define a volume map to SANscreen, and *Section 10.5.12 Add Volume Mask* (page 132) for a description of how to add a volume mask.

Field	Description										
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of masked/mapped volumes reported in each row.										
Storage	Name of the storage device for the volume referenced below.										
Volume	Name of the volume that's masked to the host port referenced to the right (described below).										
Capacity (GB)	Size of the volume, in gigabytes.										
Storage Port	Name of the storage port (on the above named storage device) from which the volume is accessible.										
LUN	Logical Unit Number used by the host to access this volume.										
Status	Mapping/masking status for the volume: <table> <tr> <th>Status</th><th>Indicates that the volume ...</th></tr> <tr> <td>No Mapping</td><td>Is not mapped to a storage port.</td></tr> <tr> <td>Allocated (no masking)</td><td>Is mapped to a storage port and masked to a host, but the masking has been disabled so the volume is accessible to any host (WWN security is disabled).</td></tr> <tr> <td>No masking</td><td>Is mapped but not masked.</td></tr> <tr> <td>Allocated</td><td>Is mapped to a storage port, and masked to a host.</td></tr> </table>	Status	Indicates that the volume ...	No Mapping	Is not mapped to a storage port.	Allocated (no masking)	Is mapped to a storage port and masked to a host, but the masking has been disabled so the volume is accessible to any host (WWN security is disabled).	No masking	Is mapped but not masked.	Allocated	Is mapped to a storage port, and masked to a host.
Status	Indicates that the volume ...										
No Mapping	Is not mapped to a storage port.										
Allocated (no masking)	Is mapped to a storage port and masked to a host, but the masking has been disabled so the volume is accessible to any host (WWN security is disabled).										
No masking	Is mapped but not masked.										
Allocated	Is mapped to a storage port, and masked to a host.										
Host	Host to which the storage volume is masked.										
Host WWN	World Wide Name (WWN) for the host port to which the storage volume is masked.										
Storage WWN	WWN for the storage port (above).										
Detailed Status	Message indicating whether there's any problem with the masking.										
Protocol Controller	Protocol converter through which the volume is mapped to the storage port (applicable only for some types of storage devices, such as EMC Clariion).										

2.5.8 Changes Detail Pane

The Changes pane displays a list of changes related to the selected path, violation, or device. To view change detail, first select either:

- A path or authorized path from the main table.
- A violation from the main table.
- Any device in the topology view, or from any main Inventory table.

SANscreen displays the following information for each change that relates to the selected item — or each set of changes that occurred at a specific date/time:

Field	Description
Time	Date/time at which a Data Source reported this event(s). <i>Note:</i> For Plans processing, this is a list of <i>future changes</i> , and this column is titled Action instead of Time.
<i>icon</i>	Icon indicating the type of event documented on the line (see page xi for a list of icons and their meanings).
Event	List of changes reported by the Data Source at the Time indicated. Click the  symbol to display more detailed change information for each event that occurred at the reported date/time.

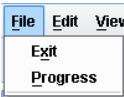
Use the  option to generate an HTML (Web-based) report from the information shown. For additional information (to filter the display, or select a range of dates to see), please refer to Chapter 8, *Reviewing Changes*, beginning on page 77.

2.6 SANscreen’s Main Menu

This section discusses the available menus, in order left-to-right as they appear in the menu bar.

2.6.1 File Menu

The File menu contains two options:

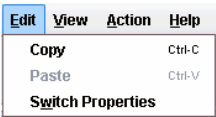


- Exit closes the client application.

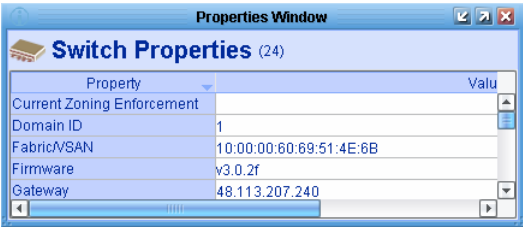
Note: All policy and administrative changes are stored at the time they are entered to SANscreen. Exiting simply closes the SANscreen client.
- Progress opens a window that shows the progress of all acquisition-related tasks (e.g., identifying a host while authorizing a path). You can continue to work with the system while these tasks are processing.

2.6.2 Edit Menu

The Edit menu includes options as follows:



- Copy applies for all screens, and lets you copy selected rows to an external application (Excel, MS Word, etc.). For task management, Copy (or <Ctrl-C>) allows you to copy a task and paste it into the plan.
- Paste (or <Ctrl-V>) applies for task management, and allows you to paste a copied task into the plan.
- <inventory type> Properties is active for Inventory icons only, and lets you display an independent pop-up showing the Properties for switches, hosts & clusters, storage devices, tapes, and generic devices:



2.6.3 View Menu

The View menu includes options as follows:

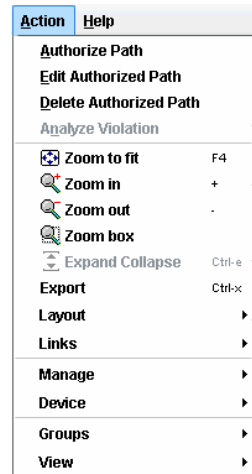
- Auto Refresh automatically refreshes the display whenever a change is reported to the SANscreen server.
- Views opens the View Control panel (see page 11).
- Layers opens the Layer Control panel (see page 10).
- Tabs opens a submenu that includes all available detail tabs. Mark the checkbox to open the corresponding pane; unmark it to hide the pane. Please refer to page 12 for more information about these detail panes.



2.6.4 Action Menu

The Action menu lists specific actions that are available for the current view and selected item(s), and is illustrated to the right for the Paths display. You can also launch this menu by right-clicking with the cursor hovering over the main table or topology pane. Because the actions vary, they are discussed where appropriate throughout this manual.

The top section of the Action menu contains actions that can be executed for the current view. For example, with Paths displayed, the top section of the Action menu (shown here) lets you authorize, edit, or delete the selected path; or analyze a violation.



In the Action menu illustrated here, the next sections apply for the Topology view, and offer actions that help manipulate that view, or manage/identify the devices in that view. These features are described with the Topology layouts in Chapter 3.

2.6.5 Help Menu

The Help menu displays information about the version of SANscreen you are running currently, and/or lets you open the *SANscreen User Manual* and *Installation and Administration Manual* in PDF format.

Chapter 3

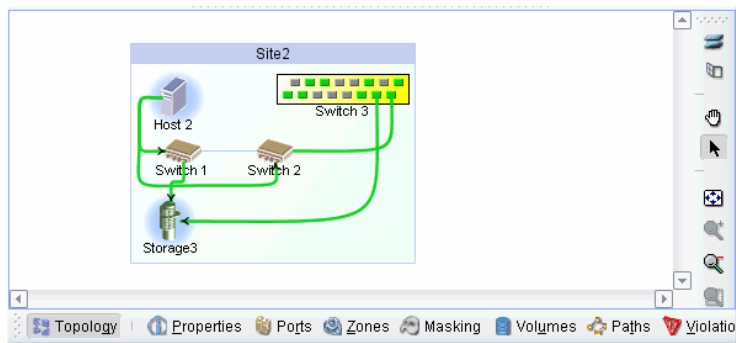
Establishing Topology Layouts

The Topology pane provides a graphic representation of your SAN, allowing you to visualize the SAN devices and their connections. Each user can organize and save the layout in a way that's most appealing to him/her. Custom views can include groups and subgroups that classify the devices in a way that's meaningful to the user.

The instructions in this chapter describe how to manipulate the graphic view and data displayed in the topology pane, thereby creating views that are most useful. Please keep in mind that each topology icon and link is *hot*: you can hover or click, to display relevant information when and where you need it.

To view the topology of your SAN:

1. Choose Topology View from the navigation tree. This presents a large view of your SAN (and no main table data).
- or*
2. Choose Violations, Authorized Paths, Paths, or Changes from the navigation tree. These views include an integrated topology pane below the main table data. You can toggle display of the topology pane from these views by clicking the Topology tab in at the bottom of the screen. :



3.1 The Topology Toolbar

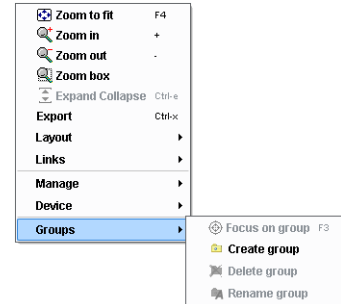
The following tools are available to help create layouts that meet your working needs. These tools are accessible through a toolbar located to the right of the topology pane.

You'll want to experiment to find the tools that work best for you.

Tool	Used to...
	Toggle Layers — Display or hide the Layer Control panel.
	Toggle Views — Display or hide the View Control panel.
	Pan — Drag the topology display around on our screen.
	Select — Select individual devices in the topology display.
	Zoom To Fit — Fit all topology inside the area displayed.
	Zoom In — Zoom in to focus on a specific environment.
	Zoom Out — Zoom out to show more of the topology.
	Zoom Box — Enlarge and center the area where you drag the tool.
	Expand/Collapse Selection — Show/hide detail for the selected item (the group layout if you select a group (site), or individual ports if you select a host, switch, or storage device).
	Focus on Selected Group — Bring the currently selected group or site to the center of the topology display.
	Create a New Group — Open a dialog that lets you create a new group (typically a site).
	Delete Group — Delete the currently selected group.
	Rename Group — Rename the currently selected group.

3.2 The Topology Menu

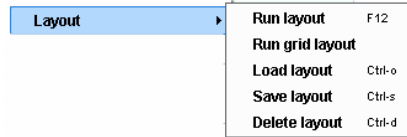
In addition to the tools described above, SANSscreen provides several options that help lay out the topology in a meaningful way. The tools/options are accessible from the Action or right-click menu (shown to the right).



Menu Option	Used to...	See page...
Export	Export a graphic image of the SAN topology.	29
Layout	Automatically arrange the topology icons.	28
Links	Customize the style of your links.	35
Manage	Launch the management console for a device, via a telnet or a Web session.	39
Device	Identify and manage devices, and perform other device-related processing.	37
Groups	Group devices so you can better manage and view them.	31
View	Create a new view, or rename or remove the currently selected view.	30

3.3 Using Layouts

Layouts lets you arrange your SAN devices to best meet your requirements. Follow the instructions below to do this:



1. Establish a starting point for the layout:
 - o Choose Run Layout from the Action or right-click menu. SANscreen positions the icons so as to minimize the number of crossed paths.
 - o Alternatively, for SANs with a limited number of devices, use the Run Grid Layout option to automatically arrange the icons in a grid, with a constant distance between each icon.
2. Create groups and subgroups for fabrics, host groups, and data centers in a way that correctly represents your organization. SANscreen does this for you automatically, but you can create new groups and modify the automatic groups as necessary. Please refer to *Section 3.5 Working With Groups*, starting on page 31 for further details.
3. Drag the icons around the topology pane until the layout looks right. Then save the layout (Save Layout) and assign it a name.

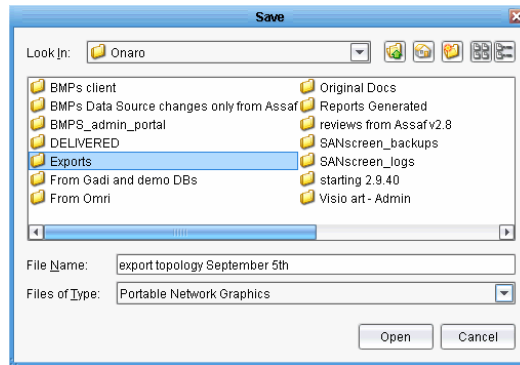
Saved layouts are available to all users, so other users can leverage your work and load the layout you saved. You'll typically use the Load Layout option when a new user is running SANscreen, or when you're running SANscreen on a new machine and you want to return to the last stable topology arrangement.

Use the Delete Layout option as necessary, to remove unused layouts.

3.3.1 Exporting the Topology Layout

You can export the image of your SAN as it appears in the topology pane, for incorporation into reports, or to be sent to a printer. To do this:

1. Open or create the layout you want in the topology pane.
2. Choose Export from the Action menu to open the Save dialog:



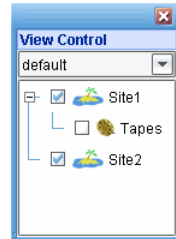
3. Using this dialog:
 - o Select a location to store the new graphics file. As necessary, change the Files of Type field to include the target directory. Use the icons in the upper right corner to go up one level, open the Desktop, create a new folder, provide a plain list, or provide a detailed list, respectively.
 - o Enter a name for the file (File Name field).
 - o Select the type of graphics file to create (Files of Type field). Selecting All Files results in a JPEG.
 - o Click Save.

The layout is now available as a separate graphics file that can be printed or incorporated into other files. As necessary, you can edit the image further using a graphics program.

3.4 Working With Views

SANs can be quite large and include many devices, and a topology that includes all devices is often too cluttered to be useful. You can create *views* that include specific device *groups*, to simplify and organize the display. The device groups can be nested, effectively creating subgroups. Please refer to page 31 for information about groups.

To look at a list of available views from the topology pane, choose View – Views from the menu (or click the Toggle Views  icon in the toolbar). The View Control pane opens, with a drop-down list of the views that have been saved.



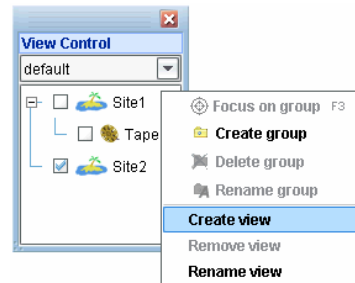
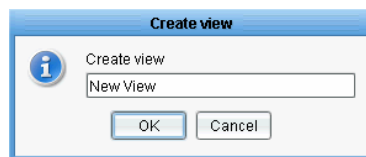
The Default view is a standard view, and cannot be deleted or renamed. This Default view always exists as the initial topology representation.

The sections below tell how to create a new view, rename a view, or remove a view.

3.4.1 Create a View

Use the right-click menu from the View Control pane (right) to create a new view. Alternatively, choose Action – View – Create View from the menu.

Assign a name for the view, then click OK:

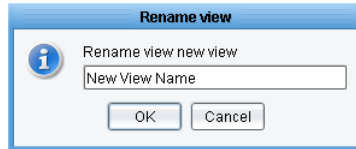


With the new view displayed, the icons maintain the same position they had previously in the topology pane, but any group names are removed. Define new groups for the view, then move your devices around to fit into the groups/subgroups, as you wish. Please refer to *Section 3.5 Working With Groups* for information about working with groups.

3.4.2 Rename a View

Use the right-click menu from the View Control pane to rename an existing view. Alternatively, choose Action – View – Rename View from the menu.

Enter the new name when prompted, then click OK:



3.4.3 Remove a View

Use the right-click menu from the View Control pane to remove an existing view and all its groups. Alternatively, choose Action – View – Remove View from the menu.

You'll be prompted to verify the delete.

3.5 Working With Groups

SANscreen automatically places new devices into topology groups and subgroups as they are added to the SAN. These automatic groups are placed in the Default view. SANscreen creates new groups when required, and adds devices to the most appropriate group/subgroup where they exist already. The groups are named Island 1 (for the group defined when the first device is discovered and added to the SAN), Island 2, Island 3, and so forth.

All the devices in each group have connectivity, and are be placed in up to four subgroups:

- The **Hosts** subgroup contains one or more hosts that have connectivity with the same set of switches.
- The switches subgroup contains all the switches for a particular fabric. The subgroup name will be either the **fabric-name**, if available, or the **fabric WWN**.
- The **Storage Devices** subgroup contains all disk storage devices that are connected to the switches in the group.

- The **Tapes** subgroup contains all tape devices that are connected to the switches in the group.

As each new device is added, as long as it's connected to a device in an existing group, it will be placed in the appropriate subgroups for that group. As soon as a device is added that's not connected to a device in an existing group, SANscreen creates a new group (Island 2, for example).

As necessary, you can create new groups — and/or manipulate the automatic groups — for specific business reasons, such as dividing hosts by user groups.

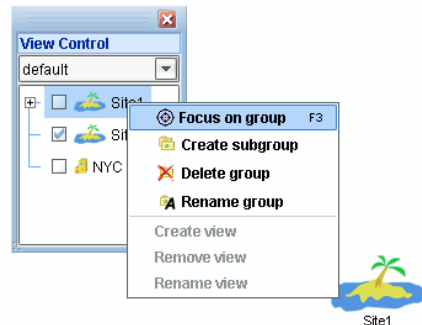
Groups are view-specific, and each view has its own grouping scheme. After you create a view — or when working with the Default view — you can define one or more groups within that view, to combine the devices in a meaningful way.

Groups can be expanded to reveal the devices within, or they can remain closed, making it easier to work with the other groups/devices in your topology. You can nest groups, thereby creating (sub) groups within groups.

This section tells how to work with groups, and details each available activity in order as the group options appear in the right-click menu available from the View Control pane, and/or the topology pane. Before starting, make sure you are working in the correct view by choosing that view from the View Control pane.

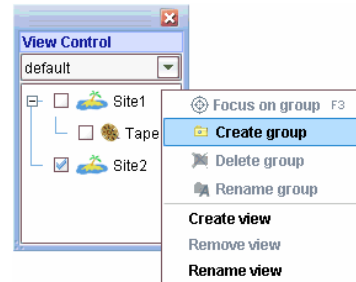
3.5.1 Focus on a Group

Choose the Focus on Group option to bring the group into focus at the center of the topology display.

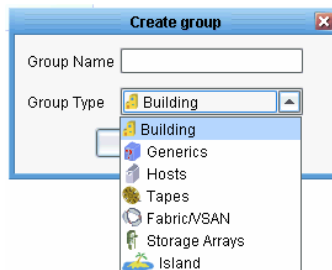


3.5.2 Create a Group (or Subgroup)

While positioned at a particular view, choose Create Group, or click the  icon, to add a new group to that view. To add a nested (sub) group, first select any icon that's part of the parent group, then choose Create Subgroup.



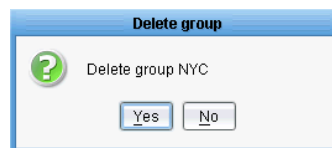
Choose the most appropriate icon for the group from the Group Type dropdown (shown below), and assign a meaningful group name. Click OK when you're through.



SANscreen adds the group to the View Control pane, and adds an empty group box to the topology display. Drag the devices you want into the new group.

3.5.3 Delete a Group

With the target group selected, choose Delete Group, or click the  icon, to delete an existing group. SANscreen verifies the request:



After you click Yes, any devices that were defined within this group will be moved to the background.

3.5.4 Rename a Group

With the target group selected, choose Rename Group, or click the  icon, to rename an existing group:



Type the new name then click OK.

3.6 Tools that Help View the SAN Topology

This section describes additional tools you'll use when working with the topology view.

3.6.1 Zoom Tools

The zoom tools let you to see the big picture, or drill in for a closer look at any level. Select the zoom tools from the Action menu or the topology toolbar.

- **Zoom-to-fit**  — Resizes the topology view to fit within the screen. This does not change the relative location of the icons and links but rather changes the presentation ratio.
- **Zoom-in**  — Increases the zoom factor to 1.5 times the original size.
- **Zoom-out**  — Decreases the zoom factor to 0.66 times the original size.
- **Zoom Box**  — Enlarges and centers an area of the image within the topology pane. (Drag the tool to the area of interest.)

3.6.2 Expand/Collapse Mode

Each SAN device can be viewed in an *expanded mode* by:

- Right-clicking the device and choosing the Expand Collapse option from the drop-down menu.

- Clicking the device, then the Expand Collapse button  to the right.

or

- Double-clicking the device.

In either case, the Expand mode shows the ports of the device and connects each link to the appropriate port. The port color reflects the port status, as follows:

Port Color	Status
Green	Functional
Blue	Unused
Red	Failure
Gray	Unknown

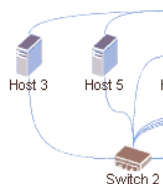
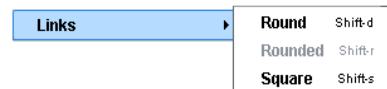
A device appears highlighted (surrounded in color) if zone-highlighting is in effect (described on page 10) and the port is a member of the highlighted zone.

3.6.3 Determining Valid Actions

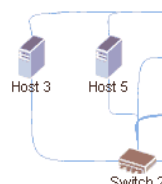
When a right-click menu is opened and the cursor is over a specific device, all the actions relevant to that device are included at the bottom of the menu. These are the same actions that appear in the Action menu.

3.6.4 Changing Link Style

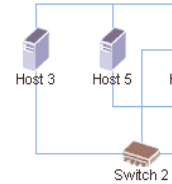
SANscreen's Action – Links option lets you customize your layout views with three different types of link style. You can choose the style that best fits your requirements. The link style is saved as part of a saved layout.



Round



Rounded



Square

3.6.5 Hovering Over an Icon to Display Detail

Detailed device, port, link, and zone information is available at a glance, by hovering the cursor over objects and connections:

- **Device properties** — Let the cursor rest on any device to view that device's properties (shown right).
- **Port properties** — In expanded mode (), move the cursor over any port to see the port detail:

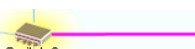


Switch 3	
WWN:	20:D0:00:00:00:00:02
IP:	190.190.181.3
Fabric (VSAN):	20:D0:00:00:00:00:00
Domain Id:	13
Ports:	16



Port fc13	
WWN:	20:0D:00:60:69:51:4F:CD
Node WWN:	10:00:00:60:69:51:4F:CD
State:	Offline
Speed:	2G
GBIC:	Short wave
Model:	9.2
Not Connected	
Fabric:	10:00:00:60:69:51:4E:6B

- **Link properties** — With the cursor over a link, the link is highlighted and its properties display (shown to the left below). If you're working in expanded mode, each link is tied to its corresponding port (shown to the right):



Link (ISL)	
DEVICE	PORT
Switch 3	fc15
Switch 2	fc0

Collapsed Mode



Link (ISL)	
DEVICE	PORT
Switch 3	fc15
Switch 2	fc0

Expanded Mode

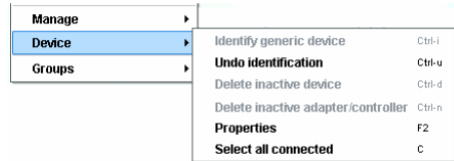
- **Zone properties** — When zones are highlighted (see page 10), position the cursor over any zone rectangle to see the zone detail:



Zone Zone Host 6	
Fabric (VSAN):	20:D0:00:00:00:00:00
Connect to Fabric (VSAN):	true
Devices:	2
Type:	WWN

3.7 Manually Identifying a Generic Device

SANscreen supports automated methods of identifying host devices and their HBAs, based on RegExp and DNS. These methods are further explained in Chapter 11.

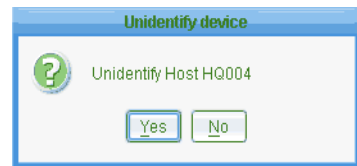


This section describes the manual methods available to identify a host with its HBAs, as well as to undo the identification for a device that was manually identified previously.

By selecting a device in the Topology view and using the Device submenu from the Action or right-click menu, you can manage the device as follows.

Note: Some of these features are also available from the Inventory Action menu. Please refer to Chapter 12 for details about the inventory displays.

- **Identify Generic Device** — Opens the Identify Selected wizard, which is used to identify generic devices (applicable only when clicking on the  icon). Follow the instructions on page 169 to identify the device.
- **Undo Identification** — Removes the identification of a device. (You cannot undo the identification for devices that are discovered through Data-Source acquisition.)



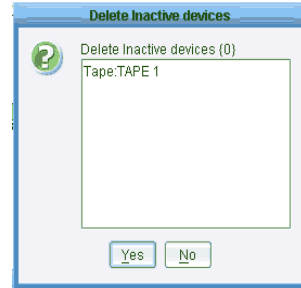
SANscreen will verify the request, as shown to the right. Click Yes to remove the device's identification data from the database, and to change its icon to a generic device icon.

3.8 Other Device-Related Activities

By selecting a device in the Topology view and using the Device submenu described above, you can also perform the following device-management activities.

Note: Some of these features are also available from the Inventory Action menu. Please refer to Chapter 12 for details about the inventory displays.

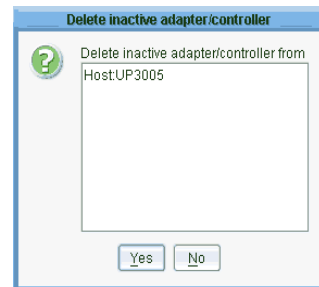
- **Delete Inactive Device** — Removes a device from the SANscreen database, typically after you decommission a piece of equipment in your SAN. SANscreen will verify the request. After you click Yes on the confirmation window, the device is removed from the SANscreen database and disappears from the topology view.



If you remove a host device, its HBAs will now appear as generic devices.

Before using this feature:

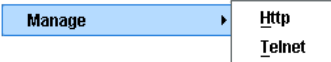
- o Make sure the device is marked as inactive. The device icon and inventory device rows should be grayed, and there should not be any links to any other devices in the topology view. This happens automatically when you remove the Data Source corresponding to the device, as detailed in the SANscreen *Installation and Administration* manual.
 - o If this is a storage or host device, go to the Authorized Paths screen and delete all APs originating from, or targeted to, the inactive device.
- **Delete Inactive Adapter/Controller** — Deletes an inactive host adapter/controller (applicable only with a host device selected). SANscreen will verify the request. After you click Yes on the confirmation window, the adapter/controller is removed from the SANscreen database. (The host device will remain connected to any other HBAs.)



- **Properties** — Opens a separate Properties window, with information that's the same as in the Properties detail pane for the selected device.
- **Select all Connected** — Selects all devices that are connected to the currently selected device. This is useful when building groups (see page 31), to select all the devices you want to place together into a group.

3.9 Managing a Device via Telnet or HTTP

SANscreen lets you open a telnet or Web-based management session to a SAN device. To do this:

1. Highlight the device with which you want to connect — either in the topology pane or in a main Inventory table.
2. Click the right mouse button to open the drop-down menu, or open the Action menu. A screenshot showing a blue button labeled 'Manage' with a right-pointing arrow. A context menu is open to the right of the button, containing two options: 'Http' and 'Telnet'.
3. From the topology view, choose Manage then select either Http or Telnet. From the inventory displays, simply choose Http or Telnet:
 - o Http opens a browser and attempts to connect to the IP address of the selected device.
 - o Telnet opens a console window and attempts to establish a connection with the selected device.

Chapter 4

Viewing and Authorizing Logical Paths

A **logical path** is the relationship between a host server and its data residing on a storage device (disk volume or tape). Each logical path is defined and identified by these two end points: the host server on one end, and the storage volume on the other. A logical path comprises physical links — starting from the link between the server and its edge switch, optionally followed by links between core switches, and completed by the link between an edge switch and a storage volume (or tape). Your SAN can have multiple physical paths for each logical path.

Each path has attributes — including the specific devices on the path between the end points, the number of possible physical paths between the two end points, the level of security of the path between the end points, volume sharing, volume mapping/masking, and so forth.

This chapter describes how to view logical paths and their attributes using the Path List main table, the topology pane, and the detail panes. It also describes how to authorize a path, which involves defining a policy that you want to enforce for the path.

4.1 Reviewing the Path List Main Table

The main Path List table lists all the logical paths in the storage area network. Click the Paths icon,  from the navigation tree (Validation category) to view this table, shown in Figure 3 on page 42.

The number following the table's title, in parentheses, identifies the total number of logical access paths in the list. Each row represents a single logical path. (If your list is grouped (), you'll have to explode the groupings to see this level of detail.) If the row is red, SANscreen has detected a path-related violation.

Click to expand a row that has a + to the left.

Click to consolidate child rows under a parent entry.

Clear all filters.

Use the drop-down list to rearrange how you view the data.

	Host	Storage	Volume	Capacity (GB)	Host ports	Hops	Host Fabrics	Since
Host 3 (1)	Host 3	Storage3		8.00	2	2,1		10/20/03 1:12 ...
Host 4 (1)	Host 4	Storage4		8.00	2	3,2		9/20/05 3:28 PM
Host A (1)	Host A	Storage3		8.00	2	2,1		10/22/03 8:37 ...
Host17 (1)	Host17	TAPE 3		0	1	1		10/20/03 1:12 ...
Host12 (7)	Host12	Storage2			2	1,1		10/20/03 1:12 ...
Host11 (9)	Host11	Storage2			2	1,1		10/20/03 1:12 ...
Host16 (10)	Host16	Storage2			2	1,1		10/20/03 1:12 ...
Host15 (24)	Host15				2	1,1		10/20/03 1:12 ...
Host 5 (1)	Host 5	Storage4		8.00	2	2,1		9/20/05 3:28 PM
Host 6 (1)	Host 6	Storage4		8.00	2	1,2		9/20/05 3:28 PM
Host B (1)	Host B	Storage3		8.00	1	2		10/23/03 2:37 ...
Host10 (19)	Host10				1,2	1,1,1,2,1		10/20/03 1:12 ...

Figure 3: Sample Path List

Each row contains the following information:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of logical paths reported in each row.
	Icon that indicates a path violation. For the No Grouping display, if SANscreen detects a violation, it highlights the row in red and displays this icon in the row. For displays that are grouped (), SANscreen highlights groups/paths that have a path violation in red, and lists the number of violations detected for the row in this field. Please refer to page 62 for a description of possible violations.
	Icon that indicates an authorized path. Either this icon appears in the row (for the No Grouping display), or the number of authorized paths in a grouping appears in this row, as explained above for the Violation icon.
Host	Name of the host from which the path originates.
Storage	Name of the storage device where the data for this path resides.
Volume	Name of the volume where the data for this path resides (not applicable for tape devices).

Field	Description
Capacity (GB)	Size of the volume, in gigabytes (not applicable for tape devices).
Host Ports	Number of host ports that can access the storage (volume or tape device).
Hops	Number of switch devices the path traverses from the host to the storage. This comma-separated list shows the number of switch hops for each physical path. For example, one access path may have two potential physical paths, each with a different number of switch devices.
Host Fabrics	Comma-separated list of fabrics to which the host is connected (fabric name if available; otherwise the fabric WWN). By filtering this field, you can view only those hosts that are connected to a particular fabric(s).
Since	Date/time when the path was first discovered.
	Icon indicating that the path's policy, specified when the path was authorized, is currently designated as a Work In Progress (see page 47). No violations are tracked for a Work In Progress.

4.2 Looking in Detail at an Access Path

When you select a logical path in the Path List main table, SANscreen highlights the row, and displays information related to the selected path in the Topology and Change List panes.

- In the Topology pane, SANscreen highlights the links in the currently selected path, as shown in Figure 4 (page 44). The highlighting is **green** when you select an authorized path, and **red** when you select a violating path.

If the logical path has two fully redundant physical paths, SANscreen highlights both paths. If the logical path does not have two fully redundant paths, SANscreen highlights the two shortest physical paths instead.

By default, SANscreen displays only the path you select in the Path List, helping you to focus on relevant configurations, particularly in large SAN environments. If you want to display all paths (with only the selected path highlighted), unmark the Path Only option in the Layer Control panel.

- The Change List (Changes detail tab) displays all the changes that occurred in the SAN related to the currently selected path. The list of changes includes all the physical actions and configuration changes performed on devices belonging to the path, implications of these actions (such as the path appearing or disappearing), and changes to the corresponding authorized path.

Please refer to Chapter 8, *Reviewing Changes*, starting on page 77, for a general description of the Changes pane.

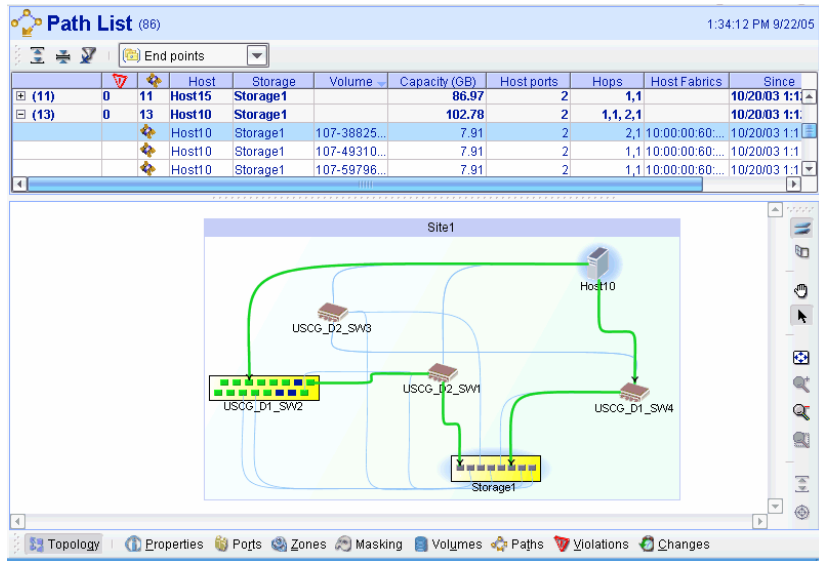


Figure 4: Selecting a Logical Path in the Path List, and the Topology Pane

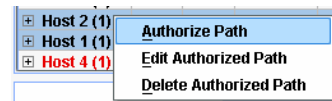
4.3 Authorizing a Logical Path

In addition to the common operations supported by all main tables (described on page 8), the Path List lets you authorize logical paths by creating a policy for each path. You can only authorize a path that has not yet been authorized, and that originates from a host.

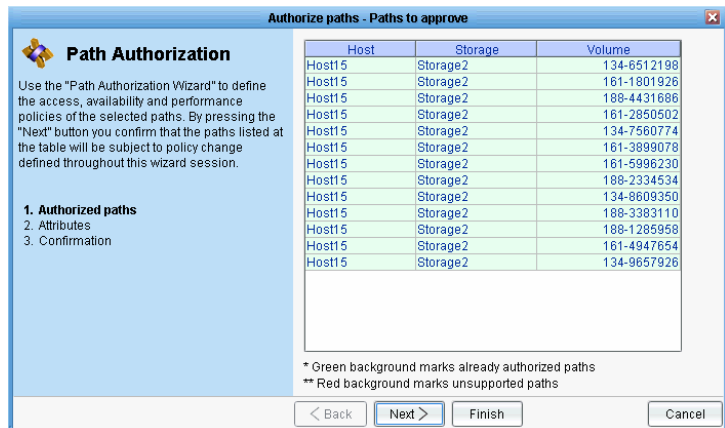
Note: Paths originating from a generic device cannot be authorized. You must identify the generic device as a host before authorizing the path.

You can authorize paths one at a time, or you can group paths that will use the same policy settings, and authorize them in a single step. In either case:

1. Select the path(s) in the Path List main table that you want to authorize. You can select a range of paths (using the <Shift> key), or multiple non-contiguous paths (using the <Ctrl> key). Each selected path will have the same policy applied.
2. Choose Authorize Path from the Action or right-click menu.



SANscreen opens the first page of the Path Authorization wizard, which lists the path(s) you selected:



3. Review the entries and then click Next. The second page lets you specify the policy settings:

Note: You can click Finish at any time, to complete the authorization using all default values.

Path Authorization

Use the "Path Authorization Wizard" to define the access, availability and performance policies of the selected paths.

- Authorized paths
- Attributes**
 - **Redundancy level** -
 - ☐ *None* - No redundancy is required
 - ☐ *No Spf* - The path must be have access to the volume from two redundant routes
 - ☐ *Dual Fabric Redundancy* - The path is able to access the volume through two fabrics and without single point of failure
 - **Sharing** -
 - ☐ *All* - Any host is permitted to access the volume
 - ☐ *Cluster* - Members of the same cluster are permitted to access the volume
 - ☐ *No Sharing* - A single host is permitted access the volume
 - **Min host ports** - Minimum number of host ports that can access the volume
 - **Max switch hops** - Maximum switch hops that separate the server from the volume
 - **Work in progress** - Check when path is not in production. These violations are not listed in the changes view
- Confirmation

Type

Redundancy level:

Attributes

Sharing:

Min host ports: ☒

Max switch hops: ☒

Work in progress: ☐

< Back Next > Finish Cancel

- Complete the fields to define the policy you want SANSscreen to enforce for the selected paths. Table 1 describes each parameter.

Table 1: Policy Options to Authorize a Path

Field	Description
Redundancy Level	Desired redundancy level: • Dual Fabric — The policy requires the host to reach the storage device through at least two different fabrics. • No SPF — The policy requires at least two paths between the host and its storage device, and SANSscreen should verify that each path travels through unique devices. In other words, all SAN devices traversed by a given path must be redundant. If two paths use the same switch, the switch is a possible point of failure for both paths and would be flagged as a violation. • None — No redundancy is required on the path.

Field	Description
Sharing	Level of volume sharing permitted by the host, as follows: - Any — Any host can access the storage, irrelevant of its cluster membership. - Cluster — Members of the same cluster can access the storage, but other hosts cannot. If a host is a member of more than one cluster (or no cluster), that host cannot access the volume. - No Sharing — Only a single host can access the volume. All access paths to the volume must originate from the same host device.
Min Host Ports	Minimum number of host ports that should be active (i.e., have access to the storage volume or tape device) for each path.
Maximum Switch Hops	Maximum number of switch hops on the shortest path between this host and its storage data. This parameter helps with SAN performance issues.
Work in Progress	Check-box used to indicate that the policy should not be enforced yet (typically because SAN changes are not yet complete). By marking this box, you will not receive violation messages. You will have to return here to uncheck this box in order for SANscreen to monitor the path(s).

5. Click Next to open the final page of the Path Authorization wizard:

Path Authorization

Use the "Path Authorization Wizard" to define the access, availability and performance policies of the selected paths. Please confirm the policy settings as summarized.

1. Authorized paths
2. Attributes
3. **Confirmation**

Type

Redundancy level: Dual Fabric

Attributes

Sharing: Any

Min host ports: 2

Max switch hops: 1

Paths

Host	Storage	Volume
Host12	Storage2	134-4415046
Host12	Storage2	134-5463622
Host12	Storage2	107-5979590
Host12	Storage2	187-9188806
Host12	Storage2	107-3882438
Host12	Storage2	107-4931014
Host12	Storage2	188-0237382

* Green background marks already authorized paths
** Red background marks unsupported paths

< Back Next > Finish Cancel

6. Confirm your selections and click Finish.

After completing the wizard, the paths you just authorized will have an authorized-path icon  in the main table, and will display in the Authorized Path List. SANscreen will monitor these paths according to your policy settings.

To make changes to the policy settings, please refer to the instructions in *Section 5.4.2 Editing an Authorized Path*, starting on page 56.

Chapter 5

Viewing Authorized Paths

SANscreen monitors your SAN based on access-control policies. These policies comprise *authorized paths* that:

- Authorize the access between a host and its data on a volume (i.e., a logical path).
- Define the required level of redundancy for the given path.

This chapter describes how to view and manage authorized paths in SANscreen. It also includes instructions to:

- Analyze the violation for a selected Authorized Path.
- Authorize a new path, should you choose to do so from the Authorized Path List
- Edit or delete a path's authorization.

Note: For the most part, you'll authorize paths from the Path List, as described in Chapter 4. This is because you can only authorize a path that has not yet been authorized, and the Authorized Path List, described in this chapter, includes only paths that have been authorized already.

5.1 Reviewing the Authorized Path List Main Table

The main Authorized Path List (APL) table includes a list of all authorized paths (APs) defined to SANscreen (see Figure 5 on page 50). Click the Authorized Paths icon  from the navigation tree (Validation category) to view this table.

The number following the table's title identifies the total number of authorized access paths in the list. Each row in the table represents an authorized path between a server and its data on a specific volume. (If your list is grouped (), you'll have to explode the groupings to see this level of detail.) If the row is red, SANscreen has detected a policy-related violation.

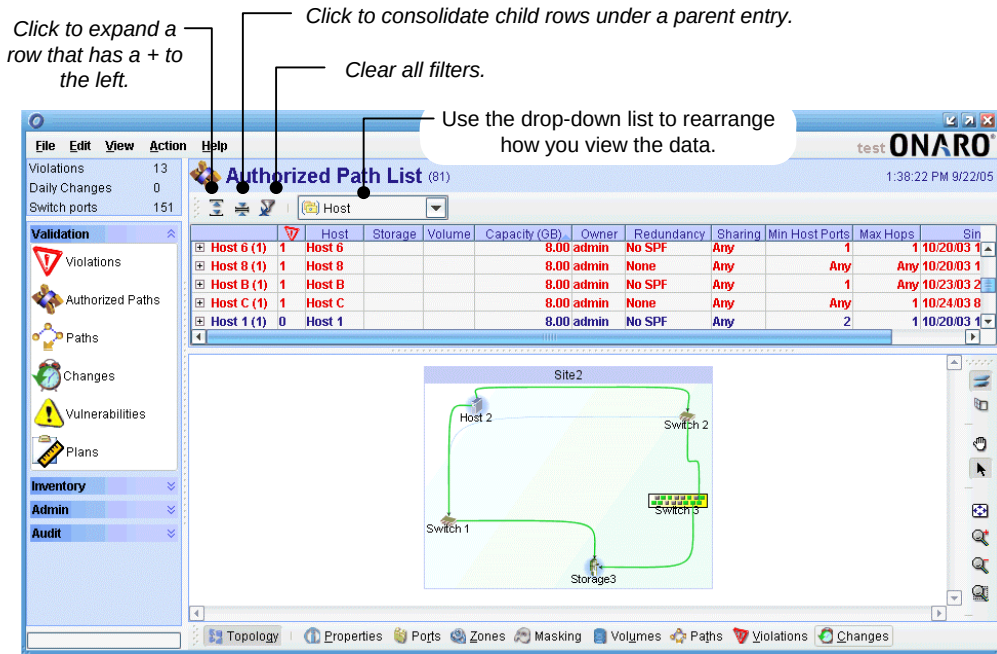


Figure 5: Sample Authorized Path List

Each row contains the following information:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of authorized paths reported in each row.
	Icon that indicates a policy violation. If an authorized path does not currently comply with the policy defined for it, SANscreen highlights the row in red and identifies the number of violations detected. Please refer to page 62 for a description of possible violations.
Host	Name of the host from which the authorized path originates.
Storage	Name of the storage device where the data for this authorized path resides.
Volume	Name of the volume where the data for this authorized path resides (not applicable for tape devices).

Field	Description
Capacity (GB)	Size of the volume, in gigabytes (not applicable for tape devices).
Owner	Name of the user who defined, and is responsible for, the authorized path.
Redundancy	Required redundancy level, as defined when the path was authorized: • None — No redundancy is required on the path. • No SPF — All SAN devices traversed by this path are redundant; therefore, failure within a single device will not cause the logical path corresponding to this authorized path to go down. The policy requires at least two paths between the host and its storage device, and SANscreen verifies that each path travels through unique devices. • Dual Fabric— The host can reach the storage device through at least two different fabrics.
Sharing	Scope of the volume sharing, as defined when the path was authorized (see page 47): • Any — Any host can access the storage, irrelevant of its cluster membership. • Cluster — Members of the same cluster can access the storage, but other hosts cannot. If a host is a member of more than one cluster (or no cluster), that host cannot access the volume. • No Sharing — Only a single host can access the volume. All access paths to the volume must originate from the same host device.
Min Host Ports	Minimum number of host ports that are active (i.e., that have access to the storage data). Value is Any if the policy does not specify any host-port redundancy.
Max Hops	Maximum number of switch hops in the authorized path, between the host and its storage data. Value is Any if the policy does not specify a maximum number of switch hops.
Since	Date/time when the authorized path was first defined.
	Icon indicating that the policy specified when the path was authorized is currently designated as a Work In Progress (see page 47), so that violations are not tracked.

5.2 Looking in Detail at an Authorized Path

When you select an authorized path in the main APL table, SANscreen highlights the row, and displays information related to the selected path in the Topology and Change List panes.

- In the Topology pane (illustrated on page 50), SANscreen highlights the links in the logical path corresponding to the currently selected authorized path. The highlighting is **green** if there are no policy violations; **red** when you select an authorized path that has violations.

If the logical path has two fully redundant physical paths, SANscreen highlights both paths. If the logical path does not have two fully redundant paths, SANscreen highlights the two shortest physical paths instead.

By default, SANscreen displays only the path you select in the Authorized Path List, helping you to focus on relevant configurations, particularly in large SAN environments. If you want to display all paths (with only the selected path highlighted), unmark the Path Only option in the Layer Control panel.

- The APL Change List (Changes detail tab) displays all the changes that occurred in the SAN related to the currently selected authorized path, as illustrated below:

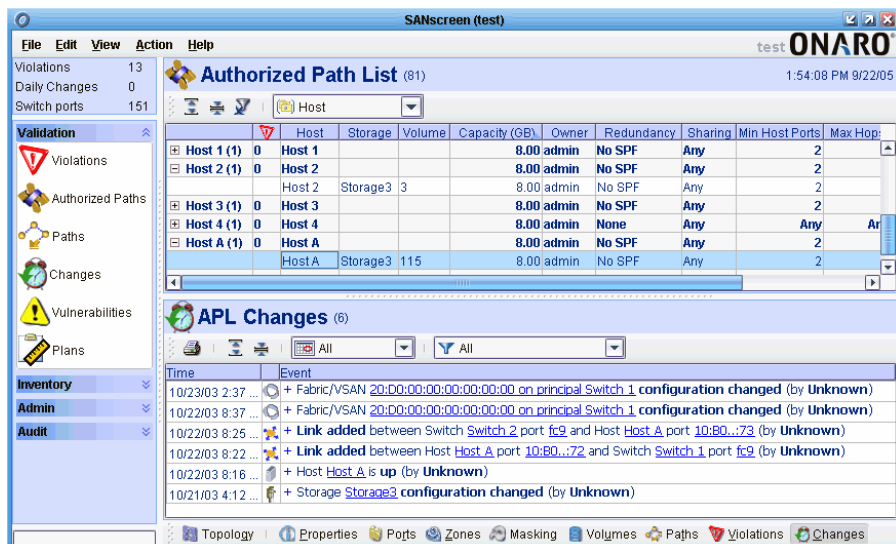


Figure 6: Selecting an Authorized Path and Viewing Changes

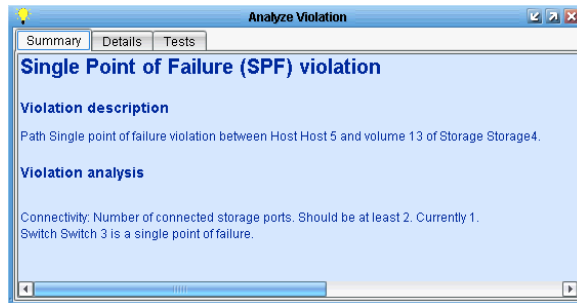
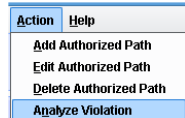
The list of changes includes all the physical actions and configuration changes performed on devices belonging to the path, implications of these actions (such as the logical path appearing or disappearing), and changes to the authorized path itself.

Please refer to Chapter 8, *Reviewing Changes*, starting on page 77, for a general description of the Changes pane.

5.3 Analyzing the Violation For an Authorized Path

If an Authorized Path displays in red, SANscreen has detected a policy-related violation. Follow these steps to analyze the violation:

1. Choose Analyze Violation from the Action or right-click menu.
2. SANscreen analyzes the situation, then displays relevant information in the Analyze Violation window, using three tabs (Summary, Details, and Tests):



Please refer to Chapter 6 *Identifying and Investigating Violations* for further details, particularly the discussion starting on page 66, which explains the violations display.

5.4 Authorization Activities

In addition to the common operations supported by all main tables (described on page 8), the Authorized Path List lets you authorize (and define) a new logical path, edit an authorization, and/or delete an authorized path, as described in the sections that follow.

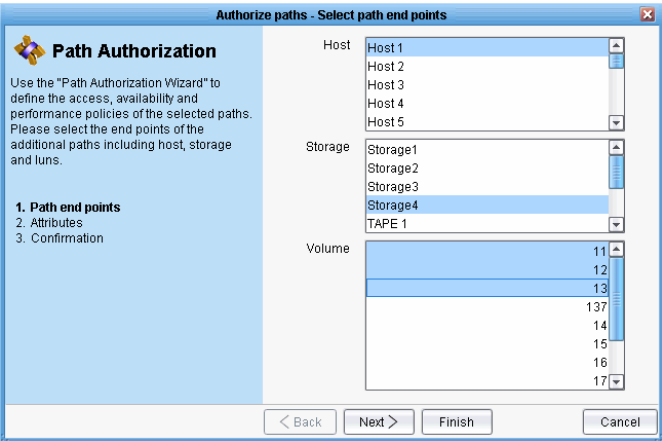
5.4.1 Authorizing a New Logical Path

You can only authorize a path that has not yet been authorized, so typically, paths are authorized from the Path List (available by clicking the Paths icon). The Authorized Path List does not list any path that's not already authorized; however, SANscreen provides a modified version of the Path Authorization wizard for use from the Authorized Path List screen. This version lets you select a host, storage device, and volume(s) individually to create a path that may not yet physically exist in your SAN, and to set policy for that path.

As with the regular Path Authorization wizard, you cannot assign policy for a generic device.

To access the APL's Path Authorization wizard from the APL main table:

1. Choose Add Authorized Path from the Action or right-click menu. This opens the first page of the APL's Path Authorization wizard, which lists all available host and storage devices:



Select the host and storage devices for the path.

2. After you select a storage device (above), the volumes defined on that device appear in the Volume list. Select the volume(s) to include in the path, then click Next.
3. The second page of the wizard prompts for policy settings:

Complete the fields for the policy you want SANscreen to enforce for the path, referring to Table 1 (page 46) for a description of each parameter.

4. Click Next to open the final page of the APL's Path Authorization wizard:

Host	Storage	Volume
Host 1	Storage4	11
Host 1	Storage4	12
Host 1	Storage4	13

5. Confirm your selections and click Finish.

After completing the wizard, the path you authorized will be included in the Authorized Path List. It will also have an authorized-path icon  in the main table of the Paths display (see Chapter 4).

SANscreen begins to monitor the path according to your policy settings.

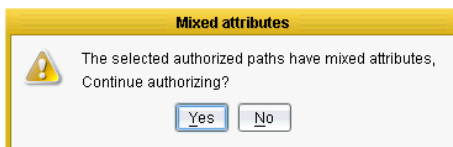
5.4.2 Editing an Authorized Path

After a path is authorized, select it in the Authorized Path List to make changes. You can change the policy for one path at a time, or you can group paths that use the same policy, and change the policy settings for all of them in a single step. In either case:

1. Select the authorized path(s) you want to change in the main table. You can select a range of paths (using the <Shift> key), or multiple non-contiguous paths (using the <Ctrl> key). Each selected authorized path will have the same changes applied to its policy.
2. Choose Edit Authorized Path from the Action or right-click menu.



If you selected more than one authorized path and they are currently defined with different policy attributes, you will receive a warning message (below). Click Yes to continue:



3. SANscreen opens the first page of the Path Authorization wizard, which lists the logical paths corresponding to the authorized paths you selected. Proceed as described for path authorization starting on page 46 (step 4), editing the current values as necessary.

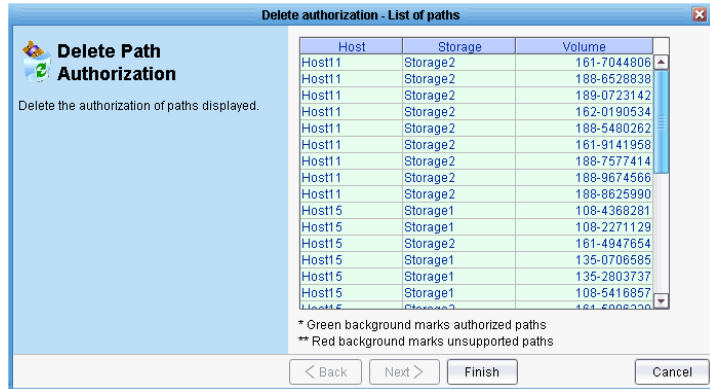
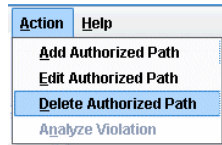
Please note that when editing the policy for multiple paths, the second page of the wizard (i.e., the policy settings) will display default values if the paths currently have different attributes.

5.4.3 Deleting a Path's Authorization

When changes are made to the physical/logical connections in your SAN, it may be easiest to remove the authorization for paths that are involved. You can delete authorization for one path at a time, or you can group paths and delete their authorization in a single step. In either case:

1. In the main table, select the authorized path(s) you want to remove. You can select a range of paths (using the <Shift> key), or multiple non-contiguous paths (using the <Ctrl> key).

- Choose Delete Authorized Path from the Action or right-click menu. This opens the Delete Path Authorization dialog, which lists the path(s) you selected:



- Review the list of authorized paths to be removed, then click Finish.

After you complete the wizard, the authorization is removed from the specified paths, making each one of them a violation. The paths will remain on the violations list (see Chapter 6) until you physically/logically remove them from the SAN.

Chapter 6

Identifying and Investigating Violations

Violations are inconsistencies between SAN paths as they appear in the Path List table (see Chapter 4), and the corresponding authorized paths (i.e., policies) as defined in the Authorized Path List (see Chapter 5). For planned tasks, violations are the same, but are based on *planned* activities instead of actual existing paths.

Each violation identifies a physical SAN connection that does not comply with its authorized path. To correct a violation, either modify the physical/logical connection(s) in your SAN, or update the authorized path.

This chapter explains how to identify violations, how to understand their cause, and how to correct them.

6.1 Identifying Violations

Click the Violations icon,  from the navigation tree (Validation category) to open the main Violation List, shown below with the Topology pane open. This list, shown in Figure 7 on page 60, reports existing or planned violations in your SAN.

The number following the table's title, in parentheses, identifies the total number of violations shown. The Violation List includes one row for each open violation. If your list is grouped (), you'll have to explode the groupings to see this level of detail.

Note: Violations that have been corrected do not appear in this table, but can be viewed from the Changes tab.

By default, all violations display in the main table; however, you can limit the list to include only those violations that are:

- **Planned** — These violations correlate to a task that's in Implementation mode (see page 96). Once a task is put into Implementation mode,

SANscreen automatically correlates that task to any outstanding violations.

- **Not Planned** — These violations do not correlate to any planned task, but are based on existing paths and authorized paths.

To limit the list, use the filter to the far right in the toolbar at the top of the main display:

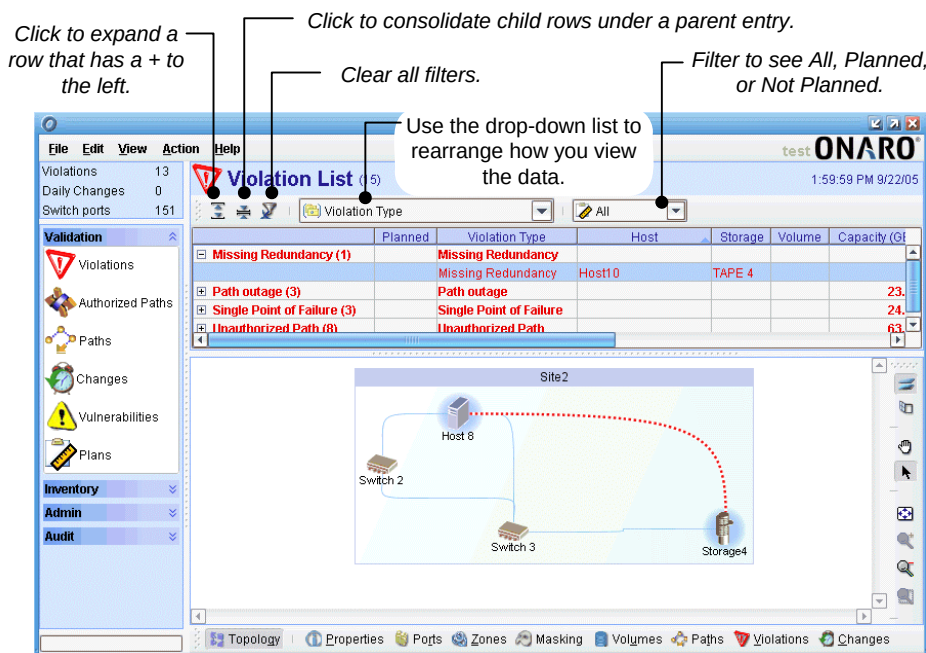


Figure 7: Sample Violation Display

The Topology pane highlights the path corresponding to the currently selected violation. By default, only the path for the selected violation displays in the Topology pane. You can change this to display all paths (with only the selected one highlighted, as illustrated in Figure 7), by unmarking the Path Only option in the Layer Control panel.

The detail panes, available at the bottom of the topology layout, provide information about selected devices in the topology view.

Within the Violation List, each row contains the following information:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of violations reported in each row.
Planned	Icon () indicating that SANscreen has correlated one or more planned tasks with the violation. If you see this icon, look in the Tasks field for a list of planned tasks that correlate to this violation.
Violation Type	Violation type, as detailed in <i>Section 6.2 Types of Violations</i> .
Host	Name of the host from which the path originates.
Storage	Name of the storage device where the data for this path resides.
Volume	Name of the volume where the data for this path resides (not applicable for tape devices).
Capacity (GB)	Size of the volume, in gigabytes (not applicable for tape devices).
Host Ports	Number of host ports that can access the storage volume or tape device (blank if none), followed by the number required by the policy, in parenthesis. There is no number in parenthesis if the selected path is not authorized, or no host redundancy is specified in the policy. Please refer to page 47 for a description of the host-port policy requirements. This field is blank (i.e., unknown) for Path Outage violations.
Hops	Actual switch hops between the host and the storage (blank if unknown, as for a Path Outage violation); followed by the number required by the policy, in parenthesis. There is no number in parenthesis if the selected path is not authorized, or no switch-hop maximum is specified in the policy. Please refer to page 47 for a description of the switch-hop policy requirements.
Sharing	Level of volume sharing permitted by the host, as specified by the policy (All, Cluster, or No Sharing). Please refer to page 47 for a description of the volume-sharing policy requirements.

Field	Description
Host Fabrics	Comma-separated list of fabrics to which the host is connected (fabric name if available; otherwise the fabric WWN). By filtering this field, you can view only those hosts that are connected to a particular fabric(s).
Since	Date/time this violation was first detected.
	Icon indicating that the path's policy, specified when the path was authorized, is currently designated as a Work In Progress (see page 47). No violations are tracked for a Work In Progress.
Tasks	Comma-separated list of planned tasks that relate to the violation. This list only applies with the Planned () icon. Please refer page 70 for more about how to investigate planned violations.

6.2 Types of Violations

SANscreen detects the following types of violations. In all cases, use SANscreen's Analyze Violation capability (detailed starting on page 66) to investigate the problem and fix it.

The table below includes suggestions to clear each type of violation. Please refer to *Section 6.4 Correcting a Violation*, starting on page 71, for a more comprehensive list of suggestions.

Violation	Description
Missing Active Host Ports	A path exists (or is planned to exist) between a server and a specific volume, but too few host ports have access to the volume. • Risk: Path performance is compromised. • Fix: If the path requires more host ports to operate correctly, correct your SAN to add the additional hosts. If the path can operate with fewer host ports, edit the policy to adjust or remove the requirement for host-port redundancy.

Violation	Description
Missing Redundancy	An authorized path exists (or is planned to exist) between a server and a specific volume, but the required <i>dual-fabric</i> redundancy does not exist. The policy specifies that the host must reach the storage device through at least two different fabrics. • Risk: Because the redundancy level is not met, a single failure could cause downtime. • Fix: If the path requires redundancy, add the second path to your SAN. If the path does not require redundancy, edit the policy (i.e., the authorized path definition) to remove the redundancy requirement.
Path Outage	According to the current SAN configuration, no path exists (or is planned to exist) between a server and a particular volume, but such a path is currently defined as an authorized path in the SANscreen database. • Risk: The path is inactive and the server cannot access its data volume, which results in downtime. • Fix: If this is a path you intend to use, analyze the cause of the outage and correct the SAN configuration. If this is a path that you removed, delete the corresponding authorized path.
Single Point of Failure	An authorized path exists (or is planned to exist) between a server and a specific volume, but the required <i>no-SPF</i> redundancy does not exist. The policy specifies that all SAN devices traversed by this path must be redundant. • Risk: Path availability is compromised. Any device that's included in the path could present a single point of failure. • Fix: If the path requires protection against a single point of failure, correct your SAN as necessary. If the path does not require protection against a single point of failure, edit the policy to remove the <i>no-SPF</i> restriction.
Switch Hop Count	A path exists (or is planned to exist) between a server and a specific volume, but there are too many switch hops in the path. • Risk: Path performance is compromised.

Violation	Description
	Fix: If the path requires fewer switch hops, correct your SAN to streamline the path. If the path can operate with more switch hops, edit the policy to reflect this.
Unauthorized Path	A path exists (or is planned to exist) between a server and a specific volume, but the path is not authorized (that is, no policy is defined for it). - Risk: This could be the result of a SAN change that inadvertently led to the creation of an invalid path, or it might represent a potential security problem. - Fix: If this is the result of a recent SAN change and the path is required, authorize the path with the correct level of redundancy and performance, referring to page 45 for instructions. If the path was created unintentionally, remove its enabling configuration parameters.
Unauthorized Sharing	The path volume is shared (or is planned to be shared) and accessible by too many hosts, in violation of the sharing policy. - Risk: Data access violation, security breach, compliance and regulation issues, or a simple mistake that may turn into application downtime and data corruption. - Fix: If the volume should be shared across multiple servers, define it as such (either All or Cluster). If the volume should not be shared to the extent that it is currently specified in the policy, change the SAN configuration to fix this problem.

6.3 Root Cause Analysis of Violations

The SANscreen solution includes various tools that aid in analyzing and identifying the cause of violations, as described in this section. Using this information, you can quickly correct the problem.

- **Section 6.3.1 *The Topology View***, below, tells how to highlight a violation in the Topology pane.
- **Section 6.3.2 *Detail Pane Data*** tells how to use the detail panes from the topology view to review device-level details.
- **Section 6.3.3 *Changes-Based Violation Investigation***, starting on page 66, tells how to view the change history for devices involved in a violation.
- **Section 6.3.4 *Analyzing Violations***, starting on page 66, tells how to use the Action or right-click menu to analyze violations.
- **Section 6.3.5 *Displaying Tasks for Planned Violations***, starting on page 70, tells how to use the planned task display to investigate planned violations.

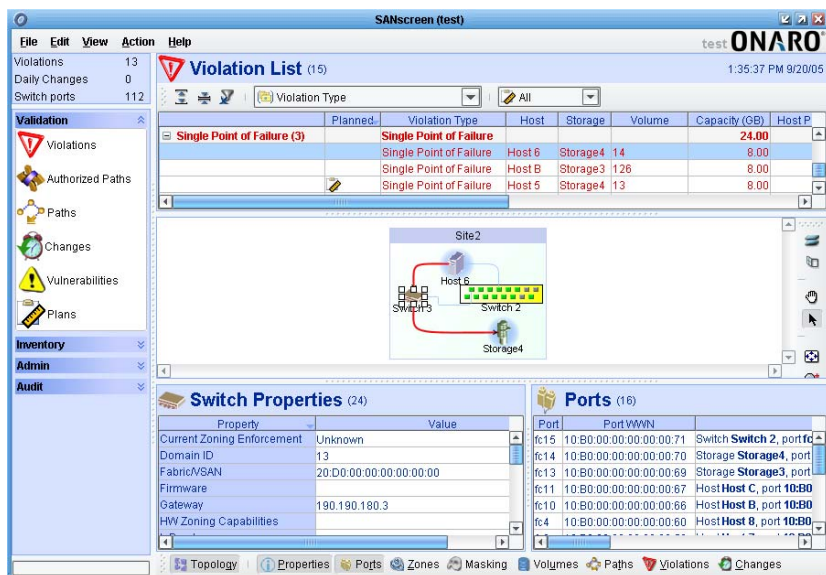
6.3.1 The Topology View

When you select a violation in the Violation List, the Topology pane displays the corresponding violating path, as illustrated in Figure 7 on page 60. Use the detail panes, available from the bottom of the topology view, to review information about devices in the topology (described next).

6.3.2 Detail Pane Data

When you select a device icon in the topology view, the detail tabs display information about that device, including connectivity, ports, logical configuration, historical changes, and so forth.

This is illustrated below for a Single Point of Failure violation, where we requested a list of properties and ports for a particular switch:



6.3.4 Analyzing Violations

To analyze a violation:

1. Select the violation in the Violation List. Make sure to expand the table so you're only working with a single path.
2. Choose Analyze Violation from the Action or right-click menu.
3. SANscreen analyzes the situation, then displays relevant information in the Analyze Violation window, using three tabs (Summary, Details, and Tests).

Action	Help
Authorize Path	
Edit Authorized Path	
Delete Authorized Path	
Analyze Violation	

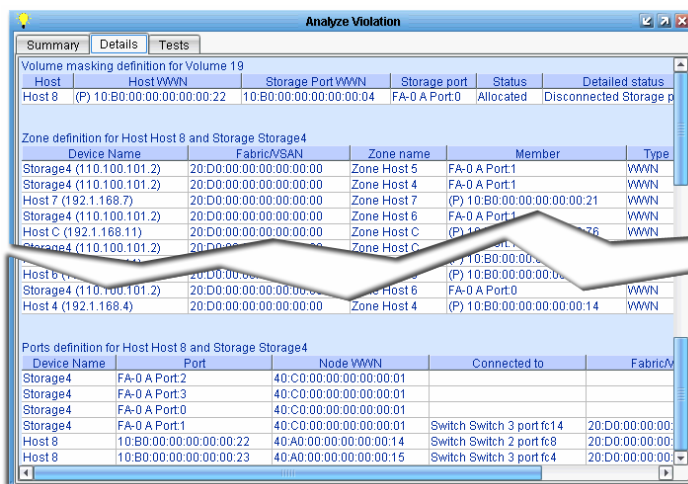
Summary Tab

SANscreen summarizes the violation analysis on the first tab. The summary looks something like this, but will vary depending on the specific violation:



Details Tab

Click the Details tab for additional information about the violation.



The details pane includes three tables:

- **Volume Masking Definition** — Details the masking in effect for the volume that appears in the currently selected violation (in the main table). Please refer to the discussion of the Masking Detail pane for field descriptions (page 18). This table helps identify issues related to masking and mapping errors.
- **Zone Definition** — Details zone membership information. There's one row in this table for each storage port and host port, for all devices involved in the violation. If a port is a member of a zone, a separate row displays for that zone to show zone membership information. This table helps identify host or storage ports that are either not zoned, or that are zoned incorrectly.

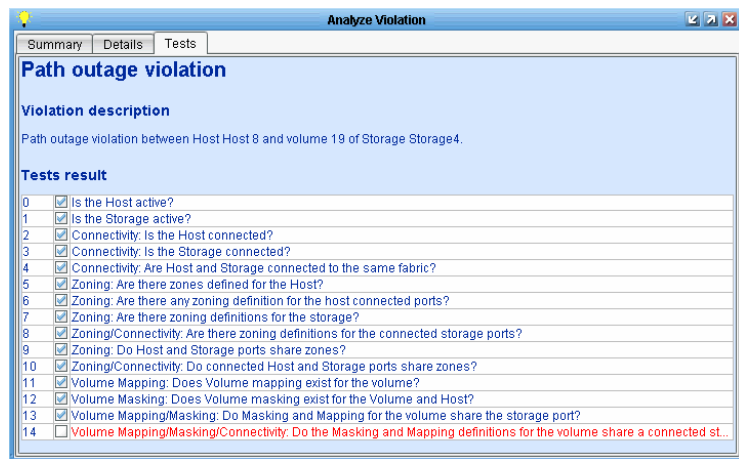
Field	Description																
Device Name	Name of the host or storage device reported on this line.																
Fabric/VSAN	Fabric/VSAN in which the reported zone participates.																
Zone Name	Name of the zone in which the reported port participates.																
Member	Name of the host or storage port referenced above (usually applicable only for storage ports).																
Type	Type of zone member: WWN or Port.																
Status	Status of the port reported on this line: <table> <tr> <th>Status</th><th>Indicates that the zoned port is...</th></tr> <tr> <td>Port connected</td><td>Connected to a switch in the same zone.</td></tr> <tr> <td>Port not connected</td><td>Not connected.</td></tr> <tr> <td>Port connected to another switch</td><td>Connected to a switch that is not in the same zone (possibly indicating a configuration mistake)</td></tr> <tr> <td>Port is connected to a fabric other than the zone's fabric</td><td>Connected to a fabric that is not in the same zone.</td></tr> <tr> <td>Port is connected but is not a VSAN member</td><td>Connected but not configured as a member of VSAN. The port is unusable until it configured to be a VSAN member.</td></tr> <tr> <td>Unnecessary zoning defines a switch's WWN</td><td></td></tr> <tr> <td>Unknown WWN</td><td>Identified by an unknown WWN (was not discovered by SANscreen).</td></tr> </table>	Status	Indicates that the zoned port is...	Port connected	Connected to a switch in the same zone.	Port not connected	Not connected.	Port connected to another switch	Connected to a switch that is not in the same zone (possibly indicating a configuration mistake)	Port is connected to a fabric other than the zone's fabric	Connected to a fabric that is not in the same zone.	Port is connected but is not a VSAN member	Connected but not configured as a member of VSAN. The port is unusable until it configured to be a VSAN member.	Unnecessary zoning defines a switch's WWN		Unknown WWN	Identified by an unknown WWN (was not discovered by SANscreen).
Status	Indicates that the zoned port is...																
Port connected	Connected to a switch in the same zone.																
Port not connected	Not connected.																
Port connected to another switch	Connected to a switch that is not in the same zone (possibly indicating a configuration mistake)																
Port is connected to a fabric other than the zone's fabric	Connected to a fabric that is not in the same zone.																
Port is connected but is not a VSAN member	Connected but not configured as a member of VSAN. The port is unusable until it configured to be a VSAN member.																
Unnecessary zoning defines a switch's WWN																	
Unknown WWN	Identified by an unknown WWN (was not discovered by SANscreen).																

- **Ports Definition** — Details port connectivity. There's one row in this table for each storage port and host port involved in the violation. This table helps identify connectivity issues.

Field	Description
Device Name	Name of the host or storage device reported on this line.
Port	Name of the host or storage port referenced above (usually applicable only for storage ports).
Node WWN	WWN for the host or storage port.
Connected to	Switch port where the reported host/storage port is connected.
Fabric/VSAN	Fabric/VSAN in which the reported port participates.
Status	Port status.

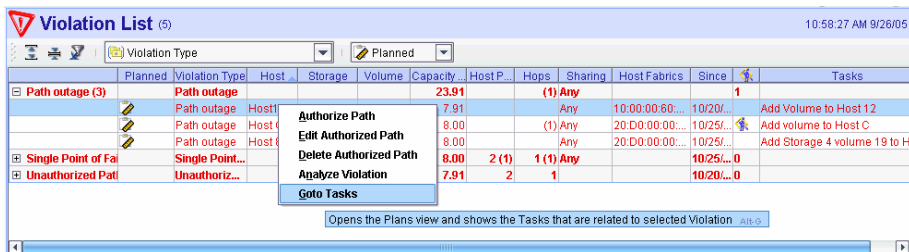
Tests Tab

Click the Tests tab for a list of the tests run by SANscreen to analyze the cause of the violation. Those tests that were successfully completed have a check mark to the left of them. Tests that could not be completed are colored in red, and reflect the root cause of the violation:

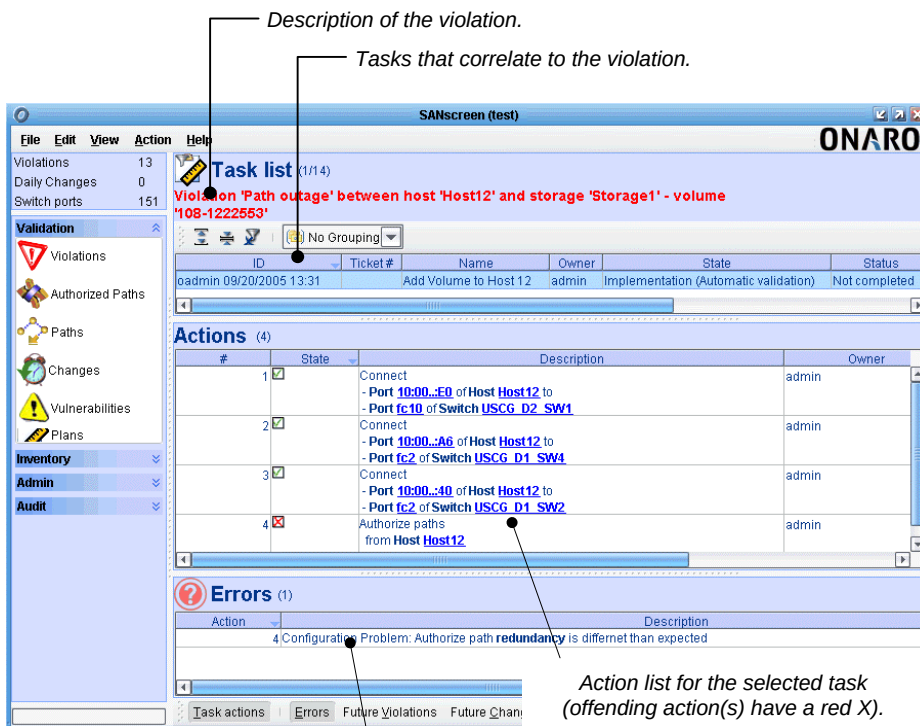


6.3.5 Displaying Tasks for Planned Violations

When a violation correlates to a planned task, SANscreen displays the Planned icon (🔧) for that violation, and identifies the planned task(s) that relate to the violation in the Tasks field. It's useful in this case to locate the offending task(s) in the Plans display. You can do this easily, by right clicking the violation and selecting Goto Tasks.



SANscreen opens the Plans display, with only the offending task(s) listed in the Task List. Review the actions and errors for each task, as illustrated below:



Error(s) causing the violation.

When you're through reviewing the information shown, you can return to the Violations display, or click Plans in the navigation tree to return to the standard planning view.

6.4 Correcting a Violation

The existence of a violation means that the actual path properties as captured by SANscreen do not comply with the path attributes that were established when the authorization was defined (or planned). The discrepancies could result from a problem in the SAN configuration, or an incorrect policy setting for the path.

- If the violation represents a problem in the SAN (actual or planned), alter the SAN configuration as necessary to resolve the violation. SANscreen will clear the violation automatically, after the change is made to the SAN.
- If the policy definition is missing or incorrect, either add, edit, or delete the policy, as necessary to clear the violation. Use the Action or right-click menu, then refer to the appropriate discussion (below) for further detail:
 - o To authorize a path that exists physically, but was not yet authorized, please refer to *Section 4.3 Authorizing a Logical Path*, beginning on page 45.
 - o To establish policy for a path that does not yet exist, refer to *Section 5.4.1 Authorizing a New Logical Path*, beginning on page 54.
 - o To edit the policy for an existing authorized path, refer to *Section 5.4.2 Editing an Authorized Path*, beginning on page 56.
 - o To delete a path's authorization policy, refer to *Section 5.4.3 Deleting a Path's Authorization*, beginning on page 56.

Authorize Path
Edit Authorized Path
Delete Authorized Path
Analyze Violation
Goto Tasks

Chapter 7

Defining and Validating Clusters

If more than one host services the same application(s) and those host devices must have access to the same volumes to work correctly, you should define these hosts as part of the same *cluster*.

Follow the steps in this chapter to define and validate host clusters.

7.1 Defining Clusters

You can add a host to a cluster through vulnerabilities processing, as described for Shared Volume Masking (page 89). In addition, you can add a host to a cluster from the inventory list, as described below.

From the Hosts & Clusters inventory list , described in *Section 12.2 Hosts & Clusters*, use the Action menu to add a host(s) to a cluster:

- **Add to Cluster** — Adds one or more selected host(s) to a cluster. If this is the first definition for the cluster, this option defines the (new) cluster in SANscreen.

Action	Help
Delete inactive device	
Delete inactive adapter	
Undo identification	
Add to cluster	
Auto clustering	
Remove from cluster	
Http	
Telnet	

Before choosing this option, use the <Ctrl> key and the left mouse button to select multiple hosts from the host list. After you choose Add to Cluster, SANscreen prompts for the cluster name and description:



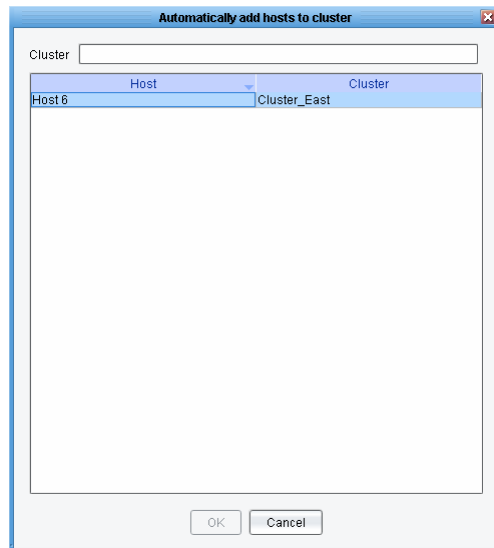
The dialog box titled "Add hosts to cluster" contains two input fields. The first field, labeled "Cluster:", has a dropdown menu with "Clusters_West" selected. The second field, labeled "Description:", contains the text "All hosts to access West Sales DB". At the bottom of the dialog are two buttons: "OK" and "Cancel".

This screen is pre-filled according to the most recent add-cluster processing. Make any changes to the description and/or cluster name, then click OK.

- **Auto Clustering** — Creates a cluster by extracting the cluster name from one or more selected hosts that are named using a format similar to this:

<host-name>_<cluster-name>

Auto clustering lets you define a regular expression (RegExp) that allows extraction of the cluster name from the host name. Enter the expression in the Cluster field:



For example, with your host names formatted as shown above:

<host-name>_<cluster-name>

Enter the regular expression `.*_(.*)` to automatically fill in the cluster names for all the hosts.

After you fill in the regular expression field, SANscreen displays the list of host names, and the cluster name extracted from the host names using the RegExp.

7.2 Validating Clusters

Click the Vulnerabilities icon  from the navigation tree (Validation category) to validate the cluster. In the top part of the display, illustrated below, look for the Incomplete Cluster Volume Sharing vulnerability. If the Occurrences count is 1 or more, at least one volume is not shared correctly by all hosts in the cluster.

**Vulnerabilities** (10)2:12:14 PM 9/22/05

Name	Description
Blocked hosts	Hosts that are connected to a fabric but cannot access any volume or tape on that fabric
Disconnected switch port zone members	Ports defined in a port-zoning configuration and have no device connected to them
Disconnected WWN zone members	WWNs defined in a WWN zoning configuration and are not connected to the fabric
High fabric port usage	Fabrics in which the number of connected ports is higher than 90%
High masking fan-out ratio	Storage ports where number of masked hosts exceeds 8
High volume allocation	Storage devices in which percentage of masked volumes exceeds 90%
Incomplete cluster volume sharing	Volumes that are not shared by all cluster hosts
Low fabric port usage	Fabrics in which the number of connected ports is lower than 70%
Shared volume masking	Volumes masked to more than one host

Incomplete cluster volume sharing (2)

Cluster

Cluster	Storage	Occurrences	Hosts
Cluster_west (2)			
Cluster_west	Storage3	4	8.00 Host 3
Cluster_west	Storage4	12	8.00 Host 4

Vulnerabilities Details

Click the cluster vulnerability in the main table to display vulnerability details.

To view details about the vulnerability(ies) in the lower part of the display, click on the Incomplete Cluster Volume Sharing vulnerability in the main table. This vulnerability, and the details reported for it, are described with the other system vulnerabilities starting on page 88.

Chapter 8

Reviewing Changes

You can display a history of SAN changes in three ways:

- By clicking the Changes  icon in the navigation tree (Validation category) to open the main Change List (illustrated below).
- By clicking in the topology pane with the Changes detail pane open, to view a list of SAN changes that relate to the currently selected device, path, authorized path, or violation.
- By selecting a path, authorized path, or violation in the main display with the Changes detail pane open, to view a list of SAN changes that relate to the currently selected item.
- By selecting a host, storage, or switch device in the Inventory, and opening the Changes detail pane.

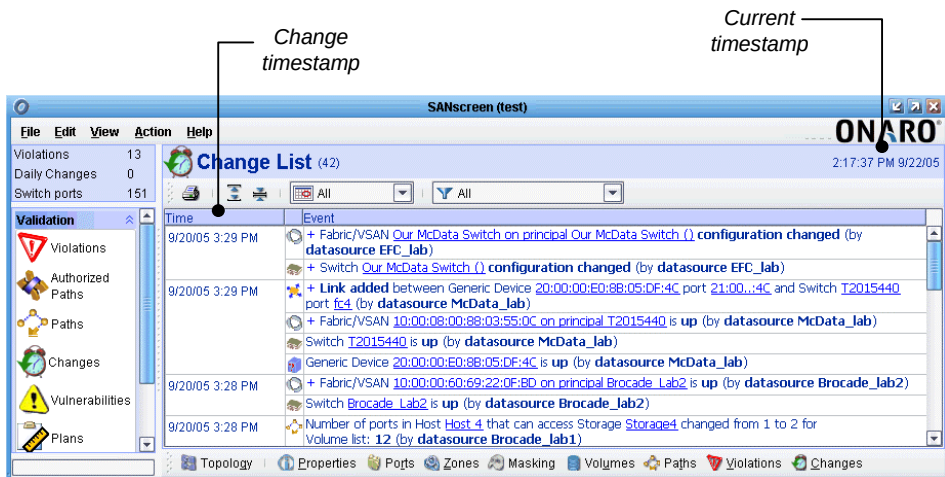


Figure 8: Sample Change List

The Change List includes physical and logical modifications to SAN devices: equipment additions and removals, zoning and volume masking

changes, cabling reconfigurations, outages, and so forth. Policy changes are recorded as a well, because they affect the identification of violations.

The number following the table's title identifies the total number of changes in the list. Each row in the table represents a specific change, and reports the impact of the change on access paths, and any violations created/resolved as a result of the change.

All changes include a time stamp to identify when the change occurred. All changes that occurred from a single action within the SAN are stamped with the same time. Thus SANscreen can recreate and display the state of your SAN at any point in time. By clicking on any change entry in the main table, you can see the state of your SAN at the moment of the change, including the topology and detail panes.

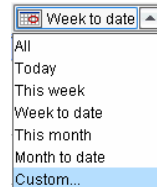
8.1 Working with the Change List

Each entry in the Change List (main table or detail pane) includes a time stamp, an icon identifying the type of change, and a description of the change action that occurred. By default, the most current change is listed at the top, and the changes are in descending order by time stamp. Click the Time column heading to reverse this order, as necessary.

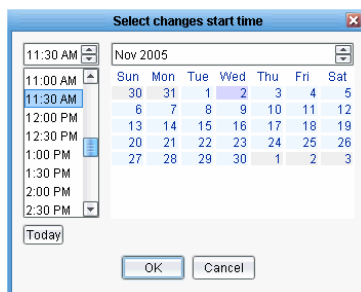
Use the icons above the display as follows:

- Click Show Details  and Hide Details  to display more or less detail.
- Use the calendar  drop-down tool to specify a time range to filter the displayed changes:

1. Click on the arrow on the right of the calendar to open a list of available time-range options (shown to the right).
2. Choose from the available options or click Custom.... For the available options (Today, This week, etc.), SANscreen limits the data in the list according to your selection (changes from today, for just this week, and so forth).



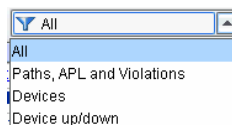
For Custom..., SANscreen prompts for the starting date/time for the changes you want to see. Choose any combination of day and time. Clicking the Today button moves the highlighted date to *today* on the calendar. In our example, we request changes starting from November 2nd at 11:30 a.m.



Click OK. SANscreen displays the change list entries beginning at your selected time, and ending at the present time.

- Use the filtering  drop-down tool to focus your attention on a particular type of change data. The tool allows you to view only logical changes, device-related changes, or device-related up/down events.

1. Click on the arrow on the right of the filter drop-down tool to open a list of filtering options (right).



2. Choose from the available options, as described below. The Change List adjusts to include only the information requested.

Filter Option	Used to display...
All	All changes.
Paths, ALP and Violations	Events relating to logical paths, policies, and violations.
Devices	Events relating to device configuration.
Device up/down	Events related to devices shutting down or booting.

8.2 Using the Topology Pane to View History

SANscreen lets you go back in time and view the state of your SAN before a violation occurred, then step through each action taken thereafter. This simplifies the process of troubleshooting and correction.

In the main Change List table, click on any change to view the topology as of the date/time that change was made (illustrated in Figure 9). Then step your way through the list, watching the topology change. As devices are added, you can select them and review the detail panes to ensure that they were added correctly.

The screenshot displays the SANscreen (test) application interface. The top menu bar includes File, Edit, View, Action, and Help. On the left, a sidebar shows various sections: Validation (Violations, Authorized Paths, Paths, Changes, Vulnerabilities, Plans), Inventory, Admin, and Audit. The main window is titled 'Change List (25)' and shows a table of events. The table has columns for Time and Event. The events listed are:

- 10/25/03 8:22 ... + 1 Violations **created** between Host Host 5 and Storage Storage4 (by Unknown)
- + 1 Violations **created** between Host Host 6 and Storage Storage4 (by Unknown)
- + 1 Violations **created** between Host Host 8 and Storage Storage4 (by Unknown)
- 1 Paths **removed** between Host Host C and Storage Storage4 for Volume list: 137 (by Unknown)
- Number of switch hops between Host Host 4 and Storage Storage4 changed from 1 to 1 for Volume list: 12 (by Unknown)
- + Link **removed** between Storage Storage4 port FA-0 A Port:0 and Switch Switch 1 port fc14 (by ...)

Below the table, a topology diagram for 'Site2' is shown. It features a central 'Switch 2' connected to 'Host 4' (top right), 'Storage4' (bottom center), and 'Switch 3' (bottom left). 'Switch 3' is also connected to 'Switch 1' (bottom right). The diagram uses green lines for connections. The bottom status bar shows tabs for Topology, Properties, Ports, Zones, Masking, Volumes, Paths, Violations, and Changes.

Figure 9: Change list with Violation

8.2.1 Generating an HTML Report of Changes

Click the printer icon  from the Changes display to generate a Web-based report of changes. If you have filtered the display (by time or content), the report includes only the changes that are displayed currently.

As required, use standard browser options to distribute or print the report.

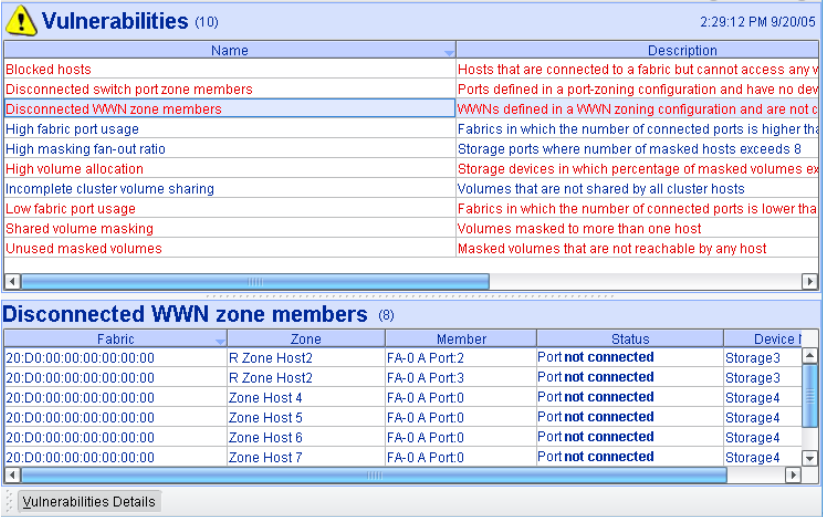
Chapter 9

Assessing Vulnerabilities

In addition to identifying access-path violations, SANscreen reports vulnerabilities — configuration and usage issues that can cause problems, even though they don't result in a path violation. SANscreen looks for vulnerabilities continually as it monitors your SAN changes.

9.1 Viewing Vulnerability Data

Click the Vulnerabilities icon  from the navigation tree (Validation category) to view SANscreen's vulnerability data, as illustrated in Figure 10:



Vulnerabilities (10)		2:29:12 PM 9/20/05	
Name	Description		
Blocked hosts	Hosts that are connected to a fabric but cannot access any v		
Disconnected switch port zone members	Ports defined in a port-zoning configuration and have no dev		
Disconnected WWN zone members	WWNs defined in a WWN zoning configuration and are not c		
High fabric port usage	Fabrics in which the number of connected ports is higher th		
High masking fan-out ratio	Storage ports where number of masked hosts exceeds 8		
High volume allocation	Storage devices in which percentage of masked volumes ex		
Incomplete cluster volume sharing	Volumes that are not shared by all cluster hosts		
Low fabric port usage	Fabrics in which the number of connected ports is lower tha		
Shared volume masking	Volumes masked to more than one host		
Unused masked volumes	Masked volumes that are not reachable by any host		

Disconnected WWN zone members (8)				
Fabric	Zone	Member	Status	Device
20:D0:00:00:00:00:00:00	R Zone Host2	FA-0 A Port:2	Port not connected	Storage3
20:D0:00:00:00:00:00:00	R Zone Host2	FA-0 A Port:3	Port not connected	Storage3
20:D0:00:00:00:00:00:00	Zone Host 4	FA-0 A Port:0	Port not connected	Storage4
20:D0:00:00:00:00:00:00	Zone Host 5	FA-0 A Port:0	Port not connected	Storage4
20:D0:00:00:00:00:00:00	Zone Host 6	FA-0 A Port:0	Port not connected	Storage4
20:D0:00:00:00:00:00:00	Zone Host 7	FA-0 A Port:0	Port not connected	Storage4

Vulnerabilities Details

Figure 10: Sample Vulnerabilities Display

This screen is divided into two parts:

- The **Vulnerabilities** main table lists each type of vulnerability that SANscreen monitors (one row per type, known as a *vulnerability topic*),

and tells how many occurrences there are of each type. Specifically, it includes the following information:

Field	Description
Name	Short description of the vulnerability.
Description	More detailed description of the vulnerability.
Occurrences	How many instances of this vulnerability have been detected in your SAN. If the count is 1 or more, the row displays in red and the Vulnerabilities Details tab applies.

- **Vulnerabilities Details** apply when you click on a red vulnerability topic in the main table. The detail pane provides appropriate information about each occurrence of the selected vulnerability. The number following the table's title identifies the total number of reported vulnerabilities of the selected type.

Each row represents a single vulnerability, and the content of the detail is specific to the selected vulnerability topic, as described starting on page 85.

9.1.1 Establishing Vulnerability Thresholds

The vulnerabilities Action menu lets you set various thresholds that determine when SANscreen reports a condition as a vulnerability. Proceed as follows to set these thresholds:

1. Choose the Configure Vulnerabilities option from the Action or right-click menu in the main table display.
2. Use the dialog that opens to configure your thresholds:

Field	Causes SANscreen to report a vulnerability for each...
High masking fan-out ratio Number of hosts masked per port	Port for which the number of masked hosts exceeds the stated number.

Field	Causes SANSscreen to report a vulnerability for each...
High volume allocation Number of masked volumes	Storage devices for which the percentage of masked volumes exceeds the stated percent.
Low fabric port usage Percentage of connected hosts	Fabric in which the number of connected ports is lower than the stated percent.
High fabric port usage Percentage of connected hosts	Fabric in which the number of connected ports is higher than the stated percent.

9.2 Vulnerability Types

The following sections provide information about each type of vulnerability that SANSscreen monitors, in order as follows:

Vulnerability Type	See page...
Blocked Hosts	85
Disconnected port zone members	86
Disconnected WWN zone members	86
High fabric port usage	87
High masking fan-out ratio	87
High volume allocation	88
Incomplete cluster volume sharing	88
Low fabric port usage	89
Shared volume masking	89
Unused masked volumes	91

9.2.1 Blocked Hosts

SANSscreen identifies hosts that are connected to a fabric but cannot access any volume or tape on that fabric.

Vulnerabilities Details

The vulnerability details include a list of blocked hosts.

9.2.2 Disconnected Port Zone Members

SANscreen identifies ports that are defined in a switch-port based zoning configuration, but that have no device connected to them.

Vulnerabilities Details

The vulnerability details include:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of items reported in the row.
Fabric	Fabric where the port is defined.
Zone	Zone where the port is defined.
Switch	Name of the switch for the unconnected port.
Member	Number to identify the unconnected port.

9.2.3 Disconnected WWN Zone Members

SANscreen identifies unconnected ports that are defined in a WWN-based zoning configuration.

Vulnerabilities Details

The vulnerability details include:

Field	Description
Fabric	Fabric where the port is defined.
Zone	Zone where the port is defined.
Member	WWN to identify the unconnected port.
Status	Status of the vulnerability (e.g., port not connected).
Device Name	Name of the switch for the unconnected port.

9.2.4 High Fabric Port Usage

SANscreen identifies fabrics in which the number of connected ports is higher than the percent configured via the Vulnerabilities Thresholds dialog, page 84 (defaults to 90%).

Vulnerabilities Details

The vulnerability details include:

Field	Description
Fabric/VSAN	Fabric/VSAN that's nearing capacity on port usage.
Used Ports	Number of ports in use currently.
Total Ports	Number of ports available for use.
Switches	Number of switches on this fabric.

9.2.5 High Masking Fan-Out Ratio

SANscreen identifies disk storage ports for which the number of masked hosts exceeds the number configured via the Vulnerabilities Thresholds dialog, page 84 (defaults to 8).

Vulnerabilities Details

The vulnerability details include:

Field	Description
Storage	Name of the disk storage device.
Port	Number to identify the port.
Host Count	Number of masked hosts for the port.
Hosts	Name(s) to identify one or more hosts that access volumes that are mapped to this port (comma-separated if more than one host).

9.2.6 High Volume Allocation

SANscreen identifies disk storage devices where the percentage of masked volumes exceeds the percent configured via the Vulnerabilities Thresholds dialog, page 84 (defaults to 90%).

Vulnerabilities Details

The vulnerability details include:

Field	Description
Storage	Name of the disk storage device.
Total Volumes	Number of volumes currently defined on this device.
Allocated Volumes	Number of masked volumes on the device.

9.2.7 Incomplete Cluster Volume Sharing

SANscreen identifies volumes that are not shared by all hosts in a cluster.

Vulnerabilities Details

The vulnerability details include:

Field	Description
Cluster	Name of the cluster being reported.
Storage	Name of the storage device for the volume below.
Volume	Name of a volume that's not shared by all hosts in the cluster.
Capacity	Size of the volume, in GB.
Hosts with Paths	List of host names that are masked to access the volume referenced above, but that cannot actually access that volume (because of an invalid zoning configuration, cabling errors, a bad mapping, connected to the wrong fabric, and so forth).
Hosts without Paths	Name of each host in the cluster that cannot access the reported volume.

9.2.8 Low Fabric Port Usage

SANscreen identifies fabrics where the number of connected ports is lower than the percent configured via the Vulnerabilities Thresholds dialog, page 84 (defaults to 70%).

Vulnerabilities Details

The vulnerability details include:

Field	Description
Fabric/VSAN	Fabric/VSAN that's low on port usage.
Used Ports	Number of ports in use currently.
Total Ports	Number of ports available for use.
Switches	Number of switches on this fabric.

9.2.9 Shared Volume Masking

SANscreen identifies disk volumes that are masked to more than one host but should not be, in cases where they are not a part of the same cluster.

Note: This vulnerability is not reported for hosts that access the same volume and are members of the same cluster.

Vulnerabilities Details

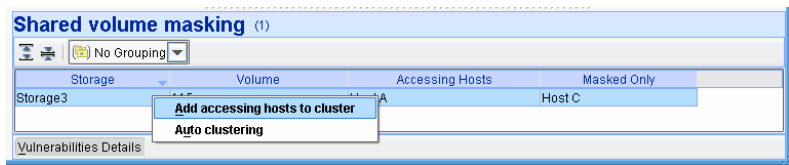
The vulnerability details include:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of items reported in the row.
Storage	Name of the storage device.
Volume	Name to identify the volume.
Capacity	Size of the volume, in GB.
Accessing Hosts	Name(s) to identify one or more hosts to which the volume is masked (comma-separated if more than one host). The host information is based on the volume-masking configuration.

Field	Description
Masked Only	Name(s) to identify one or more hosts that are enabled to access the volume via the masking mechanism, but that cannot physically access the volume (comma-separated if more than one host).

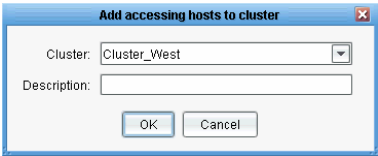
Actions

From the vulnerability details pane, right-click to open a menu that lets you add the accessing host to a cluster:

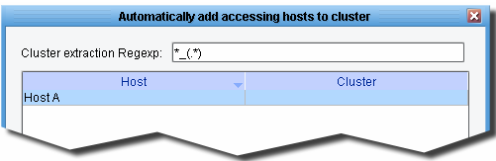


Respectively, the options let you:

- Add the host to a cluster:



- Extract the cluster name automatically using a regular expression:



The processing is identical to that described in *Section 7.1 Defining Clusters*, starting on page 73.

9.2.10 Unused Masked Volumes

SANscreen identifies masked disk volumes that cannot be reached from any host.

Vulnerabilities Details

The vulnerability details include:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of items reported in the row.
Storage	Name of the storage device for the masked volume.
Volume	Name of the masked volume that's not reachable.
Capacity (GB)	Size of the volume, in gigabytes.
Type	Vendor-specific type of volume (e.g., BCV).
Storage Port	Storage port to which the volume is masked.
Host WWN	WWN to identify the host to which the volume is masked.
Host	Name of the host to which the volume is masked.
APL	Authorized Paths icon — Displays if the masked volume participates in an authorized path (i.e., if an authorized path exists from any host to this volume).
Unused Since	Date and time that the volume was last accessible from any host.

Chapter 10

Creating, Validating and Tracking Tasks

SAN change-management, when performed in the production environment, is a major contributor to application downtime (planned and unplanned). Change-management processes require validation to assure application availability, and to maintain a validated SAN at all times. By using SANscreen's planning capabilities, you can minimize application downtime.

Follow the steps below to maintain a validated SAN change process:

1. Create a change plan using the Plans tools and Templates. (A template provides a convenient way to define repetitive tasks that add storage to a new or existing host, as detailed further starting on page 108. Templates are also used to decommission a host device.)
2. Pre-validate the change plan using the Plans tools.
3. Generate task-validation reports and distribute them by email as a hard copy.
4. Execute the plan using vendor-specific tools, tracking the execution using the Plans screen.
5. Locate any deviations from the plan and resolve them.
6. Discover any violations, investigate, and resolve them, referring to Chapter 6 (page 59) for instructions.

This chapter first introduces the Plans screens, then provides a description of the steps required to follow the validate change process (outlined above).

10.1 Plans Screen Overview

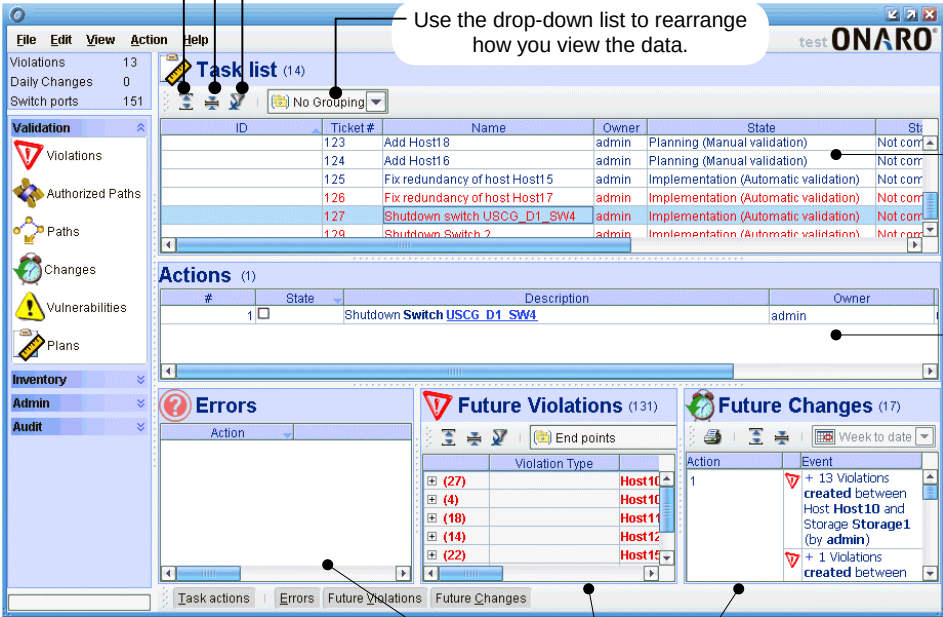
Open the Plans screen by clicking the Plans icon  from the navigation tree (Validation category):

Click to expand a row that has a + to the left.

Click to consolidate child rows under a parent entry.

Clear all filters.

Use the drop-down list to rearrange how you view the data.



ID	Ticket #	Name	Owner	State	St
	123	Add Host18	admin	Planning (Manual validation)	Not corr
	124	Add Host16	admin	Planning (Manual validation)	Not corr
	125	Fix redundancy of host Host15	admin	Implementation (Automatic validation)	Not corr
	126	Fix redundancy of host Host17	admin	Implementation (Automatic validation)	Not corr
	127	Shutdown switch USCG_D1_SW4	admin	Implementation (Automatic validation)	Not corr
	129	Shutdown Switch ?	admin	Implementation (Automatic validation)	Not corr

#	State	Description	Owner
1	☐	Shutdown Switch USCG_D1_SW4	admin

Violation Type	Host
(27)	Host10
(4)	Host10
(18)	Host11
(14)	Host12
(22)	Host15

Action	Event
1	+ 13 Violations created between Host Host10 and Storage Storage1 (by admin)
	+ 1 Violations created between

Task actions | Errors | Future Violations | Future Changes

Figure 11: Sample Plans Screen

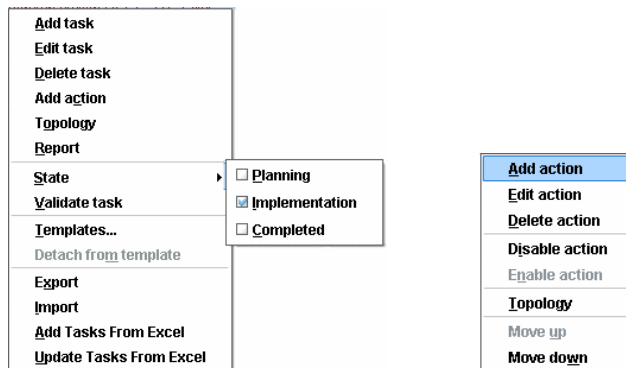
The Plans screen includes the:

-  Task List main table, which lists the planned tasks.
- Actions table (available by clicking the Task Actions tab), which lists the sequence of actions required to complete the task selected in the Task List. These actions should be executed in the order that they appear at the table.

-  Errors detail pane, which lists any errors made in planning the tasks. Please note that errors differ from future violations because they refer to problems that do not affect access paths, but that will still prevent a successful implementation of the task (for example, trying to connect a cable to a port that's not free).
-  Future Violations detail pane, which lists any access-path violations that will occur at the end of the completed task, if not resolved before implementation.
-  Future Changes detail pane, which lists the changes that will be created as a result of the ordered execution of the task actions.

10.1.1 The Plans Action Menu

With the Plans screen open, the Action menu displays a combination of the right-click menus for the Task List and Actions tables. Each entry is described below:



Task List Drop-Down Menu

Actions Drop-Down Menu

Task List Menu Entries

Option	Description
Add Task	Opens the Add New Task dialog so you can add a task.
Edit Task	Opens the Edit Task dialog to show the definition of the selected task, allowing you to make changes.
Delete Task	Deletes one or more selected task (after verification).
Add Action	Opens the Add New Action wizard, used to define a new action for the selected task. (Same as Add Action from the Actions list drop-down menu.)

Option	Description
Topology	Displays a graphical view of the SAN as it will look after execution of all actions in the selected task.
Report	Opens a Web browser and shows the validation report for the selected task. Enter your SANscreen user name and password to view the report.
State	Changes the state of one or more selected tasks (from Planning to Implementation to Completed).
Validate Task	Validates one or more selected tasks.
Templates	Opens the Templates dialog, which displays the currently saved templates. You can edit, delete, and generate a task from an existing template; or you can create a new template.
Detach from Template	Removes the association between a task and the template used to create it originally, so you can edit actions individually.
Export	Saves the task in an XML format that can be used for integration purposes.
Import	Creates new tasks based on task information in an XML user data file.
Add Tasks From Excel	Define one or more new tasks by importing them from an Excel file (available for limited actions).
Update Tasks From Excel	Update tasks that were previously defined by importing them from an Excel file (detailed on page 107).

Actions List Menu Entries

Option	Description
Add Action	Opens the Add New Action wizard, used to define a new action for the selected task. The new action will be added to the end of the action list. (Same as Add Action from the Task List drop-down menu.)
Edit Action	Opens the Edit Action dialog to show the definition of the selected action, allowing you to make changes.
Delete Action	Deletes the selected action.

Option	Description
Disable Action	Turns the action into a Work In Progress, allowing you to validate the task without this action. (The action will be ignored during validation, and related violations will not be tracked.)
Enable Action	Reverses a previous Disable Action to remove the Work In Progress status.
Topology	Displays a graphical view of the SAN as it will look after execution of all actions, up to (and including) the selected action.
Move Up	Moves the selected action up in the list, to precede other actions.
Move Down	Moves the selected action down in the list.

10.2 Creating a Change Plan

A *change plan* is a step-by-step set of instructions that provide a work order for someone to accomplish a specific SAN change. Change plans comprise a set of distinct tasks that you define, similar to a project designation in many enterprises. Each task (project) includes a series of ordered actions to be performed as part of the task.

Follow the instructions below to add tasks to your change plan. There are several approaches you can use, and you can combine these approaches to formulate your plan:

1. **Importing from Excel:** You can import task definitions from an Excel spreadsheet. Please refer to *Section 10.2.3 Importing and Updating Tasks From Excel* (page 101) for related information.

2. **Using templates:** If the task is:

- o A repetitive task to provision storage for a host (existing or new).

or

A task that decommissions a host.

...please follow the instructions in *Section 10.2.4 Defining Templates* (page 108) to define the template (applicable only for provisioning storage), and *Section 10.2.5 Generating Tasks and Actions Using Templates* (page 110) to generate a task based on a pre-defined template.

3. **Using action wizards:** For any other task, the *action wizard* lets you build a specific change plan. Please follow the instruction in *Section 10.2.1 Adding a Task to the Task List* (page 98) to add the new task, and in *Section 10.2.2 Defining Actions Using the Action Wizard* (page 100) to add actions for the task.
4. **By copying** one or more selected tasks (<Ctrl-C> or Edit – Copy from the menu) from the task list, then pasting them into the task list (<Ctrl-V> or Edit – Paste from the menu). The copied tasks will be placed at the top of the list. Make sure to rename the copied tasks, as appropriate.

In addition to adding new tasks as described above, you can export a task to an XML file, then import that file (task) into SANscreen. This is useful to copy a task into the database. To do this, please follow the instructions in *Section 10.2.6 Exporting and Importing Tasks* (page 112).

10.2.1 Adding a Task to the Task List

The main Task List table lists the tasks you define, in the order that you specify them. To add a task to this list:

1. Choose Add Task from the Action or right-click menu to open this dialog:

Fill in the fields to define the new task:

Field	Description
Name	Name of the task. Choose a name that will make it easy for you to identify the task in the list.
ID	Internally generated ID (read-only). Do not enter this field.

Field	Description
Depends On	Task whose completion is a prerequisite to performing the task you're adding. If another task must be completed before this one can begin, select that task from the drop-down list.
State	Current status for the task: • Planning — You are planning and entering the task. In this state, SANscreen does not validate your task actions unless you request it to do so by selecting Validate Task from the Action menu. • Implementation — You have begun execution of the task. In this state, SANscreen continuously pre-validates the task. Make sure to update the State field to take advantage of this feature. The Implementation state consumes more server resources and is recommended only when you are actually executing the task. • Completed — The task is completed but remains for historical tracking purposes. In this state, no further validations are performed unless you specifically request them.
Ticket #	Number of the task/project as it appears in the change ticketing/help desk system, or any other number that identifies the change.
Owner	Name of the person in charge of completing the task. If you do not enter a name, it defaults to your own SANscreen user name.
Starting	Starting date/time for the change.
Ending	Ending date/time for the change.
Comments	Text field, available for free-form comments.

2. Click OK to complete the task entry, and to add the new task at the end of the task list.
3. Enter the ordered list of actions required to complete the task, described next. Double click an action in the Actions list to edit it, as necessary.

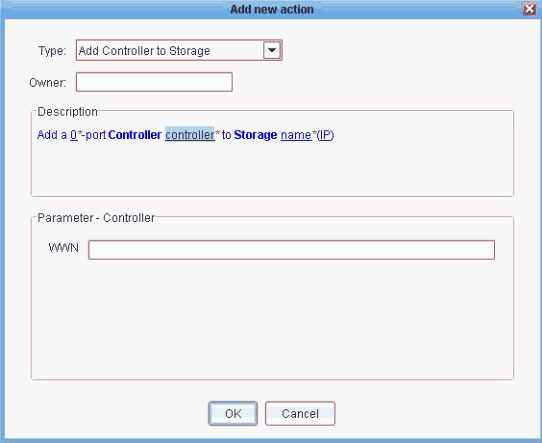
10.2.2 Defining Actions Using the Action Wizard

The Add New Action wizard steps you through the process of creating a specific list of actions for the selected task. The available action types are predefined, and each type of action requires that specific data be supplied in order that SANscreen can pre-validate the effects of the action on your existing SAN. For example, when the task requires the addition of a storage controller, you will have to provide the number of ports on the new controller, its name, and the name and IP address of the storage device where it will be installed.

You must supply *all* of the necessary information for each action. Required information is shown in the wizard using underlined blue text.

To add an action using the wizard, first click on the parent task, then:

1. Choose Add Action from the Action or right-click menu to open the dialog shown to the right.



The screenshot shows a dialog box titled "Add new action". It has a "Type:" dropdown menu with "Add Controller to Storage" selected. Below it is an "Owner:" text field. The "Description:" field contains the text "Add a 0~port Controller controller* to Storage name*(IP)". Below the description is a section titled "Parameter - Controller:" which contains a "WWN" text field. At the bottom right are "OK" and "Cancel" buttons.

2. Select the Type of action to perform from the drop-down list. Please refer to *Section 10.5 Action Types*, starting on page 117, for a description of each available action type.
3. Identify the Owner of the action — either the person who will perform the action or the one who is responsible for seeing that the action is completed. If you do not enter a name, it defaults to your own SANscreen user name.
4. Click on each of the blue underlined entries in the Description field, then enter (or select) the required information for that field. Refer to *Section 10.5 Action Types*, starting on page 117, for instructions that are specific to each type of action you can choose. In many cases, specifying one field value will define other fields automatically.
5. Click OK to complete the definition of the action, and to add the action at the end of the actions list.

10.2.3 Importing and Updating Tasks From Excel

SANscreen lets you import tasks from any Excel file that's compliant with the following versions of Excel:

Excel 97	Excel 2003
Excel 2000	Excel XP

SANscreen generates tasks and actions based on the operations imported from Excel. This section tells how to import tasks from a spreadsheet, as follows:

- **General Rules** outlines some general rules that apply when importing task data.
- **Spreadsheet Format for Task Import** (page 102) details the required format of the input data.
- **Steps to Follow to Import Tasks from a Spreadsheet** (page 106) tells how to use the task file to import tasks and actions.
- **Steps to Follow for Task Update or Delete Via Spreadsheet Import** (page 107) tells how to update previously imported task and action data.

General Rules

Each task must relate to a single host device and a single storage device (but the storage can have multiple volumes). All lines with the same Ref number relate to the same task.

You can import the following types of tasks/operations. For each set of operations, SANscreen generates a task name using the format shown (varies by action):

- **Add Host** — Adds a new host, then adds a path from that host to disk storage. . The task name is generated as:

Add new host <host-name>(<host IP>) to Storage <storage-name>

- **Add Storage to Host** — Adds a new path from an existing host to disk storage. The task name is generated as:

Add storage <storage-name> to host <host-name>(<host IP>)

- **Add Tape** — Adds a new path from an existing host to tape storage. The task name is generated as:

Add Tape <*storage-name*> to host <*host-name*>(<*host IP*>)

- **Host Decommission** — Decommissions a host from the SAN (similar to the processing described starting on page 111). The task name is generated as:

Decommission host <*host-name*>

The switches and storage devices referenced by the task operations must exist already before tasks can be imported from a spreadsheet; however, the Add Host and Add Storage to Host operations can add new volumes.

Spreadsheet Format for Task Import

The input spreadsheet file must contain the following fields in fields B1, B2, and B3, respectively. These fields serve to identify the file, and must be unique across all task-import files:

Date, in *mm/dd/yy* format (e.g., 09/30/05)

Time, in *hh:mm* am/pm format (e.g., 09:50 am)

Name of the submitter (free-form text)

The rest of the file contains one line for each task or action being added or updated, as follows. Fields are listed below moving left to right, starting with column A. All fields are required unless otherwise noted below:

Field	Description
Ref	Reference number of the task/project as it appears in the change ticketing/help desk system, or any other number that identifies the change. Note: When the Ref number displays in the main Task list, it shows up as the concatenation of this value plus the task's <i>objid</i> . Use the same reference number on all rows (actions) that apply for the same task. All lines with the same Ref value relate to a single host and storage device.
By	Name of the person in charge of completing the task. Include only in the first line for the task (i.e., with the first line that includes the task Ref number).

Field	Description
Ticket#	Optional. Number of the task/project as it appears in the change ticketing/help desk system, or any other number that identifies the change.
Operation	One of the following to identify the task action: • Add Host. • Add Storage to Host. • Add Tape. • Host Decommission. For this type of operation, the only fields that are required (in addition to the identifying information, Ref, By and Ticket Number) are the Host Name and Host IP. All other fields are ignored.
Host Name	Target host for the task, identified by name. Must be the same for all lines having the same Ref number, or must appear in only the first line for a particular Ref.
Host IP	Target host for the task, identified by IP address. Must be the same for all lines having the same Ref number, or must appear in only the first line for a particular Ref.
Adapter	World Wide Name for the HBA adapter.
HBA WWPN	World Wide Port Name of the HBA adapter. Must comply with WWN format: <i>hh:hh:hh:hh:hh:hh:hh:hh</i> <i>hh hh hh hh hh hh hh hh</i> <i>hhhhhhhhhhhhhhhh</i> Where <i>h</i> is a single (case-insensitive) hexadecimal digit.
HBA Switch	Name or WWN to identify an existing switch that's connected (or will connect) to the HBA.
HBA Port	Switch port that's connected (or will connect) to the HBA port, formatted as: <unique switch name>/<port number> Where the <unique switch name> provides enough characters to uniquely identify the switch port. For example: R1-FabricA-shelf1/21

Field	Description
	The referenced switch port must exist already in the SAN. If the identifier is not unique, the row will be excluded and an error message generated.
Fabric	Optional. Fabric/VSAN where the HBA and storage port are connected (must exist already in the SAN).
Storage/Frame	Optional. Name of the existing storage device (only one per Ref number). You must provide either the entire name, or enough of the name to uniquely identify the storage device. If the name is not unique (and equally identifies two or more storage devices), the row will be excluded and an error message generated.
Storage ID	ID of the existing storage device (e.g., Symmetrix serial number). You may specify only one storage ID per Ref number.
FA	Optional. Name of the existing FA for the path. Must exist already in the SAN.
FA WWN	WWN of the existing FA port (i.e., storage controller).
FA SW	Name or WWN to identify an existing switch that's connected (or will connect) to the storage port.
FA Port	Number of the existing switch port that's connected (or will connect) to the storage port, formatted as: <i><unique switch name>/<port number></i> Where the <i><unique switch name></i> provides enough characters to uniquely identify the switch port. The referenced switch port must exist already in the SAN. If the identifier is not unique, the row will be excluded and an error message generated.
Zone Name	Name of the zone for the HBA and storage port.
Volumes	Comma-separated list of volumes in the path (ALL for a simple disk device or a tape). Do not include ranges (i.e., use 00a, 00b, 00c instead of 00a..00c). Must be the same for all lines having the same Ref number, or must appear in only the first line for a particular Ref.
Cluster	Applicable when the host is a cluster member. Cluster name to which the host belongs (required when you specify the Volume Sharing).

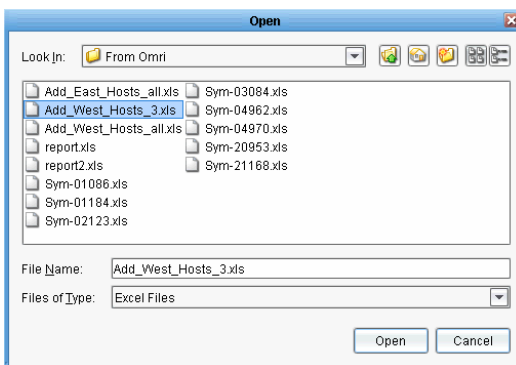
Field	Description
Redundancy	SANscreen policy — Desired redundancy level for the new path, as detailed on page 46 (Dual Fabric (or DF), No SPF (or NS), or None).
Host ports	Optional. SANscreen policy — Maximum number of host ports that can access the storage (tape device or volume referenced by the task). Include only in the first line for the task (i.e., with the first line that includes the task Ref number).
Switch Hops	SANscreen policy — Maximum number of switch devices the new path should traverses from host to storage. Include only in the first line for the task (i.e., with the first line that includes the task Ref number).
Volume Sharing	Optional. SANscreen policy — Level of volume sharing permitted by the host, as specified by the policy (Any, Cluster, or No Sharing). Please refer to page 47 for a description of the volume-sharing policy requirements. If you specify this field, you must specify the Cluster name field as well.
Start Date	Starting date for the task, specified in a field defined as having a Date format in the spreadsheet. Include only in the first line for the task (i.e., with the first line that includes the task Ref number).
Start Time	Starting time for the task, specified in a field defined as having a Time format in the spreadsheet. Include only in the first line for the task (i.e., with the first line that includes the task Ref number).
End Date	Ending date for the task, formatted as described for the Start Date, above. Include only in the first line for the task (i.e., with the first line that includes the task Ref number).
End Time	Ending time for the task, formatted as described for the Start Time, above. Include only in the first line for the task (i.e., with the first line that includes the task Ref number).
Comments	Optional. Text field, available for free-form comments.

Field	Description
	Include only in the first line for the task (i.e., with the first line that includes the task Ref number).

Steps to Follow to Import Tasks from a Spreadsheet

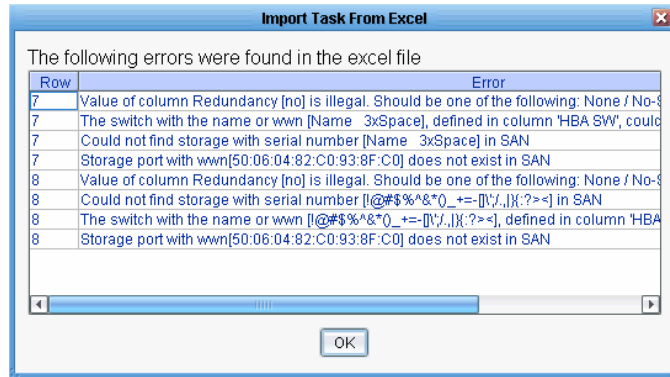
To initiate the task import from a spreadsheet:

1. Choose Action – Add Tasks from Excel from the menu to open a selection window:



2. Select the spreadsheet to import, then click Open.
3. SANSscreen imports the task data, following the rules below:
 - o Create a new task for each task that was not previously imported using the same Reference ID (from a file with the same B1-B3 file-identifying data).
 - o Include in the same task all rows with the same reference number.
 - o Generate the following action(s) for each task, as appropriate:
 - Add Host
 - Add Hosts to Cluster
 - Add HBA to Host
 - Add Volume
 - Add Volume Map
 - Add Volume Mask
 - Add Zone
 - Add Zone Member
 - Connect Ports
 - Authorize Path

4. In the event of an error (i.e., a violation of one or more field constraints), SANscreen generates a report that looks like this:



Each line identifies the exact row, in the spreadsheet, that caused the violation. Note that a single error does not stop the validation process, so the error report provides a complete list of errors for the file.

Steps to Follow for Task Update or Delete Via Spreadsheet Import

An imported spreadsheet task file can be used to update or delete task data, as follows:

- **To update task data** — You can modify a spreadsheet that was used to add tasks, then submit that file again to update those tasks. Make sure the identifying information in fields B1 – B3 is identical to the information in the original file.
- **To delete task data** — You can delete one or more tasks that were added via a spreadsheet. Simply resubmit the file as an update (above), minus whatever tasks you wish to delete. To delete all tasks, submit a file that's blank except for the identifying information in fields B1 – B3. This identifying information should be identical to the information provided when the tasks being deleted were added to the plan.

To update/delete task data:

1. Choose Action – Update Tasks from Excel from the menu to open a file-selection window (illustrated above for the add operation).
2. Select the task file to import, then click Open.
3. SANscreen imports the task data, following the rules below:

- o Delete tasks that were previously imported from a file with the same B1-B3 file-identifying data, but that are missing from the current file.
- o Modify (i.e., redefine) tasks that were previously imported from a file with the same B1-B3 file-identifying data, and that are also included in the current file.
- o Include in the same task all rows with the same reference number.
- o Include with each task an Authorize Path action.

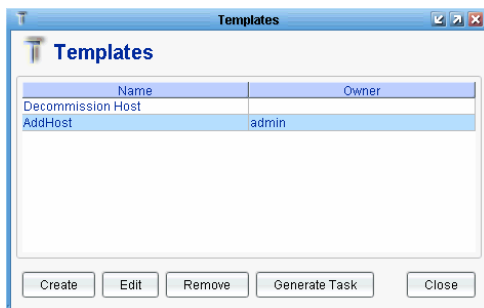
10.2.4 Defining Templates

Templates provide a way to generate tasks and actions based on the template's structure and pre-defined data, thereby enforcing uniform task-entry procedures. SANscreen templates let you:

- Define repetitive tasks that add storage to a new or existing host.
- Define tasks that decommission a host.

You can define any number of storage-to-host templates. The host-decommission template is pre-defined by SANscreen, and available for use as-is.

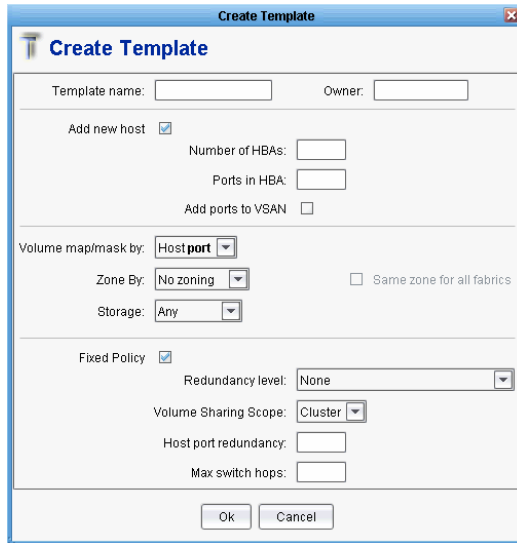
To initiate template processing, choose Templates from the Action or right-click menu of the Plans display. This opens the Templates dialog:



This dialog lists the templates you have already created and saved. You can create new storage-to-host templates from this dialog, you can select an existing template to edit or delete, or you can generate a task from a saved template.

Creating a New Template

To create a storage-to-host template, click the Create button to open this dialog:

The image shows a 'Create Template' dialog box with a blue title bar and a close button. The dialog is divided into several sections. The top section has 'Template name:' and 'Owner:' text boxes. Below this is a section for 'Add new host' with a checked checkbox, and sub-fields for 'Number of HBAs:', 'Ports in HBA:', and 'Add ports to VSAN' (unchecked). The next section is 'Volume map/mask by:' with a 'Host port' dropdown, 'Zone By:' with a 'No zoning' dropdown, and 'Storage:' with an 'Any' dropdown. There is also an unchecked checkbox for 'Same zone for all fabrics'. The final section is 'Fixed Policy' with a checked checkbox, and sub-fields for 'Redundancy level:' (set to 'None'), 'Volume Sharing Scope:' (set to 'Cluster'), 'Host port redundancy:', and 'Max switch hops:'. At the bottom are 'Ok' and 'Cancel' buttons.

- Enter a name for the template.
- Identify the owner of the template (defaults to your SANscreen user name).
- Enter choices to create the content of your template. State the best practices of your storage management, including zoning and volume map/masking types, redundancy level, volume sharing, and switch hops. If you identify a particular Storage device, every task that's generated using the template will be specific to that device; otherwise you can choose the target storage device each time you create a task using the template.
- Click OK to save the template.

Editing or Deleting a Template

Edit and delete functions apply only for storage-to-host templates:

- To edit a template, select the template you want to change then click Edit. Proceed as described above for Create processing, modifying fields as necessary then clicking OK.

- To delete a template, select that template then click Remove. SANscreen confirms that you want to delete the template before proceeding.

Generating Tasks From a Template

To generate a task from a template, click the Generate Task button, then proceed as described next in *Section 10.2.5 Generating Tasks and Actions Using Templates*.

10.2.5 Generating Tasks and Actions Using Templates

Proceed as follows to add a task or action based on a template. This is detailed for the two types of templates below (storage-to-host then host-decommission).

Generating Storage-To-Host Tasks

1. From the Plans display, choose Templates from the Action or right-click menu.
2. Select the template you'll be working with, then click Generate Task to open the following dialog:

Generate task from template 'AddHost'

Task name: Owner: Depends on:

Start time: End time: ID:

Comment: [comments](#) Ticket #:

State:

Host name: Host IP: Cluster:

Storage: [No storage selected](#) Volumes: [No Volumes selected](#)

Policy: [None redundancy, Cluster volume sharing scope](#)

Host		Connected to		Storage Port	Zone name
HBA WWN	Port WWN	Port	Fabric/SAN		
<HBA WWN>	<Port WWN>	<connected>		<Storage Port>	<Zone name>
<HBA WWN>	<Port WWN>	<connected>		<Storage Port>	<Zone name>

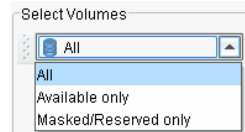
Editor

3. Complete the fields as required to define the task. When you click a blue underlined link, the bottom pane displays a list of items you can select to define that field.

To define an action for an existing task, complete the task identification fields (top-most pane) with the same information contained in the original task. The action will be added to the existing task.

4. When adding Storage, SANscreen includes the status of each volume, to help determine whether a particular volume is masked or reserved by other tasks. The possible status values are detailed on page 132.

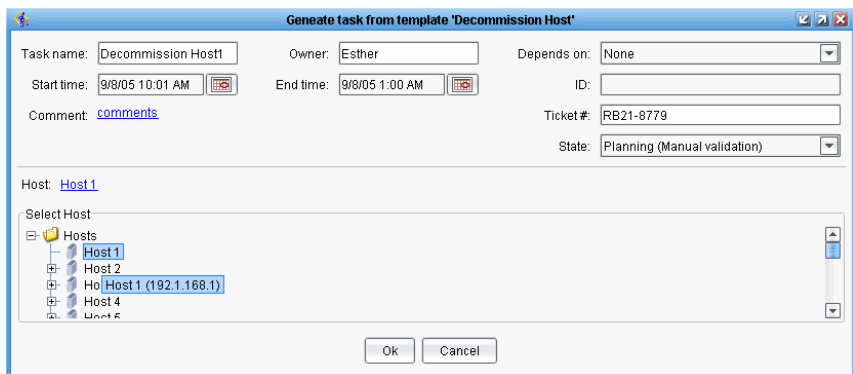
You can limit the volumes shown, by filtering the display. Click the Volumes variable to open a filter that lets you display only the available volumes, or only those volumes that are already masked and/or reserved (right).



5. Click OK to add the task or action.

Generating Host-Decommission-Tasks

1. From the Plans display, choose Templates from the Action or right-click menu.
2. Select the Decommission Host template, then click Generate Task to open the following dialog:



3. Click the Host field, then select the host to decommission from the drop-down list. Add comment if you wish, clicking on the Comment field then entering the comments in the lower pane.

Complete the fields as required to define the task. When you click a blue underlined link, the bottom pane displays a list of items you can select to define that field.

4. Click OK to add the task, and to automatically generate a set of actions to decommission the host (Remove Authorized Path, Remove Volume Mask, etc., down to Shutdown Host).

Note: If the actions are appropriate for the current time *but may be invalid at a later date*, SANscreen displays a warning.

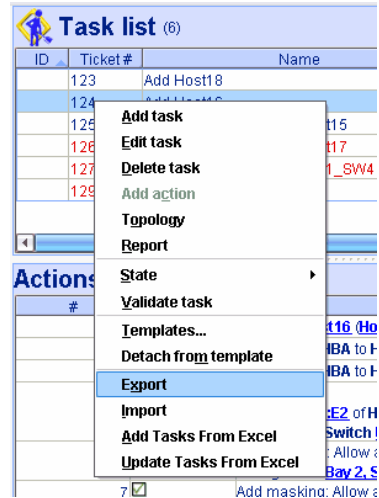
10.2.6 Exporting and Importing Tasks

Using the Export and Import task-list options, you can export a task to an XML file, then use that file:

- To import into the same task list (essentially using it as a copy-and-paste tool).
- To import the task into another SAN.

This is useful for tasks that perform a common function.

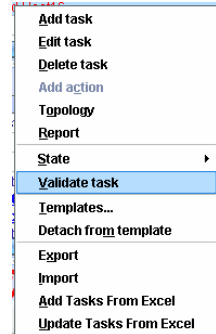
Simply follow the prompts after choosing the Export/Import option, to identify the new (to be created) XML file, or the XML file from which you want to import a task.



10.3 Pre-Validating a Task

When a task is in Implementation mode (see page 99), it's automatically validated any time the SAN changes. If the task is in the Planning or Completed mode, use the drop-down menu to manually pre-validate the integrity of the task, as necessary.

To do this, choose Validate Task from the Action or right-click menu, with the task selected. SANscreen pre-validates the task and refreshes the Plans screen. This can take a few seconds to complete. You'll see an hourglass (🕒) in the Status field as the validation proceeds.



10.3.1 Reviewing Task Validating Results

The first indication of the validation status is visible through the color of the corresponding row in the Task List:

- **Red** indicates that if the task were performed, new violations would be introduced to the SAN.
- **Blue** indicates that implementation of the task would not result in a new violation.

Review the Pre-validation column in the Task List for further details about the validation results: Failed indicates a failure and Passed indicates a successful task validation. When a validation fails, use the detail panes to investigate the violation, as described below (following this table of column values).

When a task validation fails, please refer to the information in the detail panes to investigate the problem(s):

1. View the Future Violations detail pane, illustrated below, to review the future task violations. You can analyze these violations using the Analyze Violation tool from the right-click menu, as described in *Section 6.3.4 Analyzing Violations*, starting on page 66. This tool only works on a single path, so expand (+) the Future Violations list to display each path you want to analyze.

Task list (14)

ID	Ticket#	Name	Owner	State	Sta
123		Add Host18	admin	Planning (Manual validation)	Not com
124		Add Host16	admin	Planning (Manual validation)	Not com
125		Fix redundancy of host Host15	admin	Implementation (Automatic validation)	Not com
126		Fix redundancy of host Host17	admin	Implementation (Automatic validation)	Not com
127				Implementation (Automatic validation)	Not com
128				Implementation (Automatic validation)	Not com

Analyze Violation

Summary | Details | Tests

Missing Redundancy Violation

Violation description
Path Redundancy violation between Host Host10 and volume 107-9125401 of Storage Storage1.

Violation analysis
Zoning/Connectivity: Not enough connected fabrics with shared zones between Host and Storage devices. Minimum 2. Currently 1.

Violations created
Between Host Host10 and Storage Storage1 (by admin)
+ 1 Violations created between Host Host10 and Storage Storage1 (by admin)
+ 13 Violations created

2. View the Errors detail pane to look for action-related errors. Each error listed has an identifying step (i.e., action) number to the left:

Errors (1)

Action	Description
5	Resource Problem: Port 10:00..82 is already connected to Switch USCG_D1_SW2, port fc6

3. View the Future Changes detail pane to review actions that have not yet been implemented, including future violations those actions will create:

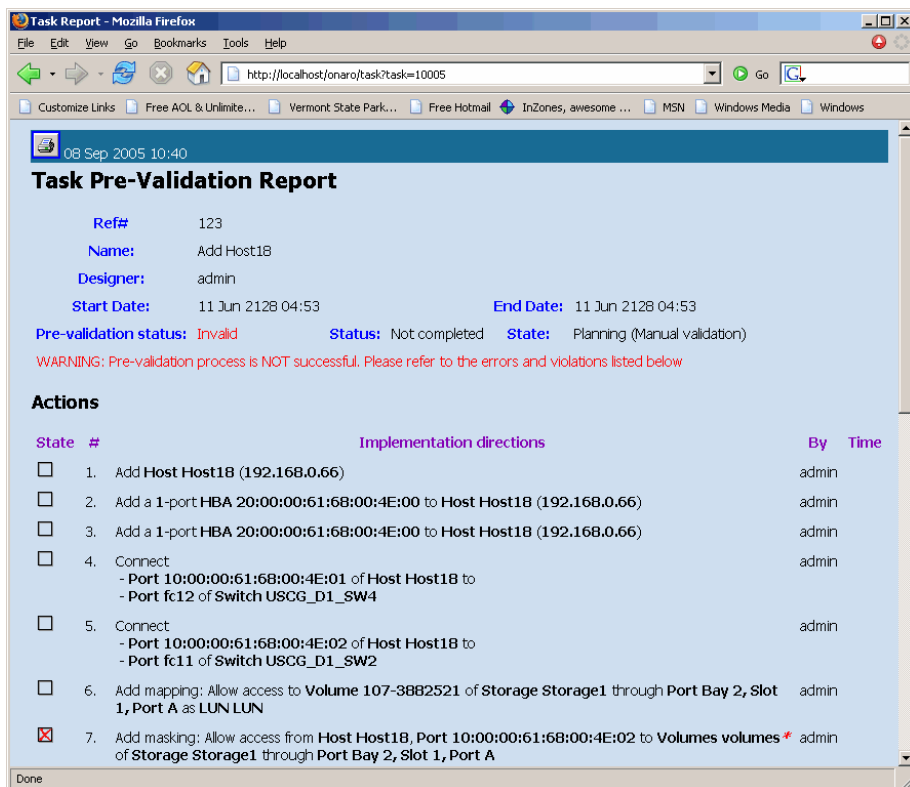
Future Changes (17)

Week to date | All

Event
+ 13 Violations created between Host Host10 and Storage Storage1 (by admin)
+ 1 Violations created between Host Host10 and Storage Storage1 (by admin)
+ 13 Violations created between Host Host10 and Storage Storage1 (by admin)
+ 2 Violations created between Host Host10 and Storage Storage2 (by admin)
+ 2 Violations created between Host Host10 and Storage Storage2 (by admin)
+ 0 Violations created between Host Host11 and Storage Storage2 (by admin)

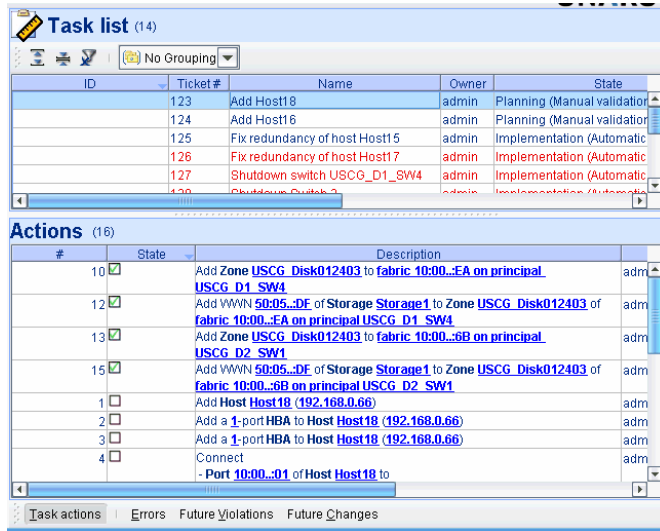
10.3.2 Generate a Task Pre-Validation Report

Choose the Report option from the Task List's right-click menu to generate a Web-based task pre-validation report. Then use standard browser options to distribute or print the report.



10.4 Tracking Task Execution

The check box to the left of each action (State field) indicates the status of that action:



The screenshot shows two windows from a management console. The top window, titled 'Task list (14)', displays a table of tasks with columns for ID, Ticket #, Name, Owner, and State. The bottom window, titled 'Actions (16)', displays a table of actions with columns for #, State, Description, and Owner. The State column in the Actions table contains checkboxes that indicate the execution status of each action.

ID	Ticket #	Name	Owner	State
123		Add Host18	admin	Planning (Manual validation)
124		Add Host16	admin	Planning (Manual validation)
125		Fix redundancy of host Host15	admin	Implementation (Automatic)
126		Fix redundancy of host Host17	admin	Implementation (Automatic)
127		Shutdown switch USCG_D1_SW4	admin	Implementation (Automatic)
128		Shutdown switch USCG_D1_SW1	admin	Implementation (Automatic)

#	State	Description	Owner
10	☒	Add Zone USCG_Disk012403 to fabric 10:00..FA on principal USCG_D1_SW4	adm
12	☒	Add WWN 50:05..DF of Storage Storage1 to Zone USCG_Disk012403 of fabric 10:00..FA on principal USCG_D1_SW4	adm
13	☒	Add Zone USCG_Disk012403 to fabric 10:00..GB on principal USCG_D2_SW1	adm
15	☒	Add WWN 50:05..DF of Storage Storage1 to Zone USCG_Disk012403 of fabric 10:00..GB on principal USCG_D2_SW1	adm
1	☐	Add Host Host18 (192.168.0.66)	adm
2	☐	Add a 1-port HBA to Host Host18 (192.168.0.66)	adm
3	☐	Add a 1-port HBA to Host Host18 (192.168.0.66)	adm
4	☐	Connect - Port 10:00..D1 of Host Host18 to	adm

Refer to this check box to verify the correct execution of the task, as follows:

- A **green check** mark indicates that the action was performed successfully.
- A **red X** indicates an error during the execution of the action (host not physically added, etc.).
- An **empty check box** indicates that the action has not been executed yet.

10.5 Action Types

This section describes the various actions that can be included in a task, and tells how to configure each type of action.

Each action type is described in the sections that follow, in order as they appear in the Add Action menu (and as summarized in Table 2). For each action type, the following information is provided:

- A sample screen.
- **Description** — Short description of the action.
- **Parameters** — Definition of parameters used to configure the action, including underlined (variable) and dark blue parameters. The dark blue parameters are provided automatically after you define or select a value for an underlined parameter. A red asterisk indicates that a field is required.
- **Validating** — Information on how the SANscreen tracks the action.
- **Prerequisites** — Requirements that must be fulfilled before the action can be evaluated during task pre-validation.
- **Implicit actions** — Additional activity/actions that occur when the described action is executed.

Table 2: Action Types (Plans Processing)

Action Type	Used to...	Page
Add Controller to Storage	Add a new port controller to an existing disk storage device.	120
Add Controller to Tape	Add a new controller to an existing tape device.	121
Add HBA to Host	Add a new host bus adapter (HBA) to an existing host.	122
Add Host	Add a new host.	123
Add Hosts to Cluster	Add one or more selected hosts to a cluster, and optionally define a new cluster for this purpose	124
Add Ports to VSAN	Add one or more ports on a Cisco switch to a virtual SAN (VSAN).	125

Action Type	Used to...	Page
Add Storage	Add a new disk storage device.	126
Add Switch	Add a new switch.	127
Add Tape	Add a new tape device.	129
Add Volume	Add a new volume to a disk storage device.	130
Add Volume Map	Add a mapping between a volume and a disk storage port.	131
Add Volume Mask	Add a masking between a volume (disk storage port) and a host.	132
Add VSAN	Allocate one or more VSAN-enabled switch devices to a new or existing VSAN.	134
Add Zone	Add a new zone to a fabric.	135
Add Zone Member (by Switch Port)	Add a particular switch port to a zone.	136
Add Zone Member (by WWN)	Add a new zone member, identified by World Wide Name (WWN).	137
Authorize Path	Authorize paths and set policy for the paths.	138
Connect Port	Verify that some device is connected to a particular switch port.	139
Connect Ports	Connect two ports.	140
Disconnect Ports	Disconnect two ports.	141
Edit Authorized Path	Edit an authorized path.	142
Enable zone configuration	Enable zone configuration.	143
Remove Authorized Path	Remove an authorized path.	144
Remove Controller from a Storage	Remove a controller from a disk storage device.	145
Remove Controller from a Tape	Remove a controller from a tape device.	146
Remove HBA from a Host	Remove an HBA from a host.	147
Remove Ports from VSAN	Remove one or more ports (on a specific switch) from a VSAN.	148

Action Type	Used to...	Page
Remove Volume	Remove one or more volumes from a disk storage device.	149
Remove Volume Map	Remove the mapping between a disk volume and a storage port.	150
Remove Volume Mask	Remove the masking between a disk volume (storage port) and a host.	151
Remove VSAN	Remove a VSAN from one or more switch devices.	153
Remove Zone	Remove a zone from a fabric.	154
Remove Zone Member	Remove a member from a particular zone.	155
Shutdown Host	Shut down a host.	156
Shutdown Storage	Shut down a disk storage device.	157
Shutdown Switch	Shut down a switch.	158
Shutdown Tape	Shut down a tape device.	159

10.5.1 Add Controller to Storage

Add new action

Type: Add Controller to Storage

Owner: admin

Description:
Add a 3-port Controller controller* to Storage name*(IP)

Parameter - Ports

Port WWN
10:80:00:00:00:00:02
10:80:00:00:00:00:03
10:80:00:00:00:00:04

Add Remove

OK Cancel

Description Adds a new port controller to an existing disk storage device.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

of Ports — Number of ports on the controller. Click Add once for each port, then specify the WWN for that port. Click Remove to delete a selected port.

Controller — WWN for the controller.

Storage name (IP) — Storage device for which you're adding the controller, identified by name and IP address. Select the device from the list of available devices.

Validating Test that the controller is up.

Prerequisites The storage device must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions If the controller was removed and now is being added (all in the same task), this action restores all of the controller's ports, port connectivity, volumes, and volume mapping/masking.

10.5.2 Add Controller to Tape

The screenshot shows a dialog box titled "Add new action". It has a "Type" dropdown menu set to "Add Controller to Tape". Below it is an "Owner" text field with the value "admin". The "Description" field contains the text "Add a 2-port Controller 50:05:07:63:00:40:4B:92 to Tape name*(IP)". The "Parameter - Controller" section has a "WWN" text field with the value "50:05:07:63:00:40:4B:92". At the bottom of the dialog are "OK" and "Cancel" buttons.

Description Adds a new controller to an existing tape device.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

of Ports — Number of ports on the controller. Click Add once for each port, then specify the WWN for that port. Click Remove to delete a selected port.

Controller — World Wide Name for the controller.

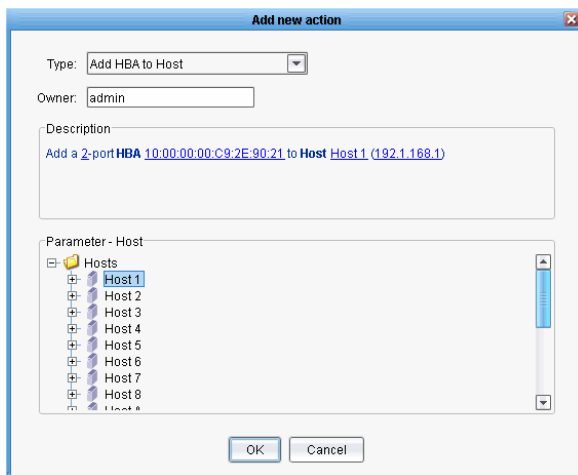
Tape name (IP)— Tape device for which you are adding the controller, identified by name and IP address. Select the device from the list of available devices.

Validating Test that the controller is up.

Prerequisites The tape device must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions If the controller was removed and now is being added (all in the same task), this action restores all of the controller's ports and port connectivity.

10.5.3 Add HBA to Host



Description Adds a host bus adapter (HBA) to an existing host.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

of Ports — Number of ports on the HBA. Click Add once for each port, then specify the WWN for that port. Click Remove to delete a selected port.

HBA Adapter— World Wide Name for the HBA adapter.

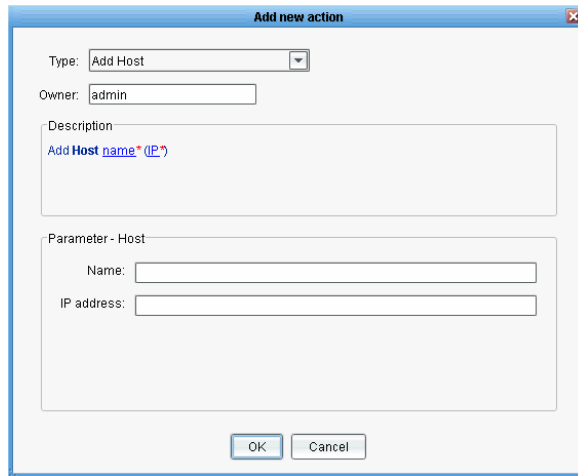
Host name — Host where you're adding the HBA, identified by name and IP address. Select the host device from the list of available devices.

Validating Test that the HBA is up.

Prerequisites The host must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions If the HBA was removed and now is being added (all in the same task), this action restores all of the host's ports, port connectivity, volumes, and volume mapping/masking.

10.5.4 Add Host



The screenshot shows a dialog box titled "Add new action". It has a "Type:" dropdown menu with "Add Host" selected. Below it is an "Owner:" text field with "admin" entered. A "Description:" text area contains the text "Add Host name* (IP*)". Below the description is a section titled "Parameter - Host" which contains two text input fields: "Name:" and "IP address:". At the bottom right of the dialog are "OK" and "Cancel" buttons.

Description Adds a new host.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the option you want:

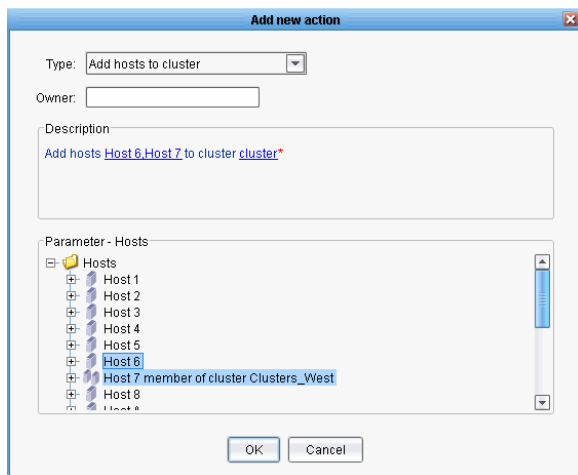
Host name (IP) — Name and IP address to identify the host. You'll be prompted to enter these values separately.

Validating Test that the host is up and the IP correlates to the host name.

Prerequisites None.

Implicit Actions If the host was removed and now is being added (all in the same task), this action restores all the host's ports, port connectivity, volumes, and volume mapping/masking.

10.5.5 Add Hosts to Cluster



Description Adds one or more selected hosts to a cluster, and optionally defines a new cluster for this purpose.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the option you want:

Hosts — Name to identify the host(s) being added. Select one or more hosts from the list of available hosts.

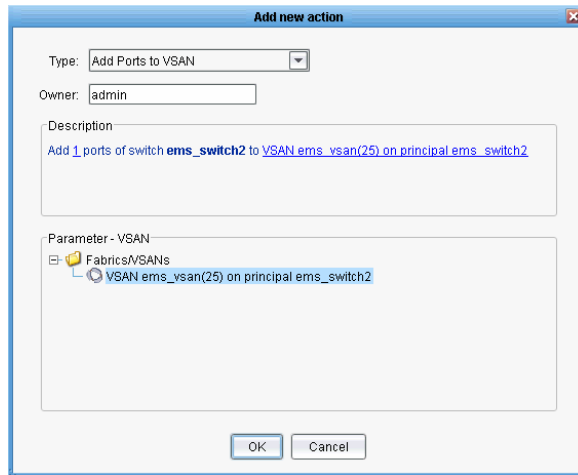
Cluster — Cluster to which the selected host(s) should belong. Choose an existing cluster from the drop-down list, or enter a cluster name to define a new cluster. Please note that any given host can only belong to, at most, one cluster.

Validating Test that the host is up and not already a member of another cluster. If the host is a member of another cluster, this action takes it out of that cluster before adding it to the new cluster.

Prerequisites The host(s) must already be defined to SANscreen.

Implicit Actions None.

10.5.6 Add Ports to VSAN



Description Adds one or more ports on a Cisco switch to a virtual SAN (VSAN).

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

of ports — Number of switch ports being added to the VSAN. Select one or more ports from the list of available switch ports.

Switch name — Name of the switch whose ports are being added (filled in automatically after you select a port(s), above).

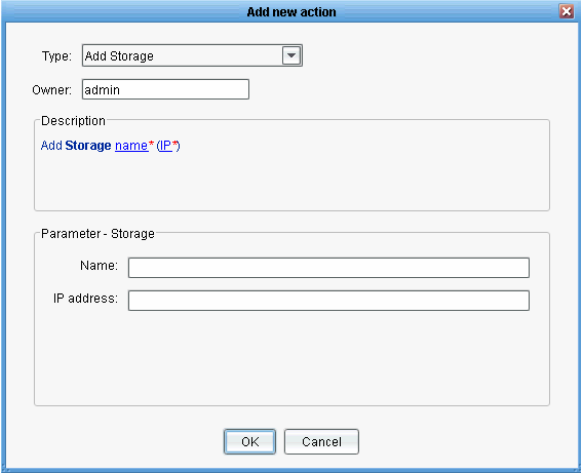
VSAN — VSAN to which you're adding the new ports. Select a VSAN from the list of fabric/VSANs.

Validating Verify by testing the VSAN configuration.

Prerequisites The VSAN and ports must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.7 Add Storage



The screenshot shows a dialog box titled "Add new action". It contains the following fields and controls:

- Type:** A dropdown menu with "Add Storage" selected.
- Owner:** A text input field containing "admin".
- Description:** A text area containing the text "Add Storage name * (IP *)". The words "Storage name" and "(IP *)" are underlined in blue.
- Parameter - Storage:** A section containing two text input fields:
 - Name:** An empty text input field.
 - IP address:** An empty text input field.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Description Adds a new disk storage device.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the option you want:

Storage name (IP) — Name and IP address to identify the storage device.

Validating Test that the storage is up and that the IP correlates to the storage name.

Prerequisites None.

Implicit Actions If the storage device was removed and now is being added (all in the same task), this action restores all the device's ports, port connectivity, volumes, and volume mapping/masking.

10.5.8 Add Switch

Add new action

Type: Add Switch

Owner: admin

Description:
Add g*-port Switch USCG_D1_SW4

Parameter - Switch

Name: USCG_D1_SW4

WWN: 10:00:00:60:69:51:4F:CD

VSAN Enabled: ☒

OK Cancel

Description Adds a new switch.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want.

If you plan to generate blade/ports (for switch cards), it's a good idea to identify the Switch parameter first, because this information is required for port generation.

of ports — Number of blades/ports on the switch. Click the appropriate tab — Blades to add switch cards, or Ports to identify the switch ports individually. Then:

- o For blades (i.e., switch cards), click Add once for each blade on the switch, then fill in the unique, numeric, blade for the blade, and the number of ports per blade:

Parameter - Ports

Blades Ports

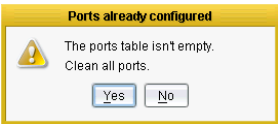
Blade number	Ports
12	15
13	15

Add Remove Generate

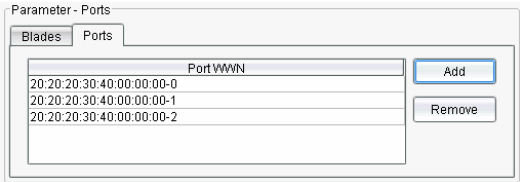
Click Generate to automatically add (generate) the ports for each blade. SANscreen calculates the ports based on the switch WWN and blade numbers, assigning each blade port a unique WWN.

(You'll have to enter the switch name and WWN before generating ports.)

As necessary, click Remove to delete a selected blade or port. If you get the message shown to the right, go to the Ports tab and Remove all the generated ports (use <CTRL-A> to select all ports), then return to the Blades tab and regenerate.



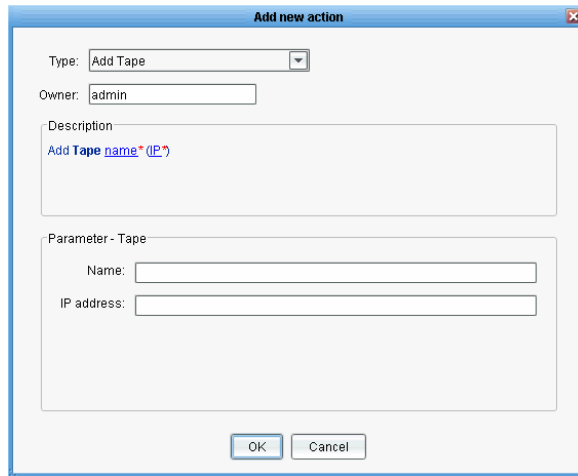
- o For ports, click Add once for each port on the switch, then fill in the WWN to identify each port. If you identified the switch already, SANscreen will pre-fill each port WWN with the WWN of the switch, followed by a dash and a port number:



- Switch** — Name and WWN to identify the switch being added, and an indication of whether the switch is VSAN-enabled. If enabled (checked), policy is determined by the VSAN, and you can add first switches (Add VSAN action) then switch ports (Add Ports to VSAN action).
- Policy** — Applicable only if the switch is not VSAN-enabled. Policy settings that apply for the switch (Domain ID, Priority, and so forth). Please refer to your switch documentation for detailed information about these settings.

Validating	Test that the switch is up and that all the policies match what was specified above.
Prerequisites	None.
Implicit Actions	None.

10.5.9 Add Tape



The screenshot shows a dialog box titled "Add new action". It contains the following fields and controls:

- Type:** A dropdown menu with "Add Tape" selected.
- Owner:** A text input field containing "admin".
- Description:** A text area containing the text "Add Tape name * (IP)".
- Parameter - Tape:** A section containing two text input fields:
 - Name:** An empty text input field.
 - IP address:** An empty text input field.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Description Adds a new tape device.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the option you want:

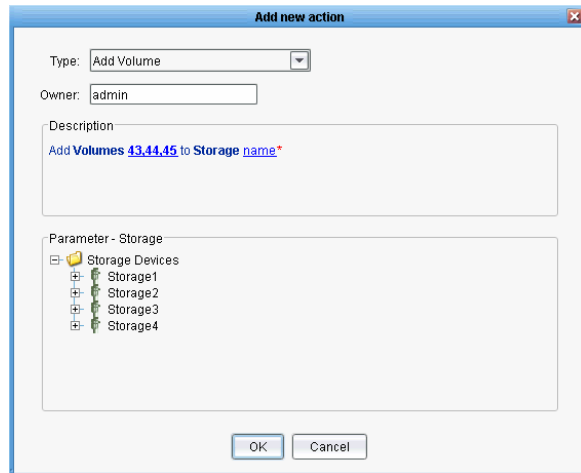
Tape name (IP) — Name and IP address to identify the tape device.

Validating Test that the tape is up and that the IP correlates to the tape name.

Prerequisites None.

Implicit Actions If the tape device was removed and now is being added (all in the same task), this action restores the device's previous connectivity.

10.5.10 Add Volume



Description Adds a new volume to a disk storage device.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Volumes — Volumes to be added. Click Add once for each volume, then specify the volume name. Click Remove to delete a selected volume.

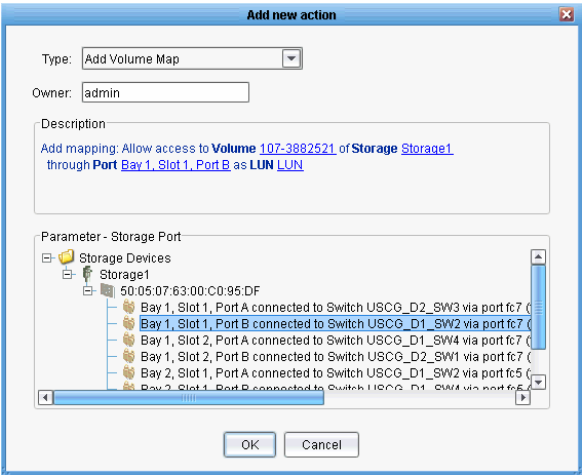
Storage name — Name of the storage device for which you're adding the volume(s). Select the device from the list of available devices.

Validating Test that the volume is up.

Prerequisites The storage device must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.11 Add Volume Map



Description Adds a mapping between a volume and a disk storage port.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Volume — Name of the volume for which you’re adding the mapping.
Select a volume from the list of available volumes. The drop-down list includes the status of each volume, as detailed on page 132. This helps to better understand if this is the right volume (i.e., whether this volume is masked and/or reserved by other tasks).

Storage name — Storage device where the volume is defined (filled in automatically after you select a volume, above).

Port — Port, on the storage device, to which the volume is mapped. Select a port from the list of available ports on the selected volume.

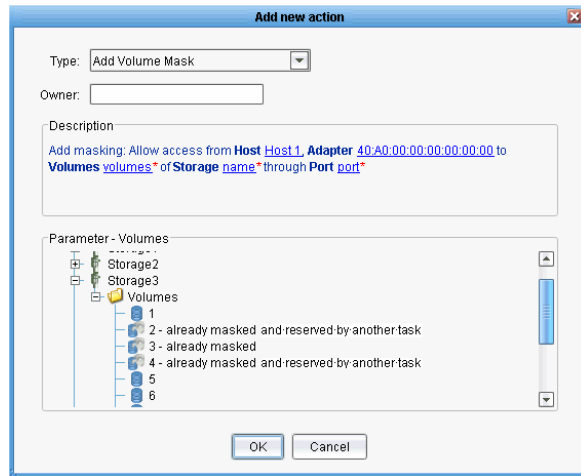
LUN — Logical Unit Number used by the host to access this volume.

Validating Test that the mapping is defined. Please note that the LUN number is not validated.

Prerequisites The volume must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that’s executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.12 Add Volume Mask



Description Adds a masking between a volume (disk storage port) and host.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Initiator (and WWN)— Host port or adapter to which the storage volume is masked. Select an **Adapter** or **Port** from the list of available adapters/ports. Both are identified by WWN in the list of available ports for each host. The host name is filled in automatically after you select an adapter/port.

Volume — Name of the volume to be masked to the host adapter or port identified above. The drop-down list includes the status of each volume, as detailed below, as well as an icon that's appropriate to that status: masked = , available = , etc. This helps to better understand if this is the right volume (i.e., whether this volume is masked and/or reserved by other tasks):

- o *no special text* (available volume) – The volume is not masked, either by the current SAN configuration, or by a planned action.
- o *Already Masked* – The volume is masked (i.e., in use by the current SAN configuration), as noted by the text that follows the status.
- o *Reserved ...* – The volume is masked by another action or task in the plan, as noted by the text that follows the status.

- o Already Masked and Reserved... – The volume is masked in the current SAN configuration, and the volume is reserved by at least one other action or task (as noted by the text that follows the status).

Storage name — Storage device where the volume is defined (filled in automatically after you select a volume, above).

Port — Name of the storage port (on the above named storage device) from which the volume is accessible to the host initiator.

Validating Check that the masking definition on the storage device matches this definition.

Prerequisites The volume must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.13 Add VSAN

The screenshot shows a Windows-style dialog box titled "Add new action". It contains the following elements:

- Type:** A dropdown menu currently showing "Add VSAN".
- Owner:** A text input field containing the text "admin".
- Description:** A text area containing the text "Add a VSAN ems_vsan(25) on principal ems_switch2 to Switches ems_switch2 with policy". The underlined portions are blue.
- Parameter - policy:** A section containing several fields:
 - Domain ID:** A text input field containing "0".
 - Priority:** A text input field containing "128".
 - Merge control:** A dropdown menu showing "PERMIT".
 - Default zone behavior:** A dropdown menu showing "PERMIT".
 - Domain ID type:** A dropdown menu.
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Description Allocates one or more VSAN-enabled switch devices to a new or existing VSAN.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

VSAN — Indication of whether the VSAN is new. Mark the New or Existing check box. If new, enter an ID between 1 and 4094, and a unique VSAN name. If existing, select the VSAN from the list of available VSANs.

Switches — Switch(es) that will be a part of this VSAN. Choose one or more switches from the list of available switches.

Policy — VSAN policy settings (Domain ID, Priority, Merge Control, and so forth). Please refer to your VSAN documentation for detailed information about these settings, as necessary. If you select more than one switch, this field is always “default policy.”

Validating Test that the VSAN is up.

Prerequisites All switch devices must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that’s executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions Creates the VSAN and/or fabric if it does not exist already.

10.5.14 Add Zone

The screenshot shows a window titled "Add new action". It has a "Type:" dropdown menu set to "Add Zone". Below it is an "Owner:" text field with "admin" entered. A "Description:" text area contains the text "Add Zone Host12 to fabric/VSAN*". Below the description is a section titled "Parameter - Fabric/VSAN" which is expanded to show a tree view. The tree view has a root node "Fabrics/VSANs" which is selected and expanded, showing three sub-items: "fabric 10:00:00:60:69:51:4E:6B on principal USCG_D2_SW1", "fabric 10:00:00:60:69:51:4E:EA on principal USCG_D1_SW4", and "fabric 20:D0:00:00:00:00:00:00 on principal Switch 1". At the bottom of the window are "OK" and "Cancel" buttons.

Description Adds a new zone to a fabric.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Zone name — Unique name to identify the zone.

Fabric/VSAN — Fabric/VSAN where you're adding the zone.

Validating Check this definition against the zoning configuration information received from the switch.

Prerequisites The fabric to which the zone is added must be defined in SANscreen as part of the SAN environment.

Implicit Actions If the zone was removed and now is being added (all in the same task), this action restores its members.

10.5.15 Add Zone Member (by Switch Port)

The screenshot shows a Windows-style dialog box titled "Add new action". It has a "Type:" dropdown menu set to "Add Zone Member (by switch port)". Below it is an "Owner:" text box with "admin" entered. A "Description:" text box contains the text "Add Port fc1 of Switch Switch 2 to Zone zone* of fabric/VSAN". Below the description is a "Parameter - Zone" section, which is expanded to show a tree view. The tree has a root node "Fabrics/VSANs" with a folder icon. Under it are several nodes: "fabric 10:00:00:60:69:51:4E:6B on principal USCG_D2_SW1", "fabric 10:00:00:60:69:51:4E:EA on principal USCG_D1_SW4", "USCG_Disk012403", "USCG_Tape012403", and "fabric 20:D0:00:00:00:00:00:00 on principal Switch 1". At the bottom of the dialog are "OK" and "Cancel" buttons.

Description Adds a particular switch port to a zone.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Port — Port to add to the zone. Select a port from the list of available switch ports.

Switch — Name of the switch whose port is being added (filled in automatically after you select a port, above).

Zone — Zone where you're adding the new member. Select a zone from the list of available zones.

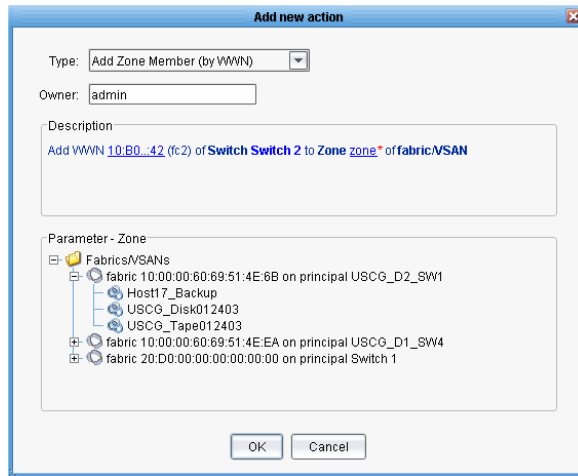
Fabric/VSAN — Name of the fabric/VSAN where the selected zone is configured (filled in automatically after you select a zone, above).

Validating Check this definition against the zoning configuration information received from the switch.

Prerequisites The fabric, zone, switch, and port must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.16 Add Zone Member (by WWN)



Description Adds a new zone member, identified by World Wide Name (WWN).

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

WWN — WWN to identify the member being added to the zone. Select a member from the list displayed host adapters and ports, switch ports, etc.

Device — Device type and name (filled in automatically after you select the zone member).

Zone — Zone where the new member will be added. Select a zone from the list of available zones

Fabric/VSAN — Name of the fabric/VSAN where the selected zone is configured (filled in automatically after you select a zone).

Validating Check this definition against the zoning configuration information received from the switch, to validate that this member was added to the zone.

Prerequisites The fabric, zone, and device must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.17 Authorize Path

The screenshot shows a window titled "Add new action" with a close button in the top right corner. Inside the window, there is a "Type:" dropdown menu set to "Authorize Path". Below it is an "Owner:" text field. A "Description:" section contains a blue hyperlink: "Authorize paths from Host Host2 to Storage Storage1(192.168.101.1) Volumes 107-4931097,107-5979673 having Policy None redundancy, Cluster volume sharing scope". Below the description is a "Parameter - Policy" section. It has a "Type:" label and a "Redundancy Level" dropdown menu set to "None". Underneath is an "Attributes" section with a "Volume Sharing Scope" dropdown menu set to "Cluster". There are two checkboxes: "Host port redundancy" and "Max switch hops", both of which are unchecked. To the right of each checkbox is a numeric input field with a value of "1" and up/down arrow buttons. At the bottom of the window are "OK" and "Cancel" buttons.

Description Authorizes and sets policy for one or more paths that connect a specific host server and its data residing on a storage device (disk volume or tape).

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Host — Name of the host from which the path(s) originate. Select a host from the list of available devices.

Storage name (IP) — Name of the storage device where the data for this path resides. For a disk device, select one or more volumes.

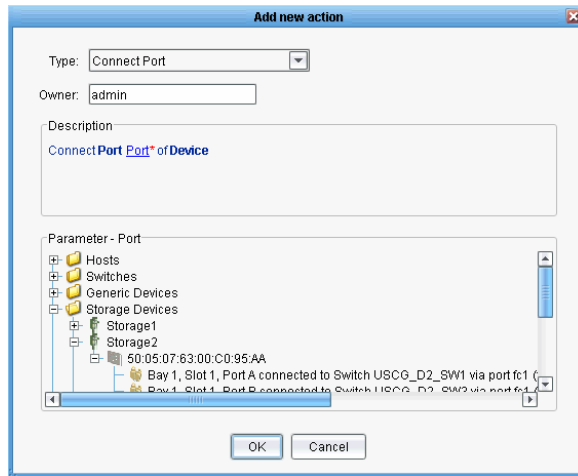
Policy — Policy attributes for the path(s). Please refer to step 4 on page 46 for information about these policy fields.

Validating Locate the exact authorized paths in SANscreen.

Prerequisites The host, storage devices, and volumes must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.18 Connect Port



Description Verifies that *some* device is connected to a particular device port.

This action is useful when there is a *plan* to connect a particular switch port to a port WWN, but that port WWN is currently unknown. With the action in place, you can track the State check-boxes (Ports detail pane) to see when the connection is actually made.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the option you want:

Port — Name of the port to check for a connection.

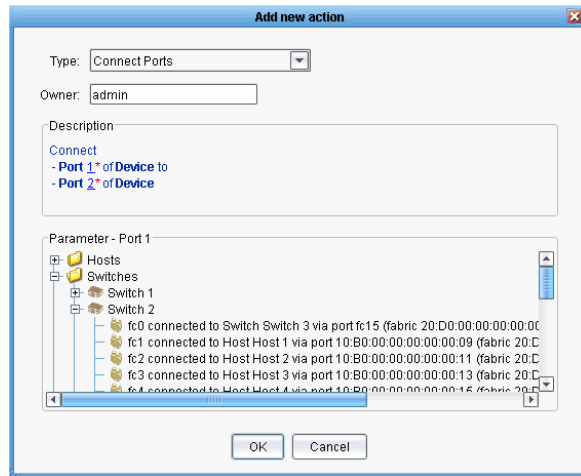
Device — Name of the device where the port is defined (filled in automatically after you select a port).

Validating Check that the port is connected to a device.

Prerequisites The device must be defined in SANscreen as part of the SAN environment.

Implicit Actions None.

10.5.19 Connect Ports



Description	Connects two ports.
--------------------	---------------------

Parameters Click each Port parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the option you want:

Port 1 and **Port 2** — Ports that you want to connect.

Device — Name of the device where each port is defined (filled in automatically after you select each port above).

Validating Verify that the two ports are connected.

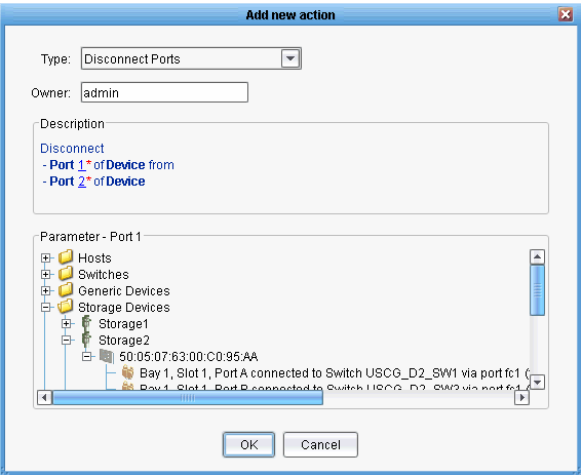
If the two ports are switch ports that belong to different fabrics, verify that the two fabrics can be merged.

Prerequisites Both ports must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Neither port can be connected to anything else.

Implicit Actions	If connecting two switch ports that do not belong to the same fabric (and for which the fabric cannot be merged), this action removes the fabric.
-------------------------	---

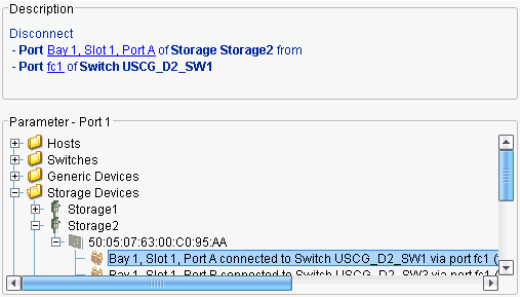
10.5.20 Disconnect Ports



Description Disconnects two ports.

Parameters Click either parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Port 1 and **Port 2** — Ports that you want to disconnect. The second (i.e., connected) port displays automatically after you select the first port:



Device — Name of the device where each port is defined (filled in automatically for both ports, after you select the first port above).

Validating Check that the exact path is deleted in SANscreen.

Prerequisites Both ports must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Both ports must be connected to each other.

***Implicit
Actions***

If disconnecting two switch ports that belong to the same fabric, this action creates a fabric and presents a single ISL (Inter-Switch Link) of the fabric.

10.5.21 Edit Authorized Path

The screenshot shows a window titled "Add new action". Inside, there's a "Type" dropdown menu currently showing "Edit Authorized Path". Below it is an "Owner" text box. A "Description" text area contains the text: "Update AP 1 APs from Host Host 2 to Storage Storage3 None redundancy No Sharing. volume sharing scope". Below the description is a "Parameter - Policy" section. It includes a "Type" dropdown, a "Redundancy level" dropdown set to "None", and an "Attributes" section. The "Attributes" section has a "Sharing" dropdown set to "No Sharing", and two checkboxes: "Min host ports" and "Max switch hops", both of which are checked and have a value of "1" next to them. At the bottom of the window are "OK" and "Cancel" buttons.

Description Edits an authorized path.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Update AP — Click *no paths selected* to view the table of currently authorized paths, then scroll through the list and select the path you want to edit.

None redundancy — Click to view the policy parameters that can be changed, then select the new policy attributes for the path:

Please refer to step 4 on page 46 for information about these policy fields.

Validating Verify that the policy was changed according to the policy attributes assigned above.

Prerequisites The authorized path must be defined in SANscreen.

**Implicit
Actions** None.

10.5.22 Enable Zone Configuration

The screenshot shows a dialog box titled "Add new action". It contains the following fields and sections:

- Type:** A dropdown menu with "Enable Zone Configuration" selected.
- Owner:** A text box containing "admin".
- Description:** A text box containing "Enable Zone Configuration".
- Parameter - Enable Zone Configuration:** A list box with a tree view. The root node is "Fabrics/VSANs". It has three child nodes, each with a plus icon and a radio button:
 - fabric 10:00:00:60:69:51:4E:6B on principal USCG_D2_SW1
 - fabric 10:00:00:60:69:51:4E:EA on principal USCG_D1_SW4
 - fabric 20:D0:00:00:00:00:00:00 on principal Switch 1
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Description

Enables zone configuration, whereby the task validation process uses a zone set for a particular fabric/VSAN that's defined within the management console, but that has not yet been activated. By using this action, the validation will take into account all underlying changes — including added/removed zones and zone members.

This action is useful to pre-validate zone-configuration changes that are entered from a switch management console (but not yet applied).

Parameters

Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the option you want:

Zone configuration — Fabric/VSAN from which to load the zone configuration information.

Validating

Check that the configuration was activated.

Prerequisites

The fabric must be defined in SANscreen.

Implicit Actions

The configuration is imported whenever the task is validated. Zoning actions occur according to the imported configuration. These actions are temporary and are available only to the validation process.

10.5.23 Remove Authorized Path

Add new action

Type: Remove Authorized Path

Owner: admin

Description: Remove no paths selected* authorized paths

Parameter - Authorized paths

Host	Storage	Volume
Host10	TAPE 2	null
Host16	Storage2	108-0173894
Host16	Storage2	135-2803654
Host16	Storage2	108-2271046
Host16	Storage2	135-1755078
Host16	Storage2	108-3319622
Host16	Storage2	108-5416774
Host16	Storage2	107-7028166
Host16	Storage2	107-6386600

OK Cancel

Description Removes an authorized path.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the option you want:

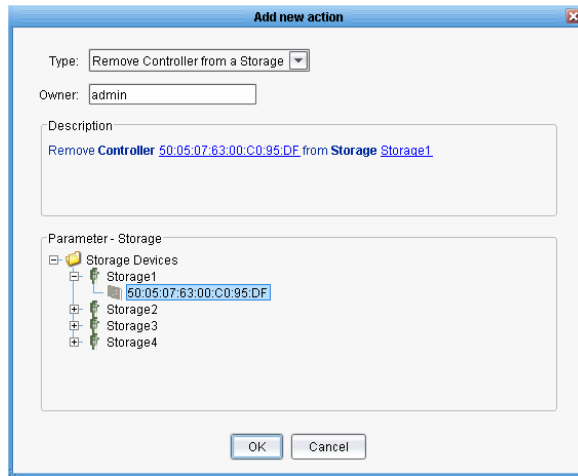
Remove — Click *no paths selected* to view the table of currently authorized paths, then scroll through the list and select the path for which to remove the authorization.

Validating Check that the path is removed from the Authorized Paths table.

Prerequisites The path must currently be authorized within SANscreen.

Implicit Actions None.

10.5.24 Remove Controller from a Storage



Description Removes a port controller from a disk storage device.

Parameters Click the Controller parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Controller — WWN of the controller you want to remove.

Storage name — Corresponding storage name (filled in automatically after you select a controller, above).

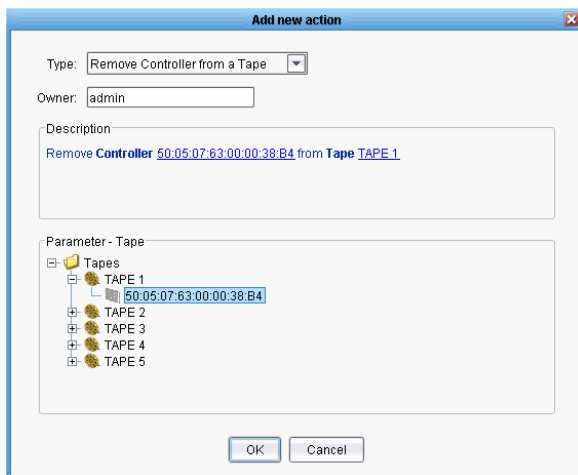
Validating Check that the controller is removed.

Prerequisites The controller must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions The ports are disconnected.

The controller's nodes and ports of the are removed, and the corresponding volumes and volume mapping/masking are removed from the storage device.

10.5.25 Remove Controller from a Tape



Description Removes a controller from a tape device.

Parameters Click the Controller parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Controller — WWN of the controller you want to remove.

Tape name — Corresponding tape name (filled in automatically after you select the controller, above).

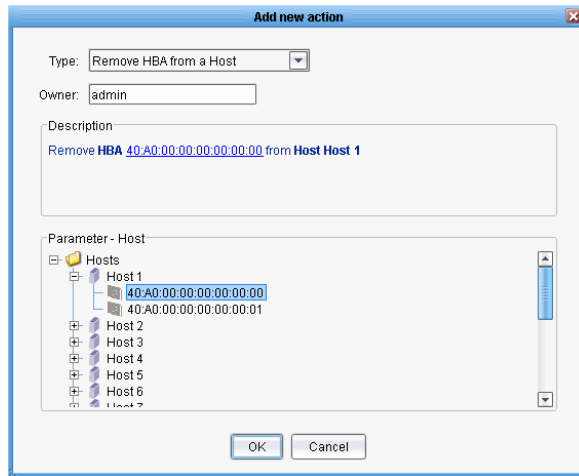
Validating Check that the controller is removed.

Prerequisites The controller must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit The ports are disconnected.

Actions The controller's nodes and ports are removed.

10.5.26 Remove HBA from a Host



Description Removes an HBA from a host.

Parameters Click the HBA parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

HBA — WWN of the HBA adapter to remove.

Host — Corresponding host name (filled in automatically after you select the HBA, above).

Validating Check that the HBA is removed.

Prerequisites The HBA must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions The ports are disconnected.

The HBA's nodes and ports are removed.

10.5.27 Remove Ports from VSAN

The screenshot shows a dialog box titled "Add new action". It contains the following fields and sections:

- Type:** A dropdown menu with "Remove Ports from VSAN" selected.
- Owner:** An empty text input field.
- Description:** A text area containing the text "Remove 0 ports of switch **switch-name** from **VSAN**".
- Parameter - Ports:** A section with a tree view showing a folder icon and the text "Switches".
- Buttons:** "OK" and "Cancel" buttons at the bottom right.

Description Removes one or more ports (on a specific switch) from a VSAN.

Parameters Click the ports parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Remove ports — Port(s) to be removed from the VSAN. Select one or more ports from the list of available switch ports.

Switch name — Name of the switch whose ports are being removed (filled in automatically after you select a port(s), above).

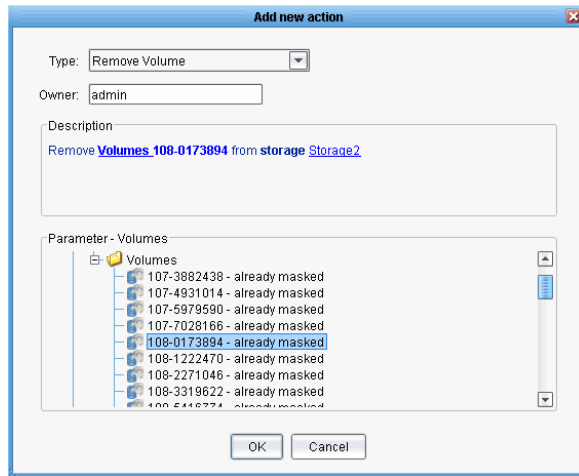
VSAN — VSAN from which you're removing the ports (filled in automatically after you select a port(s), above).

Validating Verify that the port is no longer in the VSAN.

Prerequisites The ports and VSAN must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions The VSAN is removed if all ports are removed from the VSAN.

10.5.28 Remove Volume



Description Removes one or more volumes from a disk storage device.

Parameters Click the Volumes parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Volumes — Volume(s) to be removed. Multiple volumes, if specified, must be defined on the same storage device. The drop-down list includes the status of each volume, as detailed on page 132.

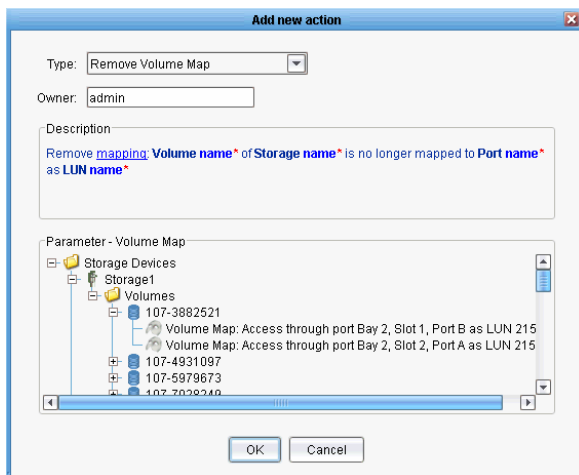
Storage — Name of the storage device where the volume(s) are defined (filled in automatically after you select the volume(s)).

Validating Check that the volume(s) are gone.

Prerequisites The volume(s) must exist on the storage device(s), either as defined to SANscreen part of the SAN environment, or as defined previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

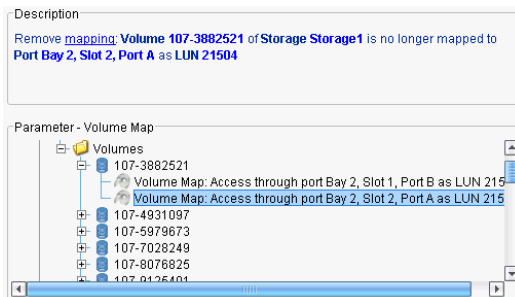
10.5.29 Remove Volume Map



Description Removes the mapping between a disk volume and a storage port.

Parameters Click the Mapping parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Mapping — Mapping to be removed. All other parameters display automatically after you select a mapping:



Volume name — Name of the volume whose mapping is being removed (filled in automatically after you select a mapping, above).

Storage name — Storage device where the volume is defined (filled in automatically after you select a mapping, above).

Port name — Port, on the storage device, for which the volume mapping will be removed (filled in automatically after you select a mapping, above).

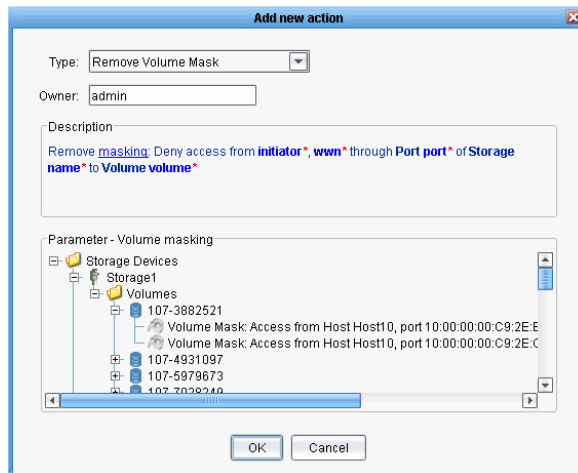
LUN name — Logical Unit Number used by the host to access this volume (filled in automatically after you select a mapping, above).

Validating Verify that the mapping configuration was removed from the storage device.

Prerequisites The volume mapping must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

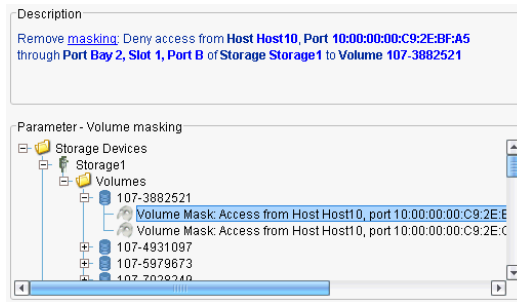
10.5.30 Remove Volume Mask



Description Removes the masking between a disk volume (storage port) and a host.

Parameters Click the Masking parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Masking — Volume mask to be removed. Select a mask from the list of available masks. All other fields display automatically after you select a mask:



Initiator — Host port for which the masking is being removed (filled in automatically after you select the mask, above).

Through port — Storage port for which the masking is being removed (filled in automatically after you select the mask, above).

Storage name — Storage device where the volume is defined (filled in automatically after you select the a mask, above).

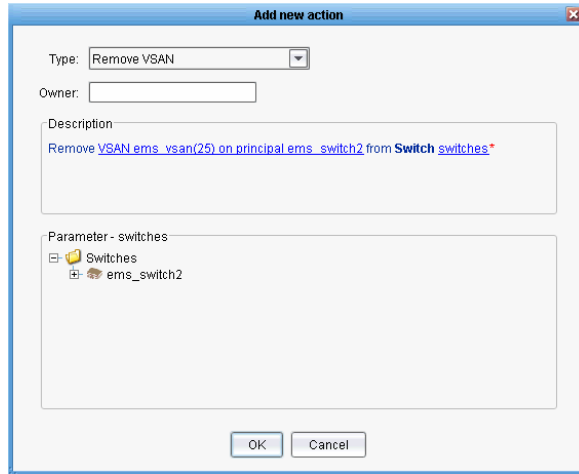
Volume — Name of the volume that's currently masked to the host port, and for which the masking is being removed (filled in automatically after you select the a mask, above).

Validating Verify that the masking configuration was removed from the storage device.

Prerequisites The volume masking must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.31 Remove VSAN



Description Removes a VSAN from one or more switch devices.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

VSAN — VSAN being removed. Select a VSAN from the list of available VSANs.

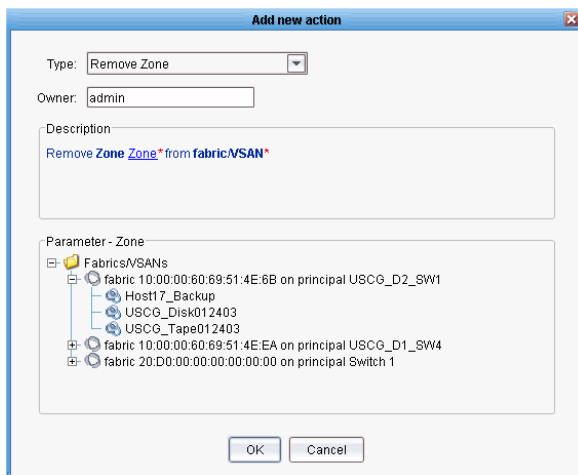
Switch — Switch(es) from which the VSAN is being removed. Chose one or more switches from the list of available switch devices.

Validating Verify that the VSAN was removed from the SAN.

Prerequisites The VSAN must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.32 Remove Zone



Description Removes a zone from a fabric.

Parameters Click the Zone parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Zone — Name of the zone being removed.

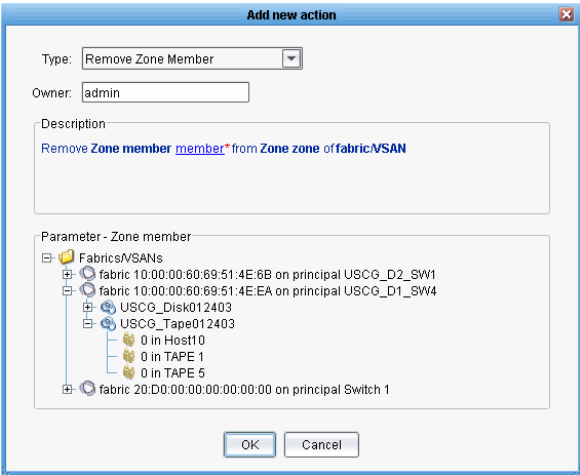
Fabric/VSAN — Fabric/VSAN where the zone is currently defined (filled in automatically after you select the zone).

Validating Check against the zoning configuration received from the switch.

Prerequisites The zone and fabric must be defined in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions All the members of the zone are removed.

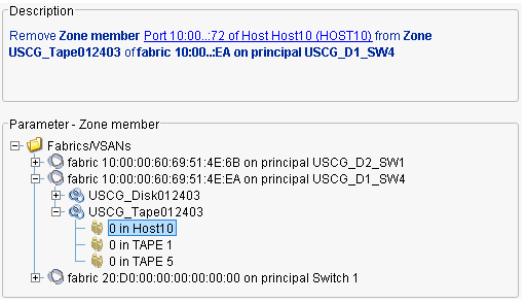
10.5.33 Remove Zone Member



Description Removes a member from a particular zone.

Parameters Click the Zone Member parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Zone member — Member to be removed from its zone. All other fields display automatically after you select a member:



Zone — Zone where the member is currently defined (filled in automatically after you select the member).

Fabric/VSAN — Fabric/VSAN where the zone is currently defined (filled in automatically after you select the member).

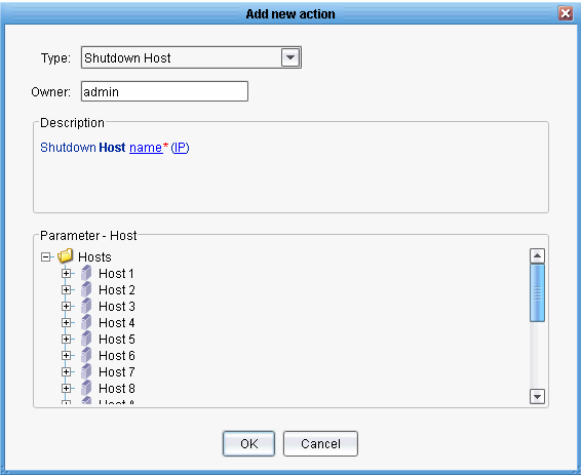
Validating Verify that the zone member was removed from the zoning configuration.

Prerequisites The member must be defined within the zone in SANscreen, either as part of the SAN environment, or previously in the current plan, or in a plan that's

executed before the current plan (i.e., a plan on which the current plan depends).

Implicit Actions None.

10.5.34 Shutdown Host



Description Shuts down a host.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

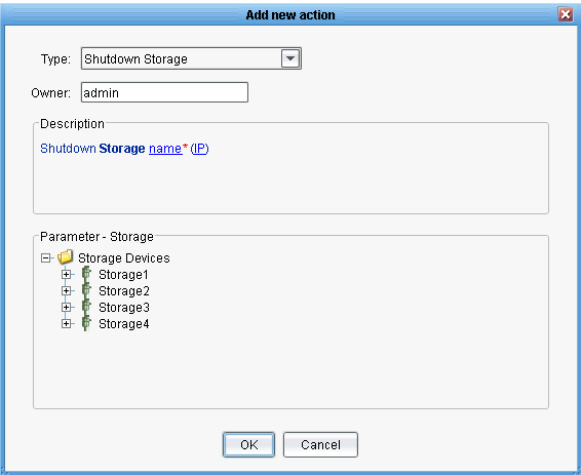
Host name (IP) — Host device to be shut down, identified by name and IP address. Select the device from the list of available hosts.

Validating None.

Prerequisites None.

Implicit Actions None.

10.5.35 Shutdown Storage



Description Shuts down a disk storage device.

Parameters Click each parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

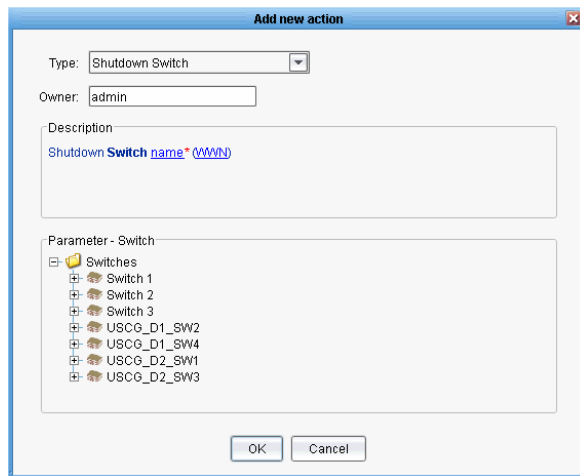
Storage name (IP) — Storage device to be shut down, identified by name and IP address. Select the device from the list of available disk storage devices.

Validating None.

Prerequisites None.

Implicit Actions None.

10.5.36 Shutdown Switch



The screenshot shows a dialog box titled "Add new action". It contains the following fields and sections:

- Type:** A dropdown menu with "Shutdown Switch" selected.
- Owner:** A text input field containing "admin".
- Description:** A text area containing the text "Shutdown Switch name* (WWN)".
- Parameter - Switch:** A section with a tree view showing a list of switches:
 - Switches
 - Switch 1
 - Switch 2
 - Switch 3
 - USCG_D1_SW2
 - USCG_D1_SW4
 - USCG_D2_SW1
 - USCG_D2_SW3

At the bottom of the dialog are "OK" and "Cancel" buttons.

Description Shuts down a switch.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

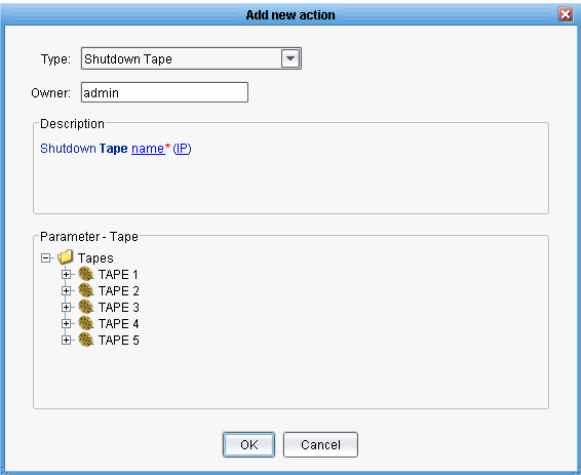
Switch name (WWN) — Switch to be shut down, identified by name and WWN. Select the switch from the list of available switch devices.

Validating None.

Prerequisites None.

Implicit Actions If the switch is between two other switch devices, and was the only channel between those two devices, shutting it down will create a new fabric.

10.5.37 Shutdown Tape



Description Shuts down a tape device.

Parameters Click the parameter (underlined in blue) to display the available selections in the Parameter area. Then proceed as described below to identify the options you want:

Tape name (IP)— Tape device to be shut down, identified by name and IP address. Select the device from the list of available devices.

Validating None.

Prerequisites None.

Implicit Actions None.

Chapter 11

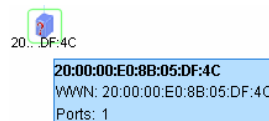
Identifying Generic Devices

When an HBA or HBA port is online and connected to a switch, that switch sometimes reports back to SANscreen about other ports that are on unknown devices. The unidentified ports, known as a *generic devices* until they are identified, might be host, storage, tape or a switch ports. Specifically, a generic device can be:

- An HBA with one or more ports.
- A storage controller or device with one or more ports.
- A switch device.
- A tape device.

Switch and storage devices are identified as soon as the correct Data Source is configured. Tapes ports have to be manually identified as tapes. Hosts represent the vast majority of generic devices, and can mostly — but not always — be identified automatically through the acquisition process. The ones that cannot be identified automatically show up as *generic devices*, and you can identify them manually.

When SANscreen detects an unidentified device, it creates a new generic device that's visible throughout SANscreen, including the various main views and an icon in the topology pane, as illustrated to the right (with pop-up information).



SANscreen also places an entry in the Identify screen for the generic device, as well as in the Generic Devices main table.

There are two ways to identify generic devices, as described in the rest of this chapter:

- Automatically, through host resolution (applicable for host devices/HBAs). This is described next, and involves setting up some configuration parameters that tell SANscreen how to resolve host names.

- Manually, from any of several screens that display generic devices. This is described stating on page 167.

In either case, you cannot identify (or un-identify) a device if it participates in an authorized path. You'll have to delete the authorized path first in this case, and rebuild it after re-identifying the device.

Once a Generic Device, Always a Generic Device

Once a generic device is discovered, it remains classified as a generic device even after it's identified, allowing you, for example, to change its identification as necessary.

Generic Devices and Violations

Generic devices may have access paths to volumes, and may be responsible for Violations.

11.1 Identifying HBA Devices via Host Resolution

If, by convention, your zone names typically include the device name (for example, zone AAA_host3_access, where the device name is host3), you can set up SANscreen so that it resolves generic host devices automatically, using either of two techniques:

- The **delimiter technique** comes up with a host name by pattern-matching the zone name(s) for the target device, then verifying that host name using DNS.
- The **RegExp technique** lets you specify regular expressions that detail how to determine the host name from the zone name(s).

Host resolution results in filling in the host name and IP address. Please refer to Appendix B (page 201) for the specific algorithms used for each technique.

Note: You can manually override any automatic host resolution.

Once you configure automatic host resolution, it occurs for all generic devices that are not yet identified, each time a:

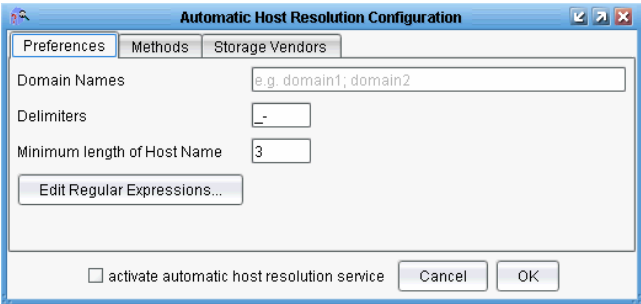
- New generic device is reported by the acquisition process.
- Zone is taken up or down.
- Member is added/removed to/from a zone.
- Host-resolution rule changes.

11.1.1 Configuring Host Resolution

Choose Configure Auto Resolution from the Identify main table’s Action menu to initiate host resolution processing.

Preferences Tab

SANscreen opens the host-resolution configuration window on the Preferences tab.

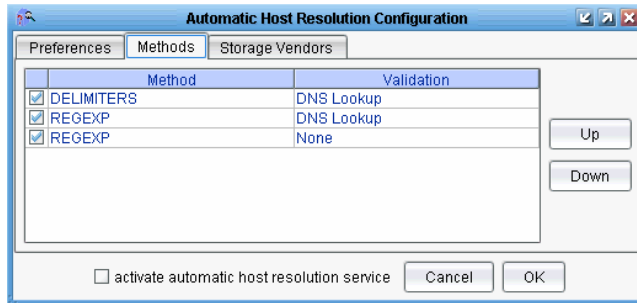


Use this tab to enter preferences related to host resolution. Please refer to Appendix B, *Host Resolution Algorithms*, for information about how SANscreen uses these parameters.

Field	Description
Domain Names	One or more domain names to be concatenated with each potential host name before performing a DNS lookup. Use commas to separate multiple names.
Delimiters	List of delimiter used to split the zone name(s) into tokens for each generic device (defaults to an underscore (_) and dash (-)).
Minimum Length of Host Name	Minimum number of characters required in a host name. SANscreen only performs DNS lookups for host names that are this long or longer.
Edit Regular Expression	Applicable only if using the RegExp technique. Click to open a window used to enter/modify the regular expressions used to extract a host name from zone name(s). Then proceed to <i>Section 11.1.2 Configuring Regular Expressions</i> for instructions.

Methods Tab

Click the Methods tab when you're through with the Preferences:

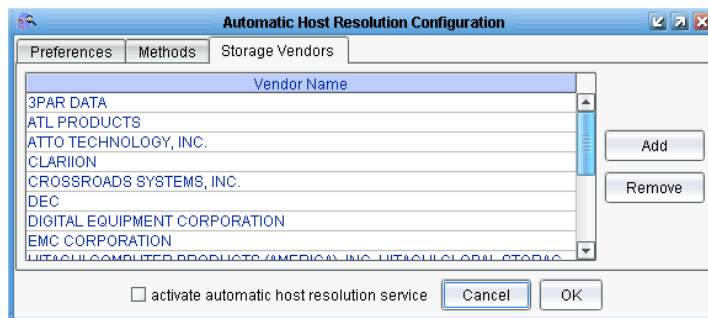


This tab lists each available resolution technique, and, for the RegExp technique, indicates whether you want to validate each resolved host name against DNS.

Mark each technique you want to use during host resolution, and make sure they are in the desired sequence. For each generic HBA device, SANscreen will try to resolve that device using the top-most technique that's marked (i.e., checked), then the next technique down, and finally the third technique from the top (if all are marked). Use the Up and Down buttons to move a technique up or down in the list, first selecting the technique you want to move, then clicking the appropriate button.

Storage Vendors Tab

Click the Storage Vendors tab when you're through with the Methods:



This tab provides a list of vendors for which SANscreen should assume their devices are storage devices (and therefore skip the device resolution). Each vendor is assigned a 3-byte identifier when they register with the IEEE, and

that 3-byte identifier is part of the WWN. SANscreen compares a device's WWN to this list to determine whether the device is a storage device.

To add a device to this list, first click Add to generate a blank line. Then enter the name of a storage vendor as it appears in the following IEEE Web site:

<http://standards.ieee.org/regauth/oui/oui.txt>

Finishing Up

When you are through:

- Mark Activate automatic host resolution service to activate the host-resolution feature.
- Click OK to save the configuration settings and close the window.

11.1.2 Configuring Regular Expressions

When you click the Edit Regular Expressions button from the Automatic Host Resolution Configuration window, SANscreen opens this window:

The screenshot shows the 'Automatic Host Resolution Regexp Wizard' dialog box. It has a title bar with 'Automatic Host Resolution Regexp Wizard' and standard window controls. The main area is titled 'Regular Expressions' and contains a table with three columns: 'Regexp', 'Format', and 'Matches'. To the right of the table are buttons for 'Add', 'Remove', 'Up', and 'Down'. Below the table is a 'Preview' button and a checkbox for 'DNS validation'. The 'Preview' section is titled 'Preview' and contains a table with two columns: 'Host' and 'Zone Names'. Below this is a section titled 'No Match' with a table with two columns: 'WWN' and 'Zone Names'. At the bottom are 'Cancel' and 'OK' buttons.

Use the upper area to specify the rules (i.e., regular expression(s)) used to extract a host name for a generic device, filling in the fields as described below. The host name is determined from the names of all zones that the

generic devices is a member of, as detailed in Appendix B, *Host Resolution Algorithms*.

Make sure to sequence the expressions in order as you want to use them to extract the host name. Use the Up and Down buttons to the right to move an expression up or down in the list, first selecting then expression you want to move, then clicking the appropriate button.

Click OK when you're through, to save the settings and close the window (and return to the host-resolution configuration window). Click Cancel to abort the operation and discard any changes made. In either case, SANscreen returns a message telling you what it's going to do:

About to update configuration, and run resolution.
or
All changes will be discarded

Field	Description
RegExp	Regular expression used to extract the host name. Notice the last (gray) line, which specifies an empty format (.*). This matches any host devices that do not match the other regular expressions, allowing you to see which devices these are (i.e., which host devices you still have to identify).
Format	Replacement string used to format the string extracted using the expression (above), to create a potential host name. Includes an optional prefix and/or suffix.
Matches	Display only. Number of matches.
Preview	Click to preview (in the Preview pane) use of the regular expression rule(s) to extract a host name. This happens automatically after you edit a rule, delete a rule, or change the order of the rules. Use this button to preview use of the expression(s) at any other time. The lower part of the window (Preview) shows the results of the simulation.
DNS Validation	Mark this checkbox to validate each potential host name against DNS.

Finishing Up

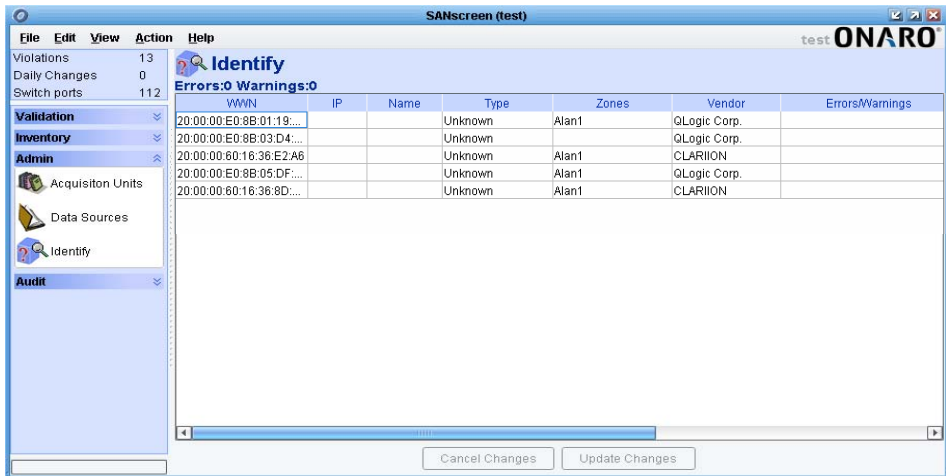
When you are through, Click OK to save the configuration settings and close the window.

11.2 Identifying Devices Manually

You can identify generic devices manually, from the Identify screen, the Topology screen, or the Generic Devices list. The processing is essentially the same regardless of the screen from which you initiate processing.

11.2.1 Identifying Devices Using the Identify Screen

To view generic devices in your SAN, click the Identify icon  from the navigation tree (Admin category):



The Identify main table contains a list of:

- Detected device ports that require identification, and
- Ports that were manually identified via the Add New Device option (see page 169).

Such ports include host HBA ports, and possibly tape ports. The following fields displays for each port:

Field	Description										
WWN	World Wide Name assigned to the generic device.										
IP	IP address assigned to the generic device.										
Name	Name of the host, storage device, tape, or switch for the generic device.										
Type	Type of device: Host, Storage (disk), Tape, or Unknown.										
Zones	Name of the zone(s) to which this port belongs, to help with the identification.										
Vendor	Name of the vendor who sells the generic device (i.e., port card), based on standard industry WWN allocation ranges.										
Errors/Warnings	Any errors/warnings that apply for the generic device, such as the same WWN identified twice in the list, or missing information.										
Resolution	Current state of resolution for the device: <table> <tr> <th>Value</th><th>Description</th></tr> <tr> <td>None</td><td>Not resolved.</td></tr> <tr> <td>Manual</td><td>Manually resolved.</td></tr> <tr> <td>Delimiter technique.</td><td>Resolved using the <i>delimiter</i></td></tr> <tr> <td>RegExp (abc.*)</td><td>Resolved using the <i>regular expression</i> technique. The actual regular expression is enclosed in parentheses.</td></tr> </table>	Value	Description	None	Not resolved.	Manual	Manually resolved.	Delimiter technique.	Resolved using the <i>delimiter</i>	RegExp (abc.*)	Resolved using the <i>regular expression</i> technique. The actual regular expression is enclosed in parentheses.
Value	Description										
None	Not resolved.										
Manual	Manually resolved.										
Delimiter technique.	Resolved using the <i>delimiter</i>										
RegExp (abc.*)	Resolved using the <i>regular expression</i> technique. The actual regular expression is enclosed in parentheses.										
Validation	Validation method used during the resolution of the generic device: None or DNS lookup. This is configured with the automatic resolution techniques in effect, as described starting on page 165.										

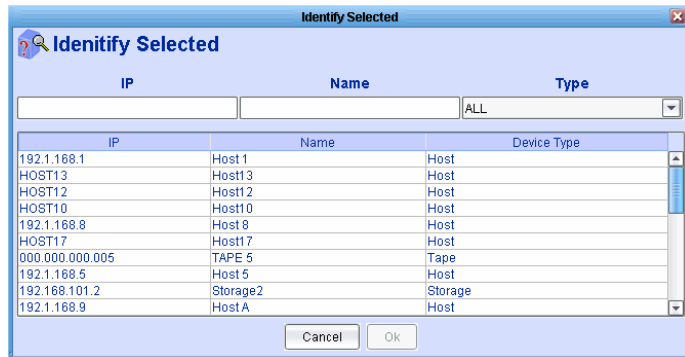
Use the Identify Action or right-click menu, as described next, to identify devices — and for related processing. When you're through, click Update Changes at the bottom of the Identify display to commit the changes to the SANscreen database.

Identify Action Menu

You can perform the following actions using the Action or right click menu from the list of generic devices.

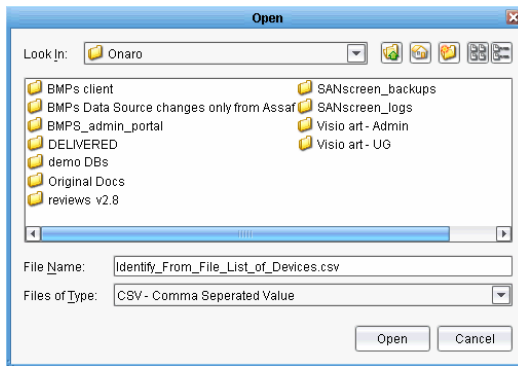
Action	Help
<u>A</u> dd new device	
<u>D</u> elete identification	
<u>C</u> ancel Selected	
<u>I</u> dentify Selected	
<u>I</u> dentify from file	
<u>C</u> onfigure auto resolution	
<u>S</u> uggest Resolution	

- **Add New Device** — Add a port that has not been discovered yet by SANscreen, but is planned for the near future. Pre-defining a device ensures that once SANscreen discovers the device, it will be identified correctly. After you choose this option, SANscreen adds a row to the main table. Click each field (WWN, IP, etc.) and fill in the information.
- **Delete Identification** — Clears any previous device identification from the selected row(s).
- **Cancel Selected** —
- **Identify Selected** — Lets you identify the devices in one or more selected rows. If more than one port belongs to the same device, select all the ports (generic devices), then click this option and proceed as described below.



- o For new devices, enter the IP, Name, and Device Type to identify the host, storage device, tape, or switch for the generic device, then click OK.
- o If the generic device (port) is on a device that's known to SANscreen, use the list at the bottom to select the parent device. As necessary, fill in the fields at the top to filter the list according to your specifications (by device type, for example). Click OK when you're through.

- **Identify From File** — Use the dialog that opens to identify a CSV-formatted file that contains a pre-defined list of ports and their device names:



Format each line of the file as shown below:

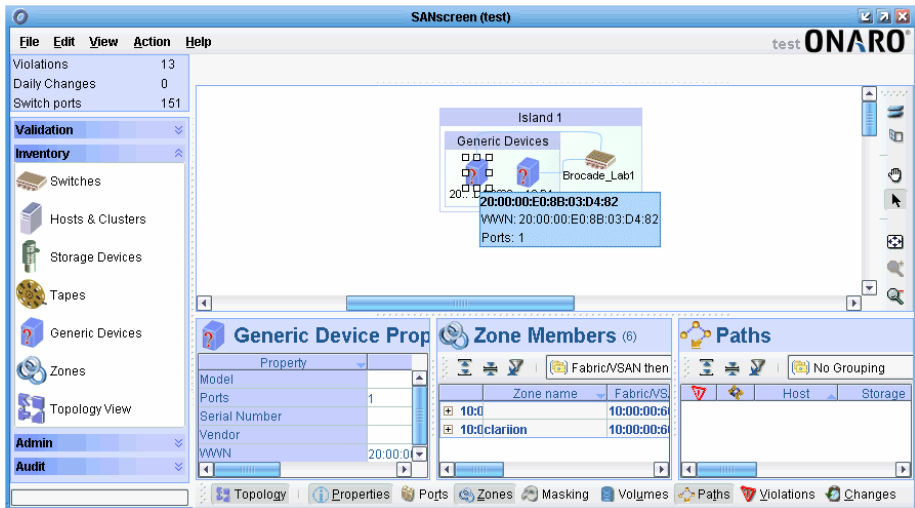
WWN,IP,Name,Type

For example: 11:22:33:44:55:66:77:88,123.23.34.45,myserver,Host

- **Configure Auto Resolution** — Initiate host resolution processing, as described starting on page 163.
- **Suggest Resolution** — Runs a host-resolution check for all selected generic devices (see page 162).

11.2.2 Identifying Generic Devices From the Topology Pane

Generic devices are represented by the  icon in the Topology view. Hover over the generic device icon with the cursor to reveal its pop-up information:



To identify generic devices from this view, first click on the icon. This lets you view information about the device in the detail panes. The amount of information obtained during acquisition varies by manufacturer and model, so the information available in the detail panes will vary correspondingly.

Use the right-click or Action menu (Device → Identify Generic Device), to open the Identify Selected wizard, then follow the instructions on page 169 to identify the device.

11.2.3 Identifying Generic Devices From the Generic Device List

As an alternative to the processing above, you can identify generic devices from the Generic Device list (under the Inventory category). Please refer to page 182 for detailed information about this list.

Click on the device you want in the inventory list, to view information about the device in the detail panes. The amount of information obtained during acquisition varies by manufacturer and model, so the information available in the detail panes will vary correspondingly.

From the Generic Device inventory list, select Identify a Generic Device from the right-click or Action menu. This opens the Identify Selected wizard. Follow the instructions on page 169 to identify the device.

Chapter 12

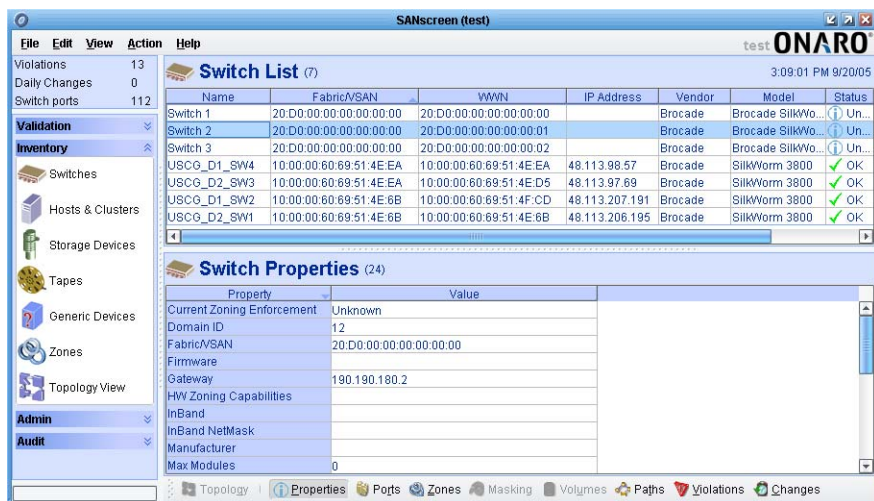
Viewing Inventory Data

The second section of the shortcut icons and navigation tree contains an Inventory of the devices in your SAN, organized by device type. Click on each icon to view information about the corresponding device type, then refer to the appropriate section below for further details:

- **Switches** — see page 173.
- **Hosts & Clusters** — see page 176.
- **Storage Devices** — see page 177.
- **Tape** — see page 181.
- **Generic Devices** — see page 182.
- **Zones** — see page 184.
- **Topology** — see page 186.

12.1 Switches

The Switch List  displays the switches that SANscreen detects in your SAN. The main table reflects the data configured in the switch itself, based on the manufacturer's configuration procedures. The number following the table heading (in parentheses) is the total number of switches:



The following information displays in the main table for each switch, assuming the information is available from the switch itself:

Field	Description
Name	Name to identify the switch.
WWN	World Wide Name assigned to the switch.
IP Address	IP address assigned to the switch.
Vendor	Name of the vendor who sells the switch.
Model	Manufacturer's model number.
Fabric/VSAN	Fabric/VSAN on which this switch is configured to operate.
Status	Current status of the switch (taken from the device itself). Please refer to the device documentation for an explanation of values.
Number of Ports	Number of ports defined on the switch.

Additional information is available from the detail tabs, at the bottom of the screen. Click on any row in the main table to view detailed information about the corresponding switch in the lower pane. Please refer to page 12 for information about these detail panes. This section only describes the Switch Properties display, which is unique to the Switch List.

12.1.1 Switch Properties Detail Tab

Click the Properties tab to display detailed information about the selected switch, as follows. Please refer to page 174 for an example of this display.

Field	Description								
Current Zoning Enforcement	Current zoning enforcement code, taken from the switch.								
Domain ID	Fabric Domain ID for the switch.								
Fabric/VSAN	Fabric/VSAN on which the switch is configured to operate.								
Firmware	Version of firmware running on the switch.								
Gateway	Switch's out-of-band IP gateway address.								
HW Zoning Capabilities	Zoning support provided by the switch's hardware.								
InBand	In-band IP address used for IP over FC.								
InBand NetMask	In-band IP network mask used for IP over FC.								
Manufacturer	Name of the manufacturer for the switch.								
Max Modules	Maximum number port modules on the switch.								
Model	Model number for the switch.								
Name	Switch name, as provided by the SAN manager at the switch console.								
OutBand	Out-of-band IP address used for switch management.								
OutBand NetMask	Out-of-band IP network mask used for switch management.								
Ports	Number of physical ports on the switch.								
Role	Switch fibre-channel role — Subordinate or Principal.								
SW Zoning Capabilities	Zoning support provided by the switch's software.								
State	Current state of the switch: <table><tr><th>State</th><th>Description</th></tr><tr><td>Online</td><td>Up and running.</td></tr><tr><td>Offline</td><td>Shut down.</td></tr><tr><td>Testing</td><td></td></tr></table>	State	Description	Online	Up and running.	Offline	Shut down.	Testing	
State	Description								
Online	Up and running.								
Offline	Shut down.								
Testing									

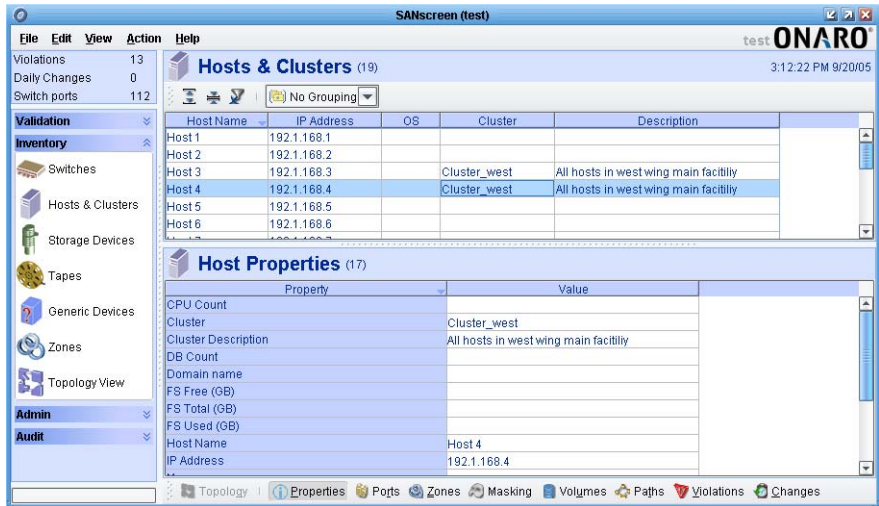
Field	Description
	Cold Reboot Booting from shutdown. Warm Reboot Restarting. Functional Unknown State cannot be determined.
Status	Current status of the switch (taken from the device itself). Please refer to the device documentation for an explanation of values.
Switch ID	Manufacturer's switch identifier.
Time Zone	Time zone the switch is configured to use.
Vendor	Name of the vendor who sells the switch.
WWN	WWN for the switch.
ZoningInstalled	Switch zoning support (for licensing purposes).

12.2 Hosts & Clusters

The Hosts & Clusters list  displays the hosts that SANscreen detects in your SAN, and any clusters that are in use and defined to SANscreen. A cluster is a group of host servers, usually dedicated for the same application, for purposes of redundancy and performance:

- Redundancy — A failure of one server will not cause the application to fail over to another server in the cluster.
- Performance — Several servers running together increase the speed and performance of the application.

You can view the table by OS, cluster name, or host name (No Grouping, illustrated below). The number following the table heading (in parentheses) is the total number of host devices in the SAN:



The following information displays in the main table for each host, assuming the information is available from the host device:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of hosts reported in each row.
Host Name	Name to identify the host.
IP Address	IP address assigned to the host device.
OS	Operating system running on the host.
Cluster	Name of the cluster (applicable if the host is a member of a cluster).
Description	Description of the cluster (applicable if the host is a member of a cluster).

Additional information is available from the detail tabs, at the bottom of the screen. Click on any row in the main table to view detailed information about the corresponding host in the lower pane. Please refer to page 12 for information about these detail panes. This section describes the Host Properties display, which is unique to the Hosts & Clusters list, then it describes clustering operations, and how to view the history for a host (including clustering changes).

12.2.1 Host Properties Detail Tab

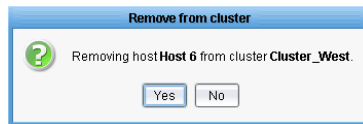
Click the Properties tab to display detailed information about the selected host, as follows. Please refer to page 177 for an example of this display.

Field	Description
Alias	Alias for the host, if any.
CPU Count	Number of CPUs running on the host.
Cluster	Cluster in which the host participates (blank if the host is not a member of a cluster).
Cluster Description	Description of the cluster (blank if the host is not a member of a cluster).
DB Count	Number of databases for the host.
Domain Name	Host DNS name.
FS Free (GB)	Amount of free storage in the host file systems, in gigabytes.
FS Total (GB)	Total amount of storage in the host file systems, in gigabytes.
FS Used (GB)	Amount of storage in the host file systems that's used, in gigabytes.
IP Address	IP address assigned to the host.
Memory	Total amount of memory available on the host.
Model	Manufacturer's model number.
Host Name	Name to identify the host.
OS	Operating system running on the host.
OS Class	Operating system class.
OS Level	Operating system level.
OS Release	Release of the operating system running on the host.
Vendor	Name of the vendor who sells the host device.

12.2.2 Adding Hosts to a Cluster and Related Processing

Use the Action menu to perform cluster operations, as follows. Please refer to *Section 7.1 Defining Clusters*, starting on page 73, for details about how to define a cluster.

- **Add to Cluster** — Adds one or more selected host(s) to a cluster.
- **Auto Clustering** — Creates a cluster by extracting the cluster name from one or more selected hosts.
- **Remove From Cluster** — Removes one or more selected hosts from a cluster. SANscreen verifies the request before finalizing it:

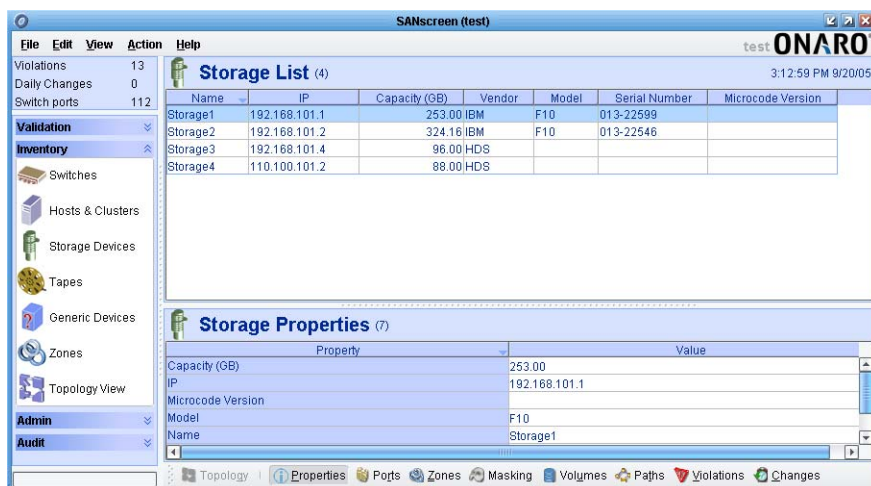


12.2.3 Viewing History

Use the History detail tab to view the history for a selected host, including clustering changes:

12.3 Storage Devices

The Storage List  displays the disk storage devices SANscreen detects in your SAN. The number following the table heading (in parentheses) is the total number of disk storage devices:



The following information displays in the main table for each device, assuming the information is available from the device itself:

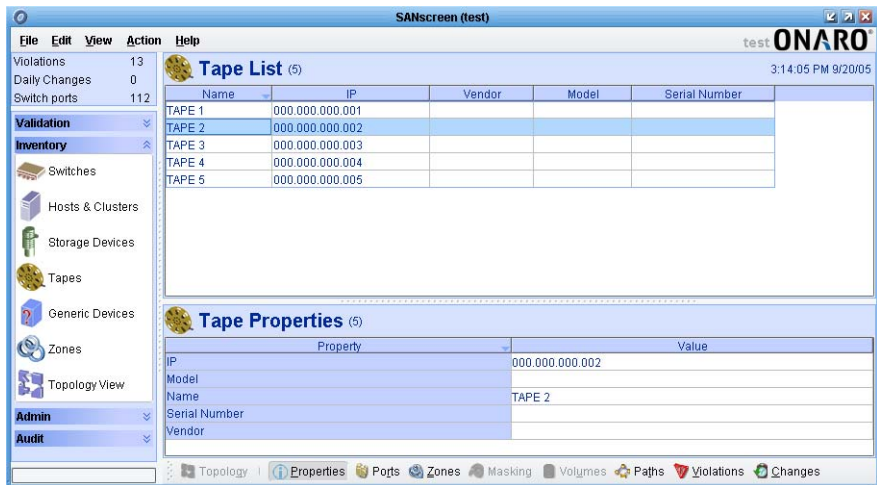
Field	Description
Name	Name to identify the storage device.
IP	IP address assigned to the storage device.
Vendor	Name of the vendor who sells the storage device.
Model	Manufacturer's model number.
Serial Number	Serial number for the storage device.
Microcode Version	Version of firmware running on the storage device.

Additional information is available from the detail tabs, at the bottom of the screen. Click on any row in the main table to view detailed information about the corresponding storage device in the lower pane. Please refer to page 12 for information about these detail panes.

The Storage Properties detail pane contains the same information as the main table, presented in alphabetical order.

12.4 Tapes

The Tape List  displays the tape devices SANscreen detects in your SAN. The number following the table heading (in parentheses) is the total number of tape devices:



The following information displays in the main table for each tape device, assuming the information is available from the device itself:

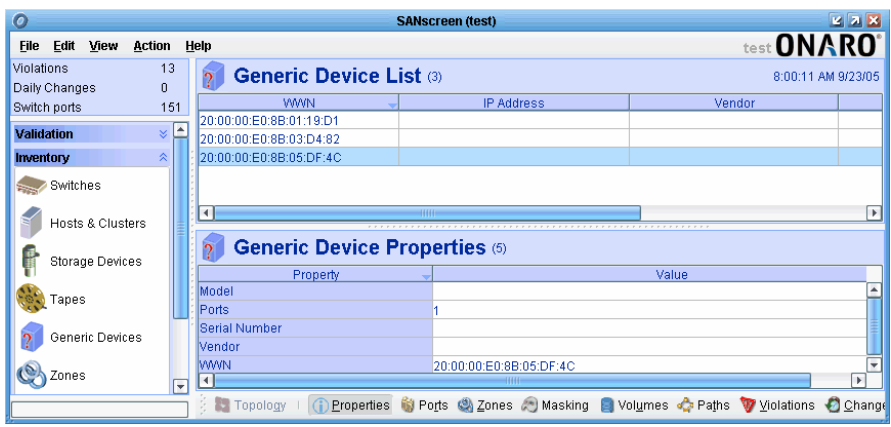
Field	Description
Name	Name used to identify the tape device.
IP	IP address assigned to the tape device.
Vendor	Name of the vendor who sells the tape device.
Model	Manufacturer's model number.
Serial Number	Serial number for the tape device.

Additional information is available from the detail tabs, at the bottom of the screen. Click on any row in the main table to view detailed information about the corresponding tape device in the lower pane. Please refer to page 12 for information about these detail panes.

The Tape Properties detail pane contains the same information as the main table, presented in alphabetical order. .

12.5 Generic Devices

The Generic Device List  displays any unidentified device ports that SANscreen detects in your SAN. Such generic devices include host HBA ports, storage ports, storage controller ports, and switch ports. The number following the table heading (in parentheses) is the total number of generic devices:



The following information displays in the main table for each generic device, assuming the information is available from the device itself (and was reported by the Data Source that discovered the generic device) — or was provided during device identification:

Field	Description
WWN	World Wide Name assigned to the generic device.
IP Address	IP address assigned to the generic device.
Vendor	Name of the vendor who sells the generic device (i.e., port card), based on standard industry WWN allocation ranges.
Model	Manufacturer’s model number.
Ports	Number of physical ports on the generic device.

Additional information is available from the detail tabs, at the bottom of the screen. Click on any row in the main table to view detailed information

about the corresponding generic device in the lower pane. Please refer to page 12 for information about these detail panes. This section describes the Generic Device Properties display, which is unique to the Generic Device List; then it points to instructions that tell how to identify a generic device to SANscreen.

12.5.1 Generic Device Properties Detail Tab

Click the Properties tab to display detailed information about the selected generic device, as follows. Refer to page 182 for an example of this display. Remember that SANscreen can only report the information that's available from the generic device itself, and was reported by the Data Source that discovered the device.

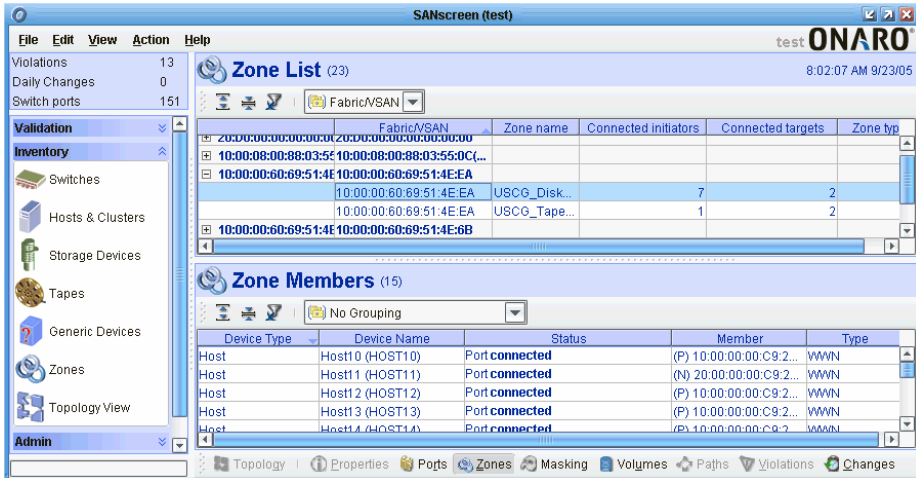
Field	Description
Model	Same as in the main table.
Ports	Same as in the main table.
Serial Number	Serial number to identify the generic device.
Vendor	Same as in the main table.
WWN	Same as in the main table.

12.5.2 Identifying a Generic Device

Please refer to Chapter 11 for general information about generic devices and how to identify them. To identify a generic device from the Generic Device List, choose Identify a Generic Device from the Action or right-click menu. This opens open the wizard described in *Section Identify Action Menu*, under Identify Selected. Follow the instructions on page 169 to identify the device.

12.6 Zones

The Zone List  displays the zones within each fabric in your SAN. The number following the table heading (in parentheses) is the total number of zones in your SAN:



The following information displays in the main table for each zone:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping (i.e., with Fabric/VSAN grouping). Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of zone configurations reported in each row.
Fabric/VSAN	Fabric/VSAN in which the zone is configured.
Zone Name	Name of the zone.
Connected Initiators	Number of host ports configured as <i>initiators</i> in the zone.
Connected Targets	Number of target storage (disk and tape) devices configured in this zone.
Zone Type	Type of zoning in effect: Zone Type Description <i>blank</i>

Field	Description
	Standard port zoning QuickLoop definition zone Fabric assist definition zone FC4 specified traffic only Illegal type

Additional information is available from the detail tabs, at the bottom of the screen. Click on any row in the main table to view detailed information about the corresponding zone in the lower pane. Please refer to page 12 for information about these detail panes. This section only describes the Zone Members display, which is unique to the Zone List.

12.6.1 Zone Members Detail Tab

Click the Zones tab to determine the members (devices) in the zone that's selected in the main table (illustrated on page 184). The following detailed information displays for each member:

Field	Description
<i>blank</i>	Applicable with any presentation order () other than No Grouping. Column that organizes the data according to the selected grouping format. The number in parentheses indicates the number of zone members reported in each row.
Device Type	Type of this device described on the line (i.e., that's a member of this zone): Host, Storage, Tape, or Generic Device.
Device Name	Name of the device.
Status	Status of the device (taken from the device itself). Please refer to the device documentation for an explanation of values.
Member	Zone member information, as is provided to the Switch or Fabric (WWN) zoning mechanism. The format of this field is detailed on page 15.
Type	Type of zoning used: WWN (for WWN-based) or Switch Port (switch-port-based).

12.7 Topology View

For information on the topology view, please refer to *Chapter 3 Establishing Topology Layouts*, beginning on page 25.

Chapter 13

Reports

Operational reports are available on-demand through the administrative portal of the system. These reports:

- Summarize the SAN configuration, violations, and utilization.
- Report on specific devices, such as EMC Symmetrix storage devices.
- Identify violation trends in the configuration..
- Report changes.
- Display task pre-validation information.

This chapter describes the reports, and provides instructions to generate them.

13.1 Accessing the Reporting Capabilities

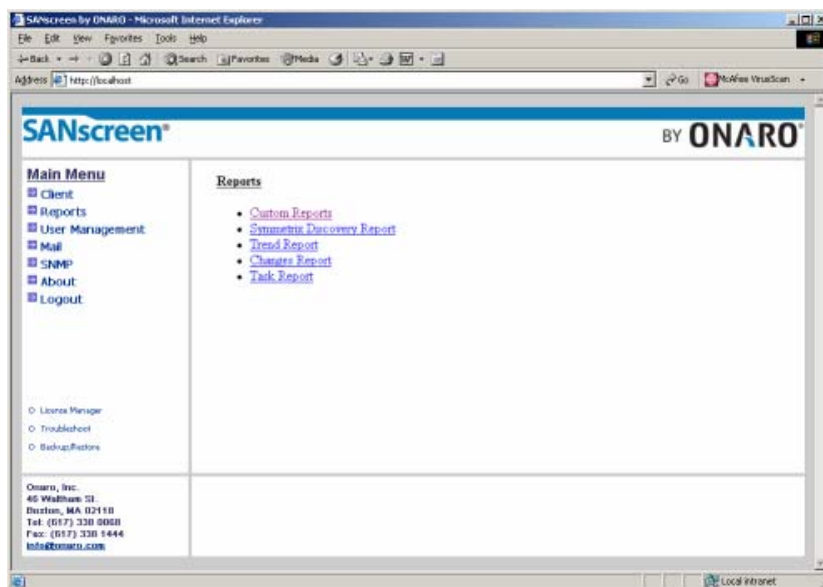
To generate the reports, first open the administration portal by entering the following URL to any Web browser. The port number will be either 80 or 8080, as configured at when the server was installed:

`http://<SANscreen_hostname>:<SANscreen_port>`

If you're accessing the client from the SANscreen server, enter:

`http://localhost`

With the portal screen open, click the Reports link from the main menu:

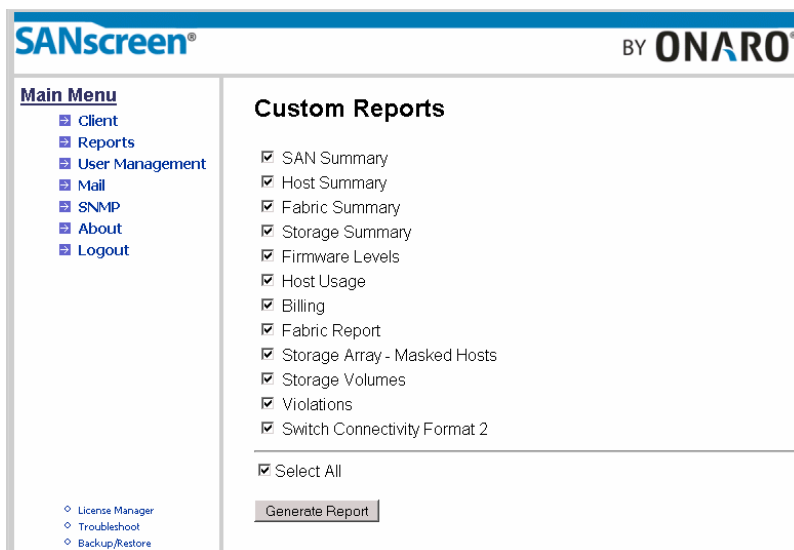


Then select the category of report you want. Refer to the page number referenced below for further details about each report.

Report Category	Description	See page...
Custom Reports	Summarizes the state of your SAN.	189
Symmetrix Discovery Report	Details all discovered Symmetrix storage devices.	192
Trend Report	Identifies violation trends in your SAN configuration.	193
Changes Report	Summarizes the SAN access and inventory information, and reports all device-configuration changes for a specified time frame.	194
Task Report	Pre-validates planned tasks.	196

13.2 Custom Reports

Select one or more custom report(s) from the list provided, then click Generate Report. Use Select All to request all the reports at once:



The screenshot shows the SANscreen web interface. At the top, the logo "SANscreen®" is on the left and "BY ONARO®" is on the right. Below the logo, there is a "Main Menu" section with a list of links: Client, Reports, User Management, Mail, SNMP, About, and Logout. Below this list, there are three links: License Manager, Troubleshoot, and Backup/Restore. The main content area is titled "Custom Reports" and contains a list of reports with checkboxes next to them: SAN Summary, Host Summary, Fabric Summary, Storage Summary, Firmware Levels, Host Usage, Billing, Fabric Report, Storage Array - Masked Hosts, Storage Volumes, Violations, and Switch Connectivity Format 2. Below this list, there is a checkbox for "Select All" and a "Generate Report" button.

SANscreen generates the reports into an Excel file (*report.xls*), then prompts you to save the file. Assign a unique name, to avoid overwriting older reports.

Each page of the Excel spreadsheet contains a different report. Click each page, in turn, to view the requested reports.

Report	Description																																						
SAN Summary	Summary of your SAN environment, including a fabric summary, a storage summary, and a logical analysis summary (i.e., paths and violations). <table> <tr> <td colspan="2">SAN Summary</td></tr> <tr> <td colspan="2">Fabric Summary</td></tr> <tr> <td>Number Of Fabrics</td><td>3</td></tr> <tr> <td>Number of Switch devices</td><td>7</td></tr> <tr> <td>Number of available switch ports</td><td>112</td></tr> <tr> <td>Number of active switch ports</td><td>84</td></tr> <tr> <td>Switch port utilization (%)</td><td>75</td></tr> <tr> <td colspan="2">Storage utilization Summary</td></tr> <tr> <td>Number of storage devices</td><td>4</td></tr> <tr> <td>Total capacity TB</td><td>0.74</td></tr> <tr> <td>Used capacity TB</td><td>0.63</td></tr> <tr> <td>Available capacity TB</td><td>0.12</td></tr> <tr> <td>Orphaned LUNs TB</td><td>0.02</td></tr> <tr> <td>Storage utilization (%)</td><td>84.2</td></tr> <tr> <td colspan="2">Logical Analysis Summary</td></tr> <tr> <td>Number of logical paths</td><td>86</td></tr> <tr> <td>Total reached capacity TB</td><td>0.63</td></tr> <tr> <td>Total violations TB</td><td>0.11</td></tr> <tr> <td>Violation (% of reached capacity)</td><td>17.3</td></tr> </table>	SAN Summary		Fabric Summary		Number Of Fabrics	3	Number of Switch devices	7	Number of available switch ports	112	Number of active switch ports	84	Switch port utilization (%)	75	Storage utilization Summary		Number of storage devices	4	Total capacity TB	0.74	Used capacity TB	0.63	Available capacity TB	0.12	Orphaned LUNs TB	0.02	Storage utilization (%)	84.2	Logical Analysis Summary		Number of logical paths	86	Total reached capacity TB	0.63	Total violations TB	0.11	Violation (% of reached capacity)	17.3
SAN Summary																																							
Fabric Summary																																							
Number Of Fabrics	3																																						
Number of Switch devices	7																																						
Number of available switch ports	112																																						
Number of active switch ports	84																																						
Switch port utilization (%)	75																																						
Storage utilization Summary																																							
Number of storage devices	4																																						
Total capacity TB	0.74																																						
Used capacity TB	0.63																																						
Available capacity TB	0.12																																						
Orphaned LUNs TB	0.02																																						
Storage utilization (%)	84.2																																						
Logical Analysis Summary																																							
Number of logical paths	86																																						
Total reached capacity TB	0.63																																						
Total violations TB	0.11																																						
Violation (% of reached capacity)	17.3																																						
Host Summary	Lists all host devices in the SAN, including a count of the following for each host: ports on the device, logical paths, total allocated capacity (GB), and violations involving the host.																																						
Fabric Summary	Lists all fabrics in the SAN, including the switches that are members of the fabric (one line per fabric/switch combination). For each switch, this report includes the firmware version, the number of ports in the fabric, and of those, the number of ports that are in use currently (i.e., defined in a logical path).																																						
Storage Summary	Lists all storage devices in the SAN, including the vendor, model number, microcode version, and a utilization summary (total capacity, allocated capacity, orphaned LUNs, and number of ports).																																						
Firmware Levels	Includes one line per host, and reports the OS, HBA vendor and model, HBA firmware version, and the firmware version of the connected switch. This report is used to analyze compliance when performing a firmware upgrade for either a switch or an HBA.																																						
Host Usage	Reports storage utilization by host (one row per host), with all the storage devices that are accessed by each host reported to the right. Includes the number of host ports, number of logical paths for the host, and allocated capacity used by the host per storage device (GB). This report is used to analyze host use of a particular storage device.																																						

Report	Description
Billing	Detailed view of storage utilization, by host — together with the cost of that storage. Also includes the Tier-1 and –2 cost per GB.
Fabric Report	One row for each switch port that's a member of a fabric. Identifies the fabric, switch (including firmware version), and port. For each port, the report identifies the connected device. This report is used to find out where a specific device is connected, and/or to locate a free switch port.
Storage Array – Masked Hosts	
Storage Volumes	Lists each storage device, together with the microcode version for that device, and volume information (volume identifier, capacity, type, and redundancy).
Violations	
Switch Connectivity Format 2	Lists all the end-point servers in the SAN, and their connectivity (HBA WWN, HBA switch-port numbers, and assigned storage port).

13.3 Symmetrix Discovery Report

The Symmetrix Discovery Report option creates and Excel-formatted report for every Symmetrix device in your SAN, and downloads the reports to you as a single zip file. Unzip the files to view them.

Each report details the configuration settings for the storage device, as shown below for device Sym-02123. There's one row for each volume on the device:

Sym Vol	Alternate-Vol	Type				Spc Typ	Size CYL	Size GB	Se
		M1	M2	M3	M4				
0000		Data	Data	N/A	N/A	VCMDB			0edm3-Pool0-stgeb03
0001		Data	Data	N/A	N/A	Volume			0ktasp71
0002		Data	Data	N/A	N/A	Volume			0ktasp71
0003		Data	Data	N/A	N/A	Volume			0ktasp71
0004		Data	Data	N/A	N/A	Volume			0ktazd72 / ktasp72
0005		Data	Data	N/A	N/A	Volume			0ktazd72 / ktasp72
0006		Data	Data	N/A	N/A	Volume			0ktasp71
0007		Data	Data	N/A	N/A	Volume			0ktasp116
0008		Data	Data	N/A	N/A	Volume			0ktasp116
0009		Data	Data	N/A	N/A	Volume			0ktasp116
000A		Data	Data	N/A	N/A	Volume			010:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17:8B / ktasp
000B		Data	Data	N/A	N/A	Volume			010:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17:8B / ktasp
000C		Data	Data	N/A	N/A	Volume			010:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17:8B / ktasp
000D		Data	Data	N/A	N/A	Volume			010:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17:8B / ktasp
000E		Data	Data	N/A	N/A	Volume			0ktazd418 / 10:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17
000F		Data	Data	N/A	N/A	Volume			0ktazd418 / 10:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17
0010		Data	Data	N/A	N/A	Volume			0ktazd418 / 10:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17
0011		Data	Data	N/A	N/A	Volume			0ktazd418 / 10:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17
0012		Data	Data	N/A	N/A	Volume			010:00:00:00:C9:2A:16:43 / 10:00:00:00:C9:2A:17:8B
0013		Data	Data	N/A	N/A	Volume			0ktasp72 / ktazd72
0014		Data	Data	N/A	N/A	Volume			0ktasp72 / ktazd72

The report includes the following fields:

Field	Description
Sym Vol	Volume number reported on this line (hexadecimal).
Alternate-Vol	Not used.
Type (M1,M2,M3,M4)	Mirror set for the volume.
Spc Typ	Specialty type.
Size CYL	Number of cylinders in the volume.
Size GB	Size of the volume, in gigabytes. For a meta volume, this is the total size of the meta (vs. individual member size).

Field	Description
Server	Name of each host server that's masked to this volume (slash separated). Displays the WWN for the server if the name is not available.
OS Type	Operating system for each server (slash separated, and in order to correspond to the Server list).
FA (Hex Lun #, Dec Lun #)	Mapped Logical Unit Numbers for each FA on the device, presented in order left-to-right according to the <i>Symmetrix FA Rule 17</i> . The LUNs are provided in hexadecimal (Hex) and decimal (Dec) format.
Meta Head	Applicable if the Spc Type field is Meta. Meta head number for the virtual volume represented by this line.
Meta Mem Num	Applicable if the Spc Type field is Meta. Meta rank (i.e., index) level for each meta member, presented in order as the volumes are defined in the meta volume.
UCB	Not used.
BCV / RDF Device Group	Not used.
BCV / RDF Composite Group	Not used.
Comments	Not used.

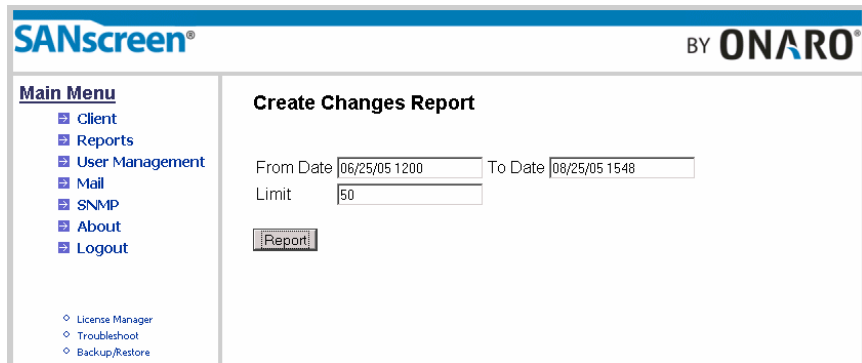
13.4 Trend Report

The trend reports are not used in the current release.

13.5 Changes Report

The Changes report summarizes the current access and inventory information for your SAN, then lists the device-configuration changes that occurred during the reported time frame. Follow these steps to request the Changes report:

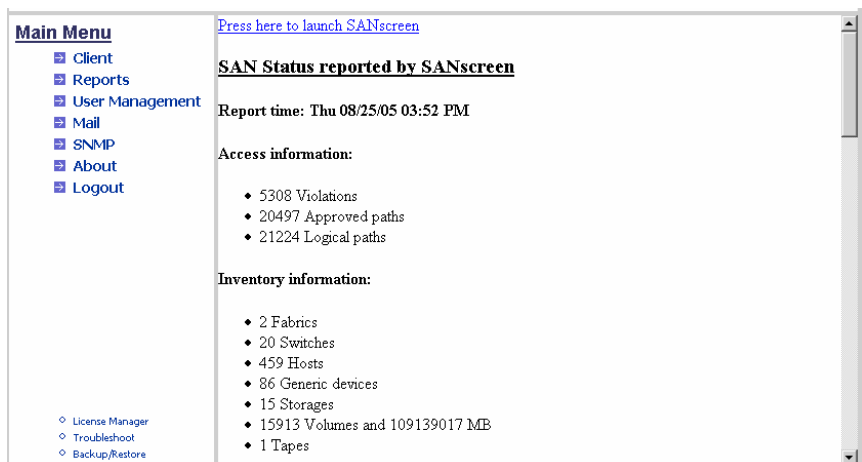
1. Select the From and To dates for which to report the changes (*mm/dd/yy hhmm* format, on a 24-hour clock):



The screenshot shows the SANscreen interface with the 'Create Changes Report' form. The form includes a 'Main Menu' on the left with links to Client, Reports, User Management, Mail, SNMP, About, and Logout. Below the menu are links for License Manager, Troubleshoot, and Backup/Restore. The main form area has a title 'Create Changes Report' and two input fields for 'From Date' (06/25/05 1200) and 'To Date' (08/25/05 1548). There is a 'Limit' input field set to 50 and a 'Report' button.

2. Specify the maximum number of changes you want to see (defaults to 1000).
3. Click Report.

SANscreen generates the report and displays it in the portal window. The top of the report gives the current date and time, a summary of access information (violations, APLs, and logical paths), and a summary of the current inventory:



The screenshot shows the SANscreen report output. It includes a 'Main Menu' on the left with links to Client, Reports, User Management, Mail, SNMP, About, and Logout. Below the menu are links for License Manager, Troubleshoot, and Backup/Restore. The main report area has a title 'SAN Status reported by SANscreen' and a 'Report time: Thu 08/25/05 03:52 PM'. It lists 'Access information' (5308 Violations, 20497 Approved paths, 21224 Logical paths) and 'Inventory information' (2 Fabrics, 20 Switches, 459 Hosts, 86 Generic devices, 15 Storages, 15913 Volumes and 109139017 MB, 1 Tapes).

A prompt at the very top (Press here...) lets you launch the SANscreen client.

The next part of the report lists all the changes for the reported time period:

The screenshot displays the SANscreen web interface. At the top, the logo "SANscreen®" is on the left and "BY ONARO®" is on the right. Below the logo, there is a "Main Menu" section with links: Client, Reports, User Management, Mail, SNMP, About, and Logout. Below this menu, there are links for License Manager, Troubleshoot, and Backup/Restore. The main content area is titled "New Changes detected by SANscreen". It shows a "Time interval from: Mon 04/25/05 12:00 PM to Thu 08/25/05 03:52 PM" and a "Change Time :Mon 06/13/05 04:48 PM". Below this, there is a section titled "Device configuration change List" which contains a list of configuration changes for various devices, including fabric and generic devices, with specific IP addresses and timestamps.

SANscreen® BY **ONARO®**

Main Menu

- Client
- Reports
- User Management
- Mail
- SNMP
- About
- Logout

License Manager
Troubleshoot
Backup/Restore

New Changes detected by SANscreen

Time interval from: Mon 04/25/05 12:00 PM to Thu 08/25/05 03:52 PM

Change Time :Mon 06/13/05 04:48 PM

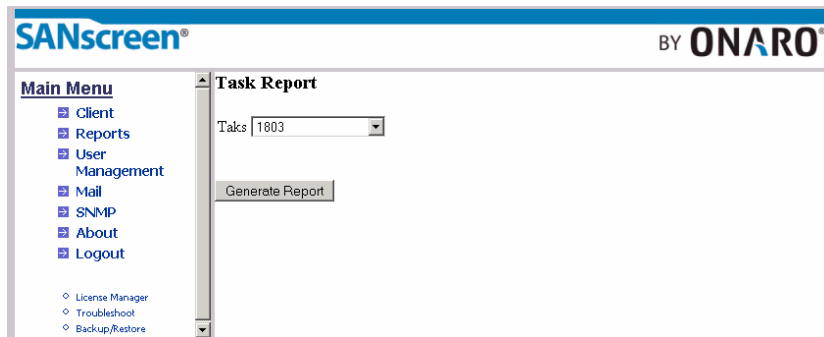
Device configuration change List

- Configuration changed in fabric [FA-CORCNX09-D1](#) on principal [FA-CORCNX09-D1](#) ([FA-CORCNX09-D1](#))
- Configuration changed in fabric [FB-CORCNX09-D2](#) on principal [FB-CORCNX09-D2](#) ([FB-CORCNX09-D2](#))
- Configuration changed in generic device [50:06:04:8A:CC:19:74:39](#)
- Configuration changed in generic device [50:06:04:8A:CC:19:74:38](#)
- Configuration changed in generic device [50:06:04:8A:CC:19:74:37](#)
- Configuration changed in generic device [50:06:04:8A:CC:19:74:36](#)
- Configuration changed in generic device [50:06:04:8A:CC:19:74:29](#)

13.6 Task Report

The Task Pre-Validation Report lets you see detailed information about any task defined to SANscreen. Please refer to Chapter 10 for information about task planning.

To generate the report, select the task to pre-validate from the drop-down list, then click Generate Report:



SANscreen displays the results in the portal window. The top of the report shows the basic task information. The bottom lists the actions defined for the task, together with a pre-validation status for each action.



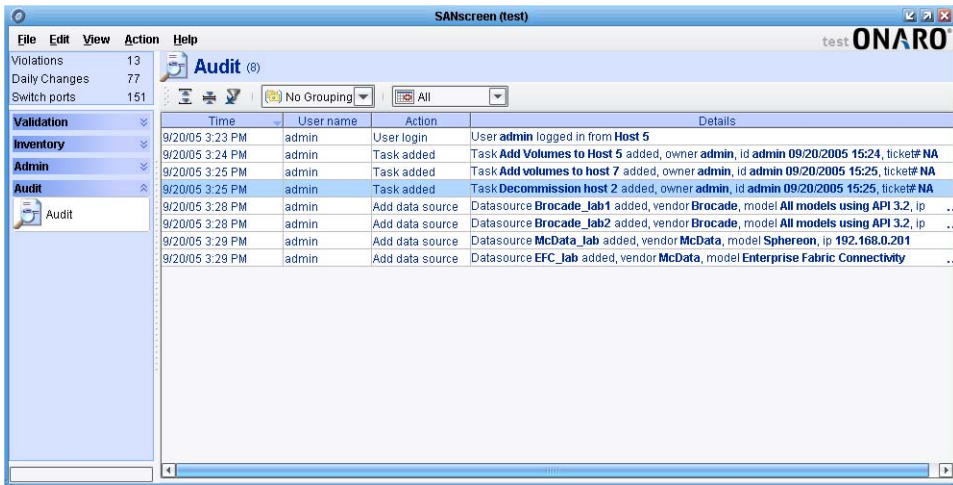
Chapter 14

Auditing User Activities

SANscreen generates audit entries for any user activities that affect the SAN or its management, including:

- User login
- Authorizing/unauthorizing a path.
- Updating an authorized path.
- Setting thresholds.
- Adding/removing a Data Source.
- Starting/stopping a Data Source.
- Updating data source property values.
- Adding/editing/deleting a task.
- Adding/removing hosts from a cluster.
- Removing a cluster.
- Identifying/unidentifying/changing identification for a generic device.

Open the Audit screen by clicking the Audit icon  from the navigation tree (Audit category):



For each activity, the display includes:

Field	Description
Time	Date and time the activity took place.
User Name	User who performed the activity.
Action	Brief description of the activity performed.
Details	Activity-specific details, including attributes set, as appropriate.

Use the left-most drop-down to group the report — by user name or activity type. Use the calendar  drop-down tool to limit the report to specific dates, referring to page 78 for instruction, as necessary .

Appendix A

Copyright Notices

This product includes and/or is shipped with code that's copyrighted by the third parties listed below. Further copyright and license information for open source code is included in the documentation.

This product includes code licensed from RSA Security, Inc.

Some portions licensed from IBM are available at
<http://oss.software.ibm.com/icu4j/>

This product includes software designed by the [MX4J project](#). Copyright © 2001. MX4J. All Rights Reserved.

This product includes software developed by the Apache Software Foundation. Copyright © 1999-2003 the Apache Software Foundation. All Rights Reserved.

This product includes software developed by Intalio Inc. Copyright © 2000-2002 Intalio Inc. All Rights Reserved. ExoLab Project (www.exolab.com).

This product includes JoeSNMP – SNMPv1 & v2 compliant libraries for Java. Copyright © 1999-2001 Oculan Corp. All Rights Reserved.
Copyright © 2001-2003 INCORS GmbH - All Rights Reserved.
Copyright © 1999 the Apache Software Foundation. All Rights Reserved.
Copyright © 2002-2003 ymnk, JCraft, Inc. All Rights Reserved.

This product includes software developed by the JDOM Project (<http://www.jdom.org/>). Copyright © 2001 Brett McLaughlin & Jason Hunter. All Rights Reserved.

This project includes the Ino software package developed by Jordan Russell. Copyright 1997 – 2003 Jordan Russell. All Rights Reserved.

The contents of this file are subject to the Mozilla Public License Version 1.0 (the “License”). You may not use this file except in compliance with the License. You may obtain a copy of the License at
<http://www.mozilla.org/MPL/>.

Software distributed under the License is distributed on an “AS IS” basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.

The Original Code is used.

Appendix B

Host Resolution Algorithms

This appendix documents the algorithms used by SANscreen to extract a host name for a generic device. The host name is determined from the names of all zones that the generic device is a member of. The processing varies, depending on whether you are using the **delimiter technique** or the **RegExp technique**. Please refer to *Section 11.1 Identifying HBA Devices via Host Resolution* (page 162) for information about how to set up host resolution.

B.1 Delimiter Technique Algorithm

SANscreen proceeds as follows to extract a host name using the delimiter technique:

1. List all the zone names of which the generic device is a member.
2. Split each zone name into *tokens*, based on the delimiter(s) specified with the host-resolution preferences (see page 163). Split the zone names first using the first delimiter specified, then using the second delimiter, and so forth until you have used each delimiter. If you specified two delimiters, each zone name will be split twice.
3. Create a list of possible host names, using every combination of adjacent tokens. For example, for zone `site_host-3_access-building3`, and an underscore delimiter, the list of host names would be:

```
Site
Host-3
Access-Building3
Site_host-3
Host-3_Access-building3
Site_host-3_Access-building3
```

If we had a second dash (-) delimiter, these additional names would be added to the list:

site_host
3_access
building3
site_host-3_access
3_access-building3
site_host-3_access-building3

SANscreen includes as potential host names only those substrings that can be formed from *all* the zone names. Any substrings that can only be formed using some — but not all — zone names are dropped. For example, in our example above, if the device belonged to another zone called zone site_host-3_access-building4, SANscreen would drop any names that included “building3” or “building4.”

4. Drop any potential host names that are shorter than the minimum length specified with the host-resolution preferences (system default is three characters).
5. Sort the list of potential host names from the longest to the shortest, with the longest at the top (i.e., checked first in the next step).
6. For each name in the list, perform a DNS lookup, first using no domain name.

Note: SANscreen uses the DNS server(s) configured for the system it’s running on.

If the DNS lookup comes up with a match to the host name, mark the generic device as resolved, and update its host name and IP address. If more than one IP address is configured for the host, use the one with the smaller hash code.

7. If no match is found, repeat the DNS lookup for each name in the list, but using the domain names specified with the host-resolution preferences (one name at a time starting with the first name). Mark the host as resolved at the first match.

B.2 Regular Expression Technique Algorithm

SANscreen proceeds as follows to extract a host name using the RegExp technique:

1. For the first regular expression that matches all the zone names for the generic device, use the replacement string — including the prefix and suffix, if configured — to construct the potential host name from the zone name(s). For example, for zone `AAA_host3_BBB`, assuming the RegExp extracted `“host3”`, a Format of `oracle_/1` would result in a potential host name of `oracle_host3`.
2. If validation is configured, perform a DNS lookup for the extracted host name. If the DNS lookup comes up with a match, mark the generic device as resolved, and update its host name and IP address. If more than one IP address is configured for the host, use the one with the smaller hash code.
3. If validation is not configured, mark the generic device as resolved and update the host name. Insert the host name in the IP field as well.

A

- about SANscreen, 1–2
 - icon summary, xiii
 - navigation tips, xvii–xx
 - quick start instructions, xii
- accessing the SANScreen client, 4–6
- acquisition
 - devices identified during, 37
 - displaying progress of related tasks, 21
 - information gathered during, 171
 - units, xiii, 7
- acronyms list, xvi
- Action menu
 - described, 22
 - same as right-click menu, xx
- actions, task, 94–95. *See also*
 - planning SAN changes; tasks, for future plans.
 - adding, 100, 111
 - described, 120–59
 - listed for future plans, 94
 - menu options, 96
 - not validating in planning state, 99
 - status of, 116
 - summary of action types, 117–19
 - viewing
 - errors for an action, 114
 - future violations for an action, 114
- administrative icons, summary of, 7
- administrative portal, xii. *See also*
 - Web browser
 - accessing reports from, 187
 - accessing through a Web browser, 5, 187
 - starting the SANscreen client
 - from, 5
- and navigation
 - authorized paths, displaying, 25
- audit icon, 7, 197
- auditing user activities, xii, 197–98
- authorized paths. *See also* authorizing
 - a path.
 - changes, reviewing for, 77
 - deleting, 56
 - described, 1, 49
 - displaying
 - changes for selected, 20
 - topology and changes for, 52–53
 - editing, 56, 118, 142
 - icon used to identify, xiii
 - identifying in
 - path display, 42
 - main table, 49–51. *See also* paths; topology view.
 - authorizing a path from, 54–55
 - deleting authorizing from, 56–57
 - editing authorizing from, 56
 - removing, 56, 118, 144
 - topology view displayed with, 25, 52
- authorizing a path. *See also*
 - authorized paths.
 - auditing, 197
 - from the authorized path list, 54–55

- from the path list, 45–48, 49
- in planning, 118. *See also*
 - authorized paths.
- policy settings, 46–47
- violation if
 - no logical path, 63
 - unauthorized, 64

C

- calendar drop-down tool, 78, 198
- change plan, SAN. *See* planning SAN changes.
- changes. *See also* changes detail pane; detail panes; topology view.
 - deleting authorization after
 - connection changes, 56
 - displaying
 - for selected authorized path, 53, 77
 - for selected device, 65, 77
 - for selected device (host), 179
 - for selected path, 44, 77
 - for selected violation, 77
 - violations as of a change, 17, 78
 - future changes, displaying, 95, 114
 - generating an HTML report of, 81, 194
 - icon used to identify, xiii
 - incomplete marked as work in progress, 47
 - main table, 77–78
 - filtering, 79
 - timestamp for, 78
 - what's included, 78
 - refreshing after, xvii, 8, 22
 - SAN
 - creating violations during, 64
 - looking for vulnerabilities
 - because of, 83
 - planning and pre-validating, 93–116. *See also* planning SAN changes.
 - tracked by SANscreen, 1–2
 - saved when entered, 21
 - stored as history, 8
 - topology view as of a change, 78, 80
 - topology view displayed with, 25
 - used to view corrected violations, 59
- changes detail pane. *See also* detail panes.
 - described, 20
 - timestamp for, 78
 - used to review history for a path or violation, 12
- clusters. *See also* hosts; hosts & clusters; inventory; topology view.
 - adding a host to, 73–74, 90, 179
 - auditing cluster activities, 197
 - described, 176
 - icon used to identify, xiii
 - removing a host from, 179
 - shared volume masking
 - vulnerability, and, 89
 - viewing changes for, 179
 - vulnerabilities related to
 - incomplete cluster volume sharing, 75, 88
- color
 - used to highlight
 - switches in fabric, 11
 - zones in topology, 11, 35
 - used to report status
 - blue, 113
 - green, xvii, 116
 - in the main table, 8
 - of planned task actions, 116
 - of pre-validation, 113
 - port status, 35
 - purple, xvii
 - red, xvii, 113, 116
- copying
 - rows to external applications, 21
 - tasks in planning, 21, 98

customer service, xi

D

Data Sources, 4, 20

- auditing, 197
- configuring, xii
- discovering generic devices using, 182, 183
- displaying information for, 7
- icon used to identify, xiii
- identifying unknown switch/storage ports, 161
- removing, 38

detail panes

- changes
 - description of, 20, 78
 - displayed for
 - authorized path, 52, 53
 - host (inventory), 179
 - path, 43, 44
 - topology detail, 60, 65
 - topology icon, 77–78
- errors (planning), 95, 114
- future changes (planning), 95, 114
- future violations (planning), 95, 113
- icons used to display, xiv
- masking, description of, 18–19
- opening from View menu, 22
- overview of (topology view), 12
- paths, description of, 13
- ports, description of, 14–15
- properties
 - description of, 12
 - generic devices, 183
 - hosts, 178
 - storage, 181
 - switch, 175–76
 - tape, 182
 - zones, 185
- used to
 - investigate violations, 113–14

verify changes, 80

used to view

- generic device details, 171, 183
- host & cluster details, 177
- storage details, 181
- switch details, 174
- tape details, 182
- zone details, 185

violations, description of, 17–18

volumes, description of, 16–17

vulnerabilities, 84

- blocked hosts, for, 85
- disconnected port zone
 - members, for, 86
- disconnected WWN zone
 - members, for, 86
- high fabric port usage, for, 87
- high masking fan-out ratio, for, 87
- high volume allocation, for, 88
- incomplete cluster volume sharing, for, 75, 88
- low fabric port usage, for, 89
- shared volume masking, for, 89
- unused masked volumes, for, 91
- zones, description of, 15–16

detail tabs, 9. *See also* detail panes.

Layers. *See* layers control.

summary of icons, xiv

Topology tab, 9, 25. *See also*

topology pane; topology view.

Views. *See* views control.

devices. *See also* hosts; storage devices; switch devices; tape devices.

changes, reviewing for, 77

connecting, 118, 140

deleting inactive, 38

adapter/controller, 38

disconnecting, 118, 141

displaying properties by hovering,

25, 36. *See also* hovering;

topology view.

- managing via telnet or HTTP, 39
- names, displaying in the topology pane, 10
- revealing in groups, 32
- disk devices. *See* devices; storage devices.
- DNS
 - used for host resolution, 164, 166, 202, 203
- dual-fabric redundancy. *See also* redundancy level, for authorized paths.
- described, 46
- violation if not present, 63

E

- Edit menu, described, 21
- errors
 - differing from future violations, 95
 - icon, xiv
- errors detail pane, 95, 114. *See also* detail panes.
- expand/collapse tools, summary of, xv, 26, 35

F

- fabrics/VSANs. *See also* VSAN; zones.
 - adding a zone to, 118, 135
 - creating groups for, 28
 - displayed for
 - a host in a path, 43
 - a port, 14, 86
 - a switch, 174, 175
 - a zone, 15, 68, 136, 137, 154, 155, 184
 - violations, 62, 69
- Domain ID for, 175
- dual-fabric redundancy
 - described, 46
 - for authorized paths, 51

- violation related to, 63
- highlighting in the topology pane, 11
- icon used to identify, xiii
- importing zone information for, 143
- removing a zone from, 119, 154
- reporting, 190
- specifying for a zone, 135
- thresholds, defining, 85
- vulnerabilities related to
 - blocked host, 85
 - high fabric port usage, 87
 - low fabric port usage, 89
- zones in, highlighting in the topology pane, 10

- File menu, described, 21

- filtering

- by date/time, 78
 - by fabric, 43, 62
 - by volume availability, 111
 - change list, 79
 - column data, xix
 - table data, xiv
 - detail panes, 12
 - violations, planned/not planned, 59

- firewall, using HTTP with, 6
- future changes detail pane, 95, 114.
 - See also* changes; detail panes.
- future violations detail pane, 95, 113.
 - See also* detail panes.
- future violations, differing from errors, 95

G

- generic devices. *See also* HBA;
 - hosts; inventory; storage devices; switch devices.
 - action taken by SANscreen for, 161
 - auditing activities for, 197

- authorization, and, 45, 54
- definition of, 161
- icon used to identify, xiii
- identifying, xii
 - from CSV file, xvi, 170
 - from Generic Device list, 172, 183
 - from Identify screen, 167–70
 - from topology view, 27, 37, 171
 - via host resolution, 162–64, 170
- main table, 161, 182–83. *See also* inventory.
- properties, explained, 183
- removing identification of, 37, 169
- viewing inventory information for, 182
- WWN used to identify zone member, 15
- groups. *See* topology view, groups.

H

HBA

- adding to host, 117, 122, 147
- as generic device, 161, 167. *See also* generic devices.
- host resolution of, 162–64, 170, 201–3
- removing from host, 118
- history of SAN changes, tracking, 2, 78–79. *See also* changes.
- host-port redundancy. *See also* redundancy, host-port.
 - defining for authorized paths, 47
 - violation if not present, 62
- hosts. *See also* clusters; detail panes; HBA; hosts & clusters; inventory; paths; ports; topology view.
 - accessing storage through host ports, 43
 - adding
 - storage to, 108
 - to a cluster, 73–74, 90, 179

- to the SAN, 117, 123
- authorizing access from, 49, 54–55
- auto grouping, and, 31
- creating groups for, 28
- decommissioning, 102, 103
 - using templates for, 97, 108, 111
- displaying
 - masking for selected item, 18
 - volumes for selected item, 16
 - zone-membership for, 67
- icon used to identify, xiii
- importing data from, 4
- masking, and, 84
 - adding masking for, 118, 132
 - removing volume masking, 151
- paths originating from, 9, 13, 41, 42, 45, 50, 61
- properties, explained, 178
- redundancy required for, 46, 47, 51, 61, 62
 - violation if not met, 63
- removing from a cluster, 179
- removing HBA from, 118, 147
- reporting, 190
 - firmware levels, 190
 - storage utilization, 190
- resolution of, automatic, 162–64, 170
 - algorithms used for, 201–3
- SANscreen server installed on, 4
- sharing volumes between, 47, 51
 - displayed for violations, 18
- shutting down, 119, 156
- switch hops from, 43, 47, 51
- vulnerabilities related to
 - blocked host, 85
 - high fabric port usage, 87
 - incomplete cluster volume sharing, 75, 88
 - low fabric port usage, 89
 - masking fan-out ratio, 87
 - shared volume masking, 89

- unused masked volumes, 91
- hosts & clusters. *See also* clusters;
hosts; inventory.
- main table, 176–77
- viewing inventory information for,
176
- hovering over icons for details, 10,
25, 36, 171
- HTML. *See* Web browser.

I

icons

- authorized path
 - in Path display, 13, 42, 48, 55,
91
- device icons in topology view, 9,
28
- displaying labels for, 10
- dragging on screen, 28
- grayed for inactive devices, 38
- hovering over for details, 10,
25, 36
- organizing into groups, 11, 28,
33
- organizing into views, 30
- using to view details, 9, 12, 65.
See also detail panes.
- generic device in topology pane,
161, 171
- hovering over for details, 171
- inventory, displaying properties
for, 21
- navigation, 4, 6–7
- summary of, xiii
- topology view tools, for, 26
- used to expand/contract table
displays, xx
- used to indicate the type of change
made, 20, 78
- violation in Path display, 8, 13, 42,
50

- work-in-progress, used to identify,
13, 43, 51, 62
- identify main table, 167–68
 - using to identify generic devices,
167–70
- inventory, 173
 - displaying
 - changes for selected item, 20,
77
 - masking for selected item, 18
 - paths for selected item, 13
 - ports for selected item, 14
 - properties for selected item, 12,
21
 - volumes for selected item, 16
 - zones for selected item, 15
 - icons, summary of, 7
 - managing devices from main
table, 37
 - via telnet or HTTP, 39

J

- Java Run Time environment
 - required for SANscreen client, 6
 - security window displayed, 6

L

- layers control (topology view), 10
 - displaying current path only, 10,
52, 60
 - displaying links, 10
 - highlighting
 - devices in a zone, 10
 - switches in a fabric, 11
 - including device labels, 10
 - opening the control panel, 22
 - SPF, highlighting, 10
- layouts. *See* topology view.
- LDAP, used to authorize SANscreen
users, 5
- links, 34

- customizing the style for, 27, 35
- displaying properties by hovering, xvii, 25, 36
- Expand mode shown connected to device ports, 35
- highlighting in topology view, 43, 52
- in logical paths, 41
- missing for inactive devices, 38
- toggling display of (topology view), 10
- logical access path, defined, 1, 41. *See also* authorized paths; paths.

M

- magnifying glass view, xvii
- main tables, 4, 25, 59–62
 - Audit List, 198. *See also* auditing user activities.
 - Authorized Path List, 49–51. *See also* authorized paths; paths.
 - Change List, 77–78. *See also* changes; changes detail pane.
 - displaying details for selected item, general, 4, 12
 - Generic Devices, 161, 182–83. *See also* generic devices; inventory.
 - Hosts & Clusters List, 176–77. *See also* clusters; hosts; hosts & clusters; inventory.
 - Identify, 167–68. *See also* identify main table.
 - Inventory. *See also* Inventory.
 - launching action menu from, 22
 - navigation used to display, 6–7
 - overview of, 8
 - Path List, 41–43. *See also* authorized paths; paths.
 - Storage List, 180. *See also* inventory; storage devices.
 - Switch List, 173–74. *See also* inventory; switch devices.

- Tape List, 181. *See also* inventory; tape devices.
- Task List, 94–95. *See also* planning SAN changes.
- viewing generic devices in, 161
- Violation List. *See also* violations.
- Vulnerabilities, 75, 83–84. *See also* vulnerabilities.
- Zones, 184–85. *See also* inventory; zones.
- mapping. *See* volume mapping.
- masking. *See also* masking detail pane; volume mapping; volume masking.
 - icon used to identify, xiv
 - IP network, 175
- masking detail pane, 18–19. *See also* detail panes.
- menus
 - Action, described, 22. *See also* Action menu.
 - Edit, described, 21
 - File, described, 21
 - View, described, 22. *See also* View menu.

N

- navigation
 - auditing, 197
 - authorized paths, displaying, 49
 - changes, displaying, 25, 77
 - generic devices, displaying for identification, 167
 - inventory, displaying, 173
 - paths, displaying, 25, 41
 - plans, displaying, 94
 - through the SANscreen client, 4, 6–7
 - topology view, displaying, 25
 - violations, displaying, 25, 59
 - vulnerabilities, displaying, 75, 83

no-SPF redundancy. *See also*
 redundancy level, for authorized
 paths.
 described, 46
 violation if not present, 63
 violation illustrated, 65

O

overview of
 icons, explained, xiii
 navigation tips, xvii–xx
 quick start instructions, xii
 SANscreen, 1–2
 SANScreen client, 3–4
 accessing the client, 4–6
 main table, 8
 menus, 21–22
 navigation, 6–7
 topology pane, 9–11

P

password
 default to access SANScreen
 client, 5
 to view validation reports, 96
Path Authorization Wizard, 45–48,
 54, 56
paths. *See also* authorized paths;
 topology view.
 authorizing. *See* authorizing a
 path.
 changes, reviewing for, 77
 described, 41
 displaying
 active-only in the topology
 pane, 10
 changes for selected, 20
 topology and changes for, 43–
 44
 icon used to identify, xiii

 main table, 41–43. *See also*
 topology view.
 authorizing a path from, 45–48
 topology view displayed with, 25,
 43
 violations, and, 8, 13, 41, 42, 71
paths detail pane, 13. *See also* detail
 panes; paths.
planning SAN changes, 1, 93
 Action menu for, 95–97
 adding actions, 100, 111
 detailed descriptions of action
 types, 120–59
 general instructions, 117
 summary of action types, 117–
 19
 copying tasks, 98
 creating a change plan, 93, 97–112
 current task status, 99
 defining dependent tasks, 99
 executing the plan, 93, 116
 future changes display, 20, 95, 114
 identifying
 errors, 95, 114
 violations, 93, 95, 113
 importing tasks for, 96, 97, 101–8
 overview of processing, 94–95
 pre-validating changes, 93, 113–
 15
 reporting pre-validation results,
 115, 196
 steps to planning, 93
 using as planning tool
 action wizards, 95, 98–100, 98–
 100, 98–100
 an XML file, 96, 98, 112
 templates, 96, 97, 108–11
plans, icon used to identify. *See also*
 planning SAN changes.
policies. *See* authorized paths;
 authorizing a path.
ports. *See also* fabrics/VSANs; hosts;
 ports detail pane; storage devices;

- switches devices; volume mapping;
- volume masking.
- adding to a VSAN, 117, 125
- color used to reflect status, 35
- connecting, 118, 140
- disconnecting, 118, 141
- displaying
 - detail by expanding, 26, 35
 - detail for selected device, 65
 - properties by hovering, 36
 - zone-membership for devices, 67
- generic device. *See also* generic devices.
 - identifying ports for, 169
 - in inventory display, 182
 - in properties display, 183
 - manually identified, 167, 169
- HBA, 147
 - identifying, 122
- highlighting by zone, 35
- host
 - accessing storage through, 13, 18, 43, 61
 - fabric port usage, 85, 87, 89
 - masking a volume to, 19, 84
 - minimum active for a path, 51
 - redundancy of, 47, 61, 62
 - zone initiators, 184
- icon used to identify, xiv
- mapped, 16
- name displayed for a violation, 68, 69
- name used to identify zone
 - member, 15
- storage
 - accessing a volume through, 19
 - add mapping for, 118, 131
 - add masking for, 118, 132
 - controller, 100, 117, 120, 145
 - remove mapping for, 119, 150
 - remove masking for, 119, 151
 - too many masked hosts, 87
- switch
 - adding to a zone, 118, 136, 137
 - identifying blades/ports on, 127, 128
 - in inventory display, 174
 - in properties display, 175
 - removing from a VSAN, 118, 148, 153
 - verifying a connection, 118, 139
- tape controller, 146
 - identifying, 121
- unidentified as generic devices, 161, 167, 182. *See also* generic devices.
- used to identify SANscreen server, 5
- vulnerabilities related to, 86, 87, 89
- WWN used to identify zone
 - member, 15, 137
- ports detail pane, 14–15. *See also* detail panes; ports.
- progress
 - displaying for acquisition tasks, 21
 - work-in-progress, identifying, xv, 13, 43, 51, 62
- properties
 - detail pane, used to show device properties, 12, 65
 - displayed by hovering over a device icon, 10, 36
 - displaying for inventory icons, 12, 21
 - generic devices, explained, 183
 - host, explained, 178
 - icon used to identify, xiv
 - storage device, 181
 - switch, explained, 175–76
 - tape device, 182
 - zone, explained, 185

Q

quick start instructions, xii

R

redundancy

- host clusters used for, 176
- host-port, 18, 47, 61, 62
- in task templates, 109
- level, for authorized paths, 49, 51, 63, 64, 142
- defining, 46
- volume, 17

refreshing the screen, xvii

- after pre-validation, 113
- automatically after acquiring change info, 8, 22

reports generated through the

- administrative portal, xii, 187–96

reports, custom, 189–91

reserving volumes. *See* volumes, reserving

right-click menus. *See* Action menu

S

SANScreen client, overview of

- window, 3

saved layouts, 35

sharing volumes. *See* volume sharing.

shortcuts. *See* navigation.

single point of failure, displaying in the topology pane, 10. *See also* no-SPF redundancy.

sorting

- column headings, xviii
- detail panes, 12

Start menu, to access SANScreen client, 4

storage devices. *See also* detail panes; devices; inventory; paths; ports; topology view; volume masking; volume mapping.

adding, 118, 126

- masking for, 118, 132
- new volume to, 118, 130
- port controller to, 117, 120
- volume mapping for, 118, 131

as generic devices, 161, 167. *See also* generic devices.

authorizing access to, 54–55

auto grouping, and, 31

displayed for a

- path, 13, 42, 50
- violation, 61, 68, 69
- zone, 185
- zone (count of), 184

displaying

- masking for selected item, 18
- volumes for selected item, 16
- zone-membership for, 67

for a path, 9, 41

icon used to identify, xiii

main table, 180. *See also* inventory; storage devices.

properties, 181

provisioning storage via

- import/export XML file, 112
- templates, 97, 108–11

removing

- a port controller from, 118, 145
- volume mapping from, 119, 150
- volume masking from, 119, 151
- volumes from, 119, 149

reporting, 190, 191

- Symmetrix, 192–93
- utilization by host, 190, 191

shutting down, 119, 157

switch hops from, 51

thresholds, defining, 85

viewing inventory information for, 180

violations related to, 17

vulnerabilities related to

- high volume allocation, 88
- masking fan-out ratio, 87

- shared volume masking, 89
- unused masked volumes, 91
- switch devices. *See also* detail panes; devices; inventory; paths; ports; switch hops; topology view.
 - adding, 118, 127
 - port to a zone, 118, 136, 137
 - ports to a VSAN, 117, 125
 - zone to a fabric, 118, 135
 - allocating to a VSAN, 118, 134
 - as generic devices, 167. *See also* generic devices.
 - auto grouping, and, 31
 - connecting ports, 118, 140
 - disconnecting ports, 118, 142
 - displayed for
 - disconnected port zone
 - member, 86
 - disconnected WWN member, 86
 - high fabric port usage (count of), 87
 - low fabric port usage (count of), 89
 - for a path, 41
 - highlighting switches in a fabric, 11
 - icon used to identify, xiii
 - main table, 173–74. *See also* inventory.
 - no SPF redundancy, and, 46
 - pre-validating zone configuration for, 118, 143
 - properties, explained, 175–76
 - removing
 - ports from a VSAN, 118, 148
 - VSAN from, 119, 153
 - zone from a fabric, 119, 154
 - reporting, 190, 191
 - connectivity report, 191
 - firmware levels, 190
 - shutting down, 119, 158
 - verifying a connection, 118, 139

- viewing inventory information for, 173
- switch hops
 - defining for authorized paths, 47
 - displayed for
 - authorized paths, 51
 - paths, 13, 43
 - violations, 18, 61
 - in task templates, 109
 - violation if too many, 63

T

- tape devices. *See also* detail panes; devices; inventory; paths; ports; storage devices; topology view.
 - adding, 118, 129
 - port controller to, 117, 121
 - as generic devices. *See also* generic devices.
 - auto grouping, and, 32
 - for a path, 41
 - icon used to identify, xiii
 - main table, 181. *See also* inventory.
 - properties, 182
 - removing port controller from, 118, 146
 - shutting down, 119, 159
 - viewing inventory information for, 181
- Task List, main table, 94–95
- tasks, for future plans. *See also* actions, task; planning SAN changes.
 - actions to complete, 94
 - adding a new task, 97–112
 - auditing, 197
 - defined, 97
 - importing from Excel, 96, 97, 101–8
 - menu options, 95
 - pre-validating, xii, 113–15

- tracking execution of, 116
- technical support, xi
- telnet, managing a SAN device using, 27, 39
- templates. *See* planning SAN changes.
- thresholds, setting
 - auditing, 197
 - fabric port usage, for, 85
 - storage devices, for, 85
 - volume masking, for, 84
- time stamp
 - displaying as of a time stamp
 - topology, 78
 - violations, 17
 - in Changes display, 78
 - in main table display, 8
- toolbar. *See* topology view, toolbar.
- topology pane. *See also* topology view.
 - and path processing, 41
 - authorized path processing, and, 52
 - changes processing, and, 77
 - controlling the information shown
 - layers, 10
 - views, 11
 - described, 4, 9–11. *See also* detail panes.
 - displaying
 - current path only, 10, 43, 52, 60
 - device names in, 10
 - links, 10
 - SPF icon, 10
 - highlighting
 - devices in a zone, 10
 - switches in a fabric, 11
 - link style, changing, 35
 - navigation used to display, 6–7
 - overview of, 9–11, 25
 - path processing, and, 43
 - showing/hiding, 25
 - violations processing, and, 60
- topology view. *See also* topology pane.
 - Action menu for, 22, 27, 34, 35
 - changes displayed for selected item, 77
 - detail panes
 - filtering, 12
 - general, 4
 - overview of, 12
 - sorting, 12
 - displaying
 - changes for selected item, 20
 - masking for selected item, 18
 - paths for selected item, 13
 - ports for selected item, 14
 - properties for selected item, 12
 - violations for selected item, 17
 - volumes for selected item, 16
 - zones for selected item, 15
 - groups, 25, 27
 - creating automatically, 31–32
 - creating, defining, deleting, renaming, 28, 32–34
 - focusing on, xv, 26
 - organizing
 - device icons into, 11, 33
 - into views, 30–31
 - hovering over icons for details, 10, 25, 36, 171
 - included with
 - authorized path display, 25, 52
 - changes display, 25, 78, 80–81
 - path display, 25, 43
 - violations display, 25, 65
 - launching action menu from, 22
 - layouts
 - creating, saving, and deleting, 28
 - exporting and printing, 29
 - managing devices from, 37
 - via telnet or HTTP, 39
 - projecting after completion of planned task, 96, 97

- recreating as of a specific timestamp, 78, 80–81
- toolbar
 - expand/collapse tools, xv, 26, 35
 - fish bowl view, xvii
 - magnified view, xvii
 - overview of, 26
 - zoom tools, xv, 26, 34

U

- user
 - authorizing through an LDAP server
 - login requirements, 5
- user name
 - defaulting for
 - planned actions, 100
 - planned tasks, 99
 - SANScreen client access, 5
 - to view validation reports, 96
 - used as default for template ownership, 109

V

- validating. *See also* validation.
 - actions, 100
 - future SAN tasks, xii, 96, 113, 143
 - reviewing results, 113–14
 - SAN, overview, xi, 1–2, 93
 - tasks in planning stages, 99
- validation. *See also* validating.
 - completed tasks, 99
 - icons
 - Authorized Paths, 49
 - Changes, 77
 - Paths, 41
 - summary of, 7
 - Violations, 59
 - Vulnerabilities, 75, 83
 - ignoring tasks during, 97

- report, generating, 115, 196
- requirements, by action type, 117, 120–59

View menu

- Auto Refresh option, xvii, 8
- described, 22
- opening/closing detail panes using, 12

views control (topology view)

- creating groups using, 32–34
- opening the views panel, 22
- organizing
 - device icons into groups, 11
 - groups into views, 30–31
- overview of, 11

violations. *See also* topology view;

violations detail pane.

- affected by policy changes, 78

- analyzing, 2, 66–69, 66–69

- changes, reviewing for, 20, 77

- contrasted to vulnerabilities, 83

- corrected, viewing, 59

- creating when removing

- authorization, 57

- defined, 59

- detail panes, and, 60, 65

- filtering, 59

- flagging SPF if shared switch, 46

- future, identifying, 95, 113

- future, investigating, 113–14

- generic devices responsible for, 162

identifying

- and correcting, xii, 53, 59, 65, 66, 71, 80, 93

- icon used to identify, xiii

- in authorized path display, 49, 50, 52, 53

- in path display, 8, 41, 42, 43

- main table, 59–62

- topology view and, 60, 65

- not tracked for work in progress, 13, 43, 51, 62

- establishing a WIP, 47, 97
 - notification of by SANscreen, 2
 - planned tasks, correlating to, 61, 62, 65, 70
 - topology view displayed with, 25, 65
 - types, explained, 62–64
 - violations detail pane, 17–18. *See also* detail panes; violations.
 - volume mapping. *See also* masking
 - detail pane; volume masking;
 - volumes.
 - adding, 118, 131
 - as path attribute, 41
 - hosts that access mapped port, 87
 - in task templates, 109
 - ports mapped to volumes, 16
 - removing, 119, 150
 - after remove storage, 145
 - restoring after adding a
 - controller, 120
 - HBA, 122
 - host, 123
 - storage, 126
 - volume masking. *See also* masking;
 - masking detail pane; volume mapping; volumes.
 - adding, 118, 132
 - as path attribute, 41
 - changes, displayed, 78
 - in task templates, 109
 - masked hosts, 17
 - removing, 119, 151
 - after remove storage, 145
 - restoring after adding a
 - controller, 120
 - HBA, 122
 - host, 123
 - storage, 126
 - thresholds, defining, 84
 - violations, and, 67
 - vulnerabilities related to
 - high masking fan-out ratio, 87
 - high volume allocation, 88
 - shared volume masking, 89
 - unused masked volumes, 91
 - volume sharing, 51
 - described, 47. *See also* authorizing a path; volumes.
 - displayed for violations, 18
 - volumes. *See also* paths; storage devices; volume mapping; volume masking; volumes detail pane.
 - adding, 118, 130, 149
 - authorizing access to, 49
 - for a path, 13. *See also* paths.
 - icon used to identify, xiv
 - removing, 119
 - reserving, 111, 132
 - vulnerabilities related to, 75, 88
 - volumes detail pane, 16–17. *See also* detail panes; volumes.
 - VSAN. *See also* fabrics/VSANs.
 - adding ports to, 117, 125
 - allocating a switch to, 118, 134
 - enabling a switch for, 128
 - removing, 119, 153
 - removing ports from, 118, 148
 - vulnerabilities. *See also*
 - vulnerabilities detail pane.
 - contrasted to violations, 83
 - icon used to identify, xiii
 - main table, 75, 83–84
 - notification of, 2
 - setting thresholds for, 84–85
 - types
 - described, 85–91
 - summary of, 85
 - vulnerabilities detail pane, 75, 84. *See also* detail panes; vulnerabilities.
- ## W
- Web browser. *See also* administrative portal.

- managing a SAN device using, 27, 39
- opening the administrative portal, 187
- using to access the SANscreen client, 5
- viewing SAN changes with, 20, 81, 194
- viewing validation reports with, 96, 115, 196
- work in progress, identifying, xv, 13, 43, 51, 62

Z

- zones. *See also* fabrics/VSANs; inventory; VSAN; Zones main table; zoning.
 - adding member to, 118, 136, 137
 - adding to fabric/VSAN, 118, 135
 - configuration, enabling, 118, 143
 - detail pane, 15–16. *See also* detail panes.
 - violations, and, 67
 - displaying properties by hovering, 36

- highlighting in the topology pane, 10, 35
- icon used to identify, xiii
- properties, explained, 185
- removing from a fabric, 119, 154
- removing member, 119, 155
- using to identify generic devices, 168
- viewing inventory information for, 184
- Zones main table, 184–85. *See also* inventory; zones; zoning.
- zoning. *See also* zones, Zones main table.
 - changes, displayed, 78
 - enforcement (switch), 175
 - in task templates, 109
 - member identification for
 - switch-port based zoning, 15, 185
 - WWN-based zoning, 15, 185
 - support (switch), 175
 - vulnerabilities related to, 86
- zoom tools, summary of, xv, 26, 34